J. Internet Comput. Serv.
ISSN 1598-0170 (Print) / ISSN 2287-1136 (Online)
http://www.jics.or.kr

블록체인 보안 이슈에 대한 분석과 해결 방안에 대한 연구☆

A Study on the Analysis and Solutions of the Blockchain Security Issues

노 시 완[1] 이 경 현[2*]
Siwan Noh Kyung-Hyune Rhee

요 약

블록체인 기반 접근제어 기술은 블론체인의 다양한 활용 사례 중 하나로 많은 분야에서 중개인 없이 사용자 간의 소유권 이전·관리를 투명하게 수행하고자 하는데 활용하고 있다. 퍼블릭 블록체인이 제공하는 투명성, 비가역성 그리고 분산의 특징은 기존의 접근제어 기술이 제공하지 못했던 새로운 장점을 제공할 수 있도록 도와준다. 하지만 현재 블록체인이 직면한 여러 보안 문제로 인해 기술의 안전성에 대한 문제점이 제기되고 있고 이를 기반으로 하는 다른 활용 사례에 대한 안전성 문제 역시 다뤄지고 있다. 본 논문에서는 블록체인 기반 접근제어 기술의 개요와 함께 직면한 여러 보안 문제 중 대표적인 문제에 대한 분석과 이를 해결하기 위한 솔루션들에 대해 분석한다. 더 나아가 트릴레마에 영향을 받지 않는 솔루션과 이를 기반으로 하는 접근제어 기술의 모델을 제시한다.

☞ 주제어 : 블록체인, 접근제어, 보안, 프라이버시

ABSTRACT

A Blockchain-based access control technology is one of the various use cases of blockchain and is used in many areas to transparently transfer and manage ownership of data between users without the trusted third party. The characteristics of transparency, Irreversibility, and decentralization provided by the public blockchain help to offer new benefits that existing access control technologies did not offer. However, various security issues facing the current blockchain are raising the issue of the safety of the technology. Therefore, in this paper, we analyze an overview of the blockchain-based access control technology and solutions of the security challenges faced. Moreover, we further present solutions that are not affected by the blockchain trilemma and models of access control technology based on them.

☞ keyword : blockchain, access control, security, privacy

1. Introduction

Blockchain or a Distributed Ledger Technology(DLT) is a technology that manages transactions based on an agreement between participants without the involvement of a trusted third party(TTP). In the central database system, when participants requested transactions to the administrator, the administrator verified the request and updated the contents of the database, but there were issues of trust to the administrator and single point of failure.

In 2008, an anonymous developer named Satoshi Nakamoto announced Bitcoin[1], which manages transactions based on agreements among participants without the involvement of the centralized manager. Along with the popularity of Bitcoin, development of cryptocurrency that added various functions or supplemented bitcoin's shortcomings was actively carried out. Moreover, not only in the financial sector but also in many other areas, blockchain technology can be found[2-8].

In the logistics sector, a blockchain-based supply chain management platform was proposed to track and manage logistics processes in real time by recording the process from the production of goods to the final destination. If the logistics

1 Interdisciplinary Program of Information Security Graduate School, Pukyong National University., Busan, 48513, Korea.
2 Department of IT Convergence and Application Engineering, Pukyong National University., Busan, 48513, Korea.
* Corresponding author (khrhee@pknu.ac.kr)
[Received 12 February 2019, Reviewed 22 February 2019(R@ 30 April 2019), Accepted 4 June 2019]
☆ This research was supported by the MSIT(Ministry of Science and ICT), Korea, under the ITRC(Information Technology Research Center) support program(IITP-2019-2015-0-00403) supervised by the IITP(Institute for Information & communications Technology Planning &Evaluation) and partially supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. NRF-2018R1D1A1B 07048944)
☆ A preliminary version of this paper was presented at APIC-IST 2018 and was selected as an outstanding paper.

record is to be recorded in the blockchain, the contents recorded in the blockchain cannot be modified due to the irreversibility of the blockchain, thus solving the problem of modifying the record and the complexity of the logistics process.

Samsung SDS simplified the shipping process by omitting the offline verification of documents created in the process by using Nexledgeer[3] which is a blockchain platform that they developed, and recording various information collected in the container during transport to the blockchain to ensure transparency in the shipping process. Wal-Mart in the U.S. is also building a system that uses IBM's blockchain technology to track the logistics transport process from a place of origin to store[4]. Once the system has been established, consumers are expected to be able to track logistics management history, and managers are expected to be able to identify problems that may occur in the shipping process in advance.

In the healthcare area[9-10], blockchain technology is used for patient-centered management of the Personal Health Information(PHI)[5-8]. In the previous medical system, the PHI of patients was owned and managed by institutions that produced records in the form of electronic medical records(EMR), and sharing of records was only possible when there were pre-created shared channels. The MIT media lab members are trying to solve this problem through an ethereum blockchain-based project called MedRec[5-6]. MedRec managed the authorization status of the PHI of patients through smart contracts to control access to the databases.

This paper aims to analyze various security issues and their solutions for data access control, one of the famous use cases of blockchain technology. The rest of this paper is organized as follows: We first introduce an overview of the blockchain technology and blockchain-based access control in Chapter II and analyzes issues and solutions that could pose a security threat to these access-control technologies in Chapter III, and finally, conclude this paper in Chapter IV.

2. Related Work

2.1 Blockchain

Although centralized systems that ensure the reliability of a system through a trusted third party(TTP) that is trusted by participants in common. However, trust in a single entity in today's Internet environment is not realistic for a number of reasons. The blockchain is a distributed database for ensuring reliability among unreliable participants without the participation of trusted intermediaries. All transactions(i.e., event) occurring in blockchain networks are added at regular intervals to the local blockchain that all participants own and manage individually, in the form of blocks which are sets of records. However, if any participant in the network can create a block(i.e., not just one participant creating the block), each participant in the network will have a different database and therefore cannot ensure the reliability of the database.

Bitcoin blockchain solves this problem through a proof-of-work(PoW). A particular participant, called a miner, creates a new block through the following process:

(1) The miner node collects the transaction records $tx = \{tx_1, tx_2, ..., tx_i\}$ that have not yet been included in the blockchain for a certain period of time.

(2) Repeat the calculation until the following formula is satisfied with the current difficulty D and hash value of the previous block T.

$$i = 0; \text{while } H(i; H(T, tx)) > D \text{ do } i{+}{+}$$

(3) If i is found to satisfy the conditions, (T, i, tx) is propagated to the blockchain network as a new block.

A node that receives a new block verifies the validity of the block and updates the local block chain through the following process:

(1) A node that receives block (T', i', tx') verifies the validity of the block through the following operation.

$$(T = T') \wedge (H(i; H(T, tx)) \leq D)$$

(2) If the block meets the conditions described in (1) then connect it to its local blockchain.

By repeating the above process, it is possible to ensure that all participants in the system manage their own ledgers individually, but all have the same ledger through consensus. Blockchain networks can generally be distinguished by public blockchain, private blockchain, permissioned blockchain, and

permissionless blockchain by regulating read and write functionality to network participants[11]. In this paper, we focus on the permissionless public blockchain such as Bitcoin blockchain. The main characteristics provided by the public blockchain are as follows:

- Transparency

Unlike a centralized server, the contents recorded in the blockchain are recorded in the local blockchain, which is individually managed by all participants, so that anyone can check the recorded contents if necessary, and thus ensure transparency in the stored records.

- Irreversibility

Records stored in the blockchain are linked to previous records in the form of the block at regular interval. In other words, blockchain is a data structure in the form of linked lists of blocks, which are bundles of records. Each block has a hash value of the previous block and a random value called a nonce. As previously explained, a nonce is a random constant that allows the hash value of the current block to meet certain conditions. The probability of solving the problem depends on the ability of the mining node.

As such, each block in the blockchain is linked together, and if an attacker modifies the data recorded in the blockchain, the hash value of the block T is changed, thereby requiring the calculation of a new nonce value that satisfies the condition. It is also known that it is impossible in reality because the hash value of a block has changed, so the nun value of a child block with a modified block must also be changed, but this requires a tremendous computational power. Therefore, blockchain has a non-inverted characteristic that it is very difficult to modify the recorded content.

- Decentralization

In the public blockchain network, all problems that arise on the network are dealt with based on agreement from the network's participants without the involvement of a network administrator. Even if there are developers who develop and distribute blockchain protocol updates, mandatory updates are not possible like traditional centralized systems. One example is Bitcoin's hard fork case.

Although Bitcoin Core Group has maintained and repaired Bitcoin core clients, it has recently failed to reach an agreement between community members on how to solve the issue of scalability. As a result, Bitcoin blockchain was hard-forked, resulting in several new altcoin blockchains(e.g., bitcoin cash, bitcoin gold).

These decentralized features prevent specific objects from being over-authorized, making them the main reason for attempting to apply blockchain in a variety of fields.

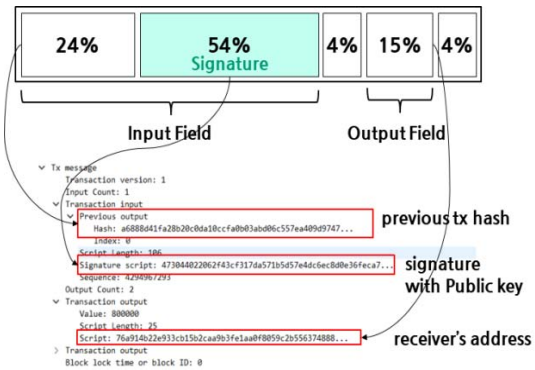
2.2 Blockchain-based Access Control

In section 2.1 we looked at an overview of the blockchain technology and its main features. In this section, we describe an overview of the blockchain-based data access control and related research that will be focused on in this paper.

Blockchain-based access control[12-13] records access to data in the blockchain, enabling anyone to verify access rights and prevent third parties from modifying or deleting recorded rights. Moreover, it enables data owners to manage access to their data without the involvement of a central administration agency. In particular, an medical information sharing system for mutual communication of patients' medical records managed individually by various agencies, patients are being utilized as a way to manage access to their medical records.

The method of recording rights to specific assets in the blockchain was used from Bitcoin. In the bitcoin protocol, users create and propagate a transaction to the network, including proof of ownership and new ownership transfers. All participants in the network validate the validity of the transaction and finalize the transaction by including it in the blockchain only if it is valid.

The structure of a bitcoin transaction can be divided into two parts, as shown in Figure 1. The input field contains a digital signature and a current owner's public key for proof of ownership, and the output field contains the address of another user to transfer ownership. The network's verifiers discard transactions generated by users who do not have ownership(i.e., do not have a corresponding secret key).



(Figure 1) A structure of Bitcoin transaction

Colored coin[14] extends the basic concept of the bitcoin to reality so that specific crypto-currency recorded in the blockchain represent real assets(such as real estate, a certain amount of cash, etc.). Users can trade assets that present real assets between users by recording the transfer of ownership in the blockchain transparently. However, there was a limit to the lack of legal evidence on the relationship between cryptocurrency and real-world assets.

As in the case of Colored coin, trading real-world assets requires a third party to ensure the relationship between the record of the blockchain and real-world assets. For this reason, digital data that does not require a guarantor is now used as the object of the trade.

In [15], Zyskind et al. proposed a method that uses the blockchain as a distributed hash table to record mapping information about who currently owns the data. Based on this, a method of trading ownership of mapping information to digital data over blockchain was proposed.[12-13].

A user who wants access to data asks the owner of the request data to create a blockchain transaction that contains information of requested data and transfer ownership. The requester demonstrates to the data keeper managing access to the database that he has appropriate rights through proof of ownership(digital signature). All these access rights are recorded in the blockchain, so third parties cannot arbitrarily modify or delete them. Moreover, It has the advantage that data owners can control access to their data themselves without the involvement of intermediaries.

3. Security Issues & Solutions

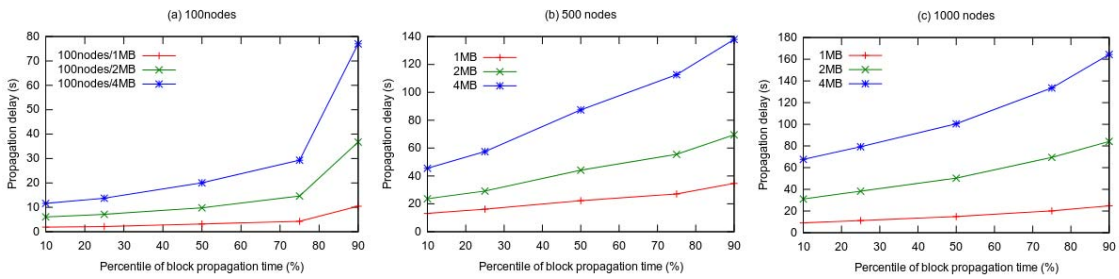
In Chapter 2, we introduced an overview of blockchain and blockchain-based access control. However, there are still many problems to achieve the advantages as mentioned earlier. In this chapter, we analyze security issues and solutions related to blockchain-based access control.

3.1 Performance

The public blockchain network manages the blockchain database through an agreement between unreliable participants. For example, the average block interval is the average time for a block to be created and the block to be propagated to all networks to reach an agreement. Therefore, if the maximum size of the block is limited, the number of transactions that can be processed per hour in the network is limited. For example, in the case of Bitcoin, the maximum size of the block is 1MB, and the average interval of the block creation is 10 minutes. On average, most of the Bitcoin transaction records have two inputs and three outputs. The structure of the transaction described in section 2.2 shows that the number of transactions that can be processed per day is approximately 300,000(about 12,000 per hour, approximately 3-4 per second). However, it has a very low throughput compared to about 2,000 transactions per second by Visa.

A blockchain-based access control technology creates transactions that contain ownership information about the shared data, the same as creating a transaction in crypto-currency.

In this process, the scalability challenges are encountered when an access control service layer is added over a public blockchain to avoid creating a new blockchain network through hard-fork. Low network throughput can take a long time to include the transfer of ownership transactions in the block, which results in difficulties in providing stable services and in reducing network safety in the blockchain. If the performance of the blockchain network is low, it may be delayed to include transactions in the block. The low performance of the blockchain network does not only reduces the availability of services, but also reduces network safety by increasing the success rate of attacks on the network.



(Figure 2) Simulation of Propagation Delay with Increasing Block Size

If a service is built on a network that is a public blockchain that already has a stable environment, it is easy to deploy and can provide stable services. However, in addition to access control service traffic, general transaction traffic is always generated, and thus cannot be free from scalability issues.

The simplest solution to this problem is to use a blockchain network that ensures fast throughput. A typical method of improving throughput in the public blockchain is to change the consensus algorithm and a reparameterization. The PoW method, a typical consensual algorithm, required high computing power and when someone created and propagated a block, other miners should discard their blocks that they were creating, so it was extremely wasteful. As the difficulty increases, more and more computational power is required to create the block, but the number of miners with these high computational power is limited, resulting in the problem of centralization of the blockchain miners.

EOS, called the 3rd generation blockchain, improved performance by using a Delegated Proof-of-Stake(DPoS)[16] as a consensus algorithm.

Under the DPoS method, participants will be given different voting rights to select the block producer(BP) based on their stake in the network. Users vote to select a group of miners to perform the block creation instead of them. Compared to the PoW method, it is possible to quickly and reliably create blocks by performing mining by designated miners(BPs) instead of competitive mining processes. However, there is a disadvantage that BP has the potential to collude and is more vulnerable to a 51% attack than the PoW method.

Another option is to modify the parameters of the blockchain protocol(such as the block size limit or the block generation interval) to remove the limit on the transactions that can be processed per unit hour. However, Croman et al. have found that this approach to scale is limited[17]. As shown in Figure 2, increasing the size of the block increases the bandwidth required during the propagation of the block, which increases the propagation delay. Propagation delay increases the probability of branching in a blockchain network, which can make the network more susceptible to other fatal attacks[18-21].

The solutions as mentioned earlier are inherently limited due to the blockchain trilemma. Blockchain trilemma refers to the problem of worsening one or all of the other attributes when attempting to improve one of the attributes of security, scalability, and decentralization. For example, EOS has improved scalability using the DPoS, but they have worsened decentralization and security by delegating blockchain network management to a small number of miners.

3.2 Privacy

Transparency is also the most significant advantage of blockchain, but it can create privacy issues as ownership transfer history is recorded in the blockchain. For example, if a patient transfers access to his or her medical data to a hospital or research institution, it is possible for a third party to track the patient's access control history through graph analysis [22-23].

Therefore, various methods have been proposed in cryptocurrency to solve the problem of exposure to transaction history[24-27]. Initially, it was proposed to prevent tracking by third parties by bringing together participants who wanted to do anonymous transactions instead of creating individual transactions [24]. However, the

issue of trust for a single object was raised because a trusted person was needed to create a mixed transaction.

Monero used a method to prevent the association of I/O values of transactions from being tracked over the blockchain. Typically, the input field contains a user's signature for proof of ownership, and the output field contains a transfer of ownership, which allows third parties to track the connectivity of the old transaction to the new transaction. In Monero, users can prevent third parties from tracking by using Ring signatures [25-26] and Stealth addresses [27].

As a way to ensure the anonymity of the sender, the sender pre-selects a set of public keys in a particular group and creates a transaction with proof of ownership called the ring signature generated using them. Verifiers in the network can verify the validity of the transaction by verifying its signature, but the verifier cannot know precisely who generated the signature in the group so that the sender's anonymity can be guaranteed.

Stealth address is a disposable address that is used to ensure the anonymity of the recipient. The sender selects a random number when creating the transaction and generates a disposable address based on the recipient's information (address) and the selected random number. It is possible to use a different address for each transaction since only recipients can generate proof of ownership for a disposable address using a secret key that corresponds to the address used to generate the disposable address (public key).

4. Proposed Protocol

4.1 Solution1: Payment channel

In Chapter 3, we analyzed security issues and solutions for blockchain-based access control technologies. Many known solutions now have limitations in their use due to blockchain trilemma. However, solutions exist to avoid blockchain trilemma, such as bitcoin blockchain's payment channel[28-30] and cross-chain[31-34].

A payment channel uses off-chain processing that processes transactions from outside of the blockchain and records only state information about them in the blockchain. Users create logical channels between them and record the initial channel state in the blockchain. The state change due to the transaction is recorded only between channel participants from outside of the blockchain, and the final state is recorded in the blockchain at the end of the channel.

The payment channel uses multi-signature to ensure fairness between users. In other words, all participants on the channel need to be signed to change the channel's state.

The change in channel state does not require consensus-based processes to be included in the block so that speed can be guaranteed. Besides, transactions other than initial and final are not recorded in the blockchain, thus ensuring user privacy.

The process of the access control protocol based on these payment channels is as follows:

(1) A data owner and requester creates a transaction that transmits their crypto-currency, which is collateral, to multi-signature addresses, and propagates it to the blockchain network (initial state transaction).
(2) Create a first state transition transaction, which includes proof of ownership for the initial state transaction and mapping information to the data, and exchange it with each other in the channel.
(3) Based on the initial state transactions recorded in the blockchain, the data keeper validates the validity of the state and verifies access to the data.
(4) Change the mapping information of the data and repeat the procedure (2) to (3).
(5) Propagate the final status transaction to the blockchain network to finalize the state of the channel.

Although it is possible to avoid the trilemma problem because most processes are performed outside of the blockchain, However, it requires the creation of channels among all participants and can also create fairness issues in the order of the exchange of state change transactions. Therefore, in this paper, we introduce how to solve this problem using a cross-chain.

4.2 Solution2: Cross-chain

Currently, most blockchain networks provide isolated network environments that are incompatible with other blockchain networks. Although trust institutions(e.g.,

crypto-currency exchange) are used to exchange information or values recorded in blockchain to other blockchains, many problems such as hacking or trust issues are highlighted. However, with cross-chain, it is possible to communicate the information recorded in the blockchain to other blockchains without the participation of trusted intermediaries.

Cross-chain can be divided into two main categories depending on whether the exchanged information can be returned to the original blockchain. The two-way exchange method[32-34] records the exchange of information in a hub blockchain database, but the one-way exchange method[31] supports cross-chain transactions between users through an unreliable broker who has access to both blockchain networks. using a hashed time lock contract(HTLC). The difference between the two methods is whether they support two-way transactions in which the exchanged information or value can return to the original blockchain. In this paper, we propose a protocol that uses a one-way method to deliver tickets accessible to specific data generated by the data owner to the access requester's blockchain.

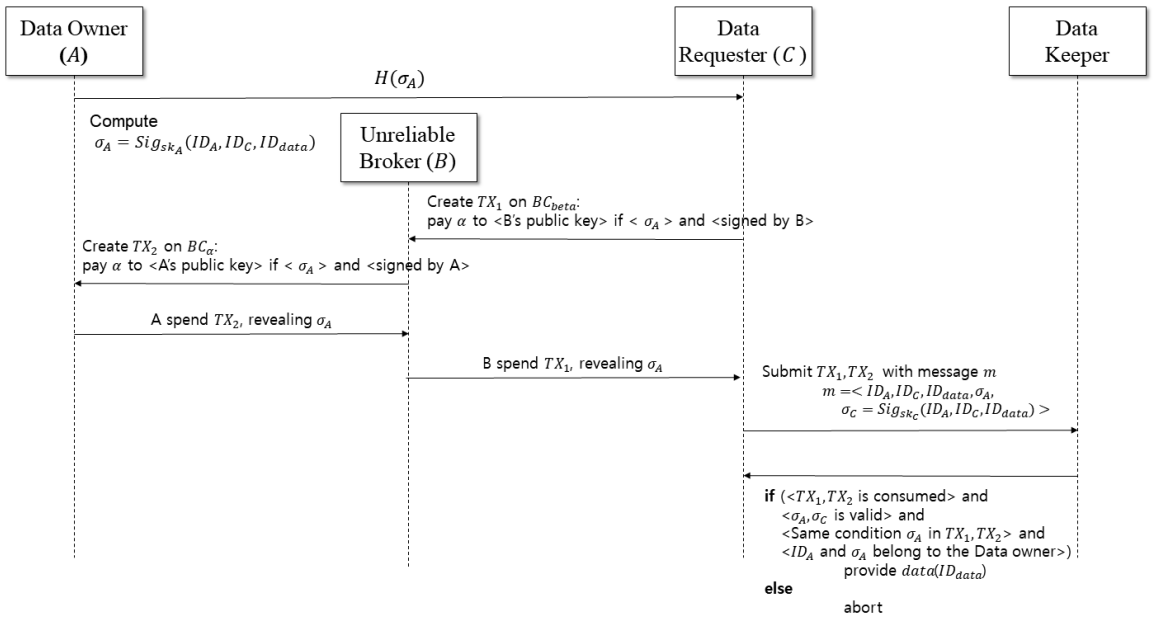
Before describing the protocol, we assume that the data owners and the requester have a crypto-currency in a different blockchain network and already know about the identity of the other party and the data that the requester wants. We also assume that there exists an unreliable broker for cryptocurrency exchanges between data owners and requestors and that the broker's information is already known.

(1) Data owner A generates a signature $\sigma_A = Sig_{sk_A}(ID_A, ID_C, ID_{data})$ and compute $H(\sigma_A)$ (where ID_A, ID_C, ID_{data} are the identifiers of the data owner, the requester and the data to be shared, respectively, and H is a cryptographic hash computation).

(2) Data owner sends $H(\sigma_A)$ to the data requester.

(3) Data requester transfer his crypto-currency to the data owner via the unreliable broker B with the HTLC condition.

(4) When a transaction TX_2 sent by a data requester



(Figure 3) The data requester cannot access the data until the transaction he creates reaches the data owner and is consumed, and the data owner cannot pay for the request without disclosing the signature for the authorization.

(Table 1) A Comparison of Methods for Improving the Trilemma Problems

	Proof-of-Work	Private blockchain	Delegated Proof-of-Stake	Payment channel	Cross-chain
Performance	Low	High	High	High	Medium
Decentralization	High	Low	Medium	Medium	High
Security	Medium	Low	Low	High	High
Interoperability	No	No	No	Yes	Yes

appears in the data owner's blockchain, the data owner consumes the transaction by revealing σ_A to the blockchain.

(5) The broker B also uses the same revealed signature σ_A to consume transactions TX_1 in the data requester's blockchain.

(6) The data requester generates an access request that includes information released in the blockchain and his signature σ_C and forwards it to the data keeper.

(7) The data keeper provides data to the data requester if the following conditions are met:

a. Transaction TX_1 and TX_2 have already been consumed.

b. Results are valid when data owner's signature σ_A and data requester's signature σ_C are verified with the information contained in the transaction TX_1, TX_2.

c. Same HTLC condition $H(\sigma_A)$ included in transaction TX_1 and TX_2

In the proposed protocol, we used HTLCs to ensure reliability in sharing among unreliable users. Transactions TX_1 and TX_2 are not valid until the signature σ_A generated by the data owner is made public on the network. The generation and exposure of signatures indicates that the data owner has received a price for access and at the same time represents the owner's permission for the data requester's request. Moreover, transactions that are transferred by the requester to the broker after the transaction is consumed by the data owner, the reliability of transactions through the unreliable broker can be guaranteed.

4.3 Comparison

In Chapter 3, we mentioned blockchain trilemma as a problem to consider in blockchain-based access control. The two solutions mentioned in Chapter 4 are best suited to blockchain-based access control among the various solutions for solving the trilemma. Table 1 is a comparison of the various solutions available in blockchain-based access control.

PoWs used in first-generation crypto-currency such as bitcoin provide low performance with competitive mining algorithms, but this ensures high decentralization. However, it is known that low performance makes it vulnerable to multiple attacks, which are considered to change to other algorithms, such as proof-of-stake. Private blockchain and DPoS algorithms can improve the performance of the blockchain, but at the same time they sacrifice the decentralization, thereby providing low security as the re-centralization of the network entails the problems of traditional centralized system.

In contrast, the two solutions proposed in Chapter 4 are ways in which you do not have to sacrifice other elements to improve one of the three elements of the trilemma. The payment channel creates an off-chain channel between users and manages the channel's state only between users of the channel outside the blockchain, thus ensuring high performance. It is also possible to establish a payment network that creates these channels across multiple blockchains to ensure interoperability between blockchains. However, there is no guarantee of high decentralization because the payment network is more likely to pass through channels with specific nodes that can operate high deposits to maintain the channel. It also has the disadvantage of being

unsuitable in environments in which intermittent transactions occur between users.

Cross-chain can improve performance by distributing the throughput it incurs in a blockchain network over multiple blockchain networks. Since multiple blockchain networks can ensure high decentralization by sharing information and values with each other, and many existing attacks target only one blockchain network, it is safe unless attacks are made simultaneously to attack all blockchain networks around the world.

5. Conclusion

In this paper, we explained access control, one of the various use cases of blockchain technology, and analyzed various security issues associated with blockchain technology. Blockchain technology faces many security issues and applications based on these blockchain technologies face the same problem. A variety of solutions have been proposed, but there is no perfect solution to solve all problems at the same time. Therefore, in this paper, we analyzed several related security issues and possible solutions. Moreover, we proposed a method that could be applied to access control technologies, minimizing the disadvantages of each solution. We believe that understanding and utilization of various solutions will be necessary for the next blockchain application research.

Reference

[1] Satoshi Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008. https://bitcoin.org/bitcoin.pdf

[2] Heejung Kang, Hye Ri Kim and Seng-phil Hong, “A Study on the Design of Smart Contracts mechanism based on the Blockchain for anti-money laundering”. Journal of Internet Computing and Services (JICS), vol. 19, pp.1-11, 2018. https://doi.org/10.7472/jksii.2018.19.5.1

[3] Samsung SDS, “Samsung SDS Nexledger™ A Blockchain Platform and Solution,” 2017. https://www.samsungsds.com/global/en/solutions/off/nexledger/Nexledger.html

[4] David Galvin, “IBM and Walmart: Blockchain for Food Safety,” IBM Corporation, 2017. https://www-01.ibm.com/events/wwe/grp/grp308.nsf/vLookupPDFs/6%20Using%20Blockchain%20for%20Food%20Safe%202/$file/6%20Using%20Blockchain%20for%20Food%20Safe%202.pdf

[5] Asaph Azaria, Ariel Ekblaw, Thiago Vieira, and Andrew Lippman, “MedRec: Using Blockchain for Medical Data Access and Permission Management,” in 2016 2nd International Conference on Open and Big Data (OBD), pp.25-30, 2016. http://dx.doi.org/10.1109/OBD.2016.11

[6] Ariel Ekblaw, Asaph Azaria, John D. Halamka, and Andrew Lippman, “A Case Study for Blockchain in Healthcare:‘MedRec’ prototype for electronic health records and medical research data,” 2016. https://dci.mit.edu/research/blockchain-medical-records

[7] Deloitte, “Blockchain: Opportunities for health care,” 2016. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/public-sector/us-blockchain-opportunities-for-healt h-care.pdf

[8] Christian Esposito, Alfredo De Santis, Genny Tortora, Henry Chang, and Kim-Kwang Raymond Choo, “Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?,” IEEE Cloud Computing, vol.5, no.1, pp.31-37, 2018. http://dx.doi.org/10.1109/MCC.2018.011791712

[9] Kyong-jin Kim and Seng-phil Hong, “Privacy Information Protection Model in e-Healthcare Environment”. Journal of Internet Computing and Services (JICS), vol. 10, pp.29-40, 2009. http://search.koreanstudies.net/thesis/thesis-view.asp?key=3505451

[10] Chung-Sun Lee, Chang-won Jeong and Su-Chong Joo, “Design and Implementation of Process Management Model applying Agent Technology”. Journal of Internet Computing and Services (JICS), vol. 8, pp.57-70, 2007. http://www.koreascience.or.kr/article/JAKO200712242655887.page

[11] Karl Wüst and Arthur Gervais, ″Do you Need a Blockchain?,″ 2018 Crypto Valley Conference on Blockchain Technology, pp. 45-54, 2018. http://dx.doi.org/10.1109/CVCBT.2018.00011

[12] Damiano Di Francesco Maesa, Paolo Mori, and Laura Ricci. “Blockchain based access control.” International Conference on Distributed Applications and Interoperable Systems, pp.206-220, 2017. https://doi.org/10.1007/978-3-319-59665-5_15

[13] Aafaf Ouaddah, Anas Abou Elkalam, and Abdellah Ait Ouahman, “Towards a novel privacy-preserving access control model based on blockchain technology in IoT.” In Europe and MENA Cooperation Advances in Information and Communication Technologies, pp. 523-533, 2017. https://doi.org/10.1007/978-3-319-46568-5_53

[14] Meni Rosenfeld, “Overview of Colored Coins,” 2012. https://bitcoil.co.il/BitcoinX.pdf

[15] Guy Zyskind and Oz Nathan, “Decentralizing privacy: Using blockchain to protect personal data,” in Security and Privacy Workshops (SPW), pp.180-184, 2015. http://dx.doi.org/10.1109/SPW.2015.27

[16] Larimer, Daniel. "Delegated proof-of-stake (dpos)." Bitshare whitepaper, 2014. https://steemit.com/dpos/@dantheman/dpos-consensus-algorithm-this-missing-white-paper

[17] Kyle Croman, Christian Decker, Ittay Eyal, Adem Efe Gencer, Ari Juels, Ahmed Kosba, Andrew Miller, Prateek Saxena, Elaine Shi, Emin Gün Sirer, Dawn Song, and Roger Wattenhofer, “On Scaling Decentralized Blockchains (A Position Paper).” In 3rd Workshop on Bitcoin and Blockchain Research, 2016. https://doi.org/10.1007/978-3-662-53357-4_8

[18] Ittay Eyal and Emin Gün Sirer, “Majority is not enough: Bitcoin mining is vulnerable,” Communications of the ACM, vol.61, no.7, pp.95-102, 2018. http://dx.doi.org/10.1145/3212998

[19] Yi Liu, Xiayang Chen, Lei Zhang, Chaojing Tang and Hongyan Kang, “An Intelligent Strategy to Gain Profit for Bitcoin Mining Pools”, Computational Intelligence and Design (ISCID) 2017 10th International Symposium on, vol.2, pp.427-430, 2017. http://dx.doi.org/10.1109/ISCID.2017.184

[20] Mauro Conti, E. Sandeep Kumar, Chhagan Lal and Sushmita Ruj, “A Survey on Security and Privacy Issues of Bitcoin”, Communications Surveys & Tutorials IEEE, vol.20, no.4, pp.3416-3452, 2018. http://dx.doi.org/10.1109/COMST.2018.2842460

[21] Kartik Nayak, Srijan Kumar, Andrew Miller and Elaine Shi, “Stubborn Mining: Generalizing Selfish Mining and Combining with an Eclipse Attack,” 2016 IEEE European Symposium on Security and Privacy (EuroS&P), Saarbrucken, pp.305-320, 2016. http://dx.doi.org/10.1109/EuroSP.2016.32

[22] Dorit Ron and Adi Shamir. “Quantitative analysis of the full bitcoin transaction graph,” International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 2013. https://doi.org/10.1007/978-3-642-39884-1_2

[23] Ober, Micha, Stefan Katzenbeisser, and Kay Hamacher. “Structure and anonymity of the bitcoin transaction graph,” Future internet vo.5, no..2 pp.237-250, 2013. http://dx.doi.org/10.3390/fi5020237

[24] Greg Maxwell. “Coinjoin: Bitcoin privacy for the real world,” Bitcoin Forum, https://bitcointalk.org/index.php?topic=279249.0

[25] Shi-Feng Sun, Man Ho Au, Joseph K. Liu and Tsz Hon Yuen, “RingCT 2.0: a compact accumulator-based (linkable ring signature) protocol for blockchain cryptocurrency monero.” In European Symposium on Research in Computer Security, pp. 456-474, Springer, Cham. 2017. https://doi.org/10.1007/978-3-319-66399-9_25

[26] Shen Noether, “Ring SIgnature Confidential Transactions for Monero,” IACR Cryptology ePrint Archive, 2015:1098, 2015. https://eprint.iacr.org/2015/1098.pdf

[27] Courtois, Nicolas T., and Rebekah Mercer. “Stealth Address and Key Management Techniques in Blockchain Systems.” In Proceedings of the 3rd International Conference on Information Systems Security and Privacy, pp.559-566, 2017. http://dx.doi.org/10.5220/0006270005590566

[28] Joseph Poon and Thaddeus Dryja, “The bitcoin lightning network.”, 2016. https://lightning.network/lightning-network-paper.pdf

[29] Christian Decker and Roger Wattenhofer, “A fast and scalable payment network with bitcoin duplex micropayment channels.” In Symposium on Self-Stabilizing Systems, pp.3–18. Springer, 2015.

https://doi.org/10.1007/978-3-319-21741-3_1
[30] Conrad Burchert, Christian Decker and Roger Wattenhofer, “Scalable Funding of Bitcoin Micropayment Channel Networks,” International Symposium on Stabilization, Safety, and Security of Distributed Systems, 2017.
http://dx.doi.org/10.1098/rsos.180089
[31] Maurice Herlihy, “Atomic cross-chain swaps,” Proceedings of the 2018 ACM Symposium on Principles of Distributed Computing. ACM, 2018.
http://dx.doi.org/10.1145/3212734.3212736
[32] Johnny Dilley, Andrew Poelstra, Jonathan Wilkins, Marta Piekarska, Ben Gorlick, and Mark Friedenbach, “Strong Federations: An Interoperable Blockchain Solution to Centralized Third Party Risks.” arXiv preprint arXiv:1612.05491, 2016.
https://arxiv.org/pdf/1612.05491.pdf
[33] “Cosmos Network - Internet of Blockchains,” Cosmos Network. https://cosmos.network/
[34] Gavin Wood, “Polkadot: Vision for a heterogeneous multi-chain framework,” White Paper, 2016.
https://polkadot.network/

◐ 저 자 소 개 ◑

노 시 완(Siwan Noh)
2016년 부경대학교 IT융합응용공학과(공학사)
2018년 부경대학교 대학원 정보보호학협동과정(공학석사)
2018년~현재 부경대학교 대학원 정보보호학협동과정 박사과정
관심분야 : 정보보호, 블록체인 보안
E-mail : nosiwan@pukyong.ac.kr

이 경 현(Kyung-Hyune Rhee)
1982년 경북대학교 수학교육과(이학사)
1985년 한국과학기술원 응용수학과(이학석사)
1992년 한국과학기술원 수학과(이학박사)
1985년~1993년 한국전자통신연구원 연구원, 선임연구원
1993년~현재 부경대학교 IT융합응용공학과 교수
관심분야 : 정보보호, 암호이론, 암호 프로토콜, 통신보안
E-mail : khrhee@pknu.ac.kr