BACHELOR OF SCIENCE WITH HONOURS IN CYBER SECURIT

Final Year Project Report

# TRANSACTION DETECTION SYSTEM BASED ON MACHINE LEARNING


Report by

CHUN YOOJIN

Supervisor

ANKIT SAURABH


Date

JULY 2022

# DECLARATION STATEMENT

I certify that the work submitted is my own and that any material derived or quoted from the published or unpublished work of other persons has been duly acknowledged.

Student Full Name: CHUN YOOJIN

Student Registration Number: 11059949

Signed: CHUN YOOJIN
Date: 15 October 2022

# ACKNOWLEDGEMENTS

I would like to thank to Ankit Saurabh for guiding me in this project. And I thank to Coventry University for giving me a great opportunity to participate in this project and varied teaching so far.

# TABLE OF CONTENTS

# LIST OF FIGURES

# GLOSSARY

Blockchain: Blockchain is based on decentralization, which is aims for peer-to-peer (P2P) transactions, away from the existing financial system that guarantees and manages all transactions in financial institutions. P2P refers to a network that connects personal computers without a server or client and each connected computer acts as a server and client and shares information.

Cryptocurrency: an electronic money that uses cryptography for secure transactions in peer-to-peer networks.

Decentralized Application: an application that can operate autonomously, typically through the use of smart contracts, that run on a decentralized computing, Blockchain, or other distributed ledger system.

Ethereum: a decentralized, open-source Blockchain with smart contract functionality. Ether (ETH) is the native cryptocurrency of the platform.

Machine learning: a field of artificial intelligence among computer science that has evolved from the research of pattern recognition and computer learning theory. it is a technology that seeks to realize functions such as human learning ability in computers.

Smart contract: a computer program or a transaction protocol that is intended to automatically execute, control, or document legally relevant events and actions according to the terms of a contract or an agreement.

Two-step authentication: to reinforce security vulnerability of a single authentication, dual authentication is a method adopted by combining two different authentications. For example, a combination of cards and personal identification numbers (PINs) can be used to increase security, such as ATM in banks.

# ABSTRACT

Although there are many cryptocurrency transactions these days, there are security problems such as frequent spam transactions and hacking. To make up for these problems, a two-factor login system is introduced, and a spam transaction detection function through machine learning is introduced to create a safe transaction culture.

Keywords – Blockchain, Machine Learning, Transaction Detection, Two-Factor Login

# 1. PROJECT PROPOSAL

## *1. Background*

This project performs spam transaction detection system to protect traders from scams such as fake cryptocurrency exchanges, rug pull scam, phishing scam, and so on. Cryptocurrency does not go through the identity authentication process through a third-party trust agency such as a bank for transactions, and because it does not use the personal information of the trading party, it is guaranteed anonymity, resulting in various scams. In this project, an identity verification function is added to the login system to add a function that allows only identified traders to trade. In addition, scam warning messages and confirmation pop-up window functions are added so that careful transactions can be made. Existing spam transactions are acquired through machine learning, and when spam transactions occur, the transaction is immediately stopped, and the trader's identity is registered in the spam list.

## *2. Problems and Solutions*

### 2.1. Problem 1

Anonymity is guaranteed by the extensive use of cryptographic technology to protect transactions between traders. So, the identity of the trader is unknown by encrypting the information of the owner and recipient of the trading. Since the trader's information is encrypted and anonymity is guaranteed, it is illegally abused for drugs, weapons, and gambling transactions and tax evasion. Such transactions cannot be tracked easily.

### 2.2. Solution 1

In case of illegal transactions, transaction tracking is possible through identification. In order to track the identity, the trader's identity is authenticated through a two-step authentication method when logging in. traders who have not been authenticated cannot trade.

### 2.3. Problem 2

Transactions are processed through a one-way hash function (SHA-256), a computer encryption technology that cannot be cancelled once it is traded. Once the transaction is completed, not only the officials but also the parties to the transaction cannot be reversed. Although unwanted transaction has completed, it is impossible to cancel the transaction once it is traded. For instance, when the account was hacked and someone else withdrew the cryptocurrency, when trader transferred the cryptocurrency to the wrong address, when trader trades accidentally, and in the event of fraud.

## 2.4. Solution 2

Before trading, a warning message that if there is any suspicious or forced trade and a confirmation message are displayed to be carefully traded. The recipient has to enter the one-time password set by the sender to accept transaction to prevent trading to wrong address accidentally.

## 2.5. Problem 3

Cryptocurrency transactions and the prices are highly increasing. As a result, it causes impersonations, phishing scams, and financial fraud attacks. Scammers install malicious code or steal assets by sending fake links. When the victim clicks the fake link, malicious code is installed, and scammer makes small payments or steals personal information secretly without victim knowing it.

## 2.6. Solution 3

Normal transactions and spam transactions are classified through machine learning, and if the transaction judged as spam transaction, it is registered in the spam transaction list. It is essential to verify the identity of the trader before the transaction. If a trader with a history of spam transactions wants to trade, the transaction is blocked automatically. Also, it is good to introduce an operator's server authority management, monitoring, and information protection management system.

# *3. Project Aim*

The aim of this project is to develop transaction detection system based on machine learning to prevent illegal and spam transactions and to secure transactions.

# *4. Project Objectives*

## 4.1. Two-factor authentication

Two-factor authentication is a system that requires user to enter a security code that is sent by SMS or e-mail every time he or she logs in. This system is inconvenient, but it is a solution that can secure the identity of users and reduce spam transactions. So, the security is expected to be strengthened with two-step authentication.

## 4.2. Double confirmation trading system

In cryptocurrency transactions, the transaction is immediately made when the transfer button is pressed, which is not cancelled. There is no way to recover the money if trader accidentally transfer money or get scammed. By introducing a double-confirmation transaction system, it

is possible to remind before transaction whether it is a spam transaction and to make a transaction carefully.

### 4.3. Classification and blocking of spam transactions based on machine learning

Some users who are not aware of spam transactions tend to be easily scammed. To prevent this situation, it is possible to detect transactions through machine learning, and classify spam transactions and normal transactions. As soon as spam transactions are detected, the transaction is blocked, and the user's identity who tried spam transaction is identified and blocked.

## *5. Project Scope*

In this study, I will develop transaction detection system based on machine learning as follows.

1) My system identifies user via authentication.
2) My system helps to trade carefully.
3) My system classifies normal transaction and spam transaction.
4) My system detects spam transaction and blocks it immediately.
5) My system has Databases.
6) My system continues to learn normal transactions and spam transactions through machine learning, and blocks spam transactions itself.

## *6. Gantt Chart*

The development plan is based on the System Development Lifecycle (SDLC), which includes planning, analysis, design, development, testing, and maintenance. The period of this project is from 22nd July 2022 to 14th October 2022.


Month 1
Month 2
Month 3
Month 4
Concept project idea
Literature review
Define problem and solution
Market research
Create Gantt chart
Define project aims and objectives
Define project scope and deliverables
Requirements gathering
Evaluate possible methods
Survey
Interview
Use case diagram
Architecture
Interface
Flowchart
Design system
Build development system
Login authentification
Double confirmation
Classify transactions
Detecting spam transactions
Blocking spam transactions
Software setup
Front-end test
Back-end test
Function test
Report
Correct system
Adapt system

## 7. Project Deliverables

1) Progress project report
2) System design
3) Code
4) Final project report

## 8. Hardware and Software Requirements

### 8.1. Hardware

MacBook Pro

### 8.2. Software

1) Mac OS Catalina Version 10.15.7
2) Visual Studio Code Version 1.70.1
3) Node.js
4) Geth
5) Truffle
6) Ganache
7) Metamask
8) Firefox web browser

# 2. LITERATURE REVIEW

## *1. What is Blockchain?*

### 1.1. Concept of Blockchain

Blockchain is a collection of blocks, and it was invented by Satoshi Nakamoto [GreeksforGreeks, 2022]. Each block contains information and has a continuity that is connected to the previous block. Blockchain is mainly used in cryptocurrency because it guarantees individual privacy and anonymity [H. Adam, 2022]. Blockchain has a decentralized system that refers to data distribution processing technology. All network participants distribute and store data, and mainly transaction details are stored. Since there is no central processing unit, data is not gathered in on place, so it is strong against hacking. Even if one is tampered with, the rest is well preserved [AWS, 2022].

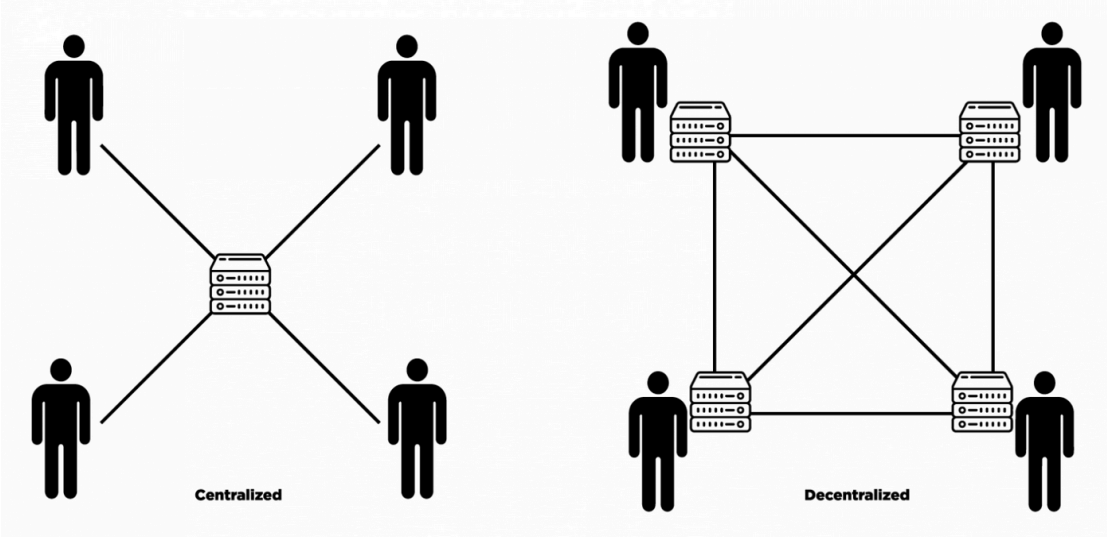



**Figure 1 Centralized and Decentralized system [W3BT, 2019]**

### 1.2. Features of Blockchain

1) Immutable

Blockchain is a permanent and unchangeable network. Blockchain technology functions through a collection of nodes. Once it validated, all records are irreversible and unchangeable. This means that not everyone on the network can edit, change, or delete it [GreeksforGreeks, 2022].

2) Secure

Banks or governments that use the existing centralized methods concentrate all data on the central server, so it can be easily hacked by attacking the central server for falsification of data. On the other hand, since the Blockchain separates and stores data by a large number of people, hackers have to attack all of the user's transaction data, so hacking is almost impossible [GreeksforGreeks, 2022].

3) Distributed and Decentralized

Blockchain is a combination of distribution and decentralization. Decentralization is a form in which a particular individual cannot manage databases, and distribution is verified by comparing it with all databases per transaction in a form in which all data are identical.

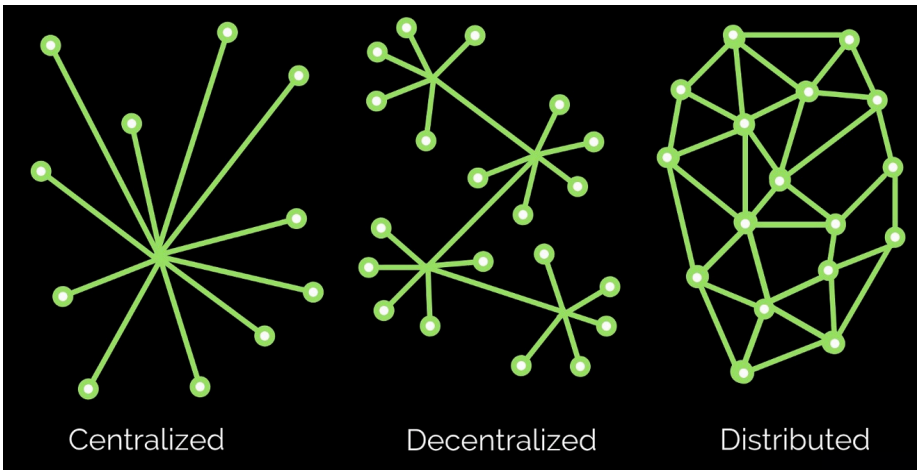



**Figure 2 The Form of Blockchain [P. Julia, 2018]**

Since Blockchain network is decentralized, an officer manager is not required, and there is no central process unit to be responsible for all decisions. Furthermore, there is no additional risk to the system as no third parties are involved. Decentralized Blockchain makes participants' profile transparent in network, so all changes are traceable and concrete [GreeksforGreeks, 2022].

## 1.3. How Does a Blockchain work?

The goal of the Blockchain is to allow digital information to be recorded and distributed, but not edited. Blockchain is also called Distributed Ledger Technology (DLT) because it is the basis of an immutable ledger, that is, a transaction record that cannot be changed, deleted, or destroyed [H. Adam, 2022].

Blockchain was first proposed as a research project in 1991, and the Blockchain concept precedes the first extensive application in use: Bitcoin, 2009. Over the next few years, the use of Blockchain has exploded through various cryptocurrencies, decentralized finance applications, Non-Fungible Token (NFT), and smart contracts [H. Adam, 2022].

Below figure shows that how does a Blockchain transaction work.

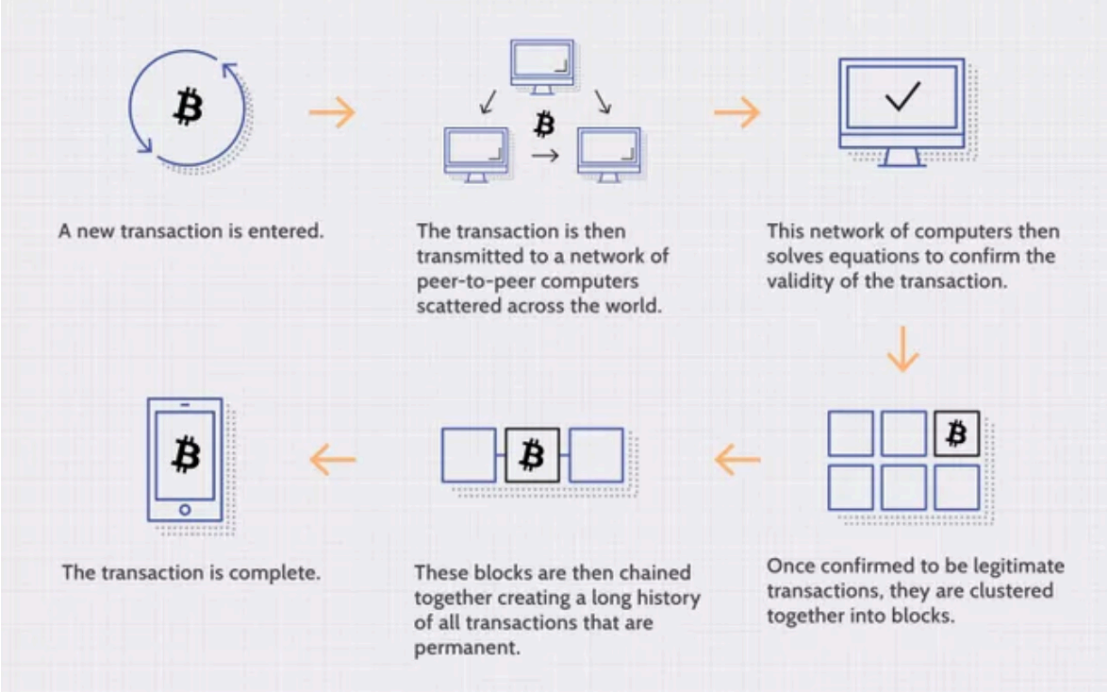



**Figure 3 Transaction Process [H. Adam, 2022]**

## *2. Cryptocurrency Scams*

Digital currency is a form of currency stored in a digital wallet, and the owner can transfer the currency to a bank account and cash it. Cryptocurrency, such as bitcoin, is different from digital currency. It uses blockchain for verification and does not run through financial institutions, so it is harder to recover from theft. Here are some of cryptocurrency scams to watch out for [H. Amanda, 2022].

### 2.1. Bitcoin investment scams

In Bitcoin investment plans, scammers introduce themselves as skilled investment managers and contact investors. As part of the plan, so-called investment managers claim to have made millions of dollars from investing in cryptocurrency and promise victims that they can make money from investing [H. Amanda, 2022].

Scammers ask for an upfront fee, and instead of making money, they steal the funds. They also claim that it is for transferring or depositing funds and require personal identification information, thus allowing access to individual cryptocurrencies [H. Amanda, 2022].

Another type of investment scam involves using fake celebrity advertisements. Scammers use celebrity's pictures and make fake accounts, advertisements, or articles to make it look like they are making a lot of money out of the investment. These claims seem legitimate to use reputable company names, which have professional-looking websites and logos. However, this advertisement is fake [H. Amanda, 2022].

## 2.2. Phishing scams

Phishing scams have been around for a long time. Scammers send e-mails containing malicious links to fake websites to collect personal information such as cryptocurrency wallet key information [H. Amanda, 2022].

Usually, phishing scams includes unusual grammar, incorrect spelling, and awkward phrases, and it is necessary to check whether the domain of the link is correct. In addition, phishing attacks tend to create pressure for victims to act quickly. For example, it sends a mail to the user that the account is about to expire, and that authentication must be completed quickly, or sends the asset to a safe wallet to prevent lose asset [H. Amanda, 2022].

To prevent phishing scams, do not enter security information from email links. Always go directly to the site, even if a legitimate website or link appears [H. Amanda, 2022].

## 2.3. Fake cryptocurrency exchanges

Scammers deceive themselves as a good cryptocurrency exchanger and attract investors. However, there is no exchange, and investors only find out that it is fake after they lose their cryptocurrency [H. Amanda, 2022].

Cryptocurrency uses blockchain for verification and does not go through financial institutions, making it more difficult to recover theft [H. Amanda, 2022].

Stick to the well-known cryptocurrency exchange market to avoid unfamiliar transactions. Before entering your personal information, you should investigate details about the reputation and legitimacy of the exchange and check the industry sites [H. Amanda, 2022].

## 2.4. Rug pull scams

Rug pull scam refers to the act of a developer or team of cryptocurrency giving up or liquidating the project and disappearing with the money of those who invested in the currency. It is one of the most worrisome risks when investing in cryptocurrency [H. Amanda, 2022].

Investors own token by exchanging Ethereum they had with listed tokens. When liquidity is created in this way, token developers withdraw all coins from the overflowing liquidity market and cash them. Then the value of the token converges to zero. Usually, for these tokens, there is no network expansion or ecosystem, and the price increases due to rumours like theme stocks [H. Amanda, 2022].

For example of rug pull, when the Squid game became a global hit on Netflix, the value of the squid coin based on it increased by a ridiculous 2,400% in just a few minutes in 2021. Squid coins were worth only $0.001 at the beginning of the transaction but soared to $2,800 in five days. At that time, Ethereum was $3,800, so it was a ridiculous price. Furthermore, it does not

have any value or ecosystem. Unsurprisingly, the coin dropped by -44,000% in value in just a few minutes after hitting its peak, making it useless again under $0 [C. Amy, 2021].

In case of the currency soaring for no reason, it is better to keep in mind that there is a rug pull risk and not approach them.

# *3. What is Ethereum?*

## 3.1. Concept of Ethereum

Ethereum, developed by Vitalic Buterin in 2015, runs various applications such as SNS, contracts, e-mails, and electronic voting as well as Bitcoin transactions and payments, and configures distributed applications (DApp) for anyone to create and use. Ethereum supports most major programming languages such as Go, Java, Python, C++, and so on [Ethereum, 2022].

The Ethereum community has built a burgeoning digital economy for developers to make money online. Users can control which data is shared with their data, and anyone can use Ethereum anywhere in the world with the Internet. Ethereum has its own cryptocurrency, ETH, and is used to pay for certain activities in the Ethereum network [Ethereum, 2022].

## 3.2. Things Ethereum Does

1) Banking for everyone

Not everyone has access to financial service, but all it takes to access Ethereum and loan, borrowing, and savings products is an Internet connection [Ethereum, 2022].

2) A more private Internet

Ethereum builds an economy based on value, not surveillance, so it is not necessary to provide all personal information to use the Ethereum application [Ethereum, 2022].

3) A peer-to-peer network

Ethereum allows users to transfer money directly or sign contracts with others without going through a intermediary companies [Ethereum, 2022].

4) Censorship-resistant

No government or company has control over Ethereum. This decentralization makes it almost impossible to prevent users from receiving payments or using services on Ethereum [Ethereum, 2022].

5) Commerce guarantees

Customers have a secure, built-in guarantee that funds will be changed only if agreed upon. Similarly, developers can be confident that the rules will not change [Ethereum, 2022].

6) All products are composable

Since all applications are built on the same Blockchain with a shared global state, they can be built with each other like Legos. This always enables better products and experiences [Ethereum, 2022].

### 3.3. Features of Ethereum

The recognition of Ethereum is inferior to Bitcoin, but it includes a smart contract function that can handle all kinds of contracts, so it is versatile. Ethereum enables the development and deployment of smart contracts. A smart contract is a simple computer program that facilitates the exchange of valuable assets between two parties, which can be money, stocks, property, or other digital assets that people want to exchange. Ethereum Virtual Machine provides the underlying technologies, architectures, and software that enable people to understand smart contracts and interact with them [DataDriveInvestor, 2021].

It is a platform that enables the development and operation of DApp, a decentralized app, and introduces an ICO method for early development funds. In ICO process, users should be careful of scams [DataDriveInvestor, 2021].

## *4. Smart Contract*

A smart contract is a self-executing contract in which the terms of the contract between the buyer and the seller are recorded directly in the code line. The codes and agreements included here exist through distributed Blockchain networks. A digital contract is signed when it writes a contract, converts it into code, and distributes it to the Blockchain. Smart contracts allow credible transactions and contracts to be carried out between different anonymous parties without central authority, legal systems, or external enforcement mechanisms. Code control execution and transactions are traceable and irreversible due to the nature of the Blockchain [F. Jake, 2022].

### 4.1. How Does a Smart Contract work?

Smart contract performs certain actions when specified conditions “if… then…” expressions. For example, if party A transfers money, then party B transfers item/property rights. A smart contract is as same as a traditional contract, except that there is no need for trust between parties. A smart contract are executed automatically by a computer program without any exceptions. As soon as certain contract conditions are met, the smart contract executes the transaction and guarantees [2MUCHCOFFEE, 2022].

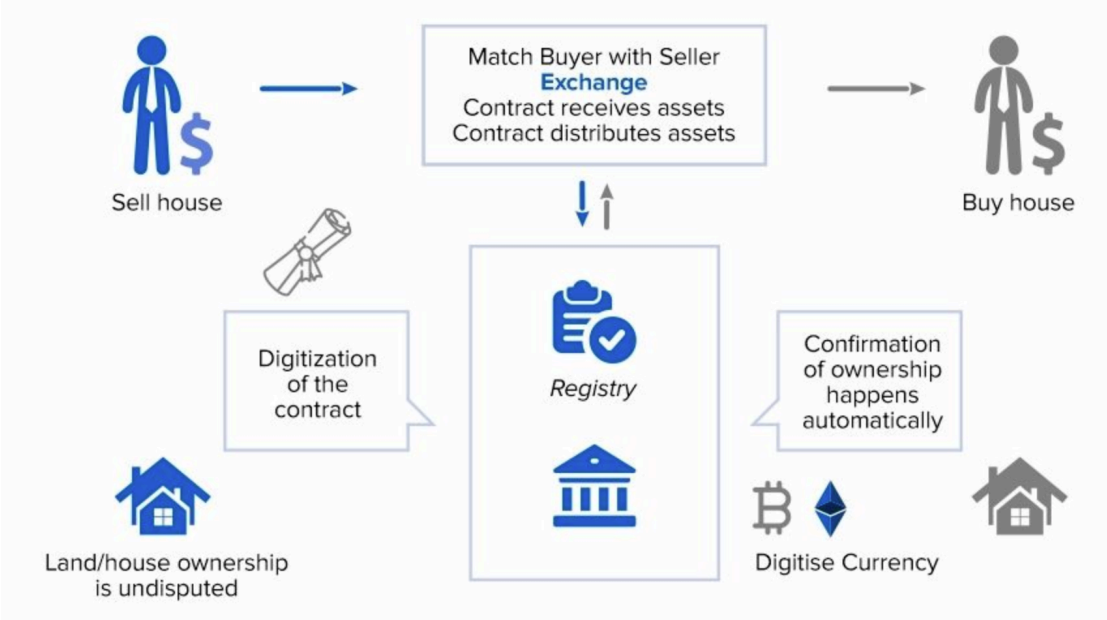



**Figure 4 Smart Contract Process [2MUCHCOFFEE, 2022]**

## 4.2. Smart Contracts Use Cases

Since the smart contract is a transaction protocol, they are highly customizable and can be developed for different types of services and solutions. Smart contracts provide increased transparency and lower operational costs as it is a decentralized and self-executing program. Some of examples include the creation of tokenized assets or shares, voting systems, cryptocurrency wallets, decentralized exchanges, games, and mobile applications. They can also be co-implemented, along with other Blockchain solutions that address areas such as healthcare, supply chain, government, and decentralized finance (DeFi) [2MUCHCOFFEE, 2022].

1) Automation of payments

The contract can be programmed so that the requested amount arrives at the specified person or organization at the specified time [2MUCHCOFFEE, 2022].

2) Registration and change of ownership

It can register necessary documents on the Blockchain to establish ownership from the start beginning and change ownership through smart contracts [2MUCHCOFFEE, 2022].

3) Energy transactions

It is believed to create a digital ecosystem for energy exchange. Therefore, the sources of electricity or fuel will be associated with smart contracts concluded only between individuals or related organizations, which in turn can personalize each customer's consumption [2MUCHCOFFEE, 2022].

4) Intellectual property

Smart contracts can be built into any digital controlled object. This is where smart assets that can be assimilated with networked objects are born. It can range from home to car. For example, rental of these properties can be automated [2MUCHCOFFEE, 2022].

5) Financial services

Cryptocurrencies open up a variety of use cases for smart contracts that would certainly not otherwise be possible. For instance, a system such as a system used by a BurstCoin can automatically check the highest price at any given time and automatically transfer inactive funds [2MUCHCOFFEE, 2022].

## 4.3. Pros and Cons of Smart Contract

First, smart contracts have autonomy, so two parties sign them without an intermediary, and Blockchain ensures the implementation of the contract. And smart contracts save significant time and speed up document processing because every step is as automated as possible and requires human existence only in the early stages of creation. Another advantage of smart contracts is secure, as is the Blockchain itself. The data recorded in the blockchain is irreversible or cannot be destroyed. In addition, smart contracts reduce the cost. It saves on involving additional specialists and operating expenses [2MUCHCOFFEE, 2022].

## 4.4. Smart Contract Market Forecast

The global smart contract market is expected to reach approximately $300 million by the end of 2023 with a CAGR of 32% over the predicted period from 2017 to 2023. Although Europe was the leader in the smart contract market, during the predicted period, North America showed significant growth and greatly expanded the use of digital technology in countries such as the United States, China, Britain, and Japan [2MUCHCOFFEE, 2022].

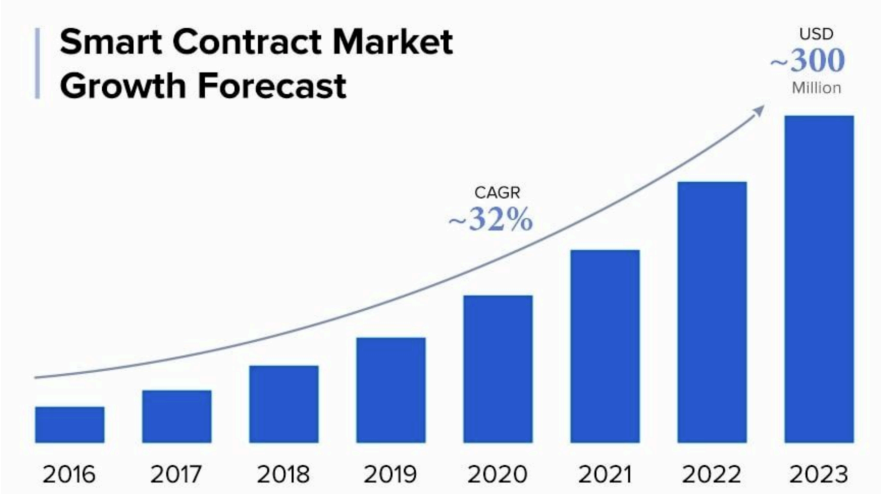



**Figure 5 Smart Contract Market [2MUCHCOFFEE, 2022]**

# *5. Decentralized Application (DApp)*

## 5.1. What is DApp?

DApp is a decentralized distributed application that operates on platform coins such as Ethereum. It is constructed based on smart contract, and DApp does not exist in Bitcoin without smart contract. It distributes, stores, and drives information on the network without a central server. Cryptocurrency and DApp are interdependent, enabling safe from data

manipulation. There are now more than 2,500 DApps and various rankings and usage coins through DApp.com [Cennz, 2022].

Most of DApps are based on the Ethereum platform. With more than 3,500 DApps already created and nearly 160,000 daily active users, these applications are likely to become standard soon. Ethereum significantly outperforms all other platforms in total DApps and the number of active users per day. Therefore, it is no surprise that Ethereum DApps receive the most attention [Velvetech, 2022].

| Platform | Total DApps | Daily active users | Transactions (24hr) | Volume (24hr) | # of contracts |
|---|---|---|---|---|---|
| Ethereum | 2,782 | 81.21k | 228.98k | 272.22k | 4.76k |
| EOS | 328 | 37.6k | 413.41k | 414.8k | 549 |
| Steem | 79 | ? | ? | ? | 174 |
| TRON | 71 | 6.43k | 17.18k | 6.69m | 211 |
| Klaytn | 65 | 16.45k | 228.33k | 78.65m | 172 |

**Figure 6 Platforms [Velvetech, 2022]**

## 5.2. DApp Games

DApp covers all Blockchain game applications, including on-chain applications and off-chain applications. Blockchain games are all games that contain Blockchain elements. It can be a game that adopts Blockchain technology at the backend, so all items obtained are safely stored in the Blockchain. It can also be a game to play using cryptocurrency and player will get cryptocurrency again as a reward. There are cryptocurrency Blockchain games using Bitcoin and ETH [Dapp, 2022].

CryptoKitties is one of the world's first game built on Blockchain technology and is a ground-breaking event that enables things like Bitcoin and Ethereum. This game has led to so many transactions that it paralyzes the network. Player can breed and own cats and get coins through the cat transactions [Dapp, 2022].

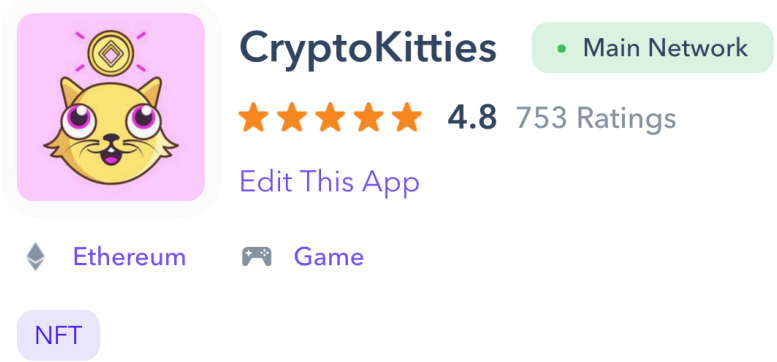



**Figure 7 CryptoKities [Dapp, 2022]**

## 5.3. How Does DApp work?

Most of the existing applications consist of three key features, interface, server, and database. Like centralized applications, DApp functionality can be divided into three basic steps: interface, smart contract, and blockchain network [Cennz, 2022].

1) Interface

The front end is almost identical to a centralized application [Cennz, 2022].

2) Smart contract

It is a part of the application that interacts with Blockchain networks. The front-end uses APIs to communicate with smart contracts [Cennz, 2022].

3) Blockchain network

Code run by the smart contract then selects and stores data on the decentralized Blockchain network [Cennz, 2022].

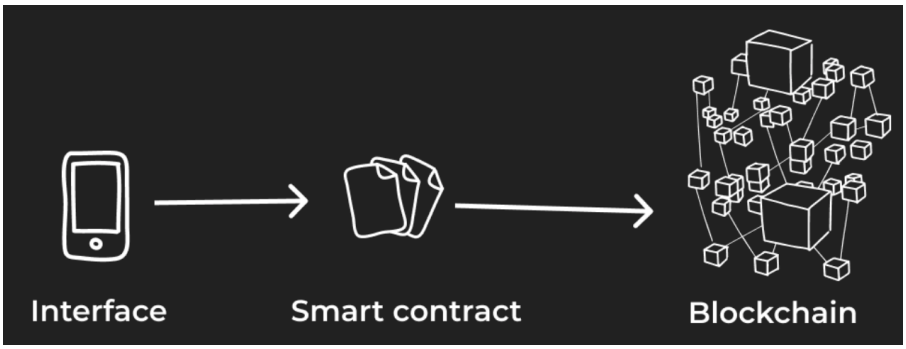



**Figure 8 DApp Process [Cennz, 2022]**

## 5.4. DApp Development

The Blockchain world is creating a vast amount of new opportunities for businesses. Blockchain technology and DApp will surely catch user's attention to increase transparency, security, and efficiency. The steps below are five steps to create DApp [Velvetech, 2022].


**Figure 9 DApp Development Steps [Velvetech, 2022]**

1) Identify the problem

It is important to identify issues that need to be addressed or future use cases of DApps. First, give an overview of the challenges you face and evaluate whether decentralized application can solve the problem [Velvetech, 2022].

2) Create a Proof-of-Concept

Proof-of-concept (POC) should be created to validate the idea and provide feasibility. Overall, it helps you test your DApp with minimal resources before you spend a lot of time

and money on the development process. It will help you identify problems and areas of improvement [Velvetech, 2022].

3) Pick a DLT platform

There are various platforms for DApp development, so you have to decide which platform is best for you. Each Blockchain platform has advantages and limitations, so it is better to have time to think about which will meet your requirements [Velvetech, 2022].

4) Develop and test the DApp

After selecting the DLT platform, you can start developing and testing DApps. Whether you are moving to a customized application development service or building through an in-house team, you need to ensure that DApps are tested thoroughly [Velvetech, 2022].

5) Launch your DApp

There is no room for error when running on a production server, so be extra careful. Do not rush the process because it is difficult to make changes once the application is deployed. As this step is high-level step, the technical aspects are much more complex. With the help of experienced experts, it helps develop Blockchain-based DApps [Velvetech, 2022].

## 5.5. DApp Development Costs

It is difficult to accurately estimate how much it costs after deploying DApps, but the four main factor below affect the cost of DApp development, which are industry, complexity, DApp type, and labour costs [Velvetech, 2022].

1) Industry

The industry which DApp will be applied has a significant impact on development costs because each sector is unique and requires a different level of sophistication. Primarily, some industries have strict compliance requirements and must respond. Some may also have a large number of users interacting with the DApp at the same time [Velvetech, 2022].

2) Complexity

As every project is complex, it is one of the biggest factors affecting the cost of deploying DApps. To determine the complexity level of the project, think about which Blockchain platform to choose which technology stack to use, whether to create a custom API, or to use a pre-built API [Velvetech, 2022].

3) DApp type

DApp can have its own Blockchain like Bitcoin or use another DApp's Blockchain like Ethereum. Therefore, there are three types of DApps, each with slightly different development costs. Type 1 DApp has its own Blockchain and being macOS. Type 2 DApp works on Type 1 Blockchain and there is nothing of its own. It is Keynote which works on macOS. And Type 3 DApp functions on a Type 2 protocol and being a template add-on that integrates into Keynote [Velvetech, 2022].

4) Labour costs

Labour costs make a big difference in DApp development budget. Fees are adjusted according to team size, location, and qualification. In addition to wages, personnel-related

costs such as recruitment, insurance and holidays should also be considered. It can be difficult to hire a Blockchain expert, so consider both the advantages and disadvantages of in-hose development and outsourcing [Velvetech, 2022].

# 3. METHODOLOGY

## *1. System Development Methodology*

The System Development Life Cycle (SDLC) process goes through the steps Analysis, Implementation, Test, and Maintenance. Since this development is my personal project as a non-expert, I chose the Waterfall model among various SDLC models. The Waterfall model is a linear sequential model that points after the next step is completed after the previous step is completed. Waterfall model has a more formal and continuous development cycle than Agile model. The project can be started easily and reliably, regardless of the size of the project as the process is long and ordered. Waterfall models are developed sequentially during planning, analysis, design, implementation, testing, and maintenance phases.

In the planning step, the outline of the objectives and requirements of the project to be carried out in the future, the progress procedure, and the budget are coordinated and confirmed.

In the analysis step, the collected data is refined and analysed in detail.

In the design step, design use case diagram, class diagram, and prototype.

In the implementation step, design and development are progressed, and each step is inspected for well-implementation, and the next step is prepared.

In the test step, front-end, back-end, and customer tests are performed, and bugs or errors that need to be fixed before the project is deployed.

In the final step, maintenance, software is constantly developed when new bugs are discovered, or software updates are required.

# 4. REQUIREMENT GATHERING

## *1. Online Survey*

“A survey on the Recognition of Blockchain and Spam Transactions.”

This survey was conducted in August 2022 by a total of 25 random people all over the worlds via online google platform. I conducted this survey to find out whether people recognize Blockchain and spam transactions and how spam transactions are frequently occurring in our society.

Question 1-3 are personal questions, which include age, gender, and occupation.
Question 4-10 are about Blockchain trading and cryptocurrency transactions.
Question 11-17 are about scam and spam transactions.
Question 18-23 are about security enhancement and finding problems of trading system.

## *2. Conclusion of Findings*

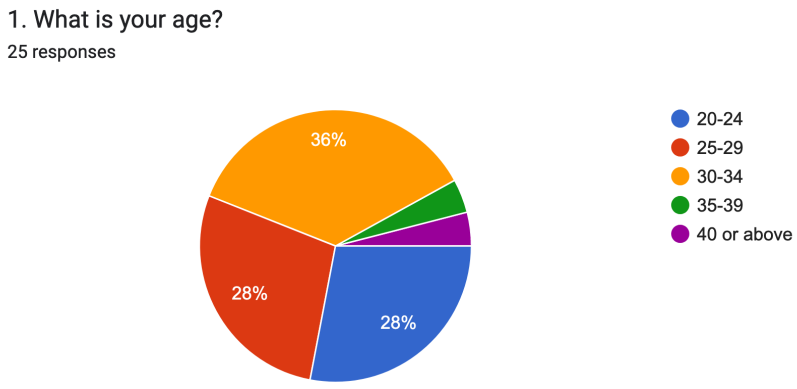



**Figure 10 Survey Q1**

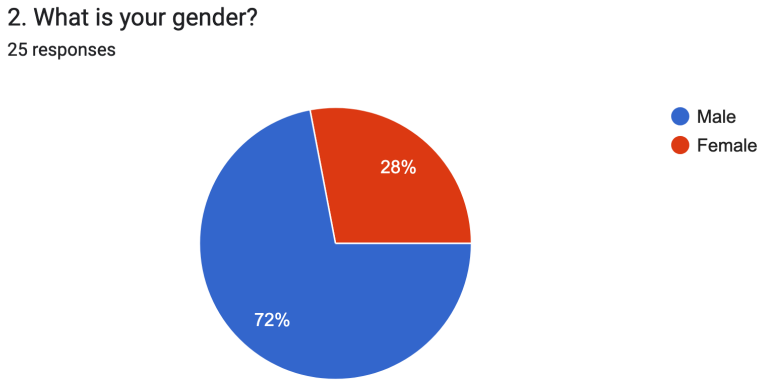



**Figure 11 Survey Q2**

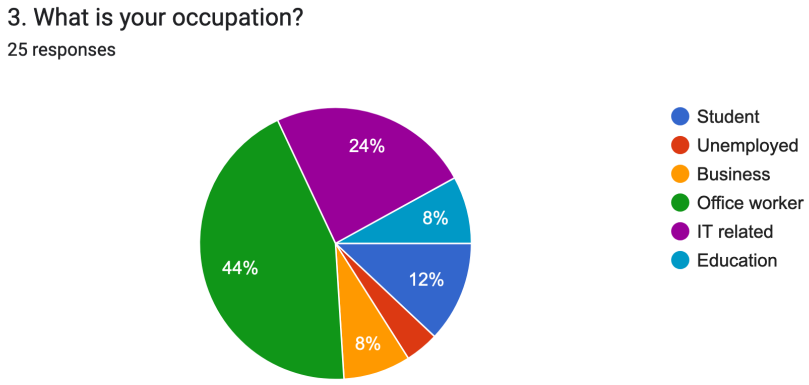



**Figure 12 Survey Q3**

A total of 25 male (72%) and female (28%) of different ages and occupations participated in the survey.

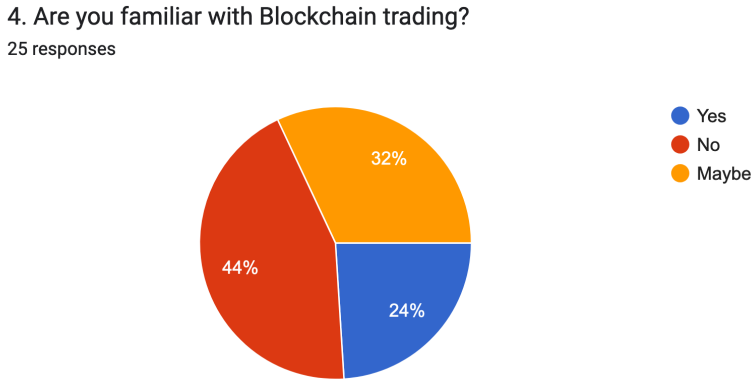



**Figure 13 Survey Q4**

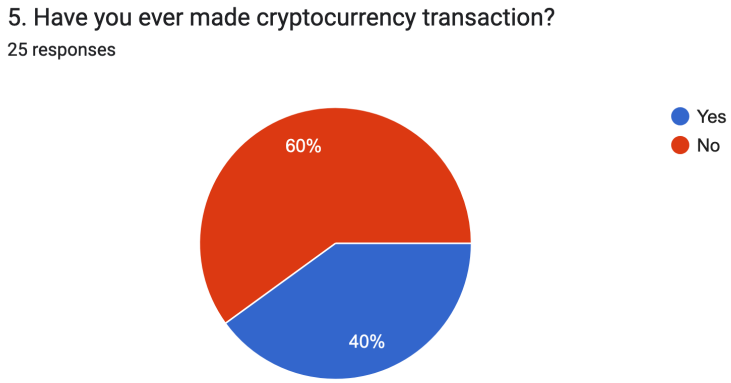



**Figure 14 Survey Q5**

According to the survey, 44% of the total were not familiar with Blockchain trading in detail. In fact, the respondents who traded cryptocurrency accounted for 40%, not more than a majority.

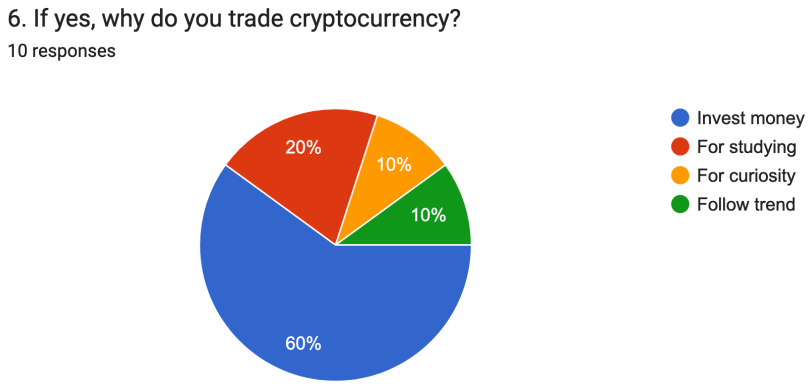



**Figure 15 Survey Q6**

60% of respondents who had an experience trading cryptocurrency were overwhelmingly trading to invest money. The rest showed 20% tendency to study, and each 10% to curiosity or follow the trend.

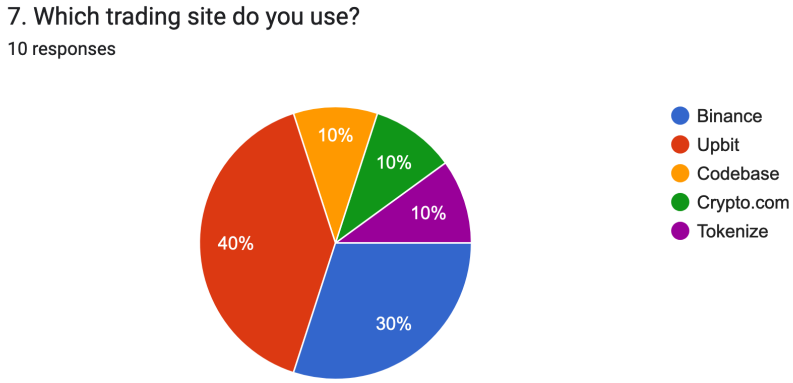



**Figure 16 Survey Q7**


**Figure 17 Survey Q8**

Upbit was the highest at 40%, the most frequently used trading site by respondents. And second highest was followed by Binance at 30%. In addition, there are 10% of each Codebase, Crypto.com, and Tokenize. The biggest reason for using the trading site was found that because it was famous, which was 70%.

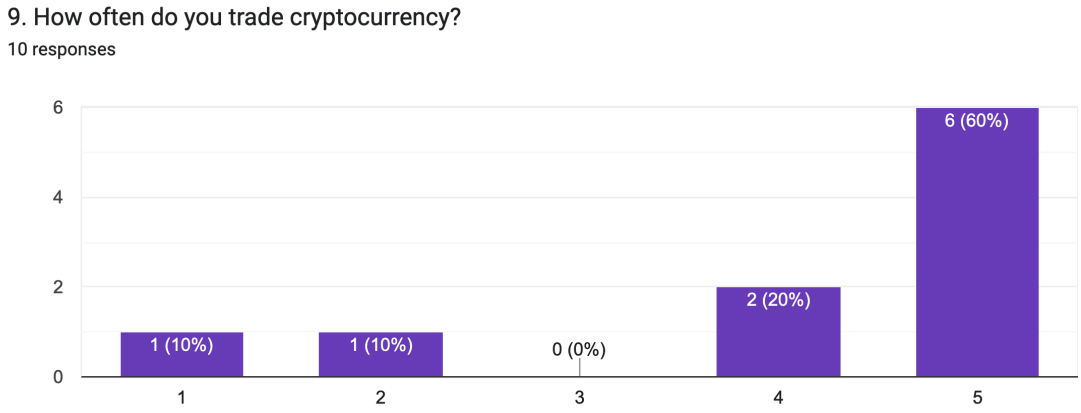



**Figure 18 Survey Q9**

Above bar graph showed that more than 60% of respondents who trading cryptocurrency frequently traded.

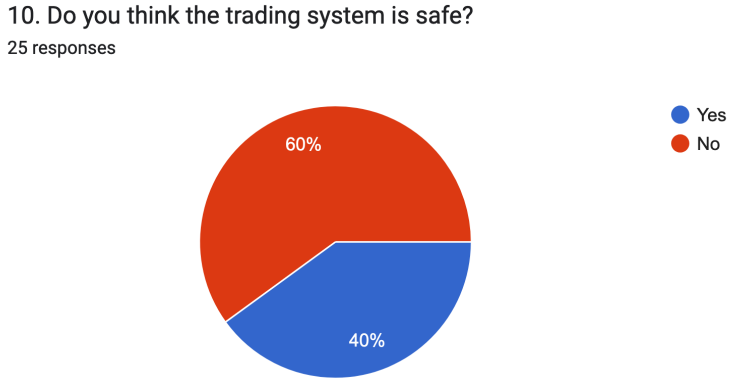



**Figure 19 Survey Q10**


**Figure 20 Survey Q11**


**Figure 21 Survey Q12**

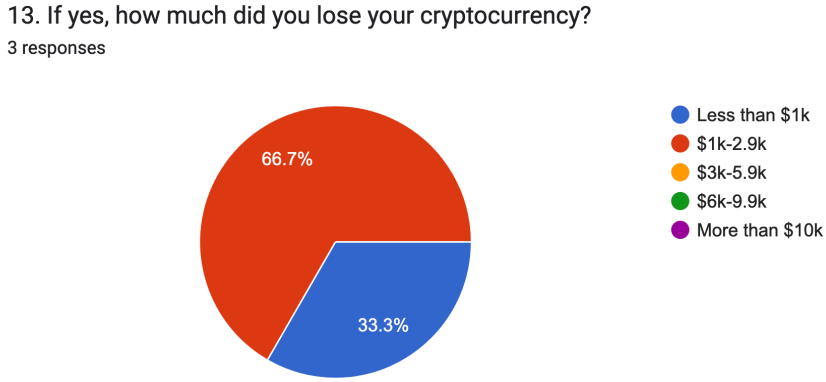



**Figure 22 Survey Q13**

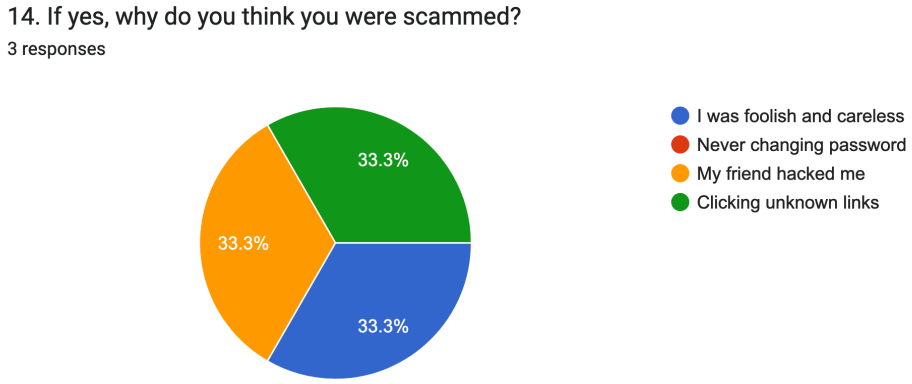



**Figure 23 Survey Q14**

60% of respondents think the trading system is unsafe. In fact, 8% of respondents have been hacked their account and 12% have been scammed. The average amount of damage was found to be $1-2k. The reasons for scam were carelessness, not changing password regularly, and being hacked by an acquaintance.

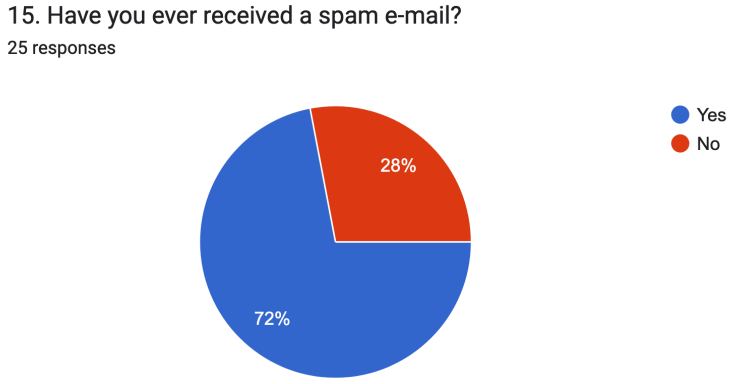



**Figure 24 Survey Q15**

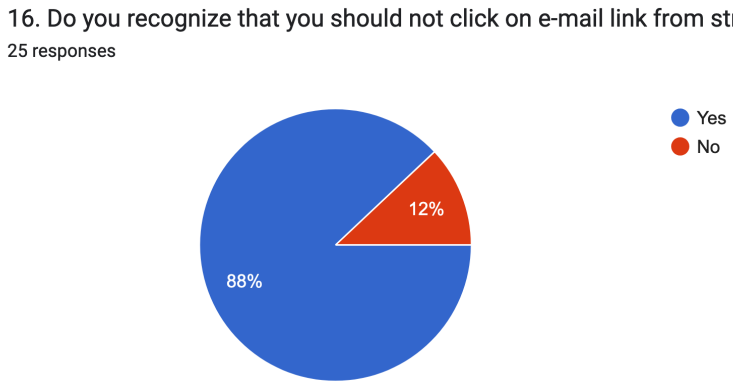



**Figure 25 Survey Q16**

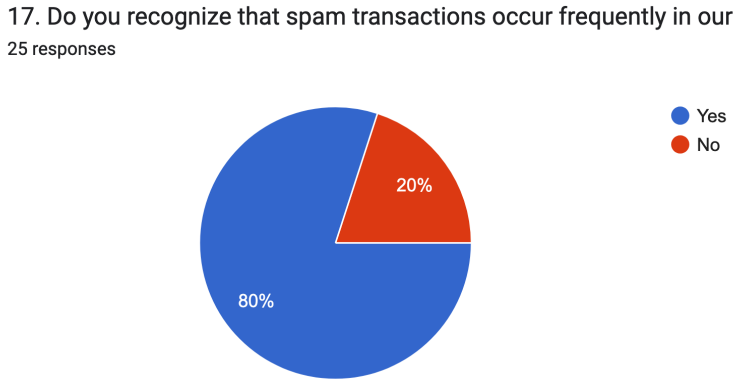



**Figure 26 Survey Q17**

72% of respondents received spam e-mail. 12% of the respondents were unaware that identified links from spam e-mail should not be opened. 20% of the respondents are completely unaware of the frequent occurrence of spam transactions in our society.

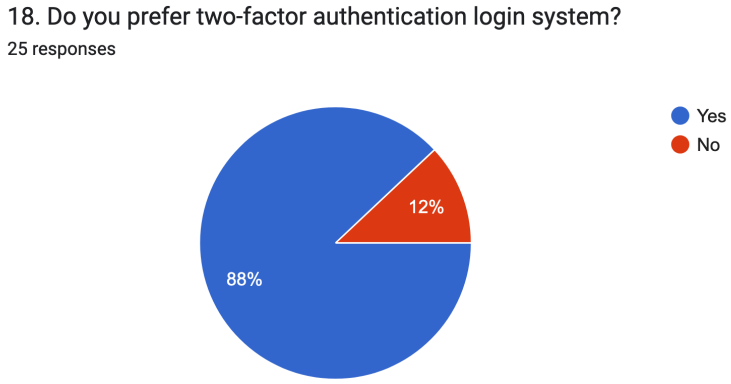



**Figure 27 Survey Q18**

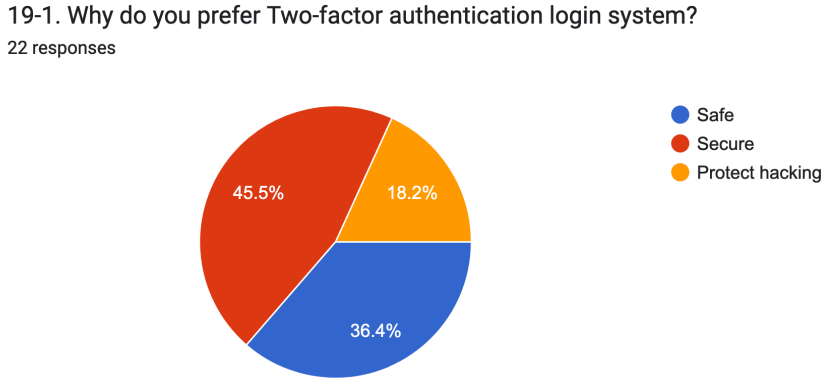



**Figure 28 Survey Q19-1**

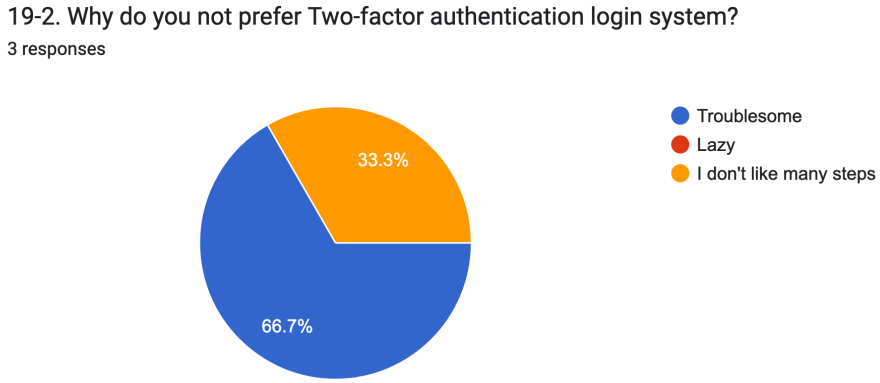



**Figure 29 Survey Q19-2**

88% of respondents said that they preferred the Two-factor authentication login system because it is secured (45.5%) and safe (36.4%). And it can prevent hacking (18.2%). 12% who do not prefer Two-factor authentication login system said that because it is troublesome (66.7%) and they do not like many steps (33.3%).

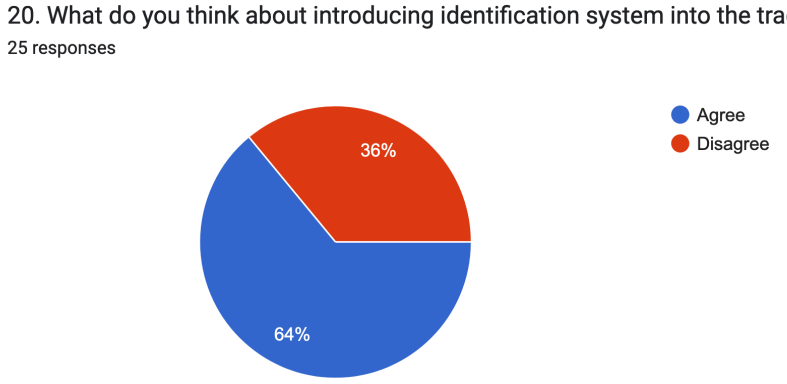



**Figure 30 Survey Q20**

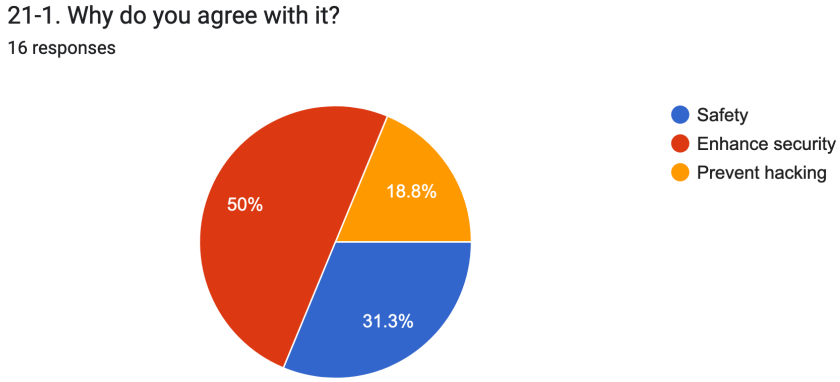



**Figure 31 Survey Q21-1**

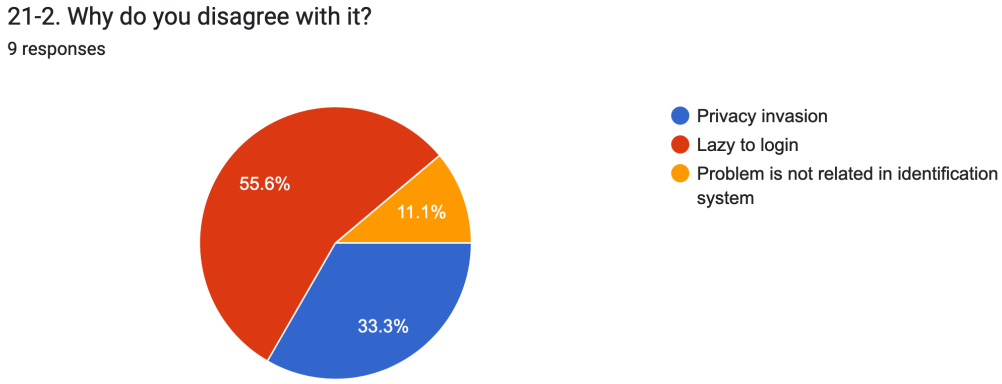



**Figure 32 Survey Q21-2**

More than a majority of 64% voted for the introduction of an identity verification system. The reason for agreement was that security enhancement was the highest at 50%, safety was 31.3%, and hacking prevention was 18.8%. And 36% disagreed with an identity verification system, 55.6% of them disagreed with it because they are lazy to login. And 33.3% said that it was because of privacy invasion, and 11.1% said that identification system is not a problem.

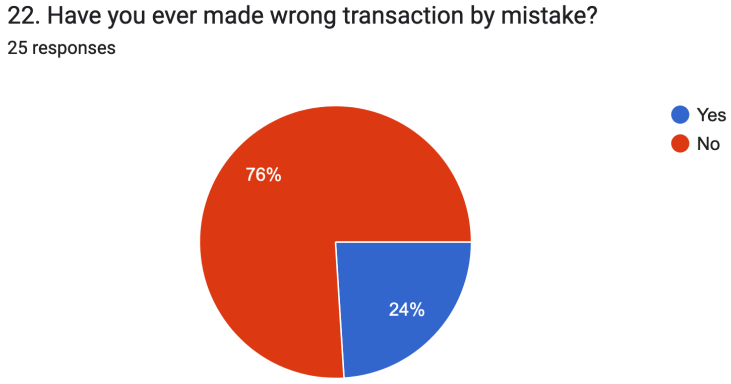



**Figure 33 Survey Q22**

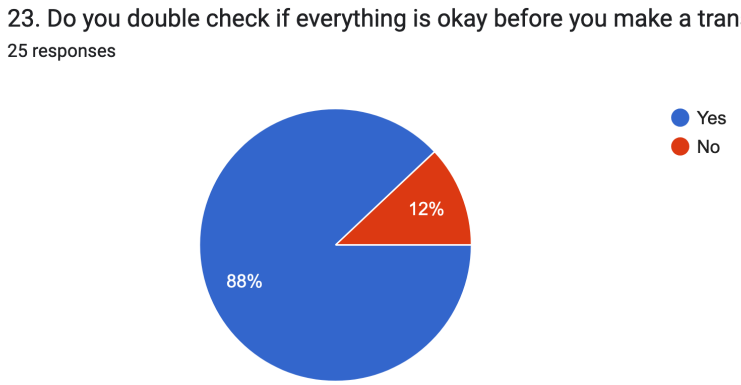



**Figure 34 Survey Q23**

According to the pie chart above, 24% have made a wrong transaction by mistake, and 12% do not double confirm that everything is okay before the transaction. Although not most people, there are some cases that transaction damage is caused by a few mistakes.

## *3. Ethical Statement*

These surveys and interviews are information obtained by requesting to anonymous majority without manipulation. Acquired information acquires minimal personal information for privacy and guarantees anonymity.

# 5. DESIGN

## *1. Use Case Diagram*

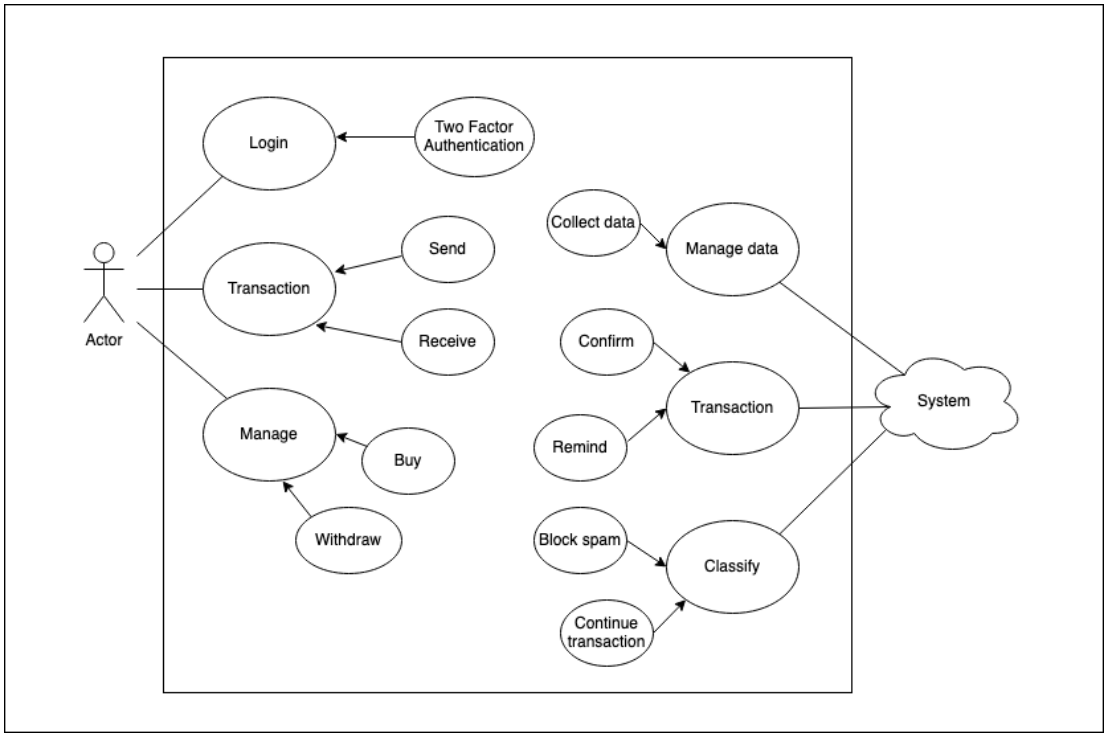



**Figure 35 Use case diagram**

## 2. *Class Diagram*

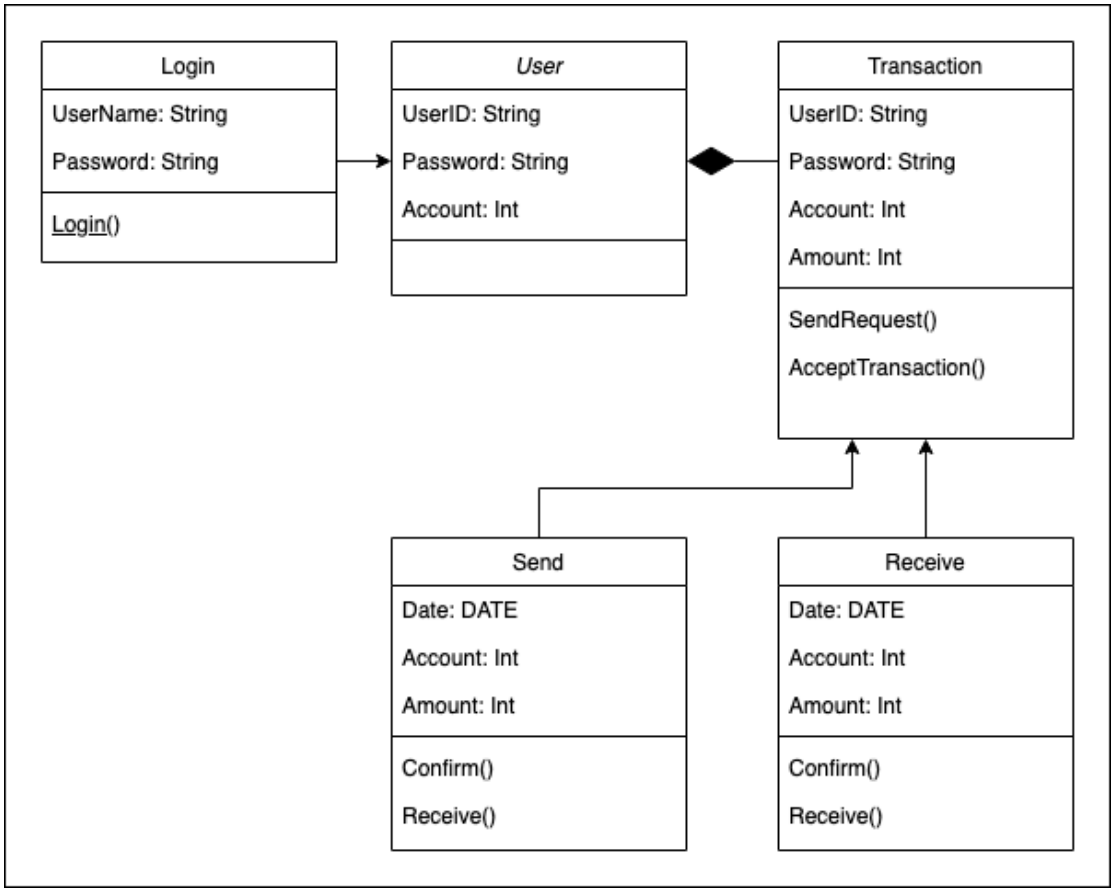



**Figure 36 Class diagram**

## 3. *Activity Diagram*

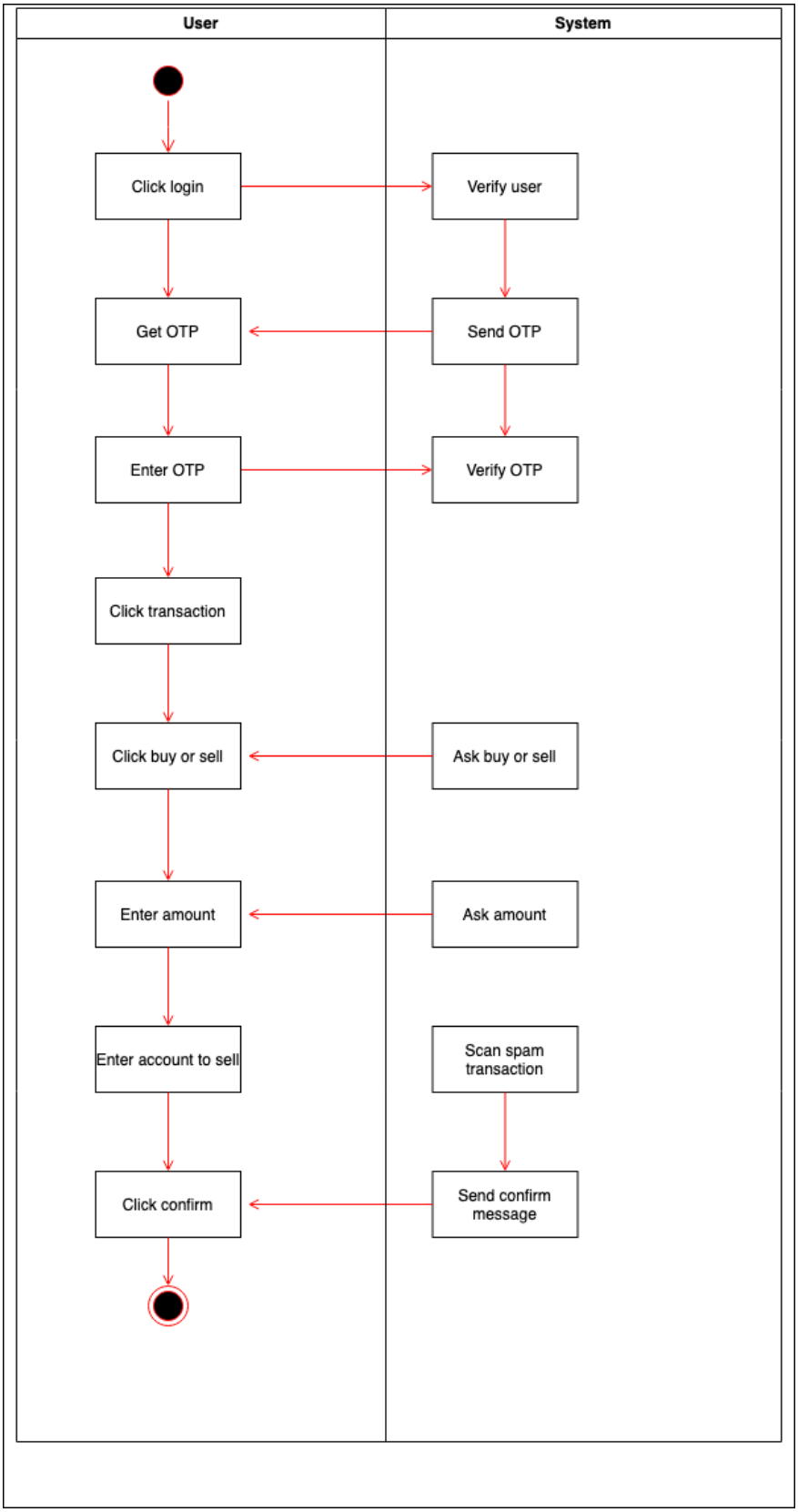



**Figure 37 Activity diagram**

# 4. Prototype Design

## 4.1. Prototype Sketches

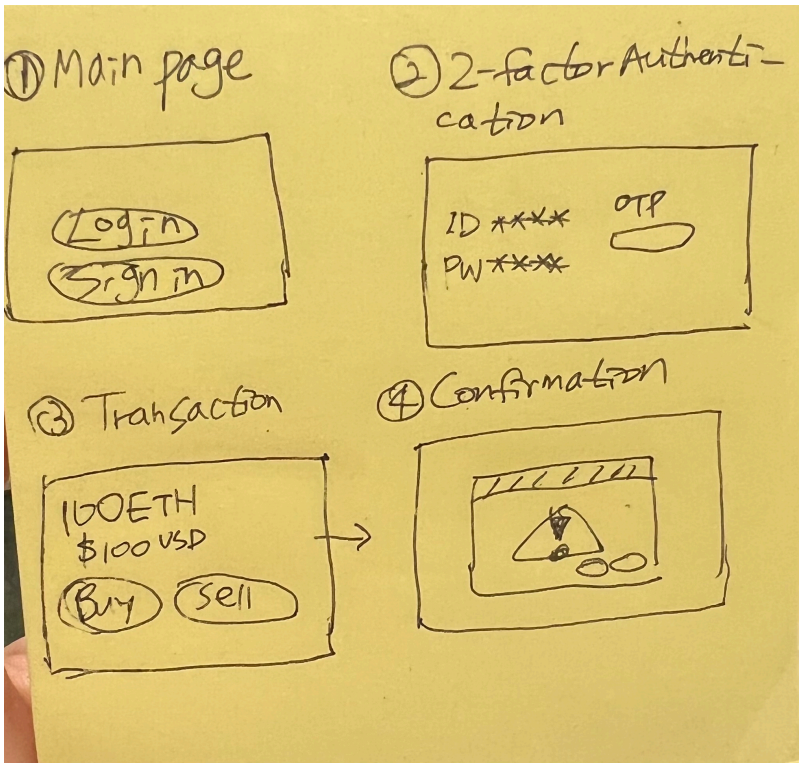



**Figure 38 Prototype sketches**

## 4.2. Prototype Code

```
// SPDX-License-Identifier: GPL-3.0
pragma solidity >=0.5.0 <0.9.0;

contract CryptoCurrency {
    enum Status { Available, Unavailable }
    Status currentStatus;

    event Trade(address _buyer, uint _value);

    address public seller;
    address public buyer;

    constructor() payable {
        currentStatus = Status.Available;
        seller        = msg.sender;
        //buyer = _buyer;
    }

    modifier checkAvailable {
        require(currentStatus == Status.Available, "Currently not
available.");
```

```
22.         _;
23.     }
24.
25.     modifier checkBuyer() {
26.         require(msg.sender == buyer, "Buyer is not same.");
27.         _;
28.     }
29.
30.     modifier checkCost(uint _amount) {
31.         require(msg.value >= _amount, "Not enough Ether provided.");
32.         _;
33.     }
34.
35.     function addBuyer() public {
36.         buyer = msg.sender;
37.     }
38.
39.     function getBuyer() public view returns(address) {
40.         return buyer;
41.     }
42.
43.     function getStatus() public view returns(bool) {
44.         if (currentStatus == Status.Available) {
45.             return true;
46.         } else {
47.             return false;
48.         }
49.     }
50.
51.     receive() external payable checkAvailable checkBuyer checkCost(1
    ether) {
52.         currentStatus = Status.Unavailable;
53.         (bool result, ) = buyer.call{ value: msg.value }("");
54.         require(result, "failed to trade.");
55.         emit Trade(msg.sender, msg.value);
56.     }
57. }
```

# 6. IMPLEMENTATION AND TESTING

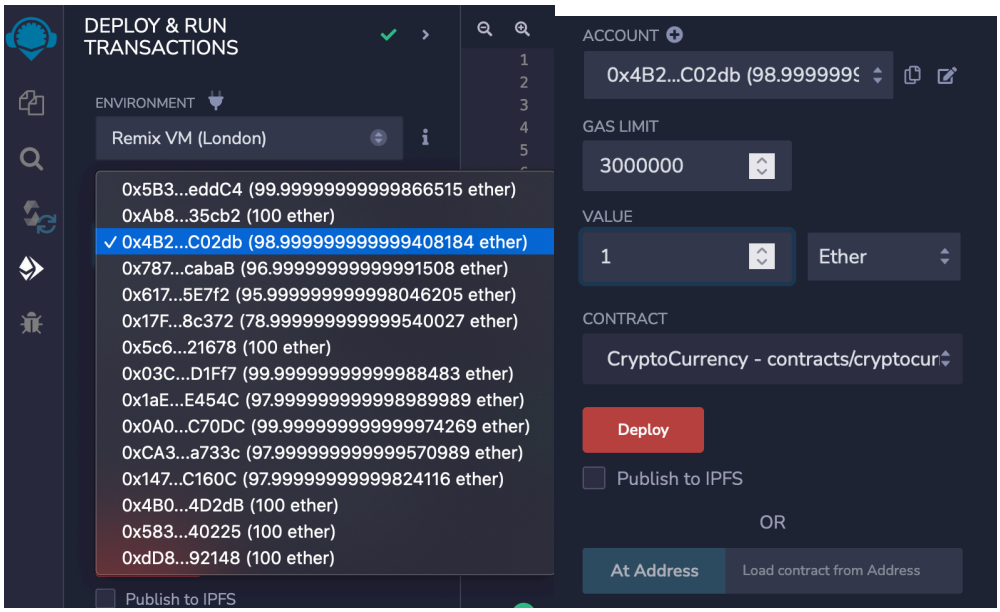
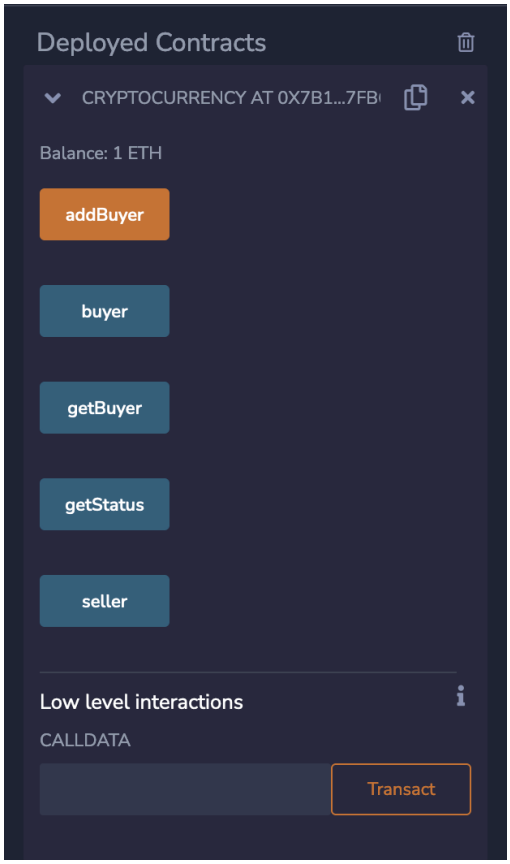



**Figure 39 Deploy and run transaction**




Deployed contracts


**Figure 40 Deploy succeed**

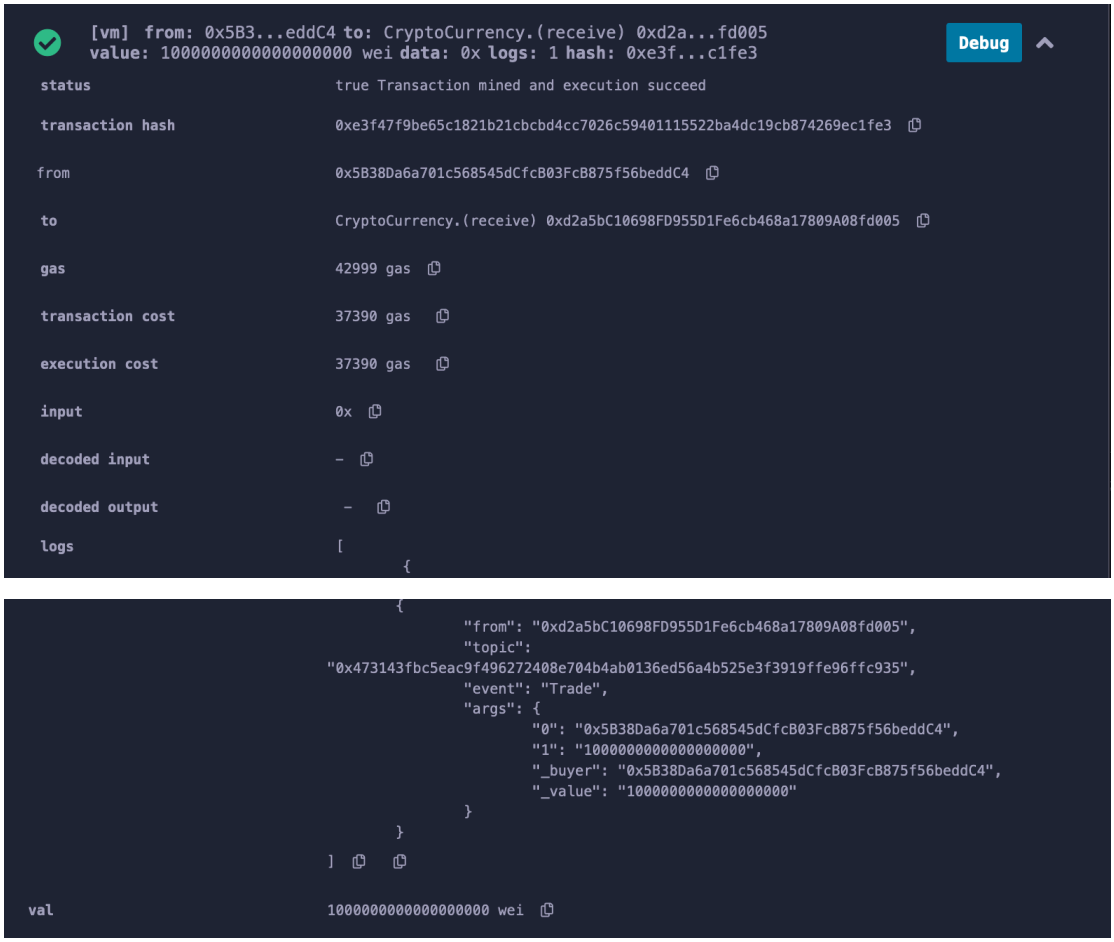



**Figure 41 Transaction Succeed**

# CONCLUSION

The main purpose of this project is to prevent spam transactions that occur frequently when trading cryptocurrency and to make proper transactions. For system development, it was developed as Remix Ethereum, and transactions without failure were implemented by implementing transactions only through designated buyers and sellers. Through this project development, there is no transaction by mistakes or fraud, so it is possible to trade cryptocurrencies more safely.

REFERENCES

H. Adam (2022). What is a Blockchain? [Online] Investopedia.com. Available at: https://www.investopedia.com/terms/b/blockchain.asp [Accessed 25th Jul. 2022].

AWS (2022). What is Decentralization in Blockchain? [Online] AWS.amazon.com. Available at: https://aws.amazon.com/blockchain/decentralization-in-blockchain/ [Accessed 25th Jul 2022].

W3BT (2019). Why Blockchain Is The Future | 10,000 Feet Up. [Online] Web 3.0 Blockchain Transition. Available at: https://w3bt.io/why-blockchain-is-the-future/ [Accessed 27th Jul 2022].

GreeksforGreeks (2022). Features of Blockchain. [Online] GreeksforGreeks. Available at: https://www.geeksforgeeks.org/features-of-blockchain/ [Accessed 27th Jul 2022].

P. Julia (2018). What's the difference between Decentralized and Distributed? [Online] Medium. Available at: https://medium.com/nakamo-to/whats-the-difference-between-decentralized-and-distributed-1b8de5e7f5a4 [Accessed 01st Aug 2022].

H. Amanda (2022). 9 Common Cryptocurrency Scams in 2022. [Online] WhatIs.com. Available at: https://www.techtarget.com/whatis/feature/Common-cryptocurrency-scams [Accessed 02nd Aug 2022].

C. Amy (2021) 'Squid Game'-inspired cryptocurrency that soared by 23 million percent now worthless after apparent scam. [Online] The Washington Post. Available at: https://www.washingtonpost.com/world/2021/11/02/squid-game-crypto-rug-pull/ [Accessed 04th Aug 2022].

Ethereum (2022). What is Ethereum? [Online] Ethereum.org. Available at: https://ethereum.org/en/what-is-ethereum/ [Accessed 04th Aug 2022].

DataDriveInvestor (2021). 5 Ethereum Features. [Online] DataDriveInvestor. Available at: https://medium.datadriveninvestor.com/5-ethereum-features-76da9462b319 [Accessed 04th Aug 2022].

F. Jake (2022). Smart Contracts. [Online] Investopia. Available at: https://www.investopedia.com/terms/s/smart-contracts.asp [Accessed 07th Aug 2022].

2MUCHCOFFEE (2022). What Is a Smart Contract and Where to Use It? [Online] 2MUCHCOFFEE. Available at: https://2muchcoffee.com/blog/what-is-a-smart-contract-and-where-to-use-it/ [Accessed 07th Aug 2022].

Cennz (2022). WHAT IS A DAPP AND WHY ARE THEY USEFUL? [Online] cennz.net. Available at: https://cennz.net/knowledge-hub/cennznet-blockchain-101/what-is-a-dapp-and-why-are-they-useful/ [Accessed 10th Aug 2022].

Dapp (2022). Games. [Online] dapp. Available at: https://www.dapp.com/topics/blockchain-games [Accessed 10th Aug 2022].

Velvetech (2022) Beginner's Guide To DApp Development. [Online] Velvetech. Available at: https://www.velvetech.com/blog/dapp-development-beginners-guide/ [Accessed 10th Aug 2022].