International Journal of Internet, Broadcasting and Communication Vol.13 No.4 1-10 (2021)
http://dx.doi.org/10.7236/IJIBC.2021.13.4.1

IJIBC 21-4-1

Research on Security Threats Emerging from Blockchain-based Services

Soonduck Yoo

Professor of Business Administration, Hansei University, Republic of Korea
koreasally@gmail.com

Abstract

The purpose of the study is to contribute to the positive development of blockchain technology by providing data to examine security vulnerabilities and threats to blockchain-based services and review countermeasures. The findings of this study are as follows. Threats to the security of blockchain-based services can be classified into application security threats, smart contract security threats, and network (P2P) security threats. First, application security threats include wallet theft (e-wallet stealing), double spending (double payment attack), and cryptojacking (mining malware infection). Second, smart contract security threats are divided into reentrancy attacks, replay attacks, and balance increasing attacks. Third, network (P2P) security threats are divided into the 51% control attack, Sybil attack, balance attack, eclipse attack (spread false information attack), selfish mining (selfish mining monopoly), block withholding attack, DDoS attack (distributed service denial attack) and DNS/BGP hijacks. Through this study, it is possible to discuss the future plans of the blockchain technology-based ecosystem through understanding the functional characteristics of transparency or some privacy that can be obtained within the blockchain. It also supports effective coping with various security threats.

Keywords: *Blockchain, Security threats, application security threats, smart contract security threats, network (P2P) security threats*

1. Introduction

Blockchain technology is widely known through Bitcoin, a cryptocurrency first applied in the financial

Field [8,9]. Despite the fact that blockchain technology overcomes some of the limitations of the security of the current system, we have a perception that blockchain is inadequate for hacking and security through news about cryptocurrency hacking [1]. Cryptocurrency hacking is the movement of electronically stored data or changing the data so that it can ultimately provide profits to the perpetrators. Therefore, a good security reinforcement method to prevent hacking is to apply measures that whatever economic benefit any hacking might yield would ultimately amount to less than the investment cost for doing so.

The distributed storage technology, which is the basis of the blockchain, is to make little or no economic gains as a result of hacking in proportion to the cost of using it to change all information held by

Manuscript Received: August. 11, 2021 / Revised: August. 15, 2021 / Accepted: August. 18, 2021
Corresponding Author: koreasally@gmail.com
Tel: Fax: +82-31-450-5187
Professor of Business Administration, Hansei University, Republic of Korea

participants. However, this does not mean that blockchain-based systems can fully respond to security threats. Therefore, it is necessary to understand the cryptographic and security functions of the blockchain in order to understand and respond to the limiting factors of the blockchain technology.

In order to effectively cope with various security threats of the blockchain, based on an understanding of the functional characteristics of transparency and privacy provided by the blockchain, it is necessary to be able to discuss the future plans of the blockchain application ecosystem [11].

The purpose of this study is to contribute to the development of newly emerging blockchain technology as a study on security threats to blockchain-based services

2. Literature Review

2.1. Blockchain-based Security Threat

Blockchain technology is a technology that can safely defend against security vulnerabilities in the existing centrally controlled cloud system by using the distributed ledger method. Therefore, blockchain technology is a cryptographic algorithm and protocol to implement the consensus method for the majority of participants used to store and manage data. Blockchain has the potential to overcome the limitations of existing technologies in all fields, such as improving the integrity of data and digital ID to increase the safety of Internet of things (IoT) devices and block Distributed Denial of Service (DDoS) attacks.

Blockchain provides reinforced elasticity, encryption, transparency, and auditing by encompassing the three elements of the CIA: confidentiality, integrity, and availability. Therefore, blockchain-based services contribute to the development of the digital age by building a reliable infrastructure [10].

2.1.1 Improve Confidentiality and Data Integrity

Confidentiality and data integrity are important factors because data can be easily manipulated or forged due to technological advances in the case of centralized development. One of the characteristics of the blockchain is that it operates without access control in a centralized way. Therefore, in general, when the data is transmitted by encrypting the entire blockchain data, it is theoretically impossible for an intervening person (ex. a third party) to intercept the data because an unauthorized person cannot access the data.

2.1.2 Digital Authentication Technology

In computer security, digital authentication is a process of attempting to verify the sender's digital identity through a log-in request. The one-way method of blockchain technology is to bundle transaction information into one encrypted block and share it with participants.

In addition, digital authentication security technologies are applied, and data is stored in a distributed data storage environment based on a chain-type link, and no one can arbitrarily change it. Research on blockchain based authentication applications as well as various cryptographic technologies that can protect the transparency and privacy of the blockchain are continually being conducted [3].

2.2. Security Enhancement Technology Applied to Bitcoin

In the case of Bitcoin, a representative case implemented with blockchain technology, various security threats emerging from electronic transactions are implemented as a technical countermeasure. Bitcoin applies not only the distributed network method, which is the basic principle of the block chain, but also public key encryption and hash encryption technology, which are cryptographic methods. In addition, double transaction prevention technology is applied in bitcoin transactions.

Table 1. Security enhancement technology applied to Bitcoin

Division		Concept
Distributed network	Distributed consensus system	In order to create a transaction in a blockchain, it adopts a distributed consensus method that approves the transaction, and is verified in a P2P distributed network without a third-party certification authority
Cryptographic technology	Public key encryption	An electronic signature algorithm (ECDSA (Elliptic Curve Digital Signature Algorithm)) is used to verify that the transaction details have not been changed by verifying the digital signature generated during interpersonal transactions. The basic principle uses anonymity
	Hash encryption	The hash code is used to find the nonce value for the purpose of proving that the information of the block including the transaction history is not changed, and for the purpose of finding a new block. (Mining) This is the process of inferring the nonce value by putting the transaction details, hash value, and nonce value of the previous block into the hash function to obtain a result value that satisfies a specific condition. (Digital Signature) Hash encryption is used in bitcoin transactions to prove the integrity of transaction information, and it is possible to guarantee the integrity of transaction details with the hash value of transaction information through public key-based encryption. (Simplified transaction verification) It has a root hash of a Merkle tree structure that accumulates the hash value of each transaction by applying the principle of easily determining whether or not the root hash value is altered when the value is changed in the middle.
Double transaction prevention technology		Using The Longest Chain Wins mechanism and the amount of money to prevent malicious actions such as sending money to more than one account at the same time. (Verification of total currency volume) When double transactions occur, the total currency volume (21 million) is exceeded. (The Longest Chain Wins) If the blockchain is forked due to redundant expenditure, it is considered to use a chain with a longer length by creating the next block first.

2.3. Preliminary Research

Kim Hee-yeol (2018) analyzed various types of security threats that threaten the blockchain system, and argued that the limiting factors of blockchain security include low Transaction Per Second (TPS) performance problems, increased storage space, and security problems [2].

Park Hyeon-Jeong “et al” (2017) argued that in order to use the blockchain for IoT security, more research is needed on vulnerabilities such as the risk of personal information leakage, the risk of data errors, and insufficient storage [7]. In the case of IoT devices, personal information is inevitably entered into the data according to the characteristics of the device, so internal data must also be encrypted to prevent security risks [4]. To defend against this, Ubirch, a startup company, used its own public key cryptography when writing data to blocks to prevent hacking threats that could occur when each IoT sensor sends data to Ubirch.

In the study, Youngsoo Kim, Youngchan Kim, and Byung-Yup Lee (2018) selected the permission-type public blockchain model as the most suitable reference model for the transport logistics tracking model considering security. A centralized model and a blockchain model were used for comparative analysis and evaluation to verify the practicality of the transport logistics tracking model [12,13].

The block chain-based transport logistics tracking model proposed in this study can be used to detect in consistency with transport information through the tracking of transport logistics by being integrated with a

real-world logistics system, and can be used as a marketing tool to enhance the corporate image.

3. Blockchain-based security threat analysis

3.1. Types and Concepts of Blockchain Security Threats

Looking at the types of threats to the security of blockchain-based services, it can be classified into application security threats, smart contract security threats, and network (P2P) security threats.

First, application security threats include wallet theft (e-wallet stealing), double spending (double payment attack), and cryptojacking (mining malware infection).

Second, smart contract security threats are divided into reentracy attack, replay attack, and balance increasing Attack.

Third, network (P2P) security threats are 51% attack, Sybil attack, balance attack, eclipse attack (false in formation propagation attack), selfish mining (selfish mining monopoly), block withholding attack (block hold attack), distributed denial of service attack (DDoS attack), Domain name system (DNS) or Border gateway protocol (BGP) hijacks, etc.

Table 2. Types of blockchain-based service security threats

Division		Division
Application security threat	Wallet Theft	After infecting the electronic wallet software running on the user's computer with malicious code such as ransomware, it freezes the assets of a specific address or steals the secret key that creates the account of each wallet. Then, by creating a forged address (account), it is an attack that transfers the cryptographic assets held by the user to another wallet.
	Double Spending	The blockchain consensus algorithm performs an attack that uses the difference in time it takes to process and verify each transaction. When the protocol inside the blockchain is hard forked, it unavoidably attacks by using the authentication key duplication phenomenon of the electronic wallet address (account) between the existing chain and the created chain.
	Cryptojacking	By installing mining software on one's PC without their knowledge of the Internet users, the infected PC mines a specific cryptocurrency, and then continuously transmits the mined cryptocurrency to the wallet of the malware distributor.
Smart Contract Security Threat	Reentracy Attack	The re-entry attack is used to construct a smart contract, and is an attack method that induces double processing by requesting a single transaction and then requesting a new transaction again before the transaction is processed.
	Replay Attack	Replay attacks in the blockchain environment can use the same authentication key for each system when a transaction that has been validated within the hard forked existing blockchain system is entered into the smart contract of the new blockchain system. Therefore, it is an attack that uses the characteristic of performing a specified procedure (remittance or withdrawal) by recognizing the validity of the authentication key in the new blockchain system.
	Balance increase attack	An attack in which an attacker forcibly transfers a certain amount to the target's account address, increases the balance, and then forcibly executes a transaction that could not be executed.
Network (P2P) security threat	51% Control Attack	Among the attack methods for the blockchain system, the most representative attack is the attack that has 51% of the total node hashing power.
	Sybil Attack	A type of 51% attack, in which an attacker randomly creates a false mining node inside the blockchain network and takes over 51%
	Balance Attack	A type of 51% attack that induces all blockchains other than the ones created by the attacker to be invalidated based on the mining performance or holdings that the attacker's node has overwhelmingly superior to other mining nodes.
	Eclipse Attack	An attack in which an attacker's node wastes hash power of neighboring nodes by continuously spreading false block information to neighboring nodes or makes transactions

		with false blocks.
	Selfish Mining	After completion of mining, the mining result is hidden without spreading it to the network. When the network share of other nodes increases, the saved block is spread to the network, thereby maintaining a high share and monopolizing the mining rewards.
	Block Withholding Attack	Blockchain consensus algorithm requires a certain amount of time to verify a transaction, and if the same or random false traffic that is infinitely repeated according to the characteristics of such a network enters the network, the time for a legitimate transaction increases infinitely. Therefore, it is an attack that makes it impossible to provide a service.
	DDoS Attack	Blockchain consensus algorithm requires a certain amount of time to verify a transaction, and if the same or random false traffic that is infinitely repeated according to the characteristics of such a network enters the network, the time for a legitimate transaction increases infinitely. Therefore, it is an attack that makes it impossible to provide a service..
	DNS or BGP hijacks	DNS and BGP intermediary hijacking attacks include falsely writing the address of the destination (e-wallet) for remittance of cryptographic assets, or hijacking the route in the middle. And general users mistake the fake system created by the attacker as an official website or official service page. o This method is a type of phishing attack in which the target person enters important information from the forged server location and leaks the target person's key information.

3.2. Application security threat

3.2.1 Wallet Theft (e-wallet stealing)

Wallet Theft freezes assets of a specific address through malware infection such as ransomware in the electronic wallet S/W running on the computer used by the attacker, or steals and falsifies the secret key that creates the account of each wallet. By creating and distributing one address (account), the cryptographic assets held by the attack target are transferred to another wallet [5].

As a representative example, Sheetcoin's wallet provides a Windows desktop app and provides the ability to manage Ethereum-based tokens in a browser. Harry Denri, security officer at blockchain company Micropto, discovered malware in the Sheetcoin wallet. In the process, he discovered that the private keys of all wallets created and managed through the program interface were transferred to a strange storage rather than the original storage.

Looking at the hacking execution process, when a user installs a Sheetcoin wallet, this program requests

permission to insert JavaScript code on 77 websites. When a user accesses one of the 77 sites, it loads an additional JavaScript file. All hacked files are composed of encrypted codes, which are activated on five specific websites, which provide services to cryptocurrency wallets and exchanges.

After the code was activated, it recorded user information to log in to the account, searched for the private key in the service dashboard, and sent the stolen data to a specific address. Through this, account information has been stolen when accessing the cryptocurrency site, allowing hackers to move cryptocurrency assets.

3.2.2 Double Spending

Double spending is an attack that uses the difference in time taken for the blockchain consensus algorithm to process and verify each transaction. When protocol inside the blockchain is hard forked, this refers to a hacking attack by using the authentication key duplication phenomenon of the electronic wallet address (account) between the existing chain and the created chain inevitably. Looking at the double spending example, the attacker was a miner who maliciously has secured control of the Bitcoin Gold (BTG) blockchain after possessing more than 51% hash power in the Bitcoin Gold network.

After that, he used a method of proceeding with a double payment attack, immediately cashing out the BTG acquired through the exchange and returning the transaction again. The total amount of damage confirmed so far is 388,200 BTG, which is about $18.6 million. All Proof of Work (POW) algorithms have a

51% attack potential, and this is a general case.

3.2.3 Cryptojacking (mining malware infection)

Cryptojacking refers to the act of installing mining software on others' PC's without their knowledge, so that the infected PC mines a specific cryptocurrency, and then continuously transmits the mined cryptocurrency to the wallet of the malware distributor. The number of minor malware samples collected by AhnLab in 2018 increased by 2,254% compared to 2017. It was confirmed that the proportion of using the CPU for mining operations was largely due to the haracteristics of malicious codes that are randomly distributed to unspecified people. In addition, out of the 3,354,000 cases of infection reported by AhnLab in 2018, the number of reported infections in the top 10 was 2,228,000, accounting for about 66% of the top 10 infection reports.

3.3. Smart Contract Security Threat

3.3.1 Reentracy Attack

The re-entry attack is used to compose a smart contract, which refers to an attack method that induces double processing by requesting a new transaction after requesting one transaction and before the transaction is processed. Reentrancy or reentry refers to an attack method that induces double processing by requesting a transaction and then requesting a new transaction again before the transaction is processed. For example, if the sender's balance is 5 million won, after requesting a transaction to withdraw 5 million won using a call function, an attack that sends a call requesting withdrawal of 5 million won again before the transaction is processed. At this time, the smart contract system tries to process the call because the balance is 5 million won for the first call.

If a call requesting withdrawal of 5 million won comes in again before this attempt is actually performed, it is judged that it is sufficient because the balance is 5 million won, and an error occurs in processing both withdrawal requests. Failure to prevent the reentrant problem will eventually lead to a double payment problem. According to Cryptopedia site, in June 2016, the DAO hack that exploited this reentrant vulnerability occurred.

This hacking technique could be prevented by appropriate code modification afterwards, but after the infamous Dao hacking incident, the Ethereum camp had to hard fork with two types of cryptocurrencies, Ethereum and Ethereum Classic.

3.3.2 Replay Attack

A replay attack is a cyber attack in which a malicious hacker intercepts valid data transmission through a network and then repeatedly uses it. As a representative example, replay attacks in the blockchain environment occur within the existing hard forked blockchain system. When a transaction that has been recognized for validity is entered into the smart contract of the new blockchain system, the same authentication key is used in a system separate from the previous system, so a phenomenon that the validity is recognized and the specified procedure (remittance or withdrawal) is per formed twice.

Reduction of the effect of replay attacks is a limitation of replay attacks. The attacker cannot change the transmitted data without rejecting the network, so the effectiveness of the past repetition attacks decreases. One way to prevent attempts at replay attacks is to add a time stamp to the data transmission. In addition, the server may store the repeated message in the cache and then limit the number of specific repetitions to prevent a continuous attack that an attacker attempts through a quick replay message.

3.3.3 Balance increase Attack

A balance increase attack refers to an attack in which an attacker forcibly remits a certain amount of money to the target's account address to increase the balance, and then forcibly executes a transaction that could not be executed.

3.4. Network(P2P) Security Threat

3.4.1 51% Control Attack

The 51% control attack is the most representative attack method for the blockchain system, and it refers to an attack that controls 51% of the hashing power of all nodes. Therefore, if the consensus algorithm is applied by attacking 51% of the chain, the node where the hacking attacker is formed is recognized as a normal node and applied.

In theory, this is possible, but if the number of participants is especially large, it is difficult to change the information of 51% of all participants. This security threat can occur when there are few participants at the beginning of service creation.

3.4.2 Sybil Attack

A Sybil attack refers to a method in which an attacker randomly creates a false mining node inside the blockchain network and takes over 51%. An example of Sybil attack in computer security is an attack that destroys the reputation system by generating multiple identities. The vulnerability of the reputation system depends on how cheaply it can create participants and the degree to which the reputation system accepts input from untrusted participants that connect to trusted participants. In 2012, it was known that existing realistic systems such as BitTorrent Mainline DHT could perform large scale Sybil attacks in a very inexpensive and efficient manner.

3.4.3 Balance Attack

It refers to an attack that invalidates all blockchains that are not blockchains created by attackers with overwhelmingly superior mining performance or holdings. In the study of Natoli, Christopher, and Vincent Gramoli (2016), researchers investigated the network delay and mining ability of attackers using high cost in Ethereum through theoretical analysis [6]. Statistics taken from the R3 consortium showed that, based on probabilistic analysis, it only took 20 minutes for a single machine to attack a group of consortiums.

3.4.4 Eclipse Attack (False Information Propagation Attack)

A false information propagation attack refers to an attack in which an attacker's node continuously propagates false block information to neighboring nodes to waste hash power of neighboring nodes or perform transactions with false blocks.

3.4.5 Selfish Mining (Selfish Mining Monopoly)

A mining monopoly means that mining has been completed, but the result of the mining is not propagated to the network, but when the network share of the handled nodes attempts to exceed the share of the attacker, the accumulated blocks are spread to the network, thereby continuously maintaining a high share. It is an attack that allows one to monopolize rewards.

Therefore, selfish mining is a personal mining node or mining pool with high hash power that creates blocks faster than other mining nodes or mining pools on the blockchain network, and it wastes resources by intentionally delaying the propagation of the generated blocks. This is an attack that can delay the creation of

blocks by hindering fair competition for mining. For example, a block is created quickly and connected to it, and the block or subsequent blocks are propagated to the network before other mining nodes or mining pools complete mining, creating a longer chain. In this case, blocks mined by other miners can be made into unusable blocks. There is also a method of relocating miners or mining pools to other branches through a branch environment so that the previous block cannot be directly continued when mining is again performed after selecting the longest chain as the main chain by changing the protocol of the blockchain.

In addition, preventing monopoly by setting a limit on the hash rate that the mining pool can occupy can be one way. In addition, if the difference between the generation time and the propagation time is large according to the time stamp recording of the generated block, it can be considered that there was an intention of a selfish mining attack. Therefore, a method of penalizing mining is also proposed as an alternative.

3.4.6 Block Withholding Attack

Similarly, block-holding attacks use a method of continuing to mine the next block without propagating the mined block if the hash power is superior to other nodes. Block withholding attacks are an attack method known in existing Bitcoin. It is required that the miner can mine from two mining pools and take advantage by holding the answer to the proof of work without notifying the mining pool operator. However, in order for such an attack to be possible, a huge amount of computing power (1% of Bitcoin's total system) is required.

3.4.7 Distributed Denial of Service Attack (DDoS Attack)

The blockchain consensus algorithm requires a certain amount of time to verify the transaction, and according to the characteristics of such a network, the same or random false traffic that is repeated infinitely can enter the network. In this case, the DDoS attack is an attack that makes it impossible to provide a fixed service because the time for a fair transaction increase infinitely. In general, DoS was done against popular sites: banks, credit card payment gateways, or root name servers.

The DNS backbone DDoS attacks against the DNS root server of October 22, 2002 and February 6, 2007 were attacks on the entire Internet by incapacitating the Internet URL address system.

3.4.8 DNS, BGP hijacks (DNS, BGP intermediary hijacking)

In the middle of DNS and BGP hijacking attacks, the address of the destination (e-wallet) for remittance of cryptographic assets is falsely written or stolen in the middle of the route, so that the general user mis-understands the fake system created by the attacker as an official website or official service page. In addition, it is a type of phishing attack that makes the target person input important information from the forged server location or leaks the key information through a specific reaction of the target person.

Hackers block access to services such as Twitter, Netflix, and PayPal. This is because they have downed the domain name system (DNS) service provider that most of the major web sites use.

The blockchain base applies the principle of “The Longest Chain Wins” when the block chain is forked by redundant expenditures, and the next block is first created, and the chain whose length on one side is longer is considered to be correct.

4. Conclusion

Blockchain-based services also have technical complexity and cannot be said to be 100% secure. In order to store information in a distributed manner based on a blockchain, there are limiting factors that appear to process various events such as restriction of processing speed and confirmation of storage location. In spite of these limiting factors, companies are converting services to blockchain services because they propose a

countermeasure to the limitations of security processing provided in the existing legacy system processing method.

This study examined the security vulnerabilities of services produced based on blockchain. Threats to blockchain-based security can be classified into application security threats, smart contract security threats, and network (P2P) security threats.

First, application security threats include wallet theft (e-wallet stealing), double spending (double payment attack), and cryptojacking (mining malware infection).

Second, smart contract security threats are divided into reentracy attack, replay attack, and balance increasing attack.

Third, network (P2P) security threats are the 51% attack, Sybil attack, balance attack, eclipse attack (false information spreading attack), selfish mining (selfish mining monopoly), block withholding attack (block holding attack), Distribution denial of service attack (DDoS attack), DNS, BGP intermediary hijacking (DNS, BGP hijacks), etc.

In this study, through understanding the cryptographic and security functions provided by the blockchain, it is possible to know where the limits of the current technology are. It also helps a clear understanding of what needs to be implemented additionally. It is possible to understand the functional characteristics of transparency that can be obtained through the blockchain or some privacy that cannot be obtained, discuss future plans of the blockchain application ecosystem, and effectively cope with various security threats.

This study contributes to the development of blockchain technology by studying security threats that are emerging according to the development of blockchain technology. In addition, it can be used as a reference when establishing policies and systems in the field of blockchain. Blockchain security threats exist in various ways, and this study deals with the representative security threats. Therefore, it is necessary to investigate more various security threats in future studies.

Acknowledgement

This work was supported by the Hansei University Research Fund of 2021

References

[1] Dasgupta, Dipankar, John M. Shrein, and Kishor Datta Gupta. "A survey of blockchain from security perspective." Journal of Banking and Financial Technology 3.1 (2019): 1-17.

[2] Hee-yeol Kim, "Analyze the security threats and countermeasures of the blockchain platform." Journal of the Korea Information Technology Society 16.5 (2018): 103-112.

[3] Joshi, Archana Prashanth, Meng Han, and Yan Wang. "A survey on security and privacy issues of blockchain technology." Mathematical foundations of computing 1.2 (2018): 121.

[4] Kumar, Nallapaneni Manoj, and Pradeep Kumar Mallick. "Blockchain technology for security issues and challenges in IoT." Procedia Computer Science 132 (2018): 1815-1823.

[5] Moubarak, Joanna, Eric Filiol, and Maroun Chamoun. "On blockchain security and relevant attacks." 2018 IEEE Middle East and North Africa Communications Conference (MENACOMM). IEEE, 2018.

[6] Natoli, Christopher, and Vincent Gramoli. "The balance attack against proof-of-work blockchains: The R3 testbed as an example." arXiv preprint arXiv:1612.09426 (2016).

[7] Park, Hyeon-Jeong, Hye-Im Yang, and Jeong-Hun Jeon. " Blockchain-based IoT security vulnerability." Korea Information Processing Society Review 24.3 (2017): 13-21.

[8] Park, Seong-Jun. "Blockchain Paradigm and Fintech Security." Information and Communications Magazine 34.3 (2017): 23-28.

[9] Yoo, Soonduck. "Blockchain based financial case analysis and its implications." Asia Pacific Journal of Innovation and Entrepreneurship (2017).
[10] Yoo, Soonduck, and Kim Kiheung. "Research on improvement measures for spreading blockchain-based services." The Korean Society for Internet Broadcasting and Communication 18.1 (2018): 185-194.
[11] Yoo, Soonduck. "Token's function and role for securing ecosystem." International Journal of Advanced Culture Technology 8.1 (2020): 128-134.
[12] Youngsoo Kim, Youngchan Kim, and Byungyop Lee. "Anomaly behavior tracking security model using private blockchain in a cloud environment." Journal of the Korea Contents Association 18.11 (2018): 475-483.
[13] Yu, Yong, et al. "Blockchain-based solutions to security and privacy issues in the Internet of Things." IEEE Wireless Communications 25.6 (2018): 12-18.