**Cover sheet for submission of work for assessment**

|  |
| --- |
| UNIT DETAILS |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Unit name | IT Security | | | Class day/time |  | Office use only |
| Unit code | COS30015 | Assign no. | 1 | Due date | 10/1/2022 |
| Name of lecture/teacher | | Dr. Nguyen Dai Tho | | | |
| Tutor/marker’s name | |  | | | |

|  |
| --- |
| STUDENT(S) |

|  |  |  |  |
| --- | --- | --- | --- |
| Family Name(S) | | Given Name(S) | Student ID Number(s) |
| (1) | Nguyen | Trung Hieu | 19021271 |

|  |
| --- |
| DECLARATION AND STATEMENT OF AUTHORSHIP |

1. I have not impersonated, or allowed myself to be impersonated by any person for the purposes of this assessment.

2. This assessment is my original work and no part of it has been copied from any other source except where due acknowledgement is made.

3. No part of this assessment has been written for me by any other person except where such collaboration has been authorised by the lecturer/teacher concerned.

4. I have not previously submitted this work for this or any other course/unit.

5. I give permission for my assessment response to be reproduced, communicated, compared and archived for plagiarism detection, benchmarking or educational purposes.

I understand that:

6. Plagiarism is the presentation of the work, idea or creation of another person as though it is your own. It is a form of cheating and is a very serious academic offence that may lead to exclusion from the University. Plagiarised material can be drawn from, and presented in, written, graphic and visual form, including electronic data and oral presentations. Plagiarism occurs when the origin of the material used is not appropriately cited.

**Student signature/s**

I declare that I have read and understood the declaration and statement of authorship.

*Nguyen Trung Hieu*

**ABSTRACT**.  
Nowaday, most of us have must heard of any cryptocurrency’s name at least once as these blockchain-based virtual currency usage has been in circulation for last twelve years and has been very trendy recently. As of now, the crypto market cap is currently sitting at $2.6 trillion. So the cryptography market indeed looks lucrative but however, it had drawed tons of attention from malicious users who attempts to hack and steal these . So concern for security of these cryptocurrency had been a concern by majority of people who participate in the market.

\_\_ This literature will dig deep in how the blockchain features play a role in cryptocurrency, defensive methods that cryptocurrency like bitcoin and ethereum used.



ASSIGNMENT 1

SECURTY IN BLOCKCHAIN-BASED CRYPTOCURRENCY

Nguyen Trung Hieu

StudentID: 19021271

Email: 19021271@vnu.edu.vn

University of Engineering and Technology

# Table of Contents

[Table of Contents 1](#_Toc92485948)

[I. Introduction: What is cryptocurrency and blockchain 2](#_Toc92485949)

[a. Some terminology 2](#_Toc92485950)

[b. 3](#_Toc92485951)

[II. Current state of art 4](#_Toc92485952)

[a. Literature review 4](#_Toc92485953)

[1. Bitcoin: A Peer-to-Peer Electronic Cash System (Length: 9) 4](#_Toc92485954)

[2. Security of Cryptocurrencies in blockchain technology: State-of-art, challenges and future prospects (Length: 35) 4](#_Toc92485955)

[3. BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network (Length: 11) 5](#_Toc92485956)

[4. Analysis of Security in Blockchain: Case Study in 51%-Attack Detecting (Length: 10) 5](#_Toc92485957)

[5. Random Mining Group Selection to Prevent 51% Attacks on Bitcoin (Length: 2) 5](#_Toc92485958)

[6. A new key protocol design for cryptocurrency wallet (Length: 6) 6](#_Toc92485959)

[7. Privacy and Security Analysis of Cryptocurrency Mobile Applications (Length: 6) 6](#_Toc92485960)

[8. Multiple Layered Security Analyses Method for Cryptocurrency Exchange Servicers (Length: 3) 6](#_Toc92485961)

[b. Analysis of the paper 6](#_Toc92485962)

[1. Blockchain 6](#_Toc92485963)

[2. 51% Attack 6](#_Toc92485964)

[3. Security of mobile device using CC 6](#_Toc92485965)

[III. Conclusion 0](#_Toc92485966)

[IV. Citation 0](#_Toc92485967)

# I. Introduction: What is cryptocurrency and blockchain

## a. Some terminology

#### Decentralized networks

A decentralized network architecture distributes workloads among several machines, instead of relying on a single central server [W5]

#### Public ledger

A record-keeping system that keeps track of participants' identities in a secure and (pseudo-)anonymous form, as well as their respective bitcoin balances and a log of all real network transactions[W10].

#### Byzantine Fault

A situation where the framework may collapse if the members cannot agree on a network approach. The Fault assumes that certain members are corrupt, ineffective, or undemocratic, emphasizing that even a single point of failure might jeopardize the entire strategy.

#### Peer-to-peer

Two users interact directly without the need of a third party or intermediary.

#### Hashpower

Hash power, or hash rate, are interchangeable terms used to describe the combined computational power of a specific cryptocurrency network or the power of an individual mining rig on that network[W9].

#### Mining

A process that using CPUs to solve various mathematical puzzles that basically the processing of transactions and an amount of cryptocurrency will be given to the miner wallet as compensation for processing the transaction.

#### Cryptocurrency wallet

A wallet where one can keep their cryptocurrency.

#### Public key

The address of someone’s cryptocurrency wallet.

#### Private Key

The code that permits one to get immediate access to their cryptocurrency wallet, similar to a password.

#### 51% Attack

A situation where more over half of the network's mining hashrate, or computer power, is controlled by a small handful of miners. The they would be able to block fresh transactions from receiving confirmations, effectively halting all transactions between merchants and customers. As a result, their transactions will be linked to the longest chain of transactions[P4].

#### Double-spend

It simply a certain amount of asset can be spent twice in a digital currency system because of faulty duplication.

## b.

Cryptocurrencies are a digital currency that utilize various cryptographic methods and algorithms like public-privte key pairs and hashing function to secure and encrypt transactions between users, hence the “crypto” part in the name. The mean of acquisition is either buying them directly from various cryptocurrency trading platform or “mining” them.

When talking about them, many people think that Bitcoin or BTC is the first one enter the exist, but actually it only the first blockchain based cryptocurrency. The pioneer of digital payment is DigiCash founded by David Chaum in 1989 and the concept of it made by him actually date back several years ealier while the first concept of blockchain worked on by Stuart Haber and Scot Stornetta started in 1991. DigiCash declare bankruptly in 1998 but many of its formula and encryption tools helped the development of modern digital currency.

In 2008, a 9 papers long whitepaper about Bitcoin made by Satoshi Nakamoto, whose identity today is still actually unknown as that’s just the name got put in the paper. In short, the document proposed a peer-to peer digital transaction network system that doesn’t need any third-parties, the record of all transactions can’t be corrupted or hard to be reversed, preventing counterfeit or double-spend, based on blockchain model[W4]. The later on success of bitcoin has launched several other cryptocurrencies into existence, most of them share the same characteristic that bitcoin has: a decentralized network with transaction recorded with blockchain technology, a public ledger.

As of now there is estimated to be 300 million cryptocurrency users worldwide, there are 18,000 businesses and brands that accept cryptocurrency as payments. Bitcoin were made available to the public in the 2009 and currently still the world most widely exchanged cryptocurrency. As of now it worths 46,412.50 USD currently and reached an annual growth rate of 274%[W1]. There will be only 21 million bitcoins that exist. It followed by Ethereum and Binace coin that while valued much less compared to bitcoin: 3,809.00 USD and 512.7 USD, still very prized.

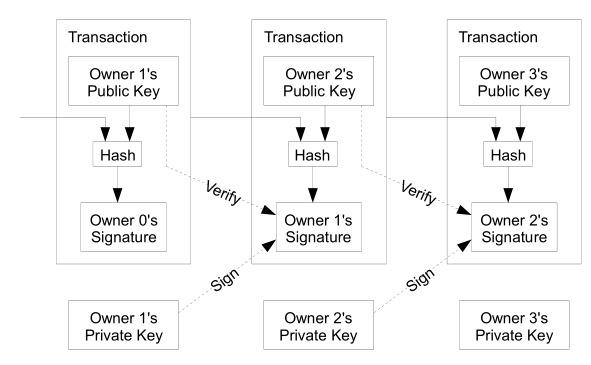
That combined with the nearly impossible to modify transactions record however has make it attractive to criminal. The victim simply cannot ask for a redo of transactions like tranditional bank if they got the wallet stolen. The thieves can remains anonmyous even if all transactions are public, the wallet address simply contain no information, make it impossble to trace the attacker. The number of Fraudulent transactions or hacking the system has rised even more as it got more popular. Nowaday attacks with damage up to hundred of million dollar happen quite common, they can also happen in smaller scale of course but in total they has accumulated $1.93 billion. The attack can be commited by a lone wolf or an entire cybercrime organization behind it. It is spectaculated that nearly $1 billion has been stolen from exchanges by two groups of cybercriminal that still active as of today[W7].

Because of that, many research and study has been done to analyze the existing security measure of blockchain-based crypto currency

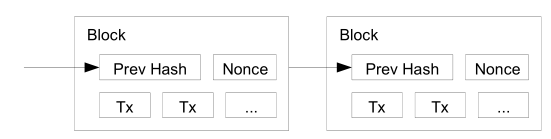
# II. Current state of art

## a. Literature review

### 1. Bitcoin: A Peer-to-Peer Electronic Cash System (Length: 9)

In this paper[1] made by Satoshi Nakamoto, who we don’t know whether they is an individual or a group as they refer to themselves as we, they propose a system that allow transactions of currency to be third-party free as back in the day most online payment system still have to go through a trusted third party like bank, using decentralized architecture and peer-to-peer transactions that is immutable through cryptography. When someone transfers a certain amount of bitcoin to another user, the network verifies various information from previous blocks to create future block to ensure the amount get exchanged is correct. The transfer is irreversible.

The group have some foresee for the potential issue the currency like double-spend. But with the blockchain model, the newly created transaction node has to be verified by other nodes in the network.

Proof of work is a major part of bitcoin. It’s attach a hash value created by SHA-256 of each transaction to a puzzle. The puzzle must be solved correctly by the sender’s system to execute the transaction. The block then will be put in the longest nodes. The transaction history will be limited to the network of blocks that increasing in length as more transaction get made and nearly impossible to modify. If attack still wish to do so they would need to have at least 51% of computational power of the network as they have to redo every future nodes and catch up with the longest nodes of transaction.

This provide an incentive for user who has enough hashpower to choose to play by the rule or stealing back past payment as mining t

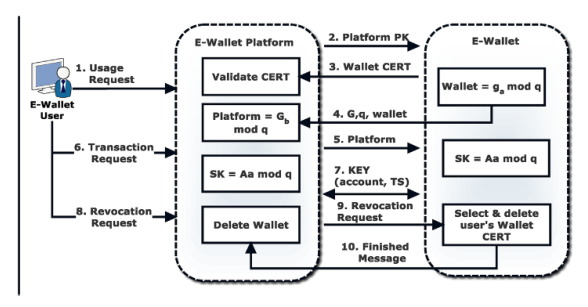
### 2. Security of Cryptocurrencies in blockchain technology: State-of-art, challenges and future prospects (Length: 35)

In this document by the team of researcher, Arunima Ghosh, Shashank Gupta , Amit Dua , Neeraj Kumar, they analyzed the blockchain

They pointed out that Illegitimate block is easility detected as authenticating is faster than creating a block

On analysis on security

Blockchain has a decentralized nature while isn’t prone to single point of failure unlike public key infrastructure (PKI), has potential for privacy protection. Bitcoin combined blockchain and cloud computing technology to create a complex security protocol and avoid Byzantine faults.



### 3. BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network (Length: 11)

Shailendra Rathore, Byung Wook Kwon, Jong Hyuk Park

This paper discuss about how blockchain can improve existing flaw of decentralized network architecture. While it isn’t about crypto currency it can give us some insight in the blockchain

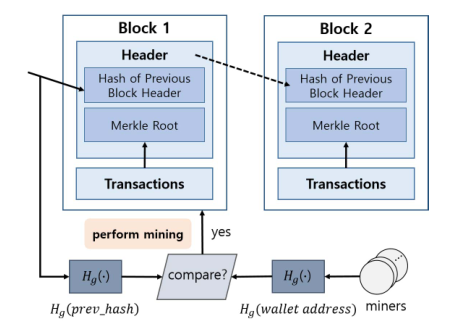
### 4. Analysis of Security in Blockchain: Case Study in 51%-Attack Detecting (Length: 10)

Congcong Ye, Guoqiang Li , Hongming cai, Yonggen Gu, Akira Fukuda.

In this document they mainly discuss about 51% Attack

A situation when a group of miners is in control of more than half of the network’s mining hashrate

### 5. Random Mining Group Selection to Prevent 51% Attacks on Bitcoin (Length: 2)

As mentioned, Bitcoin is known for resolving double-spending problems, the longest chain of block is selected to it. However, if there is a group of nodes which hash power is greater than half of the total hash power, they can perform a 51% attack. So in this document by Jaewon Bae and Hyuk Lim propose a solution to prevent said attack of a the Bitcoin network called Random Mining Group Selection.

The miner will be divided into multiple group, not all miners are always involved in the mining process, and only miners belonging to a certain group are permitted to mine the next block. The node’s mining group will be detemined by a hash function. The network can easily verify whether the node is in it correct mining group by comparing hash value of the previous block in the block header.

So with the proposed solution attacker can’t easily extend their chain of node to create a 51% attack as the mining group of each node is random.

### 6. A new key protocol design for cryptocurrency wallet (Length: 6)

Soonhwa Sung.

### 7. Privacy and Security Analysis of Cryptocurrency Mobile Applications (Length: 6)

Ashish Rajendra Sai, Jim Buckley, Andrew Le Gear.

### 8. Multiple Layered Security Analyses Method for Cryptocurrency Exchange Servicers (Length: 3)

Hironao Takahashi, Uzair Lakhani.

## b. Analysis of the paper

### 1. Blockchain

#### 1.1. Bitcoin: A Peer-to-Peer Electronic Cash System

#### 1.2. Security of Cryptocurrencies in blockchain technology: State-of-art, challenges and future prospects

#### 1.3. BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network

### 2. 51% Attack

#### 2.1. Analysis of Security in Blockchain: Case Study in 51%-Attack Detecting

#### 2.2. Random Mining Group Selection to Prevent 51% Attacks on Bitcoin

#### 2.3. A new key protocol design for cryptocurrency wallet

### 3. Security of mobile device using CC

#### 3.1. Privacy and Security Analysis of Cryptocurrency Mobile Applications

#### 3.2. Multiple Layered Security Analyses Method for Cryptocurrency Exchange Servicers

# III. Conclusion

# IV. Citation

**Version control and archival site**

[taiyounari/NetworkSecurityEssay: Network security course project (github.com)](https://github.com/taiyounari/NetworkSecurityEssay)

**Used material**

*Website articles and blogs*

[W1] [Global Cryptocurrency Ownership Data 2021 - TripleA (triple-a.io)](https://triple-a.io/crypto-ownership/)

[W2] [Cybersecurity in Cryptocurrency: Risks to Be Considered - DATAVERSITY](https://www.dataversity.net/cybersecurity-in-cryptocurrency-risks-to-be-considered/)

[W3] [Cryptocurrency Definition](https://www.investopedia.com/terms/c/cryptocurrency.asp)

[W4] [Bitcoin Definition](https://www.investopedia.com/terms/b/bitcoin.asp)

[W5] [The Difference Between Centralized and Decentralized Networks | N-able](https://www.n-able.com/blog/centralized-vs-decentralized-network#:~:text=What%20is%20a%20decentralized%20network,on%20a%20single%20central%20server.)

[W6] [51% Attack Definition](https://www.investopedia.com/terms/1/51-attack.asp)

[W7] [Once hailed as unhackable, blockchains are now getting hacked | MIT Technology Review](https://www.technologyreview.com/2019/02/19/239592/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/)

[W8] [Crypto Terms You Should Know If You Want to Invest | NextAdvisor with TIME](https://time.com/nextadvisor/investing/cryptocurrency/crypto-terms-you-should-know-before-investing/)

[W9] [Hash Power / Hash Rate | Alexandria (coinmarketcap.com)](https://coinmarketcap.com/alexandria/glossary/hash-power-hash-rate#:~:text=Hash%20power%2C%20or%20hash%20rate,mining%20rig%20on%20that%20network.&text=The%20hash%20rate%20of%20a,it%20can%20calculate%20per%20second.)

[W10] [Cryptocurrency Public Ledger Defined (investopedia.com)](https://www.investopedia.com/tech/what-cryptocurrency-public-ledger/#:~:text=The%20public%20ledger%20is%20used,transactions%20executed%20between%20network%20participants.)

*Papers and journals*

[P1] [Bitcoin: A Peer-to-Peer Electronic Cash System](https://bitcoin.org/bitcoin.pdf)

Satoshi Nakamoto

[P2] [Security of Cryptocurrencies in blockchain technology: State-of-art, challenges and future prospects](https://www.sciencedirect.com/science/article/abs/pii/S1084804520301090)

Arunima Ghosh, Shashank Gupta , Amit Dua , Neeraj Kumar

[P3] [BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network](https://www.sciencedirect.com/science/article/abs/pii/S1084804519302243)

Shailendra Rathore, Byung Wook Kwon, Jong Hyuk Park

[P4] [Analysis of Security in Blockchain: Case Study in 51%-Attack Detecting](https://ieeexplore.ieee.org/document/8563187)

Congcong Ye, Guoqiang Li , Hongming cai, Yonggen Gu, Akira Fukuda

[P5] [Random Mining Group Selection to Prevent 51% Attacks on Bitcoin](https://ieeexplore.ieee.org/document/8416225)

Jaewon Bae, Hyuk Lim

[P6] [A new key protocol design for cryptocurrency wallet](https://www.sciencedirect.com/science/article/pii/S2405959521000904)

Soonhwa Sung

[P7] [Privacy and Security Analysis of Cryptocurrency Mobile Applications](https://ieeexplore.ieee.org/document/8686583)

Ashish Rajendra Sai, Jim Buckley, Andrew Le Gear

[P8] [Multiple Layered Security Analyses Method for Cryptocurrency Exchange Servicers](https://ieeexplore.ieee.org/document/9015245/)

Shailendra Rathore, Byung Wook Kwon, Jong Hyuk Park