**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.

1. *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 very trendy recently. As of now, the crypto market cap is currently sitting at $2.6 trillion and there is estimated to be 300 million cryptocurrency users worldwide, there are 18,000 businesses and brands that accept cryptocurrency as payments. So the cryptography market indeed looks lucrative but however, it had drawed tons of attention from malicious users who attempts to hack and steal one’s cryptocurrency wallets. So concern for security of these cryptocurrency had been a really hot topic. 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

# Table of Contents

[Table of Contents 3](#_Toc92294615)

[I. Introduction: What is cryptocurrency and blockchain 4](#_Toc92294616)

[II. Current state of art 4](#_Toc92294617)

[a. literature review 4](#_Toc92294618)

[1. Bitcoin: A Peer-to-Peer Electronic Cash System 4](#_Toc92294619)

[2. Security of Cryptocurrencies in blockchain technology: State-of-art, challenges and future prospects 4](#_Toc92294620)

[III. Discussing 4](#_Toc92294621)

# 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 “mine” them or buying them in various cryptocurrency trading platform. 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. Anyway, 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[W3]. 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 [W4]) with transaction recorded with blockchain technology. Bitcoin were made available to the public in 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.\_

\_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. According to dataversity.com,[W2] at least 33% bitcoin trading sites have already been hacked, and nearly $1.7 billion in cryptocurrency has been stolen from these attack. 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. A little sidetracked as this literature focus on the defense mechanism of blockchain against attack with-in the network.

# Current state of art

## a. Literature review

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

In this paper 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

The security measurement

A major part of bitcoin: Proof-of-work

scan a value that hashed by SHA-256

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

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

### 3.

## b.

# III. Discussing

**Version control and archival site**

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

**Used material**

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

[W4] [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.)

*Papers and journals*

[P1] Bitcoin: A Peer-to-Peer Electronic Cash System

[P2] Security of Cryptocurrencies in blockchain technology: State-of-art, challenges and future prospects

[P3]