Cover sheet for submission of work for assessment

UNIT DETAILS

Unit name	Network Security			Class day/time		Office use only
Unit code	INT3307_20	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)
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 authorized 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. Plagiarized 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

ASSIGNMENT 1
SECURITY IN BLOCKCHAIN-BASED CRYPTOCURRENCY

NAME: NGUYEN TRUNG HIEU, BIRTHDATE: 16/04/2001

STUDENT ID: 19021271, EMAIL: 19021271@VNU.EDU.VN

SUMMITED IN 10/01/2022 DUE DATE: 10/01/2022

UNIVERSITY OF ENGINEERING AND TECHNOLOGY

Abstract

Nowadays, most of us have heard of at least one cryptocurrency's name, since these blockchain-based virtual currency usage has been in circulation for the last twelve years and has recently been highly popular. As of now, the crypto market cap is currently sitting at $2.6 trillion. So, while the cryptography market appears to be lucrative, it has attracted a lot of malicious users who are attempting to hack and steal these. As a result, the majority of those who participate in the market are concerned about the security of these cryptocurrencies. This research will delve into how the use of blockchain technology affects cryptocurrency security and a number of protection mechanisms against attacks.

Table of Contents

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 hashing function and public-private key pairs to encrypt transactions between users, hence the “crypto” part of 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*.

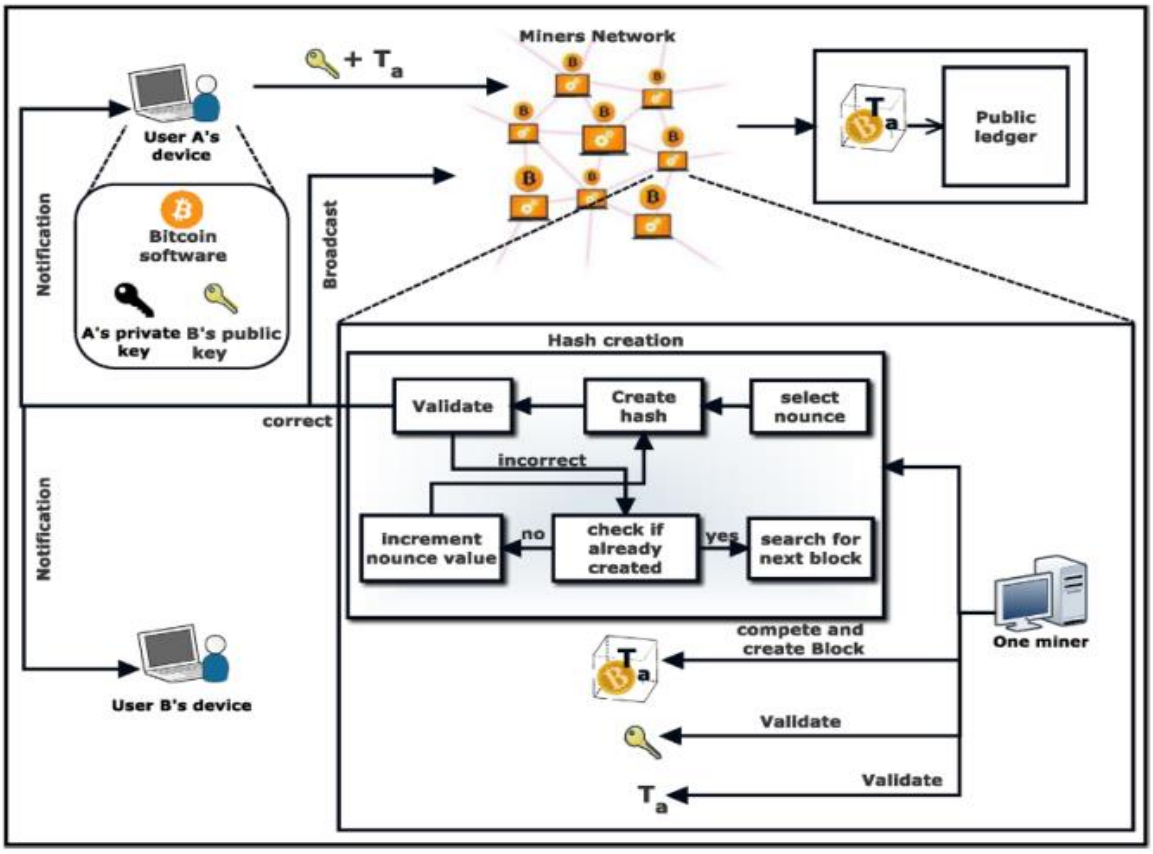


Figure 1: Life cycle of transaction in a bitcoin network [P2]

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 sky-high 46,412.50 USD, 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].

As a result, substantial research and analyses into the present security measures of blockchain-based crypto currency have been conducted. I'm writing this essay because I'm fascinated by cryptocurrency and want to learn more about it. The following literature analysis will concentrate on cryptocurrency network attack.

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]. It related to double-spending attack.

b. Literature review

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

In this paper [P1] 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. Transaction then stored in a Merkle tree data structure with auto-pruning of branches to efficiency store data.

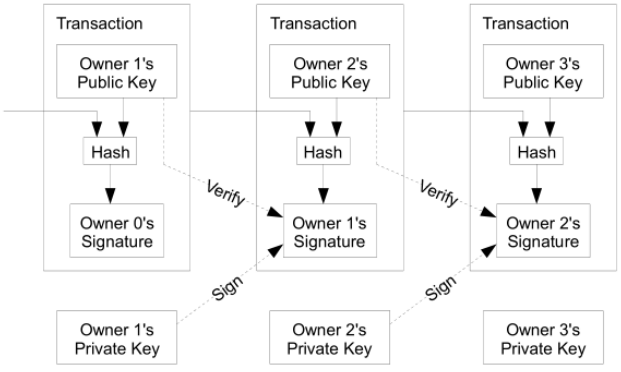


Figure 2: Transaction Structure [P1]

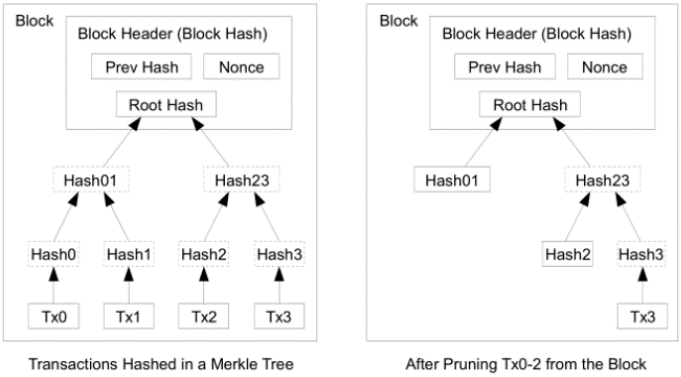


Figure 3: Merkle tree [P1]

To prevent nefarious transactions from being put into the network, he propose a proof-of-work system. It use SHA-256 to create a hash value to attaches 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. In a nut shell attacker have to alter an entire chain to modify a single transactions.

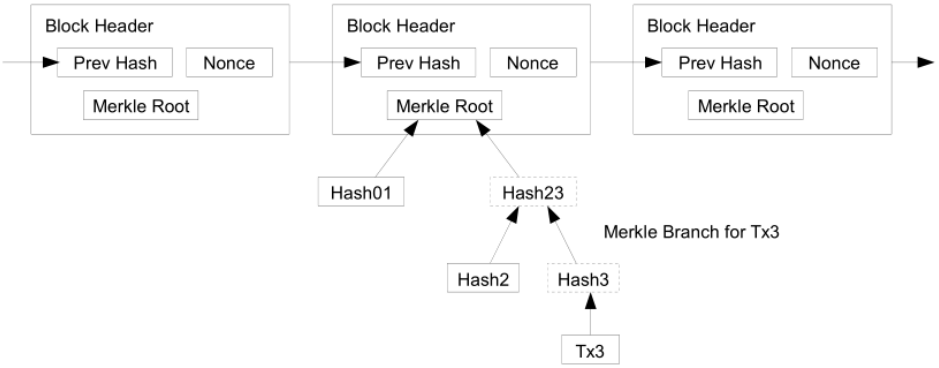


Figure 4: A proof-of-work chain [P1]

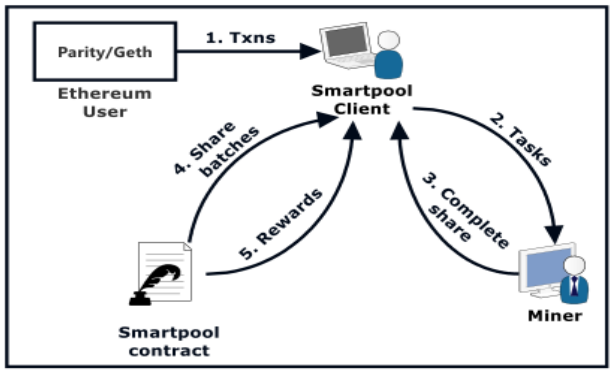
There are incentive to participate in a honest way as the miner get certain amount of bitcoin back as an award for processing the transactions of other users. And if attackers has enough hash power to overpower the network they would have to choose whether if they got more profit from just play by the 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 very slim.

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

In this document [P2] by the team of researcher, Arunima Ghosh, Shashank Gupta, Amit Dua, Neeraj Kumar, they analyzed the overall structure of blockchain as they listed several features 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.

The document also mentioned smart contracts that have been employed in a variety of new Blockchain types, with Ethereum being the first to do so. They essentially are programs that run when certain criteria are satisfied and are maintained on a blockchain. They are executed when miners mining blocks though they aren't restricted to only cryptocurrency nowadays as they are attached to blockchain technology.

Nevertheless, there are still a number of vulnerabilities of blockchain, such as 51%-Attack, Data malleability or various traditional security breaching categories like DDos, private account hacking… To combat the attacks, the authors mentioned a number of security enhancement techniques that have lately been used by the blockchain network of newer cryptocurrency.



First is SmartPool, used by Ethereum, makes use of a data structure called *augmented Merkle tree* 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 pool.

Figure 5: Process of smart pool [P2]

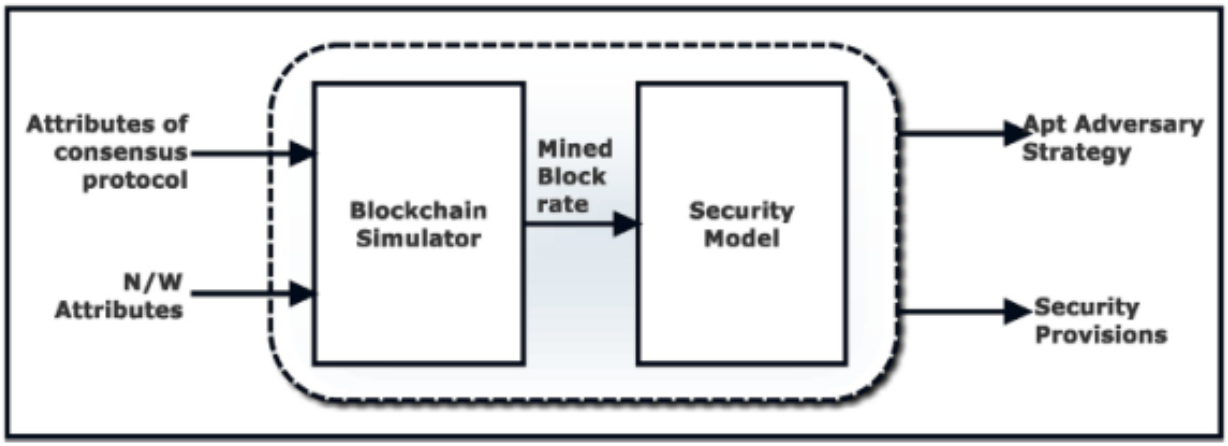
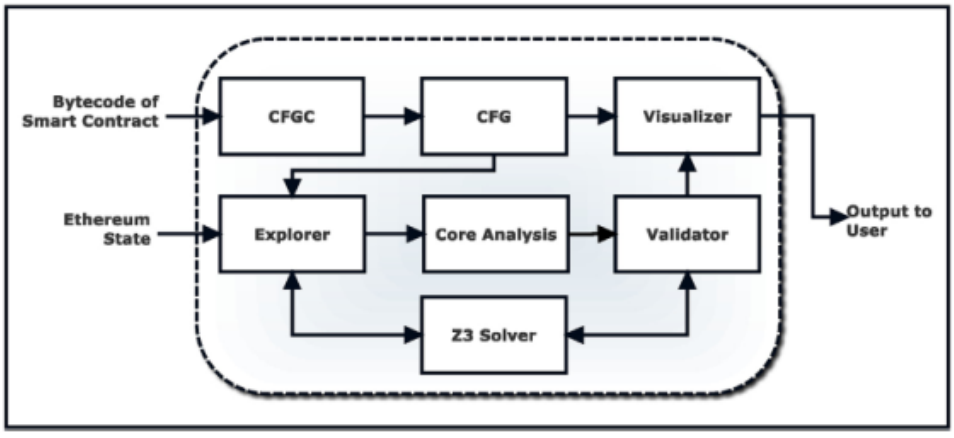


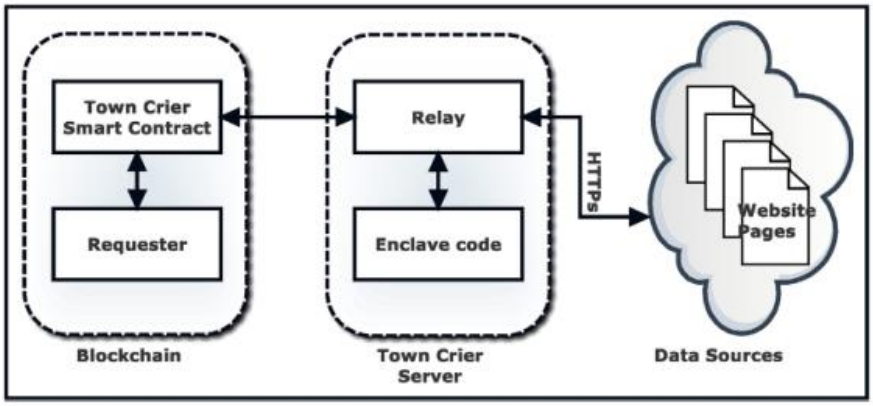
Figure 6: An overview of quantitative framework [P2]

Second is *quantitative framework* with focus on the proof of work system. It run a stimulator and the data from the stimulation will be analyzed to assess the blockchain's performance.



Third Oyente, it is an additional process that run with smart contracts to detect faults in implementation of smart contracts. The figure 7 show the structural design and execution of it.

Figure 7: Structural design and execution of Oyente[P2]



Finally Town Crier, serves as a link between smart contracts and current web sites that are already widely trusted for non-blockchain applications. It uses a blockchain front end and a trusted hardware back end to scrape HTTPS-enabled websites and provide source-authenticated data to re- lying smart contracts [P8].

Figure 8: Overview and working of Town Crier[P2]

The list doesn't stop here though, many more techniques are being developed now and we will see them in the future. We can expect the blockchain technology to be even more secure.

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

In this paper [P3] , Shailendra Rathorea, Byung Wook Kwon, Jong Hyuk Park had discuss about how blockchain can improve existing flaw of decentralized network architecture. While it isn't about cryptocurrency it can give us some insight in the blockchain. They proposed a decentralized security architecture for the IoT ecosystem that detects and mitigates security attacks. Three new contributions to IoT security have been made by the proposed architecture. First, the proposed architecture employs software defined to continuously monitor and analyze traffic data across the entire IoT ecosystem, addressing the issue of data unavailability in security detection and ensuring the best possible security defense. Second, the architecture makes use of Blockchain technology, which allows for decentralized attack detection and thus avoids the single point of failure problem that centralized and distributed architectures have. Finally, the architecture employs a layered structure, in which attacks are detected at the fog node and then mitigated at the edge node, reducing the time it takes to detect and mitigate attacks.

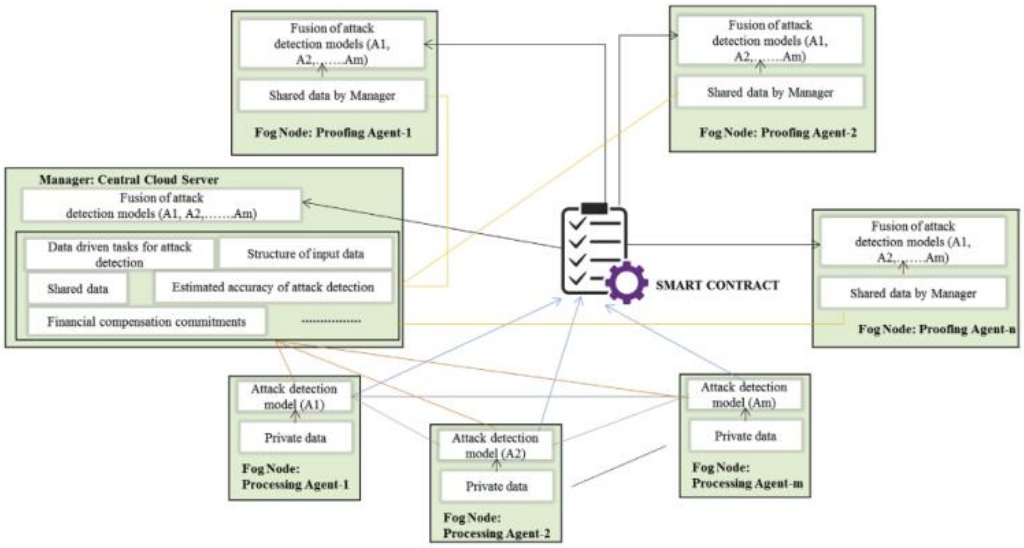


Figure 9: Work flow of the blockchain in the proposed architecture.[P3]

According to their findings, the proposed decentralized security architecture outperforms centralized and distributed security architectures and takes less time to mitigate attacks in the IoT ecosystem. Their findings also suggest that the architecture could be used with the IoT ecosystem as a security detection component that monitors and analyzes the entire IoT ecosystem's traffic data to detect and mitigate potential attacks.

So if the blockchain network is monitored, we can create a system that send alert message of the attack to all hosts quickly, therefore mitigate as many loss as possible.

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

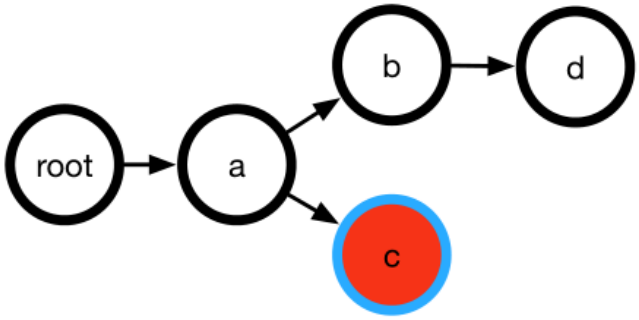


Figure 10: Attacker's strategy.[P4]

In the paper [P4] by Congcong Ye, Guoqiang Li, Hongming Cai, Yonggen Gu, Akira Fukuda, they propose a tree-structure method to simulate the blockchain process and analyze the relationship between attacking number and state number in order to assess the security of each state in this paper. They have used the 51%-Attack strategy to simulate attacker behavior and determine the state number and attacking number change trends. Afterward when the data can be extracted, the security of each state in the blockchain can be assessed. The following algorithms is the pseudo-code.

```
Algorithm 1 Obtain all state of simulation
process about blockchain
Input: The attacking power P
Output: All state of blockchain S
1: Initialize a blockchain with a honest node R
2: Create a new block based on network's
attacking power;
3: repeat
4:      create new block based on power of
        attacking P;
5:      if new block is honest one then
6:              Algorithm 2;
7:      else
8:              Choose the longest chain which
                will make attacking block safer.
9:      end if
10:     Reconstruct a new tree by connect new
        block to the chosen node;
11:     if the state of new tree is different
        from the state in S then
12:             Join the new state into S
13:     end if
14:     if the new tree reaches security state or
        attacking state then
15:             Initialize a blockchain with a
                honest node
16:     end if
17: until the state number of blockchain S
converges
18: return all state of simulation process
```

```
Algorithm 2 How to choose one node the new
honest node will connect
Input: The root of the blockchain P
Output: One node that new honest node will
connect S
1: Calculate the depth of a tree L
2: for every layer i=0 to n do
3:      for every node j=0 to m do
4:              Add weight of every node
5:       end for
6: end for
7: Choose one node based on the probability P
that was calculated above
8: return node S
```

They believe with the stimulation can create a more generic tool to detect the condition of blockchain and alert users that they may have to wait a long time to accept transactions, thereby improving blockchain security.

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

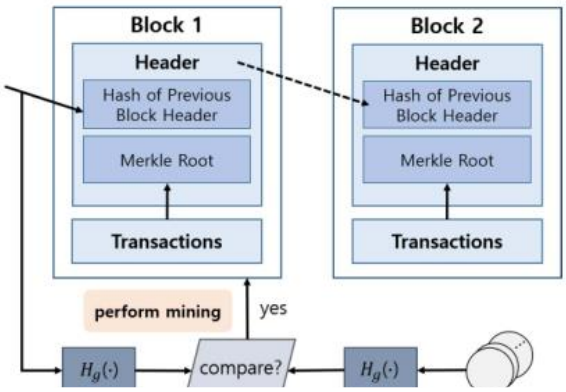


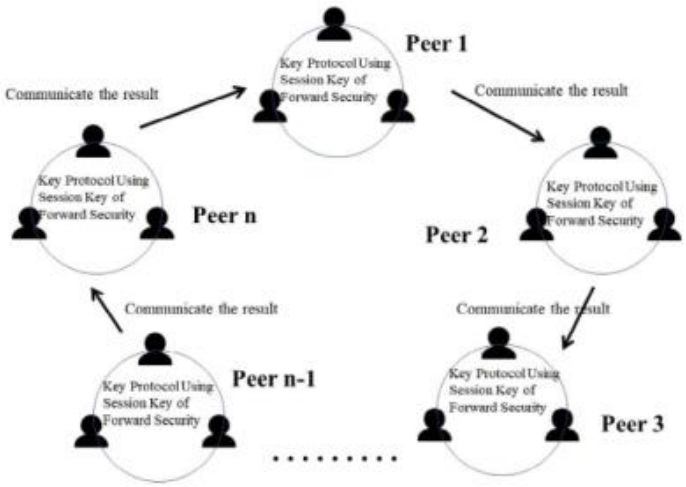
Figure 11: Schematic of a random mining group selection.[P5]

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 [P5] 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)



The bulk of cryptocurrency hacking incidents occur when a cryptocurrency wallet's information is stolen. When connecting to a transaction network, the cryptocurrency wallet is vulnerable to key theft because it is utilized for key storage. While the cash is not stored in the cryptocurrency wallet, the key that grants access to the account is. Soonhwa Sung's study [P6] proposes a key protocol that uses a session key agreement rather than key storage in a wallet to prevent wallet information theft.

This protocol is processed by the session key authentication, which uses key sessions, and the cluster key in a peer. A peer is made up of several parties, each of which has at least three members. For valid users, each peer must proceed with the key protocol using a session key depending on the forward security. Then the key uses the Federated Byzantine Agreement (FBA), requiring nodes to be known and verified before being allowed to perform transactions, based on blockchain technology to perform multiparty calculations. The keys also are used to prevent collusion between miners and data recipients on the blockchain.

c. Analysis on security of various defense mechanisms

The average CPU's processing power has increased as technology has progressed. People have even deduced which type and brand of CPU is best for cryptocurrency mining. Nothing prevents an attacker from obtaining the same CPU. And, as history has shown, someone will always find a way to defeat a complex security algorithm when given the opportunity. So cryptocurrency was not created with the intention of minimize the number of attack as much as possible, shown in the whitepaper [P1] as Satoshi Nakamoto calculated in theory the rate in which an attack can catch up with the honest chain in a proof-of-work system

$$q_z = \begin{cases} 1 & p \leq q \\ (q/p)^z & p > q \end{cases}$$

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 so p + q = 1. q_z is the probability that the attacker catch up the honest node chain when *z* block behind.

So if p > q, as the number of blocks the attacker has to catch up with grows, the probability decreases exponentially. With the odds stacked against him his chances of catching up quickly dwindle. Otherwise the attacker is guaranteed to success.

For the possibility that the attacker will be able to catch up now, they have provide an equation:

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \begin{cases} (q/p)^{(z-k)} & if\ k \leq z \\ 1 & if\ k > z \end{cases}$$

With $\lambda = z\frac{q}{p}$ as the expected value of the Poisson distribution.

In statistic, a Poisson distribution is a probability distribution that depicts the number of times an event is expected to occur over a given time period. To put it another way, it's a count distribution. Poisson distributions are frequently used to comprehend independent events that occur at a steady rate during a particular time frame. [W11] So the use of Poisson distribution fits here.

With some arrangement to prevent summing the distribution's infinite tail it became

$$1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \left(1 - (q/p)^{(z-k)}\right)$$

After the above equation converted into C

```
#include <math.h>
double AttackerSuccessProbability(double q, int z)
{
    double p = 1.0 - q;
    double lambda = z * (q / p);
    double sum = 1.0;
    int i, k;
    for (k = 0; k <= z; k++)
    {
        double poisson = exp(-lambda);
        for (i = 1; i <= k; i++)
            poisson *= lambda / i;
        sum -= poisson * (1 - pow(q / p, z - k));
    }
    return sum;
}
```

They ran the code with different probability of attacker mining faster than the honest nodes and the number of block behinds. This is the results:

When q = 0.1	
z	P
0	1.0000000
1	0.2045873
2	0.0509779
3	0.0131722
4	0.0034552
5	0.0009137
6	0.0002428
7	0.0000647
8	0.0000173

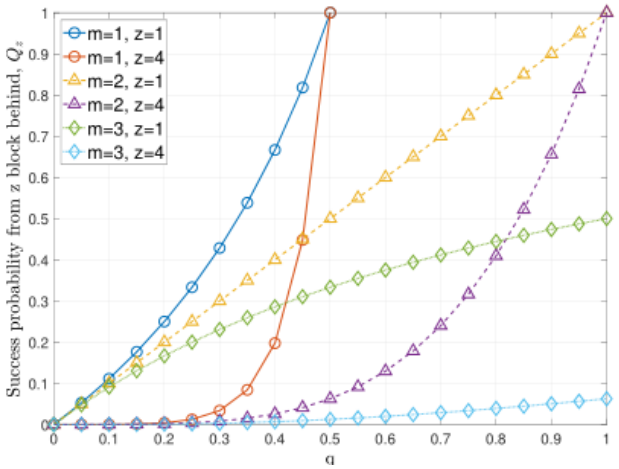
When q = 0.3	
Z	P
0	1.0000000
5	0.1773523
10	0.0416605
15	0.0101008
20	0.0024804
25	0.0006132
30	0.0001522
35	0.0000379
40	0.0000095

So with the chances are very stacked against the attacker, it provide an incentive to act honestly since it will be a waste of time and electricity for the attacker.

To furthermore secure the blockchain network, in [P5], the authors said that in (1) q is the ratio of the hash power of the attacker to the total hash power of N peers in the network (H). Assume that *m* groups have the same average number of users and the same average hash power, when random group selection is used q will be express as follow:

$$q\sim = \frac{1}{m} \cdot \frac{h}{h+(\frac{N}{m}-1)(\frac{H-h}{N-1})}$$

So with m ≥ 2, q~ cannot be greater than 50% as 1/m will less than or equal ½ and $\frac{h}{h+(\frac{N}{m}-1)(\frac{H-h}{N-1})}$ is always less than or equal to 1.



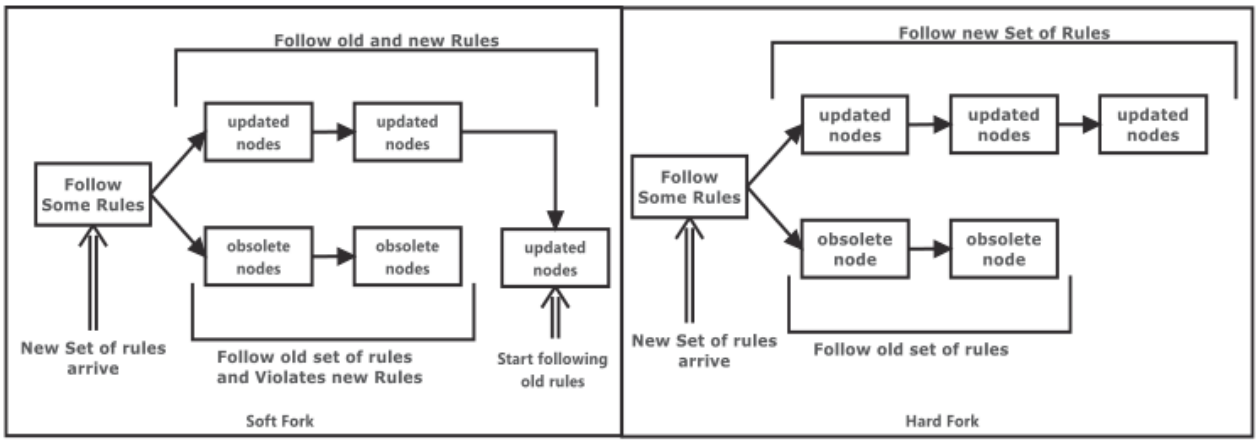
The graph from [P5] shows the probability of a successful double-spending attack. The graph was plotted into six group with z = 1 or 3 and m from 1 to 3. So when m equal 1 it is the case of a network not using the random selection group system. We can see that the attack is guaranteed to success when q slightly cross 0.5 or 50% of network hashpower no matter how many z behind.

However with just m = 2 we can see that the chance for a success attack greatly reduced even if they are only 1 block behind. To guarantee that the attack will be success attacker would need to have 100% control of the network, which obviously not happen because why would they have the need to attack their own network. So the proposed strategy can minimize the number of attacks even further.

Let us now look at some of the notable defense mechanisms that have already used mentioned in the paper [P2], *Security of Cryptocurrencies in blockchain technology: State-of-art, challenges and future prospects.*

Smart contract, according to the document [P9], are computer protocols that are designed to digitally expedite, verify, or enforce contract negotiation or performance. Financial services, prediction markets, and the Internet of Things are just a few of the uses for smart contracts.

But smart contracts come with a set of problems. First as more thing need to be calculated for each transaction, it reduce the capacity of the network as a whole. Second, because they are programs, they can include bugs. There was the infamous case of faulty execution of smart contract in Ethereum, DAO (Decentralized Autonomous Organization) hack. Users took advantage of a flaw in The DAO's code to divert one-third of The DAO's cash to a subsidiary account and $50 million dollar was lost. The attack had caused the coin to divides into two branches, one that use soft fork and the other use hard fork. In cryptocurrency, forks typically occur when one cryptocurrency is formed from the existing blockchain of another because of the demand from user. Soft fork allows miners that aren't follow the new rules to continue mining while hard fork doesn't. The following figure from [P2] shows the overview about the fork.



There also a comparison-based analysis table of two type of fork from [P2]. We can see how much rigorous hark fork is compared to soft fork.

Categories	Hard Fork	Soft Fork
Divergence type	Permanent divergence in the block chain	Temporary deviation in blockchain
Cause	The entities which are not upgraded are unable to validate the blocks constructed by the upgraded entities (obeying newer consensus protocols).	When non-upgraded nodes not following new consensus rules
Backward compatibility	Backward compatible.	Not backward compatible.
Parallelism of chains	The new as well as old blockchain execute parallelly, however both follow distinct set of protocols.	There are no parallel chains.
Funds	Brings up the issue of duel funds	No concept of duel funds
Implementation type	The new protocols which give rise to compatibility should be deployed in hard fork.	Most of the new features like check sequence verify or CSV or segregated witness are deployed by a soft fork because it is secure and more trivial.

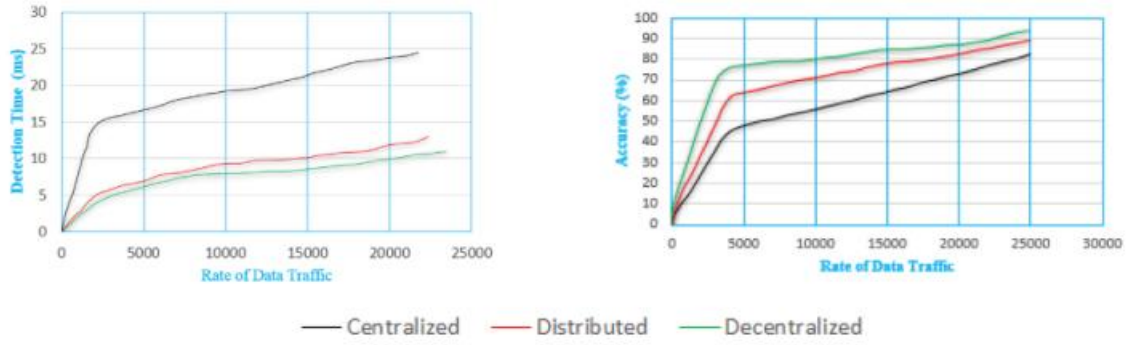
So forks are incredibly important in the bitcoin ecosystem since they are the means by which many new coins are generated or developed. As the cryptocurrency industry continues to grow and evolve, improvements for existing cryptocurrencies will be required, and many people will likely continue to generate new crypto coins through hard forks. After DAO attack and split of the Ethereum coin most people had opted to use the Ethereum version with hard fork for more security.

So after DAO attack, people have realized problem with smart contract and has proposed many technique to improve it such as SmartPool and Oyente. The following table from [P2] compare them.

Technique	Primary Focus	Key Elements used	Problem on which work is done	Deployment	Contributions	Shortcomings or challenges	Advantage
SmartPool (Loi et al. Luu et al., 2017)	Smart Contract	Introduce new data structure called augmented Merkle tree	In case one pool operator governs more than 50% of the mining power of the network, a 51% attack starts threatening the Nakamotoconsensus protocol's security	It is implemented on core network using a community Project which is crowd-funded	(1) A solution for distributed pool mining is introduced (2) Distributed pool miningprotocol is implemented as smart contract. (3) Ithas scalability and efficiency.	(1) A pool may contain many shares, therefore the contract many receive many messages. (2) In case feesfor submitingone share outweighs the incentive received, StrawmanPool cangive negative income to the mining nodes. (3) Any malicious user may witness transaction of other miners. (4) No guarantee is provided by the smart contract executing in the Bitcoin mining pool for Bitcoin payment	Decentralized, Efficiency, Secure
Oyente (Loi et al. Luu et al., 2016b)	Smart Contract	This requires two inputs-current global state of Ethereum and the bytecode of the contract.	Miners in Ethereum must follow few rules while taking part in the network, however the exists high probability of alterations of risk of not witnessing novice implementation		(1) It records many security bug classespresent in smart contracts of Ethereum. (2) It gives some solutions for the recorded bugs. (3) It gives Oyente, an virtual execution tool that helps smart contact of Ethereum for identifying bugs. (4) implements Oyente on Ethereum smart contracts as well as assures the attacks which is possible on real network of Ethereum.	5411 contracts have mishandledexceptions	(1)Bugs are Removed (2)open source

We can see that both still need many refinement. SmartPool had many inconveniences and vulnerabilities that can allow malicious user to exploit. Oyente had mishandled exceptions of 5411 contracts, according to [P7] these has taken account for 27.9% of the contracts.

The paper [P2] also mentioned that after the concept of Town Crier was put into action to improve smart contracts, many proposal for the use of artificial intelligence technique like neural network, machine learning, naïve Bayes… to create response to DDos attacks for blockchain network by using smart contract. The Town Crier server's major purpose is to acquire information requests from client contracts as well as information from targeted websites [P2]. So the faster the network the better. And according to statistic show below from paper [P3], after various experiment it conclude that decentralized blockchain networks response to attack faster than other architectures like centralized and distributed. So it's no doubt that blockchain has many potential for security improvement.



Attack mitigation time for different architectures.

Attack scenario	Architecture	Centralized	Distributed	Decentralized
TCP flooding		10s	7s	6s
ICMP flooding		11s	8s	7s
DDoS attack		14s	8s	5s

III. Conclusion

This study had looked into how the use of blockchain technology affects cryptocurrencies' security and a variety of security techniques as cryptocurrencies' use get more common. In the literature review, we had discovered that when blockchain was deployed in bitcoin, it already had several good measures in place to protect the blockchain network from assault. We also discovered how useful blockchain is in boosting cryptocurrency security. We also learn about several new types of security mechanisms that have been developed or are presently in use. From the original proof-of-work system we can enhance many aspect of it like smart contract for overall secureness of the network, stimulation of the blockchain network to assert the security of it, random mining group to reduce the chance of a 51%-Attack, and a new key protocol to prevent wallet key theft. Following that, we discussed and analyzed how effective these techniques in greater depth, and furthermore confirm that an attacker must expend significant effort to alter a single record in the blockchain network, making it impractical for the average hacker to attempt. We also focus on how faulty execution of security enhancement can also lead to costly attack. But anyway, I think that it still has many room for improvement and when combined with more advanced technology like artificial intelligence, the blockchain network can be more resilient against attacks.

IV. References

Version control and archival sites

Network security course project (github.com)

Used material (Click to redirect to the link)

Website articles and blogs

[W1] Global Cryptocurrency Ownership Data 2021 - TripleA (triple-a.io)

[W2] Cybersecurity in Cryptocurrency: Risks to Be Considered - DATAVERSITY

[W3] Cryptocurrency Definition

[W4] Bitcoin Definition

[W5] The Difference Between Centralized and Decentralized Networks | N-able

[W6] 51% Attack Definition

[W7] Once hailed as unhackable, blockchains are now getting hacked

[W8] Crypto Terms You Should Know If You Want to Invest

[W9] Hash Power / Hash Rate

[W10] Cryptocurrency Public Ledger Defined

[W11] Poisson Distribution Definition

Scientific papers and journals

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

[P2] Security of Cryptocurrencies in blockchain technology: State-of-art, challenges and future prospects Arunima Ghosh, Shashank Gupta, Amit Dua, Neeraj Kumar

[P3] BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network Shailendra Rathore, Byung Wook Kwon, Jong Hyuk Park

[P4] Analysis of Security in Blockchain: Case Study in 51%-Attack Detecting Congcong Ye, Guoqiang Li, Hongming Cai, Yonggen Gu, Akira Fukuda

[P5] Random Mining Group Selection to Prevent 51% Attacks on Bitcoin Jaewon Bae, Hyuk Lim

[P6] A new key protocol design for cryptocurrency wallet Soonhwa Sung

[P7] Making Smart Contracts Smarter Loi Luu, Duc-Hiep Chu, Hrishi Olickel, Prateek Saxena, Aquinas Hobor

[P8] Town Crier: An Authenticated Data Feed for Smart Contracts, Fan Zhang, Ethan Cecchetti, Kyle Croman

[P9] An Overview of Smart Contract: Architecture, Applications, and Future Trends Shuai Wang, Yong Yuan, Xiao Wang, Juanjuan Li, Rui Qin, Fei-Yue Wang