

The copyright © of this thesis belongs to its rightful author and/or other copyright owner. Copies can be accessed and downloaded for non-commercial or learning purposes without any charge and permission. The thesis cannot be reproduced or quoted as a whole without the permission from its rightful owner. No alteration or changes in format is allowed without permission from its rightful owner.

**AN ADAPTIVE REPUTATION-BASED BYZANTINE FAULT
TOLERANCE CONSENSUS MECHANISM FOR NODE
PERFORMANCE EVALUATION AND LEADER SELECTION IN
PERMISSIONED BLOCKCHAIN SYSTEM**

NORSHAKINAH BINTI MD NASIR

**DOCTOR OF PHILOSOPHY
UNIVERSITI UTARA MALAYSIA
2025**



Awang Had Salleh
Graduate School
of Arts And Sciences

Universiti Utara Malaysia

PERAKUAN KERJA TESIS / DISERTASI
(Certification of thesis / dissertation)

Kami, yang bertandatangan, memperakukan bahawa
(We, the undersigned, certify that)

NORSHAKINAH MD NASIR

calon untuk Ijazah
(candidate for the degree of)

PhD

telah mengemukakan tesis / disertasi yang bertajuk:
(has presented his/her thesis / dissertation of the following title):

**“AN ADAPTIVE REPUTATION-BASED BYZANTINE FAULT TOLERANCE CONSENSUS
MECHANISM FOR NODE PERFORMANCE EVALUATION AND LEADER
SELECTION IN PERMISSIONED BLOCKCHAIN SYSTEM”**

seperti yang tercatat di muka surat tajuk dan kulit tesis / disertasi.
(as it appears on the title page and front cover of the thesis / dissertation).

Bahawa tesis/disertasi tersebut boleh diterima dari segi bentuk serta kandungan dan meliputi bidang ilmu dengan memuaskan, sebagaimana yang ditunjukkan oleh calon dalam ujian lisan yang diadakan pada : **04 Jun 2025**.

*That the said thesis/dissertation is acceptable in form and content and displays a satisfactory knowledge of the field of study as demonstrated by the candidate through an oral examination held on:
04 June 2025.*

Pengerusi Viva
(Chairman for Viva)

: **Prof. Dr. Huda Haji Ibrahim**

Tandatangan
(Signature)

Pemeriksa Luar
(External Examiner)

: **Prof. Ts. Dr. Salman Yussof**

Tandatangan
(Signature)

Pemeriksa Dalam
(Internal Examiner)

: **Assoc. Prof. Ts. Dr. Mohd. Hasbullah Omar**

Tandatangan
(Signature)

Nama Penyelia I
(Name of Supervisor I)

: **Prof. Ts. Dr. Suhaidi Hassan**

Tandatangan
(Signature)

Nama Penyelia II
(Name of Supervisor II)

: **Dr. Khuzairi Mohd Zaini**

Tandatangan
(Signature)

Tarikh:
(Date) **04 June 2025**

Permission to Use

In presenting this thesis in fulfilment of the requirements for a postgraduate degree from Universiti Utara Malaysia, I agree that the Universiti Library may make it freely available for inspection. I further agree that permission for the copying of this thesis in any manner, in whole or in part, for scholarly purpose may be granted by my supervisor(s) or, in their absence, by the Dean of Awang Had Salleh Graduate School of Arts and Sciences. It is understood that any copying or publication or use of this thesis or parts thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to Universiti Utara Malaysia for any scholarly use which may be made of any material from my thesis.

Requests for permission to copy or to make other use of materials in this thesis, in whole or in part, should be addressed to:

Dean of Awang Had Salleh Graduate School of Arts and Sciences
UUM College of Arts and Sciences
Universiti Utara Malaysia
06010 UUM Sintok

Abstrak

Rantainya blok berizin semakin banyak digunakan dalam persekitaran perusahaan kerana kawalan akses yang teratur dan kebenaran mengikut peranan. Walau bagaimanapun, protokol *Practical Byzantine Fault Tolerance* (PBFT) yang banyak digunakan mengalami ketidakcekapan dalam pemilihan pemimpin secara giliran (*round-robin*) dan tidak mempunyai mekanisme bersepadu untuk penilaian prestasi nod. Kelemahan ini membawa kepada penurunan kadar pemprosesan transaksi (*throughput*), peningkatan kependaman (*latency*), dan kekangan kebolehskalaan, terutamanya di bawah keadaan kesalahan Byzantine. Kajian ini bertujuan untuk mengatasi kekangan PBFT dalam pemilihan pemimpin dan penilaian prestasi dengan mencadangkan protokol *Adaptive Reputation-Based Byzantine Fault Tolerance* (ARepBFT). Hipotesisnya ialah dengan mengintegrasikan pemarkahan reputasi dinamik bersama pemilihan pemimpin berbilang kriteria secara adaptif, proses konsensus dapat mencapai tahap kecekapan dan kebolehpercayaan yang lebih tinggi, disamping mengekalkan toleransi kesalahan Byzantine dalam sistem rangkaian blok berizin. Menggunakan *Design Research Methodology* (DRM), ARepBFT mengintegrasikan dua modul utama: CRepScore, iaitu sistem berasaskan kredit untuk penilaian prestasi nod secara berterusan, dan RepTOPS-Lead, yang menggunakan kaedah membuat keputusan TOPSIS bagi tujuan pemilihan pemimpin. Protokol ini telah dilaksanakan dalam simulator NS-3 dengan logik konsensus terbenam dan dinilai berbanding PBFT serta *Random Cluster* PBFT (RC-PBFT) di bawah bilangan nod, beban transaksi, dan nisbah kesalahan Byzantine yang berbeza. ARepBFT menunjukkan kelebihan prestasi yang konsisten berbanding PBFT dan RC-PBFT dari segi kadar transaksi, kependaman, dan kebolehskalaan. Dalam konfigurasi nod dan saiz transaksi yang berbeza, ARepBFT mencapai sehingga 24% peningkatan kadar pemprosesan dan 19% pengurangan kependaman. Mekanisme ini juga telah meningkatkan prestasi di bawah ujian tekanan nod Byzantine dan mengurangkan pemilihan ketua yang tidak normal. Hasil kajian ini membuktikan keupayaan ARepBFT mengekalkan toleransi kesalahan Byzantine dalam persekitaran rangkaian blok yang dinamik. Kajian ini memajukan PBFT dengan memperkenalkan protokol konsensus yang adaptif serta peka terhadap prestasi, menyumbang secara teori kepada bidang toleransi kesalahan Byzantine dan secara praktikal kepada pelaksanaan rangkaian blok perusahaan. Hasil kajian ini mempunyai implikasi untuk sektor yang memerlukan sistem teragih yang selamat, boleh diskala, dan boleh dipercayai, sekali gus menyokong penerimaan masyarakat yang lebih meluas terhadap teknologi terdesentralisasi yang diyakini.

Kata kunci: Lejar teragih, Kaedah pusingan-robin, Operasi ubah-pandangan, Nod tidak normal, Toleransi kesalahan.

Abstract

Permissioned blockchains are increasingly adopted in enterprise environments due to their controlled access and role-specific permissions. However, the widely used Practical Byzantine Fault Tolerance (PBFT) protocol suffers from inefficiencies in round-robin leader selection and lacks integrated mechanisms for node performance evaluation. These weaknesses lead to reduced throughput, higher latency, and scalability constraints, particularly under Byzantine fault conditions. This study aims to overcome PBFT's leader selection and performance assessment limitations by proposing an Adaptive Reputation-Based Byzantine Fault Tolerance (AREpBFT) protocol. The hypothesis is that by integrating dynamic reputation scoring with adaptive multi-criteria leader selection, the consensus process can achieve higher efficiency and reliability, while maintaining Byzantine fault tolerance in permissioned blockchain systems. Using Design Research Methodology (DRM), AREpBFT integrates two key modules: CRepScore, a credit-based system for continuous node performance evaluation, and RepTOPS-Lead, which applies the TOPSIS decision-making method for leader selection. The protocol was implemented in the NS-3 simulator with embedded consensus logic and evaluated against PBFT and Random Cluster PBFT (RC-PBFT) under varied node counts, transaction loads, and Byzantine fault ratios. AREpBFT demonstrated consistent performance advantages over PBFT and RC-PBFT in throughput, latency, and scalability. Under varying node and transaction configurations, AREpBFT achieved up to 24% higher throughput and 19% lower latency. This mechanism has also improved performance under Byzantine node stress tests and reduced the selection of abnormal leaders. These results affirm AREpBFT's adaptive strength in maintaining Byzantine fault tolerance in dynamic blockchain environments. The research advances PBFT by introducing an adaptive, performance-aware consensus protocol, contributing theoretically to the field of Byzantine fault tolerance and practically to enterprise blockchain deployment. The results have implications for sectors requiring secure, scalable, and reliable distributed systems, supporting broader societal adoption of trustworthy decentralized technologies.

Keywords: Distributed ledger, Round-robin method, View-change operation, Abnormal node, Fault tolerance.

Acknowledgements

First and foremost, I express my deepest gratitude to Allah s.w.t. for His blessings on this journey full of lessons. I would like to express my sincere thanks to my esteemed supervisors, Prof. Ts. Dr. Suhaidi Hassan and Dr. Khuzairi Mohd Zaini, for their invaluable guidance, support, and encouragement throughout the course of my research. Their expertise and insights have been instrumental in shaping this thesis. I am also profoundly grateful to the InterNetWorks Research Laboratory (IRL), the School of Computing, and the Universiti Utara Malaysia for providing the necessary resources and a conducive environment for my research.

My heartfelt thanks go to my parents, Md. Nasir and Che Robayah, who always have faith in me and pray for my success. My warm thanks also go to my siblings for their unwavering support and belief in me. Special thanks to my dear husband, Mohd Nasrol, and our precious son and daughters, your love, support, and patience have been my source of strength and motivation.

I would like to express my appreciation to my IRL colleagues who have been a constant source of support and companionship. Your encouragement and assistance have been invaluable. To all of my special friends, I would like to express my sincere appreciation for your unwavering motivation and support that kept me going.

Thank you so much for being part of this journey, even during the most challenging times of my studies. Your collective efforts and camaraderie have been instrumental in my success.

Table of Contents

Permission to Use.....	i
Abstrak	ii
Abstract	iii
Acknowledgements.....	iv
Table of Contents	iv
List of Tables.....	ix
List of Figures	xi
List of Appendices.....	xiv
List of Abbreviations.....	xvi
CHAPTER ONE INTRODUCTION.....	1
1.1 Background of the Study	2
1.1.1 Overview of Blockchain Technology.....	3
1.1.2 Permissioned Blockchain.....	4
1.1.3 Consensus Mechanism.....	4
1.1.4 Practical Byzantine Fault Tolerance (PBFT)	6
1.2 Research Motivation	6
1.3 Problem Statement	9
1.4 Research Questions	12
1.5 Research Objectives	12
1.6 Scope of the Study	13
1.7 Significance of the Study	15
1.8 Organization of the Thesis	18
CHAPTER TWO LITERATURE REVIEW	20
2.1 Blockchain Architecture and Core Components	20
2.1.1 Blockchain Applications and Use Cases.....	23
2.2 Classification of Blockchain Networks.....	25
2.2.1 Permissioned Blockchain.....	28
2.2.2 Existing Permissioned Blockchain Platforms	30

2.3	Fundamentals of Consensus Mechanism in Blockchain	31
2.3.1	Consensus mechanisms in permissioned blockchain-based systems .	34
2.3.2	Byzantine Fault Tolerance (BFT)	36
2.3.2.1	Delegated Byzantine Fault Tolerance (dBFT).....	38
2.3.2.2	Federated Byzantine Fault Tolerance (FBFT).....	39
2.3.3	Scalability Challenges of BFT-based Consensus Mechanism in Permissioned Blockchain.....	40
2.4	Practical Byzantine Fault Tolerance (PBFT).....	42
2.4.1	Working Principle of PBFT.....	44
2.4.1.1	View-Change: The Leader Replacement	46
2.4.1.2	Leader Replacement in PBFT.....	47
2.5	Critical Review: Limitations of PBFT	48
2.5.1	Scalability	49
2.5.2	Lack of Node Performance Consideration	50
2.5.3	Ineffectiveness of Leader Node Selection in the View-change Case..	51
2.6	Related Works	53
2.6.1	Synthesis of PBFT Enhancement Literature: Patterns and Gaps	65
2.7	Approaches Applicable in This Study	67
2.7.1	Reputation-based Evaluation System for Nodes Performance	68
2.7.2	TOPSIS Method for Leader Node Selection.....	70
2.8	Summary	74
 CHAPTER THREE RESEARCH METHODOLOGY.....		75
3.1	Research Approach	77
3.2	Analysis.....	78
3.2.1	Research Clarification (RC)	79
3.2.2	Descriptive Study-I (DS-I)	81
3.2.2.1	Conceptual Model of the ARepBFT consensus Mechanism	82
3.3	Design.....	86
3.4	Experimentation	88
3.4.1	Verification and Validation.....	90
3.5	Evaluation	94

3.5.1	Evaluation Approach Consideration	95
3.5.2	Evaluation Environment	97
3.5.2.1	Network Simulator 3 (NS-3)	99
3.5.2.2	Experiments Steps	100
3.5.2.3	Experiment Setup	101
3.5.3	Performance Metrics	106
3.6	Summary	110
CHAPTER FOUR AREPBFT DESIGN AND IMPLEMENTATION.....		112
4.1	ARepBFT: An Overview	113
4.2	Design Principles of ARepBFT	115
4.2.1	Reputation-based Evaluation System.....	115
4.2.2	Integration of Multi-Criteria Decision Making (MCDM) and Reputation-based System.....	117
4.3	Implementation of ARepBFT	122
4.3.1	System model	123
4.3.1.1	Network Environment.....	124
4.4	Credit-based Reputation Scoring Scheme (CRepScore)	128
4.4.1	Ranking Score Table (RST) Generation	132
4.4.2	Node Rank Determination	135
4.4.3	Node Score Computation.....	137
4.4.4	Node Status Determination	140
4.4.4.1	Consensus Nodes Exclude and Inclusion	144
4.4.5	CRepScore Verification and Validation	146
4.4.5.1	Verification of CRepScore	146
4.4.5.2	Validation of CRepScore	147
4.4.5.2.1	Validation of the Ranking Score Table Generation	148
4.4.5.2.2	Validation of the results.....	150
4.5	Reputation-based Technique for Order of Preference by Similarity to Ideal Solution for Leader Node Selection Scheme (RepTOPS-Lead).....	152
4.5.1	Leader Node Selection	155

4.5.2	A Computational Example of the Process in RepTOPS-Lead.....	159
4.5.3	Verification of RepTOPS-Lead	167
4.5.4	Validation of RepTOPS-Lead	168
4.5.4.1	Scenario 1: Impact of Abnormal Nodes on the Probability of Abnormal Leader.....	171
4.5.4.2	Scenario 2: Impact of Network Size on the Probability of Abnormal Leader	174
4.5.4.3	Scenario 3: Impact of Network Load on the Probability Abnormal Leader.....	177
4.5.4.4	Discussion on the Validation of ARepBFT	179
4.6	Summary	180

**CHAPTER FIVE PERFORMANCE ANALYSIS AND EVALUATION
OF AREPBFT182**

5.1	ARepBFT: A Review	183
5.2	Performance Evaluation of ARepBFT	186
5.2.1	Simulation Scenarios	189
5.2.2	Scenario 1: Simulation Using Different Number of Consensus Nodes	190
5.2.2.1	Performance Evaluation of ARepBFT versus PBFT and RC-PBFT across Different Number of Consensus Nodes..	193
5.2.3	Scenario 2: Simulation Using Different Transaction Sizes	199
5.2.3.1	Performance Evaluation of ARepBFT versus PBFT and RC-PBFT across Different Transaction Sizes	202
5.2.4	Scenario 3: Simulation in the Presence of Byzantine Nodes	209
5.2.4.1	Performance Evaluation of ARepBFT versus PBFT and RC-PBFT in the Presence of Byzantine Nodes	212
5.2.5	Discussion on ARepBFT Performance	219
5.2.5.1	Scalability Analysis	221
5.3	Summary	227

CHAPTER SIX CONCLUSION AND FUTURE WORK229

6.1	Summary of Research	229
6.2	Research Contribution.....	232

6.3	Research Limitations	234
6.4	Recommendations for Future Work.....	236
	REFERENCES	238

List of Tables

Table 2.1	<i>Permissionless Vs Permissioned Blockchain</i>	30
Table 2.2	<i>Comparison Table of PBFT Related Works</i>	62
Table 3.1	<i>Comparison of Performance Evaluation Techniques</i>	96
Table 3.2	<i>Specification and Configuration of the Host Computer for Simulation Setting</i>	102
Table 4.1	<i>Explanation of Notations used in the System</i>	130
Table 4.2	<i>Node Status and Authority Assignment Setting Table</i>	142
Table 4.3	<i>Table of Decision Matrix and Examples of Data Values</i>	160
Table 4.4	<i>Computation of r_{ij} for C_1</i>	161
Table 4.5	<i>Computation of r_{ij} for C_2</i>	161
Table 4.6	<i>Computation of r_{ij} for C_3</i>	162
Table 4.7	<i>Normalized Decision Matrix</i>	162
Table 4.8	<i>The Weighted Normalized Decision Matrix</i>	163
Table 4.9	<i>The Computation of the Separation Measures for PIS</i>	164
Table 4.10	<i>The Computation of the Separation Measures for NIS</i>	165
Table 4.11	<i>The Computation of the TOPSIS Score (Closeness Coefficient)</i>	166
Table 4.12	<i>The Configuration of the Scenario Environment</i>	170
Table 4.13	<i>Experiment Result of Probability Abnormal Leader Nodes for Scenario 1</i>	171
Table 4.14	<i>Experiment Result of Probability Abnormal Leader Nodes for Scenario 2</i>	175
Table 4.15	<i>Experiment Result of Probability Abnormal Leader Nodes for Scenario 3</i>	177
Table 4.16	<i>A Comparative Analysis of BFT-based Leader Election Methods</i>	181
Table 5.1	<i>Simulation Parameters for Different Number of Consensus Nodes Scenario</i>	192
Table 5.2	<i>Experimental Result of Transaction Throughput (TPS) for Scenario 1</i>	194
Table 5.3	<i>Experimental Result of Transaction Latency (ms) for Scenario 1</i>	197

Table 5.4	<i>Simulation Parameters for Different Transaction Sizes Scenario</i>	201
Table 5.5	<i>Experimental Result of Transaction Throughput (TPS) for Scenario 2</i>	203
Table 5.6	<i>Experimental Result of Transaction Latency (ms) for Scenario 2</i>	206
Table 5.7	<i>Simulation Parameters in the Presence of Byzantine Nodes Scenario</i> ..	211
Table 5.8	<i>Experimental Result of Transaction Throughput (TPS) for Scenario 3</i> ..	213
Table 5.9	<i>Experimental Result of Transaction Latency (ms) for Scenario 3</i>	216
Table 5.10	<i>Summary of Throughput Performance Scalability Scaling with Transaction Size (%)</i>	222
Table 5.11	<i>Summary of Throughput Performance Scalability with Network Nodes (%)</i>	224

List of Figures

Figure 1.1	Scope of the study	14
Figure 2.1	The core components of the blockchain system [54]	21
Figure 2.2	The structure of the block in the blockchain [55]	22
Figure 2.3	A comprehensive overview of the blockchain transaction workflow that describes the step-by-step process of a blockchain transaction, from start to finish [7], [58], [59]	23
Figure 2.4	The framework of a blockchain-based supply chain [71]	25
Figure 2.5	"Normal Case Operation" of PBFT [37], [19]	45
Figure 2.6	A round-robin method for replacing the leader node during the view-change process in PBFT	49
Figure 2.7	Visual map of literature review	67
Figure 2.8	Steps in TOPSIS method	72
Figure 3.1	Research Approach	79
Figure 3.2	Main steps in Research Clarification (RC)	80
Figure 3.3	Steps in Descriptive Study-I (DS-I)	82
Figure 3.4	Conceptual model of ARepBFT	84
Figure 3.5	The development process of the schemes	87
Figure 3.6	The steps of Verification and Validation	93
Figure 3.7	Simulation steps	100
Figure 3.8	Visual Studio Code IDE loaded with the Blockchain Simulator NS-3	103
Figure 4.1	System model of ARepBFT in permissioned blockchain for supply chain enterprise	126
Figure 4.2	The overall processes of the ARepBFT consensus mechanism	129
Figure 4.3	The working flow of the CRepScore scheme for consensus nodes reputation evaluation	132
Figure 4.4	The output of the RS_L for 20 Consensus Nodes	135
Figure 4.5	The output of the RS_L for 30 consensus nodes	135
Figure 4.6	The output of the "Node Rank Determination"	137

Figure 4.7	Node score calculation	140
Figure 4.8	Node status determination	144
Figure 4.9	The process of the node state transition in CRepScore	145
Figure 4.10	CRepScore verification	147
Figure 4.11	The dynamic changes of ranking score table for 20 and 30 nodes	148
Figure 4.12	The validation of CRepScore.....	151
Figure 4.13	Leader node selection by RepTOPS-Lead for view-change case.....	155
Figure 4.14	Leader node replacement in RepTOPS-Lead.....	159
Figure 4.15	RepTOPS-Lead verification	168
Figure 4.16	Leader node selection	168
Figure 4.17	Changes in the number of abnormal leader nodes with the different number of abnormal nodes assigned.....	173
Figure 4.18	Changes in the probability of abnormal leader nodes with the different number of abnormal nodes assigned	173
Figure 4.19	Changes in the number of abnormal leader nodes with the different number of consensus nodes.....	176
Figure 4.20	Changes in the probability of abnormal leader nodes with the different number of consensus nodes.....	176
Figure 4.21	Changes in the number of abnormal leader nodes with the different size of transactions.....	178
Figure 4.22	Changes in the probability of abnormal leader nodes with the different size of transactions.....	178
Figure 5.1	Comprehensive overview of ARepBFT consensus process with view-change case.....	185
Figure 5.2	Comparison of consensus throughput under different number of consensus nodes	194
Figure 5.3	Comparison of transaction latency under different number of consensus nodes	197
Figure 5.4	Comparison of consensus throughput under different number of transactions	203

Figure 5.5	Comparison of transaction latency time under different size of transactions	206
Figure 5.6	Throughput comparison in the presence of Byzantine nodes.....	213
Figure 5.7	Latency comparison in the presence of Byzantine nodes.....	217
Figure 5.8	Scalability analysis of throughput scaling with transaction size	222
Figure 5.9	Scalability Analysis	224

List of Appendices

Appendix A	The TOPSIS Steps for Leader Selection in RepTOPS-Lead254
Appendix B	Calculation of Decision Criteria Weights Using the Entropy Method in RepTOPS-Lead ...257

List of Abbreviations

BFT	Byzantine Fault Tolerance
BGP	Byzantine General Problem
CFT	Crash Fault Tolerant
CRepScore	Credit-Based Reputation Scoring Scheme
DBFT	Delegated Byzantine Fault Tolerance
DLT	Distributed Ledger Technology
DPoS	Delegated Proof of Stake
ARepBFT	Adaptive Reputation-based Byzantine Fault-Tolerance
DRM	Design Research Methodology
DS-I	Descriptive Study-I
DS-II	Descriptive Study-II
FBA	Federated Byzantine Agreement
FBFT	Federated Byzantine Fault Tolerance
Industry 4.0	The Fourth Industrial Revolution
MCDM	Multi-Criteria Decision Making
NS-3	Network Simulator 3
OASC	Organic Agricultural Supply Chain
P2P	Peer-to-peer
PBFT	Practical Byzantine Fault Tolerance
PoS	Proof of Stake
PoW	Proof of Work
PS	Prescriptive Study
RC	Research Clarification
RepTOPS-Lead	Reputation-based Technique for Order of Preference by Similarity to Ideal Solution for Leader Node Selection Scheme
SMR	State Machine Replication
TPS	Transactions per second
TOPSIS	Technique for Order Preference by Similarity to an Ideal Solution

CHAPTER ONE

INTRODUCTION

Within the context of the Fourth Industrial Revolution (Industry 4.0), blockchain represents an innovative technology currently being considered for integration into a digital industrial system. The permissioned blockchain was developed as an alternative to the public blockchain, specifically designed to meet the demand for deployment in industry-specific business networks with private transactions that require transaction throughput and low latency [1]. Most consensus protocols in permissioned blockchain systems are grounded in Byzantine Fault Tolerance (BFT), originating from solutions to the Byzantine Generals Problem (BGP) [2], [3]. Practical Byzantine Fault Tolerance (PBFT) is among the prevalent BFT-based consensus mechanisms. Although PBFT is theoretically intended to handle Byzantine faults, it is challenged by its high communication complexity and inherent inefficiencies. These result in network scalability problems, characterized by increased latency and reduced throughput as the network size increases, hindering its effectiveness in larger networks. In addition, PBFT was confronted with the lack of consensus node evaluation and the ineffectiveness of round-robin leader replacement during view-change operations. The main research objective of this study is to develop a consensus mechanism that includes the ability to evaluate consensus nodes and improve the selection of the leader node during view-change case in a permissioned-blockchain environment.

This chapter describes this study within its context, where the general background of the research is briefly described. This chapter begins with a preliminary overview of blockchain technology, research background, and the research challenges in Section 1.1. Section 1.2 explores several factors that motivate the need for studying the design and concept behind the blockchain consensus mechanism, specifically for the reputation evaluation of the nodes and the selection of the leader node. The problem

REFERENCES

- [1] I. Surjandari, H. Yusuf, E. Laoh, and R. Maulida, “Designing a permissioned blockchain network for the halal industry using hyperledger fabric with multiple channels and the raft consensus mechanism,” *Journal of Big Data*, vol. 8, no. 1, pp. 1–16, 2021.
- [2] N. Z. Tomić, “A review of consensus protocols in permissioned blockchains,” *Journal of Computer Science Research*, vol. 3, no. 2, pp. 32–39, 2021.
- [3] P. Hooda, “practical byzantine fault tolerance(pbft),” Accessed August. 27, 2023, 2022. [Online]. Available: <https://www.geeksforgeeks.org/practical-byzantine-fault-tolerancepbft/>
- [4] M. Alazab and S. Alhyari, “Industry 4.0 innovation: A systematic literature review on the role of blockchain technology in creating smart and sustainable manufacturing facilities,” *Information*, vol. 15, no. 2, p. 78, 2024.
- [5] T. Alladi, V. Chamola, R. M. Parizi, and K.-K. R. Choo, “Blockchain applications for industry 4.0 and industrial iot: A review,” *IEEE Access*, vol. 7, pp. 176 935–176 951, 2019.
- [6] I. Meidute-Kavaliauskiene, B. Yıldız, Ş. Çiğdem, and R. Činčikaitė, “An integrated impact of blockchain on supply chain applications,” *Logistics*, vol. 5, no. 2, p. 33, 2021.
- [7] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das, “Everything you wanted to know about the blockchain: Its promise, components, processes, and problems,” *IEEE Consumer Electronics Magazine*, vol. 7, no. 4, pp. 6–14, 2018.
- [8] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” *Decentralized Business Review*, p. 21260, 2008.
- [9] R. da Rosa Righi, A. M. Alberti, and M. Singh, *Blockchain Technology for Industry 4.0*. Springer, 2020.
- [10] K. E. Wegrzyn and E. Wang, “Types of blockchain: Public, private, or something in between,” 2021. [Online]. Available: <https://www.foley.com/en/insights/publications/2021/08/types-of-blockchain-public-private-between>
- [11] L. G. Jaeger. Public versus private: What to know before getting started with blockchain. (2018). [Online]. Available: <https://www.ibm.com/blogs/blockchain/2018/10/public-versus-private-what-to-know-before-getting-started-with-blockchain/>
- [12] H. Fu, C. Zhao, C. Cheng, and H. Ma, “Blockchain-based agri-food supply chain management: case study in China,” *International Food and Agribusiness Management Review*, vol. 23, no. 5, pp. 667–679, 2020.

- [13] IBM. What is blockchain security? (2022). [Online]. Available: <https://www.ibm.com/topics/blockchain-security>
- [14] V. Chawla. What are the top blockchain consensus algorithms? (2020). [Online]. Available: <https://analyticsindiamag.com/blockchain-consensus-algorithms/>
- [15] G. Iredale. Introduction to Permissioned Blockchains. (2019, June 02). [Online]. Available: <https://101blockchains.com/permissioned-blockchain/>
- [16] V. Hassija, S. Zeadally, I. Jain, A. Tahiliani, V. Chamola, and S. Gupta, "Framework for determining the suitability of blockchain: Criteria and issues to consider," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 10, p. e4334, 2021.
- [17] A. Baliga, "Understanding blockchain consensus models," *Persistent*, vol. 4, no. 1, p. 14, 2017.
- [18] D. P. Oyinloye, J. S. Teh, N. Jamil, and M. Alawida, "Blockchain consensus: An overview of alternative protocols," *Symmetry*, vol. 13, no. 8, p. 1363, 2021.
- [19] S. Zhang and J. H. Lee, "Analysis of the main consensus protocols of blockchain," *ICT Express*, vol. 6, no. 2, pp. 93–97, jun 2020.
- [20] S. Rouhani, "Data trust framework using blockchain and smart contracts," Ph.D. dissertation, University of Saskatchewan, 2021.
- [21] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *International journal of web and grid services*, vol. 14, no. 4, pp. 352–375, 2018.
- [22] H. Buch, "Improving performance and scalability of blockchain networks," [www.wipro.com. https://www.wipro.com/blogs/hitarshi-buch/improving-performance-and-scalability-of-blockchain-networks/](https://www.wipro.com/blogs/hitarshi-buch/improving-performance-and-scalability-of-blockchain-networks/), (accessed Sept. 29, 2022).
- [23] P. Swathi and M. Venkatesan, "Scalability improvement and analysis of permissioned-blockchain," *ICT Express*, vol. 7, no. 3, pp. 283–289, 2021.
- [24] N. Gaur, A. O'Dowd, P. Novotny, L. Desrosiers, V. Ramakrishna, and S. A. Baset, *Blockchain with hyperledger fabric: Build decentralized applications using hyperledger fabric 2*. Packt Publishing Ltd, 2020.
- [25] S. Gupta, S. Rahnama, and M. Sadoghi, "Permissioned blockchain through the looking glass: Architectural and implementation lessons learned," in *2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS)*. IEEE, 2020, pp. 754–764.
- [26] L. Lamport, "Time, clocks, and the ordering of events in a distributed system," *Communications*, 1978.

- [27] F. B. Schneider, “Implementing fault-tolerant services using the state machine approach: A tutorial,” *ACM Computing Surveys (CSUR)*, vol. 22, no. 4, pp. 299–319, 1990.
- [28] Cointelegraph, “Permissioned blockchain vs. permissionless blockchain: Key differences,” Accessed August. 21, 2022 [Online]. [Online]. Available: <https://cointelegraph.com/blockchain-for-beginners/>
- [29] A. Technologies. Solving the “Blockchain Trilemma”. (2023, Oct 29). [Online]. Available: <https://algorandtechnologies.com/technology/solving-the-blockchain-trilemma>
- [30] A. Hafid, A. S. Hafid, and M. Samih, “Scaling blockchains: A comprehensive survey,” *IEEE Access*, vol. 8, pp. 125 244–125 262, 2020.
- [31] X. Zhang, M. Xue, and X. Miao, “A consensus algorithm based on risk assessment model for permissioned blockchain,” *Wireless Communications and Mobile Computing*, vol. 2022, 2022.
- [32] M. Castro and B. Liskov, “Practical byzantine fault tolerance and proactive recovery,” *ACM Transactions on Computer Systems (TOCS)*, vol. 20, no. 4, pp. 398–461, 2002.
- [33] M. T. de Oliveira, L. H. Reis, D. S. Medeiros, R. C. Carrano, S. D. Olabarriaga, and D. M. Mattos, “Blockchain reputation-based consensus: A scalable and resilient mechanism for distributed mistrusting applications,” *Computer Networks*, vol. 179, p. 107367, 2020.
- [34] C. Yang, T. Wang, and K. Wang, “A consensus mechanism based on an improved genetic algorithm,” *Open Access Library Journal*, vol. 7, no. 9, pp. 1–6, 2020.
- [35] M. S. Salisu, “Practical byzantine fault tolerance (pbft) in blockchain,” Accessed Sept. 22, 2023, 2023. [Online]. Available: <https://www.linkedin.com/pulse/practical-byzantine-fault-tolerance-pbft-blockchain-m-seun-salisu->
- [36] L. Lamport, “Proving the correctness of multiprocess programs,” *IEEE transactions on software engineering*, no. 2, pp. 125–143, 1977.
- [37] M. Castro, B. Liskov *et al.*, “Practical byzantine fault tolerance,” in *OsDI*, vol. 99, no. 1999, 1999, pp. 173–186.
- [38] K. Khullar, “Implementing pbft in blockchain,” Accessed August. 27, 2023, 2019. [Online]. Available: <https://medium.com/coinmonks/implementing-pbft-in-blockchain-12368c6c9548>
- [39] G. Zhang, F. Pan, S. Tijanac, and H.-A. Jacobsen, “Prestigebft: Revolutionizing view changes in bft consensus algorithms with reputation mechanisms,” *arXiv preprint arXiv:2307.08154*, 2023.
- [40] “Implementing practical byzantine fault tolerance (pbft),” 2023, accessed: 2024-01-15. [Online]. Available: <https://sgibala.com/02-01-implementing-pbft/>

- [41] Q. Zhou, H. Huang, Z. Zheng, and J. Bian, "Solutions to scalability of blockchain: A survey," *Ieee Access*, vol. 8, pp. 16 440–16 455, 2020.
- [42] "The blockchain trilemma: Fast, secure, and scalable networks," [gemini.com. https://www.gemini.com/cryptopedia/blockchain-trilemma-decentralization-scalability-definition](https://www.gemini.com/cryptopedia/blockchain-trilemma-decentralization-scalability-definition), (accessed Oct. 08, 2022).
- [43] D. Khan, L. T. Jung, and M. A. Hashmani, "Systematic literature review of challenges in blockchain scalability," *Applied Sciences*, vol. 11, no. 20, p. 9372, 2021.
- [44] X. Yu, J. Qin, and P. Chen, "Gpbft: A practical byzantine fault-tolerant consensus algorithm based on dual administrator short group signatures," *Security and Communication Networks*, vol. 2022, 2022.
- [45] K. Lei, Q. Zhang, L. Xu, and Z. Qi, "Reputation-based byzantine fault-tolerance for consortium blockchain," in *2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS)*, 2018, pp. 604–611.
- [46] S. Liu, R. Zhang, C. Liu, and D. Shi, "P-pbft: An improved blockchain algorithm to support large-scale pharmaceutical traceability," *Computers in biology and medicine*, vol. 154, p. 106590, 2023.
- [47] M. Hussain, A. Mehmood, M. A. Khan, R. Khan, and J. Lloret, "Reputation-based leader selection consensus algorithm with rewards for blockchain technology," *Computers*, vol. 14, no. 1, p. 20, 2025.
- [48] S. Liu, R. Zhang, C. Liu, C. Xu, and J. Wang, "An improved pbft consensus algorithm based on grouping and credit grading," *Scientific Reports*, vol. 13, no. 1, p. 13030, 2023.
- [49] N. Jiang, F. Bai, L. Huang, Z. An, and T. Shen, "Reputation-driven dynamic node consensus and reliability sharding model in iot blockchain," *Algorithms*, vol. 15, no. 2, p. 28, 2022.
- [50] D. Huang, Y. Huang, and Y. Yang, "Improved pbft consensus algorithm based on node evaluation and dynamic management," in *Proceedings of the 2023 4th International Conference on Big Data Economy and Information Management*, 2023, pp. 851–855.
- [51] J. Zhang, Y. Yang, D. Zhao, and Y. Wang, "A node selection algorithm with a genetic method based on pbft in consortium blockchains," *Complex & Intelligent Systems*, vol. 9, no. 3, pp. 3085–3105, 2023.
- [52] H. Qin, Y. Cheng, X. Ma, F. Li, and J. Abawajy, "Weighted byzantine fault tolerance consensus algorithm for enhancing consortium blockchain efficiency and security," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 10, pp. 8370–8379, 2022.
- [53] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," *Telematics and informatics*, vol. 36, pp. 55–81, 2019.

- [54] P. W. Khan and Y. Byun, "A blockchain-based secure image encryption scheme for the industrial internet of things," *Entropy*, vol. 22, no. 2, p. 175, 2020.
- [55] Y.-C. Chen, Y.-P. Chou, and Y.-C. Chou, "An image authentication scheme using merkle tree mechanisms," *Future Internet*, vol. 11, no. 7, p. 149, 2019.
- [56] J. Zhang, "Deploying blockchain technology in the supply chain," in *Computer Security Threats*. IntechOpen London, 2019, p. 57.
- [57] Savjee, "How does a blockchain work - simply explained," savjee.be. <https://savjee.be/videos/simply-explained/how-does-a-blockchain-work/>, (accessed Sept. 13, 2022).
- [58] N. M. Nasir, S. Hassan, K. M. Zaini, and N. Nordin, "Blockchain trust impact in agribusiness supply chain: a survey, challenges, and directions," in *2022 IEEE Region 10 Symposium (TENSYP)*. IEEE, 2022, pp. 1–6.
- [59] A. M. S. Saleh, "Blockchain for secure and decentralized artificial intelligence in cybersecurity: A comprehensive review," *Blockchain: Research and Applications*, vol. 5, no. 3, p. 100193, 2024.
- [60] M. J. M. Chowdhury, A. Colman, M. A. Kabir, J. Han, and P. Sarda, "Blockchain versus database: a critical analysis," in *2018 17th IEEE International conference on trust, security and privacy in computing and communications/12th IEEE international conference on big data science and engineering (TrustCom/BigDataSE)*. IEEE, 2018, pp. 1348–1353.
- [61] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "Medrec: Using blockchain for medical data access and permission management," in *2016 2nd international conference on open and big data (OBD)*. IEEE, 2016, pp. 25–30.
- [62] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, and F. Wang, "Secure and trustable electronic medical records sharing using blockchain," in *AMIA annual symposium proceedings*, vol. 2017. American Medical Informatics Association, 2017, p. 650.
- [63] M. Turkanović, M. Hölbl, K. Košič, M. Heričko, and A. Kamišalić, "Eductx: A blockchain-based higher education credit platform," *IEEE access*, vol. 6, pp. 5112–5127, 2018.
- [64] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, "Blockchain: A distributed solution to automotive security and privacy," *IEEE communications magazine*, vol. 55, no. 12, pp. 119–125, 2017.
- [65] M. Samaniego, U. Jamsrandorj, and R. Deters, "Blockchain as a service for iot," in *2016 IEEE international conference on internet of things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData)*. IEEE, 2016, pp. 433–436.

- [66] I. Konstantinidis, G. Siaminos, C. Timplalexis, P. Zervas, V. Peristeras, and S. Decker, “Blockchain for business applications: A systematic literature review,” in *International conference on business information systems*. Springer, 2018, pp. 384–399.
- [67] IBM. What is blockchain for business? (2022). [Online]. Available: <https://www.ibm.com/topics/blockchain-for-business>
- [68] M. S. Al-Rakhami and M. Al-Mashari, “A blockchain-based trust model for the internet of things supply chain management,” *Sensors*, vol. 21, no. 5, p. 1759, 2021.
- [69] S. Hu, S. Huang, J. Huang, and J. Su, “Blockchain and edge computing technology enabling organic agricultural supply chain: A framework solution to trust crisis,” *Computers and Industrial Engineering*, vol. 153, 3 2021.
- [70] J. Nation, “Walmart tests food safety with blockchain traceability,” *Abgerufen unter (10.09. 2018):* <https://www.ethnews.com/walmart-testsfood-safety-with-blockchaintraceability>, 2017.
- [71] ScienceSoft., “Blockchain for supply chain,” <https://www.scensoft.com/blockchain/supply-chain>, 2023.
- [72] G. M. Bakvand, “The impact of blockchain technology on trust in the supply chain,” Master’s thesis, Lund University, Sweden, 2019.
- [73] M. Alharby and A. van Moorsel, “Blocksim: An extensible simulation tool for blockchain systems,” *Frontiers in Blockchain*, vol. 3, p. 28, 2020.
- [74] G. D. Monte, D. Pennino, and M. Pizzonia, “Scaling blockchains without giving up decentralization and security: A solution to the blockchain scalability trilemma,” in *Proceedings of the 3rd Workshop on Cryptocurrencies and Blockchains for Distributed Systems*, 2020, pp. 71–76.
- [75] K. Aliche, A. Davies, M. Leopoldseder, and A. Niemeyer, “Blockchain technology for supply chains—a must or a maybe?” *McKinsey*, September, 2017.
- [76] L. G. Jaeger, “Public versus private: What to know before getting started with blockchain,” Accessed: September 17, 2022, 2018. [Online]. Available: <https://www.ibm.com/blogs/blockchain/2018/10/public-versus-private-what-to-know-before-getting-started-with-blockchain/>
- [77] E. Shein. How blockchain changes the nature of trust - linux foundation. (2019). [Online]. Available: <https://www.linuxfoundation.org/blog/how-blockchain-changes-the-nature-of-trust/>
- [78] V. Buterin, “On public and private blockchains,” <https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/>, 2015, accessed: 2024, Sept 10.
- [79] A. M. Antonopoulos and G. Wood, *Mastering Ethereum: Building Smart Contracts and DApps*. O’Reilly Media, 2018.

- [80] “What is blockchain technology?” <https://www.ibm.com/my-en/topics/what-is-blockchain>, accessed: 2021-12-30.
- [81] J. Howell. How To Implement A Permissioned Blockchain? (2024, Sept 20). [Online]. Available: <https://101blockchains.com/best-practices-for-implementing-permissioned-blockchain/>
- [82] M. Gupta, *Blockchain for dummies, 3rd IBM Limited Edition*. John Wiley & Sons, 2020.
- [83] S. Verma, D. Yadav, and G. Chandra, “Introduction of formal methods in blockchain consensus mechanism and its associated protocols,” *IEEE Access*, vol. 10, pp. 66 611–66 624, 2022.
- [84] “The future of financial markets is digital,” Accessed Sept. 22, 2024, 2024. [Online]. Available: <https://r3.com/>
- [85] C. V. Helliar, L. Crawford, L. Rocca, C. Teodori, and M. Veneziani, “Permissionless and permissioned blockchain diffusion,” *International Journal of Information Management*, vol. 54, p. 102136, 2020.
- [86] M. Soelman, “Permissioned blockchains: A comparative study,” Ph.D. dissertation, Faculty of Science and Engineering, University of Groningen, 2021.
- [87] “Quorum blockchain,” Accessed Oct. 22, 2024, 2023. [Online]. Available: <https://www.geeksforgeeks.org/quorum-blockchain/>
- [88] H. Foundation. (2025). [Online]. Available: <https://www.hyperledger.org/>
- [89] T. L. Foundation. Decentralized innovation. built on trust. (2025). [Online]. Available: <https://www.linuxfoundation.org/>
- [90] J. Kwon, “Tendermint: Consensus without mining,” *Draft v. 0.6, fall*, vol. 1, no. 11, pp. 1–11, 2014.
- [91] D. Reed, J. Law, and D. Hardman, “The technical foundations of sovryn,” *The Technical Foundations of Sovryn*, 2016.
- [92] T. L. Foundation. Hyperledger Iroha. (2025). [Online]. Available: <https://www.lfdecentralizedtrust.org/projects/iroha>
- [93] K. Olson, M. Bowman, J. Mitchell, S. Amundson, D. Middleton, and C. Montgomery, “Sawtooth: an introduction,” *The Linux Foundation*, p. 10, 2018.
- [94] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich *et al.*, “Hyperledger fabric: a distributed operating system for permissioned blockchains,” in *Proceedings of the thirteenth EuroSys conference*, 2018, pp. 1–15.
- [95] Hyperledger. Hyperledger Fabric. (2022, Oct 29). [Online]. Available: <https://hyperledger-fabric.readthedocs.io/en/latest/whatis.html>

- [96] T. L. Foundation. Hyperledger Besu. (2025). [Online]. Available: <https://www.lfdecentralizedtrust.org/projects/besu>
- [97] A. Altarawneh, “Liveness analysis, modeling, and simulation of blockchain consensus algorithms’ ability to tolerate malicious miners,” Ph.D. dissertation, University of Tennessee at Chattanooga, 2021.
- [98] K. Saito and H. Yamada, “What’s so different about blockchain? — blockchain is a probabilistic state machine,” in *2016 IEEE 36th International Conference on Distributed Computing Systems Workshops (ICDCSW)*, 2016, pp. 168–175.
- [99] C. Cachin and M. Vukolic, “Blockchain consensus protocols in the wild,” *arXiv preprint arXiv:1707.01873*, 2017.
- [100] G.-T. Nguyen and K. Kim, “A survey about consensus algorithms used in blockchain,” *Journal of Information processing systems*, vol. 14, no. 1, pp. 101–128, 2018.
- [101] S. Pahlajani, A. Kshirsagar, and V. Pachghare, “Survey on private blockchain consensus algorithms,” in *2019 1st International Conference on Innovations in Information and Communication Technology (ICIICT)*. IEEE, 2019, pp. 1–6.
- [102] S. Sayeed and H. Marco-Gisbert, “Assessing blockchain consensus and security mechanisms against the 51% attack,” *Applied sciences*, vol. 9, no. 9, p. 1788, 2019.
- [103] B. Parma, “Blockchain consensus mechanisms: A primer for supervisors,” IMF Fintech Note 22/03, Tech. Rep., 2022.
- [104] R. Chamria, “Consensus mechanisms for permissioned blockchain protocols,” Accessed Sept. 7, 2023, 2023. [Online]. Available: <https://community.nasscom.in/communities/blockchain/consensus-mechanisms-permissioned-blockchain-protocols>
- [105] Naveen. Significance of Permissioned Blockchains. (2019, Jan 7). [Online]. Available: <https://www.cashapona.com/2019/01/07/significance-of-permissioned-blockchains/>
- [106] W. Yao, J. Ye, R. Murimi, and G. Wang, “A survey on consortium blockchain consensus mechanisms,” *arXiv preprint arXiv:2102.12058*, 2021.
- [107] L. S. Sankar, M. Sindhu, and M. Sethumadhavan, “Survey of consensus protocols on blockchain applications,” in *2017 4th international conference on advanced computing and communication systems (ICACCS)*. IEEE, 2017, pp. 1–5.
- [108] R. Chami, “Your journey to consensus (part 1) — crash fault tolerance and paxos,” Accessed August. 27, 2023, 2019. [Online]. Available: <https://medium.com/@chamirachid/your-journey-to-consensus-part-1-6a88a6f818f6>
- [109] L. Lamport, R. Shostak, and M. Pease, “The byzantine generals problem,” *ACM Transactions on Programming Languages and Systems (TOPLAS)*, vol. 4, no. 3, p. 382 – 401, 1982.

- [110] P.-L. Wang, T.-W. Chao, C.-C. Wu, and H.-C. Hsiao, “Tool: An efficient and flexible simulator for byzantine fault-tolerant protocols,” in *2022 52nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*. IEEE, 2022, pp. 287–294.
- [111] S. Bano, A. Sonnino, M. Al-Bassam, S. Azouvi, P. McCorry, S. Meiklejohn, and G. Danezis, “Sok: Consensus in the age of blockchains,” in *Proceedings of the 1st ACM Conference on Advances in Financial Technologies*, 2019, pp. 183–198.
- [112] I. M. Coelho, V. N. Coelho, R. P. Araujo, W. Yong Qiang, and B. D. Rhodes, “Challenges of pbft-inspired consensus for blockchain and enhancements over neo dbft,” *Future Internet*, vol. 12, no. 8, p. 129, 2020.
- [113] R. Houben, A. Snyers *et al.*, “Cryptocurrencies and blockchain,” *Legal context and implications for financial crime, money laundering and tax evasion*, pp. 1–86, 2018.
- [114] F. Yang, W. Zhou, Q. Wu, R. Long, N. N. Xiong, and M. Zhou, “Delegated proof of stake with downgrade: A secure and efficient blockchain consensus algorithm with downgrade mechanism,” *IEEE Access*, vol. 7, pp. 118 541–118 555, 2019.
- [115] D. Schwartz, N. Youngs, A. Britto *et al.*, “The ripple protocol consensus algorithm,” *Ripple Labs Inc White Paper*, vol. 5, no. 8, p. 151, 2014.
- [116] D. Mazieres, “The stellar consensus protocol: A federated model for internet-level consensus,” *Stellar Development Foundation*, vol. 32, pp. 1–45, 2015.
- [117] J. Yoo, Y. Jung, D. Shin, M. Bae, and E. Jee, “Formal modeling and verification of a federated byzantine agreement algorithm for blockchain platforms,” in *2019 IEEE International Workshop on Blockchain Oriented Software Engineering (IWBOSE)*. IEEE, 2019, pp. 11–21.
- [118] R. Kotla, L. Alvisi, M. Dahlin, A. Clement, and E. Wong, “Zyzyva: Speculative byzantine fault tolerance,” *ACM Transactions on Computer Systems (TOCS)*, vol. 27, no. 4, pp. 1–39, 2010.
- [119] S. Gupta, J. Hellings, and M. Sadoghi, “Brief announcement: Revisiting consensus protocols through wait-free parallelization,” in *33rd International Symposium on Distributed Computing (DISC 2019)*. Schloss Dagstuhl–Leibniz-Zentrum für Informatik, 2019, pp. 44–1.
- [120] M. Yin, D. Malkhi, M. K. Reiter, G. G. Gueta, and I. Abraham, “Hotstuff: Bft consensus with linearity and responsiveness,” in *Proceedings of the 2019 ACM symposium on principles of distributed computing*, 2019, pp. 347–356.
- [121] S. Gupta, J. Hellings, S. Rahnama, and M. Sadoghi, “Building high throughput permissioned blockchain fabrics: Challenges and opportunities,” *Proceedings of the VLDB Endowment*, vol. 13, no. 12, 2020.

- [122] M. Kuzlu, M. Pipattanasomporn, L. Gurses, and S. Rahman, "Performance analysis of a hyperledger fabric blockchain framework: throughput, latency and scalability," in *2019 IEEE international conference on blockchain (Blockchain)*. IEEE, 2019, pp. 536–540.
- [123] L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, and P. Saxena, "A secure sharding protocol for open blockchains," in *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, 2016, pp. 17–30.
- [124] X. Wang and Y. Guan, "A hierarchy byzantine fault tolerance consensus protocol based on node reputation," *Sensors*, vol. 22, no. 15, p. 5887, 2022.
- [125] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future generation computer systems*, vol. 107, pp. 841–853, 2020.
- [126] K. Li, H. Li, H. Wang, H. An, P. Lu, P. Yi, and F. Zhu, "PoV: An Efficient Voting-Based Consensus Algorithm for Consortium Blockchains," *Frontiers in Blockchain*, vol. 3, mar 2020.
- [127] A. Bessani, J. Sousa, and E. E. Alchieri, "State machine replication for the masses with bft-smart," in *2014 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*. IEEE, 2014, pp. 355–362.
- [128] S. Sondhi, "Empirical performance evaluation of consensus algorithms in permissioned blockchain platforms," Master's thesis, University of Windsor (Canada), 2021.
- [129] S. Alqahtani and M. Demirbas, "Bottlenecks in blockchain consensus protocols," in *2021 IEEE International Conference on Omni-Layer Intelligent Systems (COINS)*. IEEE, 2021, pp. 1–8.
- [130] Y. Wang, M. Zhong, and T. Cheng, "Research on pbft consensus algorithm for grouping based on feature trust," *Scientific Reports*, vol. 12, no. 1, p. 12515, 2022.
- [131] N. Sharma, "Comparing byzantine fault tolerance consensus algorithms," Accessed Jan. 22, 2024, 2023. [Online]. Available: <https://blog.web3labs.com/comparing-byzantine-fault-tolerance-consensus-algorithms/>
- [132] P. Hegde and P. K. R. Maddikunta, "Secure pbft consensus-based lightweight blockchain for healthcare application," *Applied Sciences*, vol. 13, no. 6, p. 3757, 2023.
- [133] S. Liu, R. Zhang, C. Liu, C. Xu, J. Zhou, and J. Wang, "Improvement of the pbft algorithm based on grouping and reputation value voting," *International Journal of Digital Crime and Forensics (IJDCF)*, vol. 14, no. 3, pp. 1–15, 2022.
- [134] T. A. Alghamdi, R. Khalid, and N. Javaid, "A survey of blockchain based systems: Scalability issues and solutions, applications and future challenges," *IEEE Access*, 2024.

- [135] G. I. Navaroj, E. G. Julie, and Y. H. Robinson, “Adaptive practical byzantine fault tolerance consensus algorithm in permission blockchain network,” *International Journal of Web and Grid Services*, vol. 18, no. 1, pp. 62–82, 2022.
- [136] S. Mssassi and A. Abou El Kalam, “The blockchain trilemma: A formal proof of the inherent trade-offs among decentralization, security, and scalability,” *Applied Sciences*, vol. 15, no. 1, p. 19, 2024.
- [137] K. Lei, Q. Zhang, L. Xu, and Z. Qi, “Reputation-based byzantine fault-tolerance for consortium blockchain,” in *2018 IEEE 24th international conference on parallel and distributed systems (ICPADS)*. IEEE, 2018, pp. 604–611.
- [138] Z. Xiandong and F. Wenlong, “Research on practical byzantine fault tolerant consensus algorithm based on blockchain [j],” in *Journal of Physics: Conference Series*, vol. 1802, no. 3, 2021, pp. 032 022–032 029.
- [139] I. Stoica, R. Morris, D. Karger, M. F. Kaashoek, and H. Balakrishnan, “Chord: A scalable peer-to-peer lookup service for internet applications,” *ACM SIGCOMM computer communication review*, vol. 31, no. 4, pp. 149–160, 2001.
- [140] A. Dinh, “Subtle details in pbft,” Accessed Dec. 10, 2023. [Online]. Available: <https://dinhhta.github.io/pbft/>
- [141] W. Jiang, X. Wu, M. Song, J. Qin, and Z. Jia, “Improved pbft algorithm based on comprehensive evaluation model,” *Applied Sciences*, vol. 13, no. 2, p. 1117, 2023.
- [142] R. B. Othmen, W. Abbessi, S. Ouni, W. Badreddine, and G. Dequen, “Simulation of optimized cluster based pbft blockchain validation process,” in *2023 IEEE Symposium on Computers and Communications (ISCC)*. IEEE, 2023, pp. 1317–1322.
- [143] M. Yin, D. Malkhi, M. K. Reiter, G. G. Gueta, and I. Abraham, “Hotstuff: Bft consensus in the lens of blockchain,” *arXiv preprint arXiv:1803.05069*, 2018.
- [144] X. Xu, D. Zhu, X. Yang, S. Wang, L. Qi, and W. Dou, “Concurrent practical byzantine fault tolerance for integration of blockchain and supply chain,” *ACM Transactions on Internet Technology (TOIT)*, vol. 21, no. 1, pp. 1–17, 2021.
- [145] W. Liu, X. Zhang, W. Feng, M. Huang, and Y. Xu, “Optimization of pbft algorithm based on qos-aware trust service evaluation,” *Sensors*, vol. 22, no. 12, p. 4590, 2022.
- [146] L. Feng, H. Zhang, Y. Chen, and L. Lou, “Scalable dynamic multi-agent practical byzantine fault-tolerant consensus in permissioned blockchain,” *Applied Sciences*, vol. 8, no. 10, p. 1919, 2018.
- [147] Y. Li, L. Qiao, and Z. Lv, “An optimized byzantine fault tolerance algorithm for consortium blockchain,” *Peer-to-Peer Networking and Applications*, vol. 14, pp. 2826–2839, 2021.

- [148] W. Li, C. Feng, L. Zhang, H. Xu, B. Cao, and M. A. Imran, “A scalable multi-layer pbft consensus for blockchain,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 32, no. 5, pp. 1146–1160, 2020.
- [149] M. Gupta, P. Judge, and M. Ammar, “A reputation system for peer-to-peer networks,” in *Proceedings of the 13th international workshop on Network and operating systems support for digital audio and video*, 2003, pp. 144–152.
- [150] A. A. Selcuk, E. Uzun, and M. R. Pariente, “A reputation-based trust management system for p2p networks,” in *IEEE International Symposium on Cluster Computing and the Grid, 2004. CCGrid 2004*. IEEE, 2004, pp. 251–258.
- [151] Q. Zhuang, Y. Liu, L. Chen, and Z. Ai, “Proof of reputation: A reputation-based consensus protocol for blockchain based systems,” in *Proceedings of the 2019 International Electronics Communication Conference*, 2019, pp. 131–138.
- [152] J. Chen, X. Zhang, and P. Shangguan, “Improved pbft algorithm based on reputation and voting mechanism,” in *Journal of Physics: Conference Series*, vol. 1486, no. 3. IOP Publishing, 2020, p. 032023.
- [153] Y. Chen, M. Li, X. Zhu, K. Fang, Q. Ren, T. Guo, X. Chen, C. Li, Z. Zou, and Y. Deng, “An improved algorithm for practical byzantine fault tolerance to large-scale consortium chain,” *Information Processing & Management*, vol. 59, no. 2, p. 102884, 2022.
- [154] Z.-F. Wang, S.-Q. Liu, P. Wang, and L.-Y. Zhang, “Bw-pbft: Practical byzantine fault tolerance consensus algorithm based on credit bidirectionally waning,” *Peer-to-Peer Networking and Applications*, vol. 16, no. 6, pp. 2915–2928, 2023.
- [155] X. Yu, Y. Zhong, and Z. Zhang, “Byzantine fault tolerant consensus algorithm based on credit model and verifiable random function,” in *Proceedings of the 2022 6th International Conference on Electronic Information Technology and Computer Engineering*, 2022, pp. 1659–1664.
- [156] C.-L. Hwang and K. Yoon, *Multiple Attribute Decision Making: Methods and Applications A State-of-the-Art Survey*. Springer-Verlag, 1981.
- [157] R. Abu-Taha, “Multi-criteria applications in renewable energy analysis: A literature review,” *2011 Proceedings of PICMET’11: Technology Management in the Energy Smart World (PICMET)*, pp. 1–8, 2011.
- [158] M. Velasquez and P. T. Hester, “An analysis of multi-criteria decision making methods,” *International Journal of Operations Research*, vol. 10, no. 2, pp. 56–66, 2013.
- [159] M. Aruldoss, T. M. Lakshmi, and V. P. Venkatesan, “A survey on multi criteria decision making methods and its applications,” *American Journal of Information Systems*, vol. 1, no. 1, pp. 31–43, 2013.
- [160] H. Taherdoost and M. Madanchian, “Multi-criteria decision making (mcdm) methods and concepts,” *Encyclopedia*, vol. 3, no. 1, pp. 77–87, 2023. [Online]. Available: <https://www.mdpi.com/2673-8392/3/1/6>

- [161] A. M. Shahsavarani and E. Azad Marz Abadi, “The bases, principles, and methods of decision-making: A review of literature,” *International Journal of Medical Reviews*, vol. 2, no. 1, pp. 214–225, 2015.
- [162] A. Łatuszyńska, “Multiple-criteria decision analysis using topsis method for interval data in research into the level of information society development,” *Folia Oeconomica Stetinensia*, vol. 13, no. 2, pp. 63–76, 2013.
- [163] A. Bączkiewicz, J. Wątróbski, B. Kizielewicz, and W. Sałabun, “Towards objectification of multi-criteria assessments: a comparative study on mcda methods,” in *2021 16th Conference on Computer Science and Intelligence Systems (FedCSIS)*. IEEE, 2021, pp. 417–425.
- [164] G.-H. Tzeng and J.-J. Huang, *Multiple attribute decision making: methods and applications*. CRC press, 2011.
- [165] G. Ginting, M. Fadlina, A. P. U. Siahaan, and R. Rahim, “Technical approach of topsis in decision making,” *Int. J. Recent Trends Eng. Res*, vol. 3, no. 8, pp. 58–64, 2017.
- [166] Y. K. Tewatia, “Topsis method for multiple-criteria decision making (mcdm),” Accessed Dec. 10, 2024. [Online]. Available: https://github.com/Tewatia5355/Topsis_tewatia
- [167] K. Shahroudi and S. M. S. Tonekaboni, “Application of topsis method to supplier selection in iran auto supply chain,” *Journal of Global Strategic Management*, vol. 6, no. 2, pp. 123–131, 2012.
- [168] N. Ploskas and J. Papathanasiou, “A decision support system for multiple criteria alternative ranking using topsis and vikor in fuzzy and nonfuzzy environments,” *Fuzzy Sets and Systems*, vol. 377, pp. 1–30, 2019.
- [169] B. B. Gardas, A. Heidari, N. J. Navimipour, and M. Unal, “A fuzzy-based method for objects selection in blockchain-enabled edge-iot platforms using a hybrid multi-criteria decision-making model,” *Applied Sciences*, vol. 12, no. 17, p. 8906, 2022.
- [170] M. Madanchian and H. Taherdoost, “A comprehensive guide to the topsis method for multi-criteria decision making,” *Madanchian M, Taherdoost H. A comprehensive guide to the TOPSIS method for multi-criteria decision making. Sustainable Social Development*, vol. 1, no. 1, p. 2220, 2023.
- [171] L. T. Blessing and A. Chakrabarti, *DRM: A design reseach methodology*. Springer, 2009.
- [172] M. Guizani, A. Rayes, B. Khan, and A. Al-Fuqaha, *Network modeling and simulation: a practical perspective*. John Wiley & Sons, 2010.
- [173] T. Henderson. ns-3-dev. (2022, Oct 27). [Online]. Available: <https://gitlab.com/nsnam/ns-3-dev/>

- [174] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, “Lsb: A lightweight scalable blockchain for iot security and anonymity,” *Journal of Parallel and Distributed Computing*, vol. 134, pp. 180–197, 2019.
- [175] P. Foytik, S. Shetty, S. P. Gochhayat, E. Herath, D. Tosh, and L. Njilla, “A blockchain simulator for evaluating consensus algorithms in diverse networking environments,” in *2020 Spring Simulation Conference (SpringSim)*. IEEE, 2020, pp. 1–12.
- [176] V. Dedeoglu, R. Jurdak, G. D. Putra, A. Dorri, and S. S. Kanhere, “A trust architecture for blockchain in iot,” in *Proceedings of the 16th EAI international conference on mobile and ubiquitous systems: computing, networking and services*, 2019, pp. 190–199.
- [177] J. Zheng, C. Dike, S. Pancari, Y. Wang, G. C. Giakos, W. Elmannai, and B. Wei, “An in-depth review on blockchain simulators for iot environments,” *Future Internet*, vol. 14, no. 6, p. 182, 2022.
- [178] D. Thomas, A. Joiner, W. Lin, M. Lowry, and T. Pressburger, “The unique aspects of simulation verification and validation,” in *2010 IEEE Aerospace Conference*. IEEE, 2010, pp. 1–7.
- [179] O. Balci, “Verification validation and accreditation of simulation models,” in *Proceedings of the 29th conference on Winter simulation*, 1997, pp. 135–141.
- [180] C. J. Roy, “Review of code and solution verification procedures for computational simulation,” *Journal of Computational Physics*, vol. 205, no. 1, pp. 131–156, 2005.
- [181] R. G. Sargent, “Verification and validation of simulation models,” in *Proceedings of the 2010 winter simulation conference*. IEEE, 2010, pp. 166–183.
- [182] T. L. Paez, “Introduction to model validation.” Sandia National Lab.(SNL-NM), Albuquerque, NM (United States), Tech. Rep., 2008.
- [183] O. Balci, “Validation, verification, and testing techniques throughout the life cycle of a simulation study,” *Annals of operations research*, vol. 53, pp. 121–173, 1994.
- [184] H. Performance and S. W. Group, “Hyperledger blockchain performance metrics,” Hyperledger.org, Whitepaper, 2018. [Online]. Available: <https://wiki.hyperledger.org/groups/pswg/performance-and-scale-wg>
- [185] M. Belotti, N. Božić, G. Pujolle, and S. Secci, “A vademecum on blockchain technologies: When, which, and how,” *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3796–3838, 2019.
- [186] P. Thakkar, S. Nathan, and B. Viswanathan, “Performance benchmarking and optimizing hyperledger fabric blockchain platform,” in *2018 IEEE 26th international symposium on modeling, analysis, and simulation of computer and telecommunication systems (MASCOTS)*. IEEE, 2018, pp. 264–276.

- [187] R. Jain, *The art of computer systems performance analysis: techniques for experimental design, measurement, simulation, and modeling*. Wiley New York, 1991, vol. 1.
- [188] ———, *The art of computer systems performance analysis*. John Wiley & Sons, 2008.
- [189] H. Al-Bahadili, *Simulation in Computer Network Design and Modeling: Use and Analysis: Use and Analysis*. IGI Global, 2012.
- [190] O. B. Lynn, “A hybrid mechanism for sip over ipv6 macromobility and micromobility management protocols,” Ph.D. dissertation, PhD Thesis, College of Arts and Sciences, Universiti Utara Malaysia, 2008.
- [191] M. Hassan and R. Jain, *High performance TCP/IP networking*. Prentice Hall Upper Saddle River, 2003, vol. 29.
- [192] R. Banno and K. Shudo, “Simulating a blockchain network with simblock,” in *2019 IEEE international conference on blockchain and cryptocurrency (ICBC)*. IEEE, 2019, pp. 3–4.
- [193] Y. Aoki, K. Otsuki, T. Kaneko, R. Banno, and K. Shudo, “Simblock: A blockchain network simulator,” in *IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE, 2019, pp. 325–329.
- [194] Zhayujie. blockchain-simulator. (2022). [Online]. Available: <https://github.com/zhayujie/blockchain-simulator>
- [195] S. Sharma, A. N. Mahajan, and R. C. Poonia, “An inclusive survey of network simulators,” in *Proceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM)*, Amity University Rajasthan, Jaipur-India, 2019.
- [196] L. Campanile, M. Gribaudo, M. Iacono, F. Marulli, and M. Mastroianni, “Computer network simulation with ns-3: A systematic literature review,” *Electronics*, vol. 9, no. 2, p. 272, 2020.
- [197] T. L. Habibi and R. F. Sari, “Performance evaluation of quic protocol in message replication overhead in pbft consensus using ns-3,” *International Journal of Electrical, Computer, and Biomedical Engineering*, vol. 1, no. 1, pp. 44–56, 2023.
- [198] NSNAM. A Discrete-Event Network Simulator Release ns-3.29. (2023, April 27). [Online]. Available: <https://www.nsnam.org/docs/release/3.29/doxygen/index.html>
- [199] S. Wan, M. Li, G. Liu, and C. Wang, “Recent advances in consensus protocols for blockchain: a survey,” *Wireless networks*, vol. 26, no. 8, pp. 5579–5593, 2020.

- [200] H. Kakavand, N. Kost De Sevres, and B. Chilton, “The blockchain revolution: An analysis of regulation and technology related to distributed ledger technologies,” *Available at SSRN 2849251*, 2017.
- [201] A. Sarfaraz, R. Chakraborty, and D. L. Essam, “Rpoc: An efficient and scalable consensus algorithm for scm applications,” 2021.
- [202] IBM, “What is latency?” Accessed August. 27, 2024, 2023. [Online]. Available: <https://www.ibm.com/think/topics/latency>
- [203] L. community, “You’re working on a blockchain project. how do you measure performance evaluation metrics?” Accessed Sept. 22, 2024, 2024. [Online]. Available: <https://www.linkedin.com/advice/1/youre-working-blockchain-project-how-do-you-measure-ufhoc>
- [204] M. Chand, “Practical byzantine fault tolerance (pbft): Building trust in distributed systems,” Accessed August. 27, 2024, 2024. [Online]. Available: <https://medium.com/@mehar.chand.cloud/practical-byzantine-fault-tolerance-pbft-building-trust-in-distributed-systems-41183c668b93>
- [205] C. Network, “What is the byzantine fault tolerance?” Accessed August. 20, 2024, 2024. [Online]. Available: <https://www.casper.network/get-started/an-experts-guide-to-byzantine-fault-tolerance>
- [206] D. A. Cook and J. M. Skinner, “How to perform credible verification, validation, and accreditation for modeling and simulation,” *The Journal of Defense Software Engineering*, vol. 18, no. 5, pp. 20–24, 2005.
- [207] D.-Y. Zhao, Y.-Y. Ma, and H.-L. Lin, “Using the entropy and topsis models to evaluate sustainable development of islands: A case in china,” *Sustainability*, vol. 14, no. 6, p. 3707, 2022.
- [208] J. Pan and R. Jain, “A survey of network simulation tools: Current status and future developments,” Washington University in St. Louis, Technical Report, 2008.
- [209] Q. Nasir, I. A. Qasse, M. Abu Talib, and A. B. Nassif, “Performance analysis of hyperledger fabric platforms,” *Security and Communication Networks*, vol. 2018, no. 1, p. 3976093, 2018.
- [210] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun, “On the security and performance of proof of work blockchains,” in *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, 2016, pp. 3–16.
- [211] J. P. P. (NIKOLAOS.), *Multiple criteria decision aid: methods, examples and python implementations*. SPRINGER INTERNATIONAL PU, 2018.

APPENDIX A

THE TOPSIS STEPS FOR LEADER SELECTION IN REPTOPS-LEAD

This appendix documents the Technique for Order Preference by Similarity to Ideal Solution (TOPSIS) method used in the RepTOPS-Lead scheme to objectively rank consensus nodes and select the optimal leader node based on multiple performance criteria. It provides a step-by-step mathematical framework for leader selection to be replaced in view-change operation. By formalizing the decision process, it supports the study's claims about node reliability and scalability while enabling future adaptations of the weighting criteria.

Step 1: The formation of a decision matrix

The process is initiated by forming the decision matrix using Equation A.1. This involved a co-ordinated mapping of alternatives (consensus nodes) with the selected criteria of this study, indicating how each criterion is satisfied by each alternative (nodes). Given a set of alternatives $A = \{A_i \mid i = 1, 2, \dots, m\}$ and a set of criteria $C = \{C_j \mid j = 1, 2, \dots, n\}$, where $X = \{x_{ij} \mid i = 1, 2, \dots, m; j = 1, 2, \dots, n\}$ represents the decision matrix and x_{ij} is the value of i th alternative with respect to j th indicator. Each element in the decision matrix, such as $A_i C_j$, represents the intersection between the alternative and the selected criteria. Throughout all the equations presented in this section, $i = 1, 2, \dots, m$ and $j = 1, 2, \dots, n$.

$$x_{ij} = \begin{bmatrix} x_{A_1 C_1} & x_{12} & x_{13} & \cdots & x_{A_1 n} \\ x_{21} & x_{22} & x_{23} & \cdots & x_{2n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_{m C_1} & x_{m2} & x_{m3} & \cdots & x_{A_m C_n} \end{bmatrix} \quad (\text{A.1})$$

Step 2: The normalization of the decision matrix

Then it constructs a normalized decision matrix for the nodes using Equation A.2.

$$r_{ij} = \frac{x_{ij}}{\sqrt{\sum_{i=1}^n x_{ij}^2}} \quad (\text{A.2})$$

Step 3: The computation of the weighted normalized matrix

In this step, a set of weights of the selected criteria is applied to compute the weighted normalized decision matrix. The weight calculation is performed using the Entropy method as in Equation A.3 to accurately determine the relative importance of the selected criteria. The weights obtained through the Entropy method were then utilized as input in the TOPSIS framework by RepTOPS-Lead to select the optimal alternatives.

$$H_j = p_{ij} \log_2 p_{ij} \quad (\text{A.3})$$

Subsequently, a weighted normalized decision matrix is computed using Equation A.4 based on the weights assigned and the values of the normalized decision matrix. v_{ij} represent the weighted normalized value for i th node and j th criterion, while w_j is the weight for j th criterion.

$$v_{ij} = w_j \times r_{ij} \quad (\text{A.4})$$

Step 4: The determination of the positive and negative ideal solutions

The algorithm then determines both the Positive Ideal Solution (PIS) and the Negative Ideal Solution (NIS) from this normalized decision matrix using Equation A.5 and Equation A.6, respectively. These equations demonstrate that A^+ is given from aggregating the best possible values for each criterion (PIS), and A^- instead comes from the worst possible values for each criterion (NIS) of the normalized matrix.

$$A^+ = \{\max(v_{ij}) | j \in J\} \quad (\text{A.5})$$

$$A^- = \{\min(v_{ij}) | j \in J\} \quad (\text{A.6})$$

Step 5: The calculation of the separation measures

Subsequently, the algorithm calculates the separation measures and relative closeness to the ideal solution. For the separation measures, the distance of each node in the system from the PIS (Equation A.7) and the NIS (Equation A.8) is calculated, evaluating how closely they align with the intended outcomes (current leader).

$$S_i^+ = \sqrt{\sum_{j=1}^m (v_{ij} - A_j^+)^2} \quad (\text{A.7})$$

$$S_i^- = \sqrt{\sum_{j=1}^m (v_{ij} - A_j^-)^2} \quad (\text{A.8})$$

Step 6: Determining of the relative closeness to the ideal solution

Using these distances, the relative closeness (C_i^*) of the i th node is calculated using Equation A.9 for the TOPSIS score (closeness coefficient). Ultimately, the alternatives can be ranked based on the closeness coefficients, with the best alternative being the one that receives the highest score. This score provides perspective on their relative positions within the network.

$$C_i^* = \frac{S_i^-}{S_i^+ + S_i^-} \quad (\text{A.9})$$

Step 7: Ranking the alternative nodes based on TOPSIS Score

In the last step of the TOPSIS method, the alternative nodes are ranked according to their closeness coefficients, ranging from the best with the highest C_i^* value to the worst alternative, with the lowest C_i^* value. The top alternative in the list, characterized by the highest (C_i^*) value, is deemed the solution [211], [170].

APPENDIX B

CALCULATION OF DECISION CRITERIA WEIGHTS USING THE ENTROPY METHOD IN REPTOPS-LEAD

This appendix provides a tutorial on calculating objective weights for multi-criteria decision-making using the entropy method in the RepTOPS-Lead scheme. It demonstrates how to systematically evaluate network nodes based on three key criteria: Cumulative score (unique values for each node), Current Leader status (binary: leader vs. non-leader), and node status (categorical: reliable, normal, invalid). The entropy method is particularly valuable because it eliminates subjective bias in weight assignment by mathematically determining the importance of each criterion based on the diversity of data within that criterion. Criteria with more scattered or diverse data receive lower weights, while criteria with less diversity but high discriminative power receive higher weights.

In this specific example, the 'current leader' criterion receives the highest normalized weight (0.884) because it has the most uneven distribution with only one leader among 50 nodes, which makes it highly effective in distinguishing between alternatives. The document walks through the complete mathematical process, from calculating individual probabilities for each class of criterion, computing the entropy values, deriving raw weights as reciprocals of entropy, and finally normalizing these weights to sum to one. This methodology is commonly applied in network analysis, system reliability assessment, and distributed system evaluation, where objective data-driven weight assignments are preferred over subjective expert judgments. The following is a step-by-step method for applying entropy-based weighting in multi-criteria decision analysis, specifically for leader node selection in RepTOPS-Lead. The calculation is based on the example data for 50 nodes.

Step 1: Calculate the probability of each parameter.

i. Cumulative Score

Since each score has a unique number, the probability will become:

$$\begin{aligned} \text{Probability Cumulative Score} &= \frac{1}{\text{Total number of Node}} \\ \text{Probability Cumulative Score} &= \frac{1}{50} \approx 0.02 \end{aligned}$$

ii. Current Leader

$$\begin{aligned} \text{Probability Leader} &= \frac{\text{Number of Leader}}{\text{Total number of Node}} \\ \text{Probability Leader} &= \frac{1}{50} \approx 0.02 \\ \text{Probability Not Leader} &= \frac{\text{Total Number of Not Leader}}{\text{Total number of Node}} \\ \text{Probability Not Leader} &= \frac{49}{50} \approx 0.98 \end{aligned}$$

iii. Node Status

$$\begin{aligned} \text{Probability Reliable} &= \frac{\text{Total Number of Reliable Node}}{\text{Total number of Node}} \\ \text{Probability Reliable} &= \frac{9}{50} \approx 0.18 \\ \text{Probability Normal} &= \frac{\text{Total Number of Normal Node}}{\text{Total number of Node}} \\ \text{Probability Normal} &= \frac{31}{50} \approx 0.62 \\ \text{Probability Invalid} &= \frac{\text{Total Number of Invalid Node}}{\text{Total number of Node}} \\ \text{Probability Invalid} &= \frac{10}{50} \approx 0.20 \end{aligned}$$

Step 2: Entropy calculation for each class in each parameter.

$$H_j = p_{ij} \log_2 p_{ij} \tag{B.1}$$

$$H_{\text{Cumulative}} = (0.02 \times \log_2 0.02) = -0.112877124$$

$$H_{\text{leader}} = (0.02 \times \log_2 0.02) = -0.112877124$$

$$H_{\text{Not Leader}} = (0.98 \times \log_2 0.98) = -0.028563419$$

$$H_{\text{Reliable}} = (0.18 \times \log_2 0.18) = -0.445307614$$

$$H_{\text{Normal}} = (0.62 \times \log_2 0.62) = -0.427589125$$

$$H_{\text{Invalid}} = (0.20 \times \log_2 0.20) = -0.464385619$$

Step 3: Calculation of Entropy for each parameter

$$H_P = - \sum_{j=1}^c p_{ij} \log_2 p_{ij} \quad (\text{B.2})$$

Where c is the number of classes in parameter, $P(x) = p_{ij}$, and $P =$ parameter.

$$H_{\text{Total Cumulative}} = -(50 \times (-0.112877124)) = 5.64385619$$

$$H_{\text{Total leader}} = -((-0.112877124) + (-0.028563419)) = 0.141440543$$

$$H_{\text{Node Status}} = -((-0.445307614) + (-0.427589125) + (-0.464385619)) = 1.337282358$$

Step 4: Calculate the weight for each parameter. Reciprocal of the entropy.

$$\text{Weight}_{\text{Total Cumulative}} = \frac{1}{H_{\text{Total Cumulative}}} = \frac{1}{5.64385619} = 0.17718382$$

$$\text{Weight}_{\text{Total Leader}} = \frac{1}{H_{\text{Total Leader}}} = \frac{1}{0.141440543} = 7.070108627$$

$$\text{Weight}_{\text{Node Status}} = \frac{1}{H_{\text{Node Status}}} = \frac{1}{1.337282358} = 0.747785233$$

Step 5: Normalized the weight.

$$\begin{aligned} \text{Normalized Weight}_{\text{Total Cumulative}} &= \frac{\text{Weight}_{\text{Total Cumulative}}}{\text{Total weight}} \\ &= \frac{0.17718382}{0.17718382 + 7.070108627 + 0.747785233} \\ &= \mathbf{0.022161613} \end{aligned}$$

$$\begin{aligned}
 \text{Normalized Weight}_{\text{Total Leader}} &= \frac{\text{Weight}_{\text{Total Leader}}}{\text{Total weight}} \\
 &= \frac{7.070108627}{0.17718382 + 7.070108627 + 0.747785233} \\
 &= \mathbf{0.884307684}
 \end{aligned}$$

$$\begin{aligned}
 \text{Normalized Weight}_{\text{Node Status}} &= \frac{\text{Weight}_{\text{Node Status}}}{\text{Total weight}} \\
 &= \frac{0.747785233}{0.17718382 + 7.070108627 + 0.747785233} \\
 &= \mathbf{0.093530703}
 \end{aligned}$$

The sum of the weights assigned to all criteria must equal 1.