**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**.  
Nowadays, 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](#_Toc92487445)

[I. Introduction: What is cryptocurrency and blockchain 2](#_Toc92487446)

[a. Some terminology 2](#_Toc92487447)

[b. 2](#_Toc92487448)

[II. Current state of art 3](#_Toc92487449)

[a. Some more terminology used in this section 3](#_Toc92487450)

[b. Literature review 4](#_Toc92487451)

[1. Bitcoin: A Peer-to-Peer Electronic Cash System (Length: 9) 4](#_Toc92487452)

[2. Security of Cryptocurrencies in blockchain technology: State-of-art, challenges and future prospects (Length: 35) 4](#_Toc92487453)

[3. BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network (Length: 11) 5](#_Toc92487454)

[4. Analysis of Security in Blockchain: Case Study in 51%-Attack Detecting (Length: 10) 6](#_Toc92487455)

[5. Random Mining Group Selection to Prevent 51% Attacks on Bitcoin (Length: 2) 7](#_Toc92487456)

[6. A new key protocol design for cryptocurrency wallet (Length: 6) 7](#_Toc92487457)

[7. Privacy and Security Analysis of Cryptocurrency Mobile Applications (Length: 6) 8](#_Toc92487458)

[8. Multiple Layered Security Analyses Method for Cryptocurrency Exchange Servicers (Length: 3) 8](#_Toc92487459)

[b. Analysis of the paper 9](#_Toc92487460)

[1. Blockchain 9](#_Toc92487461)

[2. 51% Attack 9](#_Toc92487462)

[3. Security of mobile device using CC 9](#_Toc92487463)

[III. Conclusion 0](#_Toc92487464)

[IV. Citation 0](#_Toc92487465)

# 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 (semi-)anonymous form, as well as their respective bitcoin balances and a log of all real network transactions[W10].

#### Peer-to-peer

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

#### Cryptocurrency wallet

A wallet where one can keep their cryptocurrency.

#### 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.

#### Double-spend

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

## b. What is cryptocurrencies and how it started

Cryptocurrencies are a digital currency that utilize various cryptographic methods and algorithms like public-private 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 to 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 earlier while the first concept of blockchain worked on by Stuart Haber and Scot Stornetta started in 1991. DigiCash declare bankruptcy 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 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 worth 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 significant amount of effort required to modify transactions record however has make it attractive to criminal. The victim simply cannot ask for a redo of transactions like traditional bank if they got the wallet stolen and they most certainly can’t do that themselves. The thieves can remains anonymous even if all transactions are public, the wallet address simply contain no information, make it impossible to trace the attacker. The number of fraudulent transactions or hacking the system has raised even more as it got more popular. Nowadays attacks with damage up to hundreds 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 committed by a lone wolf or an entire cybercrime organization behind it. It is speculated 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. Some more terminology used in this section

#### 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.

#### 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.

#### Hashpower

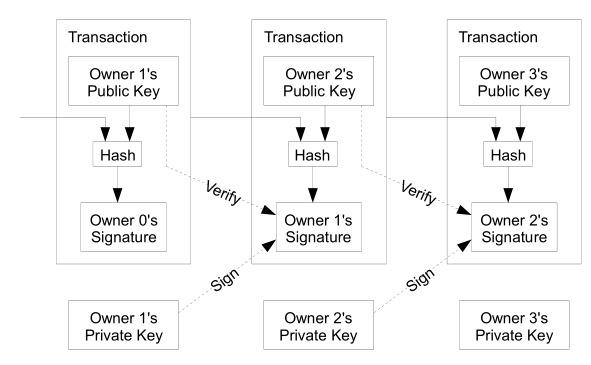
Hash power, or hash rate, are interchangeable terms used to describe the combined computational power of a specific cryptocurrency network or the power of an individual mining rig on that network[W9].

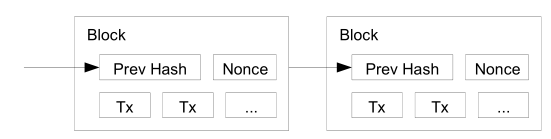
#### 51% Attack

A situation where more over half of the network's mining hash rate is controlled by a small handful of miners. 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].

## b. 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 network 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.

To prevent illusory transactions from being put into the network, he use a proof-of-work system. It attaches 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.

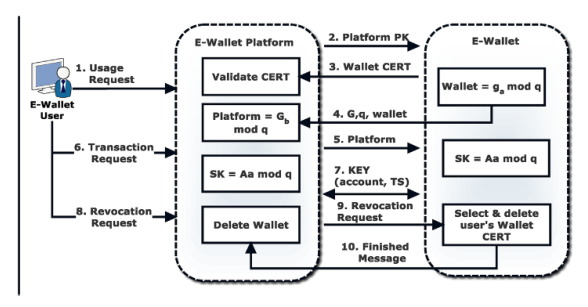
There are incentive to participate in a honest way as the miner get certain amount of bitcoin back as an award for processing the transactions of other users. And if attackers has enough hash power to overpower the network they would have to choose whether if they got more profit from just play by the rule and get coins or by making defrauded transactions to steal coins. The former ought to be more profitable though as the chance to successfully perform a 51%-Attack is slim.

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

In this document [2] by the team of researcher, Arunima Ghosh, Shashank Gupta, Amit Dua, Neeraj Kumar, they analyzed the overall structure of blockchain

On analysis blockchain, they listed several advantage of it. While blockchain has a decentralized nature, it isn’t prone to single point of failure unlike public key infrastructure (PKI) so it is Byzantine fault tolerant. It also has a good persistency as authentication of transaction is very fast with good accuracy. Users has good auditability as every records of every user is immutable can be easily traced while user still retain semi anonymity as the wallet of each user doesn’t contain any identifiable information. But there are some issue of it as while there still isn’t an efficient way of hacking blockchain network as it is very robust, people still reported damaged from attack ranging from service interruptions to thievery of confidential information and valued assets. However the number of case is relatively low compare to it scale and they concluded that with decentralization, persistency, privacy and auditability features, blockchain can be applied to enhance more conventional IT field.

Bitcoin has combined blockchain and cloud computing technology to create a complex security protocol and avoid.



The authors had investigated some of the existing security challenges of blockchain systems like 51% Attack and type of attack that can be called a subdivision of it like Selfish mine attack,

They also discuss some of the vulnerability that crypto currency has. Notably Double-spending attack, in bitcoin

To combat the attacks, the authors listed several enhancement technique to security that has been used recently to the blockchain network of newer cryptocurrency. First is SmartPool,\_\_ makes use of a data structure that has the ability to avoid the adversary from submitting the shares in various batches. Moreover, the authentication methodology of SmartPool assures that legitimate miners will get anticipated incentives even if dishonest miners are present in the poo

Next is quantitative framework with focus on the PoW

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

Shailendra Rathore, Byung Wook Kwon, Jong Hyuk Park

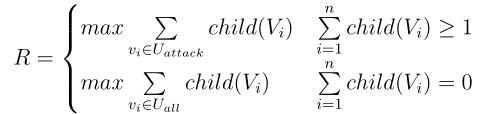
This paper discuss about how blockchain can improve existing flaw of decentralized network architecture. While it isn’t about crypto currency it can give us some insight in the blockchain

In this study, we proposed a decentralized security architecture that detects and mitigates security attacks in the IoT ecosystem. The proposed architecture has made three new contributions in the area of IoT security. First, the proposed architecture uses SDN to continuously monitor and analyze traffic data in the entire IoT ecosystem, thus mitigating the issue of data unavailability in security detection and providing optimal security defense. Second, the architecture employs the Blockchain technology which supports decentralized attack detection to overcome the single point of failure problem inherent to the centralized and distributed architectures. Finally, the architecture relies on the layered structure, where attacks are detected at the fog node and subsequently mitigated at the edge node, which contributes to shortening the time taken to detect and mitigate attacks. The results of our evaluation demonstrate that the proposed decentralized security architecture outperforms the centralized and distributed architectures and takes less time to mitigate attacks in the IoT ecosystem. Our findings also suggest that the architecture could be deployed with the IoT ecosystem as a security detection component that detects and mitigates potential attacks by monitoring and analyzing the traffic data of the entire IoT ecosystem.

### 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 have stimulated a 51%-Attacks to evaluate the security of blockchain. \_\_ Attacker will be represented as the miner that try to create illusory transactions and know whether the other block is also an illusory one so they can choose to connect to the most suitable one with the following strategy:

With *R* represents the most suitable block, *Vi* represents block *i* in attacking collection or in the whole blockchain and the *child()* function return the number of child nodes *Vi* has.

So if no attacking nodes are present on the blockchain, the attackers will choose the longest chain. Otherwise, attackers will pick the chain in which the attacking node connects to the most nodes.

Researchers found of that if there are more than 6 blocks connect to a block, the block can’t be changed in a real condition as \_\_ so if 6 of them are connected to an illusory one the attack is success

Honest miner on the other hand don’t know whether a node is fraud or not so the honest node will default the transactions in the longest chain is correct as usual.

with honest state and attack state in different condition.

The relation between In this work, we propose a tree-structure method to simulate the process of blockchain and analyze he relationship between attacking number and state number in order to evaluate the security of each state. This method is generic and concise, and any attack in blockchain can use this method to analyze their influence by changing the attacking strategy. In this paper, we apply 51%-Attack strategy to simulate the attackers’ behavior and obtain the change trend of state number and attacking number. After getting these data, we can evaluate the security of each state in blockchain.

### 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 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 determined 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 and thus reduce the chance of a 51% attack.

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

Soonhwa Sung.

The majority of hacking accidents in cryptocurrency occur when the information of a cryptocurrency wallet is stolen. Since the cryptocurrency wallet is simply used for a key storage, when connecting to a transaction network, it is vulnerable for a key theft. Blockchain is not traceable, but it should communicate to applicate data of blockchain. To communicate to applicate data of blockchain, this study proposes a key protocol design to secure cryptocurrency transactions for user privacy of cryptocurrency to resolve the drawback of decentralized exchange

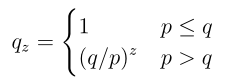
The paper proposes a new blockchain key that is able to tolerate the Byzantine faults and can be used to work correctly in an asynchronous system such as the Internet. Most hacking-related cryptocurrency incidents occur when the information of the wallet is stolen. The cryptocurrency wallet does not store the currency, but the key that has access to the account does. Thus, the study suggests the key protocol that can prevent the wallet information theft by the session key agreement instead of the key storage in a wallet. This multilateral protocol is processed by the session key authentication that uses the key sessions and by the cluster key in a peer that works multiparty computations by utilizing the FBA based on blockchain technology. The key protocol plays a major role in the cryptocurrency wallet and it uses the forward security session key and the FBA of the blockchain. The keys prevent the collusion between the miners and the data receivers who use the blockchain. The protocol ultimately does not violate the forward security. Additionally, it protects the users’ privacy because of a key agreement. Currently, many investors are concerned with cryptocurrency, but they worry about its security because it goes through decentralized exchange of blockchain market. Without decentralized exchange, the proposed protocol is processed by the session key authentication that uses the key sessions and by the cluster key in a peer that works multiparty computations by utilizing the FBA based on blockchain technology. Blockchain is not traceable, but it should communicate to applicate data of blockchain. To communicate to applicate data of blockchain, this study proposes a key protocol for user privacy of cryptocurrency to resolve the drawback of decentralized exchange. It may be played an important role in the cryptocurrency hacking accident and supported robust cryptocurrency market. The study is also scalable to other areas using secure distributed networks.

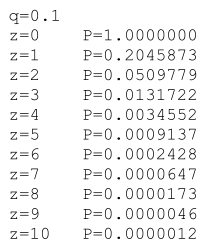
## c. Analysis of the paper

### 1. Blockchain

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

Statistically, Satoshi Nakamoto calculated in theory the rate in which an attack can catch up with the honest chain is

 With *p* represent the probability that the honest node find the new block first, *q* represent the probability that the attackers find them faster than the honest node and *qz*is the probability that the attacker catch up the honest node chain when *z* block behind.

S

#### 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

# III. Conclusion

So in this paper we can conclude that

# IV. References

**Version control and archival site**

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

**Used material (Click to open the link)**

*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](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](https://time.com/nextadvisor/investing/cryptocurrency/crypto-terms-you-should-know-before-investing/)

[W9] [Hash Power / Hash Rate](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](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