UNIVERSITY of NICOSIA

Assessing the Performance of Blockchain Protocols: Proposing and Validating a Blockchain Benchmarking Framework (BBF) through Controlled Deployments of XRPL and Ethereum

Marios N. Touloupou

PhD (Doctor of Philosophy) in Business Administration

April 2024

Marios Touloupou

NICOSIA

PhD

2024

UNIVERSITY of NICOSIA

Assessing the Performance of Blockchain Protocols: Proposing and Validating a Blockchain Benchmarking Framework (BBF) through Controlled Deployments of XRPL and Ethereum

Marios N. Touloupou

A thesis submitted to the University of Nicosia

in accordance with the requirements of the degree of

Doctor of Philosophy in the school of Business Administration,

Department of Digital Innovation

School of Business

April 2024

Abstract

The introduction of blockchain technology has brought about a fundamental change in the domain of electronic transactions, providing unparalleled standards of integrity, openness, and consistency. However, a significant research gap has existed about the absence of a versatile and all-encompassing tool for assessing the performance of various blockchain protocols, particularly their Consensus Algorithms (CAs). To address this challenge, this thesis introduces a Blockchain Benchmarking Framework (BBF) that evaluates the efficacy of blockchain protocols in terms of scalability, decentralization, and security.

The thesis starts with the identification of the research problem, followed by the definition of the study's aim and objectives. A systematic literature review (SLR) is undertaken to investigate the progression of blockchain technology, its primary classifications, the function of CAs, and established benchmarking approaches. The assessment emphasizes the absence of a comprehensive, flexible, and robust benchmarking tool, which served as the inspiration for the design and implementation of the proposed BBF. The proposed BBF is then described, including its essential components and design reasoning. Its purpose is to give an impartial and all-encompassing evaluation of blockchain performance, by considering a variety of crucial aspects.

The researcher justifies the experimental research strategy and provides a comprehensive analysis of the data gathering and analysis procedures. The utilization of the BBF in relation to the use cases yields significant observations, while also drawing attention to the constraints and possible enhancements of the BBF itself. The Revised Blockchain Benchmarking Framework (RBBF) is developed in response to the use case results. It targets the shortcomings of the originally proposed framework and provides a more resilient and adaptable instrument for evaluating blockchain protocols.

In the concluding chapter of the thesis, the research findings are synthesized, the theoretical and practical consequences of the study are discussed, and prospective avenues for future research are identified.

Keywords: Blockchain, Consensus Algorithms, XRPL, Ethereum, Byzantine Faults, Double Spend Attack, Node Failure

Acknowledgements

I would like to express my sincere gratitude to the following individuals who have played a significant role in the completion of this Ph.D. thesis:

First and foremost, I am deeply thankful to my parents, Nikos and Antroulla, for their unwavering love, support, and encouragement throughout my academic journey. Their belief in me and their sacrifices have been instrumental in shaping my aspirations and driving me towards success. I am also immensely grateful to my partner, Evgenia, for her constant understanding, patience, and encouragement. Her presence and support have been a source of motivation and inspiration during challenging times.

I extend my heartfelt appreciation to my supervisory team, Prof. Marinos Themistocleous, Dr. Klitos Christodoulou, and Dr. Elias Iosif, for their guidance, expertise, and mentorship. Their deep knowledge, constructive feedback, and dedication have played a vital role in shaping this research work and expanding my intellectual horizons. I would like to thank the faculty and staff of the University of Nicosia for providing a conducive academic environment and access to resources necessary for carrying out this research. Their commitment to excellence in education and research has been an invaluable asset throughout my Ph.D. journey.

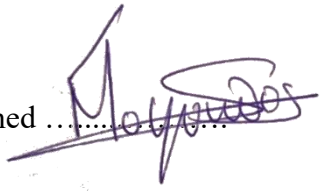
Furthermore, I acknowledge the financial support provided by the University of Nicosia towards this research. Their assistance has been pivotal in ensuring the successful execution of this study. Lastly, I would like to extend my appreciation to all my friends and family members who have stood by me and provided unwavering encouragement and understanding during this demanding endeavor. Completing this Ph.D. thesis would not have been possible without the collective support, guidance, and inspiration from all these individuals. I am truly grateful for their contributions, and I consider myself fortunate to have them in my life.

Thank you all,

Marios

Declaration

I declare that the work in this thesis was carried out in accordance with the regulations of the University of Nicosia. This thesis has been composed solely by myself except where stated otherwise by reference or acknowledgment. It has not been previously submitted, in whole or in part, to this or any other institution for a degree, diploma or other qualifications.

Signed ……  Date: 8/4/2024

List of Publications and Achievements during PhD Thesis Work

This thesis documents the research journey undertaken by Marios Touloupou. The endeavor throughout this PhD thesis has been financially supported by the UBRI project through the grants 2018-188546 and 2021-244121. A few remarkable achievements and presentations derived from this scholarly voyage are listed below:

- The insights of [1] were presented at UBRI Connect 2021, where the innovative methodologies and discoveries were shared with a diverse audience encompassing academic and industry stakeholders.
- The contributions of [2] and [7] were acknowledged for their substantial significance and were honored as part of the UBRI's university research picks.
- The contributions of [6] were conferred an XRPL grant in 2022, furnishing robust support and recognition for the research endeavors.

Journal Articles

[1] **M. Touloupou**, M. Themistocleous, E. Iosif & K. Christodoulou, "A Systematic Literature Review Towards a Blockchain Benchmarking Framework", in IEEE Access, vol. 10, pp. 70630-70644, 2022, Doi: 10.1109/ACCESS.2022.3188123.

[2] CE. Borges, E. Kapassa**, M. Touloupou**, J. Macan, D. Casado-Mansilla, "Blockchain application in P2P energy markets: social and legal aspects" Journal of Connection Science, 2022, https://doi.org/10.1080/09540091.2022.2047157

[3] **M. Touloupou,** K. Christodoulou and M. Themistocleous, "Validating the Blockchain Benchmarking Framework Through Controlled Deployments of XRPL and Ethereum," in IEEE Access, vol. 12, pp. 22264-22277, 2024, Doi: 10.1109/ACCESS.2024.3363833**.**

Book Chapters Papers

[4] Iosif E., Christodoulou K., **Touloupou M**., Inglezakis A. (2020) Leadership Uniformity in Raft Consensus Algorithm. In: Themistocleous M., Papadaki M., Kamal M.M. (eds) Information Systems. EMCIS 2020. Lecture Notes in Business Information Processing, vol 402. Springer, Cham. https://doi.org/10.1007/978-3-030-63396-7_9

[5] **M. Touloupou**, M. Themistocleous, K. Christodoulou, "Designing and Navigating the Future of Blockchain: Innovations, Challenges, and Industry Applications", in Handbook of Blockchain Technology – **In Press**.

Conference Papers

[6] **M. Touloupou**, K. Christodoulou, A. Inglezakis, E. Iosif & M. Themistocleous, "Towards a Framework for Understanding the Performance of Blockchains," 2021 3rd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), 2021, pp. 47-48.

[7] **M. Touloupou**, K. Christodoulou, A. Inglezakis, E. Iosif & M. Themistocleous., (2022) Benchmarking Blockchains: The case of XRP Ledger and Beyond. In: The Hawai'i International Conference on System Sciences (HICSS2021) http://hdl.handle.net/10125/80070

[8] Strepparava, D., Nespoli, L., Kapassa, E., **Touloupou, M**., Katelaris, L., & Medici, V. (2022). Deployment and analysis of a blockchain-based local energy market. Energy Reports, 8, 99-113. https://doi.org/10.1016/j.egyr.2021.11.283

[9] A. Kalafatelis, K. Panagos, A. E Giannopoulos, S. T Spantideas, N. C Kapsalis, **M. Touloupou**, E. Kapassa, L. Katelaris, P. Christodoulou, K. Christodoulou, P. Trakadas (2021, September). ISLAND: An Interlinked Semantically - Enriched Blockchain Data Framework. In International Conference on the Economics of Grids, Clouds, Systems, and Services (pp. 207-214). Springer, Cham. https://doi.org/10.1007/978-3-030-92916-9_19

Table of Contents

List of Tables

List of Figures/Scripts

List of Appendices

Page

Abbreviation Index

BIP	Bitcoin Improvement Proposal
BTM	Automatic Teller Machine for Bitcoin
DAO	Decentralized Autonomous Organization
DPoS	Delegated Proof of Stake
EEA	Enterprise Ethereum Alliance
EIP	Ethereum Improvement Proposal
ERC	Ethereum Request for Comments
EVM	Ethereum Virtual Machine
FA	Fundamental Analysis
LN	Lightning Network
MACD	Moving Average Convergence Divergence
MoE	Medium of Exchange
P2P	Peer to Peer
PoA	Proof of Authority
PoB	Proof of Burn
PoD	Proof of Developer
PoS	Proof of Stake
PoW	Proof of Work
SC	Smart Contract
SegWit	Segregated Witness
SoV	Store of value
TA	Technical Analysis or Trend Analysis

UoA	Unit of Account
UTC	Coordinated Universal Time
WP	Whitepaper
YTD	Year to Date
2FA	Two Factor Authentication
Addy	Address
API	Application Programming Interface
ASIC	Application Specific Integrated Circuit
BFA	Brute Force Attack
Bech32	Bitcoin address format (also known as bc1 addresses)
CPU	Central Processing Unit
BFT	Byzantine Fault Tolerance
DAG	Directed Acyclic Graph
DAPP	Decentralized Application
DDoS	Distributed Denial of Service
DEVCON	Developers Conference
GPU	Graphical Processing Unit
IPFS	Interplanetary Files System
PKI	Public Key Infrastructure
NONCE	Number used only Once

Chapter 1: Introduction

If you tell the truth, you don't have to remember anything.

Mark Twain (1835 – 1910)

Summary

In October 2008, a person or a group of people named Satoshi Nakamoto introduced Bitcoin (Nakamoto, 2008), an innovative decentralized and trusted network that has revolutionized the way we do business and disrupted the markets. In 2009 the Bitcoin blockchain was officially launched while in 2010, the first retail transaction took place, exchanging 10.000 mined Bitcoins for two pizzas. Since then, Bitcoin and blockchain technology have evolved as there has been a pressing need to improve the initial proposal. As a result, the research and community ecosystem have focused on scalability, interoperability, throughput, and latency among others to advance blockchain technology and extend its adoption to real world applications. To better explore this area, the founder of Ethereum (Buterin, 2014), coined the term "Blockchain Trilemma" to discuss the difficulties that developers confront in establishing a blockchain that is scalable, decentralized, and secure without sacrificing on any aspect. To achieve all three elements -Figure *1.1*-, blockchains are frequently required to make trade-offs:

- **Decentralized:** Constructing a blockchain system that is not controlled by a single entity.
- **Scalability:** Referring to a blockchain system's capacity to manage an increasing number of transactions.
- **Security:** Referring to the blockchain system's capacity to perform as planned and defend itself against assaults, errors, and other unforeseen concerns.

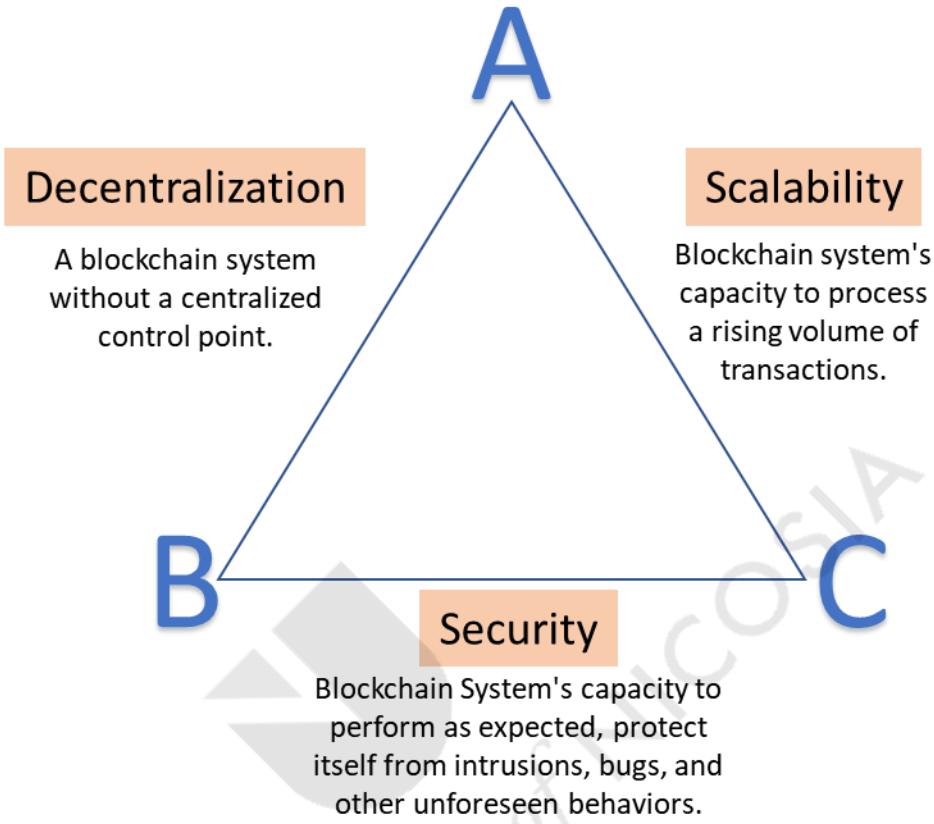


Figure 1.1: The Blockchain Trilemma

Because of this trilemma, throughout the years, an explosion of blockchain propositions appeared that led to a universe of heterogeneous blockchain protocols, each one of them having its own claims about decentralization, scalability and security. Also, each one of them has its own way to manage their faults and Byzantine attacks (Liang *et al.*, 2020) based on its Consensus Algorithm (CA) (Ferdous *et al.*, 2020). As blockchain technology is deployed and applied to new use cases, the number of available chains is expected to rise in the same way that there are so many computer networks in the globe.

As discussed in the literature, there are several claims on different blockchain propositions, however there is a lack of a way of measuring or assessing those claims. Usually, ad hoc tools and experimental settings are used to assess those new propositions (Su et al., 2022). As a result, reproducibility and comparability of these contributions to the current level of the blockchain

technology are difficult (Farooq et al., 2022). Furthermore, there is a lack of documentation, and a methodology for spinning up such networks (setting up the necessary systems and processes for these networks to function effectively) while being able to experiment in a control like environment closed to a real-world case. Finally, it is even more difficult to deploy and scale such networks or structure any experiments in a methodological way (Themistocleous *et al.*, 2020).

This thesis explores blockchain adoption by investigating how the performance of a blockchain protocol is influenced by its corresponding CA under various settings and scenarios. This chapter introduces to the topic of this PhD and it begins by reporting the background to the research problem while also it identifies the current status of the blockchain adoption to the real-world applications. Section 1.1 briefly introduces the problem area and highlights the importance of the CAs within a blockchain protocol, whereas Section 1.2 reports the aim and the objectives of the thesis. Section 1.3 provides an overview of the research methodology adopted in this research, and Section 1.4 presents the outline of the thesis.

1.1 Background to the research problem: performance of blockchains

Distributed Ledger Technology (DLT) is regarded as an append-only database that is consistently shared and synchronized, registering transactions in various places simultaneously (Maull *et al.*, 2017). Unlike traditional databases, distributed ledgers do not require a central authority to certify the validity of data. In DLTs, each node-participant processes and verifies transactions, which are then anchored to the ledger. Additionally, a DLT may be used to document static data (Panwar and Bhatnagar, 2020). Historically, ledgers existed long before the digital age, with information recorded on paper, rocks or other tangible means. As time passed, it became evident that storing data on physical copies in a single location posed significant challenges, especially considering potential disasters such as earthquakes, fires, or floods (S.Mullender, 1993). To counter these challenges, the digitization of data emerged as a solution, with the creation of digital databases that could be stored and backed up in multiple locations (Kozlovski, 2018). However, these centralized digital databases carried their own set

of risks. They were vulnerable to cyber-attacks and data breaches, and the centralization of data also meant a single point of failure.

The need for a more secure and resilient system for managing and storing data led to the emergence of Distributed Ledger Technology, providing a decentralized approach to data management. Blockchain technology, a type of DLT (Natarajan et al. 2017), involves multiple independent computers or nodes to keep synchronized copies of the same ledger. Instead of keeping data in a centralized database, data are distributed into the blockchain protocol where all participants should have the same version. Data in the blockchain consists of a set of transactions appended in a new block, thus expanding the chain. Since several nodes participate in a blockchain, a transparent method of coordinating the nodes/validators is necessary. Therefore, these systems employ agreement algorithms, commonly known as CAs or consensus mechanisms. The concept of CAs was first introduced in the literature related to distributed systems (Ongaro and Ousterhout, 2014; Xiao *et al.*, 2019; Ghaznavi *et al.*, 2020). In 1989, Lamport proposed the Paxos consensus protocol and CA (Lamport, 2001) in the area of fault-tolerant distributed systems.

With the rise of blockchain protocols, CAs have become essential, not just an option, for ensuring agreement on the data and information exchanged within the network (Baliga, 2017a). Although CAs for blockchain systems have been extensively studied (Zhao, Yang and Luo, 2019; Li *et al.*, 2020; Xiao *et al.*, 2020a), the heterogeneity of their integral components has meant that these studies have not yet provided a sufficient level of confidence in the engineering of a *one-fits-all* solution (Heb and Hauck, 2023).

Such algorithms in blockchain protocols can be classified into two categories: a. Proof-based CAs and b. Voting-based CAs according to Nguyen and Kim (2018)). Proof-based CAs were first introduced by Nakamoto. In the latter, Proof-of-Work (PoW) CA is used while the participants attempt to solve a cryptographical puzzle (Tromp, 2014). In the voting based CAs, the participants of the network share the details of the authentication of a new block or transaction before taking a final decision (Li *et al.*, 2020). Such algorithms have been introduced in several blockchain protocols such as the Ripple (XRPL) (*XRP | Ripple*, 2012). The XRPL Community introduced their own version of a Practical Byzantine Fault Tolerance (PBFT)

algorithm called Ripple Protocol Consensus Algorithm (RPCA). Both categories though, are often encounter several challenges such as security, scalability, and energy efficiency (Khosravi and Kavian, 2016; Chaudhry and Yousaf, 2019).

Despite extensive research on the topic of CAs in blockchain systems, there still remains an open research challenge due to the heterogeneity (i.e., diversity) of the integral parts of these systems. The studies mentioned in this section have not been able to provide a solution that can be universally applied to all blockchain systems due to this heterogeneity. Therefore, this thesis investigates issues caused by this heterogeneity. Various research works have been performed discussing the blockchain's issues and challenges related to the consensus mechanisms, such as those of Lin and Liao (2017a); Yeow et al (2018); and Liu et al (2019). Despite extensive research, there remains a gap in knowledge regarding the engineering of CAs (Baliga, 2017b; Chand and Liu, 2020) and in the development of frameworks capable of evaluating their performance across various settings and scenarios (Dinh *et al.*, 2018; Salman, Jain and Gupta, 2019; Xiao *et al.*, 2020a).

1.2 Research Aim and Objectives

1.2.1 Research Aim

Blockchain is a disruptive technology that transforms many industries such as healthcare, academia, supply chain, real estate management etc. (Casino et al. 2019). Initially, a lot of emphasis was given on this technology, mostly because of its link to Bitcoin and other digital currencies. At a later stage, since its characteristics allow its adoption to several domains, blockchain became a reality and it is nowadays already integrated in several industries (Leka et al. 2019). In addition, while blockchain technology creates a system designed to avoid a single point of failure, it raises certain questions due to its decentralized nature. Questions related to the decision-making process or the management of the participants inevitably arise. In contrast, in a centralized organization, decisions are typically made by a single person or a defined group of people. In the case of blockchain, where multiple nodes are spread worldwide, all participants

should comply to the rules set by the CA. In cases where nodes are not aligned with the rules, they will never get rewarded, or they could even get punished by losing their stake.

Consensus Algorithms are a vital part of a blockchain system while they play a crucial role in ensuring the protection and reliability of the latter. Being successful on choosing an appropriate CA for a specific application or use case, can lead towards a significant increase in the performance of the network. For example, Hao et al., (2018) performed an analysis of the latency and throughput of Ethereum and Hyper Ledger Fabric and observed that the CA causes performance bottlenecks. They have also realized that Functional Byzantine Fault Tolerance (FBFT) CA significantly outperforms (PoW) in terms of latency and throughput under different workloads. Sukhwani et al., (2017), examines whether a consensus mechanism utilizing PBFT may be a performance bottleneck for networks with large number of participants. The authors developed a model demonstrating that when the time taken for communication is significantly longer than the time required to read a message – by a factor of ten or more – the average time needed to reach consensus does not substantially alter as the number of network participants ("N") decreases. Moreover, Vukolić, (2016) discusses how the cryptocurrency platforms step away of their original purposes, since blockchain protocols are nowadays used also for the so-called Distributed Applications (dApps). They equate PoW-based blockchains with those built on Byzantine Fault Tolerant (BFT) state machine replication, reflecting on their scalability limitations.

From the above discussion, it appears that CAs play a crucial role in the performance of a blockchain protocol. Several studies have been conducted to identify performance issues that these algorithms may introduce in a blockchain protocol. Even though, to the best of the researcher's knowledge, there is a lack of a systematic analysis of the available CAs and comprehensive work that identifies their key characteristics. Clearly, this is an important gap that requires further investigation. CAs are a critical component of blockchain systems, and their performance under different scenarios and deployment settings is important to understand in order to select an appropriate algorithm for a given use case. Without a comprehensive analysis, it may be difficult to make informed decisions about which CA to use in a particular context. This could potentially lead to suboptimal performance of the blockchain system, such as slower

transaction processing times, higher resource consumption, lower security, or even system failure in extreme cases. Therefore, a systematic analysis and comprehensive work on identifying the key characteristics of CAs would be a valuable contribution to the field of blockchain research and development.

Hence, the aim of this thesis is to:

Investigate the performance of the blockchain consensus algorithms regarding decentralization, security, and scalability. In doing so, proposing a conceptual model to assess the performance of blockchains.

1.2.2 Research Objectives

In order to focus on the aim of this thesis, it is important to accomplish a range of different objectives which are analyzed as follows:

Objective 1: To conduct a systematic literature regarding the performance of blockchain CAs.

Objective 2: To design and implement a conceptual model for measuring the performance of the CAs.

Objective 3: To test and evaluate the proposed conceptual model.

Objective 4: To extrapolate conclusions and provide novel contributions regarding the performance of blockchain CAs.

1.3 Introduction to Research Philosophy and Approaches to Theory Development

1.3.1 Research Philosophy

Scientific research philosophy is a technique that, when applied, helps scientists produce information and ideas within their research domain. The literature discusses four main trends of

research philosophy: the positivist research philosophy, interpretivist research philosophy, pragmatist research philosophy, and realistic research philosophy (Tamminen and Poucher, 2020). In the context of this thesis, the positivist research philosophy is chosen. This choice is grounded on the belief that knowledge arises from observable and measurable phenomena. Positivism focuses on objective and empirical evidence, making it apt for the study of blockchain technology and CAs, which are tangible and quantifiable. Chapter 4 of this thesis delves deeper into the reasoning behind the selection of this research philosophy. Given the ever-evolving nature of blockchain technology and CAs, it is crucial for the researcher to utilize methods and techniques that offer objective and empirical insights, aligning with the beliefs of positivism.

1.3.2 Approach to Theory Development

With the adoption of a positivist research philosophy, the primary approach to theory development in this study is deductive. Deductive reasoning begins with a hypothesis or theory and tests it through empirical research. This approach is commonly employed in quantitative research, especially when the research problem is well-defined, and there are established theories on the subject. The primary objective of this thesis is to investigate the performance of blockchain CAs and propose a conceptual model for measuring their performance. To that end, the deductive approach is primarily used to test the hypotheses formulated based on the proposed Blockchain Benchmarking Framework (BBF) – See Section 3.4.

The goal of this thesis is not just to propose new theoretical frameworks but also to evaluate and validate established theories in the field. As such, the proposed conceptual model and the BBF are rigorously evaluated against current theories to determine their validity and effectiveness. In essence, the approach to theory development in this research predominantly hinges on deductive reasoning, aligning with the objectives and methods of the study. The intention is to further the field of blockchain technology, offering key insights beneficial to both researchers and industry practitioners.

1.3.3 Research Methodology

Quantitative research methodology is well-suited to the field of blockchain technology and CAs because it provides a structured approach to collecting and analyzing data that allows for precise and objective measurement of performance. In the field of blockchain technology, there is a need for empirical research to validate and compare the performance of different CAs. This requires the collection of quantitative data, such as transaction throughput, confirmation time, and security metrics. Quantitative research methodology allows for the collection and analysis of such data using statistical tools and techniques that can provide meaningful insights into the performance of blockchain protocols.

Furthermore, quantitative research methodology allows for the replication of experiments, ensuring the validity and reliability of the findings. This is particularly important in the field of blockchain technology, where the performance of CAs can have significant implications for the security and efficiency of blockchain protocols. In conclusion, while qualitative research methodology may be useful for exploring new perspectives and understanding the context of blockchain technology and CAs, quantitative research methodology is better suited for measuring and comparing the performance of blockchain protocols and CAs.

1.4 Thesis Outline

The structure of this thesis is based upon the methodology described by Phillips, (2000) which includes the following:

- **Background Theory**: This part of the thesis helps the researcher understand and define the research problem, and also presents the state of the art around the field of study. It serves to establish the foundation for the research being undertaken.
- **Focal Theory**: The focal theory section details the researcher's goals and justifications for the research. This includes a thorough description of what the researcher aims to achieve and why the research is being conducted.
- **Data Theory**: The third component, the data theory, justifies the relevance and validity of the material used in the thesis.

- **Novel Contribution**: The final part of the methodology, novel contribution, discusses the potential impact and importance of the thesis for the development principles.

There are seven chapters in this thesis, each of which presents facts and an understanding of the key ideas explored. Figure *1.2* provides an illustration of the thesis outline, and the following paragraphs provide an overview of each chapter's content. The next paragraphs detail the substance of each and the structure of the current edition of this thesis.

Chapter 1: Introduction

The research problem under investigation is introduced in the first chapter. It gives a history of blockchain technology and CAs. In addition, it highlights the need for a deeper comprehension of how the CAs impact the functioning of a blockchain protocol. The research aim and objectives of this thesis are also discussed, while an introduction to the research methodology and the approaches to theory development are concluding this chapter.

Chapter 2: Literature Review – Background Theory

Chapter 2 systematically reviews the literature on blockchain consensus algorithms, fulfilling Objective 1 as outlined in Section 1.2.2. Starting with an introduction in Section 2.1, it details the systematic review process across planning, conducting, and reporting phases (Sections 2.2.1 to 2.2.3), covering aspects like research questions, methodology, literature review, exclusion criteria, study quality, and data analysis. Section 2.3 presents selected articles on blockchain protocol performance and consensus algorithm design. Observations from the literature, including similarities and differences, are discussed in Section 2.4. The chapter also addresses open research challenges and gaps, setting the stage for future investigation (Section 2.5), and concludes with a summary of key insights in Section 2.6.

Chapter 3: Conceptualization of a Blockchain Benchmarking Framework

Research issues derived from the analysis of the literature review are considered in Chapter 3. Those are being used by the researcher to propose the conceptual framework (Objective 2) of this thesis. Through the parts of Chapter 3, the suggested framework, entitled "Blockchain Benchmarking Framework" is presented in depth, including the components that make up the

framework. Moreover, in Section 3.4, a set of research hypotheses are being discussed which they will serve as the foundation for testing and evaluation of the latter.

Chapter 4: Research Methodology

In Chapter 4, the research methodology is discussed in detail, covering the research design, data collection, and data analysis techniques employed in the study. The chapter emphasizes the importance of selecting appropriate research methods and justifying their relevance to the research problem. It elaborates on the choice of a quantitative research strategy and the use of experimental research with use case experiments. This chapter also describes the data sources and sampling techniques, ensuring the validity and reliability of the collected data.

Chapter 5: Empirical Data and Research Findings

Chapter 5 presents the results of the study, providing an in-depth analysis of the data collected in Chapter 4. The findings are organized according to the research objectives and hypotheses outlined in Chapter 3. This chapter utilizes appropriate analytical techniques to examine the performance of various blockchain CAs concerning decentralization, security, and scalability. The analysis offers insights into the strengths and weaknesses of the different CAs and evaluates the effectiveness of the proposed BBF.

Chapter 6: Discussion and Revision

Chapter 6 discusses the findings of the study, interpreting the performance of blockchain CAs in light of the research objectives. The chapter critically examines the empirical results, revises the initial BBF, and proposes the RBBF. The RBBF, refined based on the empirical insights, presents an enhanced tool for benchmarking blockchain CAs, setting the stage for future applications.

Chapter 7: Conclusions and Future Work

The final chapter, Chapter 7, synthesizes the findings of the study and draws conclusions regarding the performance of blockchain CAs and the utility of the proposed BBF. This chapter also discusses the implications of the study for both theory and practice, highlighting its novel contributions to the field of blockchain technology. Additionally, the chapter identifies

limitations of the research and suggests avenues for future research, providing guidance for scholars interested in further exploring the topic or refining the BBF.

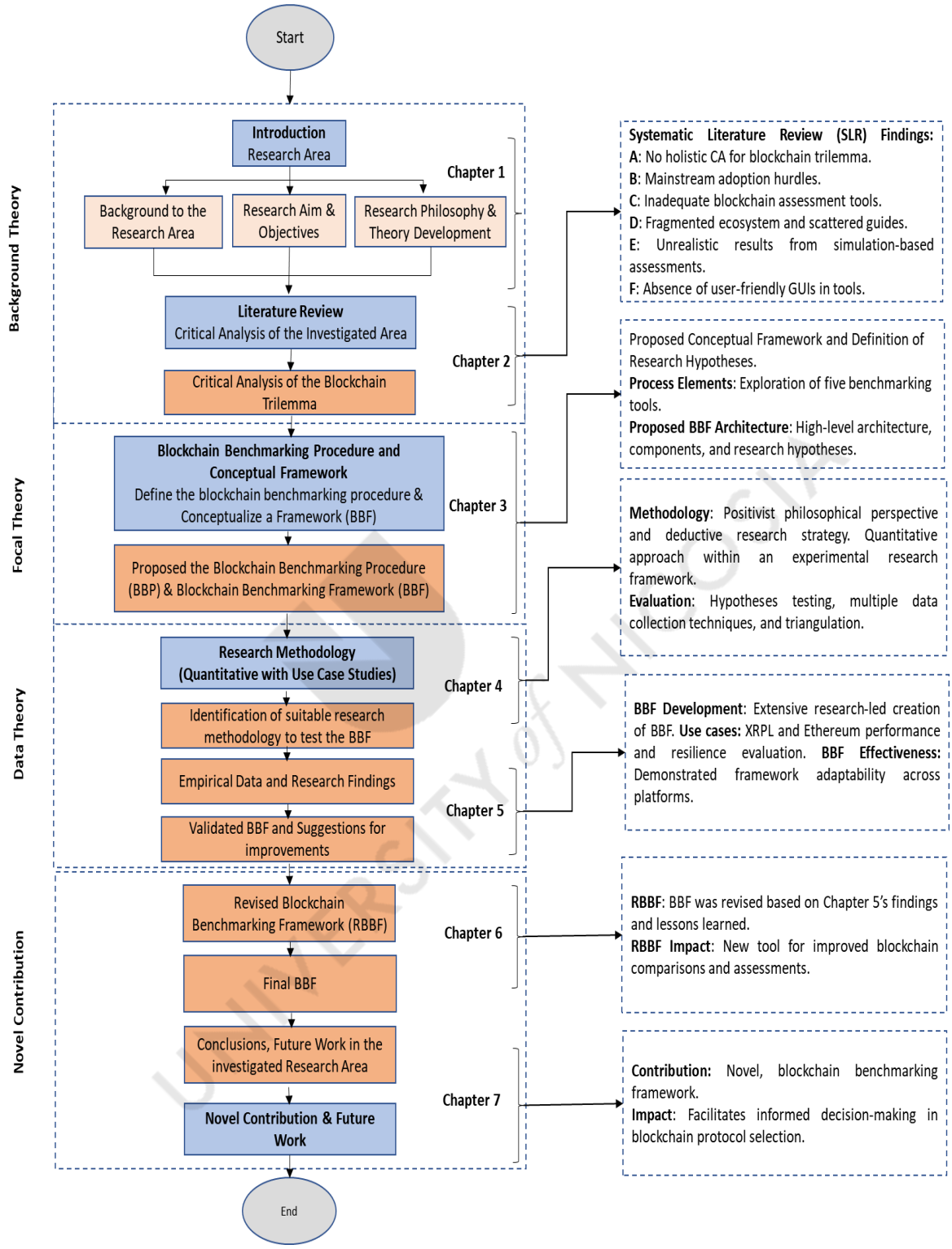


Figure 1.2: Thesis Outline

Chapter 2: Systematic Literature Review

Not everything that can be counted counts, and not everything that counts can be counted.

Albert Einstein (1879 – 1955)

Summary

Chapter 1 introduced the area under research, explained the research problem, and presented the research aim and objectives. To better explore and investigate the area under study, Chapter 2 conducts a systematic literature review to identify research areas for further investigation. Thus, blockchain protocols and how their performance is affected by the CA, are presented. Moreover, various performance measuring approaches are discussed, as they do not provide the expected level of confidence towards a generic solution measuring and assessing the performance of such networks. In addition, the design and implementation of a more advanced solution targeting the assessment of the performance claims of different blockchain protocols, is highlighted. The researcher reviews and analyses the technical aspects of a BBF, since this thesis focuses on the investigation of the performance of blockchain protocols and how the latter is affected by their corresponding CA. In doing so, the limitations of the current approaches are highlighted.

2.1 Introduction

Consensus Algorithm serves as a critical element of any blockchain protocol. The challenges associated with its implementation—primarily scalability and power consumption—pertain to the operation and efficiency of the broader blockchain protocol. Numerous studies, including those presented in (Xiao *et al.*, 2020a), have explored potential strategies to mitigate these challenges. Despite these efforts, the quest for a universally applicable solution—a 'one-size-fits-all' CA—remains elusive. This can be attributed to the diverse requirements of different blockchain applications, complicating the task of engineering a universally effective CA (Vukolić, 2017).

There is therefore a need of a more comprehensive solution, that will investigate the degree to which CAs are built and how they perform. To further investigate this area, the researcher adopts a Systematic Literature Review (SLR) aiming to deliver a clear and comprehensive review of available literature evidence on this topic. Moreover, as stated in (Tina and Sarah, 2019), a systematic literature review would also help to further dive into the corresponding field of study.

Section 2.2 introduces the concept of blockchain protocols and discuss the various types of protocols that exist. It covers the basic principles of blockchain technology and how protocols enable secure, decentralized transactions. In addition, it discusses the evolution of blockchain technology, starting from its inception with Bitcoin to the development of various other blockchain protocols. It also covers the challenges and threats faced by the blockchain industry, such as security issues, regulatory challenges, scalability concerns, and interoperability problems. Section 2.3 focuses on blockchain CAs and how they enable agreement among nodes in a decentralized network. It explains the key characteristics of CAs, such as their fault-tolerance, scalability, and security properties. The chapter discusses different types of CAs, such as PoW, PoS, and Delegated Proof-of-Stake (DPoS). It also covers emerging CAs, such as Proof-of-Authority (PoA) and Proof-of-History (PoH), and their potential impact on blockchain technology. In Section 2.4, the setup of the systematic literature review to be conducted towards the achievement of the objectives of this thesis is presented. Among others, the research

question, the keywords to be used and the databases are also defined, as part of the preparation of the SLR.

2.2 Systematic Literature Review On the Performance of Blockchain Consensus Algorithms

According to (Puljak and Sapunar, 2017), a Systematic Literature Review (SLR) is a suitable and sound approach to be used for a PhD thesis. A systematic literature review attempts 'to identify, appraise and synthesize all the empirical evidence that meets pre-specified eligibility criteria to answer a given research question. The researcher has chosen the SLR for the review of the normative literature (blockchain technology and the performance of the blockchain Cas).

A SLR requires a comprehensive examination of the available sources, the requirements should be explicitly established before the examination of the literature is carried out (Group, 2007). As it is depicted in the Figure *2.1*, the SLR process consists of three phases (Kitchenham *et al.*, 2010). Initially, during the planning phase the researcher identifies the need for conducting a SLR, develops his review protocol and then proceeds with the evaluation of this protocol. During the next phase (Conducting Phase), the search and selection of primary studies takes place, whereafter the researcher proceeds with the extraction of data and their evaluation. Finally, the last step of this phase is to synthesize the extracted data from the previous steps. In the third (3^{rd}) and final phase of this process, the researcher's objective is to disseminate the results extracted during the previous phases 1 and 2.

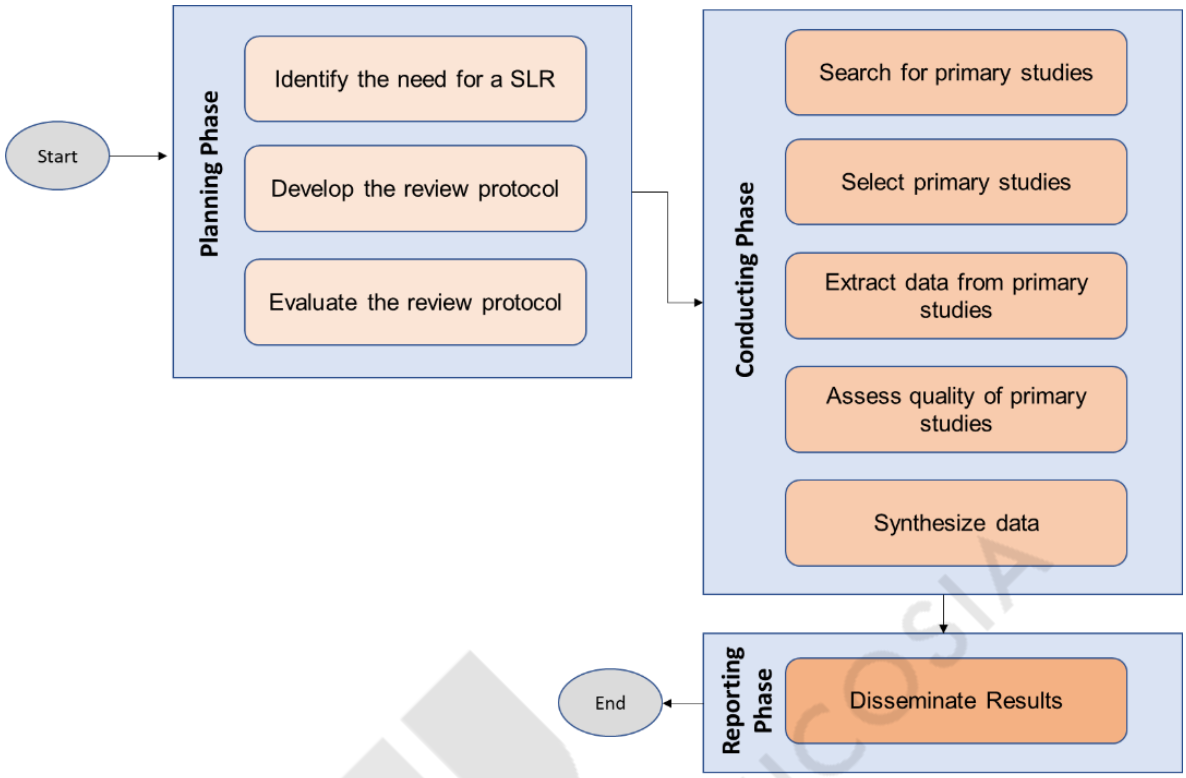


Figure 2.1: Systematic Literature Review – Phases

Phase 1 - Planning:

The initial phase is all about setting the groundwork for the review. The main objective of this phase is to clearly define the intended outcomes and goals of the review. This phase involves the creation of a detailed research protocol that serves as a roadmap for carrying out the review. It encompasses establishing a systematic plan and methodology for conducting the review which includes identifying relevant databases, keywords, and search strategies that guide the subsequent phases.

Phase 2 - Conducting:

This is the most intensive phase of the review process. It starts with the identification of relevant research materials. This involves a thorough search of literature to locate appropriate research materials that align with the review's goals. The selection of case studies is a crucial step at this juncture. Specific inclusion and exclusion criteria are established to guide the selection of studies for review, providing clear justifications for their selection. Quality

assurance of studies is also crucial; this involves setting predefined quality criteria to ensure that only studies that meet these stringent standards are included in the review. After ensuring the quality of the studies, data extraction comes next. It is performed using structured data extraction forms to systematically record and document the outcomes observed by researchers. This methodical process ensures that relevant data are carefully extracted from each selected study.

Phase 3 - Reporting:

The final phase focuses on data analysis and documentation of review outcomes. All the extracted data from the previous phase is analyzed to derive meaningful insights and answer the research questions. This analysis forms the backbone of the review findings. The last step is the documentation of review outcomes. This involves reporting the review outcomes in a comprehensive and detailed manner, articulating the findings, interpretations, and conclusions derived from the review.

2.2.1 Planning Phase

2.2.1.1 Identifying the Research Questions and goals for the review

As discussed in Section 2.2, there is a plethora of blockchain protocols, each one of them providing its own unique mechanisms and characteristics. An open research challenge in blockchain protocols is *how to reach consensus effectively*. According to the blockchain trilemma, when designing a blockchain protocol, one must make a trade-off between different aspects. For instance, one may choose to sacrifice security and decentralization in exchange for achieving faster throughput.

During the initial investigation around the topic of blockchain and Cas conducted so far in this thesis, it is realized that several research challenges and questions are still open. With the choice of conducting a SLR, it is essential to identify and set clear, focused and concise research questions. Thus, this literature review started with the following research question:

- **SLR Research Question:** How do the characteristics of a CA affect the behavior of a blockchain protocol?

The latter is pivotal in understanding the foundational mechanisms of blockchain functionality, and thereby, the broader implications of its various applications. To ensure relevance and precision, the researcher implemented rigorous selection criteria, deliberately filtering out papers with limited scope that don't align with the goals and objectives set forth in Chapter 1. This process ensures that the review remains targeted and thoroughly substantiated by pertinent sources in the field.

2.2.1.2 Research protocol: Establish the methodology to be followed during the review

Blockchain and distributed ledger technologies have emerged as rapidly evolving fields in recent years, garnering significant interest across various industries seeking to leverage their capabilities to address pressing needs. Given the dynamic nature of the topic, the researcher has opted to focus on literature published from 2018 onwards, ensuring that the review captures the most up-to-date developments and insights. In order to accommodate the diverse and rapidly evolving nature of the field, the researcher employs a multivocal systematic literature review approach (Themistocleous *et al.*, 2023). The search encompasses major databases, such as IEEE Xplore Digital Library, ScienceDirect, SpringerLink, and ACM Digital Library, to ensure a comprehensive and high-quality collection of sources. To maintain the rigor and credibility of the literature review, the initial search prioritizes academic journals, conference proceedings papers, book chapters, magazines, and peer-reviewed research articles. This approach ensures that the literature review is grounded in well-vetted and reliable sources.

As part of the multivocal systematic literature review process, the researcher subsequently incorporates non-traditional sources of information, such as white papers, blog posts, conference presentations, and expert opinions. This inclusion of multiple voices and perspectives enrich the understanding of blockchain and distributed ledger technologies, facilitating the identification of trends, gaps, areas of consensus, and points of disagreement. By integrating a wide array of resources and employing a multivocal approach, the literature review fosters a more holistic understanding of the current state of blockchain and distributed ledger technologies, providing valuable insights for future research and applications. This comprehensive review methodology

not only presents a rich picture of the topic under investigation but also serves as a solid foundation for subsequent research endeavors in this rapidly evolving domain.

Identifying Keywords and Search Queries

An initial search of the term 'blockchain' in *IEEE Xplore Digital Library* returns 292,000 results. As for the term 'consensus algorithms' the returned results are 19,900. To narrow down the search results, the researcher focuses on the RQ to identify the keywords described in Table *2.1*, as well as the research queries to be used for the retrieval of any relevant publications with the field of study.

Table 2.1: Systematic Literature Review - Keywords and Search Queries

Keywords	Search Queries
Blockchain, consensus algorithms, Mechanism, Distributed ledger technologies, Benchmarking, Framework, Evaluation,	blockchain AND "consensus mechanisms"
	blockchain AND "consensus algorithms" AND "evaluation frameworks"
	blockchain AND "consensus algorithms" AND "evaluation mechanisms"
	blockchain AND "consensus algorithms" AND evaluation
	"Distributed ledger technologies" AND consensus
	blockchain AND "benchmarking frameworks"

2.2.2 Conducting Phase

2.2.2.1 Conducting the Literature Review

When submitting the search queries in various electronic databases, the number of results obtained differs significantly. For instance, one database like Google Scholar may yield thousands of results, while others like *IEEExplore* may provide fewer results. This variation is attributed to the different database models, which made it not possible to use the exact set of search queries across all databases. As a result, different queries had to be constructed based on the specific model of each database to extract the relevant material. Additionally, the inclusion

criteria are incorporated during the initial search in each library. Starting with the *IEEE Xplore Digital Library*, the following queries are submitted:

1. **Query 1:** (blockchain AND ("consensus algorithms"))
   Results: 525
2. **Query 2:** (blockchain AND ("consensus algorithms")) AND ("evaluation frameworks")
   Results: 11
3. **Query 3:** (blockchain AND ("consensus algorithms")) AND ("evaluation mechanisms")
   Results: 17
4. **Query 4:** (blockchain AND ("consensus algorithms") AND evaluation)
   Results: 61
5. **Query 5:** (("distributed ledger technologies") AND consensus)
   Results: 273
6. **Query 6:** (blockchain AND ("benchmarking framework"))
   Results: 30

The returned results from *IEEE Xplore Digital Library are initially* **875**. As a first step of the screening process, the researcher has removed the papers published before 2018. The latter removed **88** papers from the result set. Moving to the next electronic database, *ScienceDirect*, the researcher submitted the same queries as with the first electronic database. The returned results are **1478**. Similarly, as a first step of the screening process, the researcher has removed **18** papers from the last result set (published before 2018).

1. **Query 1:** (blockchain AND ("consensus algorithms"))
   Results: 565
2. **Query 2:** (blockchain AND ("consensus algorithms")) AND ("evaluation frameworks")
   Results: 21
3. **Query 3:** (blockchain AND ("consensus algorithms")) AND ("evaluation mechanisms")
   Results: 9
4. **Query 4:** (blockchain AND ("consensus algorithms") AND evaluation)
   Results: 451
5. **Query 5:** (("distributed ledger technologies") AND consensus)

Results: 416

6. **Query 6:** (blockchain AND (“benchmarking framework”))

   Results: 16

Following the same approach, *SpringerLink* is the 3rd digital library in which the researcher submitted the above-mentioned queries in which he retrieved **2589** results. Particularly, based on the library’s search model, the following queries are submitted while **85** sources are removed as they were published before 2018:

1. **Query 1:** *with all of the words* “blockchain” AND *with the exact phrase* (“consensus algorithms”)

   Results: 1190

2. **Query 2:** *with all of the words* “blockchain” AND *with the exact phrase* (“consensus algorithms”, “evaluation frameworks”)

   Results: 0

3. **Query 3:** *with all of the words* “blockchain” AND *with the exact phrase* “consensus algorithms”, “evaluation mechanisms”

   Results: 0

4. **Query 4:** *with all of the words* “blockchain”, “evaluation” AND *with the exact phrase* “consensus algorithms”

   Results: 543

5. **Query 5:** *with all of the words* “consensus” AND *with the exact phrase* “distributed ledger technologies”

   Results: 840

6. **Query 6:** *with all of the words* “blockchain” AND *with the exact phrase* “benchmarking framework”

   Results: 16

Finally, *ACM* is the 4th digital library in which the researcher submitted the following search queries using its advance search method. *ACM initially* returned **371** results while a total of **25** papers are removed since they were published before 2018.

1. **Query 1:** (blockchain AND (“consensus algorithms”))
   Results: 189
2. **Query 2:** (blockchain AND (“consensus algorithms”)) AND (“evaluation frameworks”)
   Results: 0
3. **Query 3:** (blockchain AND (“consensus algorithms”)) AND (“evaluation mechanisms”)
   Results: 1
4. **Query 4:** (blockchain AND (“consensus algorithms”) AND evaluation)
   Results: 110
5. **Query 5:** ((“distributed ledger technologies”) AND consensus)
   Results: 63
6. **Query 6:** (blockchain AND (“benchmarking framework”))
   Results: 8

As it is depicted in Table *2.2*, after the first screening process (removing the papers published before 2018), a total of **5097** papers are left for studying. Moreover, Figure 2.2 demonstrates the steps taken towards the identification of the most related sources within the thesis field of study.

Table 2.2: Systematic Literature Review - Initial Results with 1st Screening

Digital Library	**IEEE Xplore**	**ScienceDirect**	**SpringerLink**	**ACM**
Initial Results	875	1478	2589	371
< 2018	-88	-18	-85	-25
Sum	787	1460	2504	346
Total	5097			

The next step of this systematic work is to remove any possible duplicate paper from the search results. In doing so, the search results are imported in (Mendeley), a free reference manager that could help with the storing, organizing, and filtering of the data. During this step, a total of **1755** papers were identified as duplicates and removed. Moreover, in an attempt to further narrow down the search results, the researcher used Mendeley’s search engine to execute a search in

the abstract of each paper to keep the most relevant papers with the thesis's scope. To this end, the following search query is executed removing a total number of **3110** papers:

:abstract:blockchain AND :abstract:consensus AND :abstract:performance

Executing the latter, the researcher managed to filter all papers that do not contain the word "blockchain", "consensus" and "performance" in the abstract of each paper. Eventually, the final result-set is narrowed to 232 papers**.** The final-result set is exported in Comma Separated Values (CSV) format and imported into Microsoft Excel for further analysis. During the initiation of this study, the selection of data handling tools is constrained. Many of the available tools are either not freely accessible, are prohibitively expensive, or are limited in their capabilities. Therefore, Microsoft Excel is chosen for this study, as it presented a cost-effective and widely accessible solution at the time. Excel's familiarity to many users, versatility in data handling, and robust capability to manage the data volume involved in this study made it a suitable choice. Furthermore, its wide compatibility across platforms and devices, along with its ability to produce various graphical representations, ensured that Excel served as an appropriate and efficient tool for the specific requirements of this task. To execute the final filtering of the papers and retain those most relevant to the research topic, the researcher implemented a structured framework based on a set of predefined criteria. These criteria are established in alignment with the research objectives and included factors such as the relevance of the paper's content, the methodological quality, and the publication's impact in the field. The researcher first reviewed the titles and abstracts of each paper in the result set, assessing their relevance to the research topic. Papers that did not align with the research objectives are removed at this stage. Subsequently, the researcher carefully examined the remaining papers' full texts, evaluating their methodological rigor, significance of findings, and overall contribution to the field. This process involved a critical assessment of each paper's strengths and weaknesses, as well as its applicability to the research questions being investigated.

During this filtering process, **145** papers were removed, leaving a final result set of **87** papers. This comprehensive and systematic approach ensured that the selected papers were of high quality and relevance, providing a solid foundation for the literature review and subsequent research endeavors. These are the final papers in which the researcher would study and derive

findings and observations. Figure *2.2* illustrates the steps taken towards the identification of the final sources to be included in the literature review of this thesis.

2.2.2.2 Exclusion Criteria

During the selection process in Phase 2, papers were evaluated to ensure their relevance to the core research purpose outlined in Phase 1. The selection of these papers is guided by specific inclusion and exclusion criteria which have been tailored to align with the research objectives. Here are the main categories of papers that were excluded from this research:

- **Papers with limited scope** Papers with Limited Scope: This review is primarily focused on the comprehensive analysis of CAsin the context of the blockchain trilemma. Consequently, certain papers that did not sufficiently align with this scope were excluded. For instance, papers such as "Blockchain Consensus Mechanisms and Their Applications in IoT: A Literature Survey" (Wen *et al.*, 2020) and "Byzantine fault tolerance based multi-block CA for throughput scalability" (Kim *et al.*, 2020) were excluded. While they provide valuable background information, these papers either had a very narrow focus on specific aspects of blockchain technology or were superseded by more recent and comprehensive research in the field.
- **Articles in non-English language** - During the literature search, several potential resources were retrieved from electronic sources in various languages. Each of these sources are carefully evaluated to assess their potential contribution to the research. However, due to potential inaccuracies in translation, non-English articles were ultimately excluded. This decision is taken to maintain the rigor and accuracy of the research synthesis, as precise translation could not be guaranteed.

As detailed in (Themistocleous *et al.*, 2023), on multivocal literature reviews, the selection process should be as thorough as possible to ensure the selected studies are relevant and contribute meaningfully to the review's objectives. These exclusions, while seemingly limiting, help to focus the research and provide a solid foundation for exploring the research questions more effectively.

2.2.2.3 Ensure Quality of Studies

In accordance with established international academic standards, the utilization of peer-reviewed publications serves as the most appropriate method for evaluating scholarly contributions. Adhering to this principle, the researcher is able to confidently contribute novel concepts and insights to the field, building upon the foundation of previously published works by esteemed scholars within the pertinent research domain.

2.2.2.4 Extract Data

The articles selected for further analysis were used to extract related data on the performance of the blockchain CAs regarding the blockchain trilemma.

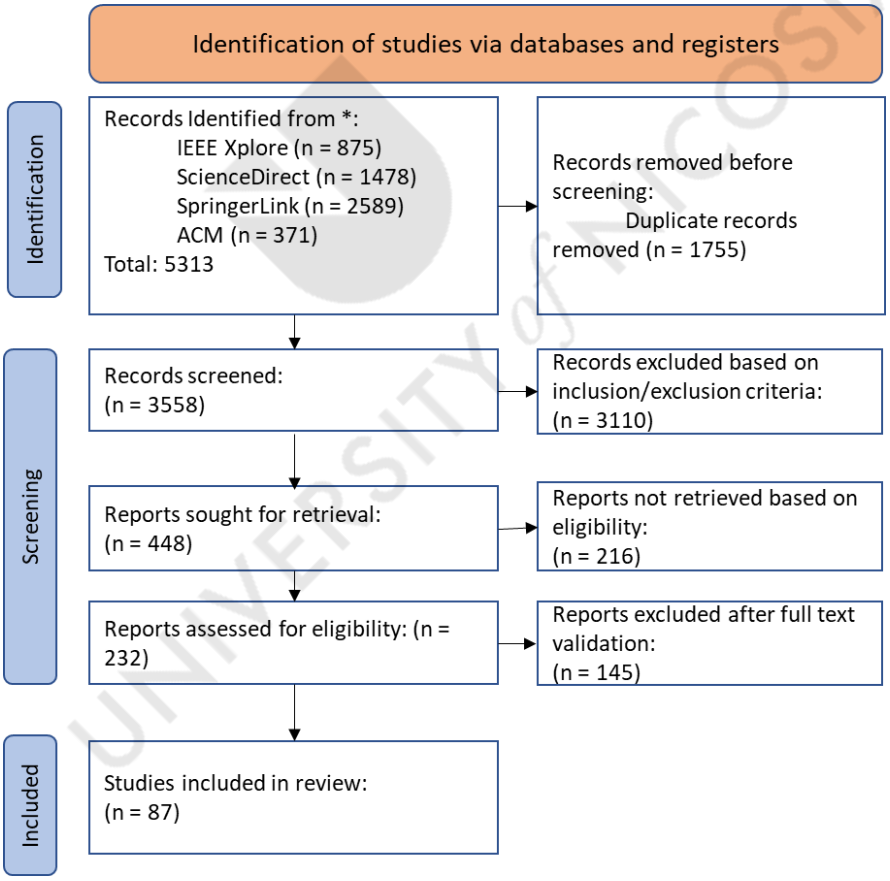


Figure 2.2: Final Sources included in SLR.

2.2.3 Reporting Phase

2.2.3.1 Analyze Data

This phase of the literature review focuses on extracting valuable insights from the research works by employing appropriate qualitative and quantitative methodologies. Qualitative methods were utilized to examine various aspects of CAs can impact the behavior of blockchain protocols, including theoretical approaches and proposals, models, and frameworks. Quantitative methods were employed to determine the frequency of research works addressing each aspect of CA performance in blockchain protocols and to examine deeper into common considerations highlighted by the selected research works.

The outcomes of the review were subsequently documented and reported in Sections 2.5.1 - 2.5.3, encompassing the comprehensive findings of the literature review process.

2.3 Systematic Literature Review Outcomes (2018 – 2021) - Selected Articles

In order to further refine the result set of **87** papers to a more focused selection, the researcher employed a multi-step approach, ensuring a rigorous justification for the final selection. As reported in Chapter 1, the aim of the thesis is to investigate the performance of blockchain CAs concerning decentralization, security, and scalability while proposing a conceptual model to assess the performance of blockchains. Having the research aim and objectives in mind, the researcher employed the following steps to reduce the sample from 87 articles to 14:

1. **Relevance to the aim and objectives:** Each paper in the result set is thoroughly assessed to determine its direct relevance to the aim and objectives of the thesis. Papers that did not contribute significantly to the understanding of the performance of blockchain CAs in terms of decentralization, security, and scalability were excluded.
2. **Methodological rigor:** The researcher evaluated the methodological quality of each remaining paper, ensuring that the studies employed robust research designs, appropriate data collection, and rigorous analysis techniques. Studies with weak methodology or unsubstantiated findings were removed.

3. **Recent and impactful publications:** Given the rapidly evolving nature of the blockchain field, the researcher prioritized recent publications that offered the latest insights into CAs' performance.
4. **Theoretical and empirical diversity:** To ensure a comprehensive understanding of the performance of blockchain CAs, the researcher aimed to include a diverse range of theoretical perspectives and empirical findings. This step involved selecting papers that presented various approaches to measuring performance and provided insights into different aspects of decentralization, security, and scalability.

Following this systematic and rigorous approach, the researcher is able to reduce the sample from 87 articles to 14, ensuring that the final selection is highly relevant, methodologically sound, and diverse, providing a strong foundation for the literature review and subsequent research activities. This carefully justified selection process mitigates the risk associated with the reduction of the sample size and ensures that the final sample offers valuable insights into the performance of blockchain CAs. Table 2.3 presents a compilation of the chosen articles for this research. The table consists of three columns:

1. The first column provides the names of the authors who conducted each research paper.
2. The second column displays the titles of the research articles.
3. The third column offers a concise description of the research work's main focus.

Table 2.3: Literature Review Selected Cases

Authors	Title	Focus
(Ferdous, Chowdhury and Hoque, 2021)	A survey of consensus algorithms in public blockchain systems for crypto currencies	Before a wide-scale adoption of blockchain can be achieved, a systematic analysis of the consensus algorithms would help to understand how and why any particular blockchain platform performs the way it functions.
(Akhtar, 2019)	From Blockchain to Hashgraph: Distributed Ledger Technologies in the Wild	How blockchain protocols perform in terms of cost, performance, latency and security based on their different implementations.
(Bodkhe *et al.*, 2020)	A survey on decentralized consensus mechanisms for cyber physical systems	On understanding the key components, functional characteristics, and architecture of different consensus algorithms used in Cyber-Physical Systems (CPS).
(Sharma and Jain, 2019)	Consensus Algorithms in Blockchain Technology: A Survey	Security and performance issues of the different consensus algorithms are required to be improved.
(Gupta *et al.*, 2019)	An in-depth look of BFT consensus in blockchain: Challenges and opportunities	On the theory behind replicated computing and consensus but also how common consensus protocols operate.
(Oh *et al.*, 2020)	Graph Learning BFT: A Design of Consensus System for Distributed Ledgers	Guidelines for the design of a BFT consensus algorithm.

(Altarawneh and Skjellum, 2020)	The security ingredients for correct and byzantine fault-tolerant blockchain consensus algorithms	How the security and performance of a blockchain is determined by the chose consensus algorithm; hence, the reliability and security of these algorithms must be assured and tested, which requires an understanding of all the security assumptions that make such algorithms correct and byzantine fault-tolerant.
(Bouraga, 2021)	A taxonomy of blockchain consensus protocols: A survey and classification framework	Reviewing 28 new consensus protocols and proposed a four-category classification framework: Origin, Design, Performance and Security. Demonstration of the applicability of the framework by classifying the 28 protocols.
(Alsunaidi and Alhaidari, 2019)	A survey of consensus algorithms for blockchain technology	Focus on the popular consensus algorithms, in order to figure out their features, and the factors that affect their performance and security.
(Pahlajani, Kshirsagar and Pachghare, 2019)	Survey on Private Blockchain Consensus Algorithms	On theory and data used for selecting suitable consensus algorithm that would help researchers for further exploring of consensus in private blockchain environment.
(Fan *et al.*, 2020)	Performance Evaluation of Blockchain Systems: A Systematic Survey	Systematic survey on the blockchain performance evaluation by categorizing all reviewed solutions into two general categories, namely, empirical analysis and analytical modelling.
(Wang, 2019)	Performance Evaluation of Hyperledger Fabric with Malicious Behavior	On how malicious behaviors significantly undermines a blockchain system.

(Bamakan, Motavali and Babaei Bondarti, 2020)	A survey of blockchain consensus algorithms performance evaluation criteria	On the evaluation criteria of the performance of blockchain consensus algorithms.
(Y. Hao *et al.*, 2018b)	Performance Analysis of Consensus Algorithm in Private Blockchain	Selecting the appropriate consensus algorithm, how it directly affects the performance of a blockchain, how consensus algorithms perform under different private blockchain protocols.

2.3.1 Research on the Performance of Blockchain Protocols

Blockchain protocols' performance is a hot topic in current research, primarily focusing on simulation frameworks and their capability to measure key performance metrics of these protocols. Some studies target public blockchains, while others focus on private ones. However, as (Faria and Correia, 2019) highlighted, there is a noticeable lack of tools available for evaluating design and implementation decisions of blockchain protocols and CAs.

One noteworthy tool is BlockBench, a framework for analyzing private blockchain protocols (Tuan *et al.*, 2017). This system is recognized for its flexibility in integrating any private blockchain. Moreover, it is proficient at gauging throughput, latency, scalability, and fault tolerance against diverse workloads. This highlights its versatility and significance in private blockchain research.

Moving on from private blockchains, researchers in (Croman *et al.*, 2016) have pinpointed scalability as a challenge for public blockchains. They explored how various bottlenecks in the Bitcoin network could impact the network's total throughput. Based on their analysis, they recommended prioritizing block size reparameterization to realize next-generation, high-load blockchain protocols, demonstrating the need for structural changes in blockchain design.

Furthermore, the authors in (Decker and Wattenhofer, 2013) investigated the propagation time of blocks and transactions within the network and concluded that the latter is the primary

cause for blockchain forks. They also demonstrated the potential benefits of pushing the network to its limit through introducing unilateral changes to the client's behavior. This study effectively illustrated how transaction dynamics can impact overall blockchain performance.

In addition, Parity (Performance Analysis | Parity Technologies - Online, 2016) is an open-source software that provides the necessary components for running a public Ethereum node. This bridges the gap between research and practical application, as benchmark results have proven Parity to be the fastest and lightest Ethereum client in terms of block processing time.

Moreover, (Gervais *et al.*, 2016) presented a compelling study on the balance between performance and security in blockchain protocols. They scrutinized existing proof-of-work-based implementations and variants of proof-of-work blockchains. Among the most prominent Blockchain Benchmark Frameworks (BBFs) used in these investigations are IBM's Caliper and Blockbench.

Specifically, Hyperledger Caliper is a blockchain benchmarking tool designed to execute benchmarks on deployed smart contracts, facilitating the analysis of throughput, latency, and resource usage of the smart contract in use. In a survey study, (Wang, Ye and Xu, 2019) classified Hyperledger Caliper and Blockbench as the two leading BBFs, offering a comparative analysis between them that showcases the need for such tools in evaluating blockchain performance.

The diversity in benchmarking tools is further exemplified in (Saingre, Ledoux and Menaud, 2020), where the researchers introduced BCTMark, a framework for benchmarking blockchain technologies in an emulated network environment. The authors showcased the flexibility of their experiments by running them on two different testbeds, thus reflecting the wide-ranging environments in which blockchains operate.

Moreover, they performed experiments on three blockchain protocols, evaluating several metrics such as Central Processing Unit (CPU) usage and energy footprint for varying numbers of clients. This highlights the complexity of performance assessment in real-world blockchain applications.

Finally, (Baliga *et al.*, 2018) took a closer look at Quorum's (ConsenSys, 2021) performance, assessing its throughput and latency characteristics under different workloads and CAs. They employed a suite of micro-benchmarks to investigate how certain transaction and smart contract parameters might impact transaction latency, demonstrating the complex interplay between specific blockchain parameters and overall performance.

In summary, this discussion illustrates the multitude of tools and methods researchers employ to assess blockchain performance and the continuous evolution of these protocols to meet future demands.

2.3.2 Research on Designing and Building a Blockchain Consensus Algorithm

Consensus Algorithms are considered to be the core mechanism in blockchain systems since they provide the network the ability to validate transactions while avoiding the need of a central authority to act as the orchestrator of the network. Moreover, based on the blockchain type Public/Private etc., a specific CA is usually more "applicable" than another. Generally, while designing and building a blockchains networks, someone would need to sacrifice a characteristic in order to gain another. For example, sacrificing transaction throughput, enhanced security and privacy may be gained. However, as stated by (Chaudhry and Yousaf, 2019) one CA cannot serve the requirements of every application. . Therefore, to effectively design and implement a CA, it is essential to conduct a comprehensive technical comparison of the existing CAs, emphasizing their respective strengths, weaknesses, and use cases (Wang and Tan, 2020). This comparison underscores the significance of the CA, as a pivotal mechanism within the blockchain framework, which constantly confronts the challenge of striking a balance between security, efficiency, and consistency.

Also, the current CAs predict the formation of block proposers, thus malicious nodes have a clearer target. For this reason, they have developed a non-interactive verifiable random node extraction approach that uses a Verified Random Function (VRF) to create block proposer randomly. This method ensures that the identity of key nodes cannot be determined before the proposal block is broadcast, as well as the node identity's unpredictability and verifiability. The

authors in (Zoican *et al.*, 2018) discuss the challenges of implementing a CA for the world of Internet of Things (IoT). They have focused on the fact that time to reach consensus in such environments should small while during their studies with the three most used CAs (PoW,PBFT, Binary Consensus) they have proposed an integrated solution which based on their simulations using Contiki IoT Operating System (OS) manages time to reach consensus in less than a second.

On the other hand, the authors in (Song *et al.*, 2019), discussed CAs of Consortium Blockchains, in which as they state, the existed CAs for consortium blockchains fail to meet the requirements of practical applications, such as satisfying low algorithm complexity, robustness and dynamic scalability. For this reason, they proposed a new CA, in the family of BFT algorithms, which applies random threshold signature consensus scheme, unique cryptographic algorithm and proactive recovery scheme to achieve fast agreement, dynamic scalability and robust system. Their approach has been implemented and tested on the Hyperledger Fabric (The Linux Foundation, 2020) blockchain, which achieves competitive throughput, dynamic scalability and better robustness than the rest of the existing solutions.

Finally, many research works are discussing the limitations of CAs in the different types of blockchain protocols but also how difficult it is and what someone would need to focus on while designing and implementing a new CA. Such works are (Cong, Ren and Pouwelse, 2018; Guo *et al.*, 2018; Dai *et al.*, 2019; Li, Jiang and Liu, 2019; Yang *et al.*, 2019; MihaljeviÄ‡, 2020).

2.4 Systematic Literature Review Advancements (2022-2023)

Given the dynamic and rapidly evolving nature of blockchain technology, it is imperative to maintain the currency and relevance of this SLR. The initial SLR process commenced in 2021, covering studies and developments in blockchain consensus algorithms from 2018 to 2021. This period marked significant advancements in blockchain technology, providing a foundational understanding of consensus algorithms' performance, challenges, and opportunities.

As this thesis concludes in January 2024, it became necessary to extend the literature review to include more recent developments and contributions to the field within the years 2022 and

2023. This extension ensures that the review captures the latest advancements, reflecting ongoing research and innovations in blockchain CAs, benchmarking frameworks, and their applications across various domains.

To achieve this, a search was conducted on Google Scholar, employing keywords such as "blockchain," "benchmarking framework," "consensus algorithms," and "performance evaluation." The search was specifically tailored to identify sources published between 2022 and 2023, yielding 15 relevant articles that significantly contribute to the understanding and advancement of blockchain technology.

The main findings from the newly identified sources include developments in benchmarking frameworks and performance measurement tools for various blockchain clients, such as Hyperledger Fabric, XRPL, and Ethereum. These advancements provide deeper insights into the performance and scalability of blockchain systems, furthering the exploration of CAs and their impact.

2.4.1 Literature Review on the Latest Collected Sources

This section provides a comprehensive summary and analysis of the identified sources focused on benchmarking blockchain performance, improving throughput, verifying and validating blockchain applications, among other topics. The inclusion of these recent studies offers a broader perspective on the state of blockchain technology, its challenges, and potential solutions.

Gromit: Benchmarking the Performance and Scalability of Blockchain Systems (Nasrulin *et al.*, 2022)**:**

Addressing the limited research on performance comparisons of blockchain systems, this paper presents Gromit, a generic framework for analyzing blockchain systems. It conducts a large-scale study involving seven representative systems with varying consensus models. The study determines peak performance with a synthetic workload and explores the robustness of the systems against network delays. The findings indicate that transaction throughput does not scale linearly with the number of validators.

Bocb: Performance Benchmarking by Analyzing Impacts of Cloud Platforms on Consortium Blockchain (Huang *et al.*, 2022)**:**

This article investigates the performance of consortium blockchain implemented on different cloud platforms. It presents a comprehensive empirical analysis, identifying potential performance bottlenecks and configuring system parameters. The evaluation results help developers select the best configuration and resources to optimize their blockchain applications on heterogeneous cloud platforms.

Performance Study for Improving Throughput in Hyperledger Fabric Blockchain Platform (Nanduri and Vemula, 2022)**:**

Focusing on improving throughput in Hyperledger Fabric, this paper supplements previous studies by providing guidelines for enhancing performance. It conducts experimental studies with different consensus mechanisms and transaction sizes. The results demonstrate significant throughput improvement compared to default configuration settings.

BlockMeter: An Application Agnostic Performance Measurement Framework For Private Blockchain Platforms (Alom *et al.*, 2022)**:**

This article presents BlockMeter, a performance benchmarking framework for private blockchain platforms. BlockMeter can measure key performance metrics of any application deployed on top of a private blockchain in real-time. The framework is evaluated by assessing the performance of Hyperledger Fabric and Hyperledger Sawtooth against various use cases.

Blockchain Verification and Validation: Techniques, Challenges, and Research Directions (Marijan and Lal, 2022)**:**

This paper provides a comprehensive survey of verification and validation (V&V) solutions for blockchain-based software applications. It synthesizes V&V tools and techniques addressing different components and layers of blockchain applications. The paper discusses challenges associated with blockchain app V&V and proposes future research directions to advance the discipline.

Designing a High Performance and High-Profit P2P Energy Trading System Using a Consortium Blockchain Network (Makhsoos, Bahrak and Taghiyareh, 2022)**:**

This paper proposes a distributed energy trading framework based on a consortium blockchain for peer-to-peer energy trading. It introduces the Jointgraph CA and a DAG-based consortium energy blockchain framework, demonstrating improved performance and profitability compared to similar P2P trading models.

Small World Network for Simulation of Blockchain Networks (Kayastha and Joshi, 2022)**:**

Addressing the oversight of node topology in blockchain simulation frameworks, this paper presents a small world network approach for more realistic simulation of network nodes and upstream layers. The simulation framework based on Small World Networks yields more accurate results and can be applied to various blockchains, including Bitcoin and Ethereum.

Blockchain Technology for Intelligent Transportation Systems: A Systematic Literature Review (Jabbar *et al.*, 2022)**:**

This systematic review explores the application of blockchain technology to intelligent transportation systems, with a focus on the Internet of Vehicles (IoV). The paper provides an overview of blockchain technology, its evolution, and its applications. It reviews state-of-the-art blockchain-based IoV solutions, classifying them based on research directions and implemented IoV layers. The review highlights open problems and future research directions in blockchain-based IoV.

Performance Modeling and Analysis of Hyperledger Fabric (Ke and Park, 2022)**:**

This paper presents a quantitative modeling and analysis of the performance of Hyperledger Fabric, a permissioned blockchain platform. It proposes queuing models for different types of nodes in Hyperledger Fabric and analyzes their performance based on transaction/block queue size, waiting time, arrival rates, and service rates. The analysis explores the co-influence of arrival rates and service rates on performance and the impact of the number of channels.

BCTC-KSM: A blockchain-assisted threshold cryptography for key security management in power IoT data sharing (Deng *et al.*, 2023)**:**

This paper proposes BCTC-KSM, a blockchain-assisted threshold cryptography solution for secure key management in power IoT data sharing. It utilizes the Pedersen threshold secret sharing algorithm to split symmetric keys into multiple fragments stored on the blockchain. The paper demonstrates how BCTC-KSM improves security and availability in power IoT data sharing.

CollaChain: A BFT Collaborative Middleware for Decentralized Applications (Tennakoon, Hua and Gramoli, 2022)**:**

This paper introduces CollaChain, a Byzantine fault-tolerant (BFT) blockchain middleware designed for decentralized applications (DApps). CollaChain leverages collaboration among participants to improve validation and throughput of smart contract requests. The paper showcases the performance advantages of CollaChain over existing blockchain solutions.

Federated Learning: Challenges, Methods, and Future Directions (Singh *et al.*, 2022)**:**

This chapter provides an overview of federated learning, covering its types, architecture, challenges, and opportunities. It discusses the need for standardized methodologies in distributed environments and explores future directions in federated learning research.

An in-depth investigation of the performance characteristics of Hyperledger Fabric (Guggenberger *et al.*, 2022)**:**

This paper presents an in-depth performance analysis of Hyperledger Fabric, a private permissioned blockchain platform. It analyzes various performance characteristics using an enhanced version of the Distributed Ledger Performance Scan (DLPS) framework, providing insights into its configuration and implementation.

Blockchain for Future Wireless Networks: A Decade Survey (Rathod *et al.*, 2022)**:**

This survey focuses on blockchain applications in future wireless networks, discussing security challenges and proposing blockchain-enabled security solutions. It presents a blockchain-based wireless network architecture and evaluates its scalability and performance metrics.

Federated Learning for the Internet-of-Medical-Things: A Survey (Prasad *et al.*, 2022)**:**

This survey focuses on federated learning (FL) in the context of the Internet-of-Medical-Things (IoMT). It discusses challenges in FL with distributed datasets and scalability concerns. The survey presents a case study of a trusted cross-cluster-based FL and highlights the potential of FL in IoMT for distributed healthcare organizations.

2.5 Observations derived from Literature Review

After conducting a thorough review of the normative literature presented in Sections 2.2 - 2.5, several key observations have emerged. These observations are depicted in Figure *2.3*, providing a visual representation of the key findings. The review of the normative literature has yielded valuable insights and has contributed to a deeper understanding of the subject matter. By analyzing and synthesizing the information gathered from these literature sources, a comprehensive overview of the research landscape has been established. The observations outlined in Figure *2.3* serve as a foundation for further analysis and discussion, guiding the subsequent phases of the research process.

- **Observation A - No current CA meets all requirements in decentralization, security, and scalability:** Existing CAs focus on the blockchain trilemma, and it appears that there is no single CA that fits all blockchain requirements in terms of decentralization, security, and scalability.
- **Observation B - Despite the growing interest in mainstream adoption of blockchain technology, there are significant gaps in meeting the actual needs:** Stability, operational efficiency, and security still lag considerably, while scalability remains a prominent challenge. In Table *2.4*, a summary of the properties of the most used CAs is depicted.
- **Observation C - The assessment of blockchain protocol performance faces obstacles due to the lack of sufficient tools, frameworks, and documentation:** This finding is reinforced by the extensive number of articles extracted during the review process. Furthermore, Section 2.3.2 validates this observation by highlighting research that

identifies the necessity for developing and implementing new CAs to enhance the shortcomings of existing ones. The lack of comprehensive tools, frameworks, and documentation becomes apparent, emphasizing the need for further advancements in this area.

- **Observation D - The fragmented landscape and accessibility challenges of the blockchain ecosystem make it difficult for both newcomers and those with some experience in the field to search, find, configure, and bootstrap a functional private blockchain protocol:** The current ecosystem is fragmented with many different parameterizations of various blockchains while the information and how-to guides are much spread in many web pages making it impossible for a beginner to search, find, configure, and bootstrap a real private blockchain protocol.
- **Observation E - There is a discrepancy between the assumptions made in blockchain simulation frameworks and the real-world performance of the Blockchain Under Test (BUT)**, leading to simulated outputs that diverge significantly from real-world scenarios**.**
- **Observation F – There is an absence of user-friendly interfaces in blockchain performance measurement tools:** To the best of the researcher knowledge the available tools for measuring the performance of blockchain protocols, lack of a Graphical User Interface (GUI) enabling a seamless interaction between the user and the tool.

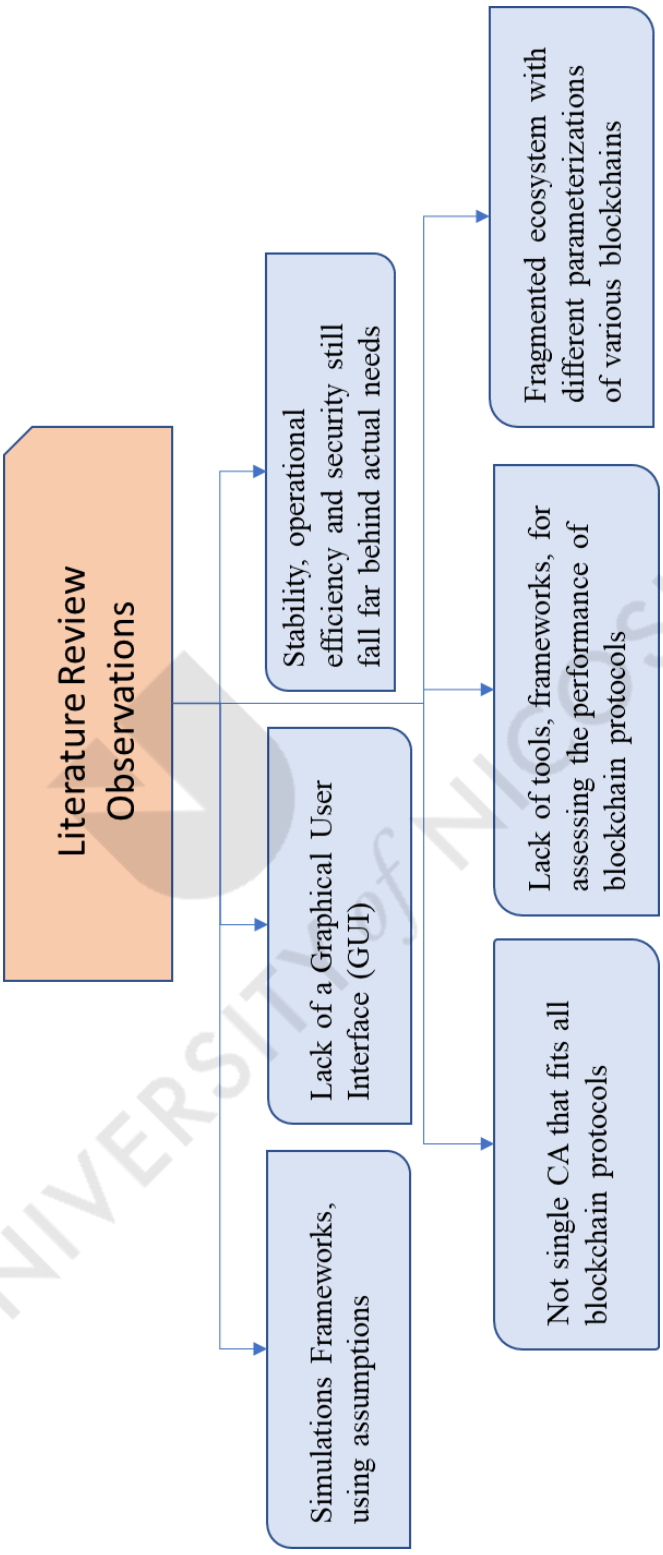


Figure 2.3: Observations Stemming from the Literature Review

Table 2.4: Summary of consensus properties

Faults Tolerated by a CA	Special Node-Crash	T < n/2 Nodes Crash	Special Node Subverted	F < n/3 Subverted Nodes
Hyperledger Fabric/Kafka	.	√	.	-
Hyperledger Fabric/PBFT	.	√	.	√
Tendermint	.	√	.	√
Symbiont/BFT-SMaRt	.	√	.	√
R3 Corda/Raft	.	√	.	
R3 Corda/BFT-SMaRt	.	√	.	√
IROHA/Sumeragi (BChain)	.	√	.	√
Kadena/ScalableBFT	?	?	?	?
Chain/Federated Consensus	-	(√)	-	-
Quorum/QuorumChain	-	(√)	-	-
Quorum/Raft	.	√	.	-
MultiChain +	.	√	.	-
Sawtooth Lake/PoET	+	√	+	-
Ripple	x	(√)	x	-
Stellar/SCP	?	?	?	?
IOTA Tangle	?	?	?	?

The following provides an explanation of the Table *2.4* symbols and notes: "√" denotes that the protocol is robust to the flaw, whereas "x" indicates that it is not; '.' indicates that there is no such special node in the protocol; '?' indicates that there is insufficient information to evaluate that properties; '(√)' indicates the crash of other nodes other than the special node; '+' PoET assumes trusted hardware is only available from one vendor; and 'x' indicates that a decision is not final in MultiChain. One of the five special nodes that are operated by default by Ripple can be compromised.

It can be observed that several CAs, such as Hyperledger Fabric/PBFT, Tendermint, Symbiont/BFT-SMaRt, R3 Corda/BFT-SMaRt, and IROHA/Sumeragi (BChain), demonstrate robustness against a significant number of fault types. These CAs can tolerate both the crash of less than n/2 nodes and the subversion of less than n/3 nodes, indicating a high level of resilience in the face of various adversarial situations. On the other hand, some CAs, like Chain/Federated Consensus and Quorum/QuorumChain, exhibit limited fault tolerance.

These CAs are only robust against the crash of other nodes apart from the special node, which may not be sufficient in some application scenarios. Furthermore, the table reveals that certain CAs, such as Kadena/ScalableBFT, Stellar/SCP, and IOTA Tangle, currently lack sufficient information to assess their fault tolerance properties. This highlights the need for further research and investigation into these algorithms to better understand their capabilities and limitations. Lastly, some CAs, like Sawtooth Lake/PoET and Ripple, have unique characteristics that set them apart from the others. For instance, PoET assumes trusted hardware is only available from one vendor.

2.5.1 Similarities and Differences

Section 2.6 provides a critical review of the normative literature and underscores the major findings, as illustrated in the observations outlined in Figure *2.3*. This section conducts an exhaustive comparison of the research papers assessed in this chapter, with the goal of pinpointing both the commonalities and disparities among them. To facilitate this comparison, Table 2.5 is presented, showcasing the findings obtained from the analysis. The critical assessment of the normative literature in Section 2.6 offers valuable insights into the research

landscape, shedding light on the overlapping themes, unique perspectives, and varying approaches explored within the selected studies. By conducting this thorough evaluation and providing a visual representation in Figure *2.3*, this section serves as a pivotal foundation for the subsequent discussions and analysis within the research study.

Table 2.5: Similarities Identified in Studied Research Works

Similarities	Research Works													
	(Ferdous, Chowdhury and Hoque, 2021)	(Akhtar, 2019)	(Bodkhe *et al.*, 2020)	(Sharma and Jain, 2019)	(Gupta *et al.*, 2019)	(Oh *et al.*, 2020)	(Altarawneh and Skjellum, 2020)	(Bouraga, 2021)	(Alsunaidi and Alhaidari, 2019)	(Pahlajani, Kshirsagar and Pachghare, 2019)	(Fan *et al.*, 2020)	(Wang, 2019)	(Bamakan, Motavali and Babaei Bondarti, 2020)	(Y. Hao *et al.*, 2018b)
There is a need for designing an efficient consensus algorithm and evaluating existing ones	√		√	√		√	√			√			√	√
There is a need for performance evaluation frameworks for blockchain and CAs	√	√	√	√	√	√	√	√	√	√	√	√	√	√
Consensus Algorithms are	√	√		√			√				√		√	√

considered the core mechanism of the blockchain protocols													
Blockchain technology has the potential to disrupt several application domains, other than currencies, touching all spheres of our lives.	√	√	√		√		√		√		√		

Regarding the identified similarities, it appears that all the references reported in Table *2.5* highlight the need for performance evaluation frameworks for blockchain protocols and CAs. Likewise, the need for designing an efficient CA and evaluating existing ones, is another similarity identified in the literature.

Furthermore, many of these studies emphasize that CAs are considered the core mechanism of blockchain protocols. Lastly, a similarity revealed by various research works (Akhtar, 2019; Alsunaidi and Alhaidari, 2019; Gupta *et al.*, 2019; Altarawneh and Skjellum, 2020; Bodkhe *et al.*, 2020; Fan *et al.*, 2020; Ferdous, Chowdhury and Hoque, 2021) underscores the fact that blockchain technology has the potential to disrupt numerous application domains beyond currencies, impacting various aspects of our lives.

Moreover, through the systematic literature review, notable distinctions have been identified and are presented in Table 2.6. The initial finding, drawn from (Ferdous, Chowdhury and Hoque, 2021), focuses primarily on the examination of performance aspects related to public blockchain protocols. This particular study stands out for its emphasis on evaluating the performance of public blockchain protocols, offering unique insights and contributing to the understanding of this specific area within the broader research landscape. The critical SLR conducted by the researcher uncovers such differences, highlights them in Table 6, enhances the comprehensiveness and richness of the research findings, and facilitates a deeper understanding of the various perspectives and research directions within the field. They also state that different variants exist for a wide range of CAs used in public blockchain systems that primarily support crypto-currencies. However, many existing crypto-currencies use such versions and internal methods, but they haven't been considered in the literature so far. On the contrary, since existing private blockchain platform lacks theory and data support for the performance analysis of the CA, (Y. Hao *et al.*, 2018b), proposed a method to evaluate the performance of CA in private blockchain protocols, specifically Ethereum and Hyperledger Fabric.

Another research work that comes from (Fan *et al.*, 2020) , states that blockchain has been hailed as a game-changing technology with applications in a variety of fields while it is also essential to assess their performance in different use cases and scenarios. Towards that goal,

they conducted a thorough survey on blockchain performance evaluation, dividing all examined solutions into two categories: empirical analysis and analytical modeling. Moreover, the authors in (Bouraga, 2021), proposed a comprehensive classification framework, integrating knowledge from multiple works in the literature, as well as introducing classification dimensions that have not been proposed before. To that end, they reviewed *28* new consensus protocols and proposed a four-category classification framework: Origin, Design, Performance and Security.

Table 2.6: Differences Identified in Studied Research Works

Differences	
Research Work	**Difference**
(Ferdous, Chowdhury and Hoque, 2021)	Studies the performance of **public** blockchain protocols.
(Bouraga, 2021)	Classifying 28 CAs in a **four-category** framework.
(Fan *et al.*, 2020)	Classifying most used CAs in a **two-category** framework.
(Y. Hao *et al.*, 2018b)	Studies the performance of **private** blockchain protocols.

2.6 Open Issues for Further Research

Through the systematic literature review (SLR), several research gaps and open issues have been identified, including insights derived from the latest sources discussed in Section 2.4. These gaps and issues warrant further investigation to advance the understanding of blockchain CAs and their potential for real-world applications. In this section, the researcher discusses four primary observations derived from the literature review, enhanced by the contributions from the newly analyzed sources.

1. **Open Research Issue 1 -** A thorough understanding of CAs is essential to unlock their full potential and identify areas for improvement. By looking into the complexities of CAs, a more robust and flexible blockchain protocol is designed.
2. **Open Research Issue 2 -** There is a need to explore adaptive and hybrid CAs, to achieve efficient, secure, and scalable blockchain solutions**.** Tailoring these algorithms to suit specific application requirements empower blockchain technology to thrive across a wide range of use cases.
3. **Open Research Issue 3 -** Advancing the mass adoption of blockchain technology is hindered by critical challenges related to security, stability, and operational efficiency, necessitating the exploration of novel CAs, optimization techniques, and architectural designs to improve blockchain protocols' performance and security.
4. **Open Research Issue 4 -** There is a lack of unified frameworks for CAs. To streamline progress, a comprehensive framework that integrates proposed CA enhancements is required. It is expected that such a unified approach will facilitate systematic evaluations and empower researchers, developers, and decision-makers to identify the most promising solutions for specific applications.

The multivocal SLR conducted in this chapter has revealed four open issues for further research related to blockchain CAs. These issues call for further investigation to advance the field and enable the development of more secure, efficient, and scalable blockchain protocol. By addressing these open issues, blockchain technology can be better equipped to disrupt various application domains and make a significant impact on our everyday lives. This, in turn,

contributes to the ongoing evolution of the blockchain ecosystem and its potential for transformative change across various industries.

2.7 Conclusions

Chapter 2 provides a comprehensive and critical examination of the literature regarding the performance of blockchain CAs and their impact on the overall behavior of a blockchain protocol. The chapter commences with a discussion on the systematic literature review methodology and lays out the strategy for its execution. It also describes and rationalizes the inclusion and exclusion criteria for the systematic literature review, thereby guaranteeing the rigor and relevance of the research.

Figure *2.1* illustrates the systematic literature review plan, adapted from the theory explained by (Brereton *et al.*, 2007), which serves as a guiding framework throughout this thesis. Additionally, Section 2.4.1.1 lists the research question that serves as the basis for the systematic literature review. This research question informs the development of search strings, enabling the extraction of pertinent data from various sources. Furthermore, Table 2.3 provides a list of selected cases that form the primary focus of this research, representing significant examples and references within the field.

Furthermore, Section 2.6 embarks on an in-depth examination of the observations and unresolved issues stemming from the systematic literature review. These observations, which are emphasized and graphically represented in Figure *2.3*, provide invaluable perspectives into the research field. The six observations revealed are as follows:

1. The pursuit of a CA that can perfectly balance decentralization, security, and scalability remains an ongoing challenge due to inherent trade-offs.
2. The gap between what is needed for mainstream blockchain adoption (notably stability, operational efficiency, and security) and current blockchain capabilities is significant.
3. Existing tools and documentation often fall short in accurately assessing blockchain protocols and guiding the development of more advanced CAs.

4. A fragmented blockchain ecosystem, featuring a wide range of blockchains and dispersed resources, poses substantial challenges to beginners.
5. There is a noticeable discrepancy between the assumptions made in blockchain simulations and the actual performance of blockchains in real-world conditions.
6. The majority of blockchain performance measurement tools lack intuitive, user-friendly interfaces, suggesting an area for potential improvement.

These observations collectively indicate open research issues that warrant further investigation. They highlight the need for additional research to address the identified gaps and open research issues, contribute to the development of robust blockchain solutions, and propel the field forward. By thoroughly examining these observations, Chapter 2 sets the stage for further analysis and exploration in subsequent chapters, enabling a comprehensive and informed research endeavor.

Chapter 3: Conceptualization of a Blockchain Benchmarking Framework

I do not fear computers. I fear the lack of them.

Isaac Asimov (1939–1992)

Summary

This chapter seeks to further investigate the observations outlined in Chapter 2, which explore blockchain CAs and their impact. These observations highlight the following challenges: a) the need for a CA balancing decentralization, security, and scalability; b) the gap between current blockchain offerings and mainstream adoption needs; c) inadequate tools for blockchain assessment; d) a fragmented ecosystem; e) disparities in simulation assumptions and real-world performance; f) and lack of user-friendly interfaces and performance measurement tools.

As a result of this exploration, Chapter 3 introduces a conceptual BBF. The proposed benchmarking framework aims to simplify the study of blockchain protocol performance, client specification assessment and to assist in selecting the most appropriate blockchain protocol for specific use cases. The BBF provides a systematic approach and seeks to enhance decision-making and to contribute to the field of blockchain performance specification.

3.1 Introduction

Chapter 2 presents a systematic literature review on the performance evaluation of blockchain protocols. Several methodologies and frameworks discuss, all aim at scrutinizing the performance of blockchain protocols and understanding the impact of CAs. However, it identifies that existing approaches fall short of the desired quality and integration levels toward a comprehensive, end-to-end blockchain benchmarking process.

In the course of this literature review, the thesis reveals a distinct lack of tools and frameworks specifically designed for measuring the performance of blockchain CAs. Moreover, a noteworthy process for measuring the performance of such protocols deduces from the surveyed literature. This five-step process comprises of:

- The selection of the blockchain protocol.
- The selection of the benchmarking scenario.
- The simulation of the benchmarking scenario.
- Data generation.
- The data assessment.

Based on the observations from Section 2.4, Chapter 3 aims to propose a conceptual BBF that is grounded on the identified benchmarking process. The proposed conceptual BBF envisions to be used as a tool for the deployment of a blockchain protocol, executing diverse malicious scenarios, collecting monitoring data, and deriving results in a unified format.

The challenges identified from the literature (as discussed in Section 2.5) serve as the foundation for the proposed conceptual framework. The extended benchmarking process also envisions for both public and private blockchain protocols. Precisely, the researcher maps the key findings from Chapter 2 to the measures to be implemented in Chapter 3. The intent is to address the concerns identified and further investigate the questions that the literature review leaves unanswered.

In response to the observations made in Chapter 2, the following primary investigative actions are proposed:

- To address Observation A, the researcher proposes the development of a conceptual framework aimed at guiding the evaluation process of a blockchain protocol. This endeavor focuses on improving the methodology for assessing blockchain performance, addressing the existing gap in the literature.
- In relation to Observation B, an investigation into the impact of CAs on the performance and overall behavior of a blockchain protocol is planned. The goal of this action is to explain the role of CAs and their influence on blockchain protocol performance.
- For Observations C and D, the integration of various blockchain simulators into the benchmarking of a blockchain is examined. Concurrently, the researcher works towards the definition of an extended and comprehensive blockchain benchmarking process. This investigative action contributes to the development of a more holistic and practical approach to blockchain benchmarking.
- Finally, in line with Observations E and F, the researcher identifies the components of a BBF and explores how these components can be orchestrated, taking into account the technical and non-technical expertise of users. This investigation is aimed at enhancing user interaction with the BBF and making it more accessible and effective.

Through these primary investigative actions, the study aims to further investigate the observations made and pave the way to the development of the proposed BBF.

The remaining sections of this chapter are organized as follows:

- **Research Challenges and Proposals:** This section provides a thorough analysis of the literature review's findings, based on the observations, similarities, and differences addressed in Section 2.4.1, as part of the first action step outlined above, to fill the research gap identified by the systematic literature review. Clearly, the findings of Chapter 2 highlight a need for performance evaluation frameworks for blockchain and CAs that improve the decision-making process and adhere to an established blockchain benchmarking process.

- **Proposed Model:** Section 3.3 presents the proposed conceptual model, considering the limitations and challenges covered in previous sections. This section also covers the identified benchmarking process as well as its extended version to be incorporated in the proposed model.
- **Research Hypotheses:** Section 3.4 defines a set of hypotheses to evaluate the proposed model. These hypotheses help assess the effectiveness and validity of the suggested approach systematically and objectively.
- **Blockchain Benchmarking Framework (Architecture):** This section presents a proposed architecture for the conceptual model presented in Section 3.3. It focuses on addressing Observations C, E, and F, derived from the literature, and provides a detailed overview of the framework's components and their roles.

3.2 Research Challenges and Propositions

This section discusses the research gap identified from the literature review. The research gap, highlighted in Observations A to F, primarily stems from the evaluation of existing tools and frameworks that assess the performance of blockchain protocols. Typically, these frameworks adhere to a standard blockchain benchmarking process comprising of mainly five steps:

- **Step 1:** Selection of the blockchain protocol.
- **Step 2:** Selection of the benchmarking scenario.
- **Step 3:** Simulation of the benchmarking scenario.
- **Step 4:** Data generation.
- **Step 5:** Data assessment.

However, for each of these steps, specific limitations are identified, which the researcher of this thesis seeks to address.

The identified limitations are enumerated as follows: The present methodologies employed for blockchain selection can accommodate less than six blockchain protocols, demonstrating a restricted scope (Tuan *et al.,* 2017). With respect to the benchmarking scenarios, existing

approaches can only support up to three, which implies a potential constraint in the comprehensiveness of the evaluation process. As for the execution of the benchmarking, reliance is solely placed on simulators, indicating a limited diversity in technique and potentially reducing the applicability of results in real-world scenarios (Saingre, Ledoux and Menaud, 2020). The data generated by current methods has been observed to deviate significantly from realistic scenarios, suggesting an accuracy concern in the interpretation of results (Benoit, Harold; Gramoli, Vincent; Guerraoui, Rachid; Natoli, 2021). Finally, the data visualization step is largely overlooked with no identifiable research works, demonstrating a clear void in this vital aspect of data presentation and analysis (Choi and Hong, 2021; Sedlmeir, 2021).

With a focus on the identified research gap (Observations A to F), as well as on the limitations of the benchmarking process, the researcher proposes an enhanced blockchain benchmarking process upon which the conceptual BBF is based. This innovative approach consolidates and integrates the five main steps identified from the literature into a more comprehensive and coherent process, aiming to overcome the identified limitations. The enhanced benchmarking process, along with the identified limitations is depicted in Figure 3.1.

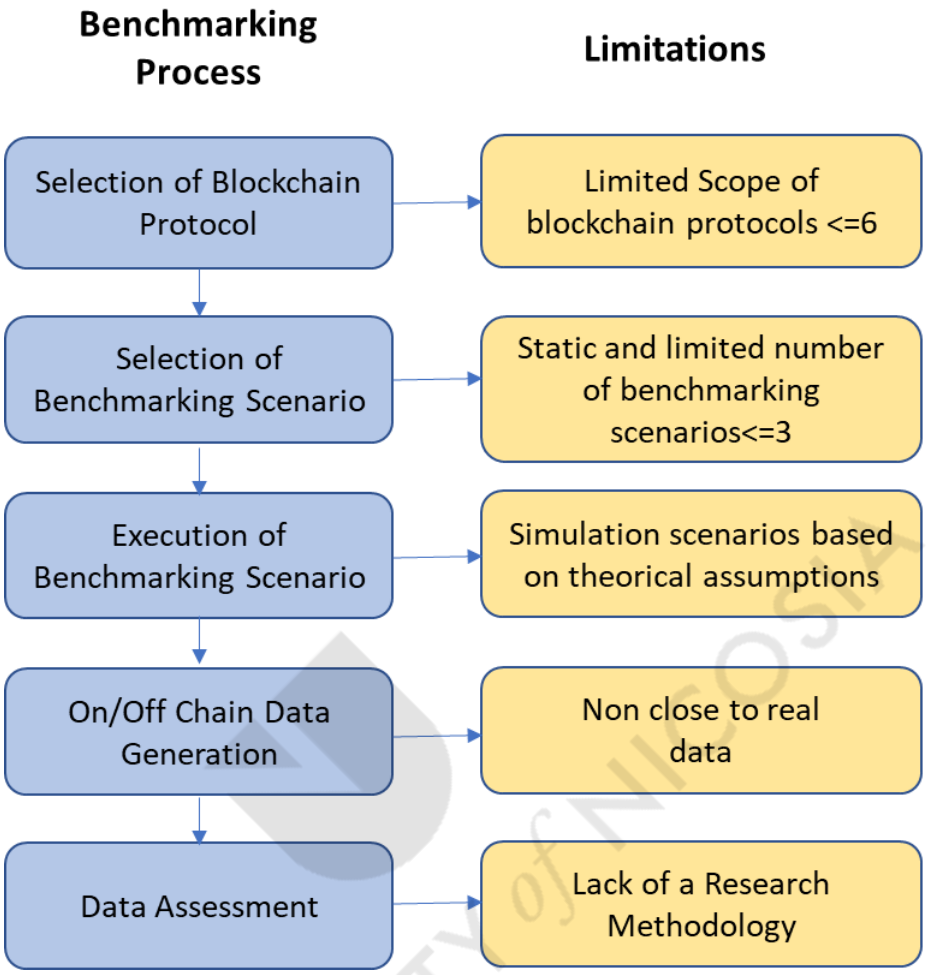


Figure 3.1:Blockhain Benchmarking Process and Current Limitations

3.2.1 A "one-fits-all" benchmarking framework for different blockchains

Blockchain technology continues to disrupt existing solutions while also new parameterizations of existing blockchains are often introduced. Moreover, each one of the blockchain protocols usually targets to improve or overcome an existing limitation or a specific use case and the team behind it introduces features that are about to differentiate their solution from the others. However, these new features often affect the overall behavior of the network while when designing a blockchain protocol you need to sacrifice one characteristic to gain another.

When it comes to the adoption of blockchain by organizations and/or individuals, a clear view of what each solution may have to offer, and under which settings or scenarios the choice of the corresponding blockchain is not suitable anymore is needed. Moreover, for blockchain protocol developers, another challenge is ensuring that the actual performance aligns with the technical specifications proposed in the theoretical framework. This alignment is essential to maintain the credibility and reliability of the blockchain solution. Thus, as described in Section 2.5.2, several solutions for BBFs have been introduced in the literature while some of them have been evolved based on some limitations of the rest. Moreover, almost all the available works even though they are adaptable in terms of integrating a new blockchain protocol, the benchmarks the user can perform are based on simulation scenarios and thus the data that the user is able to gather are far from the real-world cases. Table *3.1* groups the identified research works that focus on the performance evaluation of blockchain protocols, along with their supported characteristics. As illustrated in Table *3.1* no study has been able to support more than five blockchain protocols. Additionally, the range of metrics that can be monitored is restricted. None of these approaches offer a GUI, and the majority are designed for simulation environments based on numerous assumptions.

Table *3.1* presents an overview of selected benchmarking frameworks for evaluating the performance of public and private blockchain protocols. The frameworks are identified through a systematic literature review and are evaluated based on whether they support benchmarking of public or private blockchains, whether they include a benchmarking process, whether they include a simulator, what monitoring metrics are supported, whether they have a graphical user interface, and whether they are based on microservices architecture. The table provides a summary of five benchmarking frameworks: BlockBench, Hyperledger Caliper, BCTMark, DIABLO, and Distributed Ledger Performance Scan (DLPS). Each framework is evaluated on whether it supports benchmarking of public and private blockchains, whether it includes a benchmarking process, whether it includes a simulator, what monitoring metrics are supported, whether it has a graphical user interface, and whether it is based on microservices architecture. The symbols in the table indicate whether the framework supports a certain feature. For example, "x" means that the feature is not supported, while "√" means that it is supported. For

instance, BlockBench supports benchmarking of public blockchains and monitoring metrics such as throughput, latency, scalability, and fault-tolerance, but does not have a simulator or a graphical user interface. Hyperledger Caliper, on the other hand, supports benchmarking of private blockchains, has a simulator, and supports monitoring metrics such as transaction success rate, transaction and read latency, transaction and read throughput, and resource consumption, but does not have a graphical user interface.

Table 3.1: Research works on blockchain protocols performance evaluation.

Framework Name	Public Blockchains	Private Blockchains	Benchmarking	Simulator	Monitoring Metrics	Blockchains	GUI	Microservices Architecture
BlockBench	x	√	√	x	Throughput, latency, scalability, fault-tolerance	Ethereum, Parity, Hyperledger Fabric	x	x
Hyperledger Caliper	x	√	x	√	Transaction success rate, transaction & read latency, transaction & read throughput, resource consumption	Hyperledger Besu, Hyperledger Fabric, Ethereum and FISCO BCOS networks	x	√
BCTMark	x	√	x	√	CPU consumption, energy footprint	Ethereum Clique, Ethash and Hyperledger Fabric	x	x

DIABLO	x	√	√	√	Throughput, latency	Go Ethereum, Open Ethereum, CollaChain, Quorum, Hyperledger Fabric	x	x
Distributed Ledger Performance Scan (DLPS)	x	√	√	x	Throughput, latency	Eth. (Geth), Eth. (Parity), Fabric, Indy, Quorum, Sawtooth	x	x

Proposition 1 – Comprehensive end-to-end benchmarking for multiple blockchain integration:

The researcher proposes an end-to-end blockchain benchmarking process, which is a comprehensive approach covering all aspects of the benchmarking process from protocol selection to data assessment. This approach, seeks to address the challenges identified from the literature review conducted in Chapter 2, and is further strengthened by the following proposals:

1. **Protocol selection**
    - **Gap:** Current benchmarking methodologies often cater to a limited set of blockchain protocols, restricting the scope of analysis in a rapidly-evolving blockchain ecosystem.
    - **Benefit:** The proposed process's ability to support an indefinite number of blockchains ensures future-proofing against emerging protocols. Dynamic integration templates mean faster, more agile adaptation to new technologies.
    - **Anticipated Impact:** A benchmarking framework that can accommodate any blockchain protocol ensures continuous relevance, encourages adoption and more holistic research outcomes.
    - **Real-world Relevance:** As the blockchain ecosystem grows with new technologies and protocols, a benchmarking tool that can evolve alongside it becomes indispensable for rigorous research and application development.
2. **Benchmarking test selection**
    - **Gap:** Many benchmarking tools come with a fixed set of test scenarios, which might not cover all potential vulnerabilities or use cases.
    - **Benefit:** Comprehensive documentation and user-customizable templates mean broader test coverage, capturing potential vulnerabilities or use cases that may otherwise be overlooked.

- **Anticipated Impact:** By enabling diverse and custom testing, the benchmarking process can help in identifying and rectifying weaknesses before blockchain solutions are deployed in real-world situations.
- **Real-world Relevance:** With blockchain technologies penetrating sectors like finance, governance, and healthcare, ensuring their resilience against a diverse range of scenarios is critical to secure real-world implementations.

3. **Simulation of unforeseen behavior**
   - **Gap:** Simulated environments often lack the unpredictability of close to real-world blockchain deployments using the real clients, leading to potentially skewed benchmarking results.
   - **Benefit:** Testing in real blockchain environments using actual clients ensures data authenticity, capturing discrepancies and unpredictable behaviors simulations might miss.
   - **Anticipated Impact:** Enhanced accuracy in benchmarking translates to more reliable and actionable insights for researchers and developers.
   - **Real-world Relevance:** Ensuring blockchain technologies can handle real-world unpredictabilities safeguards against potential failures when implemented in critical systems.
4. **Data generation**
   - **Gap:** Data generated in simulated environments might not truly reflect the complexities and differences of real-world blockchain operations.
   - **Benefit:** Utilizing a real blockchain protocol for data generation ensures the authenticity and relevance of the captured data.
   - **Anticipated Impact:** More realistic data means more accurate evaluations, leading to blockchain solutions that are better optimized for real-world challenges.
   - **Real-world Relevance:** As blockchains find applications in data-sensitive areas, having reliable data generation methodologies is crucial to validate and fine-tune their operational efficacy.

5. **Data assessment**
    - **Gap:** Current data assessment tools might not be user-friendly, complicating the interpretation of benchmarking results.
    - **Benefit:** A graphical user interface simplifies data assessment, making results more accessible and understandable, even for those with limited technical expertise.
    - **Anticipated Impact:** Simplified and clear interpretation of results ensures that blockchain solutions are evaluated and refined more effectively, promoting better development outcomes.
    - **Real-world Relevance:** As blockchain stakeholders expand beyond technical experts to include business leaders, policymakers, and the general public, making benchmarking data easily interpretable is key to informed decision-making and broader understanding.

The proposed benchmarking process may enable the easy deployment of a blockchain protocol, execute different malicious scenarios, gather monitoring data, and derive outcomes in a unified format. Furthermore, the proposed architecture – as discussed in Section 3.5 - for the BBF aims to serve as a staged environment for supporting blockchain researchers and developers to test and validate the performance of a blockchain protocol as well as to validate all the design decisions made by the protocol under different settings and synthetic scenarios. It also aims to provide the user with dynamicity, real-world data, and enable self-adaptation. Dynamicity means that the benchmarking framework should be able to integrate a new blockchain protocol with minimal effort. Real-world data means that the user should be able to deploy a real private blockchain protocol on a local deployment, avoiding the need for simulations and capturing real data. Lastly, the proposed architecture should enable the blockchains under test to self-adapt under certain conditions, based on various on-chain collected metrics.

3.2.2 Reproducibility, ease of use, and the need for technical expertise

Blockchain protocols are complex systems thus researchers and/or developers usually do not feel comfortable in setting up a private network (Shi *et al.*, 2021). Moreover, the current

ecosystem is fragmented with many different parameterizations of various blockchains while the documentation and how-to guides are scarced, even incomplete making it impossible for a beginner to search, find, configure, and bootstrap a real private blockchain protocol within a logical timeframe. Additionally, the existing body of literature offers limited insights regarding the performance of corporate blockchain systems. These insights, which the researcher has discovered, demonstrate significant diversity. The rapid evolution and inherent heterogeneity of blockchain implementations further complicate the situation, making it challenging to develop a universally applicable benchmarking tool that can account for these differences. This has resulted in a lack of transparency and repeatability in current benchmarking efforts, as critical parameters such as throughput and latency are not explicitly defined, and the algorithms employed to measure them often remain unspecified. Furthermore, even if a private blockchain protocol is successfully deployed, defining benchmark tests is also a difficult task. Blockchain protocols require testing and monitoring of numerous technical and non-technical parameters, including low-level metrics such as throughput and latency, and high-level metrics such as the number of active nodes and closed ledgers. Consequently, it is essential that benchmarking tests are described and configured in a user-friendly manner to reduce the requirement for technical expertise while simultaneously increasing the reproducibility of the framework.

Proposition 2 - Developing an open-source, transparent, and flexible benchmarking framework for enterprise distributed ledger technology (DLT) solutions:

The current research endeavors to address a research gap by proposing a transparent, open-source, and highly flexible benchmarking framework to acquire reliable performance data from various enterprise Distributed Ledger Technology (DLT) solutions. The proposed framework is expected to be implemented iteratively within an enterprise project to enable the reliable comparison of performance among different blockchain technologies for specific use cases. The proposed BBF aims to overcome the limitations of existing approaches by facilitating the measurement of well-defined quantitative key performance indicators of different DLTs using a universal, comprehensive, and transparent benchmarking algorithm. To reduce the complexities and technical expertise required to use the proposed benchmarking framework, the researcher plans to implement automation tools and integrate different modules and low-level

scripts within a graphical user interface. Such integration not only streamlines the user experience but also ensures that both experts and novices can derive value from the framework. The primary objective is to enhance the accessibility and user-friendliness of blockchain benchmarking to accommodate a broader spectrum of stakeholders. A detailed explanation of the GUI is provided in Section 3.5.1.3.

3.2.3 Lack of visualization environments

There have been numerous recent proposals for blockchain protocols and CAs that seek to address the blockchain trilemma. Individuals and businesses seeking to incorporate blockchain technology into their products are interested in determining which CA is best suited for their needs. However, setting up and managing a private deployment of blockchain protocols can be complex and time-consuming, especially for non-technical users, who may lack visibility into the complicated environment and struggle to identify the best blockchain solution. An intuitive user interface, catering to both technically adept and novice users, is imperative for broad utilization. The incorporation of graphical user interfaces, advantageous for enhancing user engagement, could facilitate the deployment and configuration of blockchain protocols, while concurrently providing a visual representation of the aggregated network data. However, most of the benchmarking frameworks in the literature lack a GUI to help users deploy and configure blockchain protocols or visualize the collected network data. A GUI-based BBF also helps researchers and developers fine-tune DLT-specific parameters, configure application-specific metrics, and visualize network connectivity and adaptation during runtime. To the best of the researcher's knowledge, none of the analyzed literature provides a user-friendly application to interact with underlying benchmarking tools. Thus, a user-friendly information system that can be used by both technical and non-technical personnel is proposed.

Proposition 3 – A user-friendly, GUI for multi-faceted interaction with the blockchain benchmarking framework:

To address the aforementioned issues, the researcher proposes to develop a User-friendly Interface (UI) is proposed to be integrated as part of the proposed BBF, enabling users to interact with the framework seamlessly and without technical expertise. The GUI should be designed to

cater to the needs of three categories of users: a) demand-side users, including developers, technical teams, and managers, who require tools for assessing the performance of different blockchain protocols focusing on aspects such as security and scalability, b) supply-side users, including organizations and companies that provide data and/or services and wish to adopt blockchain technology, who require a comprehensive understanding and characterization of the technical principles and characteristics of different blockchain protocols in order to determine which protocol best meets their needs and demands, and c) academic users, including researchers, students, and educators, who require a homogeneous environment for testing, running experiments, and validating research findings. The proposed UI should provide a visualization of all experiments and enable easy reproducibility. Moreover, the UI could be utilized as a teaching tool in classroom environments.

The UI should be designed to be user-friendly, with clear instructions and visualizations that enable the user to easily configure and initiate benchmarking tests. The GUI includes several input fields and options that allow the user to specify the blockchain protocol, the benchmark test, the data generation parameters, and the performance metrics of interest. Once the user submits the request, the GUI sends the necessary API calls to the benchmarking framework, which executes the tests and generates the desired outcomes. The results are then visualized in the GUI, allowing the user to easily interpret and analyze them. Overall, the proposed UI aims to provide a seamless and efficient interaction with the benchmarking framework, abstracting any underlying complexities and enabling a wider range of users to utilize and benefit from it.

3.2.4 Lack of a monitoring framework for analyzing the performance of blockchain protocols

A typical blockchain protocol consists of a collection of peer-to-peer interconnected nodes. These nodes are often hosted on cloud or on-premises infrastructure, with the blockchain runtime installed natively on a Virtual Machine (VM) or via containerization technologies like Docker. Transactions sent to the network are broadcast to all peers, while new blocks are propagated ensuring that everyone has the latest ledger version. Usually, monitoring just one of the peers is enough to provide insights about the blocks, its transaction-related events, and associated information. This is due to the distributed nature of blockchains ensuring data

consistency across nodes, making individual node monitoring representative of the network's health.

Within the blockchain domain, the prevalent instrument for observing transactional activities is typically a blockchain explorer, developed cohesively with its associated blockchain protocol. This explorer is designed to monitor specific events, presenting a visual portrayal of transactions from their initiation to subsequent queuing, processing, and their eventual integration into a new block. However, this conventional monitoring approach provides a limited perspective. It does not grant insights into essential parameters like a node's resource utilization, the status of adjacent nodes, or potential latencies within the network. An in-depth academic examination identifies a significant research gap. From an exhaustive literature analysis, various studies addressed in this thesis illuminate the lack of a comprehensive monitoring framework designed to measure blockchain performance. Additionally, the way metric data is amassed tends to be so formulaic that it constrains in-depth analysis. This constraint hinders the extraction of detailed performance interpretations of the blockchain and its affiliated CA. Furthermore, the off-chain elements, constituting the decentralized application (dApp) layer, represent another pivotal segment warranting monitoring to achieve comprehensive oversight of a blockchain-driven solution. As such, an adaptive monitoring solution is proposed, envisioned as an additional layer within the blockchain architecture, mandated to process, archive, and visually represent data generated by node participants, deployed dApps, and on-chain data, inclusive of transactions, blocks, and smart contract details.

Proposition 4 – Monitoring System for data assessment and visualization:

To enhance the benchmarking process, the researcher proposes a generic monitoring framework, which is an integral part of the BBF. This framework would consist of cutting-edge technologies responsible for processing, storing, and visualizing the data produced within the blockchain under test, as well as the data produced by the deployed dApps off the blockchain. During the deployment of the benchmarking framework, an additional set of services would be spawned to form the monitoring framework. The goal of the monitoring framework would be to collect and visualize different data from the transactions performed in the network, as well as data regarding the health of the nodes participating in the network. The proposed monitoring

framework would be considered as a black box to the blockchain protocol, as it is not aware of the specific details of the protocol. This approach provides flexibility to the user, allowing them to build a custom metric exporter that can gather data based on their specific needs and demands. Moreover, this level of abstraction can enhance security, as the framework doesn't expose protocol details, thereby reducing potential points of exploitation. Furthermore, with the ability to design tailored metric exporters, users can more effectively pinpoint and address specific performance bottlenecks or security concerns in real-time. Lastly, this decoupled design ensures easier upgrades and adaptability, future-proofing the monitoring framework against rapid technological changes in the blockchain landscape.

The black box approach was chosen to ensure the monitoring framework can be used with different blockchain protocols without needing any specific customization. By abstracting the blockchain protocol's specific details, the framework can be easily integrated with various blockchain protocols, without requiring additional development work. This also allows users to focus on their specific needs without worrying about how the framework interacts with the underlying blockchain protocol.

3.3 Proposed Model

This section focuses on the enhancement of the blockchain benchmarking process considering the limitations and challenges covered and discussed in Section 3.2. As discussed in Section 3.2, the current approaches identified in the literature have introduced a process for benchmarking blockchain protocols and their CA which consists of mainly 5 steps. Firstly, the selection of the blockchain protocol should take place (which usually happens from a predefined list of the supported protocols). Then, the benchmarking scenario should be defined and executed in the blockchain under test while monitoring data are produced by the nodes/validators of the network as well as of the deployed on-chain and off-chain applications. Finally, data assessment and analysis are taken place extracting possible outcomes in regards of the performance of the blockchain protocol and how it reacts under different settings and malicious behaviors. The benchmarking process along with the characteristics of the current approaches identified in the literature is depicted in Figure *3.1*.

Based on the research challenges discussed in Section 3.2, the researcher proposes several enhancements towards an extended version of the blockchain benchmarking process, which are presented and discussed in subsequent sections.

- **Number of supported blockchain protocols:** The researcher seeks to expand upon existing methods, which, as discussed in Section 3.2, currently support a maximum of six blockchains. In the proposed BBF, the number of supported blockchain protocols will surpass this count. Additionally, a new methodology is introduced, designed to simplify the integration of new blockchain protocols for framework users.
- **Benchmarking Metrics:** In most of the identified works, the metrics that are monitored within the framework are limited to three. Mainly these are: a) throughput of the network, b) the latency in the communication channels and c) the overall scalability of the blockchain under test. In the proposed benchmarking process, an extended list of metrics would be able to be monitored (support of metrics from the current approaches as well as application-specific metrics exported by the blockchain protocol itself). Supporting a broader range of metrics provides a more comprehensive understanding of a blockchain's performance. It allows users to tailor benchmarks to their specific needs and applications, ensuring that the evaluations are more aligned with real-world scenarios. Moreover, a metric's exporter template would be suggested for guiding the users to develop their own metric's exporter, integrating it into the final BBF.
- **Simulations vs Real Benchmarking Scenarios & Data Generation:** In most of the identified studies, the researchers introduced blockchain simulation frameworks in which they use several assumptions for the assessment of the performance of the blockchain under test. The latter results in simulated outputs - data that are often too far from real-world cases. In the proposed benchmarking process, real implementations of benchmarking tests are foreseen executed on the actual blockchain clients as they are introduced by their founders. Thus, the produced data would be close to reality, enabling the users to extract outcomes and validate them on real implementations of blockchain protocols.

- **Data Assessment:** To the best of the researcher's knowledge, existing literature seems to lack research that introduces a framework for visualizing benchmarking data assessments. The primary aim of this research is to develop and implement a monitoring system to aid in the analysis of the blockchain under test. This would entail introducing a series of services that would be regarded as crucial components towards the realization of a dynamic monitoring system that facilitates the easy storage, access, and visualization of the monitoring data generated by the blockchain under test.

Figure *3.2* illustrates the current approaches to the blockchain benchmarking process as well as the proposed enhancements. The current approaches include five main steps, which are the identification/selection of the blockchain protocol, the selection of the benchmark test, simulation/execution of the unforeseen behavior, data generation, and data assessment for deriving outcomes and results. However, the literature review identified several limitations and challenges associated with these approaches, such as the lack of real-world data and the need for a more comprehensive and user-friendly framework. To address these limitations, a set of enhancements are proposed, which are depicted in the figure. These enhancements include the integration of real-world data into the benchmarking process, the development of a user-friendly UI for interacting with the benchmarking framework, and the implementation of a monitoring system to assist in understanding and analyzing the blockchain under test. These enhancements aim to improve the benchmarking process for blockchain protocols and provide a more comprehensive and user-friendly framework for testing and evaluating their performance.

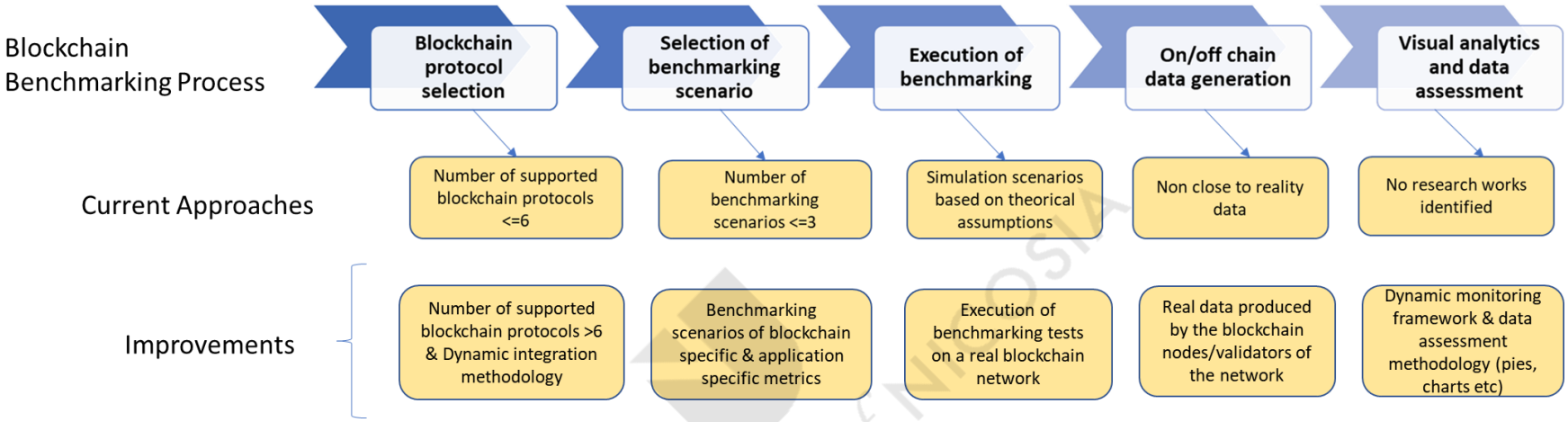


Figure 3.2: Proposed Enhanced Blockchain benchmarking process

3.4 Proposed Conceptual Blockchain Benchmarking Framework

The researcher proposes a three-layer architecture that serves as the foundation for the proposed BBF.

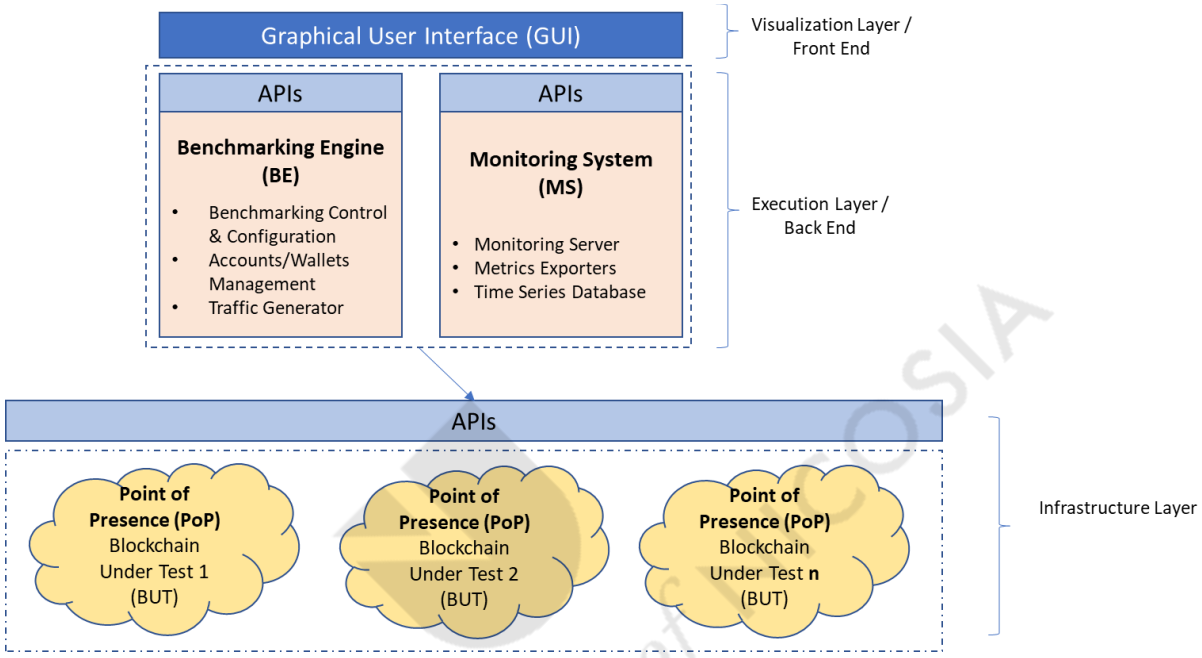


Figure 3.3: Blockchain Benchmarking Framework – Proposed Architecture

The following elements, paired with the model shown in Figure *3.3*, are suggested by the researcher for inclusion in the architecture.

1. **Visual Analytics Layer:**
   1.1. Graphical User Interface – A user friendly web interface, eliminating the gap between the non-technical users and the BBF.
2. **Execution Layer:**
   2.1. Benchmarking Engine (BE) – Automation tools and mechanisms for the deployment of a blockchain protocol consisted of *n* number of nodes/validators.

2.2. Monitoring System (MS) – Monitoring tools for storing the produced benchmarking data, processing of the benchmarking data, and visualization of the produced benchmarking data.

3. Infrastructure Layer:

3.1. This is the layer where the blockchain under test would be deployed and stress tested. Automation tools need to be developed minimizing the time for configuring and deploying a blockchain protocol.

3.4.1 Proposed BBF Components

As reported in Section 3.2 , blockchain-based protocols are complex systems that comprise of many components ranging from the underlying communication network, cryptographic libraries, gossip protocols, CAs, virtual machines, and game theoretical aspects (Xiao *et al.*, 2020b). In most cases, bootstrapping a private blockchain protocol on a local deployment and using it for testing is a challenging task. It is even more challenging to compare various private blockchain implementations in terms of transactions throughput, latency, fault-tolerance, and scalability. Moreover, having an isolated environment where you can introduce changes to the source code, test and debug the system without affecting the implementation of the production blockchain, is essential. Implementing a blockchain infrastructure considers several design choices such as network performance, network anomalies, node's misbehavior, etc. However, the latter introduces several challenges, while a blockchain protocol usually consists of several nodes running in different machines around the world (i.e., high level of distribution and decentralization). The proposed conceptual architecture of a BBF would be capable of deploying a full-meshed blockchain protocol with a given number of nodes/validators. The latter should be easy to execute, minimizing the need for technical expertise of its users.

Each architectural element of the BBF is presented in further detail in this chapter. The three layers are covered and further discussed providing the reader with a chance to comprehend how each of the components of the BBF work and interact.

3.4.1.1 Benchmarking Engine (BE)

The BBF, as well as the BE, would be designed and implemented utilizing the "microservice approach," (Dragoni *et al.*, 2017) avoid having a single monolithic application, hence addressing the scalability challenge pointed out in Observation B. This design increases the system's maintainability and scalability. Each component of the benchmarking engine should be separated from the rest of the system and may operate independently, allowing for dynamicity and ease of replacement of a non-functional process. The BE should be consisted of three main components:

- **Control & Configuration:** In a nutshell, the user of the BBF would like to deploy a blockchain protocol of *n* number of nodes/validators. The ''Control & Configuration'' mechanism would be responsible to generate the configuration files needed by the network's participants, adjusting their connectivity (making them peers), include them in the validation process (based on the corresponding CA), and finally deploy the network in the form of container instances. This component directly addresses Observation D, which highlights the challenges newcomers face in configuring and bootstrapping a functional private blockchain protocol.
- **Accounts/Wallets Management:** The execution of transactions is responsible for closing a new ledger/block and attaching it to the chain. While validators/nodes work on closing the next ledger, the produced traffic may provide vital information on the blockchain under test. Thus, using the "Account/Wallets Manager" the user would be able to generate a number of new accounts/wallets and spread the aforementioned tokens from the genesis account or from any test account made available in the genesis ledger. Given the importance of transactional efficiency in Observation B, this component plays a crucial role in achieving effective benchmarking.
- **Traffic Generator:** The traffic generator is considered the key component of the BE since it is responsible for managing the formulation of transactions, preparing them for submission (include signatures etc.) and then validate the transaction if succeeded. Also, the traffic generator would be designed to be able to adjust the transaction rate of the network. Thus, the user should be able to try different transaction rates while trying to

find the network's limits. This component is pivotal in confronting Observation E, regarding the imbalance between simulation assumptions and real-world performance, by ensuring a realistic simulation environment for the blockchain under test.

By incorporating these components into the BE, the architecture is poised to address the identified research gaps (Observations A, B, D, and E). The effectiveness of this approach is further validated through Hypotheses H1, H2, and H4.

3.4.1.2 Monitoring System

The primary objective of designing and implementing the monitoring system is to directly address Observation C, which emphasizes the need for robust tools and frameworks to assess the blockchain under test. This is of paramount importance as effective monitoring can shed light on the real-world performance of the blockchain, bridging the imbalance noted in Observation E. Consequently, several services should be included which are considered key elements towards the implementation of a dynamic monitoring system enabling easy storage, access, and visualization of the produced monitoring data. Among others, the Prometheus monitoring toolkit (*Prometheus - Monitoring System*, 2017) is suggested by the researcher to be used within the monitoring system. That includes:

- Prometheus monitoring server
- Push Gateway (supporting the scraping of the data),
- A set of metric's exporters, such as (Kastner, 2012; *Graphite Exporter*, 2012; *Docker Container Stats*, 2016)
- The alert manager (handling the alerts based on the user's specified rules.

InfluxDB, (InfluxData Inc., 2021), a high-performance time series engine would also be included for the storage of the produced time series data. Finally, Grafana, an analytical and visualization tool is proposed to be incorporated within the MS. This tool is pivotal, as it not only bridges the gap in Observation F concerning user-friendly interfaces but also ensures that data are collated and presented in an organized and structured manner. With Grafana (Grafana, 2020), users can seamlessly configure more data sources from several blockchain protocols and databases achieving a high level of interaction and contrast. Monitoring data can then be

appended in charts and pies, or even extracted in a friendly manner providing easy understanding of the overall findings. Figure *3.4* illustrates the architecture of the MS, along with the interactions between its components.

By implementing this MS, the architecture is primed to address the challenges identified in Observations C and F. The effectiveness of this approach is evaluated through Hypothesis H2.

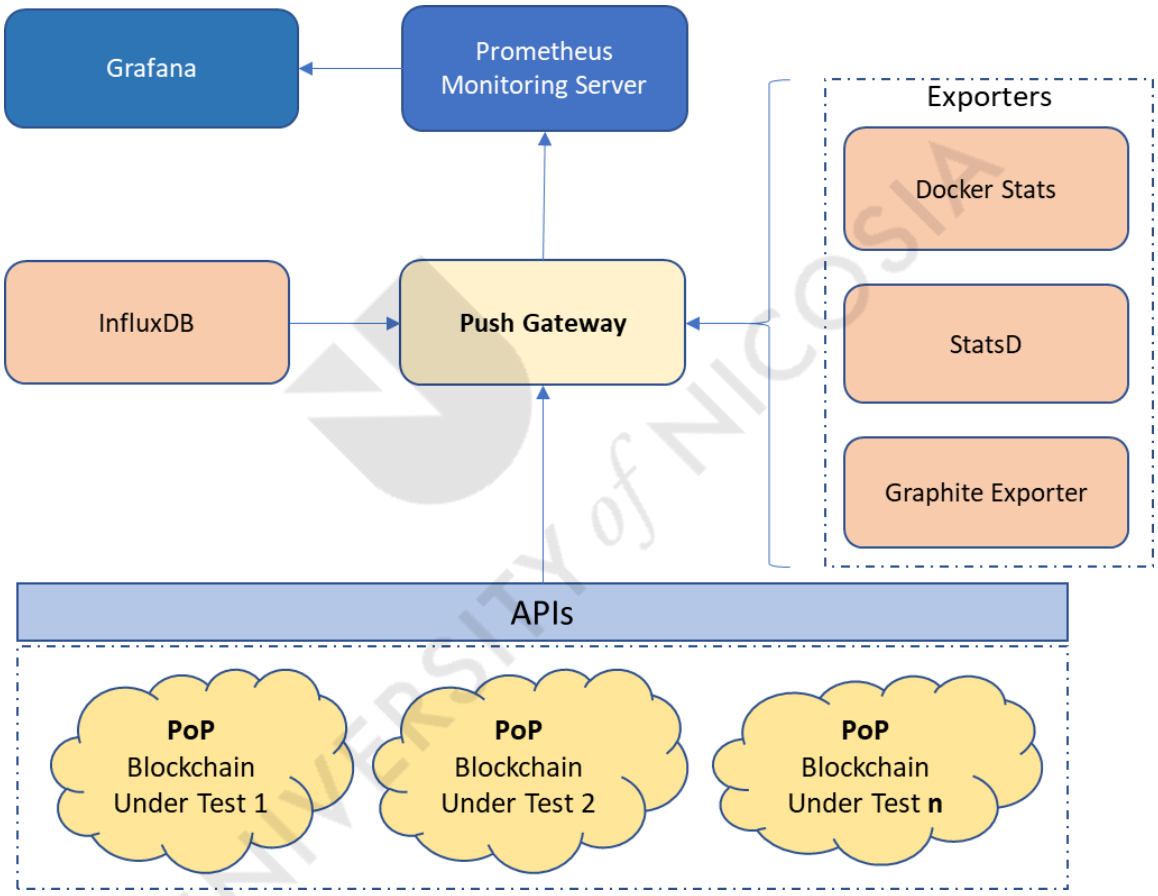


Figure 3.4: Monitoring System – Architecture

3.4.1.3 Graphical User Interface – BBF's Access Portal

In light of Observation F, which identified a palpable absence of user-friendly interfaces in blockchain performance measurement tools, the introduction of a GUI for BBF serves as a distinct advantage over current solutions. The primary objective of the BBF's GUI is to mitigate the barrier that exists between non-technical users and complex frameworks. This ensures that those lacking specific technical expertise may effectively utilize and engage with the system.

Moreover, addressing the fragmentation challenges of Observation D, the GUI offers an intuitive platform for users to engage seamlessly with the underlying mechanisms of both the BE and the MS. In doing so, it aids in demystifying the complexities surrounding blockchain protocols and operations, fostering an inclusive environment for both novices and experts.

The portal for the BBF will be designed and developed using cutting-edge technologies, adhering to material design principles. Through the API interfaces presented by each service of the BE and the MS, it ensures a smooth communication conduit with the rest of the system. Eschewing the need for back-end services, the portal would rely entirely on the API provided by the various platform microservices via the BBF. The UI files would be facilitated by a dependable web server such as Nginx (Nedelcu, 2010).

Delineating its features, the Portal would be organized into several modules:

- **Dashboard screen**: As the user's initial touchpoint post-login, it offers a snapshot of the platform's current status.
- **Users section**: Catering to administrative needs, this section allows for the creation and editing of user profiles, dictating access levels across the portal.
- **Testing and Benchmarking**: Acting as the heart of the BBF's operations, users can manage blockchain protocols and execute benchmark tests on the selected blockchain.
- **Monitoring System**: A direct bridge to Observation C, this section fosters interaction with the MS. Facilitating users' exploration of monitoring data acquired from benchmarking activities, it provides visual depictions such as pie charts and diagrams to extract meaningful insights from unprocessed data.

The GUI/Access Portal for the BBF is presented here as a conceptual design, reflecting an initial vision for a user-friendly interface. It is important to note that the BBF is an evolving tool, and this GUI design will undergo iterative refinements informed by subsequent empirical testing and user feedback. Moreover, the Portal is set to be developed in parallel with the BBF, incorporating novel features as they materialize. With the BBF's portal, the architecture effectively responds to the challenges pinpointed in Observations D and F. The value proposition of this interface is validated through Hypotheses H3.

3.5 Research Hypotheses

As a result of the analysis presented in this chapter, the researcher proposes an architecture for the conceptual model described in Section 3.3. This proposal emerges from the identified research gap (Observations A-F), as observed in Chapter 2-Section 2.4. The challenges revealed critical aspects in the field of blockchain technology. From the limitations of current CAs to the deficiencies in tools and frameworks for blockchain protocol performance assessment, the need for better integration in the blockchain ecosystems, and ensuring simulations that mirror real-world performance, the gamut of challenges is extensive.

The intent behind formulating these hypotheses is two-fold. Firstly, they aim to validate the proposed model's capacity to effectively address the highlighted challenges. Secondly, they serve as quantifiable and empirical checkpoints to ascertain the model's real-world applicability and efficacy.

In order to address these challenges and further enhance the conceptual clarity of this thesis, the researcher has delineated a collection of hypotheses in the subsequent work. Each hypothesis, deeply rooted in the research gap identified from the systematic literature review, is tailored to scrutinize a specific aspect of the proposed architecture. They function as the fundamental basis for the testing and assessment of the model, demonstrating the ever-changing connections between the proposed model's components and the broader objectives of the research.

- **Hypothesis 1 (H1):** The development of a new blockchain CA that adequately balances decentralization, security, and scalability enhances the operational efficiency and security of blockchain applications. (Targets: Observation A and B)
    - **Corresponding Architectural Component:** H1 evaluates the capabilities and design of the Benchmarking Engine (BE), which is responsible for evaluating different CAs and their associated efficiencies.

- **Hypothesis 2 (H2):** The implementation of comprehensive tools, frameworks, and documentation significantly improve the assessment and performance of blockchain protocols. (Targets: Observation C)
    - **Corresponding Architectural Component:** H2 scrutinizes both the Benchmarking Engine (BE) for its performance assessment functionalities and the Monitoring System (MS) for its analytical capabilities.

- **Hypothesis 3 (H3):** Enhancing the accessibility and usability of blockchain ecosystems, including seamless configuration, and bootstrapping of private blockchain protocols, encourage the adoption and understanding of blockchain technologies. (Targets: Observation D)
    - **Corresponding Architectural Component:** H3 is primarily linked to the GUI – BBF's Access Portal, which serves as the primary point of interaction for users.

- **Hypothesis 4 (H4):** Blockchain simulation frameworks that closely mimic real-world conditions provide more accurate and reliable performance assessment results than those based on theoretical assumptions. (Targets: Observation E)
    - **Corresponding Architectural Component:** H4 aligns with the Benchmarking Engine (BE), particularly in how it simulates and evaluates blockchain operations.

Figure *3.5* provides a concise schematic of these linkages, ensuring a comprehensive understanding of the research's structure and progression.

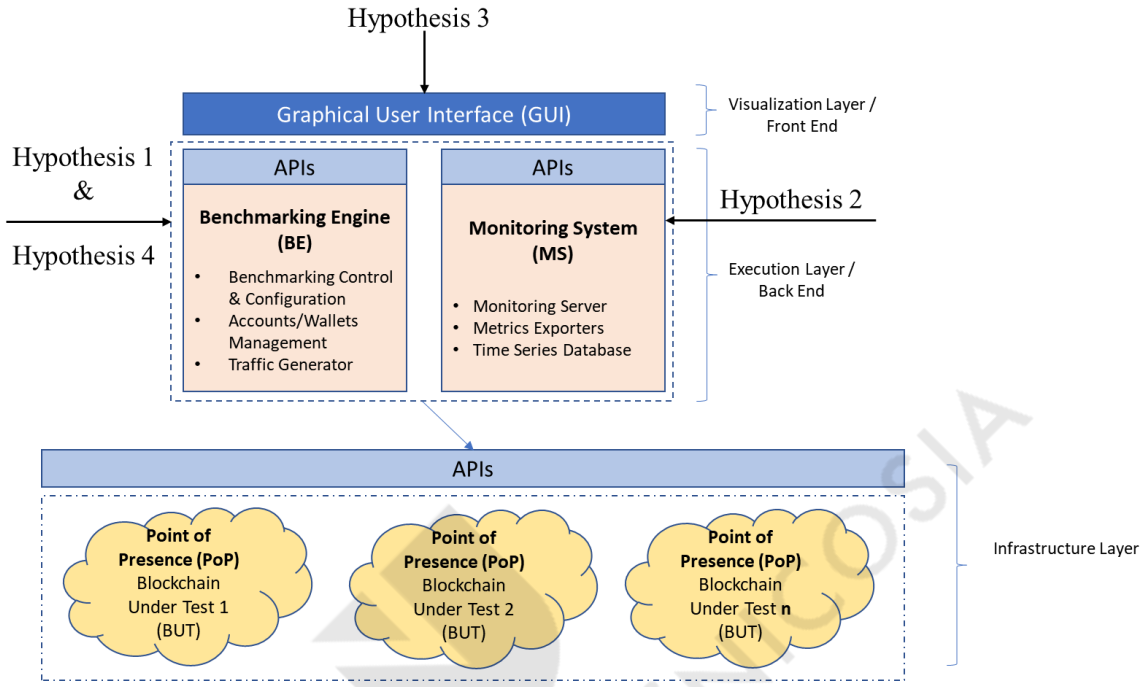


Figure 3.5: Linking Challenges, Architectural Components, and Hypotheses

3.6 Conclusions

Chapter 3 presents the proposed conceptual framework for this thesis, which not only aims to improve the decision-making process and assist experts and non-experts in choosing a suitable blockchain protocol based on their requirements and needs, but also endeavors to introduce a BBF. The BBF is envisioned as a pivotal tool for developers and researchers, enabling them to validate various implementation aspects of their theoretical constructs. By utilizing the BBF, they can rigorously test and assess their innovations, ensuring robustness and reliability, before releasing updates to the public main net of the corresponding blockchain protocol. In Chapter 3, the research challenges derived from Chapter 2 are analyzed thoroughly and discussed. Additionally, detailed proposed suggestions for the open issues are presented. As a result, the blockchain benchmarking process is proposed and depicted in Figure *3.2*. The development of the blockchain benchmarking process provides an overview of the cooperating

parts of the proposed benchmarking framework. The proposed BBF architecture is presented in detail in Section 3.5 of Chapter 3. The five proposed elements of the blockchain benchmarking process are: a) Blockchain Protocol Selection, b) Benchmarking Scenario Selection, c) Simulation of the benchmarking scenario, d) Data Generation, and e) Data Assessment. The latter is the basis for the design and implementation of the proposed conceptual framework (BBF). In the rest of this chapter, the conceptual architecture of the proposed BBF is discussed. Along with the high–level architecture of the BBF, the proposed architectural components of the BBF as these are the a) Benchmarking Engine, b) Monitoring System and c) Graphical User Interface – BBF's Access Portal are explained. Moreover, a set of research hypotheses have been included in Section 3.4, which are going to serve as the foundation for testing and evaluation of the proposed BBF. The next chapter, Chapter 4, presents and justifies the research methodology adopted to test the proposed model.

Chapter 4: Research Methodology

The beginning of knowledge is the
discovery of something we do not understand.

Frank Herbert (1920 – 1986)

Summary

In this chapter, the research methodology developed to evaluate the conceptual framework outlined in Chapter 3 is presented. The chapter begins by exploring several research procedures and approaches. It explains the choice of a positivist philosophical perspective and a deductive research strategy. Next, it justifies the quantitative research approach and concludes with a description of the experimental research protocol's design. This protocol integrates three pivotal components: a) design, b) experimental research/data collection involving two different blockchain clients, and c) data analysis as collected from the execution of experiments.

4.1 Introduction

This thesis investigates the dynamics of blockchain CAs, with a particular emphasis on their scalability, security, and decentralization. Central to this investigation is the aim to propose a conceptual model that can assess the performance of these blockchains. Chapter 2 details a SLR, with the key findings outlined in Section 2.3. These findings pave the way for the researcher to conceptualize a BBF as described in Chapter 3. Moving into this chapter, the justification for selecting the specific research methodology to test the conceptual framework is described.

The research onion model by Saunders et al., (2019) serves as a guide, presenting a comprehensive overview of the decision-making layers involved in the research design. As depicted in Figure *4.1*, it is comprised by six distinct layers: research philosophy, research approach, research strategy, choices, time horizon, data collection methods, and data analysis methods. Each layer offers a range of options, allowing the researcher to make informed decisions best suited to this study.

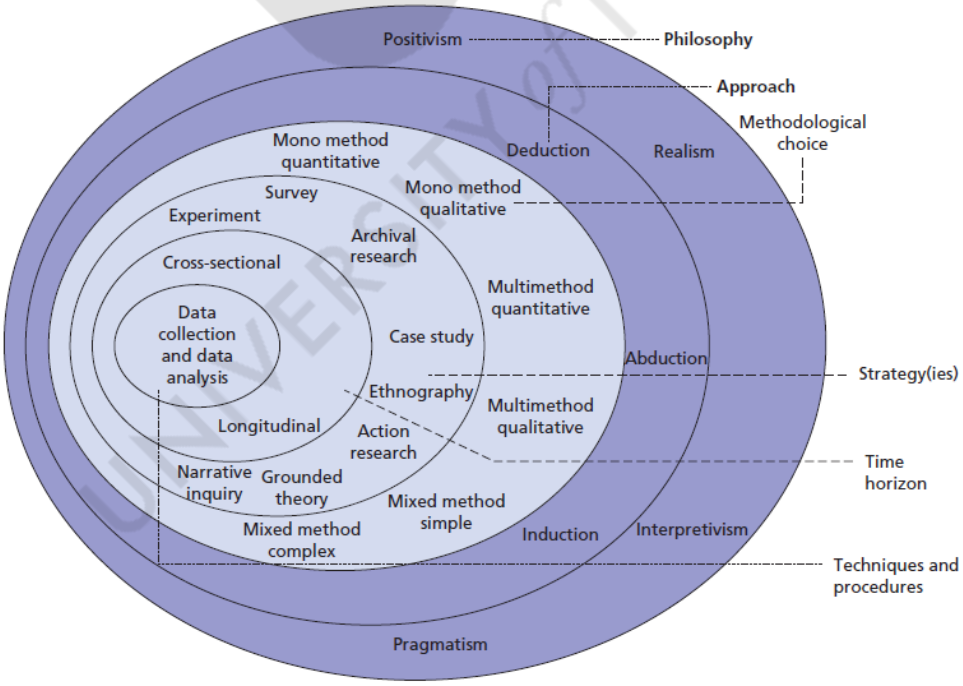


Figure 4.1: Research Onion Model. Source:(Saunders et al., 2019)

In the following sections, the researcher elaborates on the available research philosophies and approaches while also discussing the specific methodology adopted for this thesis. Section 4.2.1 describes the available philosophical perspectives while in Section 4.2.2 the research approaches are elaborated upon. In Section 4.2.3, the researcher justifies the selection of positivism research philosophy, as this is aligned with the objectives of this study, and deductive research approach. In the rest of this chapter, the methodological approach is also discussed as well as the research strategy. Finally, the chapter concludes with a description of the experimental research protocol's design which integrates three pivotal elements: a) research design, b) experimental research/data collection, and c) data analysis.

4.2 Selecting a Research Philosophy and Approach

Prior to determining the most suitable research philosophy and methodology for this thesis, it is critical to conduct a comprehensive examination of the existing philosophical perspectives and associated research approaches in the field of computer science. This analysis fulfills two primary objectives: it enhances comprehension of the dynamic relationship between blockchain technology and computer science; and it provides the rationale for the researcher's selected philosophical position and approach for this study.

4.2.1 Philosophical Perspectives

Philosophical perspectives are fundamental foundations in the world of academic research, providing a structured lens through which researchers analyze, comprehend, and interact with the phenomenon under examination. These viewpoints not only have an impact on the approaches, tactics, and instruments utilized, but also provide direction for the analysis and interpretation of the study results. A comprehensive understanding of these paradigms is needed to justify the chosen research methodology and ensure its alignment with the research objectives of this thesis (Tamminen and Poucher, 2020).

According to Park, et al., (2020), positivism philosophical perspective holds that knowledge is derived from measurable and observable occurrences and promotes empirical and methodical research. This implies the presence of an objective reality that is separate from human

perception. As a rule, positivist research is preoccupied with testing hypotheses, utilizes systematic methodology, and favors quantitative approaches to establish causal relationships and generalizable conclusions (Pawlikowski *et al.*, 2018). On the other hand, interpretivism (Ryan, 2018) places emphasis on the inherent subjectivity of human knowledge, contending that reality is a product of social construction and that its understanding is contingent upon experiences and circumstances. Phenomenological research guided by this philosophical standpoint aims to comprehend the differences of experiences and meanings of individuals, placing less emphasis on generalizations and more on qualitative investigations.

Realism is a synthesis of interpretivism and positivism, as it acknowledges the existence of an objective reality apart from human cognition while also permitting the influence of societal conceptions and individual perspectives on our comprehension of this reality (Miller and Tsang, 2011). Realism generally employs a mixed-methods strategy, which integrates qualitative and quantitative data in recognition of the significance of individual judgments and the external world. In conclusion, Pragmatism is distinguished by its adaptable research methodology, which does not adhere to a specific philosophical ideology or conception of reality (Morgan, 2014). Practical considerations and the efficacy of solutions motivate it. Diverse in nature, pragmatic research frequently employs mixed techniques to guarantee a comprehension of the study inquiry while placing considerable importance on tangible outcomes and practical implications.

4.2.2 Research Approaches

Research approaches serve as the foundation upon which the structure of a study is built. They provide a systematic pathway guiding the progression from theory to data collection, therefore bridging the gap between the philosophical underpinnings of the research and its empirical execution. There are primarily two research approaches: deductive and inductive (Soiferman, 2010). Each approach offers a unique perspective on the relationship between theory and research.

The deductive approach, alternatively referred to as the "top-down", generates more hypotheses from a broad theory. The results of systematically testing these assumptions contribute to the creation or refining of theory. Deductive research is distinguished by its

methodical framework, which commences with a well-defined hypothesis grounded in established theory and endeavors to empirically examine this hypothesis. The inductive approach, sometimes known as the "bottom-up" method, commences with observations or data. Researchers scrutinize this material in search of patterns, developing provisional hypotheses that may evolve into more extensive generalizations or theories. Exploratory and unstructured, inductive research disregards prior notions and permits hypotheses to develop from the evidence.

Abduction, a research approach that incorporates both induction and deduction, is an alternative to deductive and inductive reasoning. It begins with a collection of observations that is insufficient and then proceeds to propose the most probable explanation for the group. Iterative in nature, abductive research frequently cycles between theory and data, refines hypotheses in response to the emergence of new evidence, and attempts to account for the unexpected in a manner that advances the development of a new theory or the modification of an existing one. This method is especially advantageous in research situations where neither pure deduction nor induction are completely appropriate (Soiferman, 2010).

4.2.3 Justifying the Selection of Positivism Philosophical Stance and Deductive Research Approach

The purpose of this thesis is to test whether the proposed BBF may be utilized to verify the design choices and technical specifications of different blockchain protocols before they are made publicly available. To achieve that, an empirical research approach is required; hence, a positivist philosophical perspective is selected, as suggested by Pawlikowski et al. (2018). Positivism is consistent with the imperative to mitigate subjective biases, a critical consideration in a domain that demands reliable and credible conclusions. The dedication of this concept to standardized and replicable methodologies guarantee the applicability of the study's findings to wider contexts.

The research methodology employed in this thesis is rigorous and structured, mirroring the attributes of positivism, which entails the formulation of hypotheses - as those are discussed in Section 3.5 - followed by their empirical testing based on the collected data. By using this

methodology, the study outcomes are rendered precise and uniform, hence enhancing their credibility and applicability in both academic and practical contexts. As described by Pandey, (2019), the deductive research method satisfies the empirical testing criterion of this thesis. This methodology proceeds methodically from the hypotheses introduced in Chapter 3 to empirical examination in Chapter 5, which aligns with the objectives of the study.

The power of the deductive approach resides in its ability to empirically examine precisely stated hypotheses, assuring that the inquiry maintains fidelity to its fundamental theoretical frameworks. The thesis's precise research question is well-suited to the organized format of this method, which establishes a direct line of reasoning from the conceptual framework to the empirical assessment of the BBF. The selection of positivism and the deductive method is founded on their capacity to furnish a transparent structure for examining and validating the BBF in relation to the performance of the blockchain protocols.

4.3 Selecting a Methodological Approach

The methodological approach describes how data are collected and analyzed.

4.3.1 Qualitative vs. Quantitative Research Methods

Qualitative and quantitative research methods are two broad categories of research methods that are often used in social science research (Reichardt and Rallis, 1994). Qualitative research methods involve the collection and analysis of non-numerical data, using techniques such as interviews, observations, and documents, while quantitative research methods involve the collection and analysis of numerical data, such as surveys, experiments, and statistical analysis. One of the main differences between qualitative and quantitative research methods is the type of data that is collected. Qualitative research methods collect data in the form of words, images, and observations, and aim to gain an in-depth understanding of a particular phenomenon or issue. In contrast, quantitative research methods collect data in the form of numerical values and aim to generalize findings to a larger population. Another difference between qualitative and quantitative research methods is the way in which data are analyzed. Qualitative research methods typically involve the use of thematic analysis, where data are analyzed by identifying

recurring themes or patterns. Quantitative research methods, on the other hand, involve statistical analysis, where data are analyzed using statistical tests and measures (Bartoletti *et al.*, 2018).

The choice between qualitative and quantitative research methods depends on the research question, as well as the nature of the data that are collected (Baškarada and Koronios, 2018). Qualitative research methods are often used when the research question is exploratory and aims to gain a deep understanding of a particular phenomenon or issue. They are also useful when the data being collected are complex and difficult to quantify, such as emotions or perceptions. Quantitative research methods are often used when the research question is confirmatory and aims to test a hypothesis or generalize findings to a larger population. They are also useful when the data being collected are numerical and can be analyzed using statistical tests and measures. A brief comparison between quantitative and qualitative research methods is illustrated in Table *4.1*.

Table 4.1: Qualitative VS Quantitative Research Methods

CRITERIA	Qualitative Research Methods	Quantitative Research Methods
Data	Non-numerical (e.g., words, images, observations)	Numerical (e.g., surveys, experiments)
Aim	To gain an in-depth understanding of a particular phenomenon or issue	To generalize findings to a larger population
Analysis	Often thematic, identifying recurring themes or patterns in the data	Statistical, using tests and measures
Appropriateness	Useful for exploring complex and difficult-to-quantify data, such as emotions or perceptions	Useful for testing hypotheses and generalizing findings
Results	Descriptive and interpretive	Numerical and statistical
Samples	Often involves small, non-representative samples	Often involves large, representative samples
Focus	Focuses on the subjective experiences of individuals or groups	Employs standardized methods to measure behavior or attitudes, aiming for consistency and replicability in data collection, even when capturing subjective experiences.

4.3.2 Justifying the Quantitative Research Method

In order to test the proposed benchmarking framework, this thesis adopts a quantitative research method, underpinned by the positivist research philosophy. Multiple factors are considered while determining whether to use a quantitative or a qualitative approach. Firstly, the blockchain ecosystem is data-driven, as evidenced by its numerical metrics, such as transaction speed, network latency, and CA types. In addition to facilitating the collection of numerical data, a quantitative research approach enables the utilization of statistical analysis to derive accurate interpretations and valuable insights.

Moreover, an aspect of the quantitative paradigm is the investigation of causal relationships that exist between variables. This aspect of quantitative research is well-suited to the goals of the thesis. Additionally, the approach's commitment to positivism encourages objective and empirical observations, which are essential for maintaining the neutrality of the results. These findings are firmly based on real data. An essential component of this investigation is the implementation of the BBF, a framework that provides a standardized means of comparing blockchain protocols and their corresponding CA. The consistency and replicability of the experiments are enhanced by the BBF, hence strengthening the study's validity and reliability.

Considering the empirical characteristics of blockchain technology, the differences of its performance measures, and the objective of establishing a reliable benchmarking framework, a quantitative research methodology is deemed the most suitable technique for this study. This methodology is not solely rationalized by the data-centric nature of the topic but is also required by the need for a standardized assessment of technological performance, which is most effectively accomplished using quantitative techniques.

4.4 Selecting a Research Strategy

The research strategy delineates a cohesive structure for gathering data in a manner that adequately investigates the research questions. The decision-making process encompasses several approaches, such as experimental research, case study, survey, or another methodology,

which significantly influence the collection and interpretation of evidence in relation to the study's objectives. This strategic choice is crucial in guaranteeing the robustness of the research design and the validity and reliability of the findings.

4.4.1 Quantitative Research Strategies

Based on the positivist paradigm, quantitative research places significant emphasis on the quantification and examination of causal connections among variables. Generally, it entails the methodical and empirical examination of phenomena that are observable by computational, mathematical, or statistical methods. Various diverse tactics may be used under the quantitative methodological approach, contingent upon the characteristics of the data and the research subject at hand.

The rest of this section provides an outline and explanation of the main quantitative research strategies that are pertinent to investigations within the domain of blockchain technology.

- **Surveys:** Surveys are structured instruments designed to gather specific information from a large group of individuals. They can be cross-sectional (capturing data at a single point in time) or longitudinal (capturing data over an extended period) (Valsiner, 2000).
- **Experiments:** Experiments involve a controlled manipulation of one or more independent variables to determine their effect on a dependent variable. They often employ control groups and randomization to ensure validity (Cerniglia, Fabozzi and Kolm, 2016).
- **Quasi-experiments:** Quasi-experiments resemble experiments but lack certain controls, especially randomization. They are particularly useful when true experimental designs are unfeasible (Apuke, 2017).
- **Secondary Data Analysis:** This strategy involves analyzing data that has already been collected for some other purpose. It can save time and resources but relies on the availability and quality of existing data (Kwadwo Antwi and Hamza, 2015).
- **Simulations:** Simulations replicate real-world processes in a controlled environment. They can be particularly useful when real-world experimentation is costly, risky, or time-consuming (Brandt and Timmermans, 2021).

The subsequent sections will expound upon the justification for selecting a particular quantitative approach for this study, placing particular emphasis on its congruence with the objectives of the study and the characteristics of the collected data.

4.4.2 Justifying the Use of Experimental Research Strategy

When it comes to research strategies, the choice of a specific one must be entirely aligned with the study's overall purpose, the attributes of the data to be collected, and the research objectives. In order to investigate the performance of blockchain protocols over a range of scenarios and conditions, the experimental research approach is deemed the most suitable methodology for this thesis. This segment explains the justification that supports the latter.

- **Nature of the Study:** Through the simulation of Byzantine attacks on various blockchain protocols and monitoring their subsequent performance, this study adopts the characteristics of an experimental methodology. It emphasizes on the proactive intervention rather than just passive observation to derive insights.
- **Control and Manipulation:** Experimental research is distinguished by its capacity to apply control over variables (Chan, 2015). While some variables such as transaction volume, block size, and network size stay constant throughout this investigation, others, like the nature of the attack, vary. This regulated manipulation facilitates a more precise comprehension of the way certain modifications affect the overall performance of blockchain protocols.
- **Causal Relationships:** Experimental research excels in establishing causal relationships. By controlling and manipulating certain variables, it becomes feasible to assert with confidence that a particular change led to a specific outcome. Given that this research aims to understand how various scenarios impact the performance of blockchain CAs, establishing such causal links is imperative.
- **Validity and Reliability:** By employing controlled conditions and scenarios, experimental research enhances the internal validity of the results by ensuring that the observed outcomes are indeed the consequence of the manipulations performed.

Additionally, by following a systematic approach where variables are manipulated in a structured manner, the results become replicable, enhancing the reliability of the findings.

- **Quantitative Data Collection:** The experimental strategy aligns well with the study's reliance on quantitative data. By simulating attacks and observing outcomes, the research generates numerical data, such as transaction speeds or network latencies, which can be statistically analyzed to draw meaningful conclusions.

Considering the research objectives of this thesis, as well as the nature of data collection and analysis, the experimental research strategy emerges as the most suitable approach. It not only aligns with the methodological needs of the study but also ensures that the insights gleaned are both valid and reliable. Adopting this strategy, the research stands poised to offer robust, actionable insights into the performance of blockchain CAs across different protocols and scenarios.

4.5 Empirical Research Methodology

Drawing from Themistocleous (2004) work, the empirical research methodology encompasses three primary stages: a) Research Design, b) Data Collection, and c) Data Analysis, as these are discussed and examined in this section. These stages are crucial for structuring the research process and ensuring the validity of the findings. In the subsequent sections, the researcher delves deeper into each of these steps, providing a comprehensive understanding of their significance and application. According to Creswell (2017), the research design serves as the blueprint for the study, guiding the selection of appropriate methods and techniques to address the research hypotheses. It involves decisions related to the research approach, philosophy, and strategy that best align with the study's objectives.

The data collection stage, as highlighted by Saunders (2018) and Hair et al. (2015) involves gathering relevant information to address the research hypotheses. This stage necessitates the careful selection of suitable data sources, instruments, and sampling techniques to ensure the accuracy and reliability of the collected data. Finally, the data analysis stage, as described by (Brandão, 2015) and Ridder et al., (2014), entails the systematic examination of the collected

data to identify patterns, relationships, and insights that inform the research findings. Employing appropriate analytical methods and tools is essential for extracting meaningful conclusions from the data. In conclusion, the three stages of empirical research methodology – Research Design, Data Collection, and Data Analysis – are integral to conducting a rigorous and valid study. Further exploration of each stage in the following sections provides valuable insights into their role in shaping the research process and findings of this thesis.

4.5.1 Research Design

During the first stage of the empirical research methodology, the research design plays a crucial role. In this phase, the researcher:

- **Identifies the research problem:** This involves defining the research problem and clarifying the aim and objectives of the study. The research problem serves as the foundation for the entire investigation.
- **Develops the theoretical framework:** The researcher reviews existing literature to understand the current state of knowledge in the field, identifying key theories, concepts, and gaps that inform the development of the study's theoretical framework.
- **Adopts a research philosophy:** The researcher chooses an appropriate research philosophy, such as positivism, interpretivism, or pragmatism, which informs the underlying assumptions about the nature of reality and knowledge generation in the study.
- **Selects the research approach:** The researcher determines whether the study would follow a qualitative, quantitative, or mixed-methods approach based on the research aim and objectives, as well as the nature of the data required to address them.
- **Chooses a research strategy:** The researcher selects a suitable research strategy, such as a survey, or experiment, based on the aim, objectives, and the type of data required for this study.
- **Designs the data collection and analysis procedures:** The researcher plans how data are collected and analyzed, including selecting data sources, instruments, and sampling techniques, as well as determining appropriate data analysis methods and tools.

4.5.2 Data Collection

In the second stage of the empirical research methodology, data collection plays a vital role in generating evidence to answer the research hypotheses and address the study's objectives. As a quantitative method is selected with experimental research involving two different blockchain protocols, this section elaborates on the steps undertaken for the data collection process. The choice of two blockchain protocols is further explained and justified in Section 4.6.2.

To test and evaluate the BBF, the researcher first identifies the specific data requirements for the two blockchain use cases, focusing on decentralization, security, and scalability metrics.

- **Select data sources:** The researcher determines relevant data sources for the two selected blockchains, such as its public ledger, transaction data, network statistics, and other relevant documents or repositories that provide quantitative information on the CA and the corresponding blockchain's network performance.
- **Develop data collection instruments:** Appropriate instruments and tools are designed or selected to collect the required data from the identified sources. These may include APIs, custom scripts, or other software tools to extract quantitative data on the two blockchains under test.
- **Determine sampling techniques:** The researcher chooses appropriate sampling techniques, such as stratified sampling or time-based sampling, to ensure that the collected data are representative over time or under different conditions.
- **Collect data:** The researcher gathers the required data from the identified sources using the selected instruments and sampling techniques. This process involves extracting, organizing, and storing quantitative data on the blockchains performance metrics, such as transaction throughput, latency, and resource consumption.
- **Pre-process and prepare data:** Once the data are collected, the researcher pre-processes and prepares it for analysis. This step may involve cleaning, transforming, or aggregating the data to ensure its quality and suitability for analysis.

By following these steps, the researcher obtains robust quantitative data on the selected blockchain's performance, enabling the testing and evaluation of the BBF followed in Chapter 5.

4.5.2.1 Data Collection Tools

This section discusses the data collection tools used for the quantitative methodological approach used in this thesis. The focus is on the possible experiments, including simulation of Byzantine attacks on two different blockchain protocols, monitoring the network, and gathering data.

- **Simulation tools:** To simulate Byzantine attacks on a blockchain protocol, the researcher uses simulation tools specifically designed for blockchain protocols. These tools allow the design and execution of custom attack scenarios and the analysis of their impact on the network's performance and CA.
- **Network monitoring tools:** Monitoring the blockchains under test is essential to gather real-time data on its performance during the experiments. Tools like Grafana (Grafana, 2020), Prometheus (*Prometheus - Monitoring System*, 2017), or other blockchain monitoring solutions are employed to track key metrics such as transaction throughput, latency, and resource consumption.
- **APIs and SDKs:** The blockchains under test, provide APIs and SDKs that are used to extract data directly from the blockchain ledger. These tools facilitate access to information on transactions, state of ledger, network topology, and other relevant data points, which are then used to analyze the network's performance and the effectiveness of the BBF.
- **Custom scripts and tools:** Depending on the specific data requirements of the experiments, the researcher develops custom scripts or tools to extract, process, or analyze the data. These scripts are written in programming languages like Python, JavaScript, or others, and can interact with the blockchain’s APIs, SDKs, and monitoring tools.

- **Data storage and management tools:** Once the data are collected, the researcher stores and manages it effectively. Tools like relational databases (e.g., MySQL, PostgreSQL) or NoSQL databases (e.g., MongoDB, Couchbase) are used to store the collected data, ensuring its accessibility, consistency, and integrity.

By utilizing these data collection tools, the researcher designs and conducts experiments on the blockchain protocols, simulating Byzantine attacks, monitor the network, and gather valuable data to evaluate the BBF's performance concerning decentralization, security, and scalability metrics.

4.5.3 Data Analysis

The last stage of the empirical research methodology is data analysis, which involves interpreting the collected empirical data. Actions taken during data analysis include, among others:

- **Data cleaning and preparation:** Before analyzing the data, it is essential to clean and prepare them to ensure its quality and suitability for analysis. This step may involve removing outliers, handling missing values, and transforming variables to make the data consistent and compatible with the chosen analytical techniques.
- **Descriptive statistics:** The researcher calculates descriptive statistics, such as means, medians, standard deviations, and ranges, to provide an initial understanding of the data's distribution and characteristics.
- **Visualization:** Visualizations, including charts, graphs, and plots, are used to present the data and facilitate its interpretation. These visualizations help identify patterns, trends, and relationships in the data, making it easier to communicate the findings and draw conclusions.
- **Model evaluation:** The researcher evaluates the effectiveness and applicability of the BBF by comparing the results of the experiments with the blockchains under test against established benchmarks or theoretical expectations. This step may involve calculating performance metrics, such as accuracy, precision, or recall, to assess the framework's

effectiveness in capturing the essential aspects of decentralization, security, and scalability of the blockchain under test.

- **Interpretation and conclusions:** Finally, the researcher interprets the results of the data analysis in the context of the research questions and objectives. This step involves drawing conclusions about the performance of the blockchain CAs and the BBF, discussing the implications of the findings, and relating them to the existing literature.

By following these actions, the researcher analyzes the collected data rigorously and systematically, enabling a comprehensive understanding of the blockchain CAs' performance and the effectiveness of the proposed BBF.

4.5.3.1 Data Triangulation

Data triangulation is a research technique that involves using multiple sources, methods, or perspectives to validate and enhance the reliability and validity of the study's findings (Denzin, 2017; Roulston and Halpin, 2022). By validating the results obtained from different data sources or methodologies, researchers can increase their confidence in the conclusions drawn, reduce potential biases, and obtain a more comprehensive understanding of the phenomenon under investigation.

In the context of this study, the data triangulation process aims to ensure a thorough evaluation of the blockchain CAs and the proposed BBF. The following steps are taken to achieve the aforementioned goal:

- **Multiple data sources:** The researcher collects data from various sources, such as transaction logs, network statistics, and relevant documents or repositories. This approach enables the researcher to capture different aspects of the blockchains under test and minimize potential biases arising from a single data source. The latter is further discussed in Section 5.5.2.1.2, Section 5.5.2.2.2, Section 5.6.2.1.2, and Section 5.6.2.2.2.
- **Investigator triangulation:** Involving various research in the data analysis process help to reduce potential biases and increase the study's reliability (Moon, 2019). The researcher collaborates with other experts in the field – as discussed in Section 4.6.2.2 -, seeking their input and feedback during the data analysis and interpretation stages.

- **Theoretical triangulation:** As it is discussed in Section 5.7, the researcher compares the findings of the study with existing theories and models around blockchain and benchmarking literature. This process helps identify potential gaps or discrepancies, contributing to the development of new insights and the refinement of the BBF.

By incorporating the data triangulation process, the researcher enhances the reliability and validity of the study's findings, leading to more robust and trustworthy conclusions regarding the performance of blockchain CAs and the effectiveness of the proposed BBF.

4.6 Experimental Research Protocol

This section outlines the experimental research protocol for the empirical research conducted in this thesis, involving two different blockchain protocols. The experiment design criteria detail the criteria used to select the experiments, while the data collection procedures describe the procedures for data collection, including the collection of primary data through experiments and simulations and the collection of secondary data through literature review and other relevant sources. The data analysis techniques include descriptive statistics, visualization, and content analysis. Table *4.2* summarizes the experimental research protocol for this research:

Table 4.2: Overview of the experimental research protocol for the empirical research

Sub-section	Description
Experiment Selection Criteria	Details the criteria used to select the experiments, including two different blockchain clients.
Data Collection Procedures	Describes the procedures for data collection, including the collection of primary data through experiments and simulations.
Data Analysis Techniques	Describes the data analysis techniques employed, including descriptive and inferential statistics, visualization, and content analysis.
Ethical Considerations	Addresses ethical considerations related to the experiment, such as data privacy and security, informed consent, and confidentiality.

4.6.1 Experimental Research Overview

To evaluate the performance of various blockchain CAs regarding decentralization, security, and scalability, an experimental research approach has been chosen. The experimental method allows for a detailed examination of the chosen blockchain protocol and their corresponding CAs. This approach involves analyzing two blockchain clients, the XRP Ledger and Ethereum, each representing a different CA, to identify their strengths, weaknesses, and potential trade-offs.

4.6.2 Experimental Research Procedures

This section outlines the procedures followed during the experimental research phase. The process is designed to ensure a systematic and rigorous examination of the selected blockchain protocols and their CAs, with the goal of understanding their performance in terms of decentralization, security, and scalability.

4.6.2.1 Justification for the Selection of Two Use Cases

In the research strategy employed for this thesis, two experimental research use cases are carefully selected. This decision is based on strategic considerations that emerged from the research objectives, design, and available resources. The primary research objective is to develop, implement, and test the BBF. Testing and refining the BBF required a manageable number of use cases to ensure focused attention on each. XRPL and Ethereum arechosen as they represent significant and differing instances of blockchain technology. XRPL is a payment protocol with a unique CA, while Ethereum is a general-purpose blockchain platform employing a different consensus method. This diversity allowed for a robust test of the BBF across different blockchain types and use cases. Limiting the number of use cases to two allowed for a more detailed and focused investigation, enabling a comparative analysis and enriching the findings of the research.

4.6.2.2 Selection of XRPL and Ethereum as Experimental Research Use Cases

The choice of XRPL and Ethereum is a strategic decision driven by the specified research goals and resource availability. One of the main aims is to test the BBF across diverse CAs. Ethereum employs a proof-based CA (initially Proof of Work, transitioning to Proof of Stake), and XRPL utilizes a unique voting-based CA called the RPCA. This selection ensured a broad test of the BBF. Support from the University Blockchain Research Initiative (UBRI) provided financial resources and access to experts from the Ripple community, making XRPL an ideal choice. Bitcoin is influenced by its technical similarities to Ethereum and environmental concerns. Ethereum's transition to Proof of Stake and XRPL's RPCA offered an exploration into more energy-efficient consensus mechanisms, aligning with the trend towards greener blockchain technologies.

4.6.3 Ethical Considerations

This thesis thoroughly examines ethical considerations, despite the lack of direct human data involvement. The researcher maintains a strong attention to the concepts of intellectual property

rights and honesty. Access to and use of all data sources, with a specific emphasis on those associated with blockchain protocols, are conducted in compliance to relevant data usage regulations and regulatory frameworks. The research methodology is implemented with precision and consistency, guaranteeing that no data are manipulated or misrepresented. Maintaining transparency throughout the research process is achieved by the detailed recording of data sources, methodology, and analytical procedures. In addition, any biases in data analysis and computational processes are analyzed and addressed. This thesis is dedicated to making a serious contribution to the area of blockchain while upholding the highest standards of ethical considerations.

4.6.4 Guidelines for Reporting the Research Findings

The next chapter methodically presents the results obtained from this study and the empirical data collected. The results and findings are presented in a clear manner that fits with the research methodology described in this chapter. Chapter 5 synthesizes additional data obtained from document analysis and places it in the context of the conceptual framework and the literature examined in Chapter 2. The presentation of the main findings systematically follows the principal aims of the thesis. This organization enables readers to comprehend the accomplishment of each objective and track the progress of this study. Quantitative data are presented using appropriate statistical representations, and any apparent patterns or anomalies are addressed in the discussion of Section 5.5.2.1.2, Section 5.2.2.2.2, Section 5.6.2.1.2, and Section 5.6.2.2.2.

4.7 Conclusions

This chapter has presented a thorough discussion on the research topic, the empirical research methodology, and the experimental research protocol, all aimed towards investigating the performance of blockchain CAs, focusing on the XRPL and Ethereum blockchain protocols. The chosen research methodology is a quantitative research strategy, underpinned by a positivist research philosophy. It consists of three stages: research design, data collection, and data analysis. The data collection procedures encompass experiments, simulations, systematic

literature review, and analysis of relevant documents and repositories related to both XRPL and Ethereum.

The proposed BBF is evaluated against a set of research hypotheses as those are described in Section 3.5. Data analysis techniques employed include descriptive statistics, visualization, and content analysis, with a data triangulation process ensuring the credibility and reliability of the findings. The experimental research protocol, including use case selection criteria, data collection procedures, data analysis techniques, and limitations ensures the credibility and reliability of the study.

This research is expected to contribute to the field of blockchain technology by proposing and evaluating a conceptual model for measuring the performance of blockchain CAs. The findings could potentially aid in the development of more efficient and secure blockchain protocols, including XRPL and Ethereum, thereby advancing the field of blockchain technology.

Chapter 5: Empirical Data and Research Findings

Without data, you're just another person
with an opinion.

W. Edwards Deming (1900 – 1993)

Summary

Chapter 5 presents the evaluation results of the proposed BBF considering the performance of two blockchain protocols: the Ethereum protocol with Proof of Authority (PoA) as the corresponding CA, and the XRPL protocol using a Byzantine Fault Tolerance (BFT)-like CA called Ripple Protocol Consensus Algorithm (RPCA). The evaluation includes an analysis of key performance metrics such as latency, throughput, consensus time, as well as security aspects like the protocols' response to a double spend attack and node failure/crash test. The results confirm that the BBF can be used as an effective tool for measuring the performance of blockchain protocols, and this finding may also lead to performance improvements. The main contribution of this chapter is to test the efficacy of the proposed BBF as a tool for validating the design decisions and technical specifications of blockchain protocols in an automated and methodological way.

5.1 Introduction

Blockchain technology has the potential to revolutionize many industries by providing a decentralized and secure way of recording transactions. However, the performance of blockchain protocols is a significant concern that directly impacts its adoption. To encourage broader adoption, it's essential for blockchain to balance its core promise of decentralization and security with performance efficiency. Recognizing and addressing the inherent trade-offs among decentralization, security, and scalability remains a pivotal consideration in the evolution of blockchain protocols for practical, everyday use. The relationship between performance and adoption is evident; as the efficiency and effectiveness of these protocols increase, so does their feasibility for broader, practical use. In Chapter 2, a systematic literature review is conducted to identify research areas for further investigation. The review highlights the need for a benchmarking framework to measure the performance of blockchain protocols, assess the trade-offs between decentralization, security, and scalability and validate design decisions. In response to the latter, Chapter 3 proposes a conceptual benchmarking framework for studying and analyzing the performance of blockchain protocols.

Chapter 4 presents the research methodology developed to evaluate the conceptual framework outlined in Chapter 3 while this chapter presents the empirical data and research findings from performing an evaluation of the proposed BBF using scenarios of two different blockchain clients. The methodology used for the evaluation of the BBF comprises an experimental research design focused on each blockchain protocol. These experimental investigations include a series of tests using the BBF to measure the performance of the protocols under test in terms of latency, throughput, and consensus time.

Subsequent sections focus on the experimental use cases considering the XRPL and ETH client, studying the design decisions of each for handling *double spend* attack and recovering from *node failures* or crash.

5.2 The concept of Double Spend Attack

A double spend attack is a potential flaw in a digital cash scheme where a single digital token can be spent more than once. This is possible because a digital token consists of a digital file that can be cloned or reproduced. Unlike physical tokens, such as coins or banknotes, digital tokens can be duplicated and spent in more than one place, effectively counterfeiting the digital currency. In the context of blockchain protocols, this problem is particularly challenging (Schreiber, 2019). As transactions on these networks are not always immediately committed to the ledger and thus creating a window of opportunity for malicious actors. During this window, an attacker can send a transaction, and before it is committed to the ledger, he/she can send another transaction spending the same tokens but directed to a different address, typically one they control.

In an effective double spend attack, both transactions are validated, leading to a situation where the same number of digital tokens is spent twice, undermining the integrity of the ledger, and leading to a loss of trust in the system (Kovalchuk *et al*., 2020). The XRPL, like many other blockchain protocols, is designed to mitigate the risk of double spend attacks. The RPCA is designed to reach consensus among nodes on the transactions to be included in the next ledger. As a result, in an effectively functioning XRPL, a double spend attack would be identified and rejected during the consensus process. In the following sections, this chapter describes how this attack is simulated on the XRPL client using the BBF, and the impact it has on the system's performance and validity.

5.3 The concept of Node Failure or Crash

A common occurrence in the domain of distributed systems, such as blockchain protocols, is node failure or crash, which can have a substantial effect on the network's security and functionality (Pezoa et al. 2010). A node or validator, in this context, refers to a machine or server that participates in the network by validating and relaying transactions. Nodes or validators play a critical role in maintaining the integrity, security, and overall functioning of

the blockchain protocol. Therefore, a failure or crash involving one or more nodes could have substantial implications.

A node failure or crash, as depicted in Figure *5.1* can be defined as a sudden and unexpected termination of a node's functions and responsibilities in the network due to reasons such as hardware failure, software bugs, network disruptions, power outages, or malicious attacks. The latter can make the node become unresponsive and/or unable to participate in transaction validation and block propagation, causing it to become disconnected from the network.

The normative literature reports two primary types of node failures: crash failures and Byzantine failures. A crash failure occurs when a node stops working, failing to respond to requests or perform tasks. On the contrary, a Byzantine failure refers to a condition where a node starts to behave maliciously, potentially sending out incorrect or conflicting information to other nodes in the network.

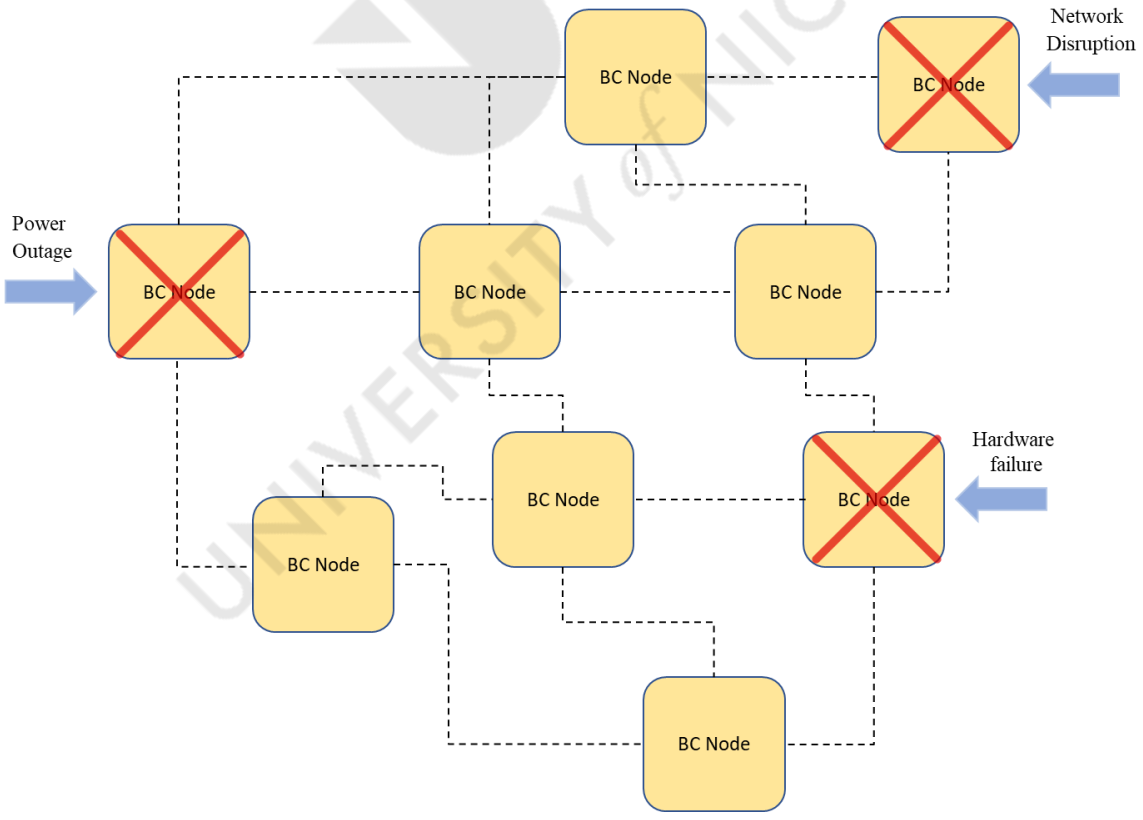


Figure 5.1: Blockchain Node Failure or Crash

In a blockchain protocol, node failures can influence the network's resilience, capacity, and performance. Specifically, they can affect the network's transaction throughput, latency, and ability to reach consensus, given that fewer nodes will be available to validate transactions and contribute to the consensus process. Moreover, in the context of the RPCA, used by XRPL, the failure of a single node may not significantly affect the network's overall operation due to its distributed nature Christodoulou et al., (2020). However, the simultaneous failure of multiple nodes, especially those possessing high influence in the network (like validators), can disrupt the consensus process, slow down transaction validations, and pose potential risks to the network's security.

5.4 Use Case One: The case of XRPL Client

This use case considers the XRPL client, utilizing the RPCA. Firstly, a detailed description of the XRPL is presented, examining its background, design principles, features, and limitations. Next, the BBF is instantiated to empirically evaluate the XRPL client's performance. This section also covers the specifics of the performance metrics chosen for this analysis, justifying their relevance to the study. In the latter part of this use case, the researcher moves onto experimental evaluations where two different Byzantine fault scenarios are executed to test the resilience and robustness of the XRPL client using the BBF as a controlled private environment.

5.4.1 XRPL Background

The XRPL, is a decentralized blockchain protocol heavily contributed to by Ripple, among other participants in its global network. Ripple's vision is to revolutionize the global payments industry using blockchain technology.

XRPL's unique feature is its CA, the RPCA (Christodoulou et al., 2020), rooted in Byzantine fault tolerance principles. Byzantine Fault Tolerance is a property of a system that allows it to function correctly even when some of its components (i.e., nodes) fail or act maliciously. RPCA, aligning with these principles, involves nodes communicating with each other to agree on a candidate set of transactions for the next ledger. Each node independently assesses the validity

of the transactions before sharing its evaluation with the network, iterating this process until consensus is reached.

In addition, XRPL uses the XRP ledger close process, a mechanism that minimizes the time taken to validate transactions and achieve consensus. It entails several stages, including transaction validation, transaction fee calculation, and consensus ledger generation, often completing within seconds.

The XRPL protocol supports various applications beyond being the underlying technology for the XRP cryptocurrency. For instance, it facilitates cross-border payments by providing a faster, more cost-effective alternative to traditional systems like SWIFT (Qiu et al. 2019). It also supports micropayments, enabling low-cost transactions for new kinds of online content and services, and enables decentralized, peer-to-peer transactions, empowering individuals to transact directly without needing a trusted third party (XRP Ledger).

5.4.2 Experimental Evaluation

This section outlines the experimental evaluation conducted for the XRPL client utilizing the BBF within an Amazon AWS EC2 instance (c5.2xlarge), comprising 8vCPUs, 16 GiB of memory, and up to 10 Gbps of network bandwidth. The experiments are designed to evaluate the XRPL client's performance in terms of transaction throughput, consensus time, and resilience to Byzantine faults such as double-spend attacks and node failures or crashes. This involves the introduction of network latency variations, simulation of node disruptions, and testing under different network conditions. Scripts developed as part of the BBF facilitate the execution of these tests, as well as the collection and subsequent analysis of data. The results from these experiments are then visualized and analyzed to offer insights into the XRPL client's operational efficiency and to validate the BBF's capability to benchmark blockchain performance effectively. The goal is to not only evaluate the performance metrics of the XRPL client but also to test the BBF's applicability and adaptability across diverse blockchain environments.

5.4.2.1 XRPL Client - Byzantine Fault: Double Spend Attack

5.4.2.1.1 Simulating and Analyzing Double Spend Attacks on XRPL using BBF

To simulate a double-spend attack on the XRPL client, a network of ten validators is deployed and configured as a full mesh network, which means every validator is connected to every other. All validators are set to participate in the consensus process and included in the Unique Node List (UNL) (Christodoulou et al., 2020). This configuration is chosen to maximize the number of nodes participating in the consensus process, making the network more robust and representative of a real-world XRPL network.

The double-spend attack is simulated using a custom script implemented in Node.js with the ripple-lib, a Ripple client library. The script is designed to send transactions to the XRPL network. In constructing transactions for the XRPL, each transaction must include a sequence number which is derived from the sequence number of the last closed ledger, incremented by one. To simulate a double-spend attack, two transactions are crafted using the same sequence number and sent into the network. As the XRPL client is designed to reject transactions with duplicate sequence numbers, the second transaction is expectedly rejected by the consensus process. The transactions are submitted through a single node, emulating a scenario where an attacker might attempt to spend the same digital tokens twice from the same point of access.

To monitor the behavior of the XRPL client and validate the design decision to use the sequence number as a defense against double-spend attacks, the hash digest of failed transactions is recorded. By employing the monitoring tools offered by the proposed BBF, the network's response to simulated attacks can be closely observed. The correlation between the hash digest of the rejected transactions and the sequence number underscores the robustness of the XRPL's security mechanisms. This tracking process confirms that the system effectively identifies and prevents duplicate transactions, ensuring the integrity of the ledger.

5.4.2.1.2 Empirical Data and Research Findings: Double-Spend Attack Analysis on XRPL

Before executing the experiment, it is essential to verify that the XRPL network is operational, synchronized, and ready to process incoming transactions. To accomplish this, the

researcher employed a *server_info.js* script, which returned comprehensive details about the current state of the network. The information included among others the build version, number of complete ledgers, synchronization duration, load factor, server state, uptime, and details of the validated ledger. The complete response from the network is depicted in Script *5.2*.

```
{
  buildVersion: '1.9.1',
  completeLedgers: '2979-4837',
  initialSyncDurationUs: '25407489',
  ioLatencyMs: 1,
  jqTransOverflow: '0',
  lastClose: { convergeTimeS: 2, proposers: 4 },
  load: {
    jobTypes: [ [Object], [Object], [Object], [Object],
[Object], [Object] ],
    threads: 6
  },
  loadFactor: 1,
  nodeSize: 'small',
  peerDisconnects: '4',
  peerDisconnectsResources: '0',
  peers: 8,
  pubkeyNode:
'n9KnmQPrUGFhCwMpVivugTgurmKTZrMJ7GSZ6KDJtQq9S144Q45G',
  pubkeyValidator:
'nHBVSL46zf5NKPitkQwnqugSjCPEukyrbbALMjYek1fSQkoFfRxV',
  serverState: 'proposing',
  serverStateDurationUs: '5587032154',
  stateAccounting: {
    connected: { durationUs: '24002763', transitions: '1' },
    disconnected: { durationUs: '1404725', transitions: '1'
},
    full: { durationUs: '5587032154', transitions: '1' },
    syncing: { durationUs: '0', transitions: '0' },
    tracking: { durationUs: '0', transitions: '1' }
  },
  time: '2023-May-26 13:24:02.203482 UTC',
  uptime: 5612,
  validatedLedger: {
    age: 3,
    hash:
'A3DF63C0286C1F7B60A4CE57B18A04D8B11B8A7E327832DE8A34F60BAB64
06A2',
    baseFeeXRP: '0.00001',
    reserveBaseXRP: '20',
    reserveIncrementXRP: '5',
    ledgerVersion: 4837
  },
```

Script 5.2: XRPL - Server Info Response

Through the course of the experiment, the resilience of the XRPL client against double-spend attacks is thoroughly tested. The custom node script is used to send two transactions with the same sequence number to the network through a single node. The first transaction is accepted, while the second is immediately identified as a duplicate and rejected. Table *5.1* illustrates the sequence of transactions and their respective outcomes:

Table 5.1: Double-Spend Attack - Transaction Execution Sequence

Transaction	Sequence Number	Transaction Hash	Result Code
1	6	36D92D9C5A5AF8390353D9D94BD8964040D323E480E5FFC09DDC1D3ED7F1442A	tesSUCCESS
2	6	705DCED51F23E8444A067EBAB615B5196463D25B719F73C26495704F7BF5C272	tefPAST_SEQ

To illustrate the transaction process in practice, the researcher examines a concrete example of a signed transaction before submitted to the network, and the result after its successful submission. The signed transaction JSON before submission is depicted in **Script 5.3**:

```
{
  "TransactionType":"Payment",
  "Account":"rHb9CJAWyB4rj91VRWn96DkukG4bwdtyTh",
  "Fee":"10",
  "Destination":"rhhPSx419uscUtcGEKxcnLyrbMxCdJdoJs",
  "DestinationTag":9318,
  "Amount":"1000000000",
  "LastLedgerSequence":267,
  "Sequence":3
}
```

Script 5.3: Signed XRPL Transaction - Before Submission

After successful submission, the transaction response is depicted in **Script 5.4**:


```
{
  "resultCode": "tesSUCCESS",
  "resultMessage": "The transaction was applied. Only
final in a validated ledger.",
  "engine_result": "tesSUCCESS",
  "engine_result_code": 0,
  "engine_result_message": "The transaction was applied.
Only final in a validated ledger.",
  "tx_json": {
    "Account": "rHb9CJAWyB4rj91VRWn96DkukG4bwdtyTh",
    "Amount": "1000000000",
    "Destination": "rhhPSx419uscUtcGEKxcnLyrbMxCdJdoJs",
    "DestinationTag": 9318,
    "Fee": "10",
    "LastLedgerSequence": 267,
    "Sequence": 3,
    "SigningPubKey":
"0330E7FC9D56BB25D6893BA3F317AE5BCF33B3291BD63DB32654A3132
22F7FD020",
    "TransactionType": "Payment",
    "TxnSignature":
"304402203C9A0F33079D822D67016C592A7CC24AD32850CBF39DDC026
ADBAB3167897841022012 21D742D4DD3A2233510685ED1495BAA403D51
DA873F4B8145B495A3D595325",
    "hash":
"288F25FA041D5C4842B98EEBD5AEB1D26348BCB7E9146A184340EE46C
9A7FA7D"
  },
  "validation_time": "107.85130000114441"
}
```


Script 5.4: Successful Transaction - Network Response

The latter, demonstrates the lifecycle of a transaction in the XRPL network. After the transaction is prepared and signed (Script 5.3), it's submitted to the network. The response (Script 5.4) contains details about the submission result, including whether the transaction is executed successfully (resultCode: tesSUCCESS), its validation time, and the transaction hash, which is a unique identifier of the transaction on the network.

From a data analysis perspective, this experiment shows key insights on how XRPL client behaves against double-spend attacks. The findings confirmed that the consensus process and sequence number mechanisms are effective in detecting and rejecting the attempt to double spend by the second fraudulent transaction. Furthermore, the transaction hashes and sequence numbers also confirmed the XRPL client's efficacy in identifying and preventing duplicate transactions. Performance measurements during the attack scenario showed no significant impact on the XRPL network's latency, throughput, or consensus time, indicating a high degree of resilience against double-spend attacks. This is crucial as the ability to maintain steady performance, even when under attack, is a key characteristic of a robust blockchain protocol.

Moreover, the findings demonstrated the usefulness of the BBF monitoring system in identifying and documenting the network's response to double-spend attacks using the XRPL client. The proposed BBF enables the user to capture real-time data, including transaction hashes and sequence numbers, and to analyze the effectiveness of the XRPL client's response mechanisms. This research highlights the role of the sequence number in preventing double-spend attacks. It is observed that the sequence number is an effective mechanism between legitimate and fraudulent transactions, preventing double-spend attacks.

5.4.2.2 XRPL Client - Byzantine Fault: Node Failure or Crash

5.4.2.2.1 Simulating and Analyzing the Node Failure or Crash

Understanding the behavior of a distributed ledger system like the XRP Ledger during disruptions, particularly node failures, is crucial to evaluating its resilience and performance. In this context, this part of the study explains how node failures are simulated and examined within an XRPL network using a series of dedicated scripts.

Firstly, a shell script is crafted to manage 10 XRPL validators, all running in Docker containers. This script simulates node crashes and recoveries by randomly stopping a validator and then restarting a previously stopped one. To ensure network stability, a particular validator, "*xrpl-validator-genesis*", is kept running throughout the experiment. The status of each validator, whether running or stopped, is logged into a Comma Separated Value (CSV) file for the subsequent analysis and discussion of Section 5.4.2.2.2. Concurrently, another script injects

a predetermined number of transactions to the network to simulate real-world network load during these disruptions.

An additional script is formulated to record the processing time for each transaction. This script logs the time taken for each transaction and stores these metrics, along with a timestamp, into a CSV file. The data includes the transaction number, the time it is sent, and the time it took to process. The complete process is illustrated in the sequence diagram of Figure *5.5*, highlighting the end-to-end workflow: how the scripts manage the XRPL validators and log their status, the methodology of sending transactions to the network, and the procedure of recording the transaction processing time. Figure *5.5* provides a visual representation of the sequence of events in the simulation of node failure and crash scenarios. Initially, a shell script is invoked to manage the XRPL validators, which includes the controlled start and stop of nodes to simulate crashes and recoveries, with the *'xrpl-validator-genesis*' remaining consistently active for network stability. The status of each validator is systematically logged. Simultaneously, transaction injection is performed by a separate script to replicate typical network traffic and load. This activity is closely followed by the transaction time logger script, which records each transaction's processing duration, appending this data alongside timestamps into a structured CSV file. Lastly, the recorded information is forwarded into a Python analysis script, designed to convert the raw data into insightful visualizations that demonstrates the network's behavior under the simulated conditions. In short, the scripts developed as part of the BBF provide a methodology for simulating node failures in an XRPL network and analyzing the results. In an attempt to understand the network's tolerance to faults, possible weak points, and overall capacity to handle disruptions, thus setting up a robust framework for more research and testing. Further discussion of the data analysis from this simulation is provided in Section 5.4.2.1.1.

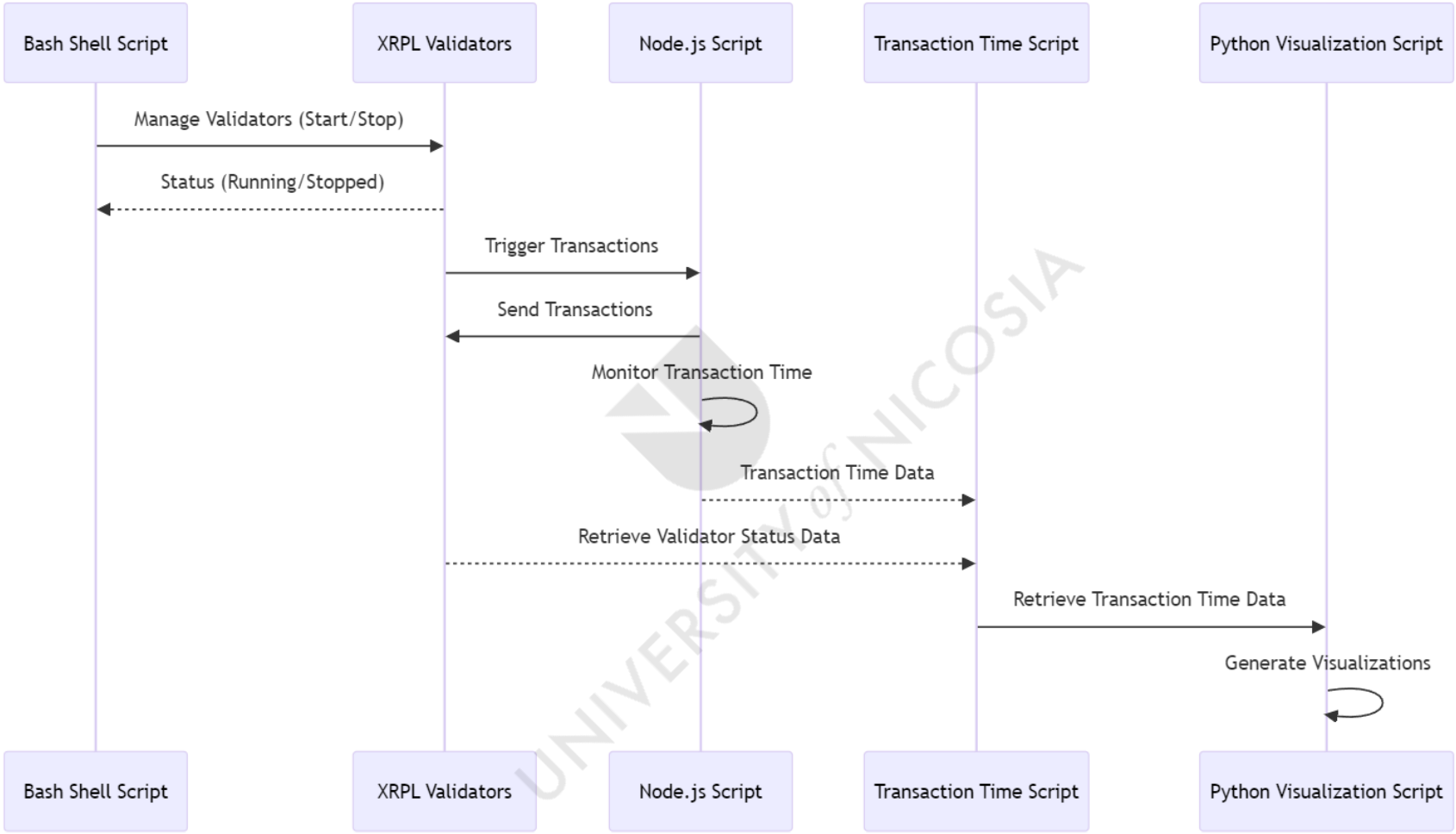


Figure 5.5: Sequence Diagram of the Simulation and Analysis of the Node Failure/Crash Scenario

5.4.2.2.2 Empirical Data and Research Findings: Node Failure or Crash

While evaluating the performance and resilience of the XRPL client during simulated node failures or crashes, both the simulation methodology and data analysis revealed several insights. The data, as observed and recorded, offers evidence of the network's behavior under node failure conditions, establishing a framework for understanding the robustness of the XRPL. The data, capturing both the status of validators (running or stopped) and transaction processing times, are accurately recorded in two CSV files— 'validator_status.csv' and 'transactions_time.csv'. The data from these files forms the basis of the empirical findings, enabling a detailed analysis of the XRPL's performance during the experiment of the simulated node crashes.

The file used to store the status of each validator provides data on the number of running and stopped validators over time, excluding the "xrpl-validator-genesis" validator, which is consistently operational to maintain network continuity. These data reflect on the network's ability to withstand random crashes and recoveries without experiencing any complete downtime. Although the number of operational validators fluctuated due to node crashes and recoveries, the blockchain under test never faced a complete breakdown, revealing a its level of fault tolerance. Next, the "transactions_time.csv" file documents transaction times, capturing the duration for each transaction along with its associated timestamp. These data offer insights into the network's performance during the execution of the node failure or crash scenario. As depicted in Figure *5.6*, despite node crashes and recoveries, transactions are processed without significant delays. Figure *5.6*, delineates the empirical data accrued during the node failure and crash simulations. The uppermost graph tracks the fluctuating count of active validators over the experimental timeframe, revealing the dynamic nature of the network's operational nodes. In contrast, the middle graph provides an inverse reflection, charting the oscillations in the number of stopped validators, thereby underscoring the effects of the simulated disruptions. The lowermost graph presents a scatter of aggregated transaction times, captured in 30-second intervals, offering insights into the transactional throughput and latency amidst the varying availability of validators.

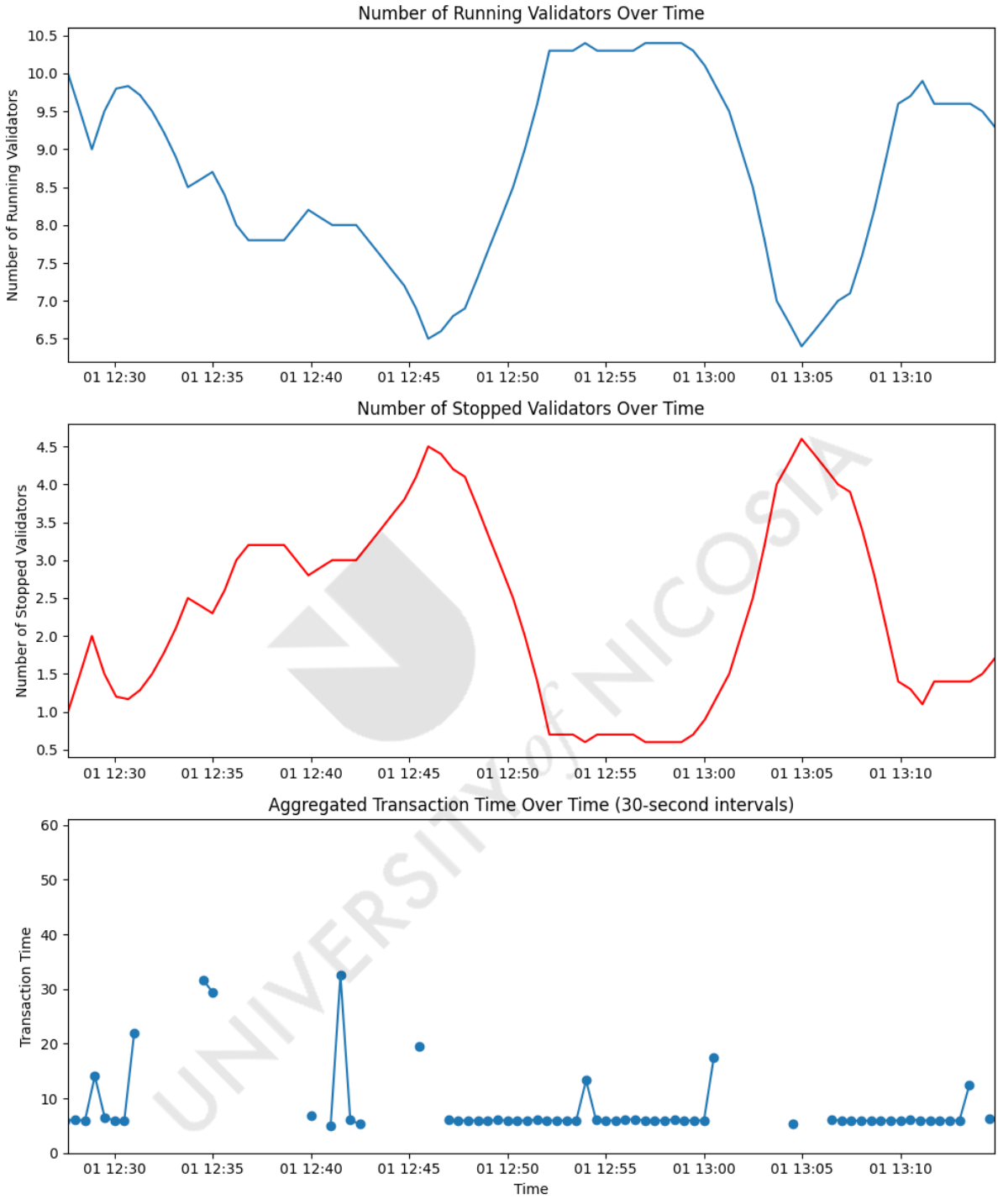


Figure 5.6: XRPL - Simulating and Analyzing the Node Failure or Crash

Throughout multiple repetitions of the simulations, a consistent behavior pattern of the XRPL system during node failures is observed by the researcher. The system showcased a reliable recovery process, where transaction processing times returned to the expected levels after several disruptions. This consistency across simulations indicates a dependable trend in the system's behavior. Recognizing this pattern, simulations are terminated once the system's recovery has reached a stable state, marked by the return to usual transaction processing times. By concentrating on this recovery phase, the study effectively examined the resilience of the XRPL during node failures, while also ensuring that the simulations extended long enough to witness the full effects and recovery from these crashes. The visualization script is used to generate graphical representations of the validator behavior and transaction submission times during the simulations. These visual representations made it easier for the researcher to identify patterns and potential performance issues. For example, despite noticeable fluctuations in the number of operational validators, a baseline operational level persisted throughout the simulation. Additionally, even if transaction times spiked during intense disruption phases, they consistently remained within reasonable bounds. This indicates that the network remains operational under node disruptions without impacting transaction processing speeds. A segment of the source code used to visualize these data is presented in Script 5.7.

```
1/2
import pandas as pd
import matplotlib.pyplot as plt

# Load the validator status data
validator_data =
pd.read_csv('C:\\Users\\touloups.m\\Desktop\\ByzantineFaults
\\XRPL\\node-crashing\\data\\validator_status.csv')

# Load the transaction time data
transaction_data =
pd.read_csv('C:\\Users\\touloups.m\\Desktop\\ByzantineFaults
\\XRPL\\node-crashing\\data\\transactions_time.csv')

# Convert the 'Timestamp' column in validator data to
datetime format
validator_data['Timestamp'] =
pd.to_datetime(validator_data['Timestamp'])

# Convert the 'Timestamp' column in transaction data to
datetime format
transaction_data['Timestamp'] =
pd.to_datetime(transaction_data['Timestamp'])

# Set the window size for the rolling average
window_size = 10

# Calculate the rolling average for the number of running
validators
running_avg =
validator_data['RunningValidators'].rolling(window=window_si
ze, min_periods=1).mean()

# Calculate the rolling average for the number of stopped
validators
stopped_avg =
validator_data['StoppedValidators'].rolling(window=window_si
ze, min_periods=1).mean()

# Preprocess transaction time data
transaction_data['Real'] =
transaction_data['Real'].str.extract(r'(\d+\.\d+)').astype(f
loat)
```

```
2/2
transaction_data.set_index('Timestamp', inplace=True)
transaction_data_agg =
transaction_data['Real'].resample('30S').mean().reset_index()

# Get the x-axis range from the validator status data
x_min = validator_data['Timestamp'].min()
  x_max = validator_data['Timestamp'].max()

# Get the y-axis range for transaction time
y_min = 0
y_max = transaction_data['Real'].max() + 10  # Add some
margin for better visualization

# Create a figure with three subplots
fig, (ax1, ax2, ax3) = plt.subplots(3, 1, figsize=(10, 12))

# Plot the smoothed number of running validators
ax1.plot(validator_data['Timestamp'], running_avg)
ax1.set_title('Number of Running Validators Over Time')
ax1.set_ylabel('Number of Running Validators')
ax1.set_xlim(x_min, x_max)  # Set x-axis range

# Plot the smoothed number of stopped validators
ax2.plot(validator_data['Timestamp'], stopped_avg,
color='red')
ax2.set_title('Number of Stopped Validators Over Time')
ax2.set_ylabel('Number of Stopped Validators')
ax2.set_xlim(x_min, x_max)  # Set x-axis range

# Plot the aggregated transaction time with markers
ax3.plot(transaction_data_agg['Timestamp'],
transaction_data_agg['Real'], marker='o', linestyle='-')
ax3.set_title('Aggregated Transaction Time Over Time (30-
second intervals)')
ax3.set_xlabel('Time')
ax3.set_ylabel('Transaction Time')
ax3.set_xlim(x_min, x_max)  # Set x-axis range
ax3.set_ylim(y_min, y_max)  # Set y-axis range

# Adjust the spacing between subplots
plt.tight_layout()
```

Script 5.7: Visualizing XRPL Node Failure or Crash - Python Code

5.4.3 Analysis and Discussion of Use Case One

The experimental investigation undertaken in this research focuses on understanding the performance of the XRPL client as well as assessing the applicability of the BBF as a tool to validate different features of the blockchain under test in an isolated environment. Two Byzantine faults are simulated, double-spend attack and node failure or crash, while the XRPL client is used to deploy a full mesh blockchain protocol.

In the context of the double-spend attack, the XRPL client demonstrated significant resistance. Transactions that attempted to double-spend are consistently detected and prevented from being included in the validated ledger. This robustness against double-spend attacks can be attributed to the CA employed by the XRPL, which emphasizes on strict transaction ordering and validation (Christodoulou et al., 2020). This validation, coupled with the uniqueness of the transaction sequence numbers for each account, ensures that double-spend transactions are effectively detected and eventually rejected.

Regarding the node failure or crash scenario, the XRPL client exhibited resilience and fault tolerance. Despite the randomized crashing and recovery of nodes, the network maintained operational continuity and processed transactions without encountering major delays or failures. This resilience against node crashes can be interpreted as an affirmation of the distributed, decentralized nature of the XRPL network, where the system can withstand individual node failures without compromising overall network performance. However, it is essential to note that the network performance is observed to experience fluctuations under node failure scenarios. Increases in transaction times during peak disruption periods suggested that such disruptions could impact network throughput. Nonetheless, these variations remained within acceptable limits, demonstrating that the XRPL can manage node disruptions without significantly compromising transaction processing times.

The implications of these findings for the XRPL network and its CA are multifold. First, the robustness against double-spend attacks underscores the effectiveness of the XRPL's CA in maintaining network security. Second, the observed resilience against node failures reflects the inherent fault tolerance of the XRPL network. Together, these findings suggest that the XRPL,

under its current design and CA, possesses considerable resistance to common Byzantine faults, further solidifying its potential for robust, decentralized financial transactions.

Finally, reflecting on the effectiveness of the BBF in benchmarking the XRPL client's performance, it is observed that the BBF served as a useful tool in simulating adversarial conditions and assessing the XRPL client's response. It enabled the systematic execution of the Byzantine faults, facilitated the collection of empirical data, and allowed the evaluation of the XRPL client's behavior under such conditions.

5.4.4 Use Case #1 - Research Hypotheses Testing

The empirical evaluation of the XRPL client enabled an in-depth exploration in understanding the behavior of the network and the application of the BBF as a useful tool towards the validation of the design decisions of the blockchain under test. In the rest of this section, the testing of the research hypotheses defined in Section 3.5 is presented:

H1:	H1 centered on conducting a comprehensive evaluation of the effectiveness of current Consensus Algorithms (CAs), and the findings affirmed the BBF's capability to thoroughly analyze the intricacies of existing CAs, thereby substantiating H1's validity.
H2:	The design and implementation of the BBF revealed significant improvements in the assessment and performance of the XRPL client. The latter supports H2, which states that comprehensive tools, frameworks, and documentation can elevate the performance analysis of blockchain protocols.
H3:	The accessibility and usability of the BBF are evidenced by its seamless configuration and bootstrapping capabilities. The latter supports H3 stating that enhancing the usability of blockchain ecosystems can foster greater adoption and understanding of the technology. This usability is facilitated through the BBF’s command line tool, serving as the access portal for users.

H4: Through the BBF's simulation of Byzantine faults on a real blockchain protocol, the study found that such frameworks provide more accurate and reliable performance assessments compared to theoretical assumptions, confirming H4.

The use of the BBF in this study underscored its utility as an effective tool for benchmarking different blockchain protocols. Its capacity to simulate Byzantine faults and measure the subsequent effects on the XRPL client provides a practical and reliable way to evaluate the client's performance. The application of the BBF, in this case, demonstrates its potential for replicable, empirical evaluations of blockchain clients, validating the worthiness of the framework. The implications of these findings extend beyond the XRPL client, opening avenues for benchmarking and performance assessments across different blockchain protocols. The utilization of BBF, with its systematic approach to the simulation of Byzantine faults, set a precedent for assessing blockchain performance under diverse adverse conditions, making it a potentially integral tool for developers, researchers, and organizations involved in blockchain technology.

5.5 Use Case Two: The case of Ethereum Client

The second use case considers the Ethereum network, with a specific client Hyperledger Besu (Praitheeshan, Pan and Doss, 2021). This specific Ethereum client is evaluated under the proposed BBF, similar to the approach used in use case one. In particular, the empirical evaluation aims to assess the performance of the Ethereum client under Byzantine fault conditions, providing insights into the robustness of the network's CA and infrastructure. It further tests the applicability and adaptability of the BBF across a different blockchain protocol, supporting its potential as a universally applicable tool for blockchain benchmarking and performance assessment. The Ethereum network introduces different features and complexities, including a Turing-complete language for smart contracts and a hybrid Proof-of-Stake/Proof-of-Work CA. These aspects make the Ethereum network a unique subject for this empirical evaluation, offering a contrasting perspective to the Ripple Protocol CA used in the XRPL client.

Subsequent sections detail the methodology employed for the empirical evaluation, the Byzantine faults simulated, the empirical data gathered, and the subsequent analysis and discussions of the findings. These outcomes shed light on the performance of the Ethereum client under adverse conditions and reflect the effectiveness and versatility of the BBF in different blockchain protocols.

5.5.1 Ethereum Background

Ethereum was founded in 2014 by Vitalik Buterin, is a decentralized, open source blockchain protocol renowned for its smart contract functionality, which has sparked the development of thousands of Decentralized Applications (DApps) (Wan *et al.*, 2019). It has a native cryptocurrency, Ether (ETH), used primarily for two purposes: as a digital currency exchange and as 'gas' to run computations and transactions on the network. The Ethereum blockchain operates on PoS CA – as of Ethereum 2.0 while when introduced started with the PoW CA. Unlike PoW, where miners solve complex mathematical puzzles to validate transactions and create new blocks, PoS allows users to 'stake' their cryptocurrency to become validators, creating blocks based on the amount of cryptocurrency they hold and are willing to 'stake' as collateral (Thin et al., 2018).

Ethereum's most distinguishing feature is the Ethereum Virtual Machine (EVM), a Turing-complete software that enables anyone to run any program, regardless of the programming language, if enough time and resources are available. The EVM makes the process of creating blockchain applications much simpler and more efficient. One of the significant uses of Ethereum has been the implementation of smart contracts, self-executing contracts with the terms of the agreement directly written into code (Tikhomirov *et al.*, 2018). They automatically execute transactions when pre-set conditions are met, eliminating the need for a trusted third party. This has opened a plethora of possibilities, from financial derivatives to property law, crowdfunding agreements, and even voting systems (Governatori *et al.*, 2018).

This underlying architecture and functionality make Ethereum a unique platform for this use case, offering different parameters and behaviors to consider during the evaluation and analysis under the BBF.

5.5.2 Experimental Evaluation

This section details the evaluation process for the Ethereum client using the BBF, applying a similar methodology as in the XRPL client's use case study. For this evaluation, the BBF is deployed on an Amazon AWS EC2 instance comparable to that used for the XRPL client, aiming to assess key performance metrics like transaction speed and the efficiency of the validation process. The resilience of the Ethereum client to various Byzantine fault scenarios, such as network latency challenges, node crashes, and the introduction of adversarial elements within the network, is a central focus of this evaluation. The experimental setup involves a series of tests designed to measure the Ethereum client's response to these challenging conditions, employing scripts from the BBF to facilitate performance testing, Byzantine fault simulation, and data analysis. The data collected from these tests are visualized and interpreted to gain insights into the Ethereum client's performance under varied operational conditions. This evaluation aims not only to assess the Ethereum client's robustness and efficiency but also to demonstrate the BBF's versatility and effectiveness in benchmarking different blockchain protocols, highlighting its ability to provide a comprehensive and comparative evaluation across diverse blockchain environments.

5.5.2.1 Ethereum Client - Byzantine Fault: Double Spend Attack

5.5.2.1.1 Simulating and Analyzing Double-Spend Attacks on ETH using the BBF

This section outlines the step-by-step process employed in an experiment aimed at simulating a double-spend attack on the Ethereum network using the BBF. The experiment is executed within a controlled environment using the private Hyperledger Besu blockchain client. The step-by-step process described in the below sections is also depicted in the sequence diagram of Figure *5.8*. Initially, the user sets up four Hyperledger Besu nodes in a Docker environment, establishing the foundational network. The system then checks the initial connectivity among validators, ensuring all nodes are in communication with each other. Following the latter, the user executes a script designed to split the network in half, creating a disruption in the normal flow of information. In this partitioned state, identical transactions are submitted to Validators 1 and 3, emulating the core condition for a potential double-spend scenario. Subsequently, a

script is executed to reconnect the network, re-establishing the connections between validators. At this point of time, each validator engages in a consensus process using the Besu CA to resolve any conflicts, thus safeguarding the integrity of the network.

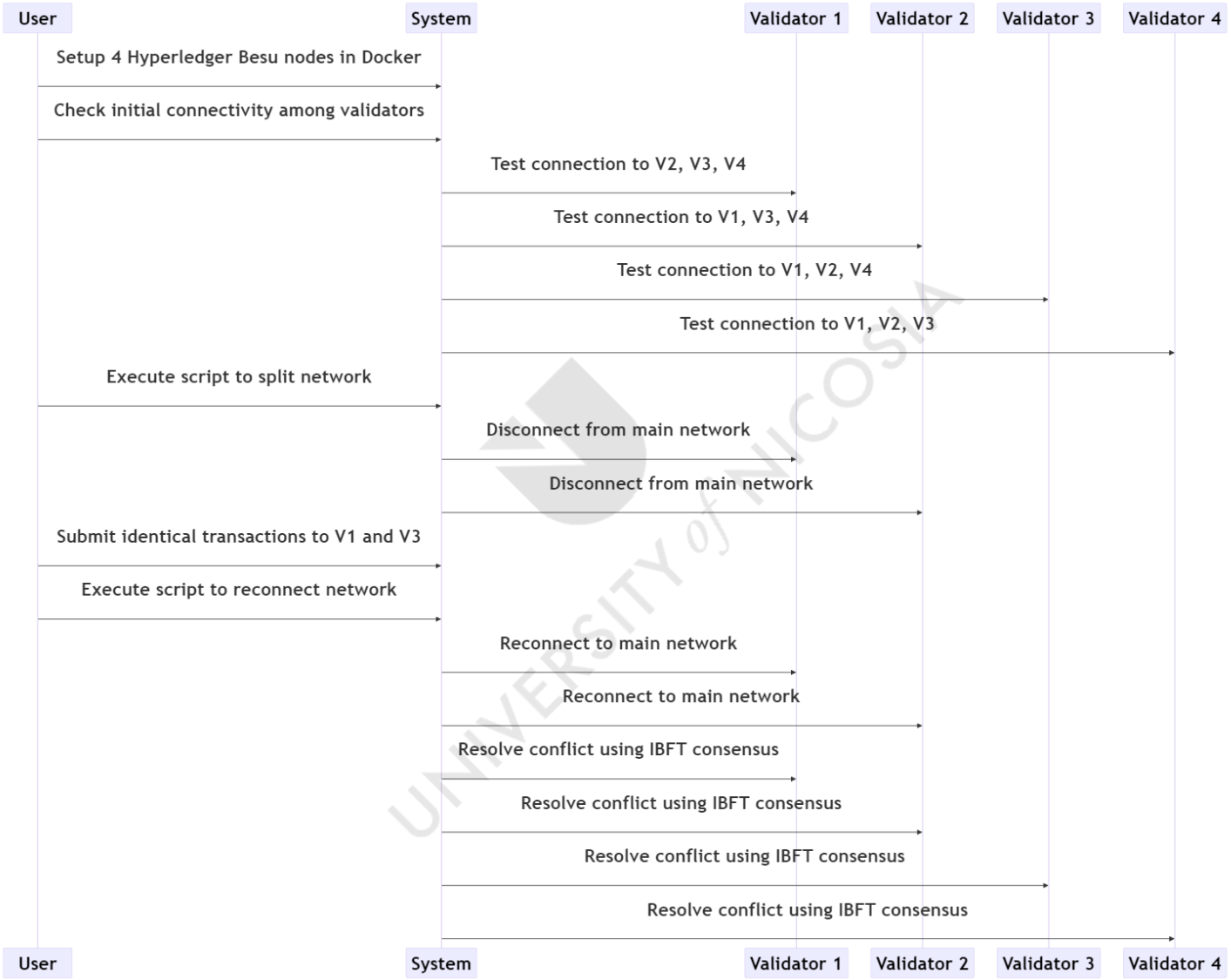


Figure 5.8: Simulating Double-Spend attack on the Ethereum private network.

The blockchain protocol is instantiated using the Docker (Docker Inc., 2022) engine, composed of four Ethereum nodes functioning as validators within the same network in their own docker container. Each node is allocated a unique IP address and port for internal communication. Network connectivity is verified via a custom script designed to check the connection status among all nodes, ensuring the effectiveness of communication channels within the network. The script used for testing the interconnectivity of the network's validators is depicted in Script *5.9*.

```
#!/bin/bash

# Array of validator container names
validators=(
"hyperledger-besu-priv-net-validator1-1"
"hyperledger-besu-priv-net-validator2-1"
"hyperledger-besu-priv-net-validator3-1"
"hyperledger-besu-priv-net-validator4-1"
)

# Loop over all validators
for i in "${!validators[@]}"; do
  # Loop over all other validators
  for j in "${!validators[@]}"; do
    if [ $i -ne $j ]; then
      # Check if validator i can connect to validator j
      if docker exec -it ${validators[$i]} bash -c "echo >
dev/tcp/${validators[$j]}/8545"; then
        echo "Connection from ${validators[$i]} to
${validators[$j]} is open."
      else
        echo "Connection from ${validators[$i]} to
${validators[$j]} is closed."
      fi
    fi
```

Script 5.9: Ethereum Network - Test Connectivity of Validators

To stimulate a double-spend scenario, the network is partitioned into two halves, thereby creating a split-brain situation. Segment 1 contained the first two validators, while Segment 2 contained the remaining ones. This partitioning is achieved using another script that uses the

Docker networking capabilities. The script used for splitting and or reconnect the network is depicted in Script *5.10*.

```
#!/bin/bash

# Docker container names
VALIDATOR1="hyperledger-besu-priv-net-validator1-1"
VALIDATOR2="hyperledger-besu-priv-net-validator2-1"

split_network() {
    # Disconnect validators 1 and 2 from the existing
network
    docker network disconnect quorum-dev-quickstart
$VALIDATOR1
    docker network disconnect quorum-dev-quickstart
$VALIDATOR2
}

reconnect_network() {
    # Reconnect validators 1 and 2 back to the existing
network
    docker network connect --ip 172.16.239.11 quorum-
dev-quickstart $VALIDATOR1
    docker network connect --ip 172.16.239.12 quorum-
dev-quickstart $VALIDATOR2
}

if [[ $1 == "split" ]]; then
    split_network
elif [[ $1 == "reconnect" ]]; then
    reconnect_network
else
    echo "Usage: $0 {split|reconnect}"
  fi
```

Script 5.10: Ethereum Split/Rejoin Network Script

Post partitioning, identical transactions are simultaneously submitted to a validator in each segment. Due to the disconnect between the two network segments, both transactions are considered valid and added to their respective blockchains, essentially creating a double-spend scenario. The python code used for simulating the double-spend scenario is depicted in Script *5.11*.

1/2

```
from web3 import Web3, HTTPProvider

# Initialize the web3 instances for each half of the
network
web3_1 = Web3(HTTPProvider('http://xx.xx.xx.xx:21001'))  #
adjust the URLs as needed
web3_2 = Web3(HTTPProvider('http://xx.xx.xx.xx:21003'))

# The account that will be doing the double spend
account = "0x21b0c2bEfdd3599fC69431b14fF45D0df9F03c23"

# The private key of the account doing the double spend
private_key =
"0x6fe8890c925cc7061e4682162077291891610bb6845441a2f0d35ce
e8f5e0edc"

# The addresses that the funds will be sent to
address_1 = "0x603Fb8848aFF62f3955DEc4940C9976776Beb171"
address_2 = "0xE493C595574c6B55cebbcbd6EfdC72842e8234CC"

# The amount to send
amount = Web3.toWei(1, 'ether')

# Get the current nonce
nonce = web3_1.eth.getTransactionCount(account)
```

```
2/2
# Create the transactions
transaction_1 = {
'to': address_1,
'value': amount,
'gas': 2000000,
'gasPrice': Web3.toWei('50', 'gwei'),
'nonce': nonce,
'chainId': 1338  # replace with your chain ID
}

transaction_2 = {
'to': address_2,
'value': amount,
'gas': 200000,
'gasPrice': Web3.toWei('100', 'gwei'),
'nonce': nonce,
'chainId': 1338  # replace with your chain ID
}
# Sign the transactions
signed_transaction_1 =
web3_1.eth.account.signTransaction(transaction_1,
private_key)
signed_transaction_2 =
web3_2.eth.account.signTransaction(transaction_2,
private_key)

# Broadcast the transactions and handle any errors
try:
    tx_hash_1 =
web3_1.eth.sendRawTransaction(signed_transaction_1.rawTran
saction)
    print(f"Transaction 1 hash: {tx_hash_1.hex()}")
except Exception as e:
    print(f"Error sending transaction 1: {e}")

try:
    tx_hash_2 =
web3_2.eth.sendRawTransaction(signed_transaction_2.rawTran
saction)
    print(f"Transaction 2 hash: {tx_hash_2.hex()}")
```

Script 5.11: Simulation of double-spend attack - Python Code

Following the transaction submission, the network is restored by reconnecting the split nodes, thus recreating a conflicting blockchain scenario. Ethereum's PoA CA is leveraged to resolve this conflict. On re-establishment of network connectivity, the conflicting transactions

are identified, and one version is discarded based on the consensus protocol, thereby preventing the double-spend situation, and maintaining the network's integrity. Despite the successful execution, the experiment encountered several challenges. The network partitioning, crucial for creating the double-spend scenario, posed initial hurdles as Docker's high-level network abstraction rendered IP table modifications ineffective. To address this, a resolution is implemented where a script is introduced to programmatically retrieve the current IP addresses post-reconnection. This step is essential to overcome the automatic assignment of new IP addresses by Docker, which led to inconsistencies. The script ensured that each validator could be accurately identified and communicated with using its updated IP address after the network is rejoined.

To maintain accessibility of the partitioned validators via their standard communication channels, specific ports are exposed using the Docker run command, ensuring that communication isn't hindered during the experiment. In conclusion, the experiment effectively simulated a double-spend attack in a controlled, private Ethereum network and demonstrated Ethereum's resilience against such attacks. Furthermore, the successful execution of this experiment underlined the utility and effectiveness of the BBF in facilitating similar simulations and analyses in a structured and methodical manner.

5.5.2.1.2 Empirical Data and Research Findings: Double-Spend Attack Analysis on Ethereum

This research set out to empirically test the resilience of an Ethereum client against double-spending attacks. The investigation leveraged a private Ethereum network, that uses the Hyperledger Besu client and hosted in a private Docker environment. Four validator nodes are configured, each running in its Docker container. The experimental setup followed the PoA consensus model where the network can tolerate at most *(N-1)/3* faulty nodes. This research exploited the partition tolerance property of the network, splitting it into two segments: one containing two validators and the other containing the remaining two.

To perform the double-spending attack, two identical transactions are crafted, each aimed at spending the same Ether funds from a particular address. In the partitioned state, these transactions are sent simultaneously to validators in separate network segments. Since the validators had no means of communicating due to the network split, they could not reach a consensus on the transactions' legitimacy.

Observations during the experiment included the successful submission of duplicate transactions and the subsequent states of these transactions upon network reconnection. Notably, despite the network split, only one of the transactions is executed successfully when network connectivity is reestablished. This result highlights Ethereum's resilience to double-spending attacks, an attribute that can be largely attributed to its implementation of the PoA CA. In the absence of a consensus, which occurs during network partition, the protocol defaults to a state of safety by rejecting conflicting transactions until consensus can be restored.

The findings reported herein align with the theoretical expectations on how the client behaves against double-spending attacks. This resilience significantly enhances Ethereum's network security, and the credibility of transactions executed on its blockchain. However, it is worth noting some limitations of the experiment. The testing environment is a simplified representation of Ethereum's real-world ecosystem. The setup with just four validator nodes may not fully emulate the complexity of a public Ethereum network where thousands of nodes participate. In addition, using the BBF in executing the simulation scenario added another layer of robustness to the research process. The framework allowed for structured and repeatable execution of the double-spending scenario, minimizing potential for human error and ensuring consistency of the experimental conditions. With the BBF, the researcher could accurately and systematically adjust network parameters, submit transactions, and track their processing status, thus providing a detailed examination of Ethereum's response to the double-spending attack.

The empirical findings from this research not only align with theoretical expectations but also serve to validate the BBF's utility in simulating complex blockchain network scenarios, suggesting its potential applicability in real-world contexts. The use of the BBF in this study illustrates the critical role of systematic tools in blockchain research, emphasizing the insightful outcomes and reliable empirical data that can be derived from such methodical approaches.

5.5.2.2 Ethereum Client - Byzantine Fault: Node Failure or Crash

5.5.2.2.1 Simulating and Analyzing the Node Failure or Crash

To evaluate the resilience of the Ethereum network and examine its behavior under unexpected conditions, the researcher conducted simulations to model scenarios where validator nodes experienced unpredictable crashes or stops. This process is vital in determining the network's robustness in the face of node failures and evaluating the impact these crashes had on transaction performance.

The simulation process comprises of a Python script - Script *5.12* - that simultaneously initiated transactions to the Ethereum network and randomly halted nodes to simulate failures. The script is designed to capture the state of the Ethereum network, sending a series of transactions and observing the behavior during node crashes. Transaction details included metrics such as transaction number, timestamp of the transaction initiation, time taken for the transaction to complete, and the transaction status. These details are monitored and logged into a CSV file named *'transactions_time_final.csv'* with the following structure:

- **Transaction**: The respective transaction numbers.
- **Timestamp**: The time at which the transaction transpired.
- **Time**: The time taken to complete the transaction.
- **Status**: The transaction's status, signifying whether it is successful or had failed.

At the same time, the state of the nodes (running or stopped), using a shell script (Script 5.13), is recorded at each logged timestamp into a dataset named *'crash_nodes.csv'*, structured as follows:

- **Timestamp**: This represents the specific time when the observation is recorded.
- **Running Validators**: This indicates the count of validators that are active at each logged timestamp.
- **Stopped Validators**: This signifies the count of validators that had halted at each recorded timestamp.

1/2

```
import requests
import csv
import time
from web3 import Web3, HTTPProvider
from web3.exceptions import TimeExhausted
import sys

# Connect to Ethereum node
w3 = Web3(HTTPProvider("http://xx.xx.xx.xx:8545"))

# Set private key
private_key =
"0x6fe8890c925cc7061e4682162077291891610bb6845441a2f0d35c
ee8f5e0edc"

# Get the account's public address
account_address =
w3.eth.account.from_key(private_key).address

# Set the recipient Ethereum address
to_address = "0x603Fb8848aFF62f3955DEc4940C9976776Beb171"

# Get the number of transactions to send from the user
num_transactions = int(input("Enter the number of
transactions: "))

# Open the CSV file and create a CSV writer
with open("transactions_time.csv", "w", newline="") as
file:
    writer = csv.writer(file)
    writer.writerow(["Transaction", "Timestamp", "Time",
"Status"])
```

2/2

```
    for i in range(1, num_transactions + 1):
        nonce =
w3.eth.get_transaction_count(account_address)
        txn = {
            "to": to_address,
            "value": w3.toWei(0.01, 'ether'),  # sending
0.01 Ether
            "gas": 2000000,
            "gasPrice": Web3.toWei('50', 'gwei'),
            "nonce": nonce,
            "chainId": w3.eth.chain_id
        }

signed_txn = w3.eth.account.sign_transaction(txn,
private_key)

        # Attempt to send the transaction and handle
potential Timeout error
        try:
            start_time = time.time()
            txn_hash =
w3.eth.send_raw_transaction(signed_txn.rawTransaction)
            w3.eth.wait_for_transaction_receipt(txn_hash)
            elapsed_time = time.time() - start_time
            status = "Successful"
        except (requests.exceptions.Timeout,
TimeExhausted) as e:
            print(f"Transaction {i} error: {str(e)} after
{time.time() - start_time} seconds.")
            elapsed_time = "Timeout"
            status = "Failed"
            continue

        # Write the transaction number, timestamp,
elapsed time, and status to the CSV file
        writer.writerow([i, time.strftime("%Y-%m-%d
%H:%M:%S", time.gmtime()), elapsed_time, status])

        print(f"Transaction {i} sent in {elapsed_time}
seconds.")
        sys.stdout.flush()
```

Script 5.12: Python Script - Execute TXs in Ethereum Network

```
#!/bin/bash

# Initialize csv file
echo "Timestamp,RunningValidators,StoppedValidators" >
validators.csv
# List of validators
validators=("hyperledger-besu-priv-net-validator1-1"
"hyperledger-besu-priv-net-validator2-1" "hyperledger-besu-priv-
net-validator3-1" "hyperledger-besu-priv-net-validator4-1")
stopped=()
while true; do
    if [ ${#validators[@]} -gt 3 ]; then
        validator=${validators[$RANDOM % ${#validators[@]}]}
        echo "Stopping $validator"
        docker stop $validator
        stopped+=($validator)
        validators=(${validators[@]//$validator})
    fi
    if (( RANDOM % 2 )) && [ ${#stopped[@]} -gt 0 ]; then
        # Select a random number of validators to start
        num_to_start=$(shuf -i 1-${#stopped[@]} -n 1)
        echo "Starting $num_to_start validators"
        for i in $(seq $num_to_start); do
            # Select a random stopped validator to start
            restartValidator=${stopped[$RANDOM %
${#stopped[@]}]}

            # Start the validator
            echo "Starting $restartValidator"
            docker start $restartValidator

            # Check if the validator was successfully started
            if [ $? -eq 0 ]; then
                # Add it back to the validators array
                validators+=($restartValidator)

                # Remove it from the stopped validators array
                stopped=(${stopped[@]//$restartValidator})
            fi
        done
    fi
    timestamp=$(date +"%Y-%m-%d %H:%M:%S")
```

Script 5.13: Simulate Node Crash Scenario on Ethereum Network

This procedure, as depicted in the sequence diagram of Figure *5.14*, illustrates the simultaneous transactions and node crashes, enabled the researcher to closely observe and record the network's performance under node failure conditions. The figure outlines the process

of simulating transactions on the Ethereum network while intentionally causing node crashes. This controlled disruption enables the researcher to monitor the network's performance during these node failure conditions. Each transaction initiation and node crash are sequentially logged, providing a detailed account of the network's behavior under stress. The compiled data from this exercise is subsequently analyzed and visualized, offering a comprehensive evaluation of the Ethereum network's robustness.

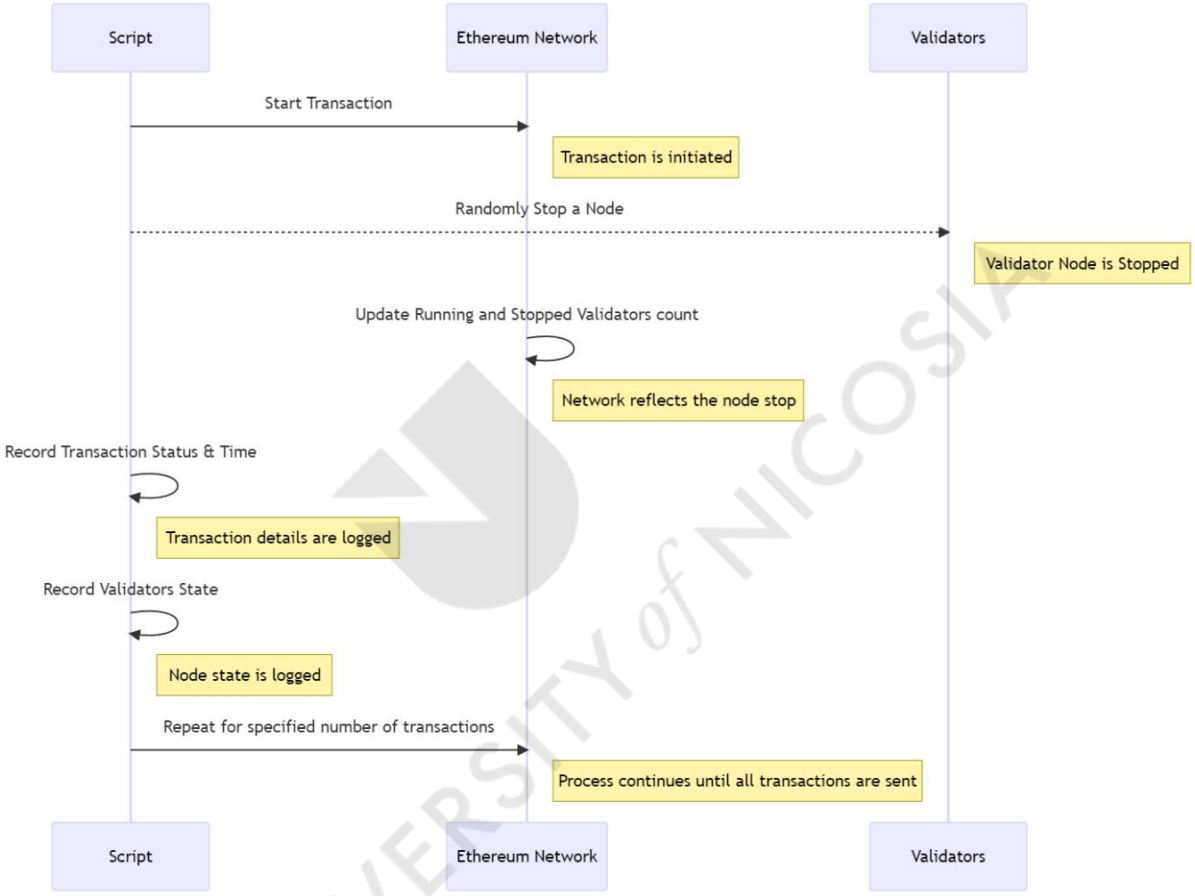


Figure 5.14: Simulating Node Crash Scenario on the Ethereum Network

5.5.2.2.2 Empirical Data and Research Findings: Node Failure or Crash

The simulation and concurrent monitoring of the Ethereum network during the node failure scenario yielded crucial data about the network's resilience and transaction performance under these conditions. The *'crash_nodes.csv'* dataset captured the count of running and stopped validators at each timestamp. Over the course of the simulation, it showed a dynamic fluctuation in these counts due to the randomly induced node stops. The *'transactions_time_final.csv*' dataset held records of each transaction, detailing the transaction number, the timestamp at which it occurred, the time taken for the transaction, and the final status of the transaction.

In the course of multiple simulations, a consistent trend emerged regarding the network's behavior under node failure scenarios. After each induced node failure, the network exhibited a predictable recovery pattern, with transaction processing times eventually stabilizing after a period of increased failures and delays. This recurring pattern led the researcher to define the endpoint for each simulation once the network's performance reached a steady state post-recovery. This 'endpoint' or cutoff point is chosen based on the observation that, after a certain point, the network consistently returned to its normal operational parameters, such as standard transaction processing times and success rates. By identifying this point of return to baseline functioning, the simulations can be halted at a moment where further repetition does not yield additional insights. This decision allows the researcher to focus on the immediate impacts of node failure and the subsequent recovery, thereby providing a comprehensive perspective on Ethereum's resilience and adaptability under such adverse conditions.

On observing the trend in the *'crash_nodes.csv'* data, it is clear that the Ethereum network showcased impressive resilience in the face of node failures. Despite the abrupt halting of validators, the network is able to maintain its functionality, underlining the inherent redundancy and robustness of decentralized blockchain protocols. The analysis of transaction data from *'transactions_time_final.csv'* yielded important insights into transaction performance under these conditions. As node failures increased, there is a notable effect on transaction times and success rates. It is observed that the rate of transaction failure and timeout events slightly increased during periods of high node failure, hinting at the network's strain under these conditions. However, the network still managed to process most of the transactions successfully, which testifies to Ethereum's robustness.

The graphical representation of the data in Figure *5.15* and Figure *5.16* provided a straightforward yet comprehensive depiction of the network's behavior during node failure. Figure *5.15*'s plots graphically track the number of validators, capturing the network's resilience through the ebb and flow of active and inactive nodes. Figure *5.16*'s scatter plot is particularly telling, as it correlates the node failures with increased transaction times and failures, offering a visual narrative of the network's stress response. The color-coding within this plot enhances the viewer's ability to quickly discern the status of transactions at a glance, efficiently communicating the resilience and recovery patterns of the Ethereum network during the simulation.

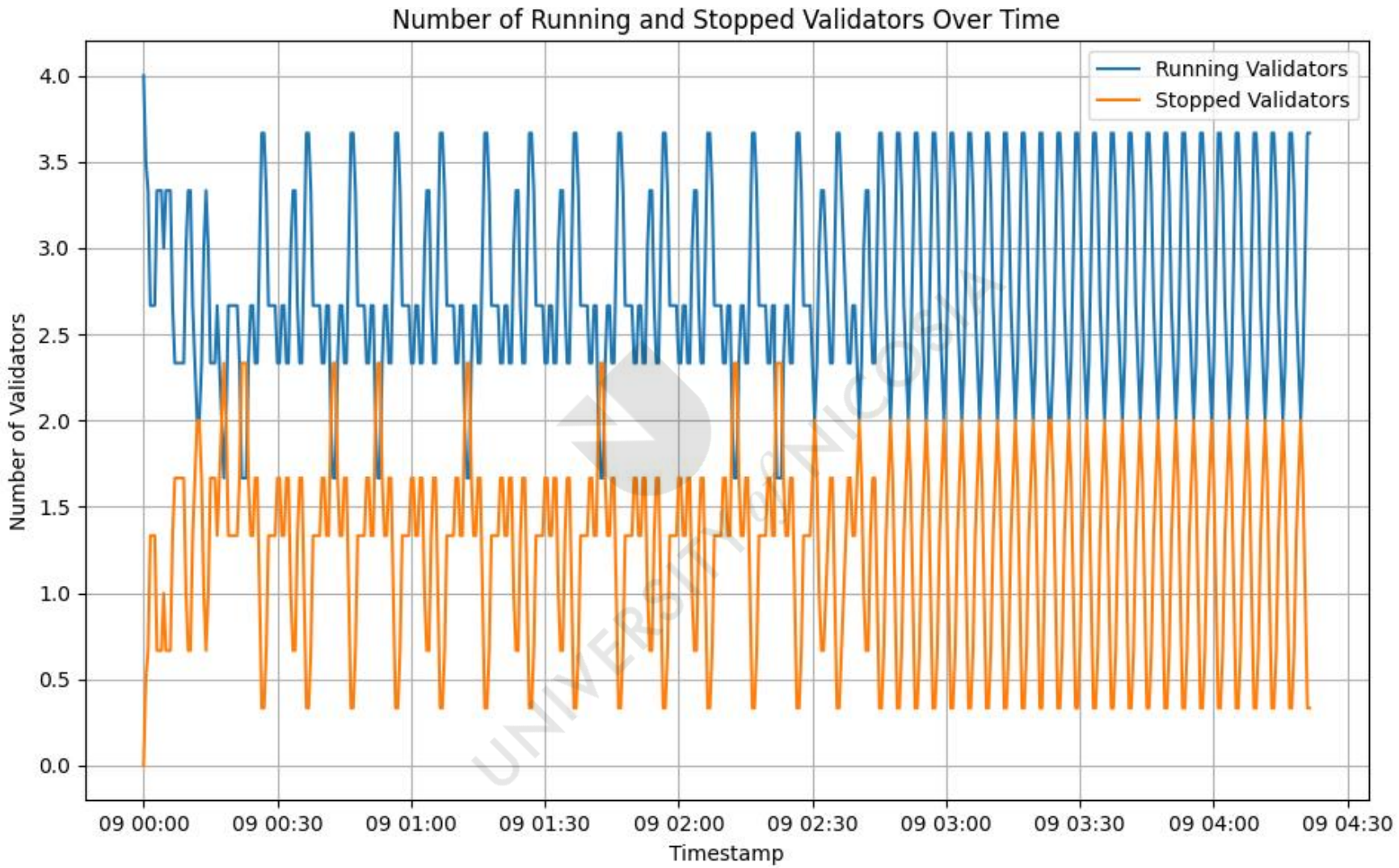


Figure 5.15: Ethereum Node Crash Scenario - Validator status over time

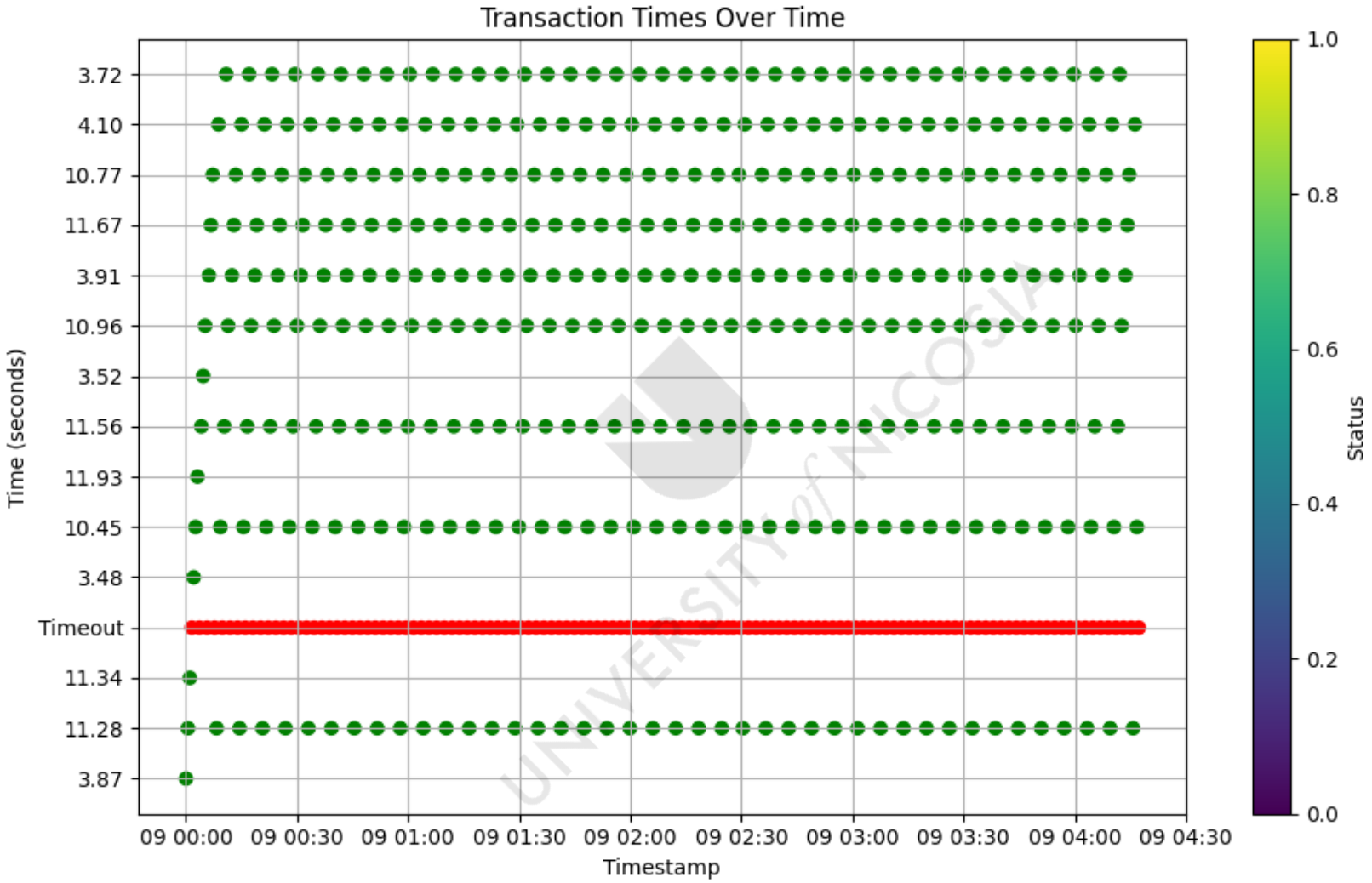


Figure 5.16: Ethereum Node Crash Scenario - Transactions' Processing Time over Time

5.5.3 Analysis and Discussion of Use case Two

For this use case, the Ethereum network instantiated with the Besu client and underwent an evaluation with the proposed BBF. The aim is to understand Ethereum's behavior and resilience under two specific adverse scenarios: a double-spend attack and node failure/crash. Starting with the foundation, a private Ethereum network is methodically set up using the BBF and Hyperledger Besu, similar to the approach employed with the XRPL client in discussed in use case one. This structured setup ensured that the experiments are conducted under standardized conditions, allowing for accurate performance assessment.

The double-spend attack simulation on Ethereum provided valuable insights into the robustness of Ethereum's CA. Similar to the XRPL client, which has mechanisms to guard against double-spend attacks, Ethereum also demonstrated its security measures against such actions. However, it's important to note that these findings should be seen as indicative rather than definitive, as blockchain security is a complex and multifaceted domain. The study revealed that Ethereum's CA plays an important role in maintaining transaction integrity, even under simulated attack conditions, suggesting its effectiveness in such scenarios without making absolute assertions about its invulnerability.

The node failure/crash experiment revealed insights into Ethereum's adaptability and fault tolerance. Drawing parallels with the XRPL client's behavior under similar conditions, Ethereum demonstrated its decentralized architecture's strength. Even in the face of sudden node interruptions, Ethereum managed to sustain operational continuity. However, the changes in performance, like longer transaction times during major node disruptions, are similar to what is observed in the XRPL network. These observations highlight the challenges blockchain protocols face in ensuring consistent performance while maintaining decentralization.

To sum up, similar to the XRPL scenario, the BBF played a pivotal role in the second use case. Its provision of a stable testing ground is instrumental in simulating various challenges and facilitated an in-depth analysis of Ethereum's operational capabilities. This underscores the BBF's significant value in blockchain research, emphasizing its contribution to consistent, reliable experimentation and analysis.

5.5.4 Use Case #2 - Research Hypotheses Testing

An in-depth analysis of the performance characteristics and resilience of the Ethereum blockchain protocol is conducted using the BBF. The key outcomes from this application can be linked to the research hypotheses defined in Section 3.5:

H1:	Hypothesis H1 is supported by the findings which reveal that the BBF effectively evaluates the performance of existing CAs within the Ethereum network, underscoring its robust analytical capabilities.
H2:	The utilization of the BBF in assessing and evaluating the Ethereum blockchain supported H2, by revealing the importance of comprehensive tools, frameworks, and documentation in enhancing the performance analysis of blockchain protocols.
H3:	The accessibility and usability of the BBF, demonstrated by the seamless integration and use of the Ethereum blockchain, lent support to H3, emphasizing that improved accessibility can foster greater adoption and understanding of blockchain technology. This usability is facilitated through the BBF's command line tool, serving as the access portal for users.
H4:	The BBF's ability to simulate real-world conditions for stress testing Ethereum's network performance confirmed H4, highlighting that frameworks closely mimicking real-world conditions yield more accurate and reliable assessments.

5.6 Comparative Analysis Across Use Cases

5.6.1 Comparing Hypotheses Across Use Cases

This section presents a comparative analysis of the research hypotheses as evaluated through the two use cases: the XRPL client and the Ethereum client. This analysis aims to highlight similarities and differences in the application of these hypotheses within each blockchain protocol, offering a detailed understanding of the BBF's applicability and effectiveness. Table *5.2* presents a side-by-side comparison of the findings related to each research hypothesis from the XRPL and Ethereum client studies, providing a clear visual representation of the outcomes for each hypothesis across the two use cases.

Table 5.2: Research Hypotheses Comparative Analysis

Hypothesis	Description	XRPL Client Findings	Ethereum Client Findings	Result
H1:	The development of a new blockchain CA that adequately balances decentralization, security, and scalability enhances the operational efficiency and security of blockchain applications.	BBF analyzed the complexities of XRPL's CA.	BBF analyzed the complexities of ETH's CA.	Supported
H2	The implementation of comprehensive tools, frameworks, and documentation significantly improve the assessment and performance of blockchain protocols.	BBF indicated performance enhancement in XRPL client assessment.	BBF improved performance analysis in Ethereum blockchain.	Supported
H3	Enhancing the accessibility and usability of blockchain ecosystems, including seamless configuration, and bootstrapping of private blockchain protocols, encourage the adoption and understanding of blockchain technologies.	BBF's usability evidenced through its command line tool for XRPL client interaction.	Usability of BBF via command line tool confirmed for Ethereum blockchain integration.	Supported

H4	Blockchain simulation frameworks that closely mimic real-world conditions provide more accurate and reliable performance assessment results than those based on theoretical assumptions.	BBF's Byzantine fault simulations provided pragmatic assessments for XRPL.	BBF effectively simulated real-world conditions in stress testing Ethereum's network.	Supported

The BBF's ability to analyze different CAs (H1) in both blockchain clients shows its flexibility and precision. The differences in the impact of Byzantine faults on each client (observed in H4) underline the unique challenges and resilience of each blockchain's architecture. Additionally, the BBF's applicability and design, H3 is confirmed by its successful use across different blockchain environments, showing its potential as a standard tool in blockchain performance evaluation. These insights have practical implications in blockchain development and benchmarking, suggesting the BBF's suitability for broad application in diverse blockchain protocols.

5.6.2 Comparing Model Key Metrics Across Use Cases

This section extends the comparative analysis to key performance metrics in the two use cases: the Ethereum protocol with PoA and the XRPL protocol using the RPCA. This comparison highlights how the BBF measures and validates crucial aspects like latency, throughput, consensus time, and security under conditions like double-spend attacks and node failures. Table *5.3* compares the validation of key performance metrics in the Ethereum and XRPL use cases. Each metric is critical for assessing the efficiency and robustness of blockchain protocols. The table shows whether the BBF effectively validated each metric in each use case.

Table 5.3: BBF Key Metrics Comparison Across Use Cases

Metric/Aspect	Description	Validated in Ethereum (PoA) Use Case	Validated in XRPL (RPCA) Use Case
Latency	Time for transaction confirmation.	Yes, with noted increases during node failures.	Yes, fluctuations observed during node failures.
Throughput	Transactions processed per time unit.	Implied stable, based on operational continuity.	Implied stable, based on operational continuity.
Consensus Time	Time to reach consensus.	Implied effective, based on attack resilience.	Implied effective, based on attack prevention.

Response to Double Spend Attack	Ability to prevent double spend attacks.	Yes, effective measures in simulations.	Yes, significant resistance demonstrated.
Node Failure/Crash Resilience	Continuity in case of node failures/crashes.	Yes, maintained operational continuity.	Yes, showed resilience and fault tolerance.

This analysis shows that both Ethereum and XRPL clients underwent thorough testing under various conditions, effectively validating several key metrics. While some metrics like latency and response to double-spend attacks are clearly confirmed in both cases, others like throughput and consensus time are more indirectly suggested by the overall resilience of the protocols. These findings highlight the BBF's capability to provide a comprehensive assessment of blockchain protocols and its flexibility in evaluating different architectures and CAs. This comparative overview not only validates the BBF as an effective tool for blockchain analysis but also deepens the understanding of the strengths and challenges of Ethereum's PoA and XRPL's RPCA, offering valuable insights for the further development and refinement of blockchain technologies and benchmarking tools.

5.7 Theoretical Triangulation and Expert Consultation

This thesis incorporates theoretical triangulation, as discussed in Section 4.5.3.1, to strengthen the empirical findings of this chapter. The study's results are cross-examined with existing theories and models in blockchain and benchmarking literature to evaluate consistency and to pinpoint areas of discrepancy. This comparison not only corroborates the empirical methods employed but also identifies potential directions for further research, contributing to the revision of the BBF.

Engagement with specialists from the University Blockchain Research Initiative (UBRI) has been a consistent feature of the research process. This study benefitted from multiple discussions in which the progression and intended functionality of the BBF were presented to and critiqued

by these experts. Their input has been essential, providing a reciprocal and constructive platform for feedback.

The modifications proposed in Chapter 6 bear the mark of these consultative sessions. The dialogue with UBRI experts has been crucial in revising the BBF, ensuring that it not only incorporates empirical evidence but also aligns with the broader scholarly dialogue in the blockchain domain.

5.8 Conclusions

The aim of this research is to design and test a BBF capable of assessing the performance metrics of diverse blockchain protocols under varied conditions. The aim is realized through rigorous research, wherein a set of metrics and evaluation methodologies are designed to provide an in-depth analysis of different blockchain clients.

The BBF is tested with two distinct use cases: the XRPL client and Ethereum client each offering their own unique set of challenges and insights. In the case of XRPL, the researcher did not merely focus on its performance under standard operations. The BBF is employed to simulate Byzantine faults, specifically a double-spend attack and node failures, to gauge XRPL's resilience and performance under these adversarial conditions. The results showcased XRPL's robustness, particularly its ability to defend against double-spend attacks, reinforcing its potential as a reliable platform for transactions. With the second use case and Ethereum client, the BBF played a pivotal role in setting up a private Ethereum network, simulating a double-spend attack, and inducing node crashes to evaluate its robustness. The Ethereum network, while displaying an inherent resilience against these scenarios, did show performance discrepancies, such as increased transaction latency during high node failures. This analysis demonstrated Ethereum's versatility as a platform for decentralized applications and its resilience against common Byzantine faults.

Across both use case studies, the BBF proved effective and versatile. It is able to adapt to the unique requirements and characteristics of each blockchain client, producing insightful results that allowed for meaningful comparisons. The framework's strengths lie in its comprehensive

nature, capturing multiple facets of blockchain performance, including transaction times, network resilience, and the impact of varying conditions on performance. Furthermore, the framework can be easily adapted to assess other blockchain protocols, demonstrating its versatility and ease of use.

Chapter 6: Revised Blockchain Benchmarking Framework

The first principle is that you must not fool yourself, and you are the easiest person to fool.

Richard Feynman (1918 – 1988)

Summary

Chapter 5 evaluates the proposed conceptual framework reported in Section 3.4 using a quantitative, positivism, deductive experimental research methodology as reported in Chapter 4. XRPL and Ethereum are selected as the use case studies of this thesis, while Chapter 5 assesses each network's performance, resilience, and response to a set of different conditions, such as double-spend attack and node failure or crash. Based on the findings of the previous chapter, Chapter 6 synthesizes insights from these use case studies to propose the Revised Blockchain Benchmarking Framework (RBBF). The chapter begins with an overview, laying the groundwork for a review of the findings from the framework's application to the two use case studies. Reflecting on both the successful outcomes and the challenges encountered, Chapter 6 proposes revisions of the initially proposed BBF. This revision aims to enhance the framework's efficiency and adaptability in diverse blockchain settings. The chapter concludes by summarizing the key findings, underscoring the role of the revised BBF in advancing the understanding of blockchain protocol performance.

6.1 Introduction

The dynamic and diverse nature of blockchain technology underscores the need for a robust and adaptable benchmarking framework. As explored in the literature review reported in Chapter 2, existing frameworks often fall short in addressing the complex characteristics of various blockchain protocols. Furthermore, there is a notable absence of a comprehensive tool or mechanism that could act as a decision-making tool, aiding in more informed and strategic evaluations of blockchain technologies.

To address these challenges, this thesis proposes a conceptual model, detailed in Chapter 3, as a tool for validating the design decisions and technical specifications of blockchain protocols in an automated and methodological way. This framework is designed to encapsulate crucial stages and elements needed for a thorough evaluation of blockchain protocols. In Chapter 4, a suitable research methodology for this thesis was selected, opting for a positivism research stance and a quantitative experimental research strategy to test the BBF.

In Chapter 5, the BBF underwent empirical evaluations involving two blockchain protocols, XRPL and Ethereum. These evaluations not only demonstrated the BBF's practical applicability but also highlighted its effectiveness in providing insightful analyses of the performance and resilience of these blockchain clients.

However, the insights gathered from these empirical evaluations indicated further complexities within the blockchain domain, necessitating additional refinement of the BBF. Consequently, Chapter 6 begins with a reflection on the lessons learned from these use case studies, as detailed in Section 6.2. Building on these insights, the chapter introduces the Revised Blockchain Benchmarking Framework (RBBF), outlined in Section 6.3. This revision incorporates modifications and enhancements to ensure that the framework remains relevant and effective in the landscape of blockchain technology. The chapter concludes with a synthesis of the key findings in Section 6.4.

6.2 Lessons Learned

The investigation into the XRPL and Ethereum use cases offered vital insights regarding the BBF's application, as proposed in this thesis. Through the experimental approach, the researcher concentrated significant understanding about the framework's effectiveness, its suitability in different contexts, and areas where it might benefit from revision. A summary of the lessons learned from the use case studies follows:

Lesson 1 - The BBF should be tailored to accommodate the specific attributes of different blockchain clients: The experiments in Chapter 5 demonstrated how the unique CAs of XRPL and Ethereum influenced their responses to Byzantine faults like double-spend attacks and node failures. The XRPL's resistance to double-spend attacks and Ethereum's resilience under node failure scenarios, as discussed in Sections 5.4.3 and 5.5.3 respectively, underscore the need for a BBF that can adapt to the unique characteristics of each blockchain client.

Lesson 2 - Comprehensive benchmarking requires considering a range of factors, including smart contracts and transaction types: The analysis in both use cases highlighted the importance of considering diverse metrics beyond TPS or latency. For instance, the impact of smart contracts and different transaction types on Ethereum's performance, as discussed in Section 5.5.3, calls for a more comprehensive benchmarking approach that accounts for various functional aspects of blockchain protocols.

Lesson 3 - The BBF should accommodate various transaction submission methods, reflecting their significant impact on blockchain performance: As discussed in Section 5.4.2.1.1 and Section 5.5.2.1.1, different transaction submission methods and their impact on blockchain performance are evident in the evaluations of both XRPL and Ethereum. The need for the BBF to accommodate varied transaction strategies is critical, as demonstrated in both use case studies.

Lesson 4 - Advanced stress testing, is essential to reveal blockchain systems' robustness and resilience: The importance of advanced stress testing methods is highlighted by the node failure scenarios in both XRPL and Ethereum analyses. These tests, as elaborated in Sections

5.4.3 and 5.5.3, reveal the systems' robustness and resilience, suggesting that the BBF should incorporate more detailed stress testing approaches.

Lesson 5 - The BBF needs to capture a broad range of performance-affecting factors: The detailed performance analyses in both use cases, especially regarding network latency and transaction processing under stress, emphasize the need for the BBF to capture a broad spectrum of performance-affecting factors, as demonstrated in Sections 5.4.3 and 5.5.3.

Lesson 6 - Empirical evaluations of blockchain protocols guide decision-making more effectively than theoretical assumptions: The empirical evaluations in both use cases illustrated how a well-designed benchmarking framework can guide decision-making, especially in selecting and deploying suitable blockchain protocols based on empirical data rather than theoretical assumptions.

6.3 The Revised Blockchain Benchmarking Framework

Drawing from the empirical examination of the XRPL and Ethereum use cases, the researcher identified key lessons and insights. These serve as the basis for modifications and revisions to the BBF proposed in Chapter 3. In light of the lessons learned discussed in Section 6.2 and their direct implications for each architectural layer of the BBF- as detailed in Table 6.1 - this section introduces detailed revisions for the proposed revised BBF. These revisions, spanning Sections 6.3.1 – 6.3.5, aim to enhance the framework's applicability towards the aim of this thesis.

Table 6.1: Alignment of Lessons Learned with BBF's three-layer Architecture

Layer	Lessons Learned
Infrastructure Layer	**Lesson 1:** Emphasizes the need for BBF's flexibility to adapt to diverse blockchain characteristics, as shown in the distinct CAs of XRPL and Ethereum.
Execution Layer	**Lesson 2:** Highlights the importance of a comprehensive approach to evaluate blockchain features beyond basic metrics. **Lesson 3:** Demonstrates the significant impact of different transaction submission methods on blockchain performance.
Execution Layer	**Lesson 4:** Indicates the necessity for advanced, protocol-specific stress testing methods, as revealed by the varied responses of XRPL and Ethereum under stress.
Visualization Layer	**Lesson 5:** Calls for a wide-ranging inclusion of performance factors to ensure a thorough benchmarking process.
Visualization Layer	**Lesson 6:** Illustrates how a well-designed BBF can guide decision-making by providing empirical data for selecting appropriate blockchain protocols.

Table *6.1* establishes a direct link between the architectural layers of the BBF and the empirical lessons derived from the examination of the XRPL and Ethereum use cases. This alignment allows a systematic framework for the next sections, whereby particular revisions to the BBF are outlined. Sections 6.3.1 through 6.3.5 analyze these revisions, outlining specific enhancements guided by these empirical findings. Consequently, this process results in the introduction of the revised BBF, as depicted in Figure *6.1*, which illustrates a more comprehensive version of the initially proposed BBF, and the architectural enhancements discussed in detail in the forthcoming sections.

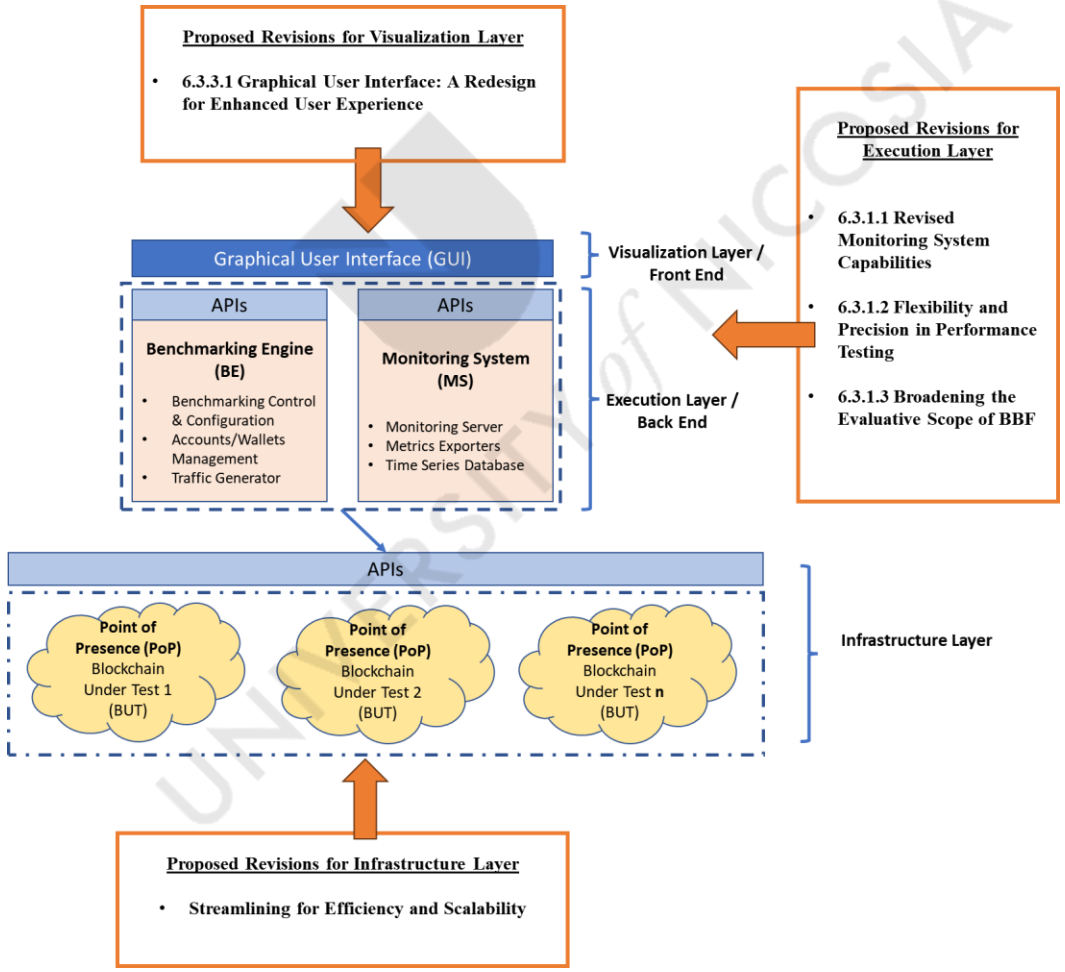


Figure 6.1: Revised Conceptual BBF

6.3.1 Execution Layer

6.3.1.1 Revised Monitoring System Capabilities

The necessity for flexibility and adaptability in the benchmarking framework, as Lesson 1 highlights, has led to the proposal of significant enhancements in the BBF's Monitoring System (MS). The proposed revised MS includes a suite of advanced data visualization tools that would aid in the interpretation of the benchmarking outcomes.

Proposed changes: The design of the visual analytics layer is proposed to be more intuitive and interactive. Users would be able to adjust settings in real-time and understand the implications of these adjustments on benchmarking outcomes. This would be facilitated using dynamic graphs, heatmaps, and other visual aids that present complex blockchain data in an easily understandable format. Furthermore, the interface would allow users to customize their view and focus on specific aspects of the data, enhancing the user's ability to interpret and interact with the information.

Examples: For instance, a user would be able to interact with the impact of transaction load on network performance through a simple slider interface and observe the effects in real-time on a dynamic graph. The graphs – as would be depicted in Figure *6.2* and Figure *6.3* - would display key performance metrics such as TPS, latency, and network resilience, clearly illustrating the impact of the transaction load.

Implications of proposed changes: These proposed changes would enhance the accessibility and usability of the BBF, empowering users to interact effectively with the system and gain deeper insights into blockchain performance. As such, the RBBF MS aims to support more informed decision-making processes, catering to both technical and non-technical users.

Figure 6.2: Enhanced Visual Analytics Layer of RBBF – Part A

Figure *6.2* illustrates the enhanced visual analytics layer, showcasing the sophisticated data visualization capabilities proposed for the RBBF. It features dynamic graphs that provide real-time insights into disk I/O performance and network traffic, enabling users to immediately grasp the impact of different benchmarking scenarios on system resources.

Figure 6.3: Enhanced Visual Analytics Layer of RBBF - Part B

Figure *6.3* offers a comprehensive view of the system's performance, with detailed visualizations of CPU usage, memory allocation, block processing, and transaction pool metrics. It demonstrates the RBBF's proposed ability to monitor and analyze complex interactions within the blockchain environment, facilitating an in-depth understanding of protocol behavior under various load conditions.

6.3.1.2 Flexibility and Precision in Performance Testing

Considering Lessons 3 and 4, it is proposed to enhance the execution layer of the BBF. The proposed changes focus on accommodating different transaction submission approaches and diverse data types, recognizing their substantial impact on blockchain performance, as identified in the empirical evaluations of Section 5.4 and Section 5.5.

Proposed changes: The Benchmarking Engine (BE), a key component of the execution layer, would include a more flexible and comprehensive suite of tools for transaction submission, aligning with Lesson 3's emphasis on the impact of transaction strategies. This would enable testing under various real-world scenarios. Additionally, the BE is proposed to feature options for handling diverse data types – as illustrated in Figure *6.4*, – reflecting Lesson 5's call for a broad range of performance factors. The MS is also planned to undergo a redesign, making it more dynamic for efficient data storage, access, and visualization.

Examples: The revised BE would simulate both uniform and non-uniform transaction submission rates, addressing Lesson 3 by reflecting varied real-world conditions. It could also test the impact of different data types, like value transfers or smart contracts, on network performance, offering insights aligned with Lesson 5.

Implications of proposed changes: These proposed enhancements aim to provide a more accurate and comprehensive evaluation of blockchain protocols. By enabling a more detailed analysis, the framework would enhance users' understanding of blockchain performance under different conditions, facilitating more informed decision-making, in line with Lesson 6.

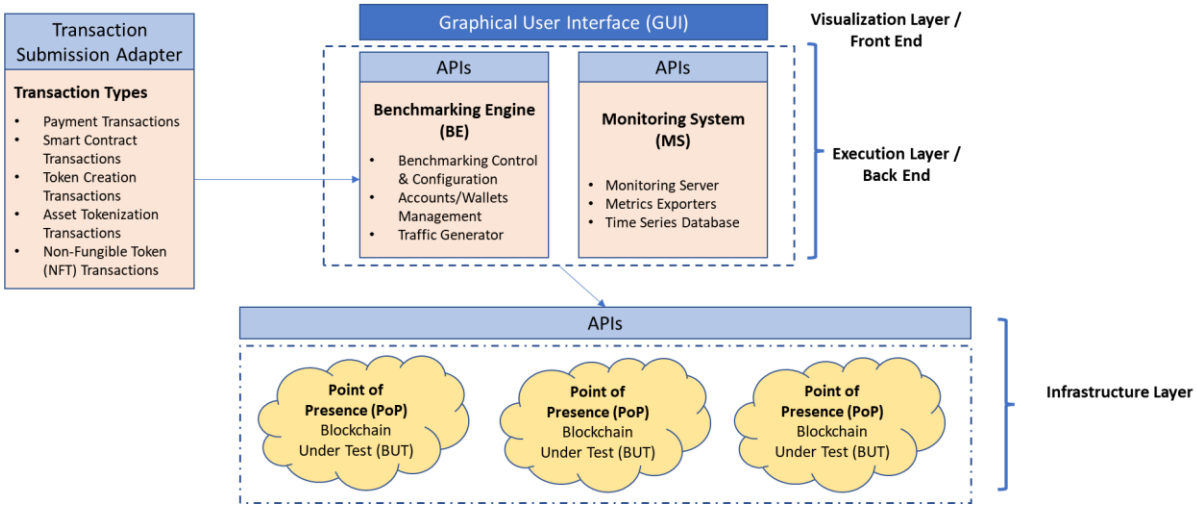


Figure 6.4: Updated execution layer of RBBF

6.3.1.3 Broadening the Evaluative Scope of BBF

The architectural components of the BBF are proposed to be revised in response to insights from Lessons 2 and 5. The RBBF is planned to expand beyond standard metrics such as Transactions Per Second (TPS) and latency, incorporating evaluations of blockchain-specific features like smart contract functionality and network latency, as well as other distinct characteristics particular to each blockchain protocol. These enhancements aim to ensure a more comprehensive evaluation of different blockchain clients.

Proposed changes: The changes to the architectural components of the BBF include the addition of new metrics and the enhancement of existing ones to achieve greater precision. For instance, the RBBF includes proposed metrics for evaluating the performance of smart contracts, recognizing their increasing importance in blockchain systems like Ethereum. It also includes proposed metrics for evaluating network latency, which is identified as a critical factor in the performance of blockchain protocols. Moreover, users would be able to include custom metrics by developing custom metrics exporters compatible with the monitoring system. The corresponding updates on the RBBF are depicted in Figure *6.5*. This figure visualizes the RBBF's enhanced architecture, showing the integration of custom metrics exporters like the Smart Contract Metrics Exporter, which feeds into a monitoring system composed of Grafana and Prometheus. It illustrates the flow from custom and standard metric exporters to the

Prometheus Monitoring Server and then to Grafana for visualization, underlining the framework's capacity for extensive and adaptable performance analysis.

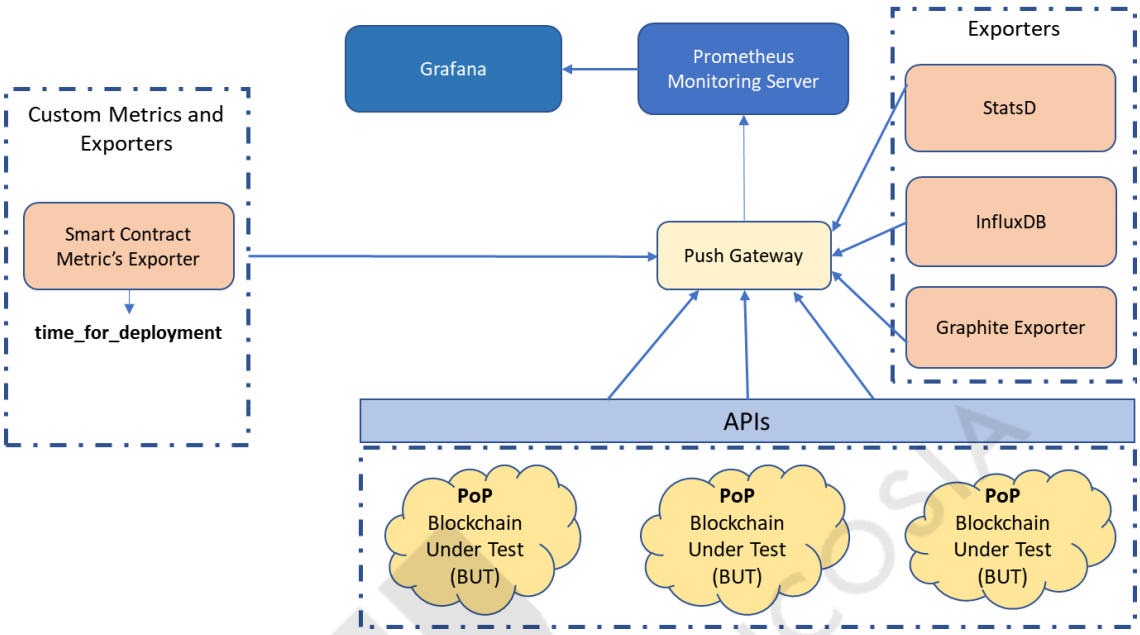


Figure 6.5: RBBF's Enhanced Architecture with Custom Metrics Integration

Examples: For example, the revised framework would now be able to evaluate the time it takes to execute a smart contract on Ethereum, considering factors like gas costs and network congestion. Similarly, it could assess the impact of network latency on the performance of XRPL, considering factors like the number of nodes and their geographical distribution.

Implications of proposed changes: These enhancements allow the BBF to support a wider spectrum of blockchain protocols, thereby aiding users in making informed decisions about the selection and utilization of different blockchain clients. Moreover, by introducing the capability to incorporate and analyze custom metrics, such as those for smart contract performance, the framework opens up new avenues for empirical research. It encourages detailed investigation into how specific blockchain features can influence overall system performance, potentially driving innovation in blockchain technology optimization and application.

6.3.2 Infrastructure Layer

6.3.2.1 Streamlining for Efficiency and Scalability

The infrastructure layer of the BBF is proposed to be streamlined to better accommodate the diverse nature of blockchain protocols, as highlighted in Lesson 6. The proposed modifications to this layer aim to simplify the configuration and deployment of different blockchain protocols, thereby reducing the time and effort required to set up benchmarking tests.

Proposed changes: The infrastructure layer is envisioned to undergo a redesign to facilitate a smoother deployment of different blockchain clients. This redesign includes the integration of pre-configured templates for common blockchain configurations, simplifying the initial setup process for various blockchain clients. Furthermore, the interface for custom configurations is proposed to be more user-friendly, enhancing ease of use for a broader range of users. Additionally, the implementation of automated scripts for deploying and dismantling test networks is planned to streamline the overall process, reducing the technical overhead for users of the BBF. These enhancements would contribute significantly to the ease of managing and executing benchmarking tests, reflecting the updated architecture of the RBBF as depicted in Figure *6.6*. The architecture illustrated in Figure *6.6* provides a visual representation of these enhancements to the infrastructure layer. It depicts the interconnectivity between the pre-configured templates, the user-friendly configuration interfaces, and the automated scripting processes, all designed to streamline the deployment of blockchain networks. This figure also emphasizes the modular design of the RBBF, showcasing how each component of the infrastructure layer contributes to a cohesive benchmarking environment that can be easily adapted to various blockchain protocols and testing scenarios.

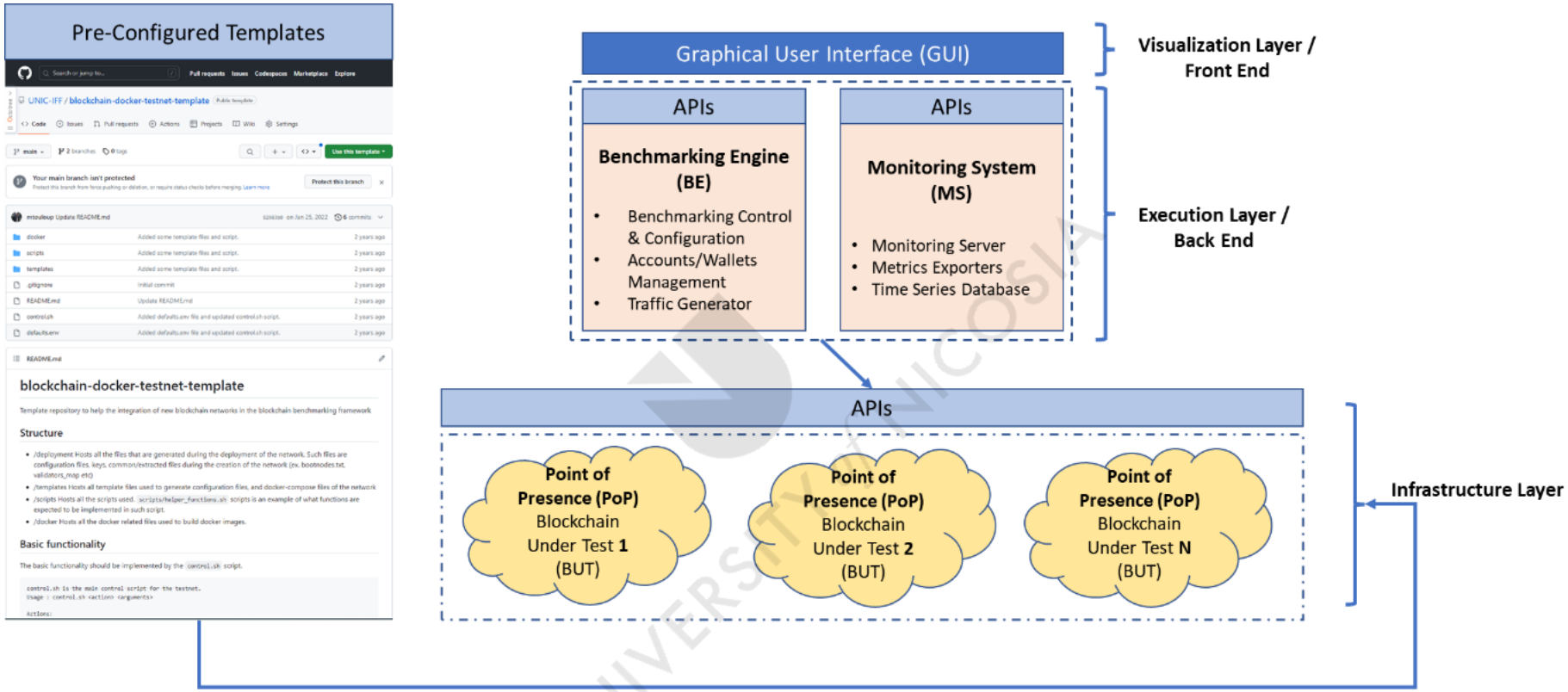


Figure 6.6: RBBF Proposed Revised Architecture

Examples: For instance, the infrastructure layer could handle the deployment of both public and private blockchain protocols, accommodating different CAs and network sizes. It would also allow for the configuration of various parameters such as block size, transaction rate, and network latency, providing a more realistic testing environment that aligns with real-world conditions.

Implications of proposed changes: The updates introduced in the infrastructure layer aim to enable the BBF to accommodate a broader range of blockchain clients, reflecting their unique characteristics and attributes. By simplifying the configuration and deployment process, the framework reduces the barrier to entry for users who wish to benchmark different blockchain protocols. This, in turn, can contribute to a more widespread and informed use of blockchain technology.

6.3.3 Visualization Layer

6.3.3.1 Graphical User Interface: A Redesign for Enhanced User Experience

The proposed enhancements to the GUI in this chapter are a continuation of the BBF's developmental journey. They are built upon the foundational ideas presented in Chapter 3 and are directly informed by the empirical insights and user interactions observed during the testing phase detailed in Chapter 5. The GUI of the RBBF is proposed to be significantly redesigned, leveraging modern web technologies, and adhering to material design principles, aligning closely with updated Lesson 5, which emphasizes the importance of user experience and ease of use for the effective adoption and utilization of blockchain benchmarking tools.

Detailed changes: The GUI will continue to be divided into modules such as the dashboard, users' section, testing and benchmarking, and monitoring system. However, each of these modules is proposed to be improved for better usability and extended applicability. For example, the dashboard is envisioned to provide a more comprehensive overview of the benchmarking results, displaying key metrics in an easy-to-understand format. The testing and benchmarking module includes advanced features proposed for configuring and running benchmarks, making it easier for users to tailor the benchmarking process to their specific needs. These enhancements are to be depicted in Figure *6.7*.

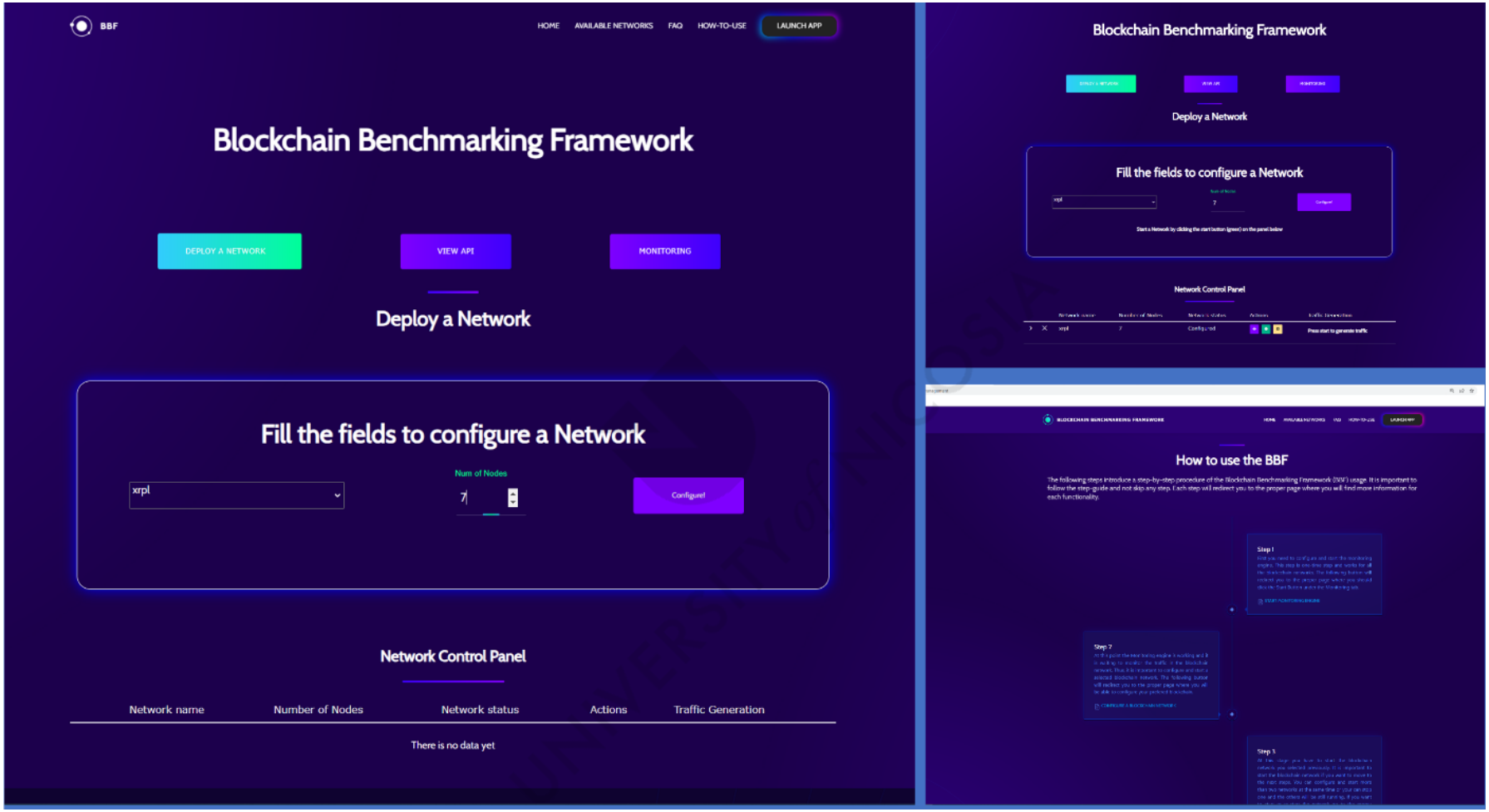


Figure 6.7: Proposed Revision for the GUI of RBBF

Examples: Specifically, within the RBBF, the MS module, to be integrated into the GUI, would provide real-time visualization of key performance indicators. This functionality would enable users to precisely measure and understand transaction finality, system throughput under varying loads, and the impact of network latency on transaction propagation. Real-time data visualization would also assist in promptly identifying and diagnosing system bottlenecks or performance degradation during benchmark execution.

Implications of proposed changes: The proposed enhancements to the GUI would not only improve the overall user experience but also make the BBF more accessible. For instance, the GUI would be designed to simplify the process of initiating and monitoring benchmark tests by abstracting the complexities of blockchain metrics collection and analysis. By providing straightforward mechanisms to initiate benchmarks and interpret results, the updated GUI would facilitate a more inclusive user engagement, extending the RBBF's reach to include a diverse range of users, from blockchain developers who may leverage the system for performance tuning to organizational decision-makers who require clarity on blockchain technology's viability for their specific use cases.

6.4 Conclusions

This chapter focuses on the analysis of findings from the application of the BBF to the XRPL and Ethereum use cases, leveraging these insights to propose enhancements for the framework. The lessons learned, as outlined in Section 6.2, inform the identification of both the strengths and areas for improvement in the BBF's application to real-world blockchain clients, highlighting the necessity for an adaptable and dynamic benchmarking tool.

The RBBF, as detailed in Section 6.3, encompasses proposed revisions that aim to elevate its functionality and relevance across various blockchain settings. The RBBF would feature an advanced visual analytics layer for more effective data interpretation, a refined execution layer for flexible benchmarking, an optimized infrastructure layer for simplified setup, and augmented architectural components that expand its evaluative scope. In addition, the user

interface is proposed to be redesigned for greater usability, making it accessible to a wider audience, including those without extensive technical expertise in blockchain technology.

The proposed revisions to the BBF address the immediate findings from the use case studies and also set a foundation for the ongoing development of blockchain benchmarking tools. The RBBF stands as a proposed robust, adaptable, and inclusive framework, poised to make a significant contribution to the field of blockchain technology. It is expected to support comparison and evaluation of diverse blockchain protocols, aiding stakeholders in making informed decisions about the adoption and implementation of blockchain systems as well as validating the design decisions of different blockchain clients. In essence, this chapter consolidates the research journey, showcasing how empirical findings catalyze the evolution of a benchmarking framework to meet the current and future demands of blockchain technology. To this end, it is worth nothing that the revised BBF needs to be tested in the practical arena before adopted.

Chapter 7: Novel Contribution and Future Work

The only limit to our realization of tomorrow will be our doubts of today.

Franklin D. Roosevelt (1882 - 1945)

Summary

Chapter 7 concludes the research presented in this thesis, highlighting its achievements, contributions, and potential areas for future work. Section 7.1 provides an overview of the thesis, integrating insights from both the literature and the empirical studies. Section 7.2 assesses the fulfillment of the thesis's objectives, while Section 7.3 presents the main findings, notably the practical refinement of the BBF informed by two use case studies involving blockchain protocols such as the XRPL and Ethereum's Besu client. The contributions of this research are discussed in Section 7.4 while Section 7.5 addresses the research limitations, providing context for the interpretation of results, with a particular focus on the evaluation of blockchain performance metrics. This thesis concludes with Section 7.6, where the researcher discusses future research directions, highlighting avenues for advancing different blockchain benchmarking methodologies.

7.1 Research Overview

This thesis focuses on the development and validation of a BBF, with an emphasis on analyzing XRPL and Ethereum, two prominent blockchain protocols. Chapter 1 sets the stage for the entire thesis, introducing the research problem by highlighting the critical impact of CAs on blockchain's functionality. Furthermore, Chapter 1 outlines the research aim and objectives, which center on understanding the influence of CAs on blockchain performance and the development of a robust benchmarking framework.

In Chapter 2, a systematic literature review surrounds blockchain technology, CAs, and existing benchmarking methods is conducted. This review highlights the need for a robust and adaptable framework for blockchain benchmarking, as summarized in Figure *2.3* . Based on these findings, an initial BBF is developed. Chapter 3 maps the development of the BBF with the research goals outlined in Chapter 1. The BBF is designed to assess the performance and robustness of different blockchain technologies, with key performance indicators such as transaction speed, scalability, security, decentralization, and sustainability. The BBF's construction and the role of these components are detailed in Section 3.5.

In Chapter 4, the research methodology is described and justified. The experimental research strategy is identified as the most suitable approach to test the BBF, with XRPL and Ethereum serving as the use case studies. The BBF is put to the test in Chapter 5, where it is applied to the XRPL and Ethereum use cases. The results of this application, as detailed in Sections 5.2 and 5.3 respectively, provide valuable insights into the strengths and weaknesses of each blockchain technology, as well as the applicability and limitations of the BBF itself.

Chapter 6 focuses on the interpretation of the use case findings and the revision process of the BBF. Based on the lessons learned from the use case studies, the BBF is revised and improved to form the revised version of the initially proposed BBF. The revised framework addresses the limitations of the original BBF and provides a more robust and dynamic tool for benchmarking blockchain protocols. The revised BBF contributes to the body of knowledge by providing a comprehensive framework for benchmarking blockchain protocols.

7.2 Meeting the Objectives of this Thesis

To realize the aim of this thesis, specific objectives are set out in Chapter 1 and have been systematically addressed in the subsequent chapters. These objectives are itemized in Table *7.1* and are further discussed in the following paragraphs:

Table 7.1: Meeting the Objectives of this Dissertation.

Objective	Chapter	Chapter Element
Objective 1: To conduct a systematic literature regarding the performance of blockchain CAs.	Chapter 2	Systematic Literature Review (SLR)
Objective 2: To design and implement a conceptual framework for measuring the performance of the CAs.	Chapter 3	Proposed Conceptual BBF
Objective 3: To evaluate the proposed conceptual framework.	Chapter 4, Chapter 5 & Chapter 6	Research Methodology, Empirical Data and Revision of the BBF
Objective 4: To extrapolate conclusions and provide novel contributions regarding the performance of blockchain CAs.	Chapter 7	Novel Contribution and Future Work

- **Objective 1:** *To conduct a systematic literature review regarding the performance of blockchain CAs.*

A systematic literature review is conducted to gain a comprehensive understanding of performance evaluation methods for blockchain CAs, as presented in Chapter 2. This review analyzes the existing literature and identifies challenges in assessing the performance of CAs. It reveals a research gap regarding the lack of a standardized and adaptable benchmarking framework that can evaluate blockchain CAs, guiding the development of the proposed BBF discussed in Chapter 3. This finding lays the foundation for the thesis's aim, as this is defined in Section 1.2.1, to create a framework that not only benchmarks the performance of CAs but also validates their design decisions in the context of different blockchain protocols.

- **Objective 2:** *To design and implement a conceptual model for measuring the performance of the CAs.*

Grounded on the findings from the literature review, a BBF is developed as this is described in Section 3.4. This framework is designed and developed to fill the gap identified in the literature, offering a novel way to assess the performance of blockchain CAs and thus the blockchain protocol itself. The BBF is presented and explained in Chapter 3, outlining its components and architecture.

- **Objective 3:** *To evaluate the proposed conceptual model.*

A research methodology –Chapter 4-, is employed to test and validate the BBF, employing a quantitative, experimental strategy that aligns with the thesis's positivist stance. This approach ensures a systematic evaluation of the proposed framework. The BBF undergoes a comprehensive examination in Chapter 5 through its application to the blockchain protocols of XRPL and Ethereum, outlined in Sections 5.4 and 5.5. The outcome of these use case studies provides critical insights into the operational efficacy and versatility of the BBF, demonstrating its ability to assess and differentiate the performance of blockchain protocols based on their consensus algorithms.

- **Objective 4:** *To extrapolate conclusions and provide novel contributions regarding the performance of blockchain CAs.*

The insights gathered from the BBF's application to XRPL and Ethereum, as presented in Chapter 5, inform the theoretical development of the revised BBF outlined in Chapter 6. This thesis proposes a set of enhancements for the BBF, anticipating a holistic approach to benchmarking blockchain CAs. Although the revised BBF remains untested within the scope of this thesis, it constitutes a significant theoretical contribution to the field, proposing a framework designed to overcome the challenges identified in the empirical analysis. The revised BBF is poised to provide a robust tool for future empirical validation and benchmarking of blockchain protocols, reflecting a deepened understanding of the dynamics of blockchain CAs.

7.3 Main Findings

This research aimed to develop and validate a BBF for evaluating and comparing different blockchain protocols. Two significant blockchain protocols, XRPL and Ethereum, are used as use case studies to test the BBF. The main findings of this experimental research are as follows:

Finding 1	Building upon the blockchain trilemma, which outlines the challenges of achieving decentralization, security, and scalability simultaneously, the literature review conducted in this thesis (Chapter 2, Sections 2.4 to 2.4.1) reveals that current CAs often struggle to uniformly address these three aspects. While many CAs aim to balance these challenges, the literature review reveals that a universally applicable solution excelling in all three aspects remains elusive. This finding, discussed in the context of existing blockchain CAs, underscores the ongoing need for research and innovation in developing CAs that can more effectively harmonize these critical features.
Finding 2	Grounded on the review of the normative literature, identified significant gaps between the theoretical advantages of blockchain technology and its practical implementation challenges are identified. Despite the enthusiasm surrounding blockchain's potential for mainstream adoption, technical

issues among others like stability, operational efficiency, and security require further advancement. Scalability remains a critical challenge, as detailed in the comparative analysis of CA properties in Table *2.4*.

Finding 3

The literature review, as conducted in Chapter 2, reveals a gap in the availability of comprehensive benchmarking tools for blockchain protocols, a point also underscored in Observation C of Section 2.4. This gap highlights a broadly acknowledged need for advanced benchmarking tools to address the current limitations in evaluating blockchain performance. The scarcity of such tools, along with the lack of complete frameworks and thorough documentation, is emphasized as a critical barrier to the effective assessment and analysis of blockchain protocol performance.

Finding 4

The application of the BBF to the XRPL and Ethereum use cases, as detailed in Chapters 5.4 and 5.5, confirms its effectiveness in assessing the performance of blockchain protocols. Its strengths lie in its comprehensive consideration of key performance indicators such as transaction speed, scalability, security, decentralization, and sustainability. The effectiveness of the BBF in capturing these performance metrics is further supported by the data presented in Table *5.3*, which provides a detailed comparison of these key indicators across the two blockchain protocols.

Finding 5

The use case studies conducted on XRPL and Ethereum, as detailed in Sections 5.4 and 5.5, provide valuable insights into the strengths and weaknesses of each blockchain client. For instance, XRPL demonstrated superior transaction speed (Section 5.4.2.1.2), while Ethereum showcased greater decentralization (Section 5.5.2.1.2). These findings illustrate the trade-offs inherent in blockchain design and emphasize the importance of

aligning the choice of blockchain technology with specific use-case requirements.

Finding 6

The research conducted in this thesis highlights the significant impact of CAs on the performance of blockchain protocols. The distinct differences in the CAs of XRPL (RPCA) and Ethereum (PoA), as examined in Sections 5.4.2.1 and 5.5.2.1, are found to significantly influence their performances in various aspects. This finding underscores the pivotal role of CAs in determining the efficiency and effectiveness of blockchain networks.

Finding 7

The empirical outcomes, as those are derived from Chapter 5, led to the identification of Lessons learned described in Chapter 6. The lessons learned highlighted the need for revisions to the initially proposed BBF.

Finding 8

The revised BBF, as proposed in Chapter 6, is shown to be a valuable tool for various stakeholders in the blockchain industry. It can aid developers in optimizing blockchain design, help investors make informed decisions, and assist regulators in understanding and assessing blockchain protocols. This utility of the revised BBF across different areas of blockchain development and deployment showcases its potential as a comprehensive tool for the blockchain community.

7.4 Novel Contribution

This thesis enriches the body of knowledge in blockchain protocols by presenting the revised BBF as its main theoretical contribution. The revised BBF is proposed as a versatile and robust tool, aiming to advance the framework for the practical assessment of blockchain technologies and contribute to the academic dialogue surrounding their evaluation. The novelties stemming from this research are systematically elaborated within this section, emphasizing the BBF's potential impact on the discipline.

Novelty 1: The Evolution and Adaptability of the BBF

The development of the BBF and its subsequent revision into the revised BBF represent significant advancements in the field of blockchain benchmarking. These improvements, specifically designed to address the limitations observed during the XRPL and Ethereum use cases, contribute to the framework's robustness and dynamism. Additionally, the BBF's adaptability is a crucial feature, considering the rapid technological advancements in blockchain protocols. This adaptability positions the BBF as an appropriate tool for the assessment of a diverse and evolving range of blockchain clients, making it a theoretically evolved tool for benchmarking blockchain protocols.

Novelty 2: Innovative Comparative Use Case Approach in Blockchain Benchmarking with the BBF

The development of an approach that integrates comparative use cases, as illustrated through the application of the BBF to XRPL and Ethereum in Chapters 5.4 and 5.5, serves as a foundational method for future benchmarking endeavors. This approach demonstrates how different blockchain protocols can be evaluated under a unified framework, providing insights into their respective strengths and weaknesses. The inclusion of these comparative use cases enriches the benchmarking process and offers a model for future empirical evaluations in the field.

Novelty 3: Comprehensive Review and Analysis of

The thesis provides an extensive review and critical analysis of blockchain protocols and benchmarking techniques, addressing the gap in existing scientific literature. This

Blockchain Protocols and Benchmarking Techniques

examination is not only confined to the literature review in Chapter 2 but also extends to Appendix III, where a detailed background on blockchain technology is presented, alongside a critical analysis of various blockchain CAs. This exploration contributes to the academic understanding of blockchain technologies and benchmarking methods, filling a notable gap of the literature.

Novelty 4: Introducing a Multi-dimensional Perspective for Assessing Blockchain Protocols

A perspective in blockchain protocol assessment is suggested, emphasizing the critical evaluation of transaction speed, scalability, security, decentralization, and sustainability, thereby enriching the body of knowledge within the thesis's domain.

Novelty 5: Enhancing the Blockchain Benchmarking Process - Streamlining and Expanding Capabilities

The thesis proposes a set of enhancements to the blockchain benchmarking process, as detailed in Chapter 3, Section 3.3. These enhancements aim to streamline the benchmarking process for various blockchain protocols by increasing the number of supported blockchains, introducing a methodology to simplify the integration of new protocols, expanding the range of monitored metrics, and focusing on real benchmarking scenarios. Furthermore, the proposed BBF includes a dynamic monitoring system to facilitate easy storage, access, and visualization of data. These improvements, illustrated in **Figure *3.2***, reduce technical barriers and simplify the benchmarking process, making it more accessible and applicable to a wider audience, including newcomers and non-experts to the blockchain field.

7.5 Research Limitations

Despite the significant contributions and findings of this research, acknowledging certain limitations encountered during the study is important. The research limitations of this thesis are as follows:

Limitation 1: Need for Wider Testing Across Various Blockchain Protocols with the BBF and RBBF	A larger sample of diverse blockchain protocols need to be tested using the BBF and RBBF. Also, the RBBF should be tested on the same use cases as the BBF (XRPL and Ethereum).
Limitation 2: Limitations in Generalizing Findings from XRPL and Ethereum to All Blockchain Protocols	The focus on two blockchain protocols, XRPL and Ethereum, to test and refine the BBF, offered valuable insights, yet these findings may not fully extend to all blockchain protocols. Each blockchain platform features distinct characteristics and constraints that might not be comprehensively addressed by the RBBF. For example, empirical evaluations of the XRPL client centered on specific types of Byzantine faults like double-spend attacks and node failures, which do not represent the full spectrum of potential issues in blockchain protocols. Similarly, the insights from the Ethereum client's analysis, conducted in a private network setting, may not directly translate to the behavior of Ethereum's public network.
Limitation 3: Context-Specific Insights - The Constraint of Focusing Solely on XRPL and Ethereum Use Cases	The research strategy, focusing on comparative use case studies of XRPL and Ethereum, provided in-depth insights but may also limit the broader applicability of the findings. These results are context-specific and may not be entirely applicable to other blockchain protocols.

Limitation 4: Challenges in Keeping Pace with the Rapid Evolution of Blockchain Technology in Benchmarking	The rapidly evolving nature of blockchain technology presents a challenge for benchmarking frameworks like the RBBF, which, despite its adaptability, may need continuous updates to account for advancements in the field. The experimental setup in Ethereum, with a limited number of validator nodes, might not fully represent the complexities of larger, operational networks.
Limitation 5: Constraints of Limited Scale Simulations in Reflecting Real-World Network Dynamics	The scale of simulations in both the XRPL and Ethereum use cases, including the number of transactions and nodes, is limited to manageable levels. This may not fully reflect the dynamics and scalability challenges of larger real-world networks. This aspect underlines the need for future iterations of the RBBF to incorporate a wider range of network conditions for enhanced reliability and applicability.

However, these limitations as discussed in Section 7.6 present opportunities for future research. They underline areas where the RBBF can be expanded and adapted to a broader range of blockchain environments.

7.6 Future Research Work

The limitations identified in the previous section open numerous avenues for future research to enhance the understanding and applicability of the BBF.

Applying the BBF to a broader range of blockchain protocols would provide more diverse data for validation and refinement. This approach not only enriches the understanding of different blockchain protocols' performance and characteristics but also tests the revised BBF's adaptability. For instance, extending the empirical evaluation to encompass a wider variety of

Byzantine faults, especially in the context of the XRPL client, could offer a more comprehensive picture of its robustness. Similarly, replicating experiments on public Ethereum networks or larger private networks would give a clearer understanding of Ethereum's performance under various conditions.

Considering the dynamic and rapidly evolving nature of blockchain protocols, regular updates and revisions to the revised BBF will be necessary. Monitoring developments in the blockchain space and assessing their implications for the BBF is crucial. This could involve incorporating new benchmarking tests or modifying existing ones to account for new features, improvements, or trends in blockchain technology. Exploring the integration of machine learning techniques within the BBF to predict and mitigate Byzantine faults in real-time, based on empirical data, could be another promising area of exploration.

Future research could also explore the impact of external factors, such as regulatory changes or economic conditions, on blockchain performance. This involves broadening the scope of the BBF to include these contextual factors for a more comprehensive understanding of blockchain performance.

Additionally, increasing the complexity and scale of experiments, such as testing with a greater number of nodes or different node configurations, would provide insights into scalability and fault tolerance capabilities of different blockchain protocols. This is particularly relevant for understanding the resilience of Ethereum and other blockchain platforms to various adversarial conditions.

Moreover, the integration with other blockchain clients for comparative studies would enhance the understanding of performance differences across various blockchain technologies. This aligns with the need to adapt and refine the BBF for a wider array of blockchain protocols, considering the distinct needs of various blockchain architectures and their consensus algorithms.

Lastly, alternative research strategies or methodologies, such as longitudinal design or mixed-methods approaches, could be explored to address the limitations of the experimental strategy

used in this study. These methods could combine quantitative benchmarking with qualitative analysis for a more holistic understanding of different blockchain protocols.

In conclusion, while notable progress has been achieved in developing benchmarking tools for blockchain protocols, there continues to be room for further refinement and exploration in the evolving and dynamic field of blockchain. The BBF, with its modular architecture, is well-positioned to adapt and evolve in response to these future research directions.

Appendix I: Blockchain Glossary

51% Attack: A 51% attack refers to a situation in which a single entity or group gains control of more than 50% of the computing power in a cryptocurrency network. This majority control can enable the entity to manipulate the network by issuing conflicting transactions or attempting to harm its integrity and security.

Address: In the context of cryptocurrencies, an address is a unique identifier used for sending and receiving transactions on the blockchain protocol. It is typically represented as a string of alphanumeric characters and serves as a destination or source for digital assets.

ASIC: Short for 'Application Specific Integrated Circuit,' an ASIC is a specialized hardware device designed for a specific purpose, such as cryptocurrency mining. ASICs are often employed in mining operations due to their efficiency and significant power savings compared to general-purpose hardware like GPUs.

Bitcoin: Bitcoin, the pioneering decentralized cryptocurrency, operates on a global peer-to-peer network without the need for intermediaries or a central issuing authority. It was the first cryptocurrency to gain widespread adoption and remains the most well-known and widely used digital currency.

Block: A block is a package of data containing a set of transactions that are permanently recorded on the blockchain. Each block is linked to the previous block, forming a chain of blocks that serves as a secure and immutable ledger of all the transactions within a cryptocurrency network.

Blockchain: A blockchain is a distributed and decentralized ledger that maintains a record of all transactions ever executed on a network. It consists of a chain of blocks, with each block containing a collection of validated transactions. The blockchain's design ensures transparency, security, and immutability, making it suitable for various applications beyond cryptocurrencies.

Block Explorer: A block explorer is an online tool that allows users to browse and view information about transactions, blocks, and addresses on a blockchain. It provides a transparent and comprehensive overview of the blockchain's activity, including details such as transaction histories, network hash rate, and transaction growth.

Block Height: Block height refers to the number of blocks that have been successfully added to the blockchain from its genesis block. It represents the chronological order of blocks in the blockchain, with each new block incrementing the block height by one.

Block Reward: A block reward is an incentive provided to miners who successfully validate and add a new block to the blockchain through the process of mining. Miners are rewarded with a certain number of newly created cryptocurrency tokens, which are generated as part of the consensus mechanism and transaction verification process.

Central Ledger: A central ledger is a traditional form of ledger maintained and controlled by a central authority or agency. Unlike distributed ledgers used in blockchain systems, central ledgers are centralized and require trust in the controlling entity.

Confirmation: Confirmation refers to the successful act of hashing a transaction and adding it to the blockchain. Once a transaction receives multiple confirmations (i.e., being included in subsequent blocks), it becomes increasingly secure and less prone to being reversed or altered.

Consensus: Consensus is the collective agreement among participants in a blockchain protocol regarding the validity of transactions and the state of the ledger. Consensus mechanisms ensure that all copies of the blockchain are synchronized, and that the ledger's integrity is maintained.

Cryptocurrency: Cryptocurrencies, also known as tokens, are digital representations of assets that utilize cryptographic techniques to secure transactions and control the creation of new units. Cryptocurrencies operate on decentralized networks and are typically not controlled by any central authority.

Cryptographic Hash Function: A cryptographic hash function is a mathematical algorithm that takes an input (such as transaction data) and produces a fixed-size and unique output (the

hash value). Cryptographic hashes are used in blockchain systems for various purposes, including transaction verification and data integrity.

Dapp: A decentralized application (Dapp) is an application that operates on a blockchain or distributed ledger system. Dapps are open-source, autonomous, and often incentivized through cryptographic tokens. They leverage the blockchain's transparency, security, and immutability to provide innovative solutions in areas such as finance, gaming, and decentralized governance.

DAO: Decentralized Autonomous Organizations (DAOs) are organizations or entities that function without centralized control or human intervention. DAOs operate based on pre-defined business rules encoded on the blockchain, allowing for transparent and trustless decision-making and governance processes.

Distributed Ledger: A distributed ledger is a type of ledger where data are stored across a network of decentralized nodes. Unlike centralized ledgers, distributed ledgers are not controlled by a single entity and often utilize CAs to ensure data consistency and integrity. Distributed ledgers can be both permissioned (restricted access) or permissionless (open to all participants).

Distributed Network: A distributed network refers to a network architecture where processing power, data storage, and decision-making authority are distributed across multiple nodes instead of being concentrated in a central data center. Distributed networks offer enhanced resilience, scalability, and fault tolerance compared to centralized systems.

Difficulty: Difficulty in blockchain mining refers to the level of computational effort required to successfully mine a new block on the blockchain. The difficulty is adjusted dynamically to ensure that blocks are added at a consistent rate, maintaining the blockchain's security and stability.

Digital Signature: A digital signature is a cryptographic code generated using public key encryption. It is attached to an electronically transmitted document to verify the document's contents and the identity of the sender. Digital signatures provide authentication, integrity, and non-repudiation for digital transactions.

Double-Spending: Double-spending occurs when a digital asset, such as a cryptocurrency, is spent more than once, resulting in a loss of transactional integrity and potential fraud. Blockchain technology prevents double spending by ensuring that transactions are recorded and verified in a transparent and immutable manner.

Ethereum: Ethereum is a blockchain-based platform designed to support the development and execution of decentralized applications (Dapps) and smart contracts. It aims to address limitations associated with censorship, fraud, and third-party interference by providing a programmable blockchain infrastructure.

EVM: The Ethereum Virtual Machine (EVM) is a Turing complete virtual machine that enables the execution of smart contracts on the Ethereum blockchain. The EVM ensures consistency and consensus across the Ethereum network by executing bytecode instructions.

Fork: In the context of blockchain, a fork occurs when a blockchain splits into two separate paths, resulting in two distinct versions of the blockchain running simultaneously. Forks can be temporary or permanent, and they may occur due to protocol upgrades, consensus rule changes, or disagreements among network participants.

Genesis Block: The genesis block is the first block in a blockchain. It serves as the foundation for subsequent blocks and contains unique information that distinguishes it from other blocks in the chain.

Hard Fork: A hard fork is a type of blockchain fork that introduces changes to the protocol, rendering previously invalid transactions valid and vice versa. Upgrading to the latest version of the protocol software is typically required for all nodes and users to participate in the forked blockchain.

Hash: Hashing refers to the process of applying a cryptographic hash function to input data, resulting in a fixed-size output (the hash). Hashes are commonly used in blockchain systems for transaction verification, block integrity, and data storage purposes.

Hash Rate: Hash rate is a measurement of the computational power expended by mining hardware in a blockchain protocol. It quantifies the number of hash calculations performed per second and serves as an indicator of mining efficiency and network security.

Hybrid PoS/PoW: A hybrid Proof of Stake/Proof of Work (PoS/PoW) consensus mechanism combines elements of both PoS and PoW algorithms. This hybrid approach aims to strike a balance between the influence of miners (work-based) and stakeholders (stake-based) in the governance and consensus of the blockchain protocol.

Mining: Mining is the process of validating and adding new transactions to the blockchain. Miners utilize computational power to solve complex mathematical problems, and in return, they are rewarded with cryptocurrency tokens for their contributions to securing the network and maintaining transactional integrity.

Multi-Signature: Multi-signature, or multi-sig, addresses require multiple cryptographic signatures (from different parties or private keys) to authorize a transaction. Multi-signature technology enhances security and prevents unauthorized access to funds by introducing additional layers of verification and approval.

Node: In a blockchain protocol, a node refers to a computer or device that maintains a copy of the blockchain's ledger and participates in the network's consensus process. Nodes are responsible for validating transactions, storing data, and relaying information to other nodes, ensuring the integrity and decentralization of the blockchain.

Oracles: Oracles are systems or services that provide real-world data to smart contracts on the blockchain. They act as bridges between the blockchain and external sources of information, enabling the execution of smart contracts based on real-time or off-chain data.

Peer to Peer: Peer-to-peer (P2P) refers to a decentralized interaction model where participants in a network interact directly with each other without the need for intermediaries or central authorities. P2P networks enable direct communication, data sharing, and resource exchange among peers, fostering decentralization and resilience.

Public Address: A public address is a cryptographic hash of a public key in a cryptocurrency system. It serves as a public identifier or destination for receiving funds and can be shared openly. Public addresses are used to send transactions to specific recipients on the blockchain.

Private Key: A private key is a confidential and securely stored piece of information that enables access to the tokens or assets associated with a specific address or wallet. Private keys are used to sign transactions and prove ownership, and they must be kept secret and protected to maintain the security of digital assets.

Proof of Stake: PoS is a consensus distribution algorithm in which the probability of creating or validating new blocks is based on the stake (ownership or holding) of a participant in the network. The more tokens a participant holds, the more likely they are to be chosen to create the next block and earn rewards.

Proof of Work: PoW is a consensus distribution algorithm in which participants (miners) must perform computational work, often involving high computational power and electricity consumption, to validate transactions and create new blocks. The difficulty of the work ensures security and prevents malicious actors from manipulating the blockchain.

Scrypt: Scrypt is a cryptographic algorithm commonly used in cryptocurrencies like Litecoin. Compared to the SHA-256 algorithm, Scrypt is designed to be computationally faster and consume less processing time, making it more suitable for certain mining operations.

SHA-256: SHA-256 (Secure Hash Algorithm 256-bit) is a cryptographic hash function used by several cryptocurrencies, including Bitcoin. It produces a fixed-size hash value and is known for its computational complexity, requiring significant processing power and time to compute, ensuring the security and integrity of blockchain transactions.

Smart Contracts: Smart contracts are self-executing agreements encoded as computer programs deployed on the blockchain. They automatically enforce the terms and conditions defined within them, eliminating the need for intermediaries and enabling trustless and transparent interactions. Smart contracts facilitate automated and secure transactions, reducing costs and increasing efficiency in various industries.

Solidity: Solidity is a programming language specifically designed for developing smart contracts on the Ethereum platform. It provides developers with a syntax and framework to write secure and reliable smart contracts that can be executed on the Ethereum Virtual Machine (EVM).

Testnet: A testnet is a separate blockchain protocol specifically created for developers to test and experiment with new features, applications, or upgrades without using real assets or affecting the main blockchain. Testnets allow developers to identify and resolve issues before deploying their applications on the live network.

Transaction Block: A transaction block is a collection of individual transactions that are bundled together and added to the blockchain as a single unit. Blocks are formed through the mining process, and once added to the blockchain, they are permanently recorded and become part of the immutable transaction history.

Transaction Fee: A transaction fee is a small amount of cryptocurrency paid by the sender of a transaction to incentivize miners to include the transaction in a block and prioritize its validation. Transaction fees contribute to network security and serve as a reward for miners who dedicate computational resources to process and verify transactions.

Turing Complete: Turing complete refers to a system or programming language's ability to perform any computation that a universal Turing machine can execute. In the context of blockchain, Turing complete languages like Solidity enable the development of complex and programmable smart contracts capable of executing a wide range of computations and logic.

Wallet: A wallet in the context of blockchain is a software application or device that stores private keys and enables users to manage their digital assets, such as cryptocurrencies. Wallets provide a user-friendly interface for securely sending, receiving, and storing digital tokens, and they may support multiple blockchain protocols and assets.

Scalability: Scalability refers to a blockchain system's ability to handle increasing transaction volumes and growing network demands without compromising performance, speed, or decentralization. Scalable blockchain solutions aim to optimize consensus mechanisms,

network infrastructure, and protocols to support a higher throughput and accommodate a larger user base.

Security: In the context of blockchain, security encompasses various measures and techniques employed to protect the network, user data, and digital assets from unauthorized access, manipulation, or attacks. These include cryptographic algorithms, private key management, consensus mechanisms, secure coding practices, and robust network infrastructure. Ensuring security is crucial for maintaining trust and integrity in blockchain ecosystems.

Appendix II: Systematic Literature Review Results

Publication Year	Authors	Title	URL
2019	Faria, Carlos; Correia, Miguel	BlockSim: Blockchain simulator	https://doi.org/10.1109/Blockchain.2019.00067
2019	Chaudhry, Natalia; Yousaf, Muhammad Murtaza	Consensus Algorithms in Blockchain: Comparative Analysis, Challenges and Opportunities	https://doi.org/10.1109/ICOSST.2018.8632190
2018	Zoican, Sorin; Zoican, Roxana; Vochin, Marius; Galatchi, Dan	Blockchain and Consensus Algorithms in Internet of Things	https://doi.org/10.1109/ISETC.2018.8583923
2020	Gupta, Suyash; Hellings, Jelle; Rahnama, Sajjad; Sadoghi, Mohammad	Blockchain consensus unraveled: Virtues and limitations	https://doi.org/10.1145/3401025.3404099
2019	Song, Anping; Wang, Jing; Yu, Wenjing; Dai, Yi; Zhu, Hongtao	Fast, dynamic and robust Byzantine fault tolerance protocol for consortium blockchain	https://doi.org/10.1109/ISPA-BDCloud-SustainCom-SocialCom48970.2019.00067

2019	Li, Lei; Jiang, Yongkang; Liu, Guanfeng	Consensus with voting theory in blockchain environments	https://doi.org/10.1109/ICBK.2019.00028
2018	Tosh, Deepak; Shetty, Sachin; Foytik, Peter; Kamhoua, Charles; Njilla, Laurent	CloudPoS: A Proof-of-Stake Consensus Design for Blockchain Integrated Cloud	https://doi.org/10.1109/CLOUD.2018.00045
2018	Androulaki, Elli; Barger, Artem; Bortnikov, Vita; Muralidharan, Srinivasan; Cachin, Christian; Christidis, Konstantinos; De Caro, Angelo; Enyeart, David; Murthy, Chet; Ferris, Christopher; Laventman, Gennady; Manevich, Yacov; Nguyen, Binh; Sethi, Manish; Singh, Gari; Smith, Keith; Sorniotti, Alessandro; Stathakopoulou, Chrysoula; Vukolić, Marko; Cocco, Sharon Weed; Yellick, Jason	Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains	https://doi.org/10.1145/3190508.3190538

2021	Burmaka, Ivan; Stoianov, Nikolai; Lytvynov, Vitalii; Dorosh, Mariia; Lytvyn, Svitlana	Proof of stake for blockchain based distributed intrusion detecting system	http://link.springer.com/10.1007/978-3-030-58124-4_23
2020	Li, Wenzheng; He, Mingsheng	Comparative Analysis of Bitcoin, Ethereum, and Libra	https://ieeexplore.ieee.org/document/9237710/
2020	MihaljeviÄ‡, Miodrag J	A Blockchain Consensus Protocol Based on Dedicated Time-Memory-Data Trade-Off	https://ieeexplore.ieee.org/document/9152814/
2019	Yang, Fan; Zhou, Wei; Wu, Qingqing; Long, Rui; Xiong, Neal N.; Zhou, Meiqi	Delegated proof of stake with downgrade: A secure and efficient blockchain consensus algorithm with downgrade mechanism	https://doi.org/10.1109/ACCESS.2019.2935149
2019	Zhang, Gengrui; Xu, Chengzhong	An Efficient Consensus Protocol for Real-Time Permissioned Blockchains Under Non-Byzantine Conditions	http://link.springer.com/10.1007/978-3-030-15093-8_21
2019	Li, Yinsheng	Emerging blockchain-based applications and techniques	http://link.springer.com/10.1007/s11761-019-00281-x

2019	Puthal, Deepak; Mohanty, Saraju P.; Nanda, Priyadarsi; Kougianos, Elias; Das, Gautam	Proof-of-Authentication for Scalable Blockchain in Resource-Constrained Distributed Systems	https://doi.org/10.1109/ICCE.2019.8662009
2021	Ferdous, Md Sadek; Chowdhury, Mohammad Jabed Morshed; Hoque, Mohammad A	A survey of consensus algorithms in public blockchain systems for crypto-currencies	https://www.sciencedirect.com/science/article/pii/S1084804521000618
2020	Misic, Jelena; Misic, Vojislav B.; Chang, Xiaolin; Qushtom, Haytham	PBFT-based ordering service for IoT domains	https://ieeexplore.ieee.org/document/9348646/
2019	Li, Ruidong; Asaeda, Hitoshi	DIBN: A decentralized information-centric blockchain protocol	https://doi.org/10.1109/GLOBECOM38437.2019.9013622
2020	Wang, Hui; Tan, Wenan	Block proposer election method based on verifiable random function in consensus mechanism	https://ieeexplore.ieee.org/document/9350766/
2019	Akhtar, Zuhaib	From Blockchain to Hashgraph: Distributed Ledger Technologies in the Wild	https://doi.org/10.1109/UPCON47278.2019.8980029

2020	Zhu, Zhiqin; Qi, Guanqiu; Zheng, Mingyao; Sun, Jian; Chai, Yi	Blockchain based consensus checking in decentralized cloud storage	https://www.sciencedirect.com/science/article/pii/S1569190X19301200
2020	Bodkhe, Umesh; Mehta, Dhyey; Tanwar, Sudeep; Bhattacharya, Pronaya; Singh, Pradeep Kumar; Hong, Wei Chiang	A survey on decentralized consensus mechanisms for cyber physical systems	https://doi.org/10.1109/ACCESS.2020.2981415
2018	Cho, Hyungmin	ASIC-Resistance of Multi-Hash Proof-of-Work Mechanisms for Blockchain Consensus Protocols	https://doi.org/10.1109/ACCESS.2018.2878895
2020	EmeÃ\S, Murat; Karatay, Melike; DalkÄ±lÄ±Ã\S, GÃ\Pkhan; AlkÄ±m, Erdem	Consensus Approaches of High-Value Crypto Currencies and Application in SHA-3	http://link.springer.com/10.1007/978-3-030-36178-5_46
2021	Mythili, R.; Venkataraman, Revathi	Proof of policy (PoP): A new attribute-based blockchain consensus protocol	http://link.springer.com/10.1007/978-981-15-6876-3_35
2020	Lv, Sai; Li, Hui; Wang, Han; Wang, Xiangui	CoT: A Secure Consensus of Trust with Delegation Mechanism in Blockchains	http://link.springer.com/10.1007/978-981-15-3278-8_7

2018	Guo, Hong; Zheng, Hongqiang; Xu, Kai; Kong, Xiangrui; Liu, Jing; Liu, Fang; Gai, Keke	An improved consensus mechanism for blockchain	http://link.springer.com/10.1007/978-3-030-05764-0_14
2018	Cong, Kelong; Ren, Zhijie; Pouwelse, Johan	A Blockchain Consensus Protocol with Horizontal Scalability	https://doi.org/10.23919/IFIPNetworking.2018.8696555
2019	Zhang, Qichao; Qi, Zhuyun; Liu, Xiaoyou; Sun, Tao; Lei, Kai	Research and Application of BFT Algorithms Based on the Hybrid Fault Model	https://doi.org/10.1109/HOTICN.2018.8606021
2020	Qiu, Zheng; Hao, Jianjun; Guo, Yijun; Zhang, Yi	Dual Vote Confirmation based Consensus Design for Blockchain integrated IoT	https://ieeexplore.ieee.org/document/9110335/
2020	Wen, Yujuan; Lu, Fengyuan; Liu, Yufei; Cong, Peijin; Huang, Xinli	Blockchain Consensus Mechanisms and Their Applications in IoT: A Literature Survey	http://link.springer.com/10.1007/978-3-030-60248-2_38
2019	Sharma, Kapil; Jain, Deepakshi	Consensus Algorithms in Blockchain Technology: A Survey	https://doi.org/10.1109/ICCCNT45670.2019.8944509
2019	Gupta, Suyash; Hellings, Jelle; Rahnama, Sajjad; Sadoghi, Mohammad	An in-depth look of BFT consensus in blockchain: Challenges and opportunities	https://doi.org/10.1145/3366625.3369437

2020	Honnavalli, Prasad B.; Cholin, Ajaykumar S.; Pai, Athul; Anekal, Achuta D.; Anekal, Aditya D.	A study on recent trends of consensus algorithms for private blockchain protocol	http://link.springer.com/10.1007/978-3-030-52535-4_4
2019	Dai, Weiqi; Xiao, Deshan; Jin, Hai; Xie, Xia	A Concurrent optimization consensus system based on blockchain	https://doi.org/10.1109/ICT.2019.8798836
2019	Kumar, Harshitha U.; Prasad, Raghavendra	Algorand: A Better Distributed Ledger	https://doi.org/10.1109/ICAIT47043.2019.8987305
2020	Oh, Myoungwon; Ha, Sujin; Yoon, Jin Hyuk; Lee, Kang Won; Son, Yongseok; Yeom, Heon Young	Graph Learning BFT: A Design of Consensus System for Distributed Ledgers	https://ieeexplore.ieee.org/document/9184895/
2021	Santiago, Carlos; Ren, Shuyang; Lee, Choonhwa; Ryu, Minsoo	Concordia: A streamlined consensus protocol for blockchain protocols	https://ieeexplore.ieee.org/document/9324848/
2020	Biswas, Sujit; Sharif, Kashif; Li, Fan; Maharjan, Sabita; Mohanty, Saraju P.; Wang, Yu	PoBT: A Lightweight Consensus Algorithm for Scalable IoT Business Blockchain	https://doi.org/10.1109/JIOT.2019.2958077

2021	Mizrahi, Avi; Koren, Noam; Rottenstreich, Ori	Optimizing Merkle Proof Size for Blockchain Transactions	https://ieeexplore.ieee.org/document/9352820/
2019	Kim, Dong Hak; Ullah, Rehmat; Kim, Byung Seo	RSP Consensus Algorithm for Blockchain	https://doi.org/10.23919/APNOMS.2019.8893063
2019	Luo, Yinghui; Deng, Xiaoshi; Wu, Yilin; Wang, Junhuan	MPC-DPOS: An efficient consensus algorithm based on secure multi-party computation	https://doi.org/10.1145/3376044.3376061
2021	Fu, Wei; Wei, Xuefeng; Tong, Shihua	An Improved Blockchain Consensus Algorithm Based on Raft	http://link.springer.com/10.1007/s13369-021-05427-8
2020	Altarawneh, Amani; Skjellum, Anthony	The security ingredients for correct and Byzantine fault-tolerant blockchain consensus algorithms	https://ieeexplore.ieee.org/document/9297326/
2019	Kashyap, R.; Arora, K.; Sharma, M.; Aazam, A.	Security-aware GA based practical byzantine fault tolerance for permissioned blockchain	https://doi.org/10.1109/CRC.2019.00041
2021	Khamar, Jalpa; Patel, Hiren	An Extensive Survey on Consensus Mechanisms for Blockchain Technology	http://link.springer.com/10.1007/978-981-15-4474-3_40

2021	Bouraga, Sarah	A taxonomy of blockchain consensus protocols: A survey and classification framework	https://www.sciencedirect.com/science/article/pii/S0957417420310587
2018	Jalalzai, Mohammad M.; Busch, Costas	Window Based BFT Blockchain Consensus	https://doi.org/10.1109/Cybermatics_2018.2018.00184
2021	Katarya, Rahul; Vats, Vinay Kumar	A Survey on Blockchain Technologies and Its Consensus Algorithms	http://link.springer.com/10.1007/978-981-15-8297-4_59
2019	Tong, Wei; Dong, Xuewen; Zheng, Jiawei	Trust-PBFT: A peertrust-based practical byzantine consensus algorithm	https://doi.org/10.1109/NaNA.2019.00066
2019	Perez, Maria Rona L.; Lagman, Ace C.; Legaspi, John Benedict C.; De Angel, Roman De M.; Awat, Kirk Alvin S.	Suitability of IoT to Blockchain protocol based on Consensus Algorithm	https://doi.org/10.1109/HNICEM48295.2019.9072857
2019	Alsunaidi, Shikah J.; Alhaidari, Fahd A.	A survey of consensus algorithms for blockchain technology	https://doi.org/10.1109/ICCISci.2019.8716424

2019	Yang, Jian; Shen, Hong	Blockchain consensus algorithm design based on consistent hash algorithm	https://doi.org/10.1109/PDCAT46702.2019.00090
2019	Lei, Kai; Zhang, Qichao; Xu, Limei; Qi, Zhuyun	Reputation-Based Byzantine Fault-Tolerance for Consortium Blockchain	https://doi.org/10.1109/PADSW.2018.8644933
2019	Wang, Haiyong; Guo, Kaixuan	Byzantine fault tolerant algorithm based on vote	https://doi.org/10.1109/CyberC.2019.00041
2020	Gorenflo, Christian; Golab, Lukasz; Keshav, Srinivasan	XOX Fabric: A hybrid approach to blockchain transaction execution	https://ieeexplore.ieee.org/document/9169478/
2019	Pahlajani, Sunny; Kshirsagar, Avinash; Pachghare, Vinod	Survey on Private Blockchain Consensus Algorithms	https://doi.org/10.1109/ICIICT1.2019.8741353
2019	França, Bruno; Wissfeld, Marvin; Berrang, Pascal; von Styp-Rekowsky, Philipp	Albatross An optimistic consensus algorithm	https://arxiv.org/abs/1903.01589
2019	Wang, Gang; Shi, Zhijie Jerry; Nixon, Mark; Han, Song	Sok: Sharding on blockchain	https://doi.org/10.1145/3318041.3355457

2020	Aswin, A. V.; Kuriakose, Bineeth	An Analogical Study of Hyperledger Fabric and Ethereum	http://link.springer.com/10.1007/978-3-030-28364-3_41
2019	Zhong, Lin; Duan, Xihua; Wang, Yujue; Chen, Jingyan; Liu, Jidong; Wang, Xiaoguang	ERoc: A distributed blockchain system with fast consensus	https://doi.org/10.1109/CyberC.2019.00043
2020	Tan, Chao; Xiong, Liang	DPoSB: Delegated Proof of Stake with node's behavior and Borda Count	https://ieeexplore.ieee.org/document/9141744/
2019	Gorenflo, Christian; Lee, Stephen; Golab, Lukasz; Keshav, Srinivasan	FastFabric: Scaling Hyperledger Fabric to 20,000 Transactions per Second	https://doi.org/10.1109/BLOC.2019.8751452
2018	Jiang, Zhiyuan; Krishnamachari, Bhaskar; Zhou, Sheng; Niu, Zhisheng	SENATE: A permissionless byzantine consensus protocol in wireless networks	https://ieeexplore.ieee.org/abstract/document/9003220
2019	Chao, Tzu Wei; Chung, Hao; Kuo, Po Chun	Fair byzantine agreements for blockchains	https://arxiv.org/abs/1907.03437#:~:text=Byzantine%20general%20problem%20is%20the,the%20security%20of%20the%20blockchain.

2020	Sharma, Deepak Kumar; Pant, Shrid; Sharma, Mehul; Brahmachari, Shikha	Cryptocurrency Mechanisms for Blockchains: Models, Characteristics, Challenges, and Applications	http://www.sciencedirect.com/science/article/pii/B9780128198162000137
2020	Kim, Soohyeong; Lee, Sejong; Jeong, Chiyoung; Cho, Sunghyun	Byzantine fault tolerance based multi-block consensus Algorithm for throughput scalability	https://doi.org/10.1109/ICEIC49074.2020.9051279
2018	Gemeliarana, I. Gusti Ayu Kusdiah; Sari, Riri Fitri	Evaluation of proof of work (POW) blockchains security network on selfish mining	https://doi.org/10.1109/ISRITI.2018.8864381
2019	Medellin, John M.; Thornton, Mitchell A.	A Discussion on Blockchain Software Quality Attribute Design and Tradeoffs	http://link.springer.com/10.1007/978-3-030-23943-5_2
2018	Berger, Christian; Reiser, Hans P.	Scaling Byzantine consensus: A broad analysis	https://doi.org/10.1145/3284764.3284767
2019	Eklund, Peter W.; Beck, Roman	Factors that impact blockchain scalability	https://doi.org/10.1145/3297662.3365818

2020	Fan, Caixiang; Ghaemi, Sara; Khazaei, Hamzeh; Musilek, Petr	Performance Evaluation of Blockchain Systems: A Systematic Survey	https://ieeexplore.ieee.org/document/9129732/
2020	Zhang, Shuangfeng; Liu, Yuan; Chen, Xingren	BIT Problem: Is There a Trade-off in the Performances of Blockchain Systems?	http://link.springer.com/10.1007/978-981-15-2777-7_11
2019	Kwon, Minsu; Yu, Heonchang	Performance Improvement of Ordering and Endorsement Phase in Hyperledger Fabric	https://doi.org/10.1109/IOTSMS48152.2019.8939202
2018	Huang, Dongyan; Ma, Xiaoli; Zhang, Shengli	Performance analysis of the raft consensus algorithm for private blockchains	https://ieeexplore.ieee.org/document/8666147
2019	Aljassas, Hamad Mousa A.; Sasi, Sreela	Performance Evaluation of Proof-of-Work and Collatz Conjecture Consensus Algorithms	https://doi.org/10.1109/CAIS.2019.8769514
2018	Jiang, Yanjun; Ding, Siye	A high performance consensus algorithm for consortium blockchain	https://doi.org/10.1109/CompComm.2018.8781067

2019	Wang, Shuo	Performance Evaluation of Hyperledger Fabric with Malicious Behavior	http://link.springer.com/10.1007/978-3-030-23404-1_15
2020	Supreet, Y.; Vasudev, P.; Pavitra, H.; Naravani, Mouna; Narayan, D. G.	Performance Evaluation of Consensus Algorithms in Private Blockchain protocols	https://ieeexplore.ieee.org/document/9213019/
2020	Bamakan, Seyed Mojtaba Hosseini; Motavali, Amirhossein; Babaei Bondarti, Alireza	A survey of blockchain consensus algorithms performance evaluation criteria	http://www.sciencedirect.com/science/article/pii/S0957417420302098
2018	Hao, Yue; Li, Yi; Dong, Xinghua; Fang, Li; Chen, Ping	Performance Analysis of Consensus Algorithm in Private Blockchain	https://doi.org/10.1109/IVS.2018.8500557
2019	Krieger, Udo R.; Ziegler, Michael H.; Cech, Hendrik L.	Performance Modeling of the Consensus Mechanism in a Permissioned Blockchain	http://link.springer.com/10.1007/978-3-030-21952-9_1
2020	Yang, Chengfu	Research on Autonomous and Controllable High-performance Consensus Mechanism of Blockchain	https://ieeexplore.ieee.org/document/9213550/

2019	Sani, Abubakar Sadiq; Yuan, Dong; Bao, Wei; Yeoh, Phee Lep; Dong, Zhao Yang; Vucetic, Branka; Bertino, Elisa	Xyreum: A high-performance and scalable blockchain for iiot security and privacy	https://doi.org/10.1109/ICDCS.2019.00190
2019	Ismail, Leila; Hameed, Heba; Aishamsi, Mahra; Aihammadi, Manayer; Aidhanhani, Noura	Towards a blockchain deployment at UAE University: Performance evaluation and blockchain taxonomy	https://doi.org/10.1145/3320154.3320156
2021	Kim, Donghee; Doh, Inshil; Chae, Kijoon	Improved Raft Algorithm exploiting Federated Learning for Private Blockchain performance enhancement	https://ieeexplore.ieee.org/document/9333932/
2020	Tang, Changbing; Wu, Luya; Wen, Guanghui; Zheng, Zhonglong	Incentivizing Honest Mining in Blockchain protocols: A Reputation Approach	https://doi.org/10.1109/TCSII.2019.2901746
2019	Lunardi, Roben C.; Michelin, Regio A.; Neu, Charles V.; Nunes, Henry C.; Zorzo, Avelino F.; Kanhere, Salil S.	Impact of consensus on appendable-block blockchain for IoT	https://doi.org/10.1145/3360774.3360798

2021	Qian, Li Ping; Wu, Yuan; Xu, Xu; Ji, Bo; Shi, Zhiguo; Jia, Weijia	Distributed Charging-Record Management for Electric Vehicle Networks via Blockchain	https://ieeexplore.ieee.org/document/9208796/
2020	Sun, Gang; Dai, Miao; Sun, Jian; Yu, Hongfang	Voting-based Decentralized Consensus Design for Improving the Efficiency and Security of Consortium Blockchain	https://ieeexplore.ieee.org/document/9219122/
2020	Javaid, Uzair; Aman, Muhammad Naveed; Sikdar, Biplab	A Scalable Protocol for Driving Trust Management in Internet of Vehicles with Blockchain	https://ieeexplore.ieee.org/document/9119117/
2019	Yu, Guangsheng; Wang, Xu; Zha, Xuan; Zhang, J. Andrew; Liu, Ren Ping	An Optimized Round-Robin Scheduling of Speakers for Peers-to-Peers-Based Byzantine Faulty Tolerance	https://doi.org/10.1109/GLOCOMW.2018.8644251
2020	Olivares-Rojas, Juan Carlos; Reyes-Archundia, Enrique; Gutierrez-Gnecchi, Jose A.; Cerda-Jacobo, Jaime; Gonzalez-Murueta, Johan W.	A Novel Multitier Blockchain Architecture to Protect Data in Smart Metering Systems	https://ieeexplore.ieee.org/document/8902082/

2020	Lin, Wenmin; Xu, Xiaolong; Qi, Lianyong; Zhang, Xuyun; Dou, Wanchun; Khosravi, Mohammad R	A Proof-of-Majority Consensus Protocol for Blockchain-Enabled Collaboration Infrastructure of 5G Network Slice Brokers	https://doi.org/10.1145/3384943.3409421
2020	Wang, Yong; Li, June; Zhao, Siyu; Yu, Fajiang	Hybridchain: A Novel Architecture for Confidentiality-Preserving and Performant Permissioned Blockchain Using Trusted Execution Environment	https://ieeexplore.ieee.org/document/9229085/
2019	Alskaif, Tarek; Van Leeuwen, Gijs	Decentralized Optimal Power Flow in Distribution Networks Using Blockchain	https://doi.org/10.1109/SEST.2019.8849153
2020	Yahaya, Adamu Sani; Javaid, Nadeem; Javed, Muhammad Umar; Shafiq, Muhammad; Khan, Wazir Zada; Aalsalem, Mohammed Y	Blockchain-Based Energy Trading and Load Balancing Using Contract Theory and Reputation in a Smart Community	https://ieeexplore.ieee.org/document/9276408/
2019	Devi, M. Shyamala; Suguna, R.; Abhinaya, P. M.	Integration of Blockchain and IoT in Satellite Monitoring Process	https://doi.org/10.1109/ICECCT.2019.8869185

2020	Liu, Han; Han, Dezhi; Li, Dun	Fabric-iot: A Blockchain-Based Access Control System in IoT	https://doi.org/10.1109/ACCESS.2020.2968492
2020	Lei, Kai; Fang, Junjie; Zhang, Qichao; Lou, Junjun; Du, Maoyu; Huang, Jiyue; Wang, Jianping; Xu, Kuai	Blockchain-Based Cache Poisoning Security Protection and Privacy-Aware Access Control in NDN Vehicular Edge Computing Networks	http://link.springer.com/10.1007/s10723-020-09531-1
2019	Salimitari, Mehrdad; Joneidi, Mohsen; Chatterjee, Mainak	AI-enabled blockchain: An outlier-aware consensus protocol for blockchain-based IoT networks	https://ieeexplore.ieee.org/document/9013824
2018	Li, Quan Lin; Ma, Jing Yu; Chang, Yan Xia	Blockchain queue theory	http://link.springer.com/10.1007/978-3-030-04648-4_3
2020	Uddin, Md. Ashraf; Stranieri, Andrew; Gondal, Iqbal; Balasubramanian, Venki	Blockchain leveraged decentralized IoT eHealth framework	http://www.sciencedirect.com/science/article/pii/S2542660520300020
2021	Bandara, Eranga; Tosh, Deepak; Foytik, Peter; Shetty, Sachin; Ranasinghe, Nalin; Zoysa, Kasun De	Tikiriâ€”Towards a lightweight blockchain for IoT	https://www.sciencedirect.com/science/article/pii/S0167739X21000583

2019	Wang, Qifan; Zhou, Lei; Tang, Zhe; Wang, Guojun	A consortium blockchain-based model for data sharing in internet of Vehicles	http://link.springer.com/10.1007/978-981-15-1301-5_21
2018	Kolekar, Sachin M.; More, Rahul P.; Bachal, Smita S.; Yenkikar, Anuradha V.	Review Paper on Untwist Blockchain: A Data Handling Process of Blockchain Systems	https://doi.org/10.1109/ICICET.2018.8533868
2019	Schulz, Kai Fabian; Freund, Daniel	A multichain architecture for distributed supply chain design in industry 4.0	http://link.springer.com/10.1007/978-3-030-04849-5_25
2020	Huang, Haiping; Zhu, Peng; Xiao, Fu; Sun, Xiang; Huang, Qinglong	A blockchain-based scheme for privacy-preserving and secure sharing of medical data	https://www.sciencedirect.com/science/article/pii/S0167404820302832
2020	Zhang, Ao; Bai, Xiaoying	Decentralized Authorization and Authentication Based on Consortium Blockchain	http://link.springer.com/10.1007/978-981-15-2777-7_22
2020	Doku, Ronald; Rawat, Danda B.; Garuba, Moses; Njilla, Laurent	Fusion of Named Data Networking and Blockchain for Resilient Internet-of-Battlefield-Things	https://doi.org/10.1109/CCNC46108.2020.9045395

2018	Xu, Chenhan; Wang, Kun; Xu, Guoliang; Li, Peng; Guo, Song; Luo, Jiangtao	Making Big Data Open in Collaborative Edges: A Blockchain-Based Framework with Reduced Resource Requirements	https://doi.org/10.1109/ICC.2018.8422561
2019	Guo, Shuxiang; Cao, Sheng; Guo, Jian	Study on Collaborative Algorithm for a Spherical Multi-robot System based on Micro-blockchain	https://doi.org/10.1109/ICMA.2019.8816560
2021	Ayaz, Ferheen; Sheng, Zhengguo; Tian, Daxin; Guan, Yong Liang	A Proof-of-Quality-Factor (PoQF)-Based Blockchain and Edge Computing for Vehicular Message Dissemination	https://ieeexplore.ieee.org/document/9205920/
2020	Zhao, Ning; Wu, Hao; Zhao, Xiaonan	Consortium Blockchain-Based Secure Software Defined Vehicular Network	http://link.springer.com/10.1007/s11036-019-01285-9
2020	Hu, Cong; Xu, Chang; Wang, Ping	Design and Implementation of a Blockchain Based Authentication Framework: A Case Study in the State Grid of China	http://link.springer.com/10.1007/978-981-15-2810-1_49

2019	Rai, Shishir; Hood, Kendric; Nesterenko, Mikhail; Sharma, Gokarna	And Blockguard: Adaptive Blockchain Security	http://link.springer.com/10.1007/978-3-030-34992-9_23
2020	Rasolroveicy, Mohammadreza; Fokaefs, Marios	Dynamic Reconfiguration of Consensus Protocol for IoT Data Registry on Blockchain	https://dl.acm.org/doi/abs/10.5555/3432601.3432632
2021	Liu, Qilie; Xu, Yinyi; Cao, Bin; Zhang, Lei; Peng, Mugen	Unintentional forking analysis in wireless blockchain protocols	https://www.sciencedirect.com/science/article/pii/S2352864820302923
2021	Qi, Heng; Wang, Junxiao; Li, Wenxin; Wang, Yuxin; Qiu, Tie	A Blockchain-Driven IIoT Traffic Classification Service for Edge Computing	https://ieeexplore.ieee.org/document/9247248/
2019	Paillisse, Jordi; Manrique, Jan; Bonet, Guillem; Rodriguez-Natal, Alberto; Maino, Fabio; Cabellos, Albert	Decentralized Trust in the Inter-Domain Routing Infrastructure	https://doi.org/10.1109/ACCESS.2019.2954096
2021	Meng, Tianhui; Zhao, Yubin; Wolter, Katinka; Xu, Cheng Zhong	On Consortium Blockchain Consistency: A Queueing Network Model Approach	https://ieeexplore.ieee.org/document/9316952/

2020	Hou, Mingyu; Kang, Tianyu; Guo, Li	A Blockchain Based Architecture for IoT Data Sharing Systems	https://ieeexplore.ieee.org/document/9156107/
2020	Chen, Xin; Shen, Jiachen; Cao, Zhenfu; Dong, Xiaolei	A Blockchain-Based Privacy-Preserving Scheme for Smart Grids	https://doi.org/10.1145/3390566.3391667
2019	Ghandour, Ahmed G.; Elhoseny, Mohamed; Hassanien, Aboul Ella	Blockchains for Smart Cities: A Survey	http://link.springer.com/10.1007/978-3-030-01560-2_9
2020	Afraz, Nima; Ruffini, Marco	5G network slice brokering: A distributed blockchain-based market	https://ieeexplore.ieee.org/document/9200915/
2018	Chen, Zhonglin; Chen, Shanzhi; Xu, Hui; Hu, Bo	A security authentication scheme of 5G ultra-dense network based on block chain	https://doi.org/10.1109/ACCESS.2018.2871642
2020	Mershad, Khaleel; Said, Bilal	A Blockchain Model for Secure Communications in Internet of Vehicles	https://ieeexplore.ieee.org/document/9316498/
2019	Chen, Yun; Xie, Hui; Lv, Kun; Wei, Shengjun; Hu, Changzhen	DEPLEST: A blockchain-based privacy-preserving distributed database toward user behaviors in social networks	http://www.sciencedirect.com/science/article/pii/S0020025519305250

2021	Hu, Sensen; Huang, Shan; Huang, Jing; Su, Jiafu	Blockchain and edge computing technology enabling organic agricultural supply chain: A framework solution to trust crisis	https://www.sciencedirect.com/science/article/pii/S036083522030749X
2019	Islam, Md Azharul; Madria, Sanjay	A permissioned blockchain based access control system for IOT	https://doi.org/10.1109/Blockchain.2019.00071
2020	Feng, Li Bo; Zhang, Hui; Wang, Jin Li	Intelligent Manufacturing Information Security Sharing Model Based on Blockchain	http://link.springer.com/10.1007/978-981-15-0238-5_21
2021	Lin, Peng; Song, Qingyang; Yu, F. Richard; Wang, Dan; Guo, Lei	Task Offloading for Wireless VR-Enabled Medical Treatment with Blockchain Security Using Collective Reinforcement Learning	https://ieeexplore.ieee.org/document/9321476/
2019	Xu, Li; Ma, Xuan; Xu, Lizhen	A Novel Adaptive Tuning Mechanism for Kafka-Based Ordering Service	http://link.springer.com/10.1007/978-3-030-30952-7_14
2020	Lao, Laphou; Li, Zecheng; Hou, Songlin; Xiao, Bin; Guo, Songtao; Yang, Yuanyuan	A survey of IoT applications in blockchain systems: Architecture, consensus, and traffic modeling	https://doi.org/10.1145/3372136

2020	Sun, Gang; Dai, Miao; Zhang, Feng; Yu, Hongfang; Du, Xiaojiang; Guizani, Mohsen	Blockchain-Enhanced High-Confidence Energy Sharing in Internet of Electric Vehicles	https://ieeexplore.ieee.org/document/9089235/
2019	Liu, Yaping; Zhang, Shuo; Zhu, Haojin; Wan, Peng Jun; Gao, Lixin; Zhang, Yaoxue	An enhanced verifiable inter-domain routing protocol based on blockchain	http://link.springer.com/10.1007/978-3-030-37228-6_4
2021	Fang, Tao; Wu, Dan; Chen, Jiaxin; Yue, Chao; Wang, Meng	Joint Distributed Cache and Power Control in Haptic Communications: A Potential Game Approach	https://ieeexplore.ieee.org/document/9385392/
2019	Hanggoro, Delphi; Sari, Riri Fitri	A review of lightweight blockchain technology implementation to the internet of things	https://doi.org/10.1109/R10-HTC47129.2019.9042431
2020	Kumar, S Naveen; Dakshayini, M	Secure sharing of health data using hyperledger fabric based on blockchain technology	https://ieeexplore.ieee.org/document/9203442/
2019	Zhou, Tong; Li, Xiaofeng; Zhao, He	Med-PPPHIS: Blockchain-Based Personal Healthcare Information System for National Physique	http://link.springer.com/10.1007/s10916-019-1430-2

		Monitoring and Scientific Exercise Guiding	
2021	Yang, Dana; Yoo, Seohee; Doh, Inshil; Chae, Kijoon	Selective blockchain system for secure and efficient D2D communication	https://www.sciencedirect.com/science/article/pii/S1084804520302885
2021	Misic, Jelena; Misic, Vojislav B.; Chang, Xiaolin; Qushtom, Haytham	Adapting PBFT for Use with Blockchain-Enabled IoT Systems	https://ieeexplore.ieee.org/document/9311430/
2020	Hao, Weifeng; Zeng, Jiajie; Dai, Xiaohai; Xiao, Jiang; Hua, Qiang Sheng; Chen, Hanhua; Li, Kuan Ching; Jin, Hai	Towards a Trust-Enhanced Blockchain P2P Topology for Enabling Fast and Reliable Broadcast	https://doi.org/10.1109/TNSM.2020.2980303
2019	Norta, Alex; Dai, Patrick; Mahi, Neil; Earls, Jordan	A public, blockchain-based distributed smart-contract platform enabling mobile lite wallets using a proof-of-stake consensus algorithm	http://link.springer.com/10.1007/978-3-030-04849-5_33
2018	Zhang, Aiqing; Lin, Xiaodong	Towards Secure and Privacy-Preserving Data Sharing in e-Health Systems via Consortium Blockchain	http://link.springer.com/10.1007/s10916-018-0995-5

2018	Xie, Wenlin; Zhou, Wei; Kong, Lanju; Zhang, Xiangdong; Min, Xinping; Xiao, Zongshui; Li, Qingzhong	ETTF: A Trusted Trading Framework Using Blockchain in E-commerce	https://doi.org/10.1109/CSCWD.2018.8465233
2019	Chai, Haoye; Leng, Supeng; Zeng, Ming; Liang, Haoyang	A Hierarchical Blockchain Aided Proactive Caching Scheme for Internet of Vehicles	https://doi.org/10.1109/ICC.2019.8761482
2019	Zhu, Saide; Hu, Huafu; Li, Yingshu; Li, Wei	Hybrid blockchain design for privacy preserving crowdsourcing platform	https://doi.org/10.1109/Blockchain.2019.00013
2019	Pourheidari, Vahid; Rouhani, Sara; Deters, Ralph	A case study of execution of untrusted business process on permissioned blockchain	https://ieeexplore.ieee.org/document/8726814
2020	Heck, Kolja; Mengelkamp, Esther; Weinhardt, Christof	Blockchain-based local energy markets: Decentralized trading on single-board computers	http://link.springer.com/10.1007/s12667-020-00399-4
2020	Ma, Zhaofeng; Zhao, Weizhe; Luo, Shoushan; Wang, Lingyun	TrustedBaaS: Blockchain-Enabled Distributed and Higher-Level Trusted Platform	https://www.sciencedirect.com/science/article/pii/S1389128620312330

2020	Ferrag, Mohamed Amine; Maglaras, Leandros	DeepCoin: A Novel Deep Learning and Blockchain-Based Energy Exchange Framework for Smart Grids	https://ieeexplore.ieee.org/document/8758147/
2019	Rebello, Gabriel Antonio F.; Alvarenga, Igor D.; Sanz, Igor J.; Duarte, Otto Carlos M.B.	BSec-NFVO: A Blockchain-Based Security for Network Function Virtualization Orchestration	https://doi.org/10.1109/ICC.2019.8761651
2021	Xu, Xiaolong; Zhu, Dawei; Yang, Xiaoxian; Wang, Shuo; Qi, Lianyong; Dou, Wanchun	Concurrent Practical Byzantine Fault Tolerance for Integration of Blockchain and Supply Chain	https://doi.org/10.1145/3395331
2019	Wang, Yu; Samavi, Reza; Sood, Nitin	Blockchain-based Marketplace for Software Testing	https://doi.org/10.1109/PST47121.2019.8949025
2020	Moh, Melody; Nguyen, David; Moh, Teng Sheng; Khieu, Brian	Blockchain for efficient public key infrastructure and fault-tolerant distributed consensus	http://link.springer.com/10.1007/978-3-030-38181-3_5
2020	Yan, Bin; Chen, Pengfei; Li, Xiaoyun; Wang, Yongfeng	Nebula: A Blockchain Based Decentralized Sharing Computing Platform	http://link.springer.com/10.1007/978-981-15-2777-7_58

2019	Sturm, Christian; Scalanczi, Jonas; Schönig, Stefan; Jablonski, Stefan	A Blockchain-based and resource-aware process execution engine	http://www.sciencedirect.com/science/article/pii/S0167739X18327158
2021	Wang, Ke; Chen, Chien Ming; Liang, Zuodong; Hassan, Mohammad Mehedi; Sarné, Giuseppe M.L.; Fotia, Lidia; Fortino, Giancarlo	A trusted consensus fusion scheme for decentralized collaborated learning in massive IoT domain	https://www.sciencedirect.com/science/article/pii/S1566253521000336
2020	Sharma, Ashish; Awasthi, Yogesh; Kumar, Sunil	The Role of Blockchain, AI and IoT for Smart Road Traffic Management System	https://ieeexplore.ieee.org/document/9344533/
2020	Liu, Yinqiu; Wang, Kun; Qian, Kai; Du, Miao; Guo, Song	Tornado: Enabling Blockchain in Heterogeneous Internet of Things Through a Space-Structured Approach	https://doi.org/10.1109/JIOT.2019.2954128
2019	Lei, Kai; Zhang, Qichao; Lou, Junjun; Bai, Bo; Xu, Kuai	Securing ICN-Based UAV Ad Hoc Networks with Blockchain	https://doi.org/10.1109/MCOM.2019.1800722

2020	Tao, Yuechen; Li, Bo; Jiang, Jingjie; Ng, Hok Chu; Wang, Cong; Li, Baochun	On sharding open blockchains with smart contracts	https://ieeexplore.ieee.org/document/9101451/
2019	Yun, Jusik; Goh, Yunyeong; Chung, Jong Moon	Trust-Based Shard Distribution Scheme for Fault-Tolerant Shard Blockchain protocols	https://doi.org/10.1109/ACCESS.2019.2942003
2019	Muttavarapu, Anudeep Sai; Dantu, Ram; Thompson, Mark	Distributed Ledger for Spammers' Resume	https://doi.org/10.1109/CNS.2019.8802789
2020	Tong, Wei; Dong, Xuewen; Shen, Yulong; Zheng, Jiawei	BC-RAN: Cloud radio access network enabled by blockchain for 5G	https://www.sciencedirect.com/science/article/pii/S0140366420319071
2020	ErenoÄŸlu, Ay\AAŸe KÃ¼bra; \AAžengÃ\Pr, Ä°brahim; ErdinÃ\S, Ozan; CatalÃ\poundso, JoÃ\poundso P S	Blockchain and its application fields in both power economy and demand side management	https://www.sciencedirect.com/science/article/pii/B9780128178621000063
2019	Hao, Weifeng; Zeng, Jiajie; Dai, Xiaohai; Xiao, Jiang; Hua,	BlockP2P: Enabling Fast Blockchain Broadcast with Scalable Peer-to-Peer Network Topology	http://link.springer.com/10.1007/978-3-030-19223-5_16

	Qiangsheng; Chen, Hanhua; Li, Kuan Ching; Jin, Hai		
2021	Liao, Dan; Li, Hui; Wang, Wentao; Wang, Xiong; Zhang, Ming; Chen, Xue	Achieving IoT data security based blockchain	http://link.springer.com/10.1007/s12083-020-01042-w
2020	Zan, Chao; Xu, Hai Chuan	A Global Clock Model for the Consortium Blockchains	http://link.springer.com/10.1007/978-981-15-2777-7_6
2020	Zhong, Botao; Wu, Haitao; Ding, Lieyun; Luo, Hanbin; Luo, Ying; Pan, Xing	Hyperledger fabric-based consortium blockchain for construction quality information management	http://link.springer.com/10.1007/s42524-020-0128-y
2019	Yi, He; Wei, Fang	Research on a suitable blockchain for IoT platform	http://link.springer.com/10.1007/978-981-10-8944-2_123
2021	Surjandari, Isti; Yusuf, Harman; Laoh, Enrico; Maulida, Rayi	Designing a Permissioned Blockchain protocol for the Halal Industry using Hyperledger Fabric with multiple channels and the raft consensus mechanism	https://journalofbigdata.springeropen.com/articles/10.1186/s40537-020-00405-7

2021	Melo, Wilson S.; Tarelho, Luiz V.G.; Rodrigues, Bruno A.; Bessani, Alysson N.; Carmo, Luiz F.R.C.	Field surveillance of fuel dispensers using IoT-based metering and blockchains	https://www.sciencedirect.com/science/article/pii/S1084804520303738
2020	Ge, Chunpeng; Ma, Xinshu; Liu, Zhe	A semi-autonomous distributed blockchain-based framework for UAVs system	http://www.sciencedirect.com/science/article/pii/S1383762120300229
2020	Ding, Yepeng; Sato, Hiroyuki	Dagbase: A Decentralized Database Platform Using DAG-Based Consensus	https://ieeexplore.ieee.org/document/9202805/
2020	Dwivedi, Sanjeev Kumar; Amin, Ruhul; Vollala, Satyanarayana	Blockchain based secured information sharing protocol in supply chain management system with key distribution mechanism	https://www.sciencedirect.com/science/article/pii/S2214212620301484
2020	Zheng, Xiao; Li, Mingchu; Chen, Yuanfang; Guo, Jun; Alam, Muhammad; Hu, Weitong	Blockchain-Based Secure Computation Offloading in Vehicular Networks	https://ieeexplore.ieee.org/document/9190065/

2020	An, Jian; Cheng, Jindong; Gui, Xiaolin; Zhang, Wendong; Liang, Danwei; Gui, Ruowei; Jiang, Lin; Liao, Dong	A Lightweight Blockchain-Based Model for Data Quality Assessment in Crowdsensing	https://doi.org/10.1109/TCSS.2019.2956481
2020	Hakiri, Akram; Sellami, Bassem; Ben Yahia, Sadok; Berthou, Pascal	A Blockchain Architecture for SDN-enabled Tamper-Resistant IoT Networks	https://ieeexplore.ieee.org/document/9248492/
2019	Qiu, Xiaoyu; Liu, Luobin; Chen, Wuhui; Hong, Zicong; Zheng, Zibin	Online Deep Reinforcement Learning for Computation Offloading in Blockchain-Empowered Mobile Edge Computing	https://doi.org/10.1109/tvt.2019.2924015
2020	He, Guobiao; Su, Wei; Gao, Shuai; Yue, Jiarui	TD-Root: A trustworthy decentralized DNS root management architecture based on permissioned blockchain	http://www.sciencedirect.com/science/article/pii/S0167739X19312762
2019	Liu, Chao; Chai, Kok Keong; Zhang, Xiaoshuai; Chen, Yue	Enhanced proof-of-benefit: A secure blockchain-enabled EV charging system	https://doi.org/10.1109/VTCFall.2019.8891291

2017	Anh Dinh, Tien Tuan; Liu, Rui; Zhang, Meihui; Chen, Gang; Ooi, Beng Chin; Wang, Ji; Dinh, Tien Tuan Anh; Liu, Rui; Zhang, Meihui; Chen, Gang; Ooi, Beng Chin; Wang, Ji	Untangling blockchain: A data processing view of blockchain systems	https://doi.org/10.1109/TKDE.2017.2781227
2021	Guo, Shaoyong; Qi, Yuanyuan; Jin, Yi; Li, Wenjing; Qiu, Xuesong; Meng, Luoming	Endogenous Trusted DRL-Based Service Function Chain Orchestration for IoT	https://ieeexplore.ieee.org/document/9326381/
2020	Hao, Kun; Xin, Junchang; Wang, Zhiqiong; Wang, Guoren	Outsourced data integrity verification based on blockchain in untrusted environment	http://link.springer.com/10.1007/s11280-019-00761-2
2020	Fan, Yuqi; Zou, Jing Lin; Liu, Siyu; Yin, Qiran; Guan, Xin; Yuan, Xiaohui; Wu, Weili; Du, Dingzhu	A blockchain-based data storage framework: A rotating multiple random masters and error-correcting approach	http://link.springer.com/10.1007/s12083-020-00895-5
2019	Liu, Xikai	A New Data Sharing Scheme Based on Blockchain	https://ieeexplore.ieee.org/document/9098301/

2020	Kaci, Abdellah; Rachedi, Abderrezak	PoolCoin: Toward a distributed trust model for miners' reputation management in blockchain	https://doi.org/10.1109/CCNC46108.2020.9045608
2021	Abd-alrazaq, Alaa A; Alajlani, Mohannad; Alhuwail, Dari; Erbad, Aiman; Giannicchi, Anna; Shah, Zubair; Hamdi, Mounir; Househ, Mowafa	Blockchain technologies to mitigate COVID-19 challenges: A scoping review	https://www.sciencedirect.com/science/article/pii/S266699002030001X
2019	Chai, Haoye; Leng, Supeng; Zhang, Ke; Mao, Sun	Proof-of-Reputation Based-Consortium Blockchain for Trust Resource Sharing in Internet of Vehicles	https://doi.org/10.1109/ACCESS.2019.2956955
2019	Putra, Dwiyan Rezkia; Anggorojati, Bayu; Hartono, Ardhi Putra Pratama	Blockchain and smart-contract for scalable access control in Internet of Things	https://doi.org/10.1109/ICISS48059.2019.8969807
2020	Li, Jiangfeng; Yu, Yifan; Hu, Shili; Zhang, Chenxi	An Authority Management Framework Based on Fabric and IPFS in Traceability Systems	http://link.springer.com/10.1007/978-981-15-2777-7_63

2021	Shynu, P. G.; Menon, Varun G.; Kumar, R. Lakshmana; Kadry, Seifedine; Nam, Yunyoung	Blockchain-based Secure Healthcare Application for Diabetic-Cardio Disease Prediction in Fog Computing	https://ieeexplore.ieee.org/document/9374954/
2021	Leal, Fátima; Chis, Adriana E; González–Vélez, Horacio	Multi-service model for blockchain protocols	https://www.sciencedirect.com/science/article/pii/S0306457321000340
2020	Liu, Yaping; Zhang, Shuo; Zhu, Haojin; Wan, Peng Jun; Gao, Lixin; Zhang, Yaoxue; Tian, Zhihong	A novel routing verification approach based on blockchain for inter-domain routing in smart metropolitan area networks	http://www.sciencedirect.com/science/article/pii/S0743731519308317
2019	Shyamala Devi, M.; Suguna, R.; Joshi, Aparna Shashikant; Bagate, Rupali Amit	Design of IoT Blockchain Based Smart Agriculture for Enlightening Safety and Security	http://link.springer.com/10.1007/978-981-13-8300-7_2
2020	Buda, Su; Wu, Celimuge; Bao, Wugedele; Guleng, Siri; Zhang, Jiefang; Yau, Kok Lim Alvin; Ji, Yusheng	Empowering Blockchain in Vehicular Environments with Decentralized Edges	https://ieeexplore.ieee.org/document/9250438/

2020	He, Sen; Ren, Wei; Zhu, Tianqing; Choo, Kim Kwang Raymond	BoSMoS: A Blockchain-Based Status Monitoring System for Defending Against Unauthorized Software Updating in Industrial Internet of Things	https://doi.org/10.1109/JIOT.2019.2947339
2021	Liu, Yihan; Li, Ke; Huang, Zihao; Li, Bowen; Wang, Guiyan; Cai, Wei	EduChain: A Blockchain-Based Education Data Management System	http://link.springer.com/10.1007/978-981-33-6478-3_5
2019	Shao, Zhedan; Zhu, Xiaorong; Chikuvanyanga, Alexander M.M.; Zhu, Hongbo	Blockchain-Based SDN Security Guaranteeing Algorithm and Analysis Model	http://link.springer.com/10.1007/978-3-030-19156-6_32
2019	Huang, Jiansen; Li, Hui; Zhang, Jiyang	Blockchain Based Log System	https://doi.org/10.1109/BigData.2018.8622204
2020	Mohanty, Sachi Nandan; Ramya, K. C.; Rani, S. Sheeba; Gupta, Deepak; Shankar, K.; Lakshmanaprabu, S. K.; Khanna, Ashish	An efficient Lightweight integrated Blockchain (ELIB) model for IoT security and privacy	http://www.sciencedirect.com/science/article/pii/S0167739X19319843

2019	Grabis, Janis; Rasnacis, Arturs	Simulation Based Evaluation and Tuning of Distributed Fraud Detection Algorithm	https://doi.org/10.1109/WSC40007.2019.9004738
2019	Singh, Pranav Kumar; Singh, Roshan; Nandi, Sunit Kumar; Nandi, Sukumar	Managing smart home appliances with proof of authority and blockchain	http://link.springer.com/10.1007/978-3-030-22482-0_16
2020	Maksymyuk, Taras; Gazda, Juraj; Volosin, Marcel; Bugar, Gabriel; Horvath, Denis; Klymash, Mykhailo; Dohler, Mischa	Blockchain-Empowered Framework for Decentralized Network Management in 6G	https://ieeexplore.ieee.org/document/9214395/
2020	R, Kavya K; M, Kavitha	Military Message Passing using Consortium Blockchain Technology	https://ieeexplore.ieee.org/document/9138014/
2019	Li, Shancang; Zhao, Shanshan; Yang, Po; Andriotis, Panagiotis; Xu, Lida; Sun, Qindong	Distributed consensus algorithm for events detection in cyber-physical systems	https://doi.org/10.1109/JIOT.2019.2906157
2020	Yang, Dana; Jeon, Sol; Doh, Inshil; Chae, Kijoon	Randomly Elected Blockchain System based on Grouping Verifiers for Efficiency and Security	https://doi.org/10.23919/ICACT48636.2020.9061277

2020	Zheng, Zehui; Pan, Jianping; Cai, Lin	Lightweight Blockchain Consensus Protocols for Vehicular Social Networks	https://doi.org/10.1109/TVT.2020.2974005
2018	Nathan, Senthil; Govindarajan, Chander; Saraf, Adarsh; Sethi, Manish; Jayachandran, Praveen	Blockchain meets database: Design and implementation of a blockchain relational database	https://doi.org/10.14778/3342263.3342632
2021	Xu, Xiaoqiong; Wang, Xiaonan; Li, Zonghang; Yu, Hongfang; Sun, Gang; Maharjan, Sabita; Zhang, Yan	Mitigating Conflicting Transactions in Hyperledger Fabric Permissioned Blockchain for Delay-sensitive IoT Applications	https://ieeexplore.ieee.org/document/9317791/
2021	Latif, Shahid; Idrees, Zeba; Ahmad, Jawad; Zheng, Lirong; Zou, Zhuo	A blockchain-based architecture for secure and trustworthy operations in the industrial Internet of Things	https://www.sciencedirect.com/science/article/pii/S2452414X20300650
2020	Guha, Krishnendu; Saha, Debasri; Chakrabarti, Amlan	Blockchain Technology Enabled Pay per Use Licensing Approach for Hardware IPs	https://ieeexplore.ieee.org/document/9116526/
2019	Viriyasitavat, Wattana; Da Xu, Li; Bi, Zhuming; Sapsomboon, Assadaporn	New blockchain-based architecture for service interoperations in internet of things	https://doi.org/10.1109/TCSS.2019.2924442

2020	Kang, J; Xiong, Z; Jiang, C; Liu, Y; Guo, S; Zhang, Y; ...	Scalable and Communication-Efficient Decentralized Federated Edge Learning with Multi-blockchain Framework	https://link.springer.com/chapter/10.1007/978-981-15-9213-3_12
2021	Rouhani, Sara; Belchior, Rafael; Cruz, Rui S.; Deters, Ralph	Distributed attribute-based access control system using permissioned blockchain	http://link.springer.com/10.1007/s11280-021-00874-7
2020	Wazid, Mohammad; Das, Ashok Kumar; Shetty, Sachin; Jo, Minho	A Tutorial and Future Research for Building a Blockchain-Based Secure Communication Scheme for Internet of Intelligent Things	https://ieeexplore.ieee.org/document/9086464/
2020	Asheralieva, Alia; Niyato, Dusit	Reputation-Based Coalition Formation for Secure Self-Organized and Scalable Sharding in IoT Blockchains with Mobile-Edge Computing	https://ieeexplore.ieee.org/document/9119383/
2019	Araujo, Rodolfo Pereira Araujo; Coelho, Igor Machado; Ochi,	LibBFT: A high-performace timed automata library collection for byzantine fault tolerance	https://doi.org/10.1109/SBAC-PAD.2019.00045

	Luiz Satoru; Coelho, Vitor Nazario		
2019	Nguyen, David; Moh, Teng Sheng	Randition: Random Blockchain Partitioning for Write Throughput	https://ieeexplore.ieee.org/document/9188068/
2019	Laube, Alexandre; Martin, Steven; Al Agha, Khaldoun	A solution to the split merge problem for blockchain-based applications in ad hoc networks	https://doi.org/10.23919/PEMWN47208.2019.8986959
2020	Han, Runchao; Shapiro, Gary; Gramoli, Vincent; Xu, Xiwei	On the performance of distributed ledgers for Internet of Things	https://www.sciencedirect.com/science/article/pii/S2542660518300416
2019	Cook, Victor; Painter, Zachary; Peterson, Christina; Dechev, Damian	Read-uncommitted transactions for smart contract performance	https://arxiv.org/abs/1905.12351
2019	Sun, Yao; Zhang, Lei; Feng, Gang; Yang, Bowen; Cao, Bin; Imran, Muhammad Ali	Blockchain-enabled wireless internet of things: Performance analysis and optimal communication node deployment	https://doi.org/10.1109/JIOT.2019.2905743
2020	Li, Xiaopeng; Li, Zhuo	A Performance Measurement and Optimization Mechanism for Blockchain Mining Pool System	https://doi.org/10.1145/3446983.3446991

2019	Liu, Mengting; Yu, F. Richard; Teng, Yinglei; Leung, Victor C.M.; Song, Mei	Performance optimization for blockchain-enabled industrial internet of things (iiot) systems: A deep reinforcement learning approach	https://doi.org/10.1109/TII.2019.2897805
2020	Li, Yixin; Cao, Bin; Peng, Mugen; Zhang, Long; Zhang, Lei; Feng, Daquan; Yu, Jihong	Direct Acyclic Graph-Based Ledger for Internet of Things: Performance and Security Analysis	https://ieeexplore.ieee.org/document/9097392/
2021	Brotsis, Sotirios; Limniotis, Konstantinos; Bendiab, Gueltoum; Kolokotronis, Nicholas; Shiaeles, Stavros	On the suitability of blockchain platforms for IoT applications: Architectures, security, privacy, and performance	https://www.sciencedirect.com/science/article/pii/S1389128621001225
2019	Yu, Shitang; Lv, Kun; Shao, Zhou; Guo, Yingcheng; Zou, Jun; Zhang, Bo	A High Performance Blockchain Platform for Intelligent Devices	https://doi.org/10.1109/HOTICN.2018.8606017
2020	Kim, Seong Kyu; Huh, Jun Ho	Blockchain agreement for self-identification of online test cheating: Improvement of Algorithm performance	https://ieeexplore.ieee.org/document/9268400/

2021	Xi Li,Zehua Wang,Victor C. M. Leung,Hong Ji,Yiming Liu,Heli Zhang	Blockchain-empowered Data-driven Networks: A Survey and Outlook	https://dl.acm.org/doi/10.1145/3446373?ai=tnkc&ui=nggk&af=T
2021	Jun Huang, Debiao He, Mohammad S. Obaidat, Pandi Vijayakumar, Min Luo, Kim-Kwang Raymond Choo	The Application of the Blockchain Technology in Voting Systems: A Review	https://dl.acm.org/doi/10.1145/3439725?ai=tnkc&ui=nggk&af=T
2021	Pin-Chun Chen,Tzu-Hsiang Kuo,Ja-Ling Wu	A Study of the Applicability of Ideal Lattice-Based Fully Homomorphic Encryption Scheme to Ethereum Blockchain	https://ieeexplore.ieee.org/document/9408585
2021	Chao Li,Balaji Palanisamy, Runhua Xu, Jinlai Xu, Jingzhe Wang	SteemOps: Extracting and Analyzing Key Operations in Steemit Blockchain-based Social Media Platform	https://dl.acm.org/doi/10.1145/3422337.3447845?ai=tnkg&ui=nggk&af=T
2021	Martijn Sauwens, Kristof Jannes, Bert Lagaisse, Wouter Joosen	SCEW: Programmable BFT-Consensus with Smart Contracts for Client-Centric P2P Web Applications	https://dl.acm.org/doi/10.1145/3447865.3457965?ai=tnkc&ui=nggk&af=T

2021	Harsh Bimal Desai, Mustafa Safa Ozdayi, Murat Kantarcioglu	BlockFLA: Accountable Federated Learning via Hybrid Blockchain Architecture	https://dl.acm.org/doi/10.1145/3422337.3447837?ai=tnkc&ui=nggk&af=T
2021	Akram Hakiri, Behnam Dezfouli	Towards a Blockchain-SDN Architecture for Secure and Trustworthy 5G Massive IoT Networks	https://dl.acm.org/doi/10.1145/3445968.3452090?ai=tnkc&ui=nggk&af=T
2021	Johannes Köstler, Hans P. Reiser, Gerhard Habiger, Franz J. Hauck	SmartStream: towards byzantine resilient data streaming	https://dl.acm.org/doi/10.1145/3412841.3441904?ai=tnkf&ui=nggk&af=T
2021	S. Pothumani	Effective Security Mechanisms for Big Data Using Block Chain Technology	https://ieeexplore.ieee.org/document/9402458?dld=aG90bWFpbC5jb20%3D&source=SEARCHALERT

2021	Jae-Yun Kim, Junmo Lee, Yeonjae Koo, Sanghyeon Park, and Soo-Mook Moon∗	Ethanos: efficient bootstrapping for full nodes on account-based blockchain	https://dl.acm.org/doi/10.1145/3447786.3456231?ai=tnkf&ui=nggk&af=T
2021	Arijet Sarker, SangHyun Byun, Wenjun Fan, Sang-Yoon Chang	Blockchain-based root of trust management in security credential management system for vehicular communications	https://dl.acm.org/doi/10.1145/3412841.3441905?ai=tnkc&ui=nggk&af=T
2021	Xinghuo Yu; Changbing Tang; Peter Palensky; Armando Colombo	Blockchain: What Does It Mean to Industrial Electronics? Technologies, Challenges, and Opportunities	https://ieeexplore.ieee.org/document/9405370?dld=aG90bWFpbC5jb20%3D&source=SEARCHALERT
2021	R.C. Suganthe; N. Shanthi; R.S. Latha; K. Gowtham; S. Deepakkumar; R. Elango	Blockchain enabled Digitization of Land Registration	https://ieeexplore.ieee.org/document/9402469?dld=aG90bWFpbC5jb20%3D&source=SEARCHALERT
2021	Muralidhara, S; Usha, B A	Review of Blockchain Security and Privacy	https://ieeexplore.ieee.org/document/9402458?dld=aG90bWFpbC5jb20%3D&source=SEARCHALERT

2020	Zhang, Yu; Jin, Menglu; Zheng, Guiping; Li, Hu	Design and Application of Product Traceability Blockchain-based Platform	https://ieeexplore.ieee.org/document/9418424/
2021	Zhang, Qinnan; Ding, Qingyang; Zhu, Jianming; Li, Dandan	Blockchain Empowered Reliable Federated Learning by Worker Selection: A Trustworthy Reputation Evaluation Method	https://ieeexplore.ieee.org/document/9415658/
2021	Li, Lanlin; Teng, Yinglei; Yu, F Richard; Song, Mei; Wang, Wenjun	Blockchain based Joint Task Scheduling and Supply-Demand Configuration for Smart Manufacturing	https://ieeexplore.ieee.org/document/9420026/
2021	Zanella, Gianluca; Liu, Charles Zhechao; Choo, Kim-Kwang Raymond	Understanding the Trends in Blockchain Domain Through an Unsupervised Systematic Patent Analysis	https://ieeexplore.ieee.org/document/9417421/
2021	Awadallah, Ruba; Samsudin, Azman; Teh, Je Sen; Almazrooie, Mishal	An Integrated Architecture for Maintaining Security in Cloud Computing Based on Blockchain	https://ieeexplore.ieee.org/document/9428346/

2020	Liu, Xiaoyu; Liu, Xiaofu; Guo, Zhenpeng	Analysis on the Thinking Innovation of Ideological and Political Education Based on the Theory of Blockchain in the Information Age	https://ieeexplore.ieee.org/document/9420703/
2020	Wang, Lingzhong	Progress and Application Analyses in Blockchain Technology	https://ieeexplore.ieee.org/document/9415682/
2021	Bidwell, Nicola J; Elsden, Chris; Trotter, Ludwig; Hallwright, Josh; Moore, Sadie; Jeite-Delbridge, Kate; Harding, Mike; Shaw, Peter; Davies, Nigel; Speed, Chris; Vines, John	A Right Time to Give: Beyond Saving Time in Automated Conditional Donations	https://ieeexplore.ieee.org/document/9426198/
2021	Ferrag, Mohamed Amine; Shu, Lei	The Performance Evaluation of Blockchain-based Security and Privacy Systems for the Internet of Things: A Tutorial	https://dl.acm.org/doi/10.1145/3411764.3445371

2021	Landwehr, Marvin; Engelbutzeder, Philip; Wulf, Volker	Community Supported Agriculture: The Concept of Solidarity in Mitigating Between Harvests and Needs	https://ieeexplore.ieee.org/document/9424688/
2021	Jelena Marjanović, Nikola Dalčeković, Goran Sladić	Improving Critical Infrastructure Protection by Enhancing Software Acquisition Process Through Blockchain	https://dl.acm.org/doi/10.1145/3411764.3445268
2021	Maya Dotan, Yvonne-Anne Pignolet, Stefan Schmid, Saar Tochner, Aviv Zohar	Survey on Blockchain protocoling: Context, State-of-the-Art, Challenges	https://doi.org/10.1109/Blockchain.2019.00067
2021	Volkan Sevindik	Blockchain based Resource Tokenization for Crowdfunding of Wireless Network Investment	https://doi.org/10.1109/ICOSST.2018.8632190
2021	Panagiotis Chatzigiannis, Foteini Baldimtsi, Constantinos Kolias, Angelos Stavrou	Black-Box IoT: Authentication and Distributed Storage of IoT Data from Constrained Sensors	https://doi.org/10.1109/ISETC.2018.8583923

Appendix III: Blockchain Protocols - Background

Blockchain Protocols

The terms "blockchain protocols" and "blockchain networks" are often utilized interchangeably, given their reference to the underlying technical rules and mechanisms that steer the function of blockchain-based systems. Such protocols can be largely divided into four central categories.

To begin with, there are public networks (Zhao, Yang and Luo, 2019) —a category where any individual with a computer and internet access can freely contribute to the network. Contrarily, private networks are restricted, demanding an invitation and authentication, typically handled either by the network's originator or a pre-set rule mechanism.

Hybrid blockchains bring another dimension, offering a blend of public and private blockchain characteristics (Kiayias and Zindros, 2018). Their operation varies depending on the selected features of centralization and decentralization.

Lastly, we have Sidechain blockchains, a system operating in parallel with the primary blockchain. Interconnections must exist between entries from the main blockchain and the sidechain, or else the sidechain runs independently. For instance, the Liquid Network, a Bitcoin sidechain, provides faster, more private transactions, yet remains tethered to the main Bitcoin blockchain. Alternatively, the Plasma sidechain, a scalability solution for Ethereum, runs independently, although it periodically commits its state to the Ethereum main chain for added security.

Despite their differences, all types of blockchains carry risks and challenges (Dinh *et al.*, 2017; Salman *et al.*, 2019; Edwards, Mashatan and Ghose, 2020). Further categorization emerges when considering permissioned and permissionless blockchains. The former, permissioned blockchains (Vukolić, 2017), require an access control layer to regulate network access. On the contrary, public or permissionless networks (Neudecker and Hartenstein, 2019) don't necessitate access control, nor do they need to ward off malicious actors. Here, anyone

with the requisite hardware and internet connectivity can join the network, even functioning as an active node generating transactions.

In the early stages of cryptocurrencies (e.g., 2009-2010), transactions were primarily for transferring a digital asset to another's wallet. Nowadays, however, transactions can serve a multitude of purposes thanks to the additional metadata that can be embedded (Faisal *et al.*, 2018). Blockchain protocols entertain various stakeholders—users, miners/validators, developers, node operators, and regulators—all working in concert to maintain the network's integrity and security.

Transactions, once logged and verified on a blockchain, get associated with the subsequent block. Every new block's authenticity must be validated by a consensus mechanism, ensuring its legitimacy and preventing double-spending. In Proof-of-Work (PoW) blockchains, miners expend computational power to resolve complex puzzles to validate a new block. In Proof-of-Stake (PoS) blockchains, validators are selected based on their stake in the network and are tasked with validating new blocks.

Block time—a key feature of blockchain systems—is vital for transaction rates, especially in cryptocurrencies. For instance, Ethereum can generate one validated block every 15 seconds (*Home | Ethereum.org*, 2013), while Bitcoin averages a new block every 10 minutes (*Bitcoin - Open source P2P money*, 2008). At times, two blocks might be generated simultaneously, creating a temporary fork—a split of the chain into two separate ones. A consensus must be reached to determine which chain to continue with. A fork might also occur with changes to the blockchain's source code.

Forks are divided into two types: hard forks (Jeffery Atik, 2018), where there's no interaction between the old and new versions, and soft forks (Lin and Liao, 2017b), which render previously valid blocks/transactions invalid. An example of a fork is the Ethereum blockchain in 2016, where a code flaw in the decentralized autonomous organization (DAO) led to a hard fork, resulting in the creation of Ethereum and Ethereum Classic.

The Evolution of Blockchain

Since the launch of Bitcoin in January 2009 until now, there has been a significant improvement in blockchain technology. Initially, with the introduction of blockchain in Bitcoin, the world often equated the technology with the cryptocurrency itself. However, it was soon recognized that blockchain is bringing about a profound transformation in the very nature of the Internet. For some time, blockchain was the technology serving Bitcoin's needs, such as decentralization of currency and financial transactions, decentralization of data storage using a distributed decentralized database, eliminating the need for "trusted" 3rd parties to verify transactions etc. Soon after, it was realized that Bitcoin could not fulfill the expectations of having a Turing Complete system (*What exactly is Turing Completeness? - Evin Sellin - Medium,* 2017), meaning that it was not possible to maintain scripts' state, or perform recursive loops.

In 2014, Ethereum project (*Home | Ethereum.org,* 2013) was introduced aiming to allow a level of scripting on top of the blockchain platform forming the so-called dApps. The technology behind Ethereum also allowed micro-payments so it could handle small value transactions while at the same time simulation of the human behavior was now possible. Ethereum also pioneered the concept of Decentralized Autonomous Organizations (DAO), a type of decentralized enterprise that operates entirely based on smart contracts (Sato and Himura, 2018).

At a later phase, numerous researchers and organizations turned their attention towards enhancing the scalability of the blockchain system. This led to the introduction of several solutions that could facilitate a higher transaction rate. As of now, Bitcoin can process about 7 transactions per second, while Ethereum can handle between 15 to 20. Litecoin (*Litecoin - Open source P2P digital currency,* 2011) handles about 56 transactions per second and finally Ripple XRPL can handle about 1500. However, the goal of most blockchain protocols, is the achievement of more transactions than the Visa payment protocol(Visa.com, 2017).

Blockchain 1.0 - The Origin of the Modern Blockchain: As previously stated, Blockchain 1.0 was the first use of Nakamoto's invention. This is the most basic type of a decentralized ledger for recording transactions and storing data across several computers. To put it simply,

the information recorded in the first blockchains was confined to the values of a 'thing' that changed ownership over time. In most situations, the 'thing' in question is a digital money. This form of Bitcoin is essentially an automated electronic currency transfer system that operates without the requirement for human participation as a trusted authority between transactions. Users can use this method to convert currencies without the involvement of a bank (either from the private or government sector). The concept allowed users to transfer monies anonymously via wallets while providing everyone connected to the blockchain with access to the whole transactional record. It was completely transparent. Early technology also allowed miners (users who assisted in transaction verification by doing cryptographic tasks on their computers) to earn rewards via the PoW methods built into the protocols. As a result of these factors, blockchain technology has become the foundation of cryptocurrency trading platforms. Bitcoin was the first cryptocurrency to be introduced in 2009, and it was quickly followed by numerous others, including Dogecoin (Dogecoin - An open-source peer-to-peer digital currency)(Dogecoin - An open-source peer-to-peer digital currency). Because cryptocurrencies were not previously subject to government restrictions or a high level of financial inspection, they were a viable alternative to trade with fiat currencies such as US dollars.

Blockchain 2.0 - Smart Contracts: The following advancement in blockchain technology enhanced the capabilities of blockchain protocols. Four years after Bitcoin's emergence, Vitalik Buterin unveiled the notion of Ethereum, a blockchain-based platform with several major advancements over the previous generation. Ethereum was the first blockchain to include smart contracts into its technology. In layman's terms, smart contracts are a collection of programs that are executed automatically when specific circumstances are satisfied. These contracts let two people or businesses to do more than just exchange bitcoin. Ethereum, for example, is a multi-component platform that includes a virtual computer with numerous layers of information, user accounts, contracts, and cost accounting (a measure known as 'gas'). As a result, smart contracts enable two parties to execute complicated activities automatically while also enabling the exchange of digital currency. As a result, Blockchain 2.0 offers a number of new options that were previously unavailable owing to the limited scope of first-generation blockchains.

Blockchain 3.0 - Decentralized Enterprise Level Applications: The next level of blockchain technology is less defined. However, experts agree that Blockchain 3.0 has a greater potential in terms of industries and sectors that it may encompass. This suggests that Blockchain 3.0 has uses in fields other than finance and economics. Sustainability, scalability, cost-effectiveness, more decentralization, and increased security are the primary objectives for this generation of blockchains. Healthcare (smart contracts for medical services and EMR storage), cybersecurity (multi-factor authentication), supply chain (smart delivery contracts), and manufacturing are examples of these uses. The technique may also be used to power computing programs such as Folding@home (Front Page - Folding@home) and supercomputers. These sectors rely on enterprise-grade technologies for business process planning and execution. Enterprise-level databases may be readily linked into decentralized systems using Blockchain 3.0 for safe and transparent documentation. Furthermore, the new technology enables the interoperability of various blockchain protocols throughout the world. COSMOS (What is Cosmos? - Cosmos Network) and Chainlink (Chainlink, 2021)ecosystems are examples of this, as they are built on the Inter-Blockchain Communication (IBC) protocol (Qasse, Talib and Nasir, 2019) and allow data transmission between multiple blockchains without undermining their sovereignty. As a result, Blockchain 3.0 necessitates creative methods to combine various technology. These include IoT devices and Application Specific Integrated Circuits (ASICS) (Rieger, 2003) designed for processing, storing, and linking blockchains.

Blockchain 4.0 – Industry Adoption: Blockchain 4.0 refers to the fourth generation of blockchain technology. It claims to give blockchain as a business-usable environment for developing and executing applications, pushing the technology to the forefront. Previous incarnations of blockchain technology have demonstrated clear potential benefits for businesses, including security, automatic record-keeping, and immutability, as well as the ability to pay invoices, bills, and salaries inside a completely secure framework. Unfortunately, blockchain has previously failed to overcome three fundamental challenges: speed was simply too slow, and only a tiny number of individuals possessed the specialized expertise necessary to work on the blockchain. Consumers, employees, and companies want web 2.0-like user experiences; blockchain was trying to offer web 1.0, with issues comparable to the first generation of online

pioneers. Blockchains like Bitcoin are referred to as 'blockchain 1.0,' since they were designed with a specific purpose in mind (supporting a cryptocurrency), are sluggish, and difficult to operate. Blockchain 2.0 would be one of the first post-Bitcoin blockchains designed to do more than just support bitcoin; 'blockchain 3.0' would be a blockchain designed specifically to support a wide range of activities and applications. Blockchain 4.0 takes that desire and makes it a reality. If it's been able to create apps that look and feel like web 2.0 apps, operate as quickly, and retain the unique benefits of blockchain technology, blockchain 4.0 is achieved.

Blockchain 5.0 – Web3.0: Blockchain 5.0 is the newest iteration of a decade-old technology, and Relictum Pro (Relictum Pro is Built on Next-Gen Blockchain 5.0) intends to use it to organize and legitimize people's economic life. The objective is to eliminate the intermediaries engaged in many areas such as transportation, lodging, banking, and so on, ensuring that transactions are faster and safer than ever before. The following are some of the reasons why Relictum Pro is poised to usher in a new era with blockchain 5.0:

Reduced Block Size: The block size of Blockchain 5.0 is just 120 bytes, which is 8,000 times less than the block size of Bitcoin, which is 1,024,000 bytes (1 MB). This allows for a significant increase in data transport and processing speed. It also expedites network information lookup.

Increased Transaction's Finality: To execute a transaction on today's blockchain, it can take up to 30 minutes to load all nodes with blocks. However, Blockchain 5.0 completes the operation in less than 2 seconds, allowing customers to transfer payments in record time.

Higher Throughput: The average number of transactions performed per second on 4th generation blockchain is between 1,000 and 900,000 per second. However, blockchain 5.0 enables transactions to exceed one million.

Blockchain Challenges

As various entities seek to incorporate blockchain technology into their existing infrastructures, emerging innovators have designed their businesses with blockchain as the core from their inception. In theory, this foundational inclusion of blockchain technology provides

them with greater adaptability and versatility compared to their more traditional competitors, and simultaneously allows them to bypass certain roadblocks that often hinder larger, more established companies in their adoption process. As blockchain technology continues to evolve, spawning diverse applications, businesses across all industries should prepare themselves to navigate an ever-changing landscape replete with new challenges and potential controversies. These challenges are explored further in the following bullet points.

- **Inefficient Technological Design**: Although blockchain technology offers many advantages, it still has a number of fundamental flaws that prevent it from gaining widespread acceptance. Bitcoin, as well as other blockchains, are well-known for their inefficient technological architecture, which results in limited scalability, network slowness, high energy consumption, and, as a result, high transaction costs (Gaur, 2020). Aside from that, there is a lack of standards and interoperability, which makes it difficult for different blockchains to connect with one another. Ethereum attempted to hide a lot of these flaws, but it was insufficient. Moreover, the decentralized applications, built with Ethereum blockchain help developers build dApps for a plethora of use cases. Some of them, however, seem to have a question of miscoding and loopholes, leading to vulnerabilities and hack-issues.
- **Scalability:** Scalability poses a major challenge when it comes to integrating blockchain into realistic business use-cases (Khan, Jung and Hashmani, 2021). The capabilities of a blockchain system primarily depend on the number of transactions each block can handle. Take the Bitcoin blockchain as an example: creating a block takes approximately 10 minutes, and the quantity of transactions each block can contain is determined by its size, which in Bitcoin's case is one Megabyte (MB). Hence, to accommodate a massive volume of real-world transactions, the system needs to be carefully designed to optimize throughput. Furthermore, in a traditional blockchain system, each node processes and stores the entire transaction history, right back to the genesis block. Therefore, it's impractical to directly extend blockchain into actual business settings where nodes have limited storage and computational capabilities. Therefore, learning how to store data efficiently in resource-constrained blockchain nodes is crucial. Lastly, networking is the

third determinant of blockchain and Distributed Ledger Technology (DLT) systems' scalability. The traditional blockchain protocol operates like a "broadcast medium", where every node disseminates all transactions. In the early stages of Bitcoin, the "block size debate" became a well-known instance highlighting the scalability challenge. The network's original protocol had a block size limit of 1MB, which was put in place as an anti-spam measure. However, as Bitcoin gained popularity, and transaction volumes grew, the 1MB limit started causing congestion and slow transactions. Several proposals were made to increase the block size, but disagreements over the proposals led to significant debates within the community. These disagreements ultimately resulted in a hard fork and the creation of Bitcoin Cash, which had a larger block size.

- **Energy Consumption:** Energy consumption is another significant barrier to blockchain acceptance (Hasib Anwar, 2018). The mining process demands substantial computational power to resolve intricate equations, thereby escalating the energy requirement. Presently, miners utilize about 0.2% of the total global electricity. If this trend continues unabated, then the power consumption by miners may exceed the world's total energy production. This issue is fast becoming one of the most critical challenges faced by this network.
- **Cost and Efficiency:** The swift and dependable execution of peer-to-peer transactions via blockchain protocols is accompanied by a considerable cumulative cost, which is more substantial for certain types of blockchain compared to others (Deloitte, 2019). This inefficiency occurs because in an effort to be the first to find a solution each node executes the same functions as any other node on its own copy of the data. For example, the Bitcoin network, which uses a PoW CA, the overall operating costs associated with the validation and exchange of public ledger transactions are projected to be as high as $600 million per year and rising. It should be also taken in mind that this amount does not include the capital costs associated with the purchase of specialist mining equipment.
- **Privacy and Security:** Security issues linked to blockchain technology have been rigorously debated. Numerous professionals and academic experts suggest that blockchain technology is incompatible with privacy laws such as the European Union's General Data Protection Regulation (GDPR) (Otto, 2018). Although digital currencies

like Bitcoin offer pseudonymity, future blockchain implementations that allow smart transactions and contracts could be directly linked to verified identities. This raises significant concerns regarding privacy and data protection of information stored and accessible on the public ledger. Participants who transfer personal data to the blockchain are more likely to be classified as GDPR *controllers*, given they define the processing information, while blockchain nodes that merely gather personal data are more likely to be identified as processors as they merely facilitate the operation of the blockchain protocol.

- **Regulation and Lack of Adequate Skill Sets:** Regulation is a key challenge facing the adoption of blockchain technology, as organizations implementing blockchain solutions without clear guidelines may potentially circumvent existing regulations (Cunha, Soja and Themistocleous, 2021). However, regulation can also be a driver of mass adoption of blockchain technology. Clear regulatory frameworks can provide legal certainty and facilitate the integration of blockchain technology into existing systems. Regulatory sandbox programs, which allow for the testing of blockchain-based solutions in a controlled environment, can also help drive innovation and adoption. In addition to regulatory challenges, the lack of adequately skilled personnel remains a major hurdle in the adoption of blockchain technology. As the technology is still evolving, few individuals possess the necessary skill sets to support its implementation. Addressing this challenge requires investment in education and training programs to develop a skilled workforce capable of supporting the growing demand for blockchain-based solutions.
- **Public Acceptance:** Last but not least, a key challenge facing the adoption of blockchain technology is the lack of public acceptance and understanding, particularly in non-banking sectors. Despite the potential benefits of blockchain technology, many individuals are still unfamiliar with how it functions and are not aware of its future use cases. This lack of knowledge and awareness can hinder adoption and limit the potential impact of blockchain solutions (Profile *et al.*, 2023). Even though this technology is creating a significant impact and drawing in more users, it is essential to enhance

education and awareness campaigns to boost public comprehension and acceptance of blockchain.

Blockchain Consensus Algorithms

Achieving consensus in distributed systems, is at the heart of this technology, including blockchain. Since by nature such systems do not rely on a central authority for the validation process of transactions, the consensus mechanism plays a crucial role towards that goal. That is to say, such a system would confirm the legitimacy of each transaction by reaching an agreement between all the network participants. Consensus mechanisms existed long before the advent of blockchain. Starting from the "Byzantine Generals Problem", that is a term carved from the definition of a situation in which two or more parties involved need to agree on a single strategy to avoid total failure, but where some of the parties involved are unethical and disseminate false information or are otherwise unreliable. In 1980, several system architectures were developed forming a distributed system, where Byzantine Fault Tolerance (BFT) consensus mechanisms where adopted. Such mechanisms include Draper's FTMP, Honeywell's MMFCS and SRI's SIFT(Hopkins, Smith and Lala, 1978; Goldberg and J., 1981; *Computer Safety, Reliability, and Security: 22nd International Conference ... - Google Books*, 2003). With the advent of blockchain though, several CAs have been implemented while each one of them aims to similar but at the same time different goals. Throughput refers to the rate at which a network can process transactions, which directly impacts its ability to cater to a high volume of users. Scalability denotes the capacity of the consensus mechanism to handle an increasing number of participants, ensuring the network's growth without incurring significant performance bottlenecks. Security is of paramount importance, as it safeguards the network from malicious attacks and preserves the immutability of the blockchain. Finality signifies the assurance that once a transaction is recorded on the blockchain, it becomes irreversible, thereby providing a stable and reliable environment for users. Finally, energy efficiency is an essential property for the sustainable operation of blockchain protocols, as it minimizes the environmental impact and ensures the long-term viability of the system.

Proof of Work (PoW): Central to the creation of new blocks in certain blockchain systems, the Proof of Work CA stands as the backbone of cryptocurrencies like Bitcoin. The underlying idea that drives this algorithm is the resolution of a mathematical problem of the utmost complexity, followed by the generation of a solution that is very simple to verify. The intensity of this computational "puzzle" is contingent on several factors - the volume of network participants, the overall computational capabilities at play, and the current level of network traffic. Every block's hash incorporates the hash of the preceding block, a feature that heightens security measures and acts as a robust defense against any potential violation of individual blocks. Furthermore, the nature of this computational challenge is such that it demands considerable resources and computational prowess. This intensity of demand ensures that the node, which successfully deciphers the puzzle, is granted the privilege of mining the succeeding block. Such a mechanism promotes fair competition and just rewards while maintaining the integrity and security of the entire blockchain protocol (Lucas and Paez, 2019).

Proof of Stake (PoS): PoS presents itself as a popular alternative to PoW, most notably exemplified by Ethereum's transition from PoW to PoS. Instead of pouring resources into expensive hardware to solve complex mathematical puzzles, as seen in PoW, validators within the PoS model invest directly in the native cryptocurrency of the network. They accomplish this by 'staking' or locking up a portion of their coin holdings. These staked validators engage in the validation of new blocks. Rewards, distributed in relation to the number of blocks validated and added to the blockchain, are directly proportional to their respective stakes, thereby enriching their holdings over time. The selection of a validator for the generation of a new block is influenced by their economic stake within the network. The PoS model fosters a sense of consensus among validators through a process that is inherently incentivized. It promotes efficiency and participation, as well as an economic balance within the network. Validators, by staking their coins, demonstrate a vested interest in maintaining network integrity and functionality, effectively minimizing any malicious behavior within the blockchain ecosystem (Vasin and Co, 2017).

Tindermint: A prominent variation of the PoW model, Tendermint, addresses crucial areas like transaction speed, scalability, and environmental impacts. It leverages the Byzantine Fault

Tolerance (BFT) algorithm to achieve its goals. A notable feature of the Tendermint blockchain is its resilience to tolerate up to a third of byzantine players in the network, making it robust in the face of potentially malicious activities. This CA showcases a broad compatibility with all programming languages, reinforcing its versatility. Validators in the Tendermint network undertake the tasks of transaction verification and the addition of new blocks to the blockchain. These validators play a crucial role in consensus-building by broadcasting cryptographic signatures that act as votes in favor of blockchain extension. To attain the status of a validator in Tendermint's system, a user must possess a certain amount of funds, which is then locked in as voting power.

Tendermint also incorporates the concept of delegation. This mechanism allows delegators to stake their tokens with a chosen validator. However, the staked tokens run a risk of being lost if the chosen validator fails to adhere to the protocol's regulations. The Tendermint consensus mandates a minimum of four validators, while the maximum limit is unrestricted. As part of the Cosmos project, Tendermint serves as the consensus protocol with a working model of 100 validators, set to increase to 300 in future iterations. Block finality is contingent upon the number of validators, and a completed block typically takes around 3 seconds, although it can be quicker. One of the main issues of the PoS model, the 'nothing-at-stake' problem, is effectively addressed in Tendermint through the bond deposit system. Releasing bond deposits involves an 'un-bonding' period, usually spanning two to three months. A potential drawback is the possibility of a fork, particularly if one-third of the validators sign multiple blocks simultaneously. Validators causing such forks face significant penalties, losing one-third of their locked stake, thereby further enhancing the protocol's security (Lei, Lan and Lin, 2020) (Baliga, 2017c).

Proof of Luck (PoL): Primarily employed within the Trusted Execution Environment (TEE) of Intel SGX platforms, the Proof of Luck CA could potentially be adapted for other systems exhibiting comparable TEE characteristics. This protocol was designed to address a series of challenges associated with conventional CAs, including their slow transaction speeds, excessive energy consumption, and time-intensive nature. A point of contention with PoL, however, is its reliance on specialized hardware, a requirement that may not be accessible to all and could

disproportionately favor those equipped with such devices. Despite this, the protocol offers robust security measures courtesy of the TEE, which thwarts any attempt at blockchain manipulation unless an attacker controls the majority of CPUs and disrupts the TEE platform. In the context of PoL, each round commences with the participant invoking the PoLRound function and submitting the most recent block to a designated chain. Upon the conclusion of the ROUND TIME, the participant activates the PoLMine function to create a new block. This newly minted block is then linked to its predecessor via the new block's headers. The protocol stipulates an inspection for parent blocks in cases where the preceding block deviates from the round block.

The PoL model ensures that participants observe the ROUND TIME interval between block mining sessions. Concurrently, it also allows them the flexibility to pivot to a 'luckier' block should they come across one in the waiting period. The PoLMine function, following a uniform distribution, generates a random value within the range [0,1] to identify the winning block amongst all blocks mined by participants in a given round.

Interestingly, the wait time here acts as a determinant of the winning block - a shorter delay signifies the 'lucky' block, while a longer one implies an 'unlucky' outcome. Consequently, there's no requirement for a participant to declare a lucky block until the completion of the mining process, thereby maintaining a fair and competitive environment (Milutinovic *et al.*, 2016) .

Proof of Disease (PoD): Designed specifically for application within the healthcare blockchain, the Proof of Disease CA seeks to facilitate rapid, cost-effective access to high-quality medical care. This innovative system bifurcates miners into two distinct categories: currency miners and medical miners. Medical miners undertake the task of validating the authenticity and adequacy of medical transactions and health status entries on the healthcare blockchain ledger. Concurrently, currency miners are responsible for scrutinizing financial transactions to preempt and prevent potential threats like Sybil and double-spending attacks. PoD's underlying foundation is based on the Ethereum platform. Consequently, the transaction fee structure and reward mechanisms for currency miners align with Ethereum's established systems. On the other hand, medical miners receive compensation from users who have

procured tokens through the medical blockchain system. This unique approach ensures that each type of miner is appropriately incentivized for their crucial roles in maintaining the integrity and efficacy of the blockchain. The PoD consensus system thus presents a synergistic model that brings together the best of healthcare and blockchain technology (Talukder *et al.*, 2018).

Raft: The Raft CA (Huang, Ma and Zhang, 2018) serves as a methodology for distributed systems, designed with a keen emphasis on simplicity and ease of understanding. Its primary function is to address the challenge of achieving agreement on a shared state across multiple servers, even in scenarios where one or more servers experience failures. The shared state is typically maintained via a replicated log, which is, in most instances, a data structure. The system's full functionality is assured, provided that a majority of the servers remain operational.

In the Raft model, consensus is achieved by electing a leader within the cluster. The leader bears the responsibilities of processing client requests and managing the replication of the log to other servers within the network. This structure results in a unidirectional flow of data - solely from the leader to the other servers.

Raft breaks down the complexity of consensus into three separate, manageable sub-problems:

1. **Leader Election**: In the event of the incumbent leader's failure, the protocol necessitates the election of a new leader.
2. **Log Replication**: The leader must ensure the synchronization of all servers' logs with its own through replication.
3. **Safety Ensurance**: If a server has committed a log entry for a particular index, it must be guaranteed that no other server can apply a different log entry for the same index.

By effectively addressing these aspects, the Raft algorithm offers a comprehensive and easy-to-understand approach to achieving consensus in distributed systems.

Proof of Personhood (PoP): PoP (Borge *et al.*, 2017) is an innovative system devised with the specific goal of mitigating security vulnerabilities, including Sybil and double-spending attacks. PoP assures pseudonymous accountability by tying real-world identities to the coin

minting process. This system employs a combination of the RandHound algorithm, the Pseudonym party concept, and the ByzCoin protocol. Aspiring coin minters must initially join the PoP as members of the Pseudonym party. Membership requires physical attendance at a specific location where the Pseudonym party is held. It's important to note that without attending these gatherings, an individual cannot engage in the minting process within this blockchain system.

Participants of the Pseudonym party are each provided with a token. This token serves multiple purposes, including authentication, validation, and functioning within the RandHound algorithm. The token possesses a predetermined validity period, during which its holder is permitted to mint. Interestingly, each member of the minting pool is allocated only one token, ensuring an equal opportunity for all minters to be rewarded for block creation. This egalitarian approach continues until every token holder has been granted the chance to mint a new block and reap the associated benefits. Thus, PoP offers a unique blend of physical and digital participation, enhancing security and fairness within the blockchain system.

Proof of Authority (PoA): In networks utilizing the PoA consensus mechanism (Tomlinson, 2013) transactions and blocks are validated by designated validators or authorized accounts. Using specific software, these validators compile transactions into blocks. While this process is largely automated, requiring little active monitoring from validators, it does necessitate stringent security measures for the computer system hosting the authority node. The term "Proof of Authority" was coined by Gavin Wood, co-founder of Ethereum and Parity Technologies. Through PoA, individuals earn the right to become validators, which inherently incentivizes them to preserve and enhance their reputational standing. With their identities tied to their validator status, they are motivated to faithfully facilitate the transaction process, lest their reputations become tarnished. This design is considered to offer higher security than Proof of Stake. While PoS may establish equal stakes between parties, it doesn't account for the totality of a party's holdings, potentially leading to skewed incentives. PoA circumvents this issue by enforcing a rule that a single validator cannot validate consecutive blocks, thereby mitigating the risk of significant damage to the authority node.

PoA is a versatile CA, applicable to both private and public networks where trust is decentralized. An example of this is the POA Network, which leverages this protocol to maintain security and efficiency.

Proof of Trust (PoT): The PoT CA (Zhu *et al.*, 2020) selects transaction validators based on the trust levels attributed to participants within the network. It employs the RAFT leader election method and Shamir's secret sharing techniques to facilitate this process. PoT was designed to overcome some of the key limitations associated with existing consensus models. Specifically, it seeks to address the low throughput and high resource consumption associated with Bitcoin's PoW protocol. Simultaneously, it confronts the scalability challenges endemic to classical Paxos- and Byzantine Fault Tolerance (BFT)-based algorithms. Furthermore, PoT extends its scope to tackle dishonest behaviors, an issue typically overlooked by conventional BFT algorithms. As such, it introduces a practical and robust accountability framework for online services.

Overall, the PoT CA presents a refined approach to achieving network consensus that is less resource-intensive, more scalable, and more capable of managing untrustworthy actions within the network, showing promise for various applications in the online service sector.

Proof of Contribution (PoC): The Proof of Contribution CA(Song *et al.*, 2021) blends concepts from both Proof of Work (PoW) and Proof of Stake (PoS) models, adding novel elements such as the "Success Time" notion and "Success Time Value" which serves as the stake. In PoC, the difficulty value for a miner's task is dynamically adjusted based on their Success Time Value. If a miner possesses a high Success Time Value, their assigned mining difficulty decreases, effectively establishing a dependency of mining effort on the Success Time Value. This results in miners with high Success Time Values having a greater probability of earning the reward for generating a new block. Contrasting with PoW and PoS, PoC has a built-in mechanism to penalize fraudulent actions. Should a miner engage in deceitful behavior, their Success Time Value is set to zero, and their address is added to a publicly accessible blacklist. Any blocks associated with a blacklisted address are disregarded by other miners, and no transactions are conducted with the blacklisted address.

This way, PoC introduces a unique CA that not only rewards contributions but also implements robust measures to discourage and penalize dishonest behavior within the network.

Ripple Protocol Consensus Algorithm (RPCA): The Ripple protocol (Amores-Sesar, Cachin and Micic, 2020) was designed with the Ripple cryptocurrency in focus, paying particular attention to the latency issues brought about by Byzantine failures. In this system, each node engages with others in its "Unique Node List" (UNL), a server hosting an array of other Ripple nodes used for reaching consensus. The configuration of this UNL is node-specific. In the Ripple ecosystem, achieving consensus is a multi-round process. In the initial round, every node gathers transactions, incorporates them into a publicly available list known as the "candidate set", and broadcasts this set to all nodes within its UNL. The nodes within the UNL then engage in a voting process to validate these transactions, and the results of these votes are propagated across the UNL.

Each node produces a candidate set and the transactions that secure the most votes move forward to the subsequent round. When a candidate set garners approximately 80% or more of the votes from all the active nodes within the UNL, it wins the vote and is ratified as a legitimate block within the Ripple environment, referred to as the "Ledger". This ledger is termed the "Last Closed Ledger (LCL)", and every node within the UNL appends it to the Ripple blockchain. Transactions that do not qualify, alongside new ones, are included in the next round of consensus. This iterative process continues until all transactions are verified and incorporated into the LCL.

Dynamic Practical Byzantine Fault Tolerance (DPBFT): The Dynamic PBFT (Hao *et al.*, 2018) is a consensus mechanism that draws from its PBFT base while bringing additional benefits to the table. DBFT possesses the same degree of security and liveliness as its PBFT counterpart. Like PBFT, it hinges on weak synchrony assumptions - a significant feature that makes it applicable over the internet. Further, as suggested by its name, Dynamic PBFT facilitates a network where replicas and nodes can join or exit the consensus network with minimal disruptions. It incorporates a mechanism to eject nodes that exhibit malicious behavior or long periods of downtime, thus amplifying the robustness of the system. A new concept, termed 'Participation Degree,' is introduced in DBFT. This measure evaluates whether a node is

sufficiently active within the network. By raising the costs of evading consensus, this makes nodes more likely to participate, thereby enhancing the system's security. Moreover, by placing malicious nodes on a blacklist, DBFT amplifies the consequences of malicious behavior, further bolstering the security of the network.

Stellar Consensus Protocol (SCP): The Stellar Consensus protocol (Mazieres, 2015) employs the concepts of quorums and quorum slices. A quorum is a large enough group of nodes required to reach consensus, while a quorum slice is a subset of a quorum that can convince a particular node to agree with it. Individual nodes can appear in multiple quorums. Quorum slices were introduced in Stellar to allow each node to select a set of nodes in its slice, enabling open membership in the network. The formation of these quorums and quorum slices draws on real-world commercial relationships between various entities, capitalizing on existing trust in business relations. Quorums must intersect to achieve global consensus across the system. The collective decision of individual nodes forms the global consensus.

The Stellar consensus protocol operates as follows: Each node casts an initial vote on transactions or statements in a process known as federated voting. In this stage, each node picks its own statement and does not accept a conflicting one. However, it can switch to a different statement if its quorum slice has already accepted it.

The next stage is acceptance. The node accepts a statement if it has not received a conflicting statement, and every node in its v-blocking set has accepted that statement. A v-blocking set is a group of nodes that can veto the decision of the current node in each quorum slice. Quorum slices interconnect, leading to quorums agreeing on a set of propositions. When all members of a quorum concur with the statement, it's referred to as confirmation. The last step in the voting process is ratification, which indicates agreement at the system level. This step ensures that nodes send confirmation messages to each other until they all agree on the final state value of the system.

Proof of Stake Velocity (PoSV): Proof of Stake Velocity (Ren, 2014) was developed in 2014 for Reddcoin, a digital social currency. This CA allows for both stake ownership and activity (velocity). It was designed as an alternative to the PoW and PoS algorithms used in

popular digital currencies like Bitcoin and Ethereum, addressing some of the social and economic issues found in PoW and PoS networks. A major problem in PoS systems is that they incentivize minters to hold onto their stake for longer periods, based on a linear coin-age function. This preference typically benefits passive holders over active network participants. PoSV addresses this issue by replacing the linear coin-age function with an exponential decay function. The exponential decay function suggests that the longer a stake is held without being used for validating transactions, the less it contributes to the owner's chances of creating the next block. This modification encourages stakeholders to actively participate in the network and frequently move their stakes. It also incentivizes participants to remain online and validate transactions, as doing so increases their chances of earning rewards. In essence, PoSV combines the concepts of coin ownership (stake) and participation (velocity) to create a more balanced and active network.

Proof of Stake Casper (PoS Casper): Casper the Friendly Finality Gadget Protocol (Sheth *et al.,* 2019) is a Proof of Stake (PoS) protocol developed to address some of the core issues that plague other consensus mechanisms in blockchain protocols, such as the "Nothing at stake" dilemma, which is prevalent in PoW and PoS systems. Designed for Ethereum's Fair Validation Consensus, the Casper PoS protocol strives to eliminate the unfair advantage of wealthier miners and ensure a fair transaction validation process. The Casper PoS protocol introduces several key improvements to the traditional PoS algorithm, including:

- **Accountability**: Casper easily identifies any violations of rules, and the guilty parties are penalized by the slashing of their deposits.
- **Dynamic validators**: Validators are given the flexibility to join and leave the validator set with a certain notice period.
- **Defenses**: Casper can fend off a variety of attacks, including long-range revision attacks where more than one-third of validators are offline.
- **Modular Overlay**: Casper is built as a modular overlay on top of the existing Proof of Work chain, allowing for an easy and straightforward implementation.

In the Casper protocol, the criterion for transaction validation requires a supermajority (more than 2/3) of the validators' stakes and at least 1/2 of the validator votes. If these conditions are

satisfied, the transaction is considered validated; otherwise, the voting continues. Validators who validate incorrect transactions are penalized by having their stakes slashed, while those who identify the validators' mistake are rewarded. The protocol also introduces the concept of "checkpoints," each consisting of a set of 100 blocks to improve efficiency.

While the Casper PoS protocol holds much promise, it is still under development and has yet to be fully implemented. There is significant uncertainty regarding its practical application and potential issues, such as a scenario where a validator's stake is slashed causing them to leave and subsequently rejoin the validator set. These challenges are being actively explored and addressed by the Ethereum development community.

Proof of Participation and Fee (PoPF): The Proof of Participation and Fees (PoPF) (Fu *et al.*, 2018) method is a blockchain-based consensus protocol typically used in cooperative cloud computing. The PoW concept is utilized, but unlike traditional PoW methods, there is no competition amongst all users for each block creation. In PoPF, a percentage of top-ranking users are selected as accountant candidates for each block generation. The ranking is determined based on users' participation and fees in the preceding transaction. The PoPF protocol only activates after certain criteria are met, involving a specific number of users as well as their level of participation and fee contribution. Until then, the PoW concept is used.

CloudPoS: Cloud Proof of Stake (CloudPoS) (Tosh *et al.*, 2018) is a consensus protocol designed for a combination of blockchain and cloud environments. Unlike the traditional PoS concept, the CloudPoS changes the notion of stake from cryptocurrency to resources (CPU power, network, and memory) held by Cloud Service Providers (CSP). CloudPoS operates in epochs, each having several stages: stake determination, resource staking and confirmation, leader election, block replication and verification, and reward distribution.

Delegated PoS (DPoS): Delegated Proof of Stake (DPoS) is a CA specifically designed for the BitShares blockchain. Unlike Proof of Work (PoW) and PoS, DPoS does not rely on a competitive process for block creation. Instead, stakeholders within the network select a predetermined number of nodes, known as witnesses, to produce blocks for a designated period of time. Additionally, there are standby nodes ready to take over if a witness fails to create a

block within a certain timeframe. The block creation process in DPoS follows a round-robin method, where each elected witness takes turns producing blocks one at a time. This rotation ensures that all witnesses have an equal opportunity to contribute to the blockchain. The authorized witnesses generate blocks at regular intervals, typically every three seconds, and the list of witnesses is rotated every 21 blocks.

To maintain the integrity of the network, DPoS has measures in place to address non-performance by witnesses. If a witness fails to produce a block within the designated time or is unable to fulfill their role, they can be replaced by a standby node from the backup list. This mechanism ensures that block production remains continuous and uninterrupted. In the DPoS CA, active participation and reliability are key factors. Witnesses are responsible for validating transactions and securing the blockchain. If a producer fails to produce blocks for a consecutive 24-hour period, they are temporarily removed from consideration as a witness. They can resume producing blocks once they notify the blockchain protocol of their intention to continue. DPoS offers faster block generation and transaction confirmation times compared to PoW-based systems, making it suitable for high-throughput applications. By delegating block production to a select group of trusted nodes, DPoS aims to achieve greater scalability, energy efficiency, and network performance (Saad and Radzi, 2020).

Proof of Burn (PoB): Proof of Burn (PoB) (Karantias, Kiayias and Zindros, 2020), is a consensus algorithm that involves validators willingly 'burning' or making unusable, a certain number of coins. This is accomplished by sending the coins to a 'burn' address, which is essentially an address from which coins cannot be spent or retrieved. The act of burning coins is seen as proof of the validators' commitment to the network. The principle behind this algorithm is that validators demonstrate their commitment by making a sacrifice. In the case of PoB, the sacrifice is financial, as validators destroy a certain number of coins. In exchange for this sacrifice, they increase their chances of being selected to mine the next block. The more coins a validator burns, the higher the probability of being chosen. This helps secure the network and deter malicious behavior by making attacks costly. However, it's worth noting that PoB might not be as environmentally friendly as it sounds because it still encourages validators to purchase and then burn coins, potentially leading to unnecessary resource consumption.

Proof of Capacity (PoC): Proof of Capacity (PoC) (BiKi.com, 2020) is another consensus algorithm where validators use their available hard drive space to participate in the mining process. This approach makes the process more energy-efficient and accessible because it doesn't require specialized, energy-consuming hardware like Proof of Work (PoW). Validators pre-generate large data sets known as 'plots' and store them on their hard drive. These plots are used during the mining process to find the solution to the next block. The more hard drive space a validator dedicates to storing these plots, the higher their chances of finding the next block. However, PoC also has its challenges, such as the potential for centralization due to the cost of hard drive space and the wear and tear on hardware from constant reading and writing..

Proof of Elapsed Time (PoET): Proof of Elapsed Time (PoET) (Chen *et al.*, 2017) is a consensus mechanism that offers a fair and efficient process for selecting the next block creator. It works by assigning each participating node a random wait time. The node that gets the shortest wait time – i.e., the node whose timer runs out first – gets the right to create the next block. This system is energy efficient and fairly distributes the opportunity to create a block among all network participants. The main downside to PoET is that it requires a trusted execution environment to ensure that nodes cannot cheat the system by altering their wait times, which can lead to centralization issues.

practical Byzantine Fault Tolerance (pBFT): Practical Byzantine Fault Tolerance (pBFT) is a consensus mechanism designed for resilience and reliability in asynchronous systems. Developed by Barbara Liskov and Miguel Castro in the late 90s, it provides a solution to the Byzantine Generals' Problem, a situation in distributed computing where components of a system fail and give incorrect information, leading to system failure. In a pBFT system, each node in the network maintains an internal state. When a request comes in, the nodes communicate with each other to agree on the service execution order based on their internal state. After a number of nodes (greater than two-thirds of the total number of nodes) agree on the order, the request can be processed. This allows the system to function correctly and reach consensus even if some nodes are faulty or malicious. However, pBFT can be resource-intensive and doesn't scale well to large networks due to the high volume of communication required

between nodes. It's often used in consortium or private blockchain protocols where the number of nodes is relatively small and more controlled.

Proof of Activity (PoA): PoA (Bentov *et al.*, 2014) is a CA that combines elements of both PoW and PoS consensus mechanisms. It aims to leverage the advantages of both approaches to create a more efficient and secure system. The mining process in PoA initially operates similar to PoW, where different miners compete to find a new block by solving computational puzzles and providing higher processing power. Once a new block is discovered, the system transitions to PoS. At this point, the newly found block only consists of a header and the miner's reward address.

In the PoS phase, a random set of validators is chosen from the blockchain protocol based on the header data of the new block. These validators are responsible for validating or signing the new block. The selection process considers the number of coins held by each validator, favoring those with a larger stake. The participation of validators ensures the integrity and authenticity of the new block. To complete the block and add it to the blockchain protocol, all validators must sign off on it. Once the required number of validators have signed, the block is recognized as a full block, and transactions can be recorded on it. The mining fees or rewards associated with the block are then divided among the miner and the validators who contributed to its validation. However, PoA has faced criticism for resembling a hybrid approach that still requires significant computational power during the PoW phase. It has been argued that this can lead to excessive energy consumption and favor those who hold a large amount of coins, potentially concentrating power in the hands of a few.

Proof of Weight: Proof of Weight (PoWeight) (Peter Compare, 2018) is a blockchain consensus technique that assigns a 'weight' to users based on the number of tokens they own within the network. PoWeight is a consensus model that originated from research conducted at the MIT Computer Science & Artificial Intelligence Laboratory and has been implemented in the Algorand cryptocurrency. In the PoWeight consensus mechanism, the network forms a committee of randomly selected network members for each transaction. The committee members are chosen based on their token holdings, with those holding more tokens assigned a higher weight. This weight reflects their influence and importance within the consensus process.

The purpose of assigning weights is to protect the network from potential double-spending attacks. As long as the majority of weighted users are trustworthy, the consensus mechanism can ensure the integrity of transactions and prevent malicious activities. When a transaction occurs on the blockchain, the committee of randomly selected network members uses their weights to collectively validate and confirm the transaction. By centralizing the consensus process within this committee, PoWeight aims to achieve efficient and secure transaction confirmation.

It's important to note that PoWeight is specifically designed to address the double-spending problem, providing protection and security in decentralized systems. The allocation of weights based on token holdings allows for a fair and reliable consensus mechanism that enhances the overall robustness of the network.

Proof of Importance (PoI): Proof of Importance (PoI) (Hazari and Mahmoud, 2019) is a CA that was first introduced in the NEM blockchain. It is designed to address some of the issues inherent in the PoS mechanism, specifically the concern that PoS systems can favor the rich (those who own more coins) and lead to a concentration of power. The central idea of PoI is that a participant's influence on the network should not be determined solely by their coin holdings but also by their network activity. It introduces a scoring system (the Proof of Importance score) that takes into account three factors:

- **Vesting**: A certain number of coins (in NEM, at least 10,000 'vested' coins) should be held in the account. The process of vesting means that the coins have been held in the account for a certain period of time. The more vested coins a user has, the higher their PoI score.
- **Transaction partners**: The diversity of a user's transactions also impacts their PoI score. If a user transacts with many different users, their score is likely to be higher. This encourages network activity and discourages "hoarding" of coins.
- **Transaction volume and frequency**: The size and number of transactions made in the last 30 days also contribute to the PoI score. This incentivizes active participation in the network.

This system encourages active participation in the network, not just passive investment. It rewards users who make transactions and interact with different participants. This way, even if someone doesn't hold a significant number of coins but is an active participant, they can still have a chance to become a validator and contribute to the network's security. However, the PoI algorithm has checks in place to ensure that participants cannot "game" the system by transacting back and forth among a small group of accounts. If two or more people complete the same transaction among themselves, it won't lead to an increase in the PoI score.

Leased Proof of Stake (LPoS): Leased Proof of Stake (LPoS) (Salimitari and Chatterjee, 2018) is a variant of the Proof of Stake CA that offers solutions for certain challenges and limitations that might be encountered in a network. In particular, it's beneficial in situations where running a full node capable of verifying on-chain transactions can be technically demanding. One key feature of LPoS is that it incentivizes smaller users (those who may not have enough resources to run a full node themselves) to support more capable validators in the network. These validators are usually more efficient and reliable in handling transactions, making the network more robust and secure. Unlike the Delegated Proof of Stake (DPoS) system, in LPoS, token holders can lease or lend their tokens directly to these validators, thereby participating in the block creation process. This enables them to earn a portion of the rewards generated from block validation, thus serving their interests in the long term. In DPoS, on the other hand, validators are selected based on the number of votes they receive from other network members, where the weight of each vote is proportional to the number of tokens held by the voting member. While this system also incentivizes token holders to participate in the network governance, it does not offer the same kind of direct participation in the block creation process as LPoS.

Comparative Analysis

To further elaborate on the key characteristics of the CAs, a comparative analysis has been conducted considering several important evaluation criteria. These criteria are as follows:

- **Decentralization**: The extent to which decision-making authority is distributed among nodes in the network.

- **Scalability**: The ability of the algorithm to handle increasing workloads effectively as the network grows.
- **Security**: The algorithm's resilience against potential attacks, vulnerabilities, and failure scenarios.
- **Energy Efficiency**: The algorithm's resource requirements, specifically with regard to energy consumption.
- **Fairness**: The equal opportunity for all nodes in the network to contribute to the consensus process.

Proof-based Algorithms

Proof-based algorithms, including Proof of Work (PoW), Proof of Stake (PoS), and their derivatives, prioritize security and decentralization. These algorithms inherently disincentivize malicious behavior due to the significant resources required to perform successful attacks (e.g., a 51% attack in PoW) (Dziembowski, 2015). However, their limitations are also apparent: PoW algorithms, for instance, are notorious for their high energy consumption and can foster centralization over time due to the formation of mining pools (Chen and Liu, 2017). PoS mechanisms, while more energy-efficient, may lead to wealth centralization, where the rich get richer, and suffer from the 'Nothing at Stake' problem (David Mazières, 2022).

To mitigate these issues, innovative proof-based algorithms have been proposed. Proof of Capacity (PoC) and Proof of Space (PoSpace), for instance, leverage storage space instead of computational power or wealth, reducing energy consumption and allowing more equal participation. However, these approaches may still face centralization risks if larger entities can afford more storage space. Proof of Elapsed Time (PoET) employs a fair lottery system for mining rights but requires a trusted execution environment, potentially limiting its decentralization (Snider, Samani and Jain, 2018).

Voting-based Algorithms

Voting-based algorithms such as the Practical Byzantine Fault Tolerance (pBFT) and its derivatives provide rapid consensus and strong fault tolerance. They typically offer high security, as they can tolerate up to 1/3 of nodes being faulty or malicious (Hao *et al.*, 2018) .However, these algorithms often face scalability issues due to their high communication complexity in large-scale networks.

Federated Byzantine Agreement (FBA)-based algorithms, such as the Stellar Consensus Protocol (SCP) and the Ripple Protocol Consensus Algorithm (RPCA), address scalability limitations through the concept of quorum slices, allowing faster consensus with open membership. However, their dependence on trusted nodes may compromise the degree of decentralization.

Hybrid Approaches

Hybrid CAs, including Delegated Proof of Stake (DPoS) and Dynamic Practical Byzantine Fault Tolerance (DPBFT), combine elements from both proof-based and voting-based algorithms to capitalize on their strengths and mitigate their weaknesses.

DPoS offers high transaction throughput and energy efficiency while maintaining a degree of decentralization through stakeholder voting. However, it remains vulnerable to collusion and centralization on the part of the chosen delegates [103]. DPBFT blends pBFT with a dynamic validator set determined by a PoS mechanism, enhancing both scalability and security while preserving decentralization [104]. Its implementation complexity, however, could be a hindrance to widespread adoption.

Assessment and Discussion of Findings

The analysis in the table below provides a comprehensive snapshot of how each CA performs against the evaluation criteria. It is evident that no single CA stands out as the superior choice across all criteria, each exhibits unique strengths and weaknesses.

Proof-based algorithms excel in security due to their inherent disincentives against attacks but often falter in terms of energy efficiency and fairness, especially in the cases of PoW and PoS. On the other hand, voting-based algorithms offer strong security and fairness but may struggle with scalability due to the high communication overhead, especially for traditional pBFT.

Hybrid algorithms present an interesting compromise, combining strengths from both categories to overcome their respective limitations. However, their increased complexity might pose integration challenges.

This analysis underscores the fact that the choice of CA is not a one-size-fits-all solution; it depends on the specific requirements and context of each blockchain application. Further research should focus on innovating more efficient CA that better balance these criteria, fostering the development of more effective, inclusive, and sustainable blockchain systems.

Consensus Algorithm	Decentralization	Scalability	Security	Energy Efficiency	Fairness
Proof of Work (PoW)	High (Risk of centralization over time due to mining pools)	Limited due to high computational requirements	High (subject to 51% attack)	Low (high energy consumption)	Limited (favors entities with higher computational resources)
Proof of Stake (PoS)	High (But can lead to wealth centralization)	High (Lighter computational requirements)	High (subject to "nothing at stake" problem)	High	High (stake size can impact fairness)
Delegated Proof of Stake (DPoS)	Limited (Risk of centralization due to delegate system)	High	High (Potential risk of collusion among delegates)	High	Limited (Potential risk of centralization and delegate collusion)
Proof of Capacity (PoC)	High (Risk of centralization due to cost of storage space)	Moderate (Limited by available storage space)	High	High (compared to PoW)	High (Proportional to available storage space)

Proof of Elapsed Time (PoET)	High (Requires trusted execution environment)	Moderate	High (If executed within a trusted environment)	High (compared to PoW)	High (Random process)
Practical Byzantine Fault Tolerance (pBFT)	High (Assuming honest majority)	Limited (Communication complexity)	High (Can tolerate up to 1/3 of nodes being faulty)	Moderate	High (All nodes have equal voting power)
Proof of Activity (PoA)	Moderate (Depends on PoS and PoW combination)	Moderate	High	Moderate (Still uses PoW for initial block discovery)	Moderate (Combines PoS and PoW systems)
Proof of Weight (PoWeight)	High (Depending on distribution of tokens)	High (Uses committee-based decision making)	High	High	High (Based on token holdings)
Proof of Importance (PoI)	High (Includes network activity as a factor)	Moderate (Depends on the specific implementation)	High (Assuming honest majority of network activity)	High	High (Balances stake size and network activity)
Leased Proof of Stake (LPoS)	High (Assuming diversified leasing)	High	High	High	High (Allows smaller stakeholders to participate)

Federated Byzantine Agreement (FBA)	Moderate (Depends on trust in validators)	High	High	High	Moderate (Depends on chosen validators)
Stellar Consensus Protocol (SCP)	Moderate (Depends on trust in validators)	High	High	High	Moderate (Depends on chosen validators)
Ripple Protocol Consensus Algorithm (RPCA)	Moderate (Depends on trust in validators)	High	High	High	Moderate (Depends on chosen validators)
Dynamic Practical Byzantine Fault Tolerance (DPBFT)	High (Depends on PoS mechanism for validator selection)	High	High	High	High (Depends on PoS mechanism for validator selection)
Tendermint Consensus	High (Assuming honest majority)	High	High (Can tolerate up to 1/3 of nodes being faulty)	High	High (All validators have equal voting power)
Proof of Authority (PoA)	Limited (Centrally controlled validators)	High	High (Assuming trustworthy validators)	High	Limited (Centrally controlled validators)
Proof of Burn (PoB)	Moderate (Potential for wealth centralization)	Moderate	High	High (Beyond initial coin burning)	Moderate (Depends on resources for coin burning)

Proof of Reputation (PoR)	High (Depends on transparent and fair reputation system)	Moderate	High (Assuming a reliable reputation system)	High	High (Assuming a fair reputation system)
Proof of Space and Time (PoST)	High (Risk of centralization due to cost of storage space)	Moderate (Limited by available storage space)	High	High (compared to PoW)	High (Proportional to available storage space)
Proof of Space (PoSpace)	High (Risk of centralization due to cost of storage space)	Moderate (Limited by available storage space)	High	High (compared to PoW)	High (Proportional to available storage space)
Proof of History (PoH)	High	High	Moderate (Depends on timestamp verification)	High	High (Assumes fair access to transaction history)
Proof of Contribution (PoC)	High (Depends on fair evaluation of contributions)	Moderate (Depends on complexity of contribution evaluation)	High (Assuming fair contribution evaluation)	High	High (Assuming fair contribution evaluation)

Proof of Assignment (PoA)	High (Depends on task assignment mechanism)	Moderate (Depends on task assignment mechanism)	Moderate (Depends on task assignment mechanism)	High	High (Assumes fair task assignment)
Proof of Trust (PoT)	High (Assuming reliable trust measurement)	Moderate	High (Assuming reliable trust measurement)	High	High (Assuming fair trust measurement)
Proof of Believability (PoB)	High (Assuming fair believability measurement)	High	High (Assuming fair believability measurement)	High	High (Assuming fair believability measurement)
Proof of Stake Velocity (PoSV)	High (Assuming fair coin age measurement)	High	High (Assuming fair coin age measurement)	High	High (Assuming fair coin age measurement)

References

Akhtar, Z. (2019) 'From Blockchain to Hashgraph: Distributed Ledger Technologies in the Wild', in *Proceedings - 2019 International Conference on Electrical, Electronics and Computer Engineering, UPCON 2019*, pp. 1–6. Available at: https://doi.org/10.1109/UPCON47278.2019.8980029.

Alom, I. *et al.* (2022) 'BlockMeter: An Application Agnostic Performance Measurement Framework For Private Blockchain Platforms'. Available at: https://arxiv.org/abs/2202.05629v1

Alsunaidi, S.J. and Alhaidari, F.A. (2019) 'A survey of consensus algorithms for blockchain technology', in *2019 International Conference on Computer and Information Sciences, ICCIS 2019*, pp. 1–6. Available at: https://doi.org/10.1109/ICCISci.2019.8716424.

Altarawneh, A. and Skjellum, A. (2020) 'The security ingredients for correct and byzantine fault-tolerant blockchain consensus algorithms', in *2020 International Symposium on Networks, Computers and Communications, ISNCC 2020*. Montreal, QC, Canada: IEEE, pp. 1–9. Available at: https://doi.org/10.1109/ISNCC49221.2020.9297326.

Amores-Sesar, I., Cachin, C. and Micic, J. (2020) 'Security Analysis of Ripple Consensus', *Leibniz International Proceedings in Informatics, LIPIcs*, 184. Available at: https://doi.org/10.4230/LIPIcs.OPODIS.2020.10.

Apuke, O.D. (2017) 'Quantitative Research Methods : A Synopsis Approach', *Kuwait Chapter of Arabian Journal of Business and Management Review*, 6(11), pp. 40–47. Available at: https://doi.org/10.12816/0040336.

Baliga, A. (2017a) 'Understanding Blockchain Consensus Models', *Whitepaper*, (April), pp. 1–14.

Baliga, A. (2017b) 'Understanding Blockchain Consensus Models'.

Baliga, A. (2017c) *Understanding Blockchain Consensus Models, Whitepaper*.

Baliga, A. *et al.* (2018) 'Performance evaluation of the quorum blockchain platform', *arXiv preprint arXiv …* [Preprint]. Available at: https://arxiv.org/abs/1809.03421.

Bamakan, S.M.H., Motavali, A. and Babaei Bondarti, A. (2020) 'A survey of blockchain consensus algorithms performance evaluation criteria', *Expert Systems with Applications*, 154, p. 113385. Available at: https://doi.org/10.1016/j.eswa.2020.113385.

Bartoletti, M. *et al.* (2018) 'Blockchain for social good: A quantitative analysis', in *ACM International Conference Proceeding Series*. Bologna, Italy: ACM Press, pp. 37–42. Available at: https://doi.org/10.1145/3284869.3284881.

Baškarada, S. and Koronios, A. (2018) 'A philosophical discussion of qualitative, quantitative, and mixed methods research in social science', *Qualitative Research Journal*, 18(1), pp. 2–21. Available at: https://doi.org/10.1108/QRJ-D-17-00042/FULL/XML.

Benoit, Harold; Gramoli, Vincent; Guerraoui, Rachid; Natoli, C. (2021) *DIABLO: A Distributed Analytical Blockchain Benchmark Framework Focusing on Real-World Workloads*. Available at: https://www.researchgate.net/publication/351866720_DIABLO_A_Distributed_Analytical_Blockchain_Benchmark_Framework_Focusing_on_Real-World_Workloads .

Bentov, I. *et al.* (2014) *Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake*. Available at: http://eprint. .

BiKi.com (2020) *What is Proof of Capacity? (PoC). Proof of Capacity (PoC) is a consensus… | by BiKi.com | Medium*. Available at: https://medium.com/@bikicoin/what-is-proof-of-capacity-poc-d9287b190af7.

Bitcoin - Open source P2P money (2008). Available at: https://bitcoin.org/en/.

Chainlink (2021) *Blockchain Oracles for Hybrid Smart Contracts*. Available at: https://chain.link/.

Bodkhe, U. *et al.* (2020) 'A survey on decentralized consensus mechanisms for cyber physical systems', *IEEE Access*, 8, pp. 54371–54401. Available at: https://doi.org/10.1109/ACCESS.2020.2981415.

Borge, M. *et al.* (2017) 'Proof-of-Personhood: Redemocratizing Permissionless Cryptocurrencies', in *2017 IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*, pp. 23–26.

Bouraga, S. (2021) ‘A taxonomy of blockchain consensus protocols: {A} survey and classification framework’, *Expert Systems with Applications*, 168, p. 114384. Available at: https://doi.org/https://doi.org/10.1016/j.eswa.2020.114384.

Brandão, C. (2015) ‘ P. Bazeley and K. Jackson, Qualitative Data Analysis with NVivo (2nd ed.) ’, *Qualitative Research in Psychology*, 12(4), pp. 492–494. Available at: https://doi.org/10.1080/14780887.2014.992750.

Brandt, P. and Timmermans, S. (2021) ‘Abductive Logic of Inquiry for Quantitative Research in the Digital Age’, *Sociological Science*, 8, pp. 191–210. Available at: https://doi.org/10.15195/V8.A10.

Brereton, P. *et al.* (2007) ‘Lessons from applying the systematic literature review process within the software engineering domain’, *Journal of Systems and Software*, 80(4), pp. 571–583. Available at: https://doi.org/10.1016/j.jss.2006.07.009.

Buterin, V. (2014) ‘A NEXT GENERATION SMART CONTRACT & DECENTRALIZED APPLICATION PLATFORM’.

Casino, F., Dasaklis, T.K. and Patsakis, C. (2019) ‘A systematic literature review of blockchain-based applications: Current status, classification and open issues’, *Telematics and Informatics*. Elsevier Ltd, pp. 55–81. Available at: https://doi.org/10.1016/j.tele.2018.11.006.

Cerniglia, J.A., Fabozzi, F.J. and Kolm, P.N. (2016) ‘Best Practices in Research for Quantitative Equity Strategies’, *The Journal of Portfolio Management*, 42(5), pp. 135–143. Available at: https://doi.org/10.3905/JPM.2016.42.5.135.

Chan, L.T.H. (2015) ‘Reader response and reception theory’, *Researching Translation and Interpreting*, pp. 146–154. Available at: https://doi.org/10.4324/9781315707280-23/EXPERIMENTAL-RESEARCH-DANIEL-GILE.

Chand, S. and Liu, Y.A. (2020) ‘What’s Live? Understanding Distributed Consensus’. Available at: http://arxiv.org/abs/2001.04787.

Chaudhry, N. and Yousaf, M.M. (2019) ‘Consensus Algorithms in Blockchain: Comparative Analysis, Challenges and Opportunities’, in *ICOSST 2018 - 2018 International Conference on Open Source Systems and Technologies, Proceedings*. Institute of Electrical and Electronics Engineers Inc., pp. 54–63. Available at: https://doi.org/10.1109/ICOSST.2018.8632190.

Chen, L. *et al.* (2017) 'On security analysis of proof-of-elapsed-time (PoET)', in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. Springer Verlag, pp. 282–297. Available at: https://doi.org/10.1007/978-3-319-69084-1_19.

Chen, S. and Liu, C.-C. (2017) 'From demand response to transactive energy: state of the art', *Journal of Modern Power Systems and Clean Energy*, 5(1), pp. 10–19. Available at: https://doi.org/10.1007/s40565-016-0256-x.

Choi, W. and Hong, J.W.K. (2021) 'Performance Evaluation of Ethereum Private and Testnet Networks Using Hyperledger Caliper', *2021 22nd Asia-Pacific Network Operations and Management Symposium, APNOMS 2021*, pp. 325–329. Available at: https://doi.org/10.23919/APNOMS52696.2021.9562684.

Christodoulou, Klitos *et al.* (2020) 'Consensus Crash Testing: Exploring Ripple's Decentralization Degree in Adversarial Environments', *Future Internet*, 12(3), p. 53. Available at: https://doi.org/10.3390/fi12030053.

Christodoulou, K *et al.* (2020) 'Consensus crash testing: exploring Ripple's decentralization degree in adversarial environments', *Future Internet* [Preprint]. Available at: https://www.mdpi.com/1999-5903/12/3/53.

Computer Safety, Reliability, and Security: 22nd International Conference ... - Google Books (2003). Available at: https://books.google.com.cy/books?id=SaJqCQAAQBAJ&pg=PA243&lpg=PA243&dq=Honeywell+MMFCS&source=bl&ots=HwBGsdu1uT&sig=ACfU3U2hVwo_-3BABrVMOanu7WsLnvA8JQ&hl=en&sa=X&ved=2ahUKEwjZj_q35abqAhXSGewKHfb_DOEQ6AEwAHoECAkQAQ#v=onepage&q=Honeywell MMFCS&f=false.

Cong, K., Ren, Z. and Pouwelse, J. (2018) 'A Blockchain Consensus Protocol with Horizontal Scalability', *2018 IFIP Networking Conference IFIP Networking and Workshops, IFIP Networking 2018 - Proceedings*, pp. 424–432. Available at: https://doi.org/10.23919/IFIPNetworking.2018.8696555.

ConsenSys (2021) *ConsenSys Quorum | ConsenSys, Online*. Available at: https://consensys.net/quorum/.

Creswell, J.W. (2017) ‘Qualitative, quantitative, and mixed methods approaches + a crash course in statistics.’, *Research Design* [Preprint].

Croman, K. *et al.* (2016) ‘On Scaling Decentralized Blockchains Initiative for CryptoCurrencies and Contracts (IC3)’, *International Conference on Financial Cryptography and Data Security*, pp. 106–125. Available at: http://fc16.ifca.ai/bitcoin/papers/CDE+16.pdf.

Cunha, P.R. da, Soja, P. and Themistocleous, M. (2021) ‘Blockchain for development: a guiding framework’, *https://doi.org/10.1080/02681102.2021.1935453*, 27(3), pp. 417–438. Available at: https://doi.org/10.1080/02681102.2021.1935453.

Dai, W. *et al.* (2019) ‘A Concurrent optimization consensus system based on blockchain’, in *2019 26th International Conference on Telecommunications, ICT 2019*, pp. 244–248. Available at: https://doi.org/10.1109/ICT.2019.8798836.

David Mazières (2022) *Stellar Consensus Protocol: An Overview*. Available at: https://blog.simbachain.com/blog/stellar-consensus-protocol-an-overview.

Decker, C. and Wattenhofer, R. (2013) ‘Information propagation in the Bitcoin network’, in *13th IEEE International Conference on Peer-to-Peer Computing, IEEE P2P 2013 - Proceedings*. Available at: https://doi.org/10.1109/P2P.2013.6688704.

Deloitte (2019) *Deloitte’s 2019 Global Blockchain Survey*.

Deng, S. *et al.* (2023) ‘BCTC-KSM: A blockchain-assisted threshold cryptography for key security management in power IoT data sharing’, *Computers and Electrical Engineering*, 108, p. 108666. Available at: https://doi.org/10.1016/J.COMPELECENG.2023.108666.

Denzin, N.K. (2017) ‘The Research Act: A Theoretical Introduction to Sociological Methods’, *The Research Act: A Theoretical Introduction to Sociological Methods*, pp. 1–368. Available at: https://doi.org/10.4324/9781315134543/RESEARCH-ACT-NORMAN-DENZIN.

Dinh, T.T.A. *et al.* (2017) ‘BLOCKBENCH: A framework for analyzing private blockchains’, in *Proceedings of the ACM SIGMOD International Conference on Management of Data*. Association for Computing Machinery, pp. 1085–1100. Available at: https://doi.org/10.1145/3035918.3064033.

Dinh, T.T.A. *et al.* (2018) 'Untangling Blockchain: A Data Processing View of Blockchain Systems', *IEEE Transactions on Knowledge and Data Engineering*, 30(7), pp. 1366–1385. Available at: https://doi.org/10.1109/TKDE.2017.2781227.

Docker Container Stats (2016). Available at: https://github.com/wywywywy/docker_stats_exporter.

Docker Inc. (2022) *Home - Docker*. Available at: https://www.docker.com/.

Dogecoin - An open-source peer-to-peer digital currency (2013). Available at: https://dogecoin.com/.

Dragoni, N. *et al.* (2017) 'Microservices: Yesterday, Today, and Tomorrow', *Present and Ulterior Software Engineering*, pp. 195–216. Available at: https://doi.org/10.1007/978-3-319-67425-4_12.

Dziembowski, S. (2015) 'Introduction to Cryptocurrencies', in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*. New York, NY, USA: Association for Computing Machinery (CCS '15), pp. 1700–1701. Available at: https://doi.org/10.1145/2810103.2812704.

Edwards, M., Mashatan, A. and Ghose, S. (2020) 'A review of quantum and hybrid quantum/classical blockchain protocols', *Quantum Information Processing*. Springer. Available at: https://doi.org/10.1007/s11128-020-02672-y.

Faisal, T. *et al.* (2018) *The Evolution of Embedding Metadata in Blockchain Transactions*.

Fan, C. *et al.* (2020) 'Performance Evaluation of Blockchain Systems: A Systematic Survey', *IEEE Access*, 8, pp. 126927–126950. Available at: https://doi.org/10.1109/ACCESS.2020.3006078.

Faria, C. and Correia, M. (2019) 'BlockSim: Blockchain simulator', in *Proceedings - 2019 2nd IEEE International Conference on Blockchain, Blockchain 2019*, pp. 439–446. Available at: https://doi.org/10.1109/Blockchain.2019.00067.

Farooq, M.S., Ahmed, M. and Emran, M. (2022) 'A Survey on Blockchain Acquainted Software Requirements Engineering: Model, Opportunities, Challenges, and Future Directions', *IEEE Access*, 10, pp. 48193–48228. Available at: https://doi.org/10.1109/ACCESS.2022.3171408.

Ferdous, M.S. *et al.* (2020) 'Blockchain Consensuses Algorithms: A Survey', *arXiv preprint arXiv …* [Preprint]. Available at: https://arxiv.org/abs/2001.07091.

Ferdous, M.S., Chowdhury, M.J.M. and Hoque, M.A. (2021) 'A survey of consensus algorithms in public blockchain systems for crypto-currencies', *Journal of Network and Computer Applications*, p. 103035. Available at: https://doi.org/https://doi.org/10.1016/j.jnca.2021.103035.

Folding@home (20000) *Front Page - Folding@home*. Available at: https://foldingathome.org/?lng=en.

Fu, X. *et al.* (2018) 'PoPF: A Consensus Algorithm for JCLedger', *Proceedings - 12th IEEE International Symposium on Service-Oriented System Engineering, SOSE 2018 and 9th International Workshop on Joint Cloud Computing, JCC 2018*, pp. 204–209. Available at: https://doi.org/10.1109/SOSE.2018.00034.

Gaur, N. (2020) 'Blockchain challenges in adoption', *Managerial Finance*, 46(6), pp. 849–858. Available at: https://doi.org/10.1108/MF-07-2019-0328/FULL/PDF.

Gervais, A. *et al.* (2016) 'On the Security and Performance of Proof of Work Blockchains', in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. New York, NY, USA: Association for Computing Machinery (CCS '16), pp. 3–16. Available at: https://doi.org/10.1145/2976749.2978341.

Ghaznavi, M. *et al.* (2020) 'Fault Tolerant Service Function Chaining', *SIGCOMM 2020 - Proceedings of the 2020 Annual Conference of the ACM Special Interest Group on Data Communication on the Applications, Technologies, Architectures, and Protocols for Computer Communication*, pp. 198–210. Available at: https://doi.org/10.1145/3387514.3405863.

Goldberg and J. (1981) 'The SIFT computer and its development. [Software Implemented Fault Tolerance for aircraft control]'. Available at: http://ntrs.nasa.gov/search.jsp?R=19820029955.

Governatori, G. *et al.* (2018) 'On legal contracts, imperative and declarative smart contracts, and blockchain systems', *Artificial Intelligence and Law*, 26(4), pp. 377–409. Available at: https://doi.org/10.1007/s10506-018-9223-3.

Grafana (2020) *Grafana: The open observability platform | Grafana Labs*, *Grafana*. Available at: https://grafana.com/.

Graphite Exporter (2012). Available at: https://github.com/prometheus/graphite_exporter.

Group, S.E. (2007) *Guidelines for performing Systematic Literature Reviews in Software Engineering*.

Guggenberger, T. *et al.* (2022) 'An in-depth investigation of the performance characteristics of Hyperledger Fabric', *Computers & Industrial Engineering*, 173, p. 108716. Available at: https://doi.org/10.1016/J.CIE.2022.108716.

Guo, H. *et al.* (2018) 'An improved consensus mechanism for blockchain', in M. Qiu (ed.) *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. Cham: Springer International Publishing, pp. 129–138. Available at: https://doi.org/10.1007/978-3-030-05764-0_14.

Gupta, S. *et al.* (2019) 'An in-depth look of BFT consensus in blockchain: Challenges and opportunities', in *Middleware 2019 - Proceedings of the 2019 20th International Middleware Conference Tutorials, Part of Middleware 2019*. New York, NY, USA: Association for Computing Machinery (Middleware '19), pp. 6–10. Available at: https://doi.org/10.1145/3366625.3369437.

Hair, J.F. *et al.* (2015) 'Essentials of Business Research Methods, Second Edition', *Essentials of Business Research Methods, Second Edition*, pp. 1–477. Available at: https://doi.org/10.4324/9781315704562/ESSENTIALS-BUSINESS-RESEARCH-METHODS-JOSEPH-HAIR-JR-MARY-WOLFINBARGER-ARTHUR-MONEY-PHILLIP-SAMOUEL-MICHAEL-PAGE.

Hao, X. *et al.* (2018) 'Dynamic Practical Byzantine Fault Tolerance', in *2018 IEEE Conference on Communications and Network Security (CNS)*, pp. 1–8.

Hao, X. *et al.* (2018) 'Dynamic practical byzantine fault tolerance', *2018 IEEE Conference on Communications and Network Security, CNS 2018* [Preprint]. Available at: https://doi.org/10.1109/CNS.2018.8433150.

Hao, Y. *et al.* (2018a) 'Performance Analysis of Consensus Algorithm in Private Blockchain', in *IEEE Intelligent Vehicles Symposium, Proceedings*. Institute of Electrical and

Electronics Engineers Inc., pp. 280–285. Available at: https://doi.org/10.1109/IVS.2018.8500557.

Hao, Y. *et al.* (2018b) 'Performance Analysis of Consensus Algorithm in Private Blockchain', in *IEEE Intelligent Vehicles Symposium, Proceedings*. Institute of Electrical and Electronics Engineers Inc., pp. 280–285. Available at: https://doi.org/10.1109/IVS.2018.8500557.

Hasib Anwar (2018) *Top 10 Blockchain Adoption Challenges | 101 Blockchains*. Available at: https://101blockchains.com/blockchain-adoption-challenges/#prettyPhoto.

Hazari, S.S. and Mahmoud, Q.H. (2019) 'Comparative evaluation of consensus mechanisms in cryptocurrencies', *Internet Technology Letters*, 2(3). Available at: https://doi.org/10.1002/itl2.100.

Heß, A. and Hauck, F.J. (2023) 'Towards a Cloud Service for State-Machine Replication'. Available at: https://doi.org/10.18420/FGBS2023F-02.

Home | Ethereum.org (2013). Available at: https://ethereum.org/.

Hopkins, A.L., Jr., Smith, T.B., I. and Lala, J.H. (1978) 'FTMP - A highly reliable Fault-Tolerant Multiprocessor for aircraft'. Available at: http://ntrs.nasa.gov/search.jsp?R=19790041704.

Huang, D., Ma, X. and Zhang, S. (2018) 'Performance analysis of the raft consensus algorithm for private blockchains', *arXiv*, 50(1), pp. 172–181.

Huang, Z. *et al.* (2022) 'Bocb: Performance Benchmarking by Analysing Impacts of Cloud Platforms on Consortium Blockchain', *SSRN Electronic Journal* [Preprint]. Available at: https://doi.org/10.2139/SSRN.4310611.

The Linux Foundation (2020) *Hyperledger Fabric – Hyperledger Foundation, Online*. Available at: https://www.hyperledger.org/use/fabric.

InfluxData Inc. (2021) *InfluxDB: Open Source Time Series Database | InfluxData*. Available at: https://www.influxdata.com/.

Jabbar, R. *et al.* (2022) 'Blockchain Technology for Intelligent Transportation Systems: A Systematic Literature Review', *IEEE Access*, 10, pp. 20995–21031. Available at: https://doi.org/10.1109/ACCESS.2022.3149958.

Jeffery Atik, G.G. (2018) 'Hard Forks on the Bitcoin Blockchain: Reversible Exit, Continuing Voice', *Stanford Journal of Blockchain Law & Policy* [Preprint].

Karantias, K., Kiayias, A. and Zindros, D. (2020) 'Proof-of-Burn', in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. Springer, pp. 523–540. Available at: https://doi.org/10.1007/978-3-030-51280-4_28.

Kastner, E. (2012) *statsd/statsd: Daemon for easy but powerful stats aggregation*. Available at: https://github.com/statsd/statsd.

Kayastha, P. and Joshi, B. (2022) 'Proceedings of 12 th IOE Graduate Conference Small World Network for Simulation of Blockchain Networks'.

Ke, Z. and Park, N. (2022) 'Performance modeling and analysis of Hyperledger Fabric', *Cluster Computing*, pp. 1–19. Available at: https://doi.org/10.1007/S10586-022-03800-2/METRICS.

Khan, D., Jung, L.T. and Hashmani, M.A. (2021) 'Systematic Literature Review of Challenges in Blockchain Scalability', *Applied Sciences 2021, Vol. 11, Page 9372*, 11(20), p. 9372. Available at: https://doi.org/10.3390/APP11209372.

Khosravi, A. and Kavian, Y.S. (2016) 'Challenging issues of average consensus algorithms in wireless sensor networks', in *IET Wireless Sensor Systems*. Institution of Engineering and Technology, pp. 60–66. Available at: https://doi.org/10.1049/iet-wss.2015.0092.

Kiayias, A. and Zindros, D. (2018) *Proof-of-Work Sidechains*.

Kim, S. *et al.* (2020) 'Byzantine fault tolerance based multi-block consensus Algorithm for throughput scalability', in *2020 International Conference on Electronics, Information, and Communication, ICEIC 2020*, pp. 1–3. Available at: https://doi.org/10.1109/ICEIC49074.2020.9051279.

Kitchenham, B.A. *et al.* (2010) 'Refining the systematic literature review process-two participant-observer case studies', *Empirical Software Engineering*, 15(6), pp. 618–653. Available at: https://doi.org/10.1007/s10664-010-9134-8.

Kovalchuk, L. *et al.* (2020) 'Decreasing security threshold against double spend attack in networks with slow synchronization', *Computer Communications*, 154, pp. 75–81. Available at: https://doi.org/https://doi.org/10.1016/j.comcom.2020.01.079.

Kozlovski, S. (2018) *A Thorough Introduction to Distributed Systems*. Available at: https://www.freecodecamp.org/news/a-thorough-introduction-to-distributed-systems-3b91562c9b3c/.

Kwadwo Antwi, S. and Hamza, K. (2015) 'Qualitative and Quantitative Research Paradigms in Business Research: A Philosophical Reflection', *European Journal of Business and Management www.iiste.org ISSN*, 7(3). Available at: www.iiste.org.

Lamport, L. (2001) *Paxos Made Simple*, *ACM SIGACT News*.

Lei, L., Lan, C. and Lin, L. (2020) 'Chained Tendermint: A Parallel BFT Consensus Mechanism', in *2020 3rd International Conference on Hot Information-Centric Networking, HotICN 2020*. Hefei, China: IEEE, pp. 25–33. Available at: https://doi.org/10.1109/HotICN50779.2020.9350801.

Leka, E., Selimi, B. and Lamani, L. (2019) 'Systematic Literature Review of Blockchain Applications: Smart Contracts', in *2019 International Conference on Information Technologies, InfoTech 2019 - Proceedings*. Institute of Electrical and Electronics Engineers Inc. Available at: https://doi.org/10.1109/InfoTech.2019.8860872.

Li, K. *et al.* (2020) 'PoV: An Efficient Voting-Based Consensus Algorithm for Consortium Blockchains', *Frontiers in Blockchain*, 3, p. 11. Available at: https://doi.org/10.3389/fbloc.2020.00011.

Li, L., Jiang, Y. and Liu, G. (2019) 'Consensus with voting theory in blockchain environments', in *Proceedings - 10th IEEE International Conference on Big Knowledge, ICBK 2019*, pp. 152–159. Available at: https://doi.org/10.1109/ICBK.2019.00028.

Liang, L. *et al.* (2020) 'SLC: A Permissioned Blockchain for Secure Distributed Machine Learning against Byzantine Attacks', in *Proceedings - 2020 Chinese Automation Congress,*

CAC 2020. Shanghai, China: IEEE, pp. 7073–7078. Available at: https://doi.org/10.1109/CAC51589.2020.9327384.

Lin, I.C. and Liao, T.C. (2017a) 'A survey of blockchain security issues and challenges', *International Journal of Network Security*, 19(5), pp. 653–659. Available at: https://doi.org/10.6633/IJNS.201709.19(5).01.

Lin, I.C. and Liao, T.C. (2017b) 'A survey of blockchain security issues and challenges', *International Journal of Network Security*, 19(5), pp. 653–659. Available at: https://doi.org/10.6633/IJNS.201709.19(5).01.

Litecoin - Open source P2P digital currency (2011). Available at: https://litecoin.org/

Liu, J. *et al.* (2019) 'Scalable byzantine consensus via hardware-assisted secret sharing', *IEEE Transactions on Computers*, 68(1), pp. 139–151. Available at: https://doi.org/10.1109/TC.2018.2860009.

Lucas, B. and Paez, R. V. (2019) 'Consensus algorithm for a private blockchain', in *ICEIEC 2019 - Proceedings of 2019 IEEE 9th International Conference on Electronics Information and Emergency Communication*. Institute of Electrical and Electronics Engineers Inc., pp. 264–271. Available at: https://doi.org/10.1109/ICEIEC.2019.8784500.

M. Phillips, S.D. (2000) *(13) How To Get a PhD: A Handbook for Students and Their Supervisors. Third Edition*. Available at: https://www.researchgate.net/publication/234627340_How_To_Get_a_PhD_A_Handbook_for_Students_and_Their_Supervisors_Third_Edition.

Makhsoos, P.T., Bahrak, B. and Taghiyareh, F. (2022) 'Designing a High Performance and High-Profit P2P Energy Trading System Using a Consortium Blockchain Network', *2022 12th International Conference on Computer and Knowledge Engineering, ICCKE 2022*, pp. 458–464. Available at: https://doi.org/10.1109/ICCKE57176.2022.9960015.

Marijan, D. and Lal, C. (2022) 'Blockchain verification and validation: Techniques, challenges, and research directions', *Computer Science Review*, 45, p. 100492. Available at: https://doi.org/10.1016/J.COSREV.2022.100492.

Maull, R. *et al.* (2017) 'Distributed ledger technology: Applications and implications', *Strategic Change*, 26(5), pp. 481–489. Available at: https://doi.org/10.1002/jsc.2148.

Maung Maung Thin, W.Y. *et al.* (2018) 'Formal Analysis of a Proof-of-Stake Blockchain', in *2018 23rd International Conference on Engineering of Complex Computer Systems (ICECCS)*. ieeexplore.ieee.org, pp. 197–200. Available at: https://ieeexplore.ieee.org/abstract/document/8595076/.

Mazieres, D. (2015) 'The Stellar Consensus Protocol - A Federated Model for internet-level consensus', *Stellar Development foundation*, 120(42), pp. 11022–11023.

MihaljeviÄ‡, M.J. (2020) 'A Blockchain Consensus Protocol Based on Dedicated Time-Memory-Data Trade-Off', *IEEE Access*, 8, pp. 141258–141268. Available at: https://doi.org/10.1109/ACCESS.2020.3013199.

Miller, K.D. and Tsang, E.W.K. (2011) 'Testing management theories: critical realist philosophy and research methods', *Strategic Management Journal*, 32(2), pp. 139–158. Available at: https://doi.org/10.1002/SMJ.868.

Milutinovic, M. *et al.* (2016) 'Proof of Luck: An Efficient Blockchain Consensus Protocol', in *Proceedings of the 1st Workshop on System Software for Trusted Execution*. New York, NY, USA: Association for Computing Machinery (SysTEX '16). Available at: https://doi.org/10.1145/3007788.3007790.

Moon, M.D. (2019) 'Triangulation: A Method to Increase Validity, Reliability, and Legitimation in Clinical Research', *Journal of Emergency Nursing*, 45(1), pp. 103–105. Available at: https://doi.org/10.1016/j.jen.2018.11.004.

Morgan, D.L. (2014) 'Pragmatism as a Paradigm for Social Research', *http://dx.doi.org/10.1177/1077800413513733*, 20(8), pp. 1045–1053. Available at: https://doi.org/10.1177/1077800413513733.

Nakamoto, S. (2008) *Bitcoin: A Peer-to-Peer Electronic Cash System*. Available at: www.bitcoin.org.

Nanduri, S. and Vemula, H. (2022) 'Performance Study for Improving Throughput in Hyperledger Fabric Blockchain Platform', *2022 IEEE 1st Global Emerging Technology Blockchain Forum: Blockchain and Beyond, iGETblockchain 2022* [Preprint]. Available at: https://doi.org/10.1109/IGETBLOCKCHAIN56591.2022.10087049.

Nasrulin, B. *et al.* (2022) 'Gromit: Benchmarking the Performance and Scalability of Blockchain Systems', *Proceedings - 4th IEEE International Conference on Decentralized Applications and Infrastructures, DAPPS 2022*, pp. 56–63. Available at: https://doi.org/10.1109/DAPPS55202.2022.00015.

Natarajan, H., Krause, S. and Gradstein, H. (2017) *Distributed Ledger Technology and Blockchain, Distributed Ledger Technology and Blockchain*. World Bank. Available at: https://doi.org/10.1596/29053.

Nedelcu, C. (2010) 'Nginx HTTP Server Adopt Nginx for your web applications to make the most of your infrastructure and serve pages faster than ever'. Available at: www.packtpub.com.

Neudecker, T. and Hartenstein, H. (2019) 'Network layer aspects of permissionless blockchains', *IEEE Communications Surveys and Tutorials*, 21(1), pp. 838–857. Available at: https://doi.org/10.1109/COMST.2018.2852480.

Nguyen, G.T. and Kim, K. (2018) 'A survey about consensus algorithms used in Blockchain', *Journal of Information Processing Systems*, 14(1), pp. 101–128. Available at: https://doi.org/10.3745/JIPS.01.0024.

Oh, M. *et al.* (2020) 'Graph Learning BFT: A Design of Consensus System for Distributed Ledgers', *IEEE Access*, 8, pp. 161739–161751. Available at: https://doi.org/10.1109/ACCESS.2020.3021225.

Ongaro, D. and Ousterhout, J. (2014) *In Search of an Understandable Consensus Algorithm*. Available at: https://www.usenix.org/conference/atc14/technical-sessions/presentation/ongaro.

Otto, M. (2018) *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation – GDPR), International and European Labour Law*. Available at: https://doi.org/10.5771/9783845266190-974.

Pahlajani, S., Kshirsagar, A. and Pachghare, V. (2019) 'Survey on Private Blockchain Consensus Algorithms', in *Proceedings of 1st International Conference on Innovations in Information and Communication Technology, ICIICT 2019*, pp. 1–6. Available at: https://doi.org/10.1109/ICIICT1.2019.8741353.

Pandey, J. (1AD) 'Deductive Approach to Content Analysis', *https://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/978-1-5225-5366-3.ch007*, pp. 145–169. Available at: https://doi.org/10.4018/978-1-5225-5366-3.CH007.

Panwar, A. and Bhatnagar, V. (2020) 'Distributed ledger technology (DLT): The beginning of a technological revolution for blockchain', *2nd International Conference on Data, Engineering and Applications, IDEA 2020* [Preprint]. Available at: https://doi.org/10.1109/IDEA49133.2020.9170699.

Park, Y.S., Konge, L. and Artino, A.R. (2020) 'The Positivism Paradigm of Research', *Academic Medicine*, 95(5), pp. 690–694. Available at: https://doi.org/10.1097/ACM.0000000000003093.

Pawlikowski, P. *et al.* (2018) 'Positivism: A concept analysis', *International Journal of Nursing & Clinical Practices*, 5(1), p. 284. Available at: https://doi.org/10.15344/2394-4978/2018/284.

Ren, L. (2014) 'Proof of Stake Velocity: Building the Social Currency of the Digital Age', *Self-published white paper*, pp. 1–13. Available at: https://www.semanticscholar.org/paper/Proof-of-Stake-Velocity%3A-Building-the-Social-of-the-Ren/8499c0b3d1138200fdebb88f964100d54a531878.

Performance Analysis | Parity Technologies (2015). Available at: https://www.parity.io/performance-analysis/

Peter Compare (2018) *What Is Proof of Weight? | CoinCodex*. Available at: https://coincodex.com/article/2617/what-is-proof-of-weight/.

Pezoa, J.E., Dhakal, S. and Hayat, M.M. (2010) 'Maximizing service reliability in distributed computing systems with random node failures: Theory and implementation', *IEEE Transactions on Parallel and Distributed Systems*, 21(10), pp. 1531–1544. Available at: https://doi.org/10.1109/TPDS.2010.34.

Praitheeshan, P., Pan, L. and Doss, R. (2021) 'Private and Trustworthy Distributed Lending Model Using Hyperledger Besu', *SN Computer Science*, 2(2), p. 115. Available at: https://doi.org/10.1007/s42979-021-00500-3.

Prasad, V.K. *et al.* (2022) 'Federated Learning for the Internet-of-Medical-Things: A Survey', *Mathematics 2023, Vol. 11, Page 151*, 11(1), p. 151. Available at: https://doi.org/10.3390/MATH11010151.

Profile, S. *et al.* (2023) 'Blockchain: The Future of Smart City Development', *International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)*, 3(1). Available at: https://doi.org/10.48175/IJARSCT-9009.

Prometheus - Monitoring System (2017). Available at: https://prometheus.io/.

Puljak, L. and Sapunar, D. (2017) 'Acceptance of a systematic review as a thesis: Survey of biomedical doctoral programs in Europe', *Systematic Reviews*. BioMed Central Ltd., p. 253. Available at: https://doi.org/10.1186/s13643-017-0653-x.

Qasse, I.A., Talib, M.A. and Nasir, Q. (2019) 'Inter blockchain communication: A survey', *ACM International Conference Proceeding Series* [Preprint]. Available at: https://doi.org/10.1145/3333165.3333167.

Qiu, T., Zhang, R. and Gao, Y. (2019) 'Ripple vs. SWIFT: Transforming Cross Border Remittance Using Blockchain Technology', *Procedia Computer Science*, 147, pp. 428–434. Available at: https://doi.org/10.1016/j.procs.2019.01.260.

Rathod, T. *et al.* (2022) 'Blockchain for Future Wireless Networks: A Decade Survey', *Sensors 2022, Vol. 22, Page 4182*, 22(11), p. 4182. Available at: https://doi.org/10.3390/S22114182.

Reichardt, C.S., Ed. and Rallis, S.F., Ed. (1994) 'The Qualitative-Quantitative Debate: New Perspectives.', *New Directions for Program Evaluation* [Preprint].

Relictum Pro is Built on Next-Gen Blockchain 5.0 (2019). Available at: https://relictum.pro/

Ridder, H.G. *et al.* (2014) 'Qualitative data analysis. A methods sourcebook', *Zeitschrift fur Personalforschung*, 28(4), pp. 485–487.

Rieger, M. (2003) 'Application Specific Integrated Circuits (ASICs)', *The Electronic Design Automation Handbook*, pp. 384–397. Available at: https://doi.org/10.1007/978-0-387-73543-6_16.

Roulston, K. and Halpin, S.N. (2022) 'The SAGE Handbook of Qualitative Research Design', *The SAGE Handbook of Qualitative Research Design* [Preprint]. Available at: https://doi.org/10.4135/9781529770278.

Ryan, G. (2018) 'Introduction to positivism, interpretivism and critical theory', *Nurse Researcher*, 25(4), pp. 14–20. Available at: https://doi.org/10.7748/NR.2018.E1466.

Saad, S.M.S. and Radzi, R. (2020) 'Comparative Review of the Blockchain Consensus Algorithm Between Proof of Stake (POS) and Delegated Proof of Stake (DPOS)', *International Journal of Innovative Computing* [Preprint]. Available at: https://ijic.utm.my/index.php/ijic/article/view/272.

Saingre, D., Ledoux, T. and Menaud, J.M. (2020) 'BCTMark: A Framework for Benchmarking Blockchain Technologies', *Proceedings of IEEE/ACS International Conference on Computer Systems and Applications, AICCSA*, 2020. Available at: https://doi.org/10.1109/AICCSA50499.2020.9316536.

Salimitari, M. and Chatterjee, M. (2018) 'An overview of blockchain and consensus protocols for IoT networks', *arXiv preprint arXiv:1809.05613* [Preprint].

Salman, T. *et al.* (2019) 'Security services using blockchains: A state of the art survey', *IEEE Communications Surveys and Tutorials*, 21(1), pp. 858–880. Available at: https://doi.org/10.1109/COMST.2018.2863956.

Salman, T., Jain, R. and Gupta, L. (2019) 'A reputation management framework for knowledge-based and probabilistic blockchains', in *Proceedings - 2019 2nd IEEE International Conference on Blockchain, Blockchain 2019*. Institute of Electrical and Electronics Engineers Inc., pp. 520–527. Available at: https://doi.org/10.1109/Blockchain.2019.00078.

Sato, T. and Himura, Y. (2018) 'Smart-Contract Based System Operations for Permissioned Blockchain', in *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, pp. 1–6.

Saunders, B. (2018) 'Saturation in qualitative research: exploring its conceptualization and operationalization', *Quality and Quantity*, 52(4), pp. 1893–1907. Available at: https://doi.org/10.1007/s11135-017-0574-8.

Saunders Mark, Lewis Philip and Adrian Thornhill (2019) 'Research Methods for Business Students', *Research Methods for Business Students*, pp. 125–171.

Schreiber, Z. (2019) 'k-root-n: An efficient O (√ n) algorithm for avoiding short term double spending in Distributed Ledger Technologies such as Blockchain.', *IACR Cryptol. ePrint Arch.* [Preprint]. Available at: https://pdfs.semanticscholar.org/6031/3aa9cee1674b23c44b2fa1c6ed6ba13ef0a0.pdf.

Search | Mendeley (2008). Available at: http://www.mendeley.com/research-papers/search/?query=PMID%3A+++++15020670

Sedlmeir, J. (2021) 'The DLPS: A new framework for benchmarking blockchains', *Proceedings of the Annual Hawaii International Conference on System Sciences*, 2020, pp. 6855–6864. Available at: https://www.scopus.com/inward/record.uri?partnerID=HzOxMe3b%5C&scp=85101021574%5C&origin=inward.

Sharma, K. and Jain, D. (2019) 'Consensus Algorithms in Blockchain Technology: A Survey', in *2019 10th International Conference on Computing, Communication and Networking Technologies, ICCCNT 2019*, pp. 1–7. Available at: https://doi.org/10.1109/ICCCNT45670.2019.8944509.

Sheth, N. *et al.* (2019) 'Casper: modification of bitcoin using proof of stake', *Smart Innovation, Systems and Technologies*, 106, pp. 79–85. Available at: https://doi.org/10.1007/978-981-13-1742-2_8/COVER.

Shi, P. *et al.* (2021) 'Blockchain-based trusted data sharing among trusted stakeholders in IoT', *Software - Practice and Experience*, 51(10), pp. 2051–2064. Available at: https://doi.org/10.1002/SPE.2739.

Singh, P. *et al.* (2022) 'Federated Learning: Challenges, Methods, and Future Directions', *EAI/Springer Innovations in Communication and Computing*, pp. 199–214. Available at: https://doi.org/10.1007/978-3-030-85559-8_13/COVER.

S.Mullender (1993) *Sape Mullender Distributed Systems (2nd Edition)*.

Snider, M., Samani, K. and Jain, T. (2018) 'Delegated Proof of Stake: Features & Tradeoffs'.

Soiferman, L.K. (2010) ‘Compare and Contrast Inductive and Deductive Research Approaches.’, *Online Submission* [Preprint].

Song, A. *et al.* (2019) ‘Fast, dynamic and robust byzantine fault tolerance protocol for consortium blockchain’, in *Proceedings - 2019 IEEE Intl Conf on Parallel and Distributed Processing with Applications, Big Data and Cloud Computing, Sustainable Computing and Communications, Social Computing and Networking, ISPA/BDCloud/SustainCom/SocialCom 2019*, pp. 419–426. Available at: https://doi.org/10.1109/ISPA-BDCloud-SustainCom-SocialCom48970.2019.00067.

Song, H. *et al.* (2021) ‘Proof-of-Contribution consensus mechanism for blockchain and its application in intellectual property protection’, *Information Processing and Management*, 58(3), p. 102507. Available at: https://doi.org/10.1016/j.ipm.2021.102507.

Su, Y., Nguyen, K. and Sekiya, H. (2022) ‘Latency Evaluation in Ad-hoc IoT-Blockchain Network’, *WSCE 2022 - 2022 5th World Symposium on Communication Engineering*, pp. 124–128. Available at: https://doi.org/10.1109/WSCE56210.2022.9916023.

Sukhwani, H. *et al.* (2017) ‘Performance modeling of PBFT consensus process for permissioned blockchain network (hyperledger fabric)’, in *Proceedings of the IEEE Symposium on Reliable Distributed Systems*. IEEE Computer Society, pp. 253–255. Available at: https://doi.org/10.1109/SRDS.2017.36.

Talukder, A.K. *et al.* (2018) ‘Proof of Disease: A Blockchain Consensus Protocol for Accurate Medical Decisions and Reducing the Disease Burden’, in *2018 IEEE SmartWorld, Ubiquitous Intelligence Computing, Advanced Trusted Computing, Scalable Computing Communications, Cloud Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, pp. 257–262.

Tamminen, K.A. and Poucher, Z.A. (2020) ‘Research philosophies’, *The Routledge International Encyclopedia of Sport and Exercise Psychology*, pp. 535–549. Available at: https://doi.org/10.4324/9781315187259-39.

Tennakoon, D., Hua, Y. and Gramoli, V. (2022) ‘CollaChain: A BFT Collaborative Middleware for Decentralized Applications’. Available at: https://arxiv.org/abs/2203.12323v1

Themistocleous, M. (2004) 'Justifying the decisions for EAI implementations: a validated proposition of influential factors', *Journal of Enterprise Information Management*, 17(2), pp. 85–104. Available at: https://doi.org/10.1108/17410390410518745.

Themistocleous, M. *et al.* (2023) 'Towards cross-border CBDC interoperability: insights from a multivocal literature review', *Journal of Enterprise Information Management*, ahead-of-print(ahead-of-print). Available at: https://doi.org/10.1108/JEIM-11-2022-0411.

Themistocleous, M. *et al.* (2020) 'Blockchain in academia: Where do we stand and where do we go?', in *Proceedings of the Annual Hawaii International Conference on System Sciences*, pp. 5338–5347. Available at: https://doi.org/10.24251/hicss.2020.656.

Tikhomirov, S. *et al.* (2018) 'SmartCheck: Static Analysis of Ethereum Smart Contracts', in *Proceedings of the 1st International Workshop on Emerging Trends in Software Engineering for Blockchain*. New York, NY, USA: Association for Computing Machinery (WETSEB '18), pp. 9–16. Available at: https://doi.org/10.1145/3194113.3194115.

Tina, P.P. and Sarah, T. (2019) *Why systematic reviews matter*, *Elsevier Connect*. Available at: https://www.elsevier.com/connect/authors-update/why-systematic-reviews-matter

Tomlinson, R.D. (2013) 'Let's Look to Proof for Authority', *http://dx.doi.org/10.1080/00094056.1954.10726556*, 31(3), pp. 137–140. Available at: https://doi.org/10.1080/00094056.1954.10726556.

Tosh, D. *et al.* (2018) 'CloudPoS: A Proof-of-Stake Consensus Design for Blockchain Integrated Cloud', *IEEE International Conference on Cloud Computing, CLOUD*, 2018-July, pp. 302–309. Available at: https://doi.org/10.1109/CLOUD.2018.00045.

Touloupou, M. *et al.* (2022) 'Benchmarking Blockchains: The case of XRP Ledger and Beyond', *Proceedings of the 55th Hawaii International Conference on System Sciences* [Preprint]. Available at: https://doi.org/10.24251/HICSS.2022.730.

Tromp, J. (2014) *Cuckoo Cycle: a memory bound graph-theoretic proof-of-work*.

Tuan, T. *et al.* (2017) 'BLOCKBENCH: A Framework for Analyzing Private Blockchains', in *Proceedings of the 2017 ACM International Conference on Management of Data*. New York, NY, USA: Association for Computing Machinery (SIGMOD '17), pp. 1085–1100. Available at: https://doi.org/10.1145/3035918.3064033.

Valsiner, J. (2000) 'Data as representations: contextualizing qualitative and quantitative research strategies', *https://doi.org/10.1177/053901800039001006*, 39(1), pp. 99–113. Available at: https://doi.org/10.1177/053901800039001006.

Vasin, P. and Co, B. (2017) *BlackCoin's Proof-of-Stake Protocol v2*. Available at: www.blackcoin.com

Visa.com (2017) *VISA Fact Sheet January 2017*. Available at: https://usa.visa.com/dam/VCOM/global/about-visa/documents/visa-facts-figures-jan-2017.pdf.

Vukolić, M. (2017) 'Rethinking permissioned blockchains', in *BCC 2017 - Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts, co-located with ASIA CCS 2017*, pp. 3–7. Available at: https://doi.org/10.1145/3055518.3055526.

Vukolić, M. (2016) 'The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication', *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 9591, pp. 112–125. Available at: https://doi.org/10.1007/978-3-319-39028-4_9.

Vukolić, M. (2017) 'Rethinking permissioned blockchains', in *BCC 2017 - Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts, co-located with ASIA CCS 2017*. New York, New York, USA: Association for Computing Machinery, Inc, pp. 3–7. Available at: https://doi.org/10.1145/3055518.3055526.

Wan, Z. *et al.* (2019) 'Blockchain Federation for Complex Distributed Applications', in J. Joshi et al. (eds) *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. Cham: Springer International Publishing, pp. 112–125. Available at: https://doi.org/10.1007/978-3-030-23404-1_8.

Wang, H. and Tan, W. (2020) 'Block proposer election method based on verifiable random function in consensus mechanism', in *Proceedings of 2020 IEEE International Conference on Progress in Informatics and Computing, PIC 2020*. Shanghai, China: IEEE, pp. 304–308. Available at: https://doi.org/10.1109/PIC50277.2020.9350766.

Wang, R., Ye, K. and Xu, C.Z. (2019) 'Performance Benchmarking and Optimization for Blockchain Systems: A Survey', in *Lecture Notes in Computer Science (including subseries*

Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). Springer Verlag, pp. 171–185. Available at: https://doi.org/10.1007/978-3-030-23404-1_12.

Wang, S. (2019) 'Performance Evaluation of Hyperledger Fabric with Malicious Behavior', in J. Joshi et al. (eds) *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. Cham: Springer International Publishing, pp. 211–219. Available at: https://doi.org/10.1007/978-3-030-23404-1_15.

Wen, Y. *et al.* (2020) 'Blockchain Consensus Mechanisms and Their Applications in IoT: A Literature Survey', in M. Qiu (ed.) *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. Cham: Springer International Publishing, pp. 564–579. Available at: https://doi.org/10.1007/978-3-030-60248-2_38.

What exactly is Turing Completeness? - Evin Sellin - Medium (2017). Available at: https://medium.com/@evinsellin/what-exactly-is-turing-completeness-a08cc36b26e2

What is Cosmos? - Cosmos Network (no date). Available at: https://v1.cosmos.network/intro

Xiao, Y. *et al.* (2019) *Distributed Consensus Protocols and Algorithms*.

Xiao, Y. *et al.* (2020a) 'A Survey of Distributed Consensus Protocols for Blockchain Networks', *IEEE Communications Surveys and Tutorials*, 22(2), pp. 1432–1465. Available at: https://doi.org/10.1109/COMST.2020.2969706.

Xiao, Y. *et al.* (2020b) 'A Survey of Distributed Consensus Protocols for Blockchain Networks', *IEEE Communications Surveys Tutorials*, 22(2), p. 1. Available at: https://doi.org/10.1109/COMST.2020.2969706.

XRP | Ripple (2012). Available at: https://ripple.com/xrp/

XRP Ledger Overview - XRPL.org (no date). Available at: https://xrpl.org/xrp-ledger-overview.html#fast-efficient-consensus-algorithm

Yang, F. *et al.* (2019) 'Delegated proof of stake with downgrade: A secure and efficient blockchain consensus algorithm with downgrade mechanism', *IEEE Access*, 7, pp. 118541–118555. Available at: https://doi.org/10.1109/ACCESS.2019.2935149.

Yeow, K. *et al.* (2018) 'Decentralized Consensus for Edge-Centric Internet of Things: A Review, Taxonomy, and Research Issues', *IEEE Access*, 6, pp. 1513–1524. Available at: https://doi.org/10.1109/ACCESS.2017.2779263.

Zhao, W., Yang, S. and Luo, X. (2019) 'On consensus in public blockchains', in *ACM International Conference Proceeding Series*. New York, New York, USA: Association for Computing Machinery, pp. 1–5. Available at: https://doi.org/10.1145/3320154.3320162.

Zhu, X. *et al.* (2020) 'An improved proof-of-trust consensus algorithm for credible crowdsourcing blockchain services', *IEEE Access* [Preprint]. Available at: https://ieeexplore.ieee.org/abstract/document/9104671/.

Zoican, S. *et al.* (2018) 'Blockchain and Consensus Algorithms in Internet of Things', in *2018 13th International Symposium on Electronics and Telecommunications, ISETC 2018 - Conference Proceedings*, pp. 1–4. Available at: https://doi.org/10.1109/ISETC.2018.8583923.