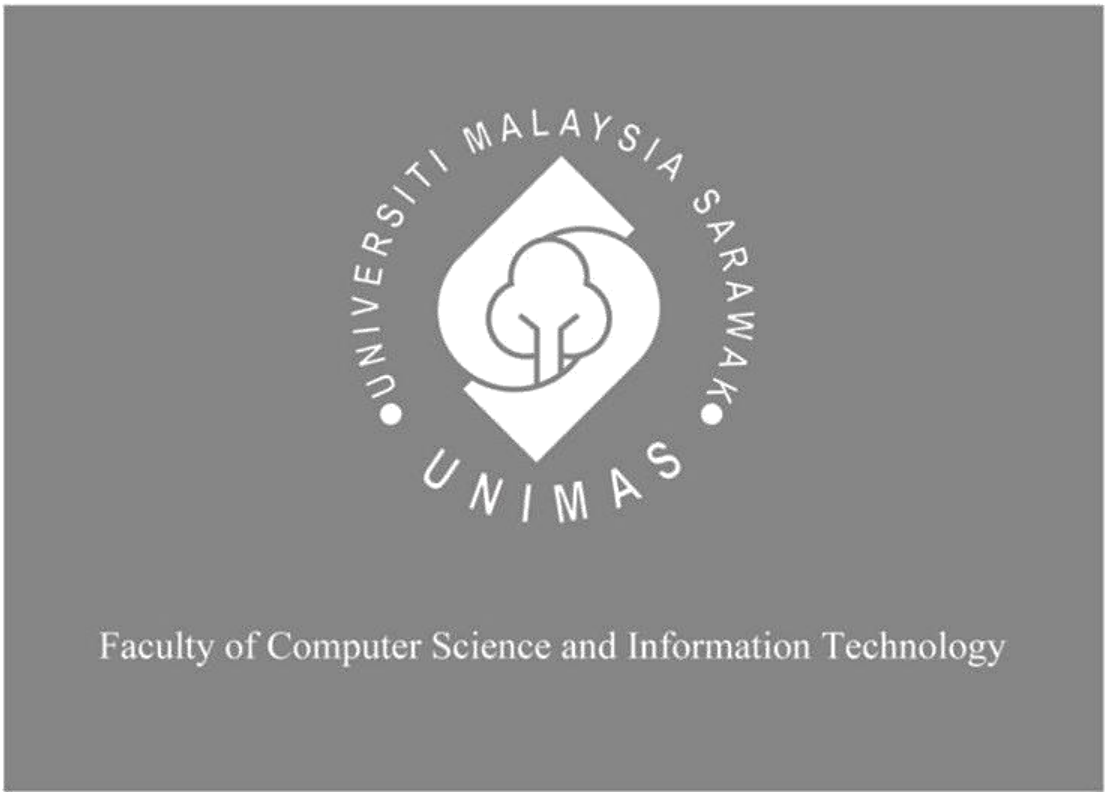

FRACTIONAL PROPERTY OWNERSHIP BY USING BLOCKCHAIN ALGORITHM

Gan Jia Wei

Bachelor of Computer Science with Honours (Computational Science)

2019

FRACTIONAL PROPERTY OWNERSHIP
BY USING
BLOCKCHAIN ALGORITHM

GAN JIA WEI

This project is submitted in partial fulfilment of the
requirements for the Degree of
Bachelor of Computer Science with Honours

Faculty of Computer Science and information Technology
UNIVERSITI MALAYSIA SARAWAK
2019

PECAHAN PEMILIKAN HARTANAH
DENGAN MENGGUNAKAN
ALGORITMA BLOCKCHAIN

GAN JIA WEI

Projek ini merupakan salah satu keperluan untuk Ijazah
Sarjana Muda Sains Komputer dan Teknologi Maklumat

Fakulti Sains Konputer dan Teknologi Maklumat
UNIVERSITI MALAYSIA SARAWAK
2019

UNIVERSITI MALAYSIA SARAWAK

THESIS STATUS ENDORSEMENT FORM

TITLE FRACTIONAL PROPERTY OWNERSHIP BY USING BLOCKCHAIN ALGORITHM

ACADEMIC SESSION: 2018/2019

(CAPITAL LETTERS)

hereby agree that this Thesis* shall be kept at the Centre for Academic Information Services, Universiti Malaysia Sarawak, subject to the following terms and conditions:

1. The Thesis is solely owned by Universiti Malaysia Sarawak
2. The Centre for Academic Information Services is given full rights to produce copies for educational purposes only
3. The Centre for Academic Information Services is given full rights to do digitization in order to develop local content database
4. The Centre for Academic Information Services is given full rights to produce copies of this Thesis as part of its exchange item program between Higher Learning Institutions [or for the purpose of interlibrary loan between HLI]
5. ** Please tick (√)

☐	CONFIDENTIAL	(Contains classified information bounded by the OFFICIAL SECRETS ACT 1972)
☐	RESTRICTED	(Contains restricted information as dictated by the body or organization where the research was conducted)
☑	UNRESTRICTED	

(AUTHOR'S SIGNATURE)

Permanent Address

No. 4, Jalan SR 8/9, Taman Putra Indah, Serdang Raya, 43700 Seri Kembangan, Selangor

Date: 21/5/2019

Validated by

(SUPERVISOR'S SIGNATURE)

Dr Muhamad Taufan bin Haji Abdan
Senior Lecturer
Faculty of Computer Science and Information Technology
University Malaysia Sarawak

Date: 21/05/2019

Note * Thesis refers to PhD, Master, and Bachelor Degree
** For Confidential or Restricted materials, please attach relevant documents from relevant organizations / authorities

DECLARATION

I hereby declare that this project is my original work. I have not copied from any other student's work or from any other sources except where due reference or acknowledgement is not made explicitly in the test, nor has any part has been written for me by another person.

……

(GAN JIA WEI) 21st May 2019

Matric No.: 51826

ACKNOWLEDGEMENT

First of all, I wish to express my deepest gratitude to my supervisor, Dr. Mohammad Imran bin Bandan, who has been wholeheartedly guided me, and provided invaluable and continuous support throughout this project. Besides, I would like to thanks Prof. Wang Yin Chai who has provided us with useful lessons during lectures. Furthermore, I would like relay a thousand thanks to Mr. Daniel Loh, CEO of Sage Interactive Sdn Bhd, who allowed me to use the company's system as my final year project.

I would also like to take this chance to express my appreciation to all the respondent who have helped and contribute to this project including my friends and course mates. Last but not least, I feel thankful and grateful for my family who have given me support on completing this project.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

Fractional property ownership has been a trend for property investors because of its flexibility that allows investors to invest fractionally in not only one property, but several properties. Fractional ownership is being defined as a percentage ownership in an asset. Fractional ownership shares are the assets sold to the property investors who share the benefits of the asset such as usage rights, income sharing and priority access. With fractional ownership, the value of the shares increases with the assets increases in value. In other words, fractional ownership is a form of collaborative consumption where overall cost of a property is split among a group of property owners. By doing so, we implemented ERC20 token as smart contract to fractionalise the a single token into shares. Nonetheless, there are also increasingly more perpetrators tried to penetrate the investment details of the investors in order to tamper with the information for their personal gain. Therefore, to safeguard the investment/transaction details of the investors, a secure cryptosystem is required to safeguard the sensitive transaction data. In our project, we are going to develop a property website where it provides fractional property investment for the investors. Furthermore, blockchain technology will be implemented in order to safeguard the investment/transaction details. Therefore, the transaction details are meddle-proof and immutable. This ensures the accountability, confidentiality, and integrity of the transaction details. At the same time, we have taken full advantage of the key characteristics of Ethereum blockchain technology to not only ensure that upmost security is provided to the transaction details, but also to solve the issues of heavy cost and bottleneck induced by heavy traffic of transactions, to provide anonymity for the investors, and to verify and track the transactions effectively. In the near future, we are going to integrate the module in a property website to allow fractional property investment for the investors in real world.

ABSTRAK

Pemilikan harta pecahan telah menjadi trend bagi para pelabur hartanah oleh kerana fleksibiliti yang membenarkan para pelabur untuk melabur secara kecil-kecilan dalam bukan hanya satu hartanah, tetapi beberapa hartanah. Pemilikan pecahan didefinisikan sebagai peratusan pemilikan dalam aset. Saham pemilikan pecahan adalah aset yang dijual kepada pelabur hartanah yang berkongsi manfaat aset seperti hak penggunaan, perkongsian pendapatan dan akses keutamaan. Dengan pemilikan pecahan, nilai saham meningkat dengan aset yang meningkat dalam nilai. Dengan kata lain, pemilikan pecahan adalah satu bentuk penggunaan kolaboratif di mana kos keseluruhan sesuatu harta dipecahkan kepada sekumpulan pemilik hartanah. Dengan berbuat demikian, kami melaksanakan token ERC20 sebagai kontrak pintar untuk memecahkan satu token kepada beberapa saham. Walau bagaimanapun, terdapat semakin banyak pelaku yang cuba menembusi butiran pelaburan para pelabur untuk merosakkan maklumat demi keuntungan peribadi. Oleh itu, untuk melindungi butiran pelaburan atau transaksi para pelabur, cryptosystem yang selamat diperlukan untuk melindungi data sensitif transaksi. Dalam projek kami, kami akan membangunkan laman web hartanah di mana laman web tersebut dapat menyediakan pelaburan harta pecahan untuk para pelabur. Tambahan lagi, teknologi blockchain akan dilaksanakan untuk melindungi butiran pelaburan / transaksi. Oleh itu, butir-butir transaksi adalah tahan campur tangan dan tidak dapat diubah. Ini akan memastikan kebertanggungjawab, kerahsiaan, dan integriti butiran transaksi. Pada masa yang sama, kami telah memanfaatkan sepenuhnya ciri-ciri utama teknologi blockchain Ethereum bukan sahaja untuk memastikan jaminan keselamatan diberikan kepada butir-butir transaksi, tetapi juga untuk menyelesaikan isu-isu kos berat dan kesesakan yang disebabkan oleh transaksi yang banyak, untuk menyediakan anonimiti ataupun privasi kepada para pelabur, dan untuk mengesahkan dan menjejaki transaksi secara berkesan. Dalam masa terdekat, kami akan mengintegrasikan modul dalam laman web hartanah untuk membolehkan pelaburan hartanah pecahan untuk pelabur dalam alam realiti.

Chapter 1: Introduction

1.1 Introduction

Fractional property ownership has been a trend for property investors because of its flexibility that allows investors to invest fractionally in not only one property, but several properties. Fractional ownership is being defined as a percentage ownership in an asset. Fractional ownership shares are the assets sold to the property investors who share the benefits of the asset such as usage rights, income sharing and priority access. With fractional ownership, the value of the shares increases with the assets increases in value. In other words, fractional ownership is a form of collaborative consumption where overall cost of a property is split among a group of property owners. Shareholders are able to buy shares that represents a fraction of property. When property is sold out for a profit by a fractional owner, it serves as a form of property investment. A fractional property ownership or the transaction details of the investors will be recorded as a prove that the investment has been done. However, there are increasingly more perpetrators tried to infiltrate the investment details of the investors in order to tamper with the information for their personal gain. Therefore, to safeguard the investment/transaction details of the investors, a secure cryptosystem is required to safeguard the sensitive transaction data. Blockchain technology is being used to safeguard fractional property ownership functionally in the current existing system because it is a digitized, decentralised, public ledger of all cryptocurrency transactions, and most importantly it provides security for the details of property investment. A block is a 'current' part of a blockchain, which records the transaction/investment details. Once completed, a block goes into the blockchain as a permanent database. Each time a block gets completed, a new one is generated. There is a countless number of such blocks in the blockchain, connected to each other in proper linear, chronological order. The blockchain was designed so the investment/transaction details are immutable, meaning they cannot be deleted. The blocks are added through cryptography,

ensuring that they remain meddle-proof; meaning that the data can be distributed, but not copied.

1.2 Problem Statement

There are more and more people wish to invest in property due to lucrative returns. But most of the people unable to afford the purchase the property due to significant increase of property value over the years. As this problem emerged, people prefers to have a fraction of property ownership, so that they will not be financially burdened. To address this problem, fractionalisation of property ownership is introduced for the investors, so that they can not only invest a fraction in a single property unit, but multiple property units as well. As fractional property ownership is more affordable and it spreads the costs around ("Fractional Ownership: 9 Reasons Why You Should Look Into It", 2017). Furthermore, the shares is saleable and transferrable without any hassle. Nonetheless, the existence of fractional property ownership bears another problem. The concern is that there are increasingly more perpetrators attempted to infiltrate the transaction details for their personal gains. Therefore, a blockchain is designed to overcome the abovementioned issues.

1.3 Project Description

There are increasingly more people tried to invest in property as they foresee the future prospects and long-term benefits of property investment. However, most of the people cannot seem to afford high-priced property due to significant increase of property value over the years.. Hence, I proposed fractional property ownership to make real estate investing more accessible to the investors by lowering capital requirements. Also, to allow the investors to buy multiple shares from different property units. The transaction/investment details will be store in the database afterwards. However, the transaction/investment details in the database can still be tampered by the perpetrators since the database itself did not provide any trustworthy security. Hence, a blockchain cryptosystem will be implemented in order to safeguard the sensitive data. The blockchain is meddle-proof where it provides imperishable evidence for the investment done by the investor.

1.4 Scope

Fractional property ownership module is a simple-looking yet complicated system that is develop for fractional property investors. The main focus of this system is to provide fractional property investment for investors. Besides, the blockchain will emphasizes on providing security for sensitive transaction details.

1.5 Aims and Objectives

The aim and objectives of this system are as follow:

1. To implement fractional property ownership module where investors can buy shares and transfer shares.
2. To design a blockchain that stores and safeguard the transaction details of fractional property investment.

1.6 Significance of Project

The focus of the project is to develop a fractional property ownership module by using blockchain technology where it can be implemented in a property website in the future.

1.7 Expected Outcome

A fractional property ownership that allows investors to buy property shares and transfer property shares between investors. Afterwards, the transaction/investment details is safeguarded by blockchain where it allows everyone to access only to view but cannot tampered with.

1.8 Project Outline

The project outline is categorized into six chapters:

i. Chapter 1: Introduction

Chapter 1 provides the overview of fractional property ownership and blockchain technology.

ii. Chapter 2: Literature Review

Chapter 2 further elaborates on the concepts of fractional property ownership and blockchain technology. Furthermore, this chapter provides the study of various blockchain platforms to decide on which platform to be used for module development. In addition, this chapter provides a brief review on existing fractional property ownership modules as a reference for future implementation into the property website.

iii. Chapter 3: Requirement Analysis and Design

Chapter 3 describes the methodology used for the module development. Besides, there are three system designs shown in this chapter which are architectural design, modules design, and interface design. Use case diagram and sequence diagram are included in modules design.

iv. Chapter 4: Implementation

Chapter 4 reports on implementation of fractional property ownership module. It also elaborates on the functionality in the module. Also, this chapter presents and discusses the interface and functionality of the module, as well as the code snippet used for the front-end development of the module. Moreover, logic code of the smart contract is further explained in this chapter.

v. Chapter 5: Testing

Chapter 5 shows the software testing performs on the fractional property ownership module. The results of functionality testing and usability testing are illustrated to evaluate whether the module has achieve its requirement specification, and determine whether the system is user friendly.

vi. Chapter 6: Conclusion and Future Works

Chapter 6 discusses about contribution, limitation and future works of the project. A conclusion is given to summarize the project as a whole.

1.9 Conclusion

In conclusion, fractional property ownership module is an investment module that can be integrated in a property website to allow fractional property investment by the investors. The blockchain will be used in the development of fractional property ownership to tokenize the shares and protect the sensitive information (e.g. transaction details) of the investors. Also, this module will provides very much needed confidentiality and integrity for fractional property investment.

Chapter 2: Literature Review

2.1 Introduction

In this chapter, the concept of fractional property ownership and overview of blockchain technology will be discussed. In the overview of the blockchain technology, the general architecture of the blockchain, key characteristics of blockchain, consensus algorithm of blockchain, and the concept of blockchain technology will be covered and explained in details. Furthermore, the features between various blockchain platforms will also be compared to decide on the blockchain platform that best suited for the development of fractional property ownership module. In addition, the similar existing module will also be reviewed as a future references for integration in a property website.

2.2 Fractional Property Ownership

According to Chen (2018), fractional property ownership is a percentage ownership in a property. Fractional ownership in a property are sold to individual shareholders who share the benefits of the property such as usage rights, income sharing, priority access and reduced rates. In this project, we are going to design a blockchain to store the transaction details for each fraction of the property sold. Once a fraction is sold, its information and details will be registered in the blockchain under the owner's account. Also, the fraction could be transferred to another owner.

2.3 Overview of Blockchain Technology

In this section, the general architecture of the blockchain, key characteristics of blockchain, consensus algorithm of blockchain, and the concept of blockchain technology will be covered and explained in details.

2.3.1 General Architecture of Blockchain

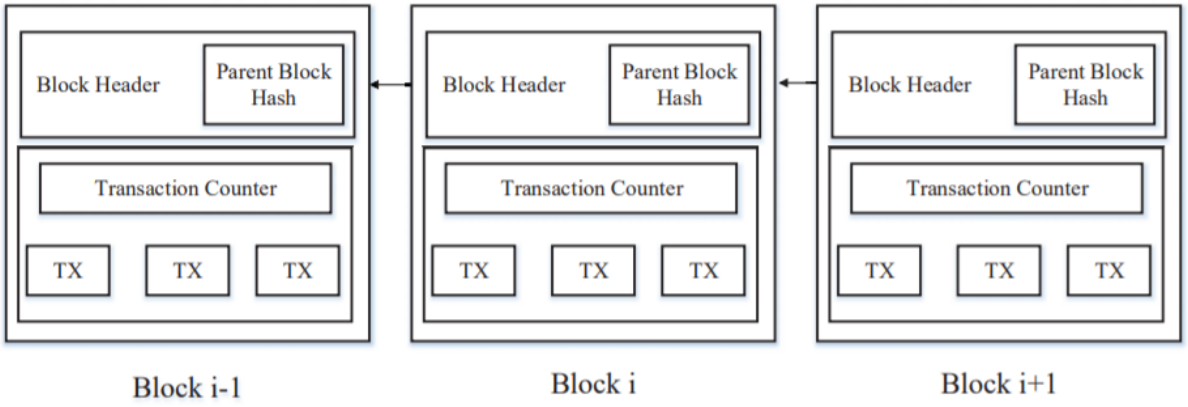

Figure 2.1: An example of blockchain (Zheng et al., 2017).

Blockchain is a sequence of blocks. In each block, it holds a complete list of transaction records like conventional public ledger. Figure 2.1 depicts an example of blockchain which consists of a continuous sequence of blocks. A block has a parent block which stores the previous block hash in the block header. It is worth mentioning that uncle blocks (children of the block's ancestors) hashes would also be stored in Ethereum blockchain (Zheng et al., 2017).

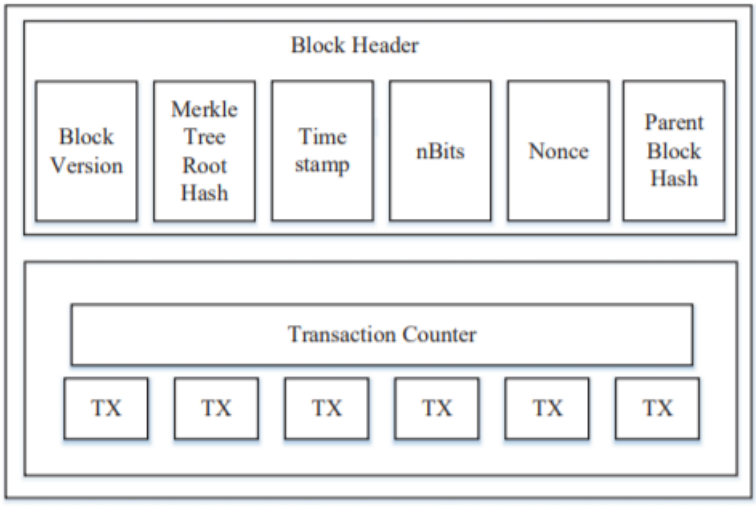

Figure 2.2: Block structure (Zheng et al., 2017).

As shown in Figure 2.2, a block consists of the block header and the block body. In the block header, there are block version, Merkle tree root hash, time stamp, nBits, nonce, and parent block hash. The block header determines the set of block validation rules to abide.

Merkle tree root hash is the hash value of all transactions in the block. Timestamp is the current universal time in seconds since the blockchain started up. nBits is the maximum level of bits for a valid block hash considered to be acceptable. Nonce is a 4-byte field, that normally begins with 0 and increases for every hash calculation. Parent block hash is a 256- bit hash value that points to the previous block. The block body is composed of a transaction counter and transactions. The maximum number of transactions that a block can contain depends on the block size and the size of each transaction.

2.3.2 Key Characteristics of Blockchain

According to Zheng et al. (2017), blockchain has the key characteristics of decentralization, persistency, anonymity, and auditability. The use of decentralised transaction system by blockchain has resolved the issues of heavy cost and bottleneck induced by heavy traffic of transactions which has to be validated through one central trusted agency because there is no central trusted agency. Therefore, consensus algorithms are employed to maintain data consistency in distributed network. Furthermore, the trait of persistency implies that it is nearly impossible to delete or rollback transactions once they are included in the blockchain. As anonymity suggested, each user can interact with the blockchain with a generated address without revealing the real identity of the user. Last but not least, the auditability of the blockchain means that the transactions can be easily verified and tracked.

2.3.3 Consensus Algorithms of Blockchain

In blockchain, how to reach a consensus in distributed environment is a challenge because there is no central node that ensures ledgers on distributed nodes are consistent. Therefore, some protocols or approaches are needed in order to reach a consensus in blockchain. However, we are going to discuss the most popular approaches which are currently adopted by the two biggest blockchain giants known as Bitcoin and Ethereum. But before we begin to

explain on consensus algorithm, it's important to understand what is node in blockchain on first-hand. A node is a device or program or client that communicates with the blockchain network. A famous example of node for Ethereum blockchain is Go-Ethereum (Geth).

PoW (Proof of Work) is a consensus approach used in Bitcoin blockchain. In PoW, each node of the network is calculating a hash value of the block header. The block header contains a nonce and miners would change the nonce frequently to get different hash value. The consensus requires that the calculated value must be equal to or smaller than a certain given value (Zheng et al.). When one node reaches the target value, it would broadcast the block to other nodes and all other nodes must mutually confirm the correctness of the hash value. If the block is validated, other miners will append this block to their own blockchains. Miners have to do a lot of computer calculations in PoW, yet these works waste too much resources.

PoS (Proof of Stake) is an energy-saving alternative to PoW. PoW (Proof of Work) is a consensus approach currently employed by Ethereum blockchain. In PoS, the creator of a new block is chosen in a deterministic way, where miners have to prove the ownership of the amount of currency (Zheng et al.). It is believed that people with more currencies is less likely to attack the network. The selection based on account balance is quite unfair because the single richest person is bound to be dominant in the network. As a result, many solutions such as Blackcoin and Peercoin are proposed with the combination of the stake size to decide which one to forge the next block. The PoS system has no block reward for the miners who forge the blocks, therefore they only take the transaction fees. Unfortunately, as the mining cost is nearly zero, attacks might come as a consequences. Therefore, Casper protocol is introduced in PoS system to set some circumstances under which miners who violates some set of rules might have their deposits being confiscated.

In a nutshell, PoS saves more energy and is more cost-effective in comparison to PoW. Also, PoS is a safer network as attacks become more expensive because Ethereum blockchain

is able to manipulate market price immediately. Many blockchains adopt PoW at the beginning and transform to PoS gradually.

2.3.4 Concept of Blockchain

As mentioned before, blockchain is a chain of blocks that stored digital information in a public ledger or database. In fact, the blocks on the blockchain are made up of digital pieces of information. Specifically, they made up of three parts: blocks store information about the transactions, blocks store information who is participating in transaction, and blocks store information that distinguishes them from other blocks. Figure 2.1 above shows that each block stores a unique code called hash that distinguish the blocks apart from each other. The transaction information and transaction participants information can be viewed by the investors through a dedicated website for a particular blockchain platform. The reason that blockchain is chosen to implement fractional property ownership because it is very difficult to go back and alter the contents of the block. That's because each block contains its own hash, along with the hash of the block before it. Hash codes are created by a math function that turns digital information into a string of alphanumerical values (Fortney, 2018). If that information is being tampered with, the hash code will changes as well. For instance, if an imposter wants to change the contents of a single block, then the imposters need to change every single block after it on the blockchain in order to cover their tracks. Recalculating all those hashes would consume an enormous and improbable amount of computing power. In other words, it is very difficult to tamper and delete a block once it is added to the blockchain.

2.4 Comparison of Features between Blockchain Platforms

The following Table 2.1 shows the summary of features of top five blockchain platforms ("The top 5 enterprise blockchain platforms you need to know about", 2018) that has normally been used for enterprises. The comparison is made to determine the best blockchain platform for the project's blockchain development.

Table 2.1: Summary of features of top five blockchain platforms.

	Ethereum	Hyperledger Fabric	R3 Corda	Ripple	Quorum
Industry focus	Cross-Industry	Cross-Industry	Financial Services	Financial Services	Cross-Industry
Ledger Type	Permission-less	Permissioned	Permissioned	Permissioned	Permissioned
Cryptocurrency	Ether (ETH)	None	None	Ripple (XRP)	None
Consensus Algorithm	Proof of Stake	Pluggable Framework	Pluggable Framework	Probabilistic Voting	Majority Voting
Governance	Ethereum Developers	Linux Foundation	R3 Consortium	Ripple Labs	Ethereum Developers & JP Morgan Chase
Smart contract functionality	Yes	Yes	Yes	No	Yes

Ethereum is an open-source and blockchain-based distributed computing platform proposed by Vitalik Buterin. Ethereum is known for running smart contracts on a custom-built blockchain. Ethereum Virtual Machine (EVM) provides the run-time environment to smart contracts in Ethereum. Ethereum have been widely adopted because it is a public (permission-less) blockchain platform built for restricted access versus mass consumption (Takyar, n,d,). Moreover, the Ethereum community has made a transition from PoS (Proof of Stake) to PoW (Proof of Work) based platform because PoS is relatively greener and cheaper distributed form of consensus. Furthermore, PoS is a safer network compared to PoW as attacks becomes more expensive with rapid market price manipulation. Ether is a native cryptocurrency of Ethereum, used for fuelling the Ethereum ecosystem. A developer who builds applications using Ethereum has to pay charges in Ethers, for executing transactions and running apps on the Ethereum