**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 of many 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 3](#_Toc92400117)

[I. Introduction: What is cryptocurrency and blockchain 4](#_Toc92400118)

[II. Current state of art 5](#_Toc92400119)

[a. Literature review 5](#_Toc92400120)

[1. Bitcoin: A Peer-to-Peer Electronic Cash System (Length: 9) 5](#_Toc92400121)

[2. Security of Cryptocurrencies in blockchain technology: State-of-art, challenges and future prospects (Length: 35) 6](#_Toc92400122)

[3. BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network (Length: 11) 6](#_Toc92400123)

[4. Analysis of Security in Blockchain: Case Study in 51%-Attack Detecting (Length: 10) 6](#_Toc92400124)

[5. Random Mining Group Selection to Prevent 51% Attacks on Bitcoin (Length: 2) 6](#_Toc92400125)

[6. A new key protocol design for cryptocurrency wallet (Length: 6) 6](#_Toc92400126)

[7. Privacy and Security Analysis of Cryptocurrency Mobile Applications (Length: 6) 6](#_Toc92400127)

[8. Multiple Layered Security Analyses Method for Cryptocurrency Exchange Servicers (Length: 3) 6](#_Toc92400128)

[b. 6](#_Toc92400129)

[III. Analyzing 6](#_Toc92400130)

[IV. Conclusion 7](#_Toc92400131)

[V. Citation 7](#_Toc92400132)

# I. Introduction: What is cryptocurrency and blockchain

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, a process that using CPUs to solve various mathematical puzzles that basically the processing of transactions and the miner will be compensated an amount of cryptocurrency.

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 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 networks (a decentralized network **architecture distributes workloads among several machines**, instead of relying on a single central server [W5]) with transaction recorded with blockchain technology.

Bitcoin were made available to the public in the later year: 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. There is estimated to be 300 million cryptocurrency users worldwide, there are 18,000 businesses and brands that accept cryptocurrency as payments

\_

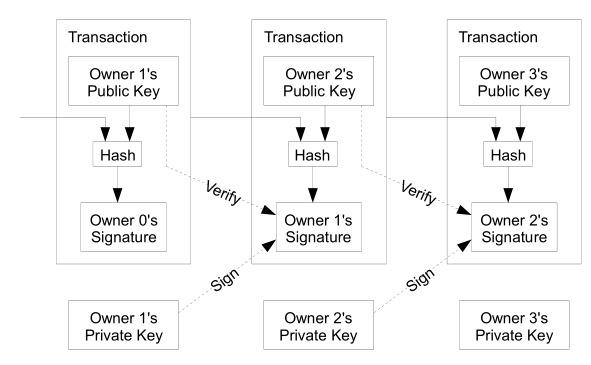
In these day bitcoin attack with damage up to hundred of million dollar happen quite common, they can also happen in smaller scale of course but in total they has added up to $1.93 billion. A majority of attack occur when the information of a cryptocurrency wallet is stolen, as it simply used as a key storage so when connected to a decentralized network, it is vulnerable to key theft. Though some time it happen through a hacked cryptocurrency trading platform. It they can happen when attacker put malicious script into the UI of the sites by exploiting existing vulnerability of website components. By that or phishing hackers can access to user information and token and even can bypass two-factor authentication. An attack like this has stolen $78 million dollar once. There is also the 51% attack that is basically when a majority of a blockchain network is controlled by a certain group of people,\_\_ The number of Fraudulent transactions or hacking the system has rised even more as it got more popular.

# 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, as aforemention he 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 security measurement

Double-spending is simply a certain amount of digital currency can be spent at least more than two as the asset get duplicated. But with the blockchain model, the newly created transaction node has to be verified by other nodes in the network. With the proof-of-work system,\_\_

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. Otherwise it will fail.

The

Depend on a honest host, that mean a node that used by CPU mining most, the strong honest host prevent

attacker attempt to modify a past block, as in how blockchain work, they have to also redo the previous proof of work block and catch up with the honest block,

Giving incentive to play fair so it reduce number of attack as the attacker decide whether to play fair or continue greedy if he has a rig that strong enough to bypass the pow

As mentioned to overpower

Against other type of attack like trying to take down the network, it’s impossible

### 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

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

Shailendra Rathore, Byung Wook Kwon, Jong Hyuk Park

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

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

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

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

### 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.

# III. Analyzing

# IV. Conclusion

# V. 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 (investopedia.com)](https://www.investopedia.com/terms/c/cryptocurrency.asp)

[W3] [Bitcoin Definition (investopedia.com)](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 (investopedia.com)](https://www.investopedia.com/terms/1/51-attack.asp)

*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