A SIMPLIFIED CONSENSUS PROTOCOL SIMULATOR WITH APPLICATIONS ON PROOF OF CONTRIBUTION-X

OYINLOYE DAMILARE PETER

UNIVERSITI SAINS MALAYSIA

2023

A SIMPLIFIED CONSENSUS PROTOCOL SIMULATOR WITH APPLICATIONS ON PROOF OF CONTRIBUTION-X

by

OYINLOYE DAMILARE PETER

**Thesis submitted in partial fulfilment of the requirements
for the degree of
Doctor of Philosophy**

March 2023

ACKNOWLEDGEMENT

To God be the glory, great things He hath done. All thanks to the giver of life for the opportunity to start and complete this research. Thank you Lord. This programme would not have been a success without the help and support of those around me, some of which I will mention here.

First and foremost, I would like to thank my dear wife for her patience and support throughout the period of my PhD research. Babe, this will never have been possible without your understanding and support. Thank you! To my sons, Anfanioluwa and Anrolaoluwa, thank you for coping with my absence and I hope you know that you are an integral part of this success. Not forgetting my late parents, especially my mum who gave it all to see me through my education right from elementary to the University. Thank you mum, I hope I have made you proud. I love you both sincerely.

Next, I will like to thank my supervisor, Dr. Je Sen Teh. He has been a very dedicated and supportive supervisor, willing to do anything to help me succeed in this research. I'm deeply honored to have been under his tutelage. Thank you Dr. Teh! I will also like to thank Dr. Jiashen Teh for his contribution towards the success of this research. I would like to thank all my friends, family member and associates for their support and contributions throughout the duration of this programme. Lastly, I would like to appreciate the Tertiary Education Trust Fund Nigeria for their support and commitment to the success of this programme. Thank you Tetfund!

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ABMS	Agent Based Modelling and Simulation
AMU	Authenticated Mining Unit
AP	Adjourn Period
ARP	Address Resolution Protocol
ASICs	Application Specific Integrated Circuits
BFT	Byzantine Fault Tolerance
BTC	Bitcoin
CA	Certificate Authority
CAP	Consistency, Availability and Partition Tolerance
COV	Coefficient of Variation
CPE	Consensus Protocols Based on Effort
CPPB	Consensus Protocol Based on Past Behavior
CPR	Consensus Protocols Based on Reputation
CPW	Consensus Protocols Based on Wealth
DAO	Decentralized Autonomous Organization
DDoS	Distributed Denial of Service
DLT	Decentralized Ledger Technology
DNS	Domain Name System
dPoR	Delegated Proof of Reputation
DPoS	Delegated Proof of Stake
dPoW	Delayed Proof of Work
GA	Genetic Algorithm
JADE	Java Agent Development Framework

MC	Monte Carlo
MDP	Markov Decision Process
NC	Nakamoto Consensus
NSMC	Non-Sequential Monte Carlo
P2P	Peer to Peer
PBFT	Practical Byzantine Fault Tolerance
PCA	Patient-Centric Agent
PoA	Proof of Authority
PoAj	Proof of Adjourn
PoB	Proof of Burn
PoC	Proof of Capacity
PoCt	Proof of Contribution
PoCX	Proof of Contribution X
PoE	Proof of Evolution
PoET	Proof of Elapsed Time
PoEx	Proof of Experience
PoF	Proof of Familiarity
PoL	Proof of Learning
PoP	Proof of Phone
PoPF	Proof of Participation and Fees
PoR	Proof of Reputation
PoRX	Proof of Reputation X
PoS	Proof of Stake
PoSe	Proof of Search
PoSn	Proof of Sincerity

PoT	Proof of Trust
PoV	Proof of Vote
PoW	Proof of Work
RSU	Road Side Unit
SMC	Sequential Monte Carlo
SQL	Structured Query Language
SQLi	Structured Query Language Injection
TPS	Transaction Per Second
UTXO	Unspent Transaction Output

SIMULATOR PROTOKOL KONSENSUS DIPERMUDAHKAN DENGAN APLIKASI PADA BUKTI SUMBANGAN-X

ABSTRAK

Protokol konsensus rantaian blok ialah komponen seni bina utama rangkaian rantaian blok. Banyak penambahbaikan protokol konsensus rantaian blok yang popular seperti *Proof of Work* (PoW) dan *Proof of Stake* (PoS) telah membawa kepada kelahiran protokol konsensus alternatif, beberapa daripadanya memenuhi bidang tertentu seperti perubatan atau pengangkutan.Walau bagaimanapun, kebanyakan protokol konsensus yang dicadangkan baru-baru ini kekurangan analisis dan pengesahan yang menghalang penggunaan protokol ini dalam rangkaian rantaian blok dunia sebenar. Banyak penyelidikan telah dilakukan dalambidang protokol alternatif, salah satunya ialah kelas protokol konsensus yang dikenali sebagai protokol konsensus berdasarkan tingkah laku masa lalu-Consensus Protocol Based on Past Behaviour (CPPB). Walau bagaimanapun, kerja-kerja ini tidak termasuk analisis keselamatan dan prestasi kelas protokol konsensus ini. Jurang ini dirapatkan dalam tesis ini dengan mencadangkan rangka kerja simulasi ringkas yang dipanggil SIM-P yang membolehkan simulasiyang tepat kelakuan protokol konsensus ini dengan mudah. SIM-P ialah simulator stokastik berasaskan ejen yang bergantung pada kaedah Monte Carlo berjujukan untuk memodelkan cara penerbit blok dipilih.Model simulasi telah dibangunkan untuk PoW sebagai model asas untuk tujuan penandaarasan dan dua CPPB iaitu *Proof of Reputation X* (PoRX) dan *Proof of Contribution* (PoCt).Tiga (3) model simulasi yang dibangunkan telah dilaksanakan dengan Python dan prestasinya dianalisis dari segi daya pemprosesan, rintangan terhadap 51% dan penggunaan tenaga sebagai metric penilaian.CPPB yang dianalisis ini juga telah ditanda aras terhadap PoW.Berdasarkan penemuan kerja penyelidikan ini, CPPB baharu, yang dipanggil *Proof of Contribution X* (PoCX) telah dicadangkan dengan prestasi yang dipertingkatkan.PoCX seterusnya digunakan pada domain penjanaan dan pengedaran tenaga solar terikat grid sebagai bukti konsep untuk mempamerkan cara protokol itu digunakan. Rangka kerja simulasi yang dicadangkan dalam penyelidikan ini boleh digunakan oleh protokol konsensus lain untuk analisis prestasi dan keselamatan.Hasil analisis CPPB terpilih (PoRX, PoCt) dan PoCX yang direka bentuk baharu, yang ditanda aras dengan PoW akan berguna dalam membuat keputusan untuk penggunaan protokol konsensus rantaian blok pada masa hadapan.

A SIMPLIFIED CONSENSUS PROTOCOL SIMULATOR WITH APPLICATIONSON PROOF OF CONTRIBUTION-X

ABSTRACT

Blockchain consensus protocols are the major architectural components of blockchain networks. Numerous enhancements of popular blockchain consensus protocols, such as Proof of Work (PoW) and Proof of Stake (PoS), have led to the emergence of alternative consensus protocols, some of which cater to specific areas such as medicine or transportation. A considerable amount of research has been done on these alternative protocols, one class of which is known as Consensus Protocols Based on Past Behaviour (CPPB). However, these protocols remain relatively unknown and lack performance analysis, which hinders their possible deployment in real-world blockchain networks because the strengths and weaknesses of these consensus protocols cannot be determined. This problem stems from the lack of simulation tools for other consensus protocols that are not mainstream. This gap is bridged by proposing a simple simulation framework called SIM-P, which can accurately simulate the behaviour of these consensus protocols with ease. SIM-P is an agent-based stochastic simulator that relies on the sequential Monte Carlo method to model how block publishers are selected. Simulation models are developed for PoW as a base model for benchmarking purposes, as well as for two selected CPPBs: Proof of Reputation X (PoRX) and Proof of Contribution (PoCt). The three (3) simulation models developed are implemented with Python, and analysed with throughput, resistance against 51% and energy consumption as evaluation metrics. These analysed CPPBs are also benchmarked against PoW.Based on the findings of this research work, a new CPPB, called Proof of Contribution X (PoCX) is proposed with enhanced performance. PoCX is further applied to a grid-tied solar energy generation and distribution domain as a proof of concept to showcase how the protocol is applied. Experimental results show that PoCX, PoRX, and PoCt consume less energy, have a higher throughput, and are more resistant to 51% attacks compared to PoW. The simulation framework proposed in this research can be used by other consensus protocols for performance and security analysis. The analysis results of the selected CPPBs (PoRX, PoCt) and the newly designed PoCX, benchmarked against PoW, will be useful in decision making for the future deployment of blockchain consensus protocols.

CHAPTER 1

INTRODUCTION

1.1 Introduction

Since its inception, blockchain technology and its applications have been of great interest in the financial sector. One of the most popular use cases of blockchain, cryptocurrencies, relies on cryptographic algorithms, such as asymmetric-key encryption and hash functions, to facilitate secure financial transactions between various parties or nodes (Yu, et al., 2019). Blockchain can be viewed as a fully replicated distributed database system that keeps a record of all transactions in a network. All of these transactions are also stored by every contributing node or unit within the network itself (Zou, et al., 2019). It has a distributed consensus protocol running on every participating node, managing message exchanges and local decision making to enforce network consistency.

Consensus protocols are a set of rules that participating nodes in a network use to decide whether a transaction is valid (Alzahrani &Bulusu, 2018). This ensures that all participants collectively maintain a common transaction ledger. On cryptocurrency platforms, blockchain keeps track of currency transactions in a successive and orderly form to achieve a tamper-proof record (Liu, et al., 2019). With the rise of Ethereum and other blockchain-based distributed computing platforms, transactions also include data that are required to execute smart contracts. Blockchain as a term connotes that transaction records between participating nodes in a system or network are stored in a data format known as a “block”. A sequential set of these connected blocks arranged in ascending order is referred to as the chain of blocks (i.e., “blockchain”). Permission-less blockchain networks do not need a centralized authorizing figure; interested nodes can join without restrictions, and it permits a large number of participating nodes in the consensus process (Domenico &Baronchelli, 2019; Yavuz, et al., 2018)

Bitcoin is without a doubt the most mainstream or well-known use case of blockchain technology. It was introduced as an alternative form of currency with the aim of overcoming the limitations of fiat money (Giungato, et al., 2017). Bitcoin's underlying blockchain mechanism keeps a record of cryptocurrency transactions among participating nodes. Each node involved in the transaction possesses two keys: a private key and a public key (Chen, et al., 2018). The transaction address of a participating node is the hash value of the public key, which also serves as the node's identity. As multiple private–public key pairs can be generated, nodes can thus have more than one identity, leading to attacks such as a Sybil attack (Zhang &Lee, 2019). Transactions are signed with a node's private key and are sent to all other nodes in the network for verification. With a decentralized consensus architecture, the participating nodes come to an agreement on both the sequence and validity of all transactions. The records of these transactions are stored in blocks.

The current block of any block sequence has a timestamp and is connected to prior blocks by cryptographic hash values. Participating nodes cannot delete a block but can append new ones. The chaining of these blocks results in a shared, distributed database with an immensely growing record of transactions that are irreversible and immutable. It is difficult for anyone to tamper with block information without other nodes detecting the changes (Shen &Pena-Mora, 2018). Unlike the days of centralized ledgers in the custody of a single point of authority, blockchains are essentially decentralized databases that are collaboratively managed by multiple participating entities. One important element of blockchain technology is its underlying consensus mechanism, known as the consensus protocol. These protocols decide which node is allowed to add a new block to the chain. Blockchain consensus protocols can be classified into four distinct classes based on how block publishers (or block leaders) are selected as follows:

1. Consensus Protocols Based on Effort (CPE) which requires that participating nodes provide proof of effort or work expended to show that they are more qualified than others to publish a block.

2. Consensus Protocols Based on Wealth (CPW) where participating nodes are required to show a proof of wealth or coin staked in the network to be eligible for block publishing.

3. Consensus Protocols Based on Past Behavior (CPPB) where proof of past good behaviour and conduct are required by participating nodes to be selected or elected to publish blocks.

4. Consensus Protocols Based on Representation (CPR) where some nodes are selected or elected by other participating nodes to act in the overall interest of the entire network. Some are elected or selected based on the work done, wealth staked or past history of good behavior.

Well-established consensus protocols include Proof ofWork (PoW) (Sharkey & Tewari, 2019), Proof of Stake (PoS) (King &Nadal, 2012;Puthal &Mohanty, 2019) and their variants (Lu, 2018).Also, numerous lesser known blockchain consensus protocols have been proposed, some of which are for specific areas of application such as medicine and electric vehicles. Some of these alternative protocols, Proof of Reputation (PoR) (Gai, et al., 2018), Proof Reputation X (PoRX) (Wang, et al., 2020), Delegated Proof of Reputation(dPoR) (Do, et al., 2019), Proof of Trust (PoT)(Zou, et al., 2019), Proof of Contribution (PoCt) (Xue, et al., 2018), decide who appends a block by considering past behaviors of nodes, wherein nodes with a good record of behaviour i.e. timely block publishing and general good conduct are rewarded with some kind of trustworthiness which leads to a reputation rise for the node. These protocols belong to the CPPB class. Participating nodes with a higher good behaviour history can provide a more stable and reliable service compared with those with insignificant level of good behaviour and those with none. Unlike with proof of work where nodes solve hash puzzle within the shortest to be selected to publish a block, CPPBselects the node with the highest level of good behaviour record in the group.

CPE are classes of consensus protocols that consume enormous energy or requires high computational power. Although they are the most widely accepted class of protocol and most public blockchain implementations are done on CPEs.CPW are consensus protocols that encourages the rich dictating how the network is being run and the also it makes the rich richer and the poor poorer. It has a better scalability compared to the CPE. As the number of participating nodes increases, the efficiency does decline.

CPPB requires participating nodes to show a record of good past behaviour which cannot be transferred, stolen or bought but can only be earned.CPR are protocols selected or elected to act on behalf of the entire network. These protocols are either selected/elected based on the show of effort, a show of wealth, a record of past behaviour or just on the basis of luck.

1.2 Research Motivation

Blockchain technology has seen a meteoric rise in popularity since its inception with cryptocurrencies being its most common application. Its application has span across different spheres of life from transcript verification to health and many others. Consensus protocols are the bedrock of this trustless technology and they are not without challenges.

Mainstream consensus protocols, such as PoW and PoS, are still far from perfect due to their negative impact on the environment and tendency to reward the wealthy. Therefore, it is necessary to explore alternative protocols. However, these alternatives are often not as thoroughly analysed, so it is uncertain whether they can truly outperform the mainstream protocols. Investigating these alternatives can lead to the development of more efficient, fair, secure, and environmentally friendly consensus protocols, which will ultimately benefit the growth and advancement of blockchain technology and its applications.

1.3 Research Problem

Unfortunately, majority of protocols that belong to the class of CPPB lack proper security and performance analysis. Many protocols belonging to this class are alternative protocols that are relatively new and unknown(Zou, et al., 2019; Gai, et al., 2018; Wang, et al., 2020; Do et al., 2019; Xue, et al., 2018). In addition, there has not been any thorough security analysis of these CPPB protocols (Zou, et al., 2019; Gai, et al., 2018; Wang, et al., 2020; Do et al., 2019; Xue, et al., 2018). Rather, more attention and focus has been on Nakamoto consensus, a PoW-based protocol used in Bitcoin which belongs to CPE (Kaur, et al., 2021). This problem stems from lack of simulation tools for other consensus protocols. Most security analyses have been performed on consensus protocols based on PoW and its enhancements (Tuyet, et al., 2018; Rafael, et al., 2017; Wei, et al.,2018).

However, PoW and its enhancements consume enormous energy, which does not support the global sustainability goals and might hamper the adoption of blockchain in critical sectors. Hence the need to investigate alternative consensus protocols. Some of the widely adopted consensus protocols have undergone stringent performance evaluation. Cachin and Vukolic (2017) evaluated the performance of CPE with node identity management, consensus finality, scalability, throughput, energy consumption as performance indicators.

The performance of CPW and CPR were analyzed byXiao et al. (2020). Chain-based PoS, Committee-based PoS and BFT-based, Delegated Proof of Stake (DPoS), Proof of Authority (PoA), Proof of Elapsed Time (PoET), PoR were analysed (Xiao, et al., 2020) with block proposal, block validation, information propagation, block finalisation, incentive mechanism, fault tolerance, transaction capacity as performance indicators. In contrast, CPPBs lack performance and security analysis (Bano, et al., 2019) which makes it difficult for these protocols to be adopted in real life scenarios because their strengths and weaknesses cannot be ascertained. This hampers the overall growth and adoption of (alternative) consensus protocols.

Many simulators have been proposed over the years for blockchain networks that use popular protocols such as PoW and PoS (Alharby & van-Moorsel, 2019;Faria & Correia, 2019; Stoykov, et al., 2017; Gervais, et al., 2016; Dinh, et al., 2017; Kulkarni 2020). Although these were blockchain simulators rather than simulators that catered specifically to consensus protocols, they still provided experimental data for these protocols in terms of performance and security. However, adapting some of these simulators to other protocols, especially alternative protocols, is non-trivial. One of the main reasons is that these simulators also include the other technology layers in the blockchain network which are not required if the goal is just to simulate a consensus protocol. Hence there is a need for a simple yet flexible consensus protocol simulator that can be adapted to various types of consensus protocols with ease.

Despite various enhancements of blockchain consensus protocols, mainstream consensus protocols are associated with performance and security drawbacks(Zhang, & Lee, 2020; Cao, et al., 2020; Lin & Liao, 2017; Atzei et al., 2017; Khalilov & Levi, 2018). High energy consumption, low throughput, double spending, 51% and selfish mining attacksare some of the most prevalentconsensus protocols drawback, which has hampered the overall grow and adoption of blockchain in real-world scenarios (Kaur, et al., 2021). Therefore, there is still a need for an enhanced consensus protocol with has high throughput, resistance against 51% attack and energy efficient. The three main problems being addressed in this research are:

1. Existing consensus protocols based on past behaviour lack performance and security analysis.

2. Lack of a simplified and flexible consensus protocols simulation framework that can be easily adapted to various types of consensus protocols.

3. Conventional consensus protocols have drawbacks such as high energy consumption, low throughput and 51% attack.

1.4 Research Questions

The research questions answered in this research are as follows;

1. How well do alternative consensus protocols perform as compared to the state of the art such as PoW?

2. How can a simple and flexible consensus protocol simulation framework be designed?

3. How can an enhanced consensus protocol be designed to have low energy consumption, high throughput and resistance against 51%?

1.5 Research Objectives

The overall aim of this thesis is to contribute towards the enhancement of consensus protocols in terms of both design and analysis, specifically of alternative protocols. This can be achieved by first proposing a simplified simulation framework which is then used to analyse existing alternative protocols. Based on the findings, an enhanced consensus protocol can then be designed.

Majority of the simulators proposed over the years are for the entire blockchain networks covering many layersand not specifically for consensus protocols (Alharby & van-Moorsel, 2019; Faria & Correia, 2019; Zander et al., 2019; Stoykov et al., 2017; Kulkarni, 2020). One of the objectives of this thesis is to develop a simple yet flexible consensus protocol simulation framework that can be adapted to various types of consensus protocols with ease.Also, asimulation model of PoW as the base model or benchmark is developed, on which the accuracy of the proposed simulator is verified.The proposed simulation framework can be used to analyse consensus protocols specifically.

As the majority of CPPBs lack security and performance analysis,another objective of this thesis is to provide new performance and security analyses for existing alternative consensus protocols such as PoRX and PoCtusing the proposed simulation framework.These two CPPBs are selected based on their inbuilt features of combining their reputation/contribution attributes with any other PoX mechanism belonging to other classes of protocols like PoW from CPE and PoS from CPW. The combination of these attributes (reputation and contribution) with the PoX mechanism helpsscale the difficulty of nodes based on their earned reputation or contribution.

The difficulty scaling enhances throughput and reduces energy consumption, as nodes whose difficulties were scaled down, find blocks much faster and with fewer computations/trials.To achieve the objective of producing new performance and security analyses for alternative protocols, simulation models for CPPBs such as PoRx and PoCt need to be developed. Additional attributes representing reputation and success time need to be factored into the simulation in addition to the initial node hash rate. Then the developed simulation models are implemented and analysed. These models can be used as a base for simulating other similar consensus protocols in the future.

Furthermore, experimental results of PoRX and PoCtarepresented benchmarked against PoW. A comprehensive analysis of the resistance of these selected CPPBs against 51% attacks isperformed to determine if these alternative protocols outperform the mainstream consensus protocols such as PoW and PoS in terms of performance and security. PoRX (Wang, et al., 2020) and PoCt (Xue, et al., 2018) will be the focus in this phase. The performance and security analysis of these protocols is expected to give a clearer view of the security and performance of these CPPBS. This analysis will contribute towards developing a more efficient, secure, fair and environmentally friendly consensus protocols that will contribute positively towards the enhancement of blockchain consensus protocols.The performance of these CPPBs will be analysed and evaluated with throughput, energy consumption and security as performance metrics. The simulationmodel proposed can also be used to analyse other CPPBs with similar properties.

It has been identified that most of the derivatives and enhancements of the traditional consensus protocols like the PoW, PoS and their variants might have traded security for enhanced performance or performance for high energy consumption (Cao, et al., 2020; Zhang,& Lee, 2020). To achieve a better balance of these requirements, another objective of this thesis is to design an enhanced blockchain consensus protocol known as proof of contribution X (PoCX). It has a generalized design that is applicable to multiple scenarios. One such application which is depicted in this thesis as proof-of- concept is for a grid-tied solar energy distribution system. A simulation model is also proposed to analyse the performance and security of PoCX benchmarked against PoW, PoRX and PoCt.

Completing these objectives achieves the overall aim which is to contribute towards the enhancement of consensus protocols in terms of both design and analysis.The research objectives are listed as follows:

1. To propose asimplified and yet flexible simulation framework for consensus protocols.

2. To provide performance and security analyses for existing alternative consensus protocols (CPPBs) using the proposed simulation framework.

3. To design an enhanced consensus protocol based on past behaviour that is energy efficient, has high general performance and resistance against 51% attack.

1.6 Research Contribution

The first contribution of this research is aflexible,multi-agent based, stochastic simulator for consensus protocols called SIM-P. SIM-P is simple and flexible, as it can be easily modified to simulate any class of consensus protocol by modifying a few lines of code in the attributes module.SIM-P has been coded with simple syntax in mind to facilitate ease of use. The base model itself is less than 100 lines of code, and modifying the base model to simulate PoRX is done by changing the parameters to include an additional attribute, "reputation," which requires changing fewer than 10 lines of code in the base model.A simulation model for PoW is developed as the base model,which can not only be used to verify the correctness of the statistical assumptions made for the simulator, but also as a benchmark for other consensus protocols. The performance and security analysis of PoW will be performed using throughput, energy consumption and security as metrics, and the results will be compared to theoretical estimates.

Simulation models for other consensus protocols such as PoRX and PoCt are also developed for an in-depth performance and security analysis of these consensus protocols based on past behaviour.Simulation models for these protocols were not previously available. These models will provide new insights into the performanceand security of these protocols.The development of models for these CPPBs will also showcase the flexibility of the proposed simulation framework. Also, these simulation models can be used to develop models for other new protocols in the future.The analysis will validate or invalidate claims that these protocolshave improved performance and security featurescompared to conventional consensus protocols.

Also, this analysis will allow proper evaluation of the security strengths, drawbacks and resistance of these alternative protocols to known consensus protocol attacks which will contribute to a wider adoption of these protocols. The performance oftheseCPPBswill be evaluated using metrics such as throughput, energy consumption and security. The overall performances of the-state-of-the-art consensus protocols are also evaluated with the above metrics. The developed simulation framework can be adopted for the analysis of other consensus protocols in the future. This will allow stakeholders to be able to affirm and compare the performance of alternative consensus protocols withthe mainstream consensus protocols.

An enhanced consensus protocol (PoCX) based on behaviourwith a better performance, energy efficient and improved resistance against 51%attack compared to the existing protocols based on past behaviouris designed. It has a generalized design that is applicable to multiple scenarios. One such of concrete application as depicted in this thesis is for a grid-tied solar energy distribution system. A simulation model is proposedfor PoCX and performance will be analysed with throughput, energy consumption and security as metrics. Experimental results and analysis were also presented.

The contributions of this work are summarized as follows:

1. A multi-agent based, stochastic simulator for consensus protocols (SIM-P) and PoW simulation model as a base model or benchmark.

2. Simulation models,performance and security analysis for CPPBs such as PoRX and PoCtbenchmarked against PoW.

3. An enhanced CPPB with high throughput, energy efficient, resistance against 51% attack.And as proof-of-concept, a grid-tied solar energy distribution framework based on the proposed consensus protocol.

1.7 Scope of the Research

This research will be on class of blockchain CPPBs and blockchain consensus protocol simulation framework. PoW belonging to blockchain class CPE is only simulated as a benchmark to verify the accuracy of the proposed simulation framework. The focus of this research will be on protocols such as PoRXand PoCt, all belonging to class of CPPB. Additionally, this research will not cover generic or cyber-attacks, but will specifically examine resistance against 51% attack, a known consensus protocol attack that can lead to other attacks. If an adversary controls 51% of a network, they can perform other attacks such as double spending (Frankenfield, 2021).

1.8 Research Methodology

First, a review of literatures on CPPB, attacks on consensus protocols and their history,consensus protocols simulation frameworks, conventional consensus protocols, security and performance metrics of protocols are examined; knowledge of previous work and the state of the art will provide insights to the various types of security and performance analysis approaches that exist, attacks and features of consensus protocols.A simplified consensus protocols simulator (SIM-P) that can accurately simulate the behaviour of these consensus protocols with ease was then proposed. It is an agent-based stochastic simulator that relies on the sequential Monte Carlo method to model how block publishers are selected. The likelihood of each node (represented as agents) being selected as a block publisher is represented by independent trials in a binomial experiment.PoW is widely used as a benchmark for performance comparison of blockchain consensus protocols (Alharby,& van-Moorsel, 2019; Stoykov, et al.,2017; Gervais et al., 2016). The PoW will be simulated as the base model to verify the accuracy of the simulation results.

Simulation models for promising CPPBs (such as PoRX and PoCt) are developed as a proof of concept. These CPPBs are analysed to quantify their strengths and weaknesses, benchmarking them with mainstream protocols (PoW), analysing their resistance against 51% and other resulting consensus protocol attacks. The performance of the selected CPPBs is also analysed with (throughput, energy consumption and security) as evaluation metrics.A performance and security analysis of PoRX and PoCt benchmarked against PoW is also presented. These chosen CPPBs (PoRX and PoCt) are two of the best performing CPPBs based on the review performed in Chapter 2.

Finally, a new CPPB known as PoCXis designed, leveraging on the non-transferable attribute ‘contribution’. Nodes’ contribution is not easily manipulated compared to other chain assets like stake and work done. The contribution of a node in relation to its consumption will determine its chances of being selected as block leader in each round. PoCX is energy efficient, resistant against 51% attack and has a high throughput. This new protocol will be simulated with the consensus protocols simulator proposed in the previous phase. The overall flow of the research is visually depicted in Figure 1.1 and mapped to the each of the research objectives. This diagram is a summarized version of the research methodology. An expanded version of the figure is available in Chapter 3.

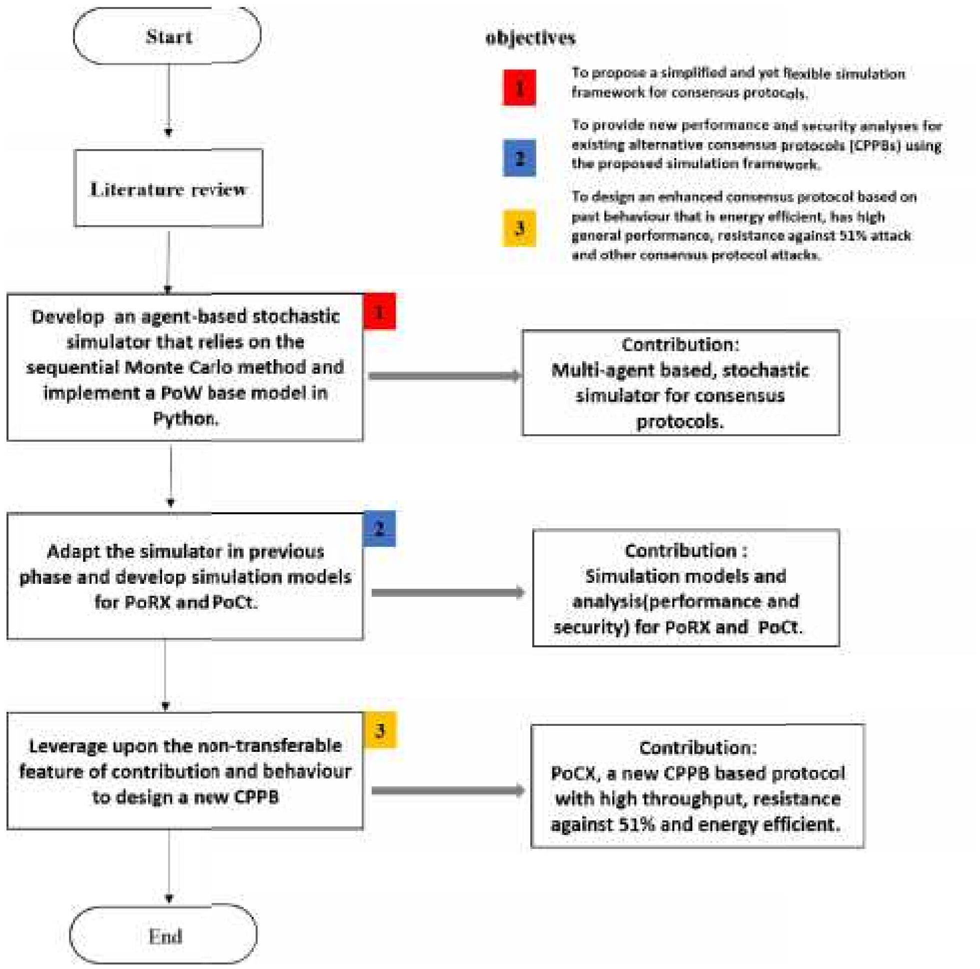
Start
Literature review
Develop an agent-based stochastic simulator that relies on the sequential Monte Carlo method and implement a PoW base model in Python.
1
Contribution: Multi-agent based, stochastic simulator for consensus protocols.
Adapt the simulator in previous phase and develop simulation models for PoRX and PoCt.
2
Contribution : Simulation models and analysis(performance and security) for PoRX and PoCt.
Leverage upon the non-transferable feature of contribution and behaviour to design a new CPPB
3
Contribution: PoCX, a new CPPB based protocol with high throughput, resistance against 51% and energy efficient.
End
objectives
1 To propose a simplified and yet flexible simulation framework for consensus protocols.
2 To provide new performance and security analyses for existing alternative consensus protocols (CPPBs) using the proposed simulation framework.
3 To design an enhanced consensus protocol based on past behaviour that is energy efficient, has high general performance, resistance against 51% attack and other consensus protocol attacks.

Figure 1.1 Research Flow and the Corresponding Objectives

1.9 Organisation of Thesis

This thesis is organized as follows: Chapter 1 has the background, problem statement, research questions, research objectives, research contributions, research scope and boundaries, research methodology and organization of thesis. Chapter 2 provides a detailed literature review of conventional consensus protocols, alternative protocols, blockchain network attacks and specific consensus protocol attacks, security analysis, performance analysis and evaluation metrics, comparison of alternative protocols with scalability, throughput, energy consumption and finality as metrics. The steps in achieving the specific objectives are presented in Chapter 3.

The methods are broadly broken into 6 steps and a detailed description of each step is highlighted in this chapter.

Chapter 4 contains the design of a blockchain consensus protocols simulator (SIM-P), development of simulation models for PoW as benchmarking purposes and some CPPBs(PoRX and PoCt). It also detailed experiments, results and discussion of the simulation of PoW, PoRX and PoCt. Chapter 5contains the design of the generalized version of PoCX, its architecture, and block structure. The application of PoCX to a specific scenario and the development steps for its simulation model is also presented in this chapter. Also,Chapter 5 contains experimental results and discussion of PoCX. Lastly, Chapter 6 has the conclusion, limitation, and future work.

CHAPTER 2

LITERATURE REVIEW

2.1 Overview

The purpose of this chapter is to describe the blockchain technology, its core components and architecture as presented in Section 2.2. It also highlights the different types of blockchain with examples in Section 2.3. Section 2.4 introduces the concept of consensus protocols and presents a classification of blockchain attacks. Section 2.5 presents a review of existing blockchain simulators and a discussion on security and performance analysis approaches for consensus protocols. Then, the chapter introduces the state-of-the-art consensus protocols and alternative protocols, highlighting their strengths and weaknesses in Section 2.6, with a comparative analysis of alternative protocols presented in Section 2.7. Sections 2.8 and 2.9 present the identified research gaps and chapter summary, respectively.

2.2 Blockchain

Blockchain is a growing list of records in form of blocks linked together securely. Blockchains are shared and distributed databases that can store digital footprints securely without a centralized control point (Andoni, et al., 2019). A sample chain of blocks is depicted in Figure 2.1.

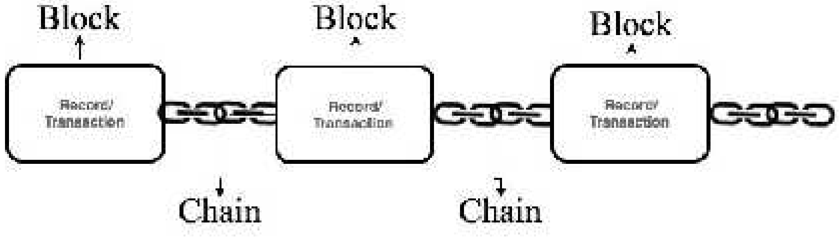

Figure 2.1 Blocks of Chains

Blockchain consist of small and important elements of called a block. Blocks are collection of transactions or any information which can be represented as a page of a ledger, signed by a hash that verifies the authenticity of the transaction or information.

Blockchain is a type of decentralized ledger technology (DLT) in which transactions are recorded with an immutable cryptographic signature called a hash. DLT are decentralized database managed by multiple participating nodes in a network. A hash is a fixed length string of numbers and letters produced by hash functions. A hash function is a mathematical function that takes a variable number of characters and converts it to a string with a fixed length of characters. If a change occurs in a string, no matter how small, it will create a completely new hash. The hash values constitute the chain between the blocks. It is like the backbone of the blockchain.

Blockchains are transparent, tamper-evident, protected and most times immutable systems that can enable unique results, especially when merged with smart contracts (Wang, et al., 2019). Transactions are duplicated and distributed across the entire network of participating nodes in the chain. Each block in the chain contains a number of transactions, and every time a new transaction occurs on the blockchain, a record of that transaction is added to every participant's copy of the record which makes the system transparent.

Records on blockchain are tamper-evident; they cannot be changed without a detailed record of the activities documented. Information such as who changed the record, what was changed, at what time, are documented for other participating nodes. However, blockchain in itself might not be totally immutable or tamper-proof but the immutability feature of blockchain is enforced by consensus protocols which make it almost impossible to change an already validated record in the chain. Such trust and assurance are usually provided by a central point of authority like banks, which ensure that a transaction sent and validated from customer A to customer B cannot be reversed arbitrarily by either. In a decentralized scenario, the middleman is expected to enforce agreements between parties but in blockchain, these agreements are enforced by smart contacts.

Smart contracts are protocols that are designed to digitally facilitate, verify, or enforce the negotiation or performance of a contract or agreement between parties. It also the strict adherence to agreements among participating parties without a third party. They permit trusted transactions and agreements among anonymous parties without necessarily having some sort of central authority or an external enforcement protocol. Smart contracts are written in programming languages such as C++, Solidity, Java, Java script and Goland. Blockchain uses the public-key cryptography or asymmetric cryptography, where two different keys (public and private keys) are required for encryption and decryption, respectively.

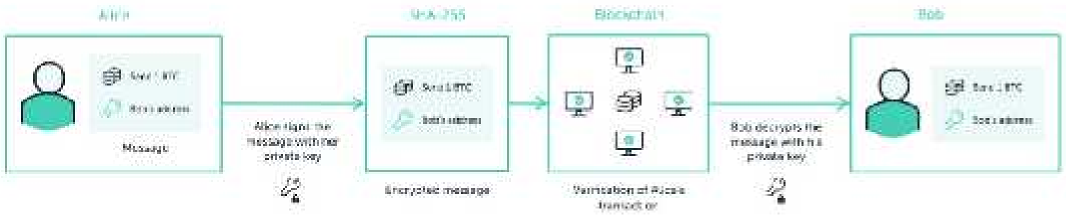
Alice
Send 1 BTC
Bob's address
Message
Alice signs the message with her private key
SHA-256
Send 1 BTC
Bob's address
Encrypted message
Blockchain
Verification of Alice's transaction
Bob decrypts the message with his private key
Bob
Send 1 BTC
Bob's address

Figure 2.2 Bitcoin Transaction Encryption

Figure 2.2 depicts a typical Bitcoin transaction scenario where Alice decides to purchase an item from Bob's store for 1 BTC, Alice presents his public key (the address that contains Alice's 1BTC) and digital signature (which is the private key uniquely append the transaction) in order to prove that the spending is legitimate. This signature can only be produced by someone with knowledge of the private key, which in this case is Alice. However, anyone with access to the public key and digital signature can genuinely verify if Alice has ownership over the 1BTC she intends to spend. Everyone on this network can verify and accept Alice transactions as genuine and valid without revealing Alice private key.

Also, blockchain can be described as a decentralized record book for documenting activities of multiple users without a centric control hub using cryptographic program. All participating users validate the block to be appended to the chain, and a consensus mechanism ensures that all participants jointly agree to a specific order at which blocks are added (Sayeedn & Marco-Gisbert, 2019). Furthermore, blockchains permits automatic execution of smart contracts in peer-to-peer (P2P) networks (Andoni, et al., 2019).

Recently, blockchains has suddenly become an item of interest to developers in the security sphere. Bitcoin (Nakamoto, 2008) and Ethereum being household names, the investors, researchers, developers, enthusiasts, and academia in the financial space, had shown keen interest in its evolving growth. With the increase in its acceptability by major vendors as well as consortium of banks as a legal exchange, blockchains must continue to improve its security and overall throughputs to achieve a more secure, dependable, and reliable system. Blockchain usage cuts across different spheres aside the security space, with different innovations been churned out daily in financial technology, health systems, manufacturing and distribution systems, road maintenance and safety, environmental and disaster management.

There are basically three major groups of blockchains: public blockchains, private and consortium blockchains. Public blockchains is permission-less system that allows participation by all users in a network, whereas private blockchain is a closed system that allows only a few users to participate, which are usually between trusted users (Pungila & Negru 2020). Finally, consortium blockchain is a hybrid of public and private blockchains. These types of blockchains are detailed in the following subsection.

2.3 Types of Blockchain

Blockchain can be broadly grouped into three (3) distinctive groups which will be described in the following subsections: public, private and consortium blockchains. Consensus protocols are designed for these different groups of blockchain. Some consensus protocols are designed for specific types of blockchain, while others are general.

2.3.1 Public Blockchain

Public blockchain is a permission-less system that allows anyone to join anonymously and transact in the network. This type of network has no restriction on the participatory and validatory roles. Every participating node has a copy of the ledger which makes it possible for anyone to access the network. The most important feature of this class of blockchain is that no single entity has a complete control of the network, which ensures the security of data and helps in the immutability of the records (Lai & Lee Kuo Chuen, 2018). All participating node in this blockchain have equal authority which makes it fully distributed. Verification of transactions are done with consensus protocols where participants are required to do some work to make the network and functional.

Public blockchains are characterized with lower transaction speed (Casino, et al., 2019). Bitcoin performs an average of about 7 transactions per hour compared to VISA which performs a little above 24,000 transactions per second (Fluence, 2019). Also, public blockchains are not scalable because the network gets more clumsy and slower as the size of the network increases (Seth, 2022). Bitcoin, Ethereum, and Litecoin are some of the examples of public blockchain. Figure 2.3 depicts a public blockchain and the lightening symbol indicates a validator node. All the nodes in a public blockchain are validators.

Lightening symbol indicates a validator node.

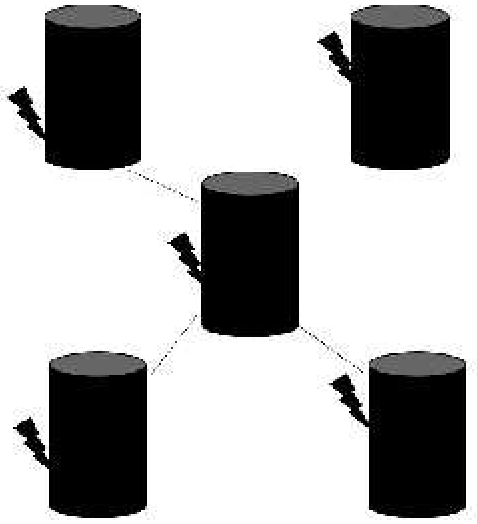

Figure 2.3 Public Blockchain

2.3.2 Private Blockchain

Private blockchain is best described as a blockchain that works in a closed network. It requires that participants be invited before they can participate in the network. It is a permissioned blockchain. Transactions in this network are visible only to participants who are part of the network. They are more centralised, they are governed and regulated by an entity that ensures that participants are well guided.

Private blockchains may have a token, depending on the preference of the blockchain owner. This class of blockchains usually have a network administrator who can take care of the user permissions in case any particular user requires additional authority on the go (Seth, 2022).As there are fewer participants in a private blockchain compared to a public blockchain, it takes lesser time to reach a consensus and faster compared to the public blockchain. Also, private blockchains are more scalable because only a few nodes are selected to validate transactions. Even as the network grows bigger, the speed and efficiency will not diminish (Sharma, 2019).

However, private blockchains are not really decentralized as there are still central points of authority controlling the network. Multichain, Hyperledger Fabric (Hyperledger, n.d.), Hyperledger Sawtooth and Corda are examples of private blockchains. Figure 2.4 depicts a private blockchain and the lightening symbol indicates a validator node. Only one node is a validator node.