THE STUDY OF BLOCKCHAIN TECHNOLOGY AND DIGITAL CURRENCY: A CASE STUDY OF DIGITAL CURRENCY CREATION BASED ON ETHEREUM NETWORK

NUTTIRA THONGLIAM

A THEMATIC PAPER SUBMITTED IN
PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR
THE DEGREE OF MASTER OF SCIENCE
(INFORMATION TECHNOLOGY MANAGEMENT)
FACULTY OF GRADUATE STUDIES
MAHIDOL UNIVERSITY
2019

Thematic Paper
entitled

THE STUDY OF BLOCKCHAIN TECHNOLOGY AND DIGITAL CURRENCY: A CASE STUDY OF DIGITAL CURRENCY CREATION BASED ON ETHEREUM NETWORK

.....
Miss Nuttira Thongliam
Candidate

.....
Assoc. Prof. Adisorn Leelasantitham,
Ph.D. (Electrical Engineering)
Major advisor

.....
Asst. Prof. Supaporn Kiattisin,
Ph.D. (Electrical and Computer
Engineering)
Co-advisor

.....
Prof. Patcharee Lertrit,
M.D., Ph.D. (Biochemistry)
Dean
Faculty of Graduate Studies
Mahidol University

.....
Asst. Prof. Supaporn Kiattisin,
Ph.D. (Electrical and Computer
Engineering)
Program Director
Master of Science Program in
Information Technology Management
Faculty of Engineering
Mahidol University

Thematic Paper
entitled

THE STUDY OF BLOCKCHAIN TECHNOLOGY AND DIGITAL CURRENCY: A CASE STUDY OF DIGITAL CURRENCY CREATION BASED ON ETHEREUM NETWORK

was submitted to the Faculty of Graduate Studies, Mahidol University
for the degree of Master of Science (Information Technology Management)
on
June 10, 2019

.....
Miss Nuttira Thongliam
Candidate

.....
Smitti Darakorn Na Ayuthaya,
Ph.D. (Public Administration)
Chair

.....
Assoc. Prof. Adisorn Leelasantitham,
Ph.D. (Electrical Engineering)
Member

.....
Chaiyaporn Panyindee
Ph.D. (Electrical Engineering)
Member

.....
Asst. Prof. Supaporn Kiattisin,
Ph.D. (Electrical and Computer Engineering)
Member

.....
Prof. Patcharee Lertrit,
M.D., Ph.D. (Biochemistry)
Dean
Faculty of Graduate Studies
Mahidol University

.....
Asst. Prof. Jackrit Suthakorn,
Ph.D. (Robotics)
Dean
Faculty of Engineering
Mahidol University

ACKNOWLEDGEMENTS

Foremost, I would like to express my deepest appreciation to all those who provided me the possibility to complete this research, special gratitude I give to my advisor, Assoc. Prof. Adisorn Leelasantitham, whose contribution in stimulating suggestions and encouragement, helped me to coordinate my research especially in guide this research. Besides advisor, I would like to thank my research committee: Smitti Darakorn Na Ayuthaya, Asst. Prof. Supaporn Kiattisin, and Chaiyaporn Panyindee for their encouragement, insightful comments, and their questions.

Furthermore, I would also like to acknowledge with much appreciation the crucial role of the staffs, who gave the permission to use all required equipment and the necessary materials to complete the research. Special thanks go to friends, who help me to assemble the parts and gave suggestion everything.

Finally, I would like to thank all of those who I have not listed above.

Nuttira Thongliam

THE STUDY OF BLOCKCHAIN TECHNOLOGY AND DIGITAL CURRENCY: A CASE STUDY OF DIGITAL CURRENCY CREATION BASED ON ETHEREUM NETWORK

NUTTIRA THONGLIAM 5937539 EGIT/M

M.Sc. (INFORMATION TECHNOLOGY MANGEMENT)

THEMATIC PAPER ADVISORY COMMITTEE: ADISORN LEELASANTITHAM, Ph.D., SUPAPORN KIATTISIN, Ph.D.

ABSTRACT

This research focuses on Blockchain technology, which receives a lot of attention currently due to its structure that focuses on the data transmission between clients without central control. Blockchain not only helps reduce the cost of moving data but also reduce the risk of cybercrime due to the data encrypted to control security during data transportation and data integrity validation between each client. The research also focuses on the case of creating a digital currency or Cryptocurrency based on Ethereum network to comprehend about Blockchain algorithm. Moreover, the research also compares Blockchain network and digital wallet platforms to investigate which one is effective and suitable for each kind of user.

The study finds that the Blockchain networks have several objectives and their algorithms have different processes according to the suitability of the purpose. MetaMask is the appropriate tool for beginners to develop digital currency because the tool is an extension of Chrome, web browser developed by Google, which comes with Ethereum network as Blockchain that supports the development of both production environment and testing environments. This research helps persons who are interested in Blockchain technology and digital currency creation process as a guideline for using this powerful technology and helps them decide to change the traffic structure for reducing costs and increasing security during data transportation.

KEY WORDS: BLOCKCHAIN/ CRYPTOCURRENCY/ DIGITAL WALLET

64 pages

การศึกษาเทคโนโลยีบล็อกเชนและสกุลเงินดิจิทัล กรณีศึกษาการสร้างสกุลเงินดิจิทัลบนเครือข่ายเอธิเรียม

THE STUDY OF BLOCKCHAIN TECHNOLOGY AND DIGITAL CURRENCY: A CASE STUDY OF DIGITAL CURRENCY CREATION BASED ON ETHEREUM NETWORK

ณัฐฐิรา ทองเหลี่ยม 5937539 EGIT/M

วท.ม. (เทคโนโลยีการจัดการระบบสารสนเทศ)

คณะกรรมการที่ปรึกษาสารนิพนธ์: อดิศร ลีลาสันติธรรม, Ph.D., สุภาภรณ์เกียรติสิน, Ph.D.

บทคัดย่อ

เนื่องจากเทคโนโลยีบล็อกเชน (Blockchain) และสกุลเงินดิจิทัล (Cryptocurrency) เป็นเทคโนโลยีที่สามารถส่งข้อมูลระหว่างเครื่องผู้ใช้งานโดยปราศจากเครื่องควบคุมส่วนกลางและมีการเข้ารหัสข้อมูลรวมถึงมีการตรวจสอบความถูกต้องซึ่งกันและกันระหว่างเครือข่ายผู้ใช้งาน ทำให้ข้อมูลมีความปลอดภัย ป้องกันการปลอมแปลง ใช้เวลาในการยืนยันความถูกต้องน้อยลงและค่าใช้จ่ายในการรับ/ส่งข้อมูลมีราคาที่ถูกลง จึงทำให้เทคโนโลยีนี้ได้รับความสนใจเป็นอย่างมากในปัจจุบัน การศึกษาวิจัยนี้ยังมุ่งเน้นศึกษาการสร้างสกุลเงินดิจิทัล บนเครือข่ายเอธิเรียม (Ethereum) เพื่อทำความเข้าใจในกระบวนการทำงานของเทคโนโลยีบล็อกเชน รวมถึงการเปรียบเทียบเครือข่ายบล็อกเชน และศึกษาเครื่องมือในการพัฒนาสกุลเงินดิจิทัล ซึ่งสามารถสร้างสกุลเงินดิจิทัลให้มีความเร็วรวดและมีประสิทธิภาพ ผลการศึกษาพบว่า การพัฒนาระบบบนเทคโนโลยีบล็อกเชน นั้นสามารถทำได้หลากหลายตามจุดประสงค์ที่แตกต่างกันออกไปเช่น การจัดเก็บเอกสาร การรับส่งข้อมูลทางการเงิน รวมถึงสกุลเงินดิจิทัล ซึ่งทำให้ขั้นตอนกระบวนการภายในของเทคโนโลยีก็มีความแตกต่างกันตามความเหมาะสมของจุดประสงค์นั้น ๆ

การศึกษาวิจัยนี้ได้ใช้เครื่องมือเมตะมาร์ค (MetaMark) ซึ่งเป็นเครื่องมือที่เหมาะสมสำหรับผู้เริ่มต้นพัฒนาสกุลเงินดิจิทัล เนื่องจากเครื่องมือนี้เป็นส่วนขยายของเว็บเบราว์เซอร์โครม (Chrome) ซึ่งสามารถใช้งานได้กับเครือข่ายเอธิเรียมที่รองรับการพัฒนาทั้งระบบสภาพแวดล้อมในการใช้งานจริง และระบบสภาพแวดล้อมเพื่อใช้ในการทดสอบ การศึกษาวิจัยเรื่องนี้สามารถช่วยให้ผู้พัฒนาระบบ และผู้ที่สนใจ เข้าใจถึงกระบวกการทำงานของบล็อกเชน และการสร้างสกุลเงินดิจิทัลบนเครือข่ายบล็อกเชน หรือใช้ประกอบการตัดสินใจเปลี่ยนแปลงโครงสร้างการรับส่งข้อมูลเดิม เพื่อลดค่าใช้จ่าย เพิ่มความปลอดภัยและความถูกต้องในการส่งต่อข้อมูล

64 หน้า

CONTENTS

CONTENTS (cont.)

LIST OF TABLES

LIST OF FIGURES

CHAPTER I
INTRODUCTION

This chapter introduces the thematic paper, the study of Blockchain technology and digital currency with a case study of digital currency creation based on Ethereum network. The chapter is consisted of background, problem statement, purpose of study, scope of study, definitions, and expected results.

1.1 Background and Problem Statement

Currently, we are living in an era of digital world where technology is influenced how human living by disguise in everyday life. Technology evolution rate is continuous increases, so people cannot stop improving himself to abreast it. Everyone should always study at all times to keep pace with the world that is never stopped growing. In the hope that, people to be able to apply the new knowledge to be benefits that make our lives more convenient. In addition, Blockchain technology is affected finance, people have alternative ways for payment such as online banking. As a result, the online currency is available with various payment systems.

Cryptocurrency is digital currencies performed by using encryption and decryption algorithm to secure transactions and control the creation of new coins. The traditional currencies is open, we enable to know our transactions who receive the money from you or you transfer to someone. However, the encryption in the ledgers of all transactions makes it difficult to counterfeit. The hallmark of Cryptocurrency that government cannot control the value and unable to handle it due to full decentralization system [1]. For this reason, Cryptocurrency is the fastest and most convenient way to pay for worldwide privacy. The emergence of Cryptocurrency may be another turning point in the evolution of money.

1.2 Purpose of Study

1) To study Blockchain technology by analysis Blockchain network and digital wallet platform.

2) To study the Cryptocurrency creation process base on Ethereum network as the case study of this research.

3) To compare the top rank of Cryptocurrency and digital wallet platform.

1.3 Scope of the study

The scope of this research is focused on Blockchain network comparison and digital wallet platform comparison. Moreover, we focus on the case study of digital currency creation based on Ethereum network. The factors for Blockchain network comparison are Blockchain's objective, stored data type, developed language, participation, currency, block-release timing, transaction size, transaction rate, consensus type, and mining algorithm. On the other hand, the factors for digital wallet comparison are digital wallet type, web browser extension, private key on client side, and private key or password recovery.

1.4 Definitions

1.4.1 Blockchain

Blockchain is a network system to store online transactions. The network looks like a spider web network, which holds statistics on financial transactions and other digital assets without intermediary such as financial institution, settlement office, etc.

1.4.2 Cryptocurrency

Cryptocurrency is decentralized digital currency using encryption to secure transactions and control the creation of new coins. In general, Cryptocurrency is open source but encryption process in each block that makes it difficult to counterfeit.

Moreover, the government cannot control the value Cryptocurrency because it cannot handle due to full decentralization.

1.4.3 Digital wallet

Digital wallet used to keep digital assets. The digital wallet contains two components, which are block address and private key. The address like a bank account number, which is a long set of numeric codes, one set that used to be the address transfer. The private key or signature is an indication of digital wallet ownership. They key is an account password to verify identity.

1.5 Expected benefits

1.5.1 Academic benefits

1.5.1.1 Expanding knowledge of research that related to Blockchain technology and digital currency with a case study of digital currency creation based on Ethereum network.

1.5.2 Business benefits

1.5.2.1 To guide for new joiners to learn about Blockchain technology and digital wallet platform.

1.5.2.2 To guide for web application development design. The research explains about Blockchain that can improve the data structure by increased security level.

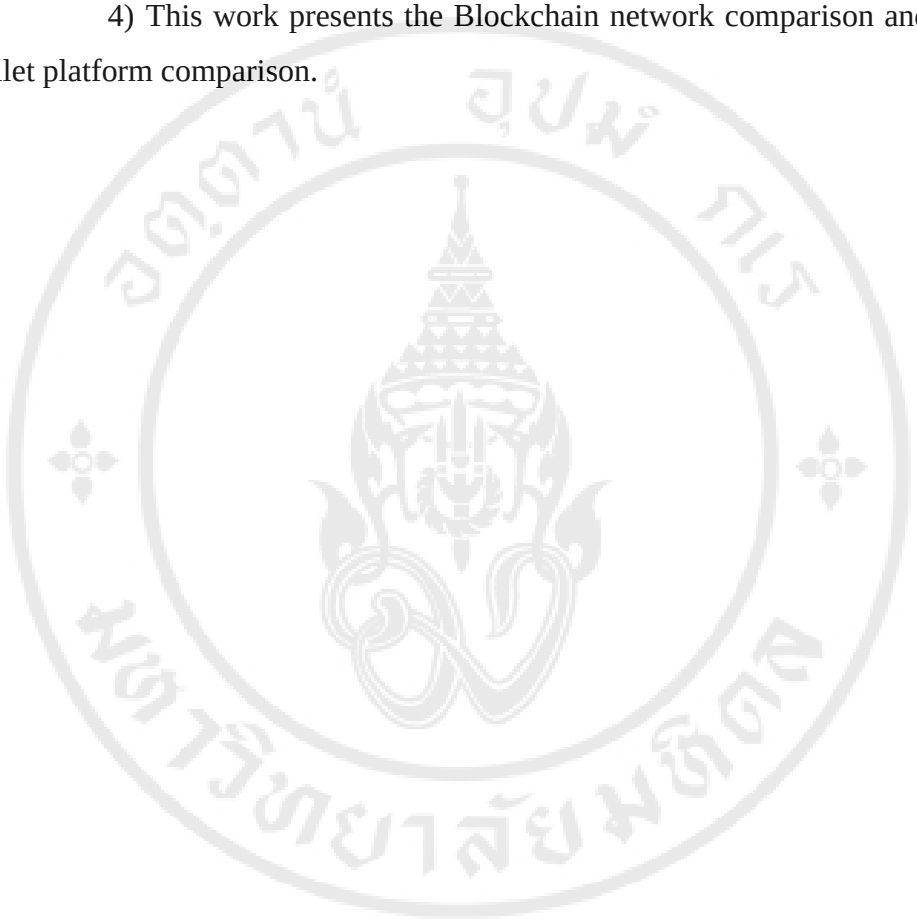
1.6 Expected Results

1) This research can be applied to other application development. This research is unable to apply Blockchain technology in order to increase security level in application development.

2) This research can be a guideline for application developer to select a high security data structure for their works.

3) This research can be a guideline for a new Blockchain joiner to select a suitable digital wallet platform.

4) This work presents the Blockchain network comparison and the digital wallet platform comparison.



CHAPTER II
LITERATURE REVIEW

The world of financial technology should be more familiar with Blockchain. Digital currency or Cryptocurrency is difficult to explain because of complexity. After Bitcoin become popular, many organizations bring the concept of Bitcoin to develop their digital currencies in a similar way, but they changed some technical details [9]. As a result, we have to study more about the background of Cryptocurrency, Blockchain and smart contact, which is an evolution of Blockchain.

2.1 Introduction of Cryptocurrency

Cryptocurrency is created based on computer system. The system work without central controller which is different from fiat currency. The system creator has to specify how to get money, amount of money that transfer in the system and how to use money. Moreover, everyone in the system receive each other transactions this is more secure and reveal.

Bitcoin is the first Cryptocurrency, so it is a trend that people around the world are keeping eyes on it. For this reason, the demand is increased and the price has increased about 600% since the beginning of 2017. Bitcoin has outperformed traditional currencies in many areas, such as faster international money transfers because intermediaries are not required to confirm the transaction. As a result, the transfer is completed within 10 minutes, which is much faster than the previous one, which takes at least 2-3 days. Bitcoin is also highly secure as people in the system will have the same database and real-time transactional data is recognized, so it is difficult to attack the system.

The popularity of Bitcoin has affected in Cryptocurrency. More than one thousand currencies have been created by following the Bitcoin system. It has been enhanced a variety of features. For example, the Ethereum, which is Outstanding in

terms of smart contracts to determine conditions of the transaction, such as create conditions to pay good when the good has been received or auto insurance claim when the plane is delayed. On the other hand, the Ripple is focused on international transfers that make the transfer safe and faster in just seconds. Both Cryptocurrencies are getting more attention from investors and financial institutions because there are benefits and can be applied to a variety of applications. As a result, the price has risen more than 3,000% from the beginning of 2017 (figure 2.1), making both currencies worth more than 20% of the Cryptocurrency market. Bitcoin also accounts for more than half and the rest are other currencies as shown in figure 2.2.

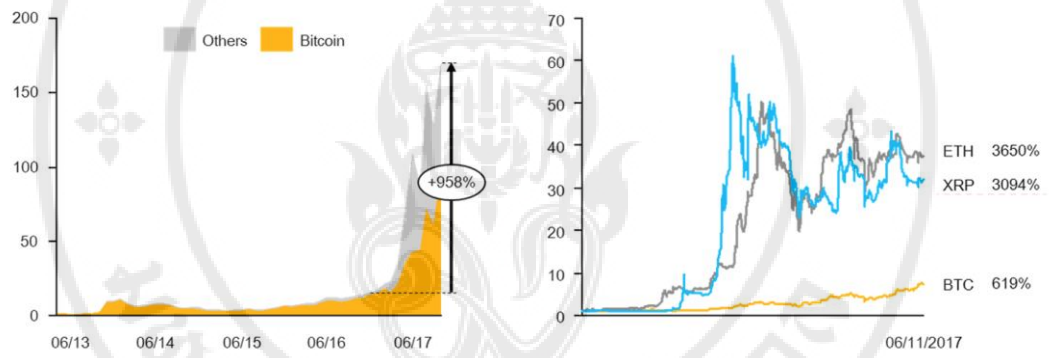


Figure 2.1 Increasing rate of Cryptocurrency value

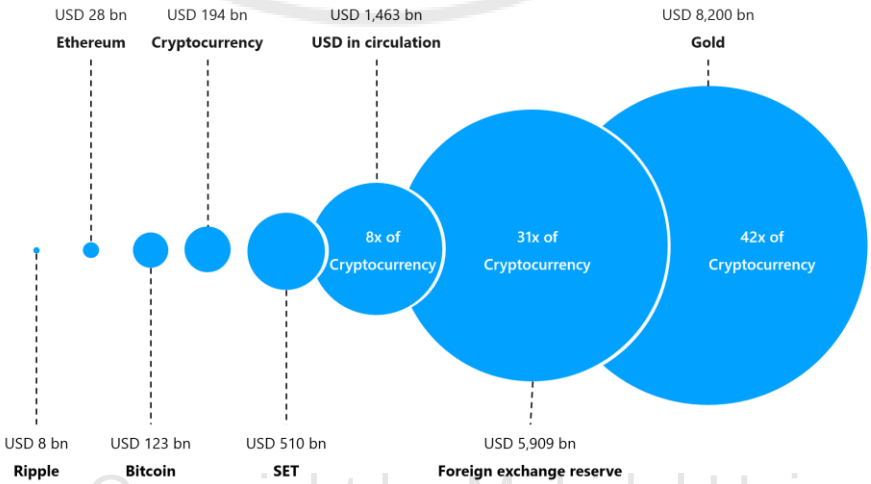


Figure 2.2 Cryptocurrency market value

However, the Cryptocurrency will be replacing the traditional currency might not be easy due to many restrictions such as small market capitalization and exchange rate fluctuations. Currently, Cryptocurrency has a very small market value which is smaller than the US dollar, which have been trading at a high level since the beginning of the year. Digital money like Bitcoin, Ether or Ripple has the potential to swing up to 14% within a day while the traditional currency fluctuated no more than 0.5%. The Cryptocurrency do not have the confidence that reflected in the number of stores accepting payment in digital currency and the user rate is very small, although the technology is being created for 8 years. Morgan Stanley shared about the number of stores accepting digital payments fell from five in the first quarter of 2016 to three in the second quarter of 2017. While most merchants still accept payments via Visa, Mastercard or PayPal.

The perspective of government and central banks in each country has not trusted the Cryptocurrency because the countries had been used Cryptocurrency are a limited number of official and alternative currencies, such as Japan, which allow Bitcoin to be one of the legitimate forms of payment. In addition, a number of countries have issued licenses to operate digital currency exchange services. Cryptocurrency is just a digital asset that has no value in itself. Moreover, some countries are moving and signalling negative signals, such as the Chinese government's ban on initial coin offering (ICO) and shutting down companies that offer digital currency exchanges.

Thai regulatory authorities, the Bank of Thailand (BOT), have not yet controlled and supervised Cryptocurrency officially. In contrast, there is a positive outlook on the development of new financial innovations (FinTech). BOT has not been announced Cryptocurrency to be able to pay the legal debt and recommended people should be aware of the risks of holding digital currency. However, the Thai regulatory authorities are paying attention to the backdrop of the technology which is Blockchain. It has the main feature in the area of data transparency, including developing regulations to support financial innovation such as creating a regulatory sandbox to enable entrepreneurs to test new financial products that are not legal in this case will help build confidence in the business sector to invest in the education and development of services using these technologies. The development Cryptocurrency

for using in financial institutions and public sector, there is a higher chance than the use of guests. Several financial institutions have begun to develop their own digital currency for use in banking transactions, such as Citigroup and MUFG, while the government is likely to develop the currency of each country to encourage people to use it. This will help the business sector and the public sector to reduce their transaction costs and management costs.

Blockchain and smart contracts have the potential and benefits to be applied to the business sector in the future. It can be applied to work processes that require verification and validation. This will help reduce the running time and increase efficiency for organizations. Firstly, keeping history of maintenance or aircraft maintenance, more efficient investigation of trading data. Secondly, record of medical records for use in analysis, which can determine the level of access to information. Lastly, tracking status and quality of goods, especially live food in real time.

Indeed, the demand for digital currency will rise sharply, but Cryptocurrency also faces many challenges, it is not only exchange rate fluctuations, but also the views of the regulators of each country. It is not easy for people to use it in public. However, the concept of Cryptocurrency which is the Bitcoin based on Blockchain technology is potential and can be applied to organizations to make the process work quickly and efficiently.

2.2 Introduction of Blockchain

Nowadays, it is undeniable that Blockchain technology is an innovation transformed the global industry. It is known that the person who created Blockchain is Satoshi Nakamoto or the father of the Cryptocurrency as Bitcoin that many people know well. Blockchain is a technology that had been changed the world as the Internet changed the world in the 1990s. It is a comparison that Blockchain is now like the Internet at the beginning. The financial sector has to working hard to try to figure out how to use Blockchain although it may not be applied in a concrete way.

Blockchain is a network system for storing online transaction accounts. The network is created like a spider web to keep statistics on financial transactions and

other assets in the future without a financial institution as central of exchanging. The Blockchain system does not have any middleware. For example, Bitcoin transaction will be generated Token code to communicate with each Blockchain to verify credible before the transaction is completed.

Blockchain is a network of transactions without middle of the existing financial institutions in the world, so this reduces cost of transaction. For this reason was effected intermediary financial institutions and liquidation office no need in the future if this technology is completely replaceable.

The information on Blockchain will be accessible to everyone. The Blockchain's database will not be stored in one place and unable to change. This means that the information recorded on Blockchain is publicly disclosed and can be verified. This data is not centralized control and protect. The hacker will not be able to hack this information because there is no central to attack that means if they want to hack to change that information. They must attack all distributed databases at the same time. Thousands of computers, millions of computers, will take care of this, giving everyone access to this information. Blockchain technology is a robust system. The information stored in boxes on Blockchain is not controlled by only one person and single point of failure cannot affect the system. Bitcoin was created in 2008. At that time Bitcoin's Blockchain never reported that its system was faulty or failed. However, hacking or mishandling occurs because of human error or human error at present. For example, hacking the web.

Ian Khan, a technology writer, said in Tedx, “The interesting thing about Blockchain is a mechanism to make everyone express their responsibility. Eliminate mistakes that may occur in transactions or errors caused by human actions or machines, or even exchanges that are not subject to the consent of the parties involved. In addition, the overriding importance of Blockchain technology has been help ensure the authenticity of the transaction by recording data not just to the primary recorder but it is the recorder of every connected party. Through a secure authentication mechanism.”.

Blockchain network uses the consensus algorithm. The system monitors transactions occurring during specific period such as Bitcoin checks every 10 minutes. Each of these is stored in a box called Block. The block has key features as follows:

1) Transparency of publicly accessible information

2) Data cannot be changed because it requires tremendous processing power to override all data on the network.

Theoretically, it is possible to have someone do that, but in practice, it is very difficult. The attempt to intervene Blockchain to steal coins is required electrical power to send by using computer processing is more than one country.

Vitalik Buterin, creator of Ethereum coin, said that "Blockchain technology address the problem of management. When I talk about this in the West, people say they trust Google, Facebook or a bank. People living in other continents do not trust many organizations and companies, which I refer to as Africa, India, Eastern Europe, or Russia. It is not about having to be rich to access this technology. In fact, Blockchain technology has the potential to reach even the most affluent countries."

A computer network is called a node will create a block. A node is a computer that is connected to a Blockchain network by using a client to authenticate and forward the transaction. The node receives a copy of Blockchain that is automatically downloaded when it enters the Blockchain network. All nodes are Blockchain administrators and come into the system voluntarily without centralization called decentralized, but all the nodes that come into Blockchain are intended to obtain the newly excavated Bitcoin. Initially Bitcoin was the reason Blockchain was created, but now Blockchain has become a technology. It has the potential of being the most active. Currently, there are thousands of digital coins like Bitcoin in the market for about $1,600, while the Blockchain technology has been adapted to other industries.

Larry Summers, former US Secretary of the Treasury, said that "Bitcoin has a personality like a fax machine. One fax machine is just a useless door barrier, but in a world where everyone has a fax machine, it is considered to be a great value."

Blockchain technology is designed as a decentralized technology. Decentralized technology affects Blockchain performance. The Blockchain is a new commercial transaction monitoring, where traditional authentication may become unnecessary. Nearly all trading on the Blockchain can be done at the same stock exchange, or it may cause some types of recordings, such as land registration, to become fully public and thus decentralize. The world's computer networks utilize Blockchain technology to handle digital coin transaction databases. This means that

digital coin is managed by its own network without centralized power, the network is a person-to-person or peer-to-peer operation that does not have to depend on the central itself.

Nowadays, the financial industry seems to be the one who uses most of Blockchain technology, especially with the transfer of money across the country. Currently, Blockchain developers are in demand in the global market. Using Blockchain technology makes it possible to cut intermediary for transactions. Think of a simplified personal computer today with an innovative Graphical User Interface (GUI). The digital financial world is a wallet that stores digital coins and other Cryptocurrency to transfer or use to purchase online transactions. In the future, wallet applications may handle identity verification in many other ways.

William Mougayar, author of The Blockchain Business: Promise, Practice, and Application of the Next Internet Technology, said that "Identity in the online world is decentralized and we will own the information that really belongs to us."

Blockchain does not only play a role in financial transactions. It might be used for other tasks such as collecting election statistics for greater transparency, inter-cloud lending, co-location service, peer-to-peer lending, etc. Moreover, financial institutions such as Citibank, NASDAQ, and VISA have invested in leading Blockchains such as Chain.com to preserve this technology market as well.

Blockchain concept is back in trade again with new style of development for using in alternative ways with is outside of using as transaction which are not popular, and the increasing rate of devices to use the Internet of Things concepts need to be managed about the security between devices. In addition, the contacts have to collect transaction that affects Blockchain to focus on personal privacy, which has become a major contributor by simplifying the operating system, higher flexibility for responding to the users quickly.

However, Blockchain was successful in order to change the situation of digital financial services to find an experienced partner for working with various complex systems at every level of usage both small or large which is the heart of this issue. This business idea have not likely to happen in the last five years, but now the ideas have become a determinant of future. All of this can be done by selecting appropriate software as a key variable [3].

2.3 Introduction of smart contact

Distributed ledger or distributed database contains the contract instructions that effect when the specified conditions in the contracts invoked immediately. This is the reason, smart contracts was programmed to work when the conditions specified in the contract achieved, such as the instrument can be ordered when financial instruments meet the standards set with Blockchain technology. After that the payment transaction will create automatically.

Many people are familiar with Blockchain as a technology behind the development of digital currency, such as Bitcoin or Ethereum, which is becoming increasingly popular. If you focus on the principles of Blockchain from the basics. Firstly, distributed ledger is a type of database that acts as an electronic transaction account. The data is distributed throughout each transaction, a distributed ledger is a transaction that is a golden copy or a trustworthy document. The advantage of this type of database is a transparent transaction because everyone in the system perceives all transactions occur, so everyone in the network can make sure who does what due to Blockchain is a technology that uses a distributed ledger database.

Smart Contract is a contractual terms or conditions. The code is stored in the network Blockchain, if the statement is in accordance with the terms of the agreement. The system will process the transaction automatically. The idea of making a Smart Contract was made by a computer scientist named Nick Szabo, who initiated the idea of taking Blockchain to the smart contract. It is well known that Blockchain technology does not require any intermediaries or staff to check documents. Everything has worked with computers. Moreover, It also enhances data security by storing information in a distributed ledger which distribute data to everyone in the network. Everyone in the network has the same information and it is a witness that this promise has taken place and really achieved. We can not be corrupt the smart contract which has been described as if-this-then-that that means if this is the case then do it automatically from start to finish.

The Smart Contract has been used seriously. The US government agency, The Delaware Public Archives (DPA), has introduced a Smart Contract to destroy documents and information on the due date, Smart Contract will destroy the document or database. Being able to use the Smart Contract can help the state save more money

compared to the cost of destroying data stored in the central database or destruction of documents or data in a non-digital format. In addition, the White Paper for Smart Contract was launched by the chamber of digital commerce, which identifies Smart Contract applications in a variety of areas, including digital identity, records, securities, financial trading, derivatives trading, financial data recordings, mortgages, land title recording, supply chain management, auto insurance, Clinical trials and cancer research. Consequently, this technology is another hope to be used in a number of industries.

If you are talking about the work of a distributed ledger that mean the operation of a distributed, non-centric database system, but if you talk about distributed ledger used in Smart Contract, that means another technology to become a financial provider such as Credit Card Payment, Payment in transit, Payment of rent.

Smart contact uses Blockchain as background technology, which is distributed ledger, so many company created this technology, called distributed ledger platform, with various purposes to support as follows:

1) Bitcoin is designed to process exchanges. However, it can process the exchange of documents in the form of Smart Contract.

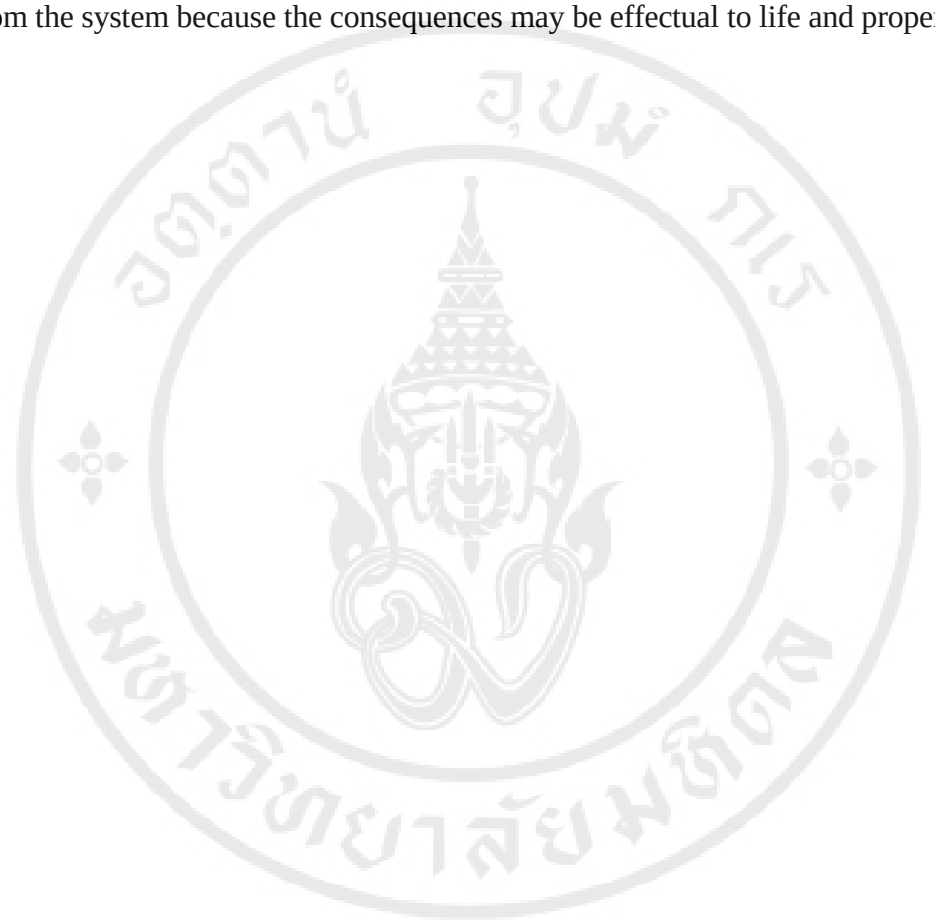
2) NXT uses Blockchain to be the smart contract that the developer has created a completed contract. The user can use without modifying.

3) Ethereum is a Blockchain designed for Smart Contract. You can write code to design your Smart Contract. Pay for the Ethereum currency for Smart Contract processing.

Smart Contract offers the innovation. It may be more than a digital currency, we do not just exchange money through the Internet. We are exchanging documents, exchange of property, etc. This exchange is transparent due to everyone in the Blockchain network can check it. However, if the code in the Smart Contract face with a problem, we can not complain the system, although a mistake led to a massive loss of life or death. This is the main trouble that the government has to focus on by managed the use of Smart Contract.

Smart Contract may not come out in the Blockchain now. Developers and people with cool ideas are refining it. This innovative innovation transforms your everyday life, we need to concern are we ready to deal with Smart Contract [5].

Smart Contract is another technology to keep an eye on, if it is developed well. We believe this technology is another strategy to change in many business areas because the contract of Smart Contract is very useful. In fact, Smart Contract will replace the paper contract by evaluation and finding solutions to errors that may occur from the system because the consequences may be effectual to life and property [6] [7].



CHAPTER III
RESEARCH METHODOLOGY

After we studied about Cryptocurrency, Blockchain and smart contact from the previous chapter. Blockchain technology is data collection, which is not required central controller called decentralized, so the data is kept inside the block on the Blockchain network. This chapter focused on Blockchain architecture, which is the main concept of every Cryptocurrency. Moreover, Cryptocurrency tool preparation is described in this part before we move to implementation and analysis results in the next chapter.

3.1 Study the Blockchain network and digital wallet platform

3.1.1 Blockchain networks

Blockchain is a network system to store online transactions. The network looks like a spider web network, which holds statistics on financial transactions and other digital assets without intermediary such as financial institutions, settlement office, etc.

3.1.1.1 Bitcoin

Bitcoin is the first digital currency that boomed up. On the other hand, Blockchain is the technology behind the currency, which control the process of transaction. Both were invented by Satoshi Nakamoto. Currently, Bitcoin development had been taken care by a non-profit organization called Bitcoin Foundation that has many stakeholders established together. Consequently, Bitcoin is a digital currency that comes first, the popularity of Bitcoin is also ranked first. It is estimated that the value of all Bitcoin in the market value is 15 billion dollars.

Currency name: Bitcoin

Currency abbreviation: BTC

Background technology: Bitcoin Blockchain

Provider: Bitcoin Foundation

Website: https://bitcoin.org

3.1.1.2 Ethereum

The popularity of Bitcoin has influenced on many organizations to create the same digital currency and one of them is the Ethereum, which has been developed by Vitalik Buterin, a young Russian who is only 23 years old. Before Vitalik established Ethereum Foundation, he has worked at the Bitcoin Foundation as a developer. He found the shortcomings and limitations of Bitcoin. For this reason was causing him to start building Ethereum in Switzerland. The ability of Ethereum is considered equal to the Bitcoin, but it has a new feature called Smart Contracts that allows us to write programs into the Ether currency data to work automatically when conditions are met. This capability allows us to create various applications to transfer data based on the network. This feature allows to manipulate the usage patterns in a vast way, unlike Bitcoin that focuses on transactions only. Currently, the market value is second only to Bitcoin that is about 1 billion dollars.

Currency Name: Ether

Currency Abbreviation: ETH

Background Technology: Ethereum Blockchain

Provider: Ethereum Foundation

Website: https://www.ethereum.org

3.1.1.3 Ripple

Ripple was founded in 2013 by another group of developers who want to create a better system than Bitcoin. The Ripple system is different from the Bitcoin and Ethereum systems that are open source, which is allowed anyone who interested in currency exchange between each other to develop software based on Ripple network. However, Ripple network is a closed system controlled by Ripple. The advantage of the closed system is easier to check the identity of the participant, which is higher security and faster processing because of wasting time checking the

accuracy of data is less than the others. Currently, the Ripple's market value is about 200 million dollars, considered as the third place after Bitcoin and Ethereum. However, over the past few years, Ripple has turned into a huge financial institution market. Who are aware of distributed ledger technology and want the same technology as Blockchain but use it in a closed network instead, which is quite good and there are many big banks around the world joining Ripple in Thailand. Indeed, the Siam Commercial Bank (SCB) participated in order to transfer the international money under the Ripple system.

Currency name: Ripple
Currency abbreviation: XRP
Background technology: Ripple Transaction Protocol (RTXP)
Provider: Ripple
Website: https://ripple.com

3.1.1.4 Hyperledger

Hyperledger is a distributed ledger technology similar to Blockchain but developed by many major IT companies. Hyperledger is caused by the needs of the global IT organizations such as IBM, Intel who see the benefits of Blockchain processing used in Bitcoin but do not want to use as financial transactions. Moreover, the companies have the same direction to develop this technology so they established the Hyperledger project instead of develop separately that reduce. The non-profit organization, Linux Foundation, is a mediator of this project. Hyperledger is different from the previous three systems that do not have their own currency because Hyperledger is just a "software" that works only. The usage must be based on the purpose of each project. For example, some banks may use the Hyperledger software to process internal data on their own servers without having to mess with external agencies.

Currency name: -
Currency abbreviation: -
Background technology: Name depend on project
Provider: Linux Foundation
Website: https://www.hyperledger.org

3.1.2 Digital wallet platforms

To keep digital assets, we need digital wallet. The digital wallet contains two components which are block address and private key [8]. The address like a bank account number, which is a long set of numeric codes, one set that is used as the address transfer. The private key or signature is an indication of digital wallet ownership, this is an account password to verify identity. We can use the digital wallet by giving your account number or address to someone who need to transfer digital assets to your account. However, the private key is the most important that do not let anyone know because it used to be your identity that is password to access your digital wallet. In addition, the difference between digital wallet and general bank account is ownership level. The bank accounts will be able to be suspended anytime. If the bank verifies that there is something wrong with your bank account. On the other hand, you are only one who own the private key, so no one can interrupt or interfere with your transaction without showing that you are the real owner. Digital wallet categorized into three types as follows:

1) Desktop and mobile wallet

Desktop and mobile wallet allow user to hold the private keys with themselves that means we have to be responsible for keeping the private key or Mnemonics, which is secret phase, by ourselves, as long as we can remember. The private keys are allowed us to access our address with any desktop wallet or mobile wallet application from anywhere or simultaneously. Moreover, we can restore our address which is used as a link to our address in Blockchain when we lost laptop or mobile phone. The examples of desktop wallet and mobile wallet are shown below.

- Desktop wallet such as Bitcoin Core, Electrum, Exodus, etc.
- Mobile wallet such as Mycelium, Blockchain, Jaxx, Bread, etc.

2) Hardware wallet

Hardware wallet has features as same as the previous wallet type. Hardware wallet has added another level of security which is an air-gap that means our private key are not being stored on devices connected to the Internet, so it is more difficult to hack a private key. If we want to retrieve balance of Cryptocurrency, we

have to provide the wallet's address to watch-only address application. In another case, if we want to transfer money, we must connect to the hardware wallet. Hardware wallet is same as the desktop wallet and mobile wallet, so we can back up the wallet with Mnemonics, it contains 12-24 words, then we can restore the wallet, if it lost. The examples of hardware wallet are Trezor, Ledger, etc.

3) Paper wallet

We can use websites like BitAddress.org, Bitcoinpaperwallet.com to create the address and the private key. After that, we write down the private key on the paper and keep it well. If we need to deposit the digital asset by using the received address. If we need to withdraw the digital asset, we import the private key, that we write down to the paper, into the desktop wallet or mobile wallet. Then we will delete it on the application for safety.

After we know more about the three types of digital wallet, this research shows the top rank of digital wallet that appropriate to the starter who need to use the Cryptocurrency.

3.1.2.1 MetaMask

MetaMask is not only launched on desktop wallet, but also launched on mobile as mobile wallet. It was launched in 2016 to be an ERC-20 as a digital wallet to keep Cryptocurrencies and also a Decentralized Application or DApp [9]. It has an attractive and simple interface. MetaMask allows users to use the full functionality that means the users have to take responsibility for their own private keys and if storing them on the cloud or public platforms, it may not be safe.

3.1.2.2 Myetherwallet

Myetherwallet is an open source interface program to create a digital wallet based on Ethereum Blockchain [10], which uses a simple authentication system to log in to the wallet. Normally, if we are an online member, we can log on the website anywhere by providing the password to access the Dashboard, but we don't have to enter a password to access the Myetherwallet because it requires private key or file stone to log in into the wallet instead. This method is safe and easy to use, so it

became a digital wallet that was chosen to be used for making an initial coin offering or ICO and many startup companies funds through ICO coins, they always choose Myetherwallet.

3.1.2.3 Exodus

Exodus is launched in 2017 with the concept of trust and reliability. It is established to be local digital wallet as a software platform. It can be installed on laptop and supports Windows, MAC, and Linux as operating system. Moreover, it allows us to keep many types of Cryptocurrency in one account [11]. Currently, Exodus also provides the wallet on a mobile platform. Exodus always concerns about program size, so it is the one that provides a small handful of assets and quickly add more in future releases. Exodus allows us to convert our coins within the wallet. However, we will have to pay a commission for the conversion.

3.1.2.4 Coinbase

The announcement of the CME Group discusses about the launch of the futures trading board for Bitcoin has caused its price to rise sharply at that moment. Coinbase is one of the largest Cryptocurrency trading sites in the world. the number of new applicants increasing to 100,000 in the 24 hours after the announcement. Coinbase is a Cryptocurrency exchange service provider with approximately 11.9 million users in 32 countries around the world. Coinbase also offers a convenient feature for online merchants to receive Cryptocurrency as a simple payment method. Coinbase is considered as the first success startup company in the US market that had previously raised 100 million dollars in August 2017 and worth over 1.6 billion dollars. In addition, the CEO, Brian Armstrong, is top rank on the Fortune magazine as well [12].

3.2 Analyzing Blockchain architecture

3.2.1 Blockchain architecture

Blockchain is common technology that any organization can establish to use as data transferring with decentralize concept in order to understand how its working, we need to learn more about abstraction layers of Blockchain. Blockchain architecture device into six layers as figure 3.1.

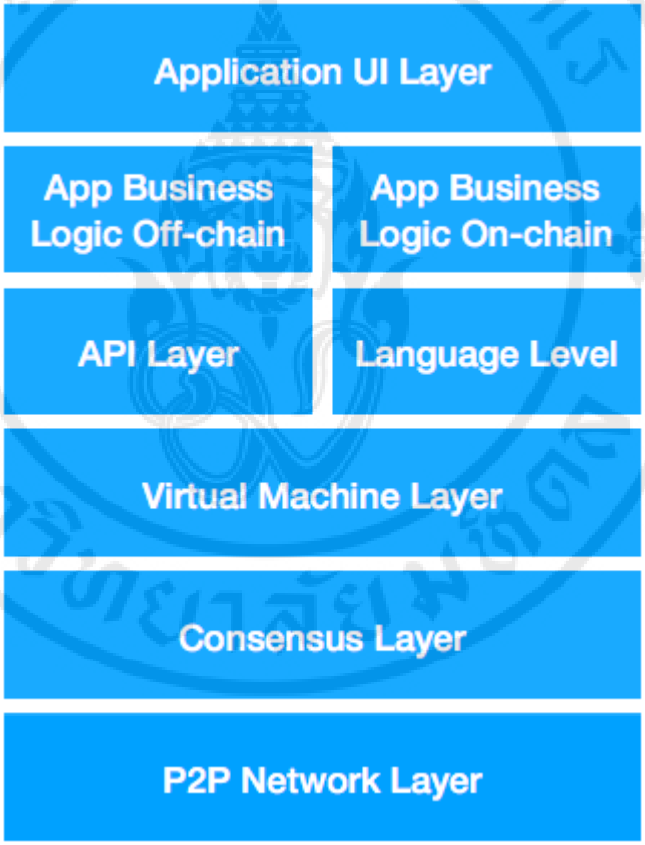


Figure 3.1 Blockchain architecture abstraction layers

3.2.1.1 Peer-to-peer network layer

Peer-to-peer or P2P network layer is the first layer which is responsible as central controller, which discovery and transfer data from client to client directly because Blockchain is distributed ledger platform so their clients can transfer

data without central control. This layer also keeps program instruction as functionality. For example, Ethereum uses the DEVP2P library as P2P network layer [13].

3.2.1.2 Consensus Layer

Consensus means trusting when the block sends or receive transaction, each block has to authorize that transaction. Consensus layer is especially part of the architecture. Each block on the Blockchain include this layer individually in order to responsible for generating the new block and validate the transaction from another block. There are various consensus protocols, but we focus on two types. First, Proof of Work or POW, which uses hash algorithm to control consensus in the Blockchain. This concept comes from denial of service or DDoS attraction, the attacker sends many fake transactions to destroy a computer resource. In fact, this concept established by Cynthia Dwork and Moni Naor back in 1993 after that Bitcoin has been applied the concept by Nakamoto. However, hash algorithm requires high performance computers to calculate, also called mining. The objective is to be the first miner who can solve algorithm then new block will generate as a reward. The background PoW steps after the new transaction generated as shown below.

1) The transactions are packed together as the block.

2) Miners validate transactions within each block by solving proof of work algorithm with brute force.

3) Who is the first solving problem will get a reward from the provider.

4) The authorized transaction will store in Blockchain and inform to the network.

To solve the algorithm, protocol commits nonce as a threshold for decreasing the data level in each block. That mean nonce is the difficulty level, which is influenced to the number of miner, difficult level is high if number of miner is high. The difficulty level is calculated by concerned about how long that block will be destroyed or generated. For this reason, the cost to generate new block is increasing so the miners always upgrade their computer to be higher performance [14].

On the other hand, Proof of Stack or PoS was established with the same purpose to get the new block, but it is different algorithm. The PoS will decide miner who is the most wealth without reward that means the number of block

always same as the first time that block created. The wealthiest miner will stake and receive transaction fees as benefits. The example of this consensus type is Peercoin, the first digital currency that used PoS as a consensus concept in 2012. However, Ethereum is one foundation that has direction to establish a new protocol called Casper, which is replaced PoW with PoS [15].

Another concept is Proof of Authority or PoA, which is used to authorize a person who can create the new block. PoA was established to overcome with PoW and PoS problems. The method combined the good part of PoW and PoS, so the PoA is appropriated for private Blockchain due to Blockchain is controlled by the creator. As a result, PoA is the fast method because the new block knows the destination exactly. In fact, PoA was applied to private Blockchain for business to business or B2B [16] such as Tomochain, etc.

3.2.1.3 Virtual machine layer

Some provider protocol combines a consensus layer and virtual machine layer to be consensus layer due to some responsibility are overlapping. The purpose of virtual machine layer is basic validation in terms of common information validation in each block e.g. amount transfer, owner signature, block's nonce, transaction fee calculation, and transfer digital asset by updating amount at destination address [17]. This layer device into two types, which categorized based on the way to write programs to solve any reasonable computational problem.

Turing complete, it has allowed the program to perform looping and branching statements as well as local state storage. This functionality is important to have in order to implement most non-trivial computer programs. The example of Blockchain is Ethereum, which is used Solidity as Turing complete. The Turing completeness is important for Ethereum smart contracts because you have the ability to implement sophisticated logic [18]. On the other hand, Turing incomplete is absolutely different from the previous one. It is developed by removing the looping feature to avoid any spam or network overload. The example of Turing incomplete Blockchain is Bitcoin. For this reason, Ethereum try to overcome the problem of infinite looping using a concept called Gas to be a threshold for stopping the loop.

3.2.1.4 API layer and VM programing language

3.2.1.4.1 API layer

Application Programming Interface or API is the fourth layer, which represented as interface of each block in the Blockchain that allow the server to receive the request and send the response. The miners can access protocol network easier via API [19]. For example, Web3.js communicate Ethereum network with JSON Remote Procedure Call or JSON RPC [20] as figure 3.2.

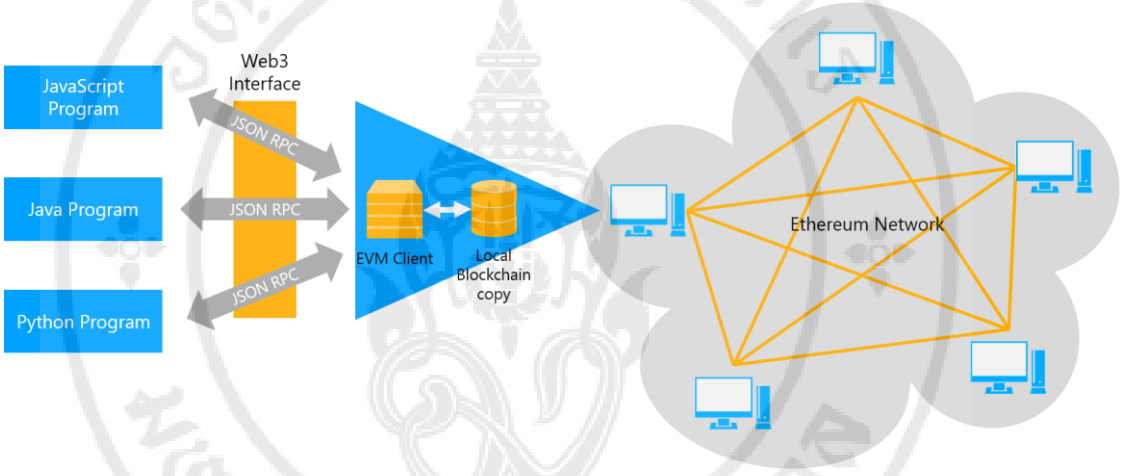


Figure 3.2 Client communicate to Ethereum diagram

3.2.1.4.2 VM programing language

Blockchain become huge technology that affects computer language providers to improve their language for allowing Blockchain development. In addition, Blockchain contains many blocks so the object oriented programming language is properly such as Java, C#, Javascript, SQL, C++, Golang, etc. However, we focus on Ethereum so we should focus on languages that provide for Ethereum Blockchain development as shown below [21].

1) Solidity

According to Solidity website said that “Solidity is an object-oriented, high-level language for implementing smart contracts which are programs which govern the behaviour of accounts within the Ethereum state. Solidity was influenced by C++, Python and JavaScript and is designed to target the Ethereum

Virtual Machine (EVM). It is statically typed, supports inheritance, libraries and complex user-defined types among other features. Thus, Solidity allows you can create contracts for uses such as voting, Crowdfunding, blind auctions, and multi-signature wallets.” [22].

2) Golang

Refer to definition of Golang in its website said that “The Go programming language is an open source project to make programmers more productive. Go is expressive, concise, clean, and efficient. Its concurrency mechanisms make it easy to write programs that get the most out of multicore and networked machines, while its novel type system enables flexible and modular program construction. Go compiles quickly to machine code yet has the convenience of garbage collection and the power of run-time reflection. It's a fast, statically typed, compiled language that feels like a dynamically typed, interpreted language.” [23].

3.2.1.5 Application business logic layer

The application business logic layer is developed by the third parties, which depend on the project objective to control how transaction in the Blockchain working. This layer includes two types. First, on chain transactions, which reflect the main Blockchain ledger, so every block allow to visible each other. To develop this type, we need to use fourth level language, which is part of layer two or consensus layer, and it is executed by layer 3, VM layer. In contrast, off-chain transactions, which allow only trusted parties to receive agreements. This type will be used when the Blockchain require to interact with other Blockchain which separate into three types as follow: Oracles, DApps, and specific domain off chain system with lite protocol and scalability solutions. Indeed, off-chain transactions become popular due to cheaper, faster, and more privacy [24]. Example methods of off-chain transactions are Credit-based solutions, Trusted third parties, and etc.

3.2.1.6 Application UI layer

The application UI layer is interface of DApp as digital wallet that allow users to interact with the system easily. This layer usually develops by web programming, e.g. HTML5, CSS, and etc.

3.2.2 Inside the block

Blockchain can categorize into three types. First, private Blockchain established to use for a specific organization. Of course, only nodes from that organization can visibly and join the consensus. Second, consortium Blockchain allows only selected node to be visible and join the consensus due to this type of Blockchain usually established for many organizations. The last one is public Blockchain, which is allowed every node to visible and join the consensus. For Immutability for public Blockchain is impossible because of the number of participants. For this reason, the public Blockchain also take more propagated time, which is different absolutely from private and consortium Blockchain. The table 3.1 shows summary of three different types.

Table 3.1 Summary of Blockchain types

Property	Public Blockchain	Consortium Blockchain	Private Blockchain
Determination	All nodes	Selected nodes	One organization
Read permission	Public	Public or restricted	Public or restricted
Immutability	Nearly impossible	Tampered	Tampered
Efficiency	Low	High	High
Centralized	No	Partial	Yes

Basically, Blockchain is combined of blocks and chain (figure 3.3). The block consists of header and body. For block header, it contains a hash of the previous block, which connects the blocks together as a chain. Each block has only one parent block except the first block called genesis block [25]. Additional, the block header also includes significant components as shown below.

- Block version: A set of block validated condition
- Merkle tree root hash: All hash values of transactions in the block
- Timestamp: The time when the block is created with unit of second
- nBits: Threshold for block hash validation

- Nonce: Normally, it is set at zero, then it will be increased when hash calculation happens. (4 Bytes)
- Parent block hash: Hash value of parent block or previous block (256 Bits)

The block body contains transaction counter. The block size and transaction size are affected the maximum number of transactions in the block. To authenticate the block which uses an asymmetric cryptography algorithm as a digital signature.

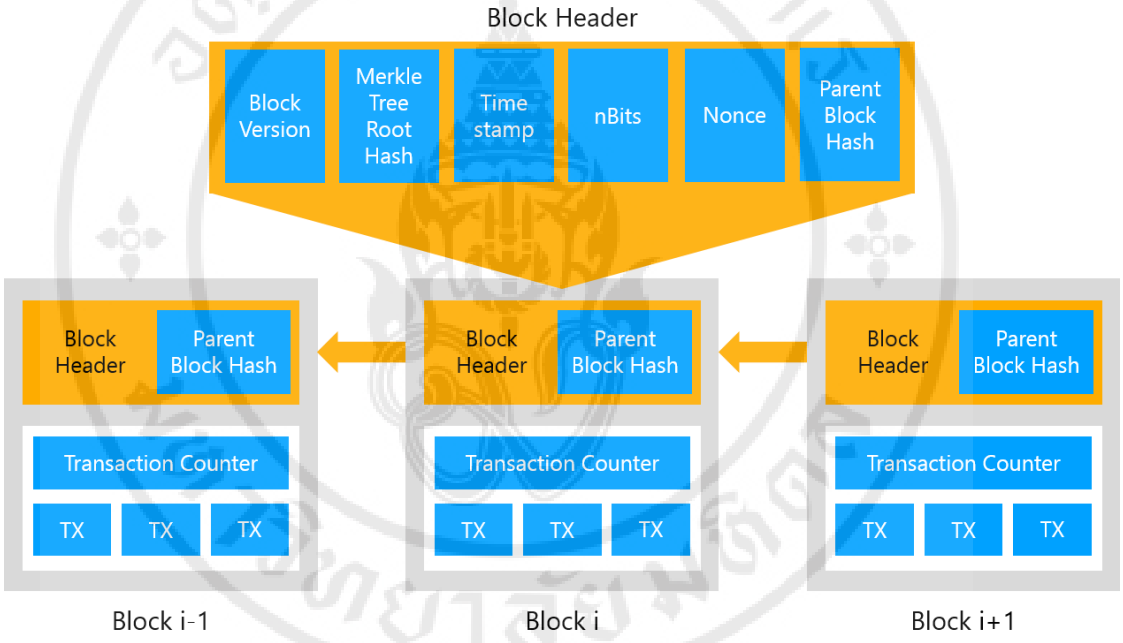


Figure 3.3 Sequence of block as Blockchain

3.2.3 DApp front-end workflow

DApp or Decentralize application is concept of application development, which is using Blockchain or smart contact as data structure. The application transfers data without central control. The data is stored in the client's space. However, the data is kept with high security with encryption algorithm on the Blockchain that preserves digital assets and the block will not be destroyed. The DApp instructions from frontend to backend are shown in figure 3.4.

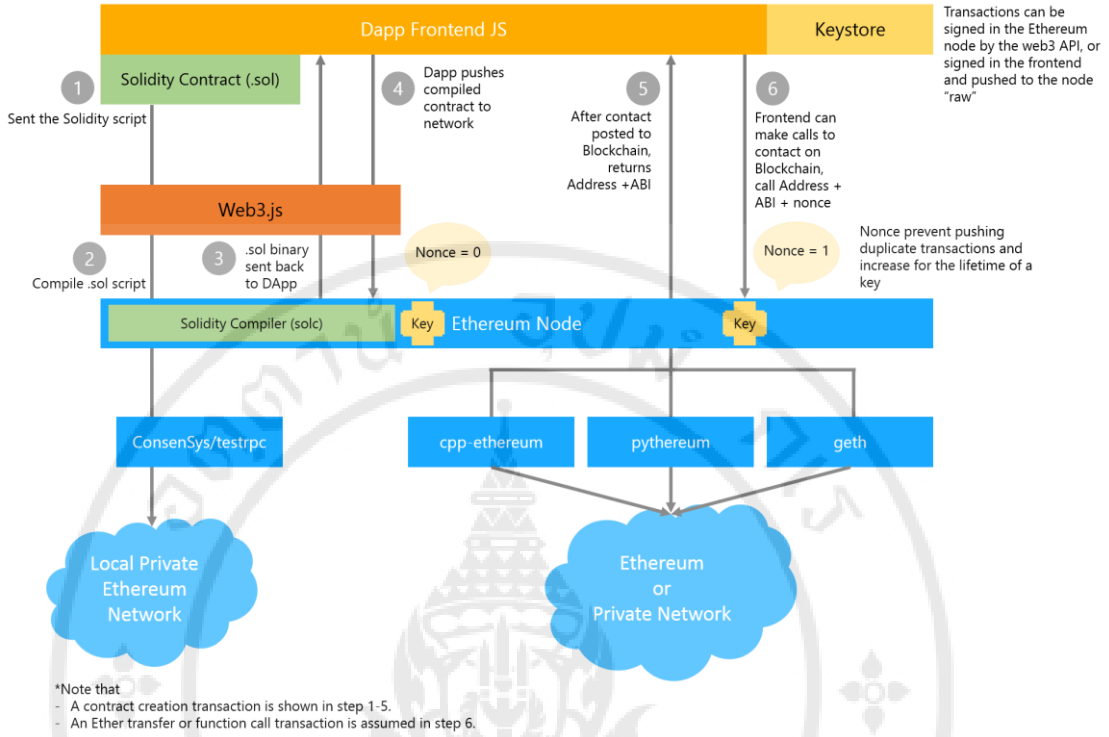


Figure 3.4 DApp instructions from front-end to backend

In this part, we share about using MetaMask, which is the digital wallet with the Ethereum network as DApp architecture. Before going to implement step, we have to prepare our devices.

3.3 Prepare develop tools for the case study

3.3.1 Browser installation

MetaMask allow us to install on many browsers, which are Chrome, Firefox, Opera, and Brave. Chrome, web browser provided by Google, is the familiar one that we always use, so we will install Chrome as the next step. However, we must check that our devices meet the minimum system requirement as show below [26].

Installation Chrome Browser on Windows requires OS:

- Windows 7
- Windows 8
- Windows 8.1
- Windows 10 or later
- With an Intel Pentium 4 processor or later that's SSE2 capable.

Installation Chrome Browser on Windows servers requires OS:

- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016

Installation Chrome Browser on Mac requires OS:

- OS X Yosemite 10.10 or later

Installation Chrome Browser on Linux requires OS:

- 64-bit Ubuntu 14.04+
- Debian 8+
- openSUSE 13.3+
- Fedora Linux 24+
- With an Intel Pentium 4 processor or later that's SSE2 capable

If our devices match to the requirement, we can download Chrome by access https://www.google.com/chrome/ then click ‘Download Chrome’ as figure 3.5. We should active the installer after finishing download then follow its steps to complete the installation.

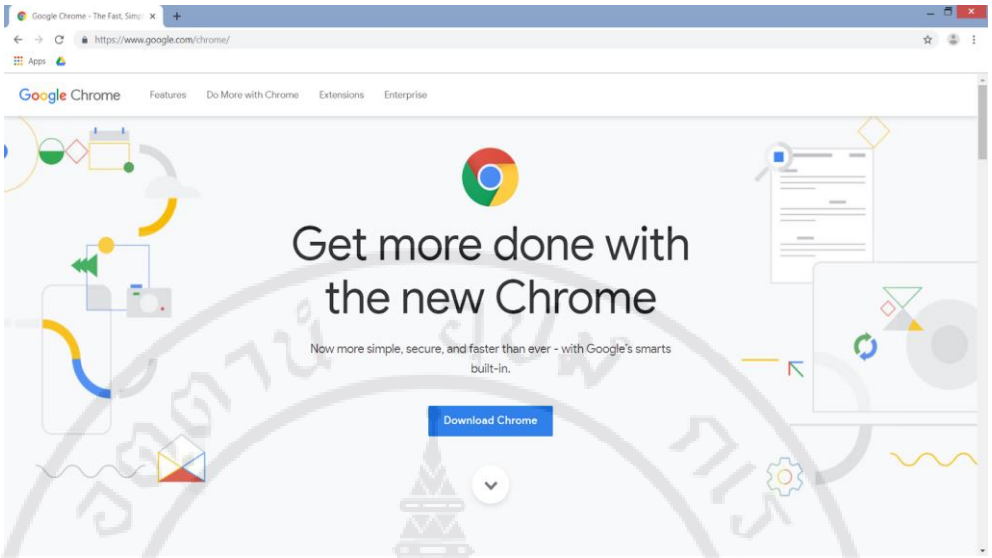


Figure 3.5 Chrome download page

3.3.2 MetaMask Installation

After Chrome installed to the device, we have to install MetaMsk is developed with the objective of being the easiest way for everyone to interact with Ethereum. Moreover, MetaMask avoid running full Ethereum node, so it helps us to execute Ethereum DApp and save our resources. Refer to an article about the differences between full node and Light node in medium.com [27] said that "A full node has a copy of the entire state of the Ethereum Blockchain and executes every transaction that gets mined that requires upwards of 120GB of storage and 8GB+ of memory. It can take several hours for a full node to join the network and become fully synchronized."

We have to access https://chrome.google.com/webstore/detail/metamask/nkbihfbeogaeaoehlefnkodbefgpgknn, which is Chrome Web Store. However, we can go to https://metamask.io/ that provided links to the other browser extension. Figure 3.6 is shown the extension page, then click on 'Add to Chrome' button, it will ask you to accept the extension via a prompt box as figure 3.7.

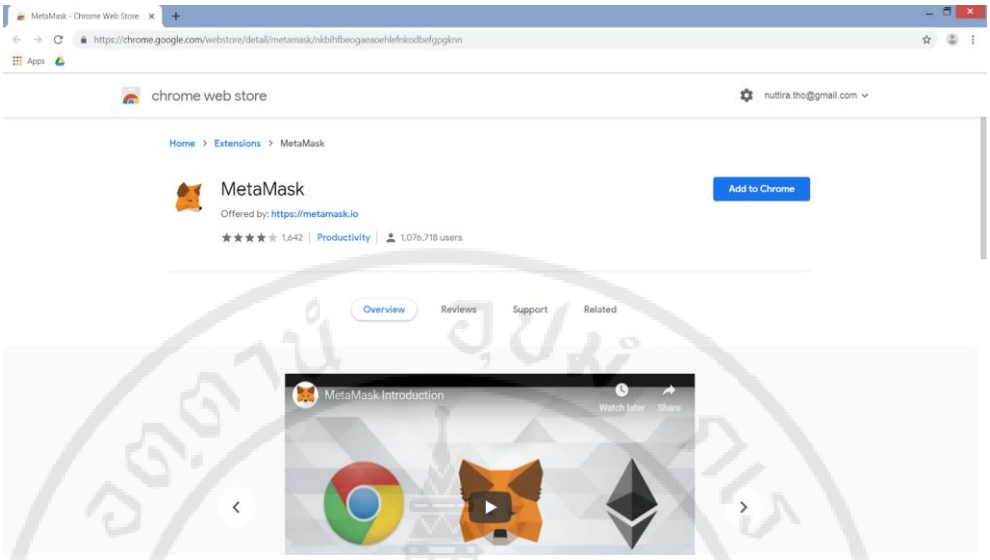


Figure 3.6 MetaMask extension on Chrome Web Store

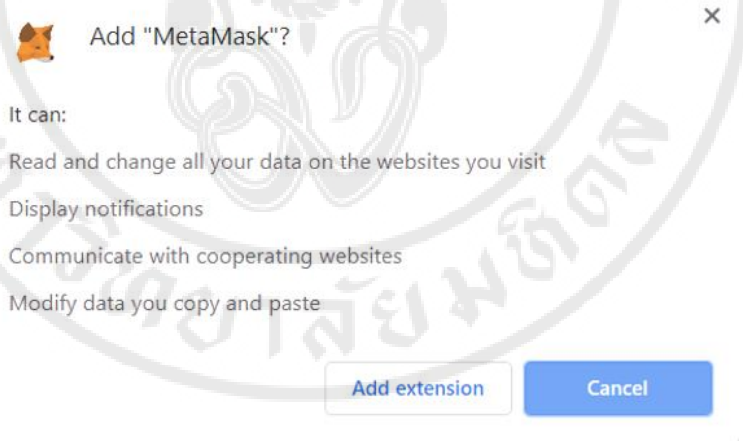


Figure 3.7 MetaMask extension prompt

After accepting the extension by click on ‘Add extension’ button, it will download the extension and bring to MetaMask page automatically. The MetaMask icon will appear on the browser's menu bar at the top-right window as figure 3.8.

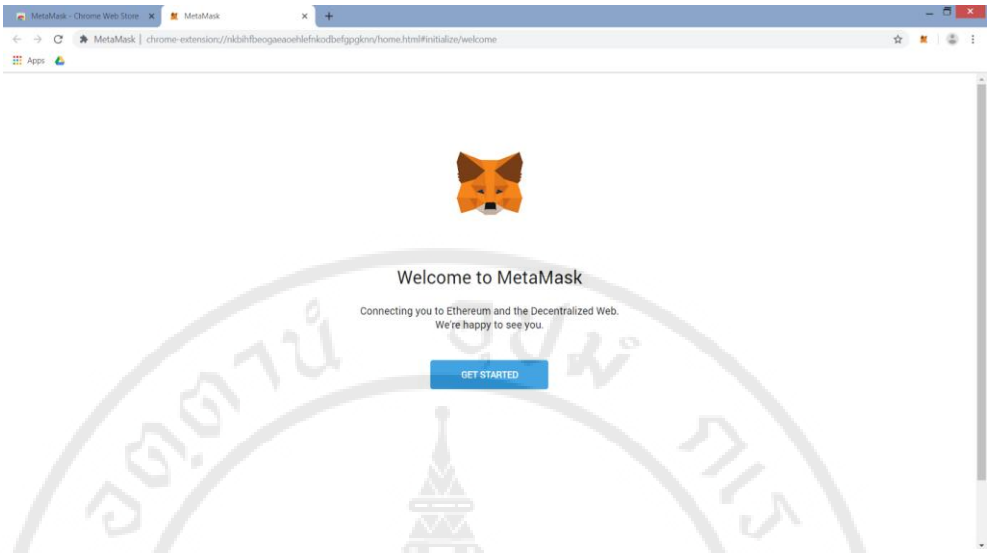


Figure 3.8 MetaMask page after finished extension installation

After that click on 'Get Started' button, it will bring you to setting our wallet as figure 3.9. If you already have a seed phase, which is a secret phrase as a password, to import the backup of your wallet then click on 'Import Wallet' button. On the other hand, click on 'Create a Wallet' button if you are new joiner or you need to create the new one. Moreover, both alternatives will bring you to MetaMask improvement acceptation form, this part is up to you to allow the provider to get your activities when using the app.

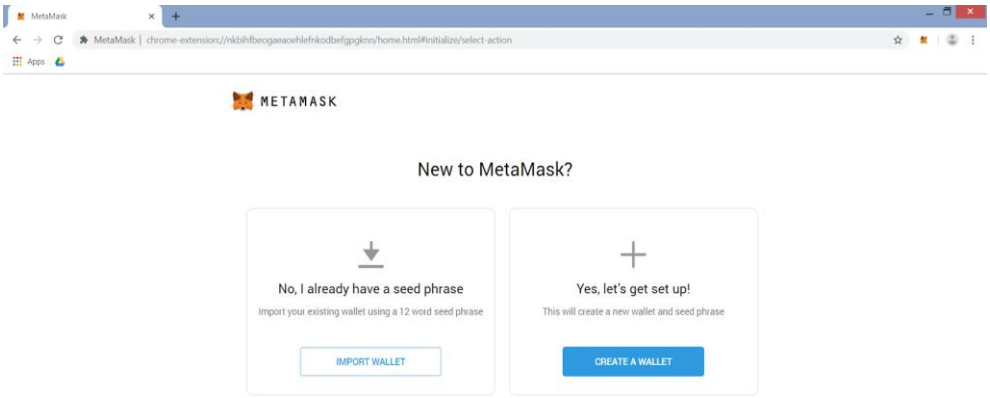


Figure 3.9 MetaMask alternative account setting page

After finishing the form, it will ask you for a seed phase and a new password (figure 3.10) then type the phrase and check box for accepting Term of Use if you choose to get wallet backup. Then again, it will ask you for the new password and send your seed phase. Remember that you have to keep the seed phrase as secret, you have to click on 'Click Here to Reveal Secret Words' (figure 3.11) then remember it as the password and check the box for accepting the terms of use after that 'Next' button will active, click on it that will bring you to confirm the seed phase by ordering the words which is the last step of MetaMask account creation. As a result, we got the digital wallet with zero ETH as shown figure 3.12.

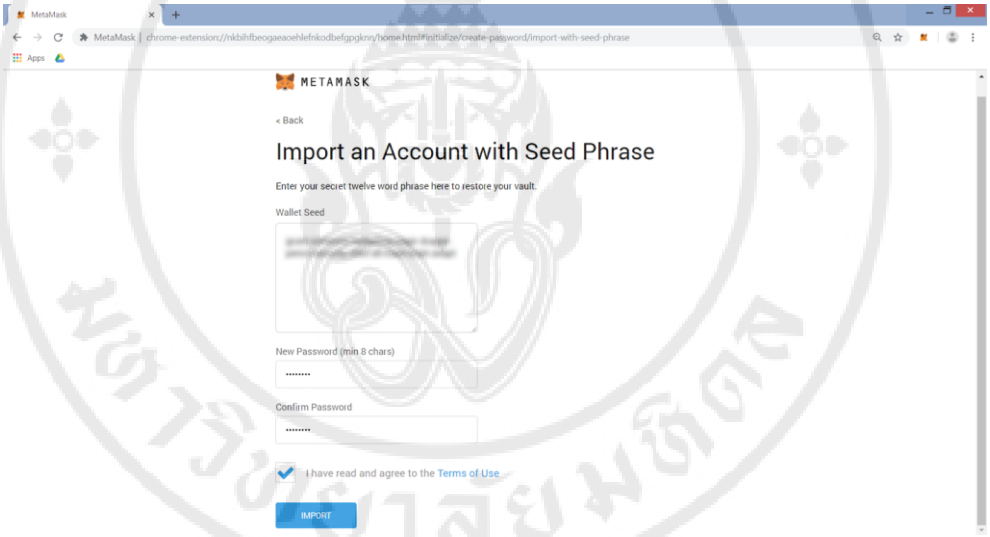


Figure 3.10 Import MetaMask wallet account page

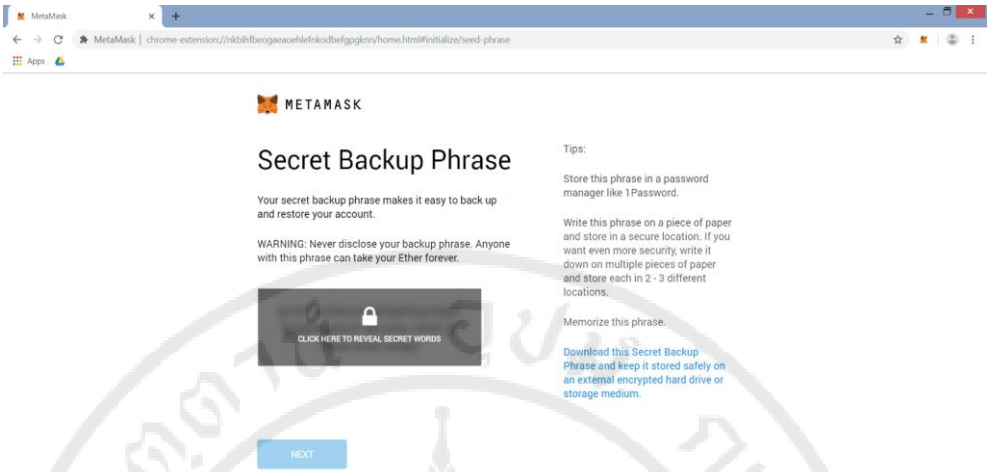


Figure 3.11 Create new MetaMask wallet account page

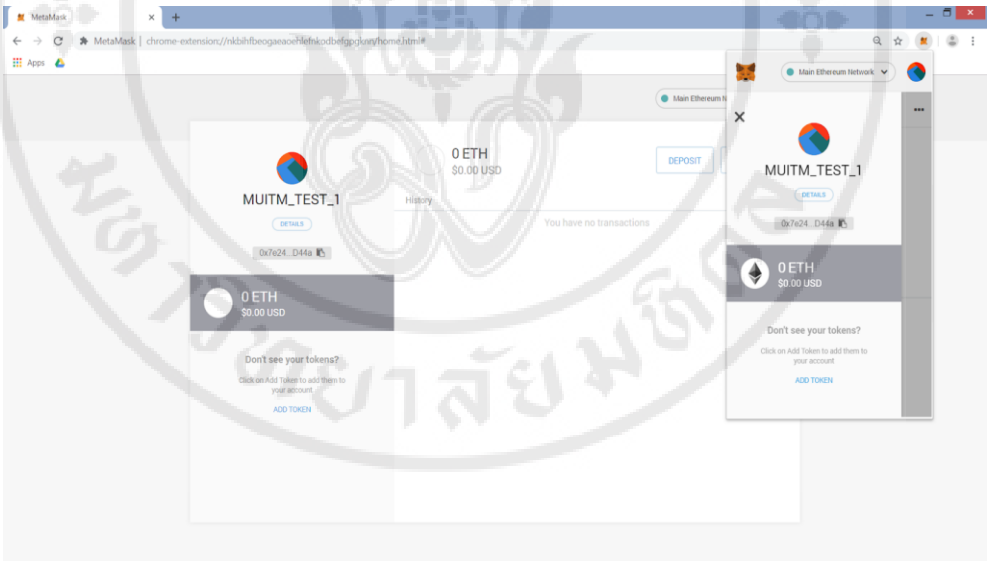


Figure 3.12 MetaMask wallet

3.3.3 GitHub Registration

Normally, we must test the system by using digital asset, so we should get the free coin. To top up the coins to digital wallet, we must access the faucet website for activating the free coin. It requires us to login with GitHub account. If you have not been joined GitHub, you can register at https://github.com/join.

CHAPTER IV
RESULTS AND DISCUSSION

After we finished studying Blockchain technology and prepare tool for Cryptocurrency development, which is the case study of this research. Moreover, this chapter is also focused on comparison in terms of Blockchain technology and digital wallet application based on Blockchain.

4.1 Resources preparing for case study

4.1.1 Implement digital currency

Before starting this topic, you have to complete the requirement in the previous topic, which is Chrome installation with MetaMask extension, digital wallet creation, and register GitHub account [28] [29]. Next, we focus on our case study on digital currency creation that you can follow the steps below.

4.1.2 MetaMask network selection

MetaMask is established to support the Ethereum networks not only the real one, but also include the test networks (figure 4.1) [30]. It provides several network as follows:

4.1.2.1 Ethereum Main Network

Ethereum Main Network or Ethereum Mainnet is the real network, each node in this network contains the real Ether value which is valuable for miner to make an income. The Mainnet is launched in 2015 [31]. The concept is based on Bitcoin Blockchain with some improvement in order to use Blockchain as data structure in other applications with Proof of Work (PoW) as consensus algorithm.

4.1.2.2 Ethereum Testing Network Ropsten

Ethereum Testing Network Ropsten or Ethereum Testnet Ropsten is the first testing network with Proof of Work (PoW) as consensus algorithm. It is established in November, 2016. The Ropsten was attacked by Denial of Service in February 2017. Consequently, the network decreased the rate of synching and it affected the clients to consume a lot of disk space. After that it was become usable again in March 2017. Indeed, Ropsten is most efficient Ethereum testing network due to it is recreated based on the real network, so their system and conditions are same. However, it has no immunity to cybercrime as a result of the situation in February 2017.

1) Ethereum Testing Network Kovan

Ethereum Testing Network Kovan or Ethereum Testnet Kovan is the second testing network with Proof of Authority (PoA) as consensus algorithm. This Testnet was started in March 2017 for supporting the client while maintained the Ropsten after faced with cybercrime. Moreover, Koven is popular Ethereum Testnet after Robsten was broken and it is immune to cybercrime. It is supported only parity command that means it cannot be mined. The miners have to access Faucet to get the coin.

2) Ethereum Testing Network Rinkeby

Ethereum Testing Network Rinkeby or Ethereum Testnet Rinkeby is the last testing network in this research coming with Proof of Authority (PoA) as same as Ethereum Testing Network Kovan, so it’s immune to Cybercrime and it cannot be mined. However, Ethereum provided Kovan to support parity command. On the other hand, Ethereum provide Rinkeby to support geth command.

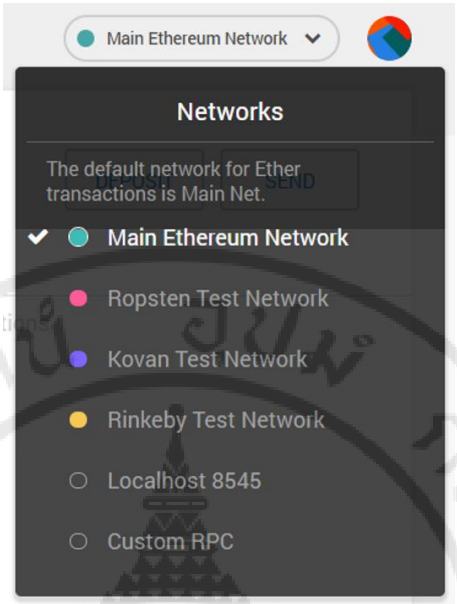


Figure 4.1 Ethereum network lists are supported by MetaMask

Table 4.1 Ethereum network comparison

Property	Main network	Ropsten	Kovan	Rinkeby
Network ID	1	3	42	4
Consensus algorithm	PoW	PoW	PoA	PoA
Block time	13.5 sec.	30 sec.	4 sec.	15 sec.
Chain data size (April 2018)	133 GB	15 GB	13 GB	6 GB
Command	geth or parity	geth --testnet or geth --networkid 3 parity --chain ropsten	parity --chain kovan	geth --rinkeby or geth --networkid 4

Table 4.1 shows the Ethereum network comparison. Indeed, the case study, digital currency creation based on Ethereum network is focused on Ethereum testing network Kovan due to it is testing network that we can use as a sandbox.

4.1.3 Adding ETH to digital wallet with Faucet

Adding ETH to the digital wallet, we need to access the Faucet website for getting the free coin. Many advertisements shown on the website. As you have seen before many websites can earn money via user access them. Therefore, Faucet is another one that earns income when miners or clients landing their websites [32]. The lists below are Faucet websites that support different types of Ethereum environments.

1) Ethereum Mainnet: https://ethereum-faucet.org/
2) Ethereum Testnet Ropsten: https://faucet.ropsten.be/
3) Ethereum Testnet Kovan: https://faucet.kovan.network/
4) Ethereum Testnet Rinkeby: https://faucet.rinkeby.io/

Faucet not only supports Ethereum, but also supports other Cryptocurrencies [33] such as Bitcoin, etc. In this part, we focus on the Ethereum Testnet Kovan so we have to access the Kovan's Faucet website then it requires a Github account. After clicking on 'Login with Github' button, it will bring us to landing Github's sign-in page if we have not signed-in yet. Faucet page requests the digital wallet address. The address comes from wallet on MetaMask by copying the wallet's address in the account details of the MetaMask extension (figure 4.2). Figure 4.3 shows the result after we input the address after that the coin will be increased to be one ETH. Please remind that Faucet allows requesting ETH only one time for every 24 hours.

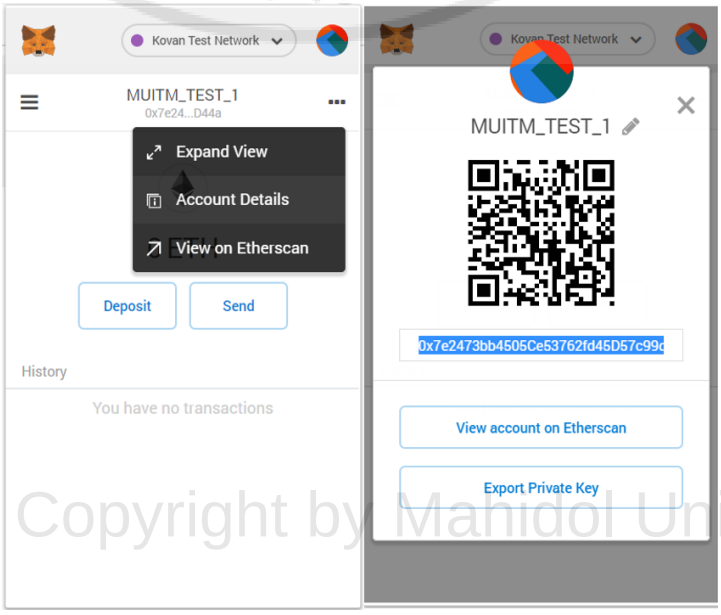


Figure 4.2 Account details on MetaMask extension

Figure 4.3 Ethereum Testnet Kovan's Faucet with digital wallet's address

4.2 Cryptocurrency implementation

4.2.1 Develop digital currency with Solidity by using Remix as IDE

After we finished that previous step. Next, we can start coding as developed step. We have to access http://remix.ethereum.org and create a new Solidity script, which is shown in the appendix.

4.2.2 Solidity deployment as Blockchain to the network

To deploy the code, we should select 'version:0.5.1+commit.c8a2cb62' with auto compile, the version of compiling that depend on your choice. The IDE compiles the code automatically after the code has changed (figure 4.4).

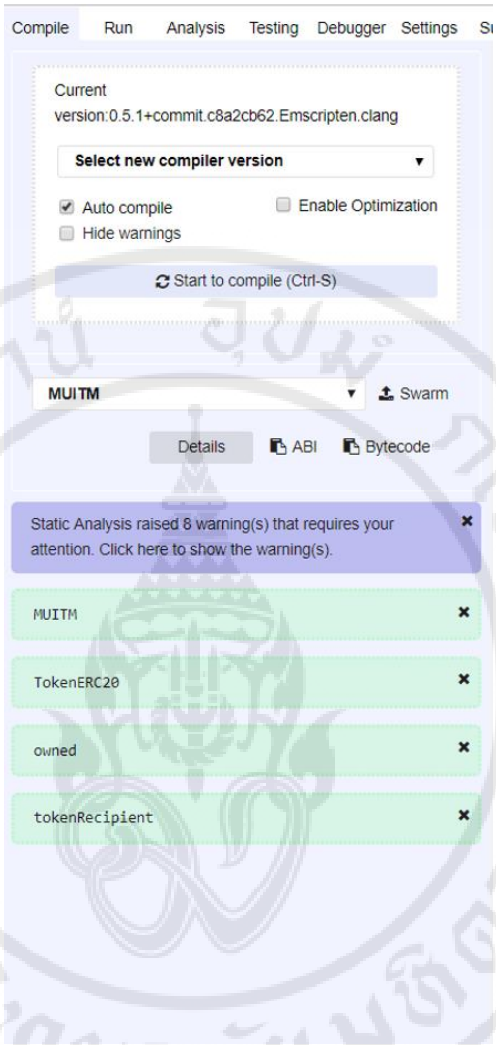


Figure 4.4 Solidity compiler setting

4.2.3 Create the new Cryptocurrency

After compiling the solidity code in the previous step, then we focus on creating the new digital currency, we have to config the system in 'Run' tab as shown in figure 4.5. The configuration consists of four components as follows as:

1) Environment: The environment is used to create the new currency.

2) Account: Digital wallet account that used to pay Gas as fee for transferring the digital asset.

3) Gas limit: The limitation of total fee that uses to spend for this transfer.

4) Value: Amount of gas is used to create the transaction in each round.

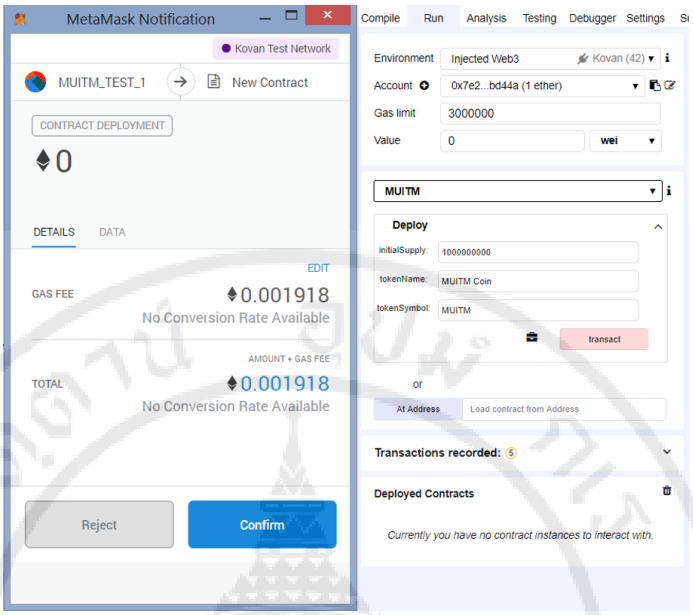


Figure 4.5 Solidity configuration

We have to custom another configuration follows the new Cryptocurrency requirement. The components of configuration are shown below.

1) initialSupply: Amount of digital asset is used in this transaction with uint256 as a unit.

2) tokenName: The name of new Cryptocurrency.

3) tokenSymbol: The abbreviation of new Cryptocurrency.

When finished filling the both of configuration, then click ‘transaction’ button (figure 4.5). MetaMask window appears to confirm the gas payment. Consequently, the new Cryptocurrency is created in the environment that specify in the configuration. The address is shown in the console below as figure 4.6.

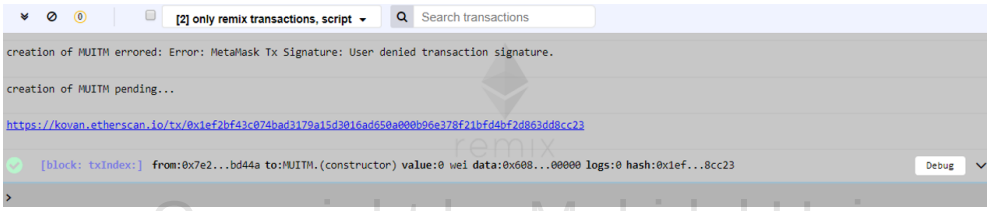


Figure 4.6 Console is shown the results after running to create the new Cryptocurrency

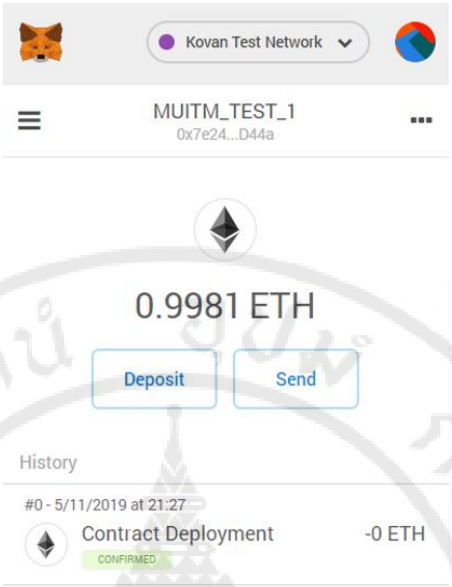


Figure 4.7 MetaMask wallet show amount of ether

The console is shown Etherscan link, which shows the new block details. Moreover, the MetaMask wallet show amount of ether that is decreased because of transaction fee (figure 4.7). Moreover, we can add the new currency to the MetaMask wallet by adding a new token that is described in the next step.

4.2.4 Adding the new Cryptocurrency to the digital wallet

To add the new currency that is created in the previous step to the wallet by going to the wallet, then click on the MetaMask menu and click ‘Add Token’ button and select ‘Custom Token’ tab as figure 4.8. Copy the address of new Cryptocurrency that is shown at the console. After that paste the address, token details are shown automatically, then the wallet contains two Cryptocurrencies as figure 4.9.

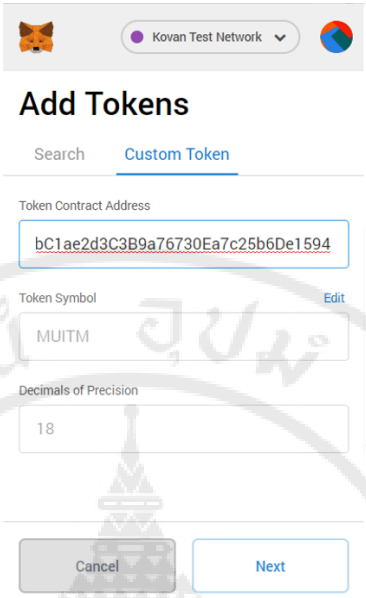


Figure 4.8 Adding token page on MetaMask with the new Cryptocurrency details

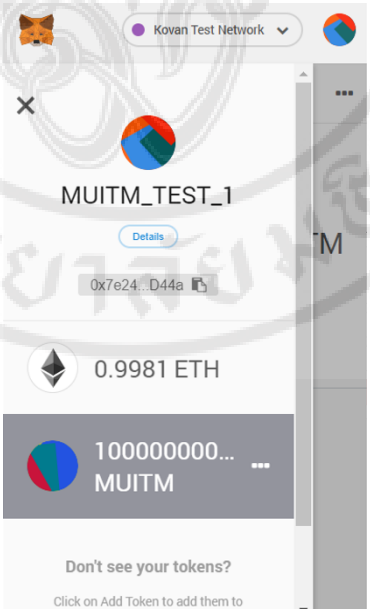


Figure 4.9 MetaMask wallet with two Cryptocurrencies

4.3 Blockchain analysis

This session is focused on two types of comparisons in terms of Blockchain technology and digital wallet.

4.3.1 Blockchain comparison

Table 4.2 shows the Blockchain comparison.

Table 4.2 Blockchain network comparison

Property	Bitcoin	Litecoin	Ethereum
Blockchain objective	Cryptocurrency	Cryptocurrency	Run smart contracts
Stored data type	Cryptocurrency transactions, plus some additional data in coinbase or OP_RETURN transactions	Cryptocurrency transactions, plus some additional data in coinbase or OP_RETURN transactions	Cryptocurrency, digital assets, smart contracts
Developed language	Script	Script	Solidity, Serpent, LLL
Participation	Download the source code from GitHub, and follow their instructions. Obtain currency from online trading service.	Download the source code from GitHub, and follow their instructions. Obtain currency from online trading service.	Download the source code from GitHub, and follow their instructions. Obtain currency from online trading service.
Currency	bitcoin (BTC)	litecoin (LTC)	ether (ETH or ETC)
Block release time	10 min	2.5 min	13.5 min
Transaction size	min.: 200 bytes, avg.: 250 bytes	N/A	no max (actual max: 89 kB)

Table 4.2 Blockchain network comparison (cont.)

Property	Bitcoin	Litecoin	Ethereum
Transaction rate	avg.: 3 trans./sec., theoretical max.: 7 trans./sec.	theoretical max.: 28 trans./sec.	no maximum
Consensus type	Nodes verify blocks and transactions, and select Blockchain with the most blocks.	Nodes verify blocks and transactions, and select Blockchain with the most blocks.	Nodes verify blocks and transactions, and select Blockchain with the most blocks on Virtual Machine
Mining algorithm	PoW	PoW	PoW using Ethash algorithm

Property	Hyperledger Fabric	Hyperledger Sawtooth	Hyperledger Iroha
Blockchain objective	Enable the creation of Blockchains for industry use cases.	Enable companies to deploy their own Blockchains.	Provide tools that integrate easily into existing environments.
Stored data type	Chaincode (i.e. smart contracts)	Anything that can be defined by a “transaction family”.	(unknown)
Developed language	Go (golang), Java (in progress)	Python	(unknown)
Participation	Create a Blockchain: Download source and follow instructions.	Download the source code from GitHub and follow their instructions.	(unknown)

Table 4.2 Blockchain network comparison (cont.)

Property	Hyperledger Fabric	Hyperledger Sawtooth	Hyperledger Iroha
	Join existing network: Register with a proof of identity to the network membership services.		
Currency	N/A	Initially provides the MarketPlace transaction family, which can track assets.	(unknown)
Block release time	(unknown)	Configurable	2 sec.
Transaction size	(unknown)	(unknown)	(unknown)
Transaction rate	> 10k trans./sec.	(unknown)	(unknown)
Consensus type	Pluggable consensus framework; 2 plugins provided: PBFT, and "dummy" plugin	Provides two: Proof of Elapsed Time (PoET), and Quorum Voting	Sumeragi
Mining algorithm	N/A	N/A	(unknown)

4.3.2 Digital wallet application based on Blockchain comparison

Table 4.3 shows the digital wallet comparison. The digital wallet can be categorized into two groups based on the way to keep private key, which is the most important of digital wallet.

The first group, the private key is kept with user such as MetaMask, Myetherwallet, Exodus. The advantage of this group is only person who has the private key can access the wallet and invoke functions for creating transactions. The disadvantage of this group is user cannot access the wallet if user cannot remember the private key or the wallet is in an invalid state that affects the transaction cannot be made.

Another group, the private key is kept by the provider company who provides the digital wallet. The advantage of this type, the user can create an account by providing username and password usually, so the wallet can be recovered if the user forgets their password. However, if the provider company has been discontinue that is caused to affect the user's account inaccessible.

Table 4.3 Digital wallet platform comparison

Property	**MetaMask**	**Myetherwallet**	**Exodus**	**Coinbase**
Digital wallet type	Website wallet	Website wallet	Desktop wallet	Website wallet
Web Browser plugin	Chrome, Firefox, Opera	Chrome	No	No
Private key on client side	Yes	Yes	Yes	No
Private key or password recovery	No	No	No	Yes

CHAPTER V
CONCLUSION

5.1 Conclusion

The Blockchain comparison shows that no Blockchain networks are exactly same although they come from the concept of Bitcoin's Blockchain. However, many Blockchains are created to overcome or improve the weaknesses of Bitcoin's Blockchain. The competitors may contrast in objective, process, consensus algorithm, or some different ways. The contrast can be positive or negative based on the requirement for decentralized application, which is used Blockchain as data structure. In addition, Blockchain influences the financial technology in order to be Cryptocurrency as digital assets, which are used to exchange like physical asset. In order to start Blockchain development, this research recommends Ethereum network because Ethereum provides the testing networks, and we can get the free coin with Faucet. Moreover, Ethereum is covered to create decentralize application, which is increase security level in area of data structure. To work with Ethereum network, MetaMask is the appropriate digital wallet for starter due to it is the Chrome's extension with simple interface and small program size. Indeed, the transfer fee will be kept when the new transaction is created, which is MetaMask revenue.

5.2 Future works

For further work, a variety of consensus algorithm has to be concerned for a Blockchain development in order to performance comparison in several environments to decrease the resources in terms of cost, decision, and time.

REFERENCES

1. FBS Markets Inc., “Cryptocurrency,” [Online]. Available: https://fbs.co.th/glossary /cryptocurrency-13.
2. Digital Ventures and Mark Blognone, "Explanation the Different of Bitcoin, Blockchain, Ethereum, Ripple, and Hyperledger," Feb. 14, 2017. [Online]. Available: http://www.dv.co.th/blog-th/what-is-differences-bitcoin-blockchain- ethereum-ripple-hyperle.
3. Knowled, “What is Blockchain?,” Jun. 10, 2016. [Online]. Available: http://www.aripfan.com/what-is-blockchain.
4. Blockgeeks Inc., “What is Blockchain Technology?,” 2016. [Online]. Available: https://blockgeeks.com/guides/what-is-blockchain-technology.
5. Earth, "What is Smart Contract?," Jun. 8, 2017. [Online]. Available: https://siamblockchain.com/2017/06/08/smart-contract-%E0%B8%84%E0%B8%B7%E0%B8%AD%E0%B8%AD%E0%B8%B0%E0%B9%84%E0%B8%A3.
6. Caitlin long, Distributed: Smart Contact, Nashville: BTC Inc., 2017.
7. Digital Ventures, “Smart Contact – Another technology further develop from Blockchain,” [Online]. Available: http://dv.co.th/blog-th/smart-contract-blockchain.
8. Blockchain Review, "Get to Know Wallet, A Bag That Will Help You to Store Your Digital Money," Jul 27,2018. [Online]. Available: https://blockchain-review.co.th/blockchain-review/what-is-cryptocurrency-wallet.
9. Wiput Watanasupt, "MetaMask or ERC-20 Token Storage Bag, Popular Application Launched on Mobile Phones," Nov 1, 2018. [Online]. Available: https://siamblockchain.com/2018/11/01/most-popular-ethereum-wallet-metamask- finally-releases-mobile-client.
10. Ton, "myetherwallet.com Review," Jul 27, 2017. [Online] Available: http://www.icoreview.com/review-myetherwallet-2017-thai.

11. Tanwa, "Installing and Using The Exodus Wallet Program to Store Cryptocurrency Coins," Sep 21, 2018. [Online]. Available: https://ctc.in.th/index.php?r=blog-post%2Fview&id=66.
12. Jiraboon Narktong, "Coinbase, Bitcoin Trading Website Has New 100,000 Subscribers Within A Day," Nov. 4, 2017. [Online]. Available: https://siamblockchain.com/2017/11/04/bitcoin-exchange-coinbase- adds-100000-users-in-24-hrs-shows-surging-interest-in-crypto.
13. Scan Pay, "Towards Common Blockchain Architecture an "ISO OSI for Blockchain" Primer," Nov. 23, 2017. [Online]. Available: https://medium.com/ @scanpayasia /towards-common-blockchain-architecture-an-iso-osi-for-blockchain-primer-778 db4e5b35c.
14. Jiraboon Narktong, "Proof of Work vs Proof of Stake," Aug. 13, 2017. [Online]. Available: https://siamblockchain.com/2017/08/13/proof-of-work-vs-proof-of-stake.
15. Blockgeeks Inc., "Proof of Work vs Proof of Stake: Basic Mining Guide," 2017. [Online]. Available: https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake.
16. Nuuneoi, "Knowing The Different Blockchain Consensus Protocol," Mar. 8, 2018. [Online]. Available: https://nuuneoi.com/blog/blog.php?read_id=933.
17. Katalyse, "Blockchain Basics - What is EVM?," Jun. 18, 2018. [Online]. Avalilable: https://cryptodigestnews.com/blockchain-basics-what-is-evm-52d83616764.
18. Balachander Chokkalingam, "To Better Understand Turing-Complete Blockchains, What Is An Example and A Non-Example of Turing-Complete Blockchains? If A Non-Example Does Not Exist, Why Mention It at All?," Jan. 2, 2018. [Online]. Available: https://www.quora.com/To-better-understand-Turing-complete-blockchains-what-is-an-example-and-a-non-example-of-Turing-complete-Blockchains-If-a-non-example-does-not-exist-why-mention-it-at-all.
19. Lazar Jovanovic, "Blockchain Crash Course: Protocols, DApps, APIs and DEXs," Jun. 5, 2018. [Online]. Available: https://medium.com/market-protocol/blockchain-crash-course-protocols-dapps-apis-and-dexs-4c324964f9c2.

20. Gregory, "Intro to Web3.js - Ethereum Blockchain Developer Crash Course," May. 15, 2019. [Online]. Available: http://www.dappuniversity.com /articles/web3-js-intro.
21. Michael Draper, "The Most Popular Programming Languages Used in Blockchain Development," Jan. 18, 2019. [Online]. Available: https://medium. freecodecamp.org/the-most-popular-programming-languages-used-in-blockchain-development-5133a0a207dc.
22. Ethereum Foundation, "Solidity Document," [Online]. Available: https://solidity. readthedocs.io/en/latest.
23. Google Inc., "GO Language Document," [Online]. Available: https://golang.org/doc.
24. Blockbasis, "What Is The Difference Between On-Chain and Off-Chain Transactions?," [Online]. Available: https://blockbasis.com/help/ blockchain/ difference-chain-off-chain-transactions.
25. Zibin Zheng1, Shaoan Xie1, Hongning Dai2, Xiangping Chen4, and Huaimin Wang3, “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends,” presented at 6th IEEE International Congress on Big Data, 2017.
26. Google Inc., "Chrome Browser System Requirements," [Online]. Available: https://support.google.com/chrome/a/answer/7100626?hl=en.
27. Andrey Petrov, "An Economic Incentive for Running Ethereum Full Nodes," May. 9, 2018. [Online]. Available: https://medium.com/vipnode/an-economic-incentive-for-running-ethereum-full-nodes-ecc0c9ebe22.
28. Tanya Sattaya-aphitan, "Solidity Training: How to Develop Smart Contract on Ethereum Blockchain," Sep. 12, 2018. [Online]. Available: https://medium. com/@drtan/%E0%B8%9A%E0%B8%B1%E0%B8%99%E0%B8%97%E0%B8%B6%E0%B8%81%E0%B8%81%E0%B8%B2%E0%B8%A3%E0%B8%AD%E0%B8%9A%E0%B8%A3%E0%B8%A1-solidity-%E0%B9%80%E0%B8%82%E0%B8%B5%E0%B8%A2%E0%B8%99-smart-contract-%E0%B8%9A%E0%B8%99-ethereum-blockchain-fc7b7b4847ef?fbclid=IwAR3AP5bL8pjLHeYlVVexBBivcANLQ9QQkmhz5xvQMtKVaD4UhN3Tt1W03EM.

29. Thushara Jayasinghe, "Create Your Own Cryptocurrency in Ethereum Blockchain," Jul. 17, 2018. [Online]. Available: https://medium.com/ coinmonks/create-your-own-cryptocurrency-in-ethereum-blockchain-40865db8a29f?fbclid=IwAR1EUiXDE7HN3E0osR7G5DCBd4JDHdJLQvKCy0wxHT3bx80QYVjDbdVBbvg.
30. Medvedev, "Comparison of The Different TestNets," Nov. 7, 2017. [Online]. Available: https://ethereum.stackexchange.com/questions/27048/ comparison-of- the-different-testnets.
31. Ethereum Foundation, "Ethereum Document," [Online]. Available: https://www.ethereum.org/beginners.
32. Admin, "What Is A Faucet System and Why Give Away Free Digital Currency?," Sep. 1, 2017. [Online]. Available: https://www.onlinebegin.com/faucet-system.
33. Ofir Beigel, "The Complete Beginner's Guide to Making Money From Bitcoin Faucets," Sep. 3, 2018. [Online]. Available: https://99bitcoins.com/ complete-beginners-guide-make-money-bitcoin-faucet.

APPENDIX

SOLIDITY SOURCE CODE

```
pragma solidity >=0.4.22 <0.6.0;

contract owned
{
    address public owner;

    constructor() public
    {
        owner = msg.sender;
    }

    modifier onlyOwner
    {
        require(msg.sender == owner);
        _;
    }

    function transferOwnership(address newOwner) onlyOwner public
    {
        owner = newOwner;
    }
}

interface tokenReceiver
{
    function receiverApproval(address addressFrom, uint256 totalValue, address
addressToken, bytes8 extraData) external;
}
```

```
contract TokenERC20
{
    // Token's public variables
    string public tokenName;
    string public tokenSymbol;
    uint8 public tokenDecimal = 18;
    // Suggests to set 18 for decimal which is the strongest
    uint256 public totalSupply;
    // Provides array with all balances
    mapping (address => uint256) public tokenAllBalance;
    mapping (address => mapping (address => uint256)) public tokenAllowance;
    // Generates a public event on the Blockchain that will inform client
    event tokenEventTransfer (address indexed addressFrom, address indexed
addressTo, uint256 totalValue);
    // Generates a public event on the Blockchain that will inform client
    event tokenEventApproval (address indexed addressOwner, address indexed
addressSpender, uint256 totalValue);
    // Informs client for amount burnt
    event tokenEventBurn (address indexed from, uint256 totalValue);

     //Initial contract with initial tokens
    constructor
    (
        uint256 initialSupply,
        string memory initialName,
        string memory initialSymbol
    ) public
    {
        totalSupply = initialSupply * 10 ** uint256(tokenDecimal);  // Update total
supply
        tokenAllBalance[msg.sender] = totalSupply;                // Initial tokens
        tokenName = initialName;                                  // Set token name
```

```
        tokenSymbol = initialSymbol;                    // Set total symbol
    }

    //Internal transfer
    function tokenTransfer(address addressFrom, address addressTo, uint totalValue)
internal
    {
        // Prevent transfer to 0x0 address by using burn function
        require(addressTo != address(0x0));
        // Validate sender balance before transfer
        require(tokenAllBalance[addressFrom] >= totalValue);
        // Validate overflows
        require(tokenAllBalance[addressTo] + totalValue >
tokenAllBalance[addressTo]);
        // Save this for an assertion in the future
        uint tokenPreviousBalances = tokenAllBalance[addressFrom] +
tokenAllBalance[addressTo];
        // Decrease sender's balance
        tokenAllBalance[addressFrom] -= totalValue;
        // Increase receiver's balance
        tokenAllBalance[addressTo] += totalValue;
        emit tokenEventTransfer(addressFrom, addressTo, totalValue);
        // Assert function is used for static analysis to find errors in your code. This is
garuntee this process never fail
        assert(tokenAllBalance[addressFrom] + tokenAllBalance[addressTo] ==
tokenPreviousBalances);
    }
```

```
    /*
    Transfer token function
        Transfer tokens from ower to receiver by using address as wallet
    Parameter description
        addressTo   : Receiver's address
        totalValue  : Amount of token
    */
    function transferOwner(address addressTo, uint256 totalValue) public returns (bool
status)
    {
        tokenTransfer(msg.sender, addressTo, totalValue);
        return true;
    }

    /*
    Transfer token from other function
        Transfer tokens from sender to receiver by using address as wallet
    Parameter description
        addressFrom : Sender's address
        addressTo   : Receiver's address
        totalValue  : Amount of token
    */
    function transferOther(address addressFrom, address addressTo, uint256 totalValue)
public returns (bool success)
    {
        require(totalValue <= tokenAllowance[addressFrom][msg.sender]);
        tokenAllowance[addressFrom][msg.sender] -= totalValue;
        tokenTransfer(addressFrom, addressTo, totalValue);
        return true;
    }
```

```
/*
Set allowance function
    Set spend limitation for other address
Parameter description
    addressSpender  : Spender's address that requests autholization
    maxValue        : Maximum amount that allows to spend
*/
function approveOwner(address addressSpender, uint256 maxValue) public returns
(bool status)
{
    tokenAllowance[msg.sender][addressSpender] = maxValue;
    emit tokenEventApproval(msg.sender, addressSpender, maxValue);
    return true;
}

/*
Set allowance to other function
    Set spend limitation to other address and inform it
Parameter description
    addressSpender  : Spender's address that requests autholization
    maxValue        : Maximum amount that allows to spend
    extraData       : Extra information for sending to the approved contract
*/
function approveOther(address addressSpender, uint256 maxValue, bytes8
extraData) public returns (bool status)
{
    tokenReceiver spender = tokenReceiver(addressSpender);
    if (approveOwner(addressSpender, maxValue))
    {
        spender.receiverApproval(msg.sender, maxValue, address(this), extraData);
        return true;
    }
```

```
    }

    /*
    Destroy function
        Remove tokens from the system irreversibly
    Parameter description
        burnValue   : Amount of token to burn
    */
    function burnOwner(uint256 burnValue) public returns (bool status)
    {
        require(tokenAllBalance[msg.sender] >= burnValue);
        tokenAllBalance[msg.sender] -= burnValue;
        totalSupply -= burnValue;
        emit tokenEventBurn(msg.sender, burnValue);
        return true;
    }

    /*
    Destroy from other function
        Remove tokens from the system irreversibly on behalf of other address
    Parameter description
        addressFrom : Sender's address
        burnValue   : Amount of token to burn
    */
    function burnOther(address addressFrom, uint256 burnValue) public returns (bool
status)
    {
        require(tokenAllBalance[addressFrom] >= burnValue);
        require(burnValue <= tokenAllowance[addressFrom][msg.sender]);
        tokenAllBalance[addressFrom] -= burnValue;
        tokenAllowance[addressFrom][msg.sender] -= burnValue;
        totalSupply -= burnValue;
```

```
        emit tokenEventBurn(addressFrom, burnValue);
        return true;
    }
}

/*
    Main Cryptocurrency
*/
contract MUITM is owned, TokenERC20
{
    uint256 public coinSellPrice;
    uint256 public coinBuyPrice;
    mapping (address => bool) public coinFrozenAccount;
    event coinEventFrozenFunds(address addressTarget, bool frozen);

    // Initializes contract with initial supply tokens to the creator of the contract
    constructor
    (
        uint256 initialSupply,
        string memory initialName,
        string memory initialSymbol
    )
    TokenERC20(initialSupply, initialName, initialSymbol) public {}

    // Internal transfer, this is same as tokenTransfer in TokenERC20
    function coinTransfer(address addressFrom, address addressTo, uint totalValue)
internal
    {
        require (addressTo != address(0x0));
        require (tokenAllBalance[addressFrom] >= totalValue);
        require (tokenAllBalance[addressTo] + totalValue >=
tokenAllBalance[addressTo]);
```

```
        require(!coinFrozenAccount[addressFrom]);
        require(!coinFrozenAccount[addressTo]);
        tokenAllBalance[addressFrom] -= totalValue;
        tokenAllBalance[addressTo] += totalValue;
        emit tokenEventTransfer(addressFrom, addressTo, totalValue);
    }

    /*
    Coin transfer function
        Transfer coins to target wallet
    Parameter description
        addressTarget   : Targer's address
        totalAmount     : Amount of coin
    */
    function coinTransfer(address addressTarget, uint256 totalAmount) onlyOwner
public
    {
        tokenAllBalance[addressTarget] += totalAmount;
        totalSupply += totalAmount;
        emit tokenEventTransfer(address(0), address(this), totalAmount);
        emit tokenEventTransfer(address(this), address(addressTarget), totalAmount);
    }

    /*
    Coin frozen function
        Allow or prevent |target wallet to/from sending and receiving coins
    Parameter description
        addressTarget   : Targer's address
        freeze          : Freeze status
    */
    function freezeAccount(address addressTarget, bool freeze) onlyOwner public
    {
```

```
        coinFrozenAccount[addressTarget] = freeze;
        emit coinEventFrozenFunds(addressTarget, freeze);
    }

    /*
    Set coin price function
        Set new price for coin as exchange rate
    Parameter description
        newSellPrice    : Selling price
        newBuyPrice     : Buying price
    */
    function setCoinPrices(uint256 newSellPrice, uint256 newBuyPrice) onlyOwner
public
    {
        coinSellPrice = newSellPrice;
        coinBuyPrice = newBuyPrice;
    }

    /*
    Buy coin function
        Buy coins at current buying price
    */
    function buyCoin() payable public {
        uint totalAmount = msg.value / coinBuyPrice;
        coinTransfer(address(this), msg.sender, totalAmount);
    }

    /*
    Sell coin function
        Sell coin at current selling price
    Parameter description
        totalAmount     : Amount coins to be sold
```

```
    */
    function sellCoin(uint256 totalAmount) public
    {
        address atAddress = address(this);
        require(atAddress.balance >= totalAmount * coinSellPrice);
        coinTransfer(msg.sender, address(this), totalAmount);
        msg.sender.transfer(totalAmount * coinSellPrice);
    }
}
```

BIOGRAPHY

NAME	Miss Nuttira Thongliam
DATE OF BIRTH	15 July 1993
PLACE OF BIRTH	Bangkok, Thailand
INSTITUTIONS ATTENDED	Mahidol University, 2012-2016 Bachelor of Science (Information and Communication Technology) Mahidol University, 2016-2019 Master of Science (Information Technology Management)
RESEARCH GRANTS	273 Samsen Road, Watsamphraya, Phra Nakhon District, Bangkok 10200
HOME ADDRESS	68 Moo 8 Phutthamonthon Sai 4 Road, Taweewattana, Taweewattana District, Bangkok 10200 Tel. 090-962-3444 E-mail : nuttira.tho@gmail.com
EMPLOYMENT ADDRESS	273 Samsen Road, Watsamphraya, Phra Nakhon District, Bangkok 10200 Tel. 02-283-5160 E-mail : nuttirth@bot.or.th
PUBLICATION / PRESENTATION	NUTNAPIN S., NUTTIRA T., NUTTAMON W. AND PAWITRA C., " BEEVALUATOR: AN ONLINE EVALUATION SYSTEM WITH KPIS MATCHING," ICT-ISPC, 2016.