International Journal of Security and Its Applications
Vol. 10, No. 11 (2016), pp.201-210
http://dx.doi.org/10.14257/ijsia.2016.10.11.18

Study on Rule-based Data Protection System Using Blockchain in P2P Distributed Networks

Kyong Jin Kim[1] and Seng Phil Hong[2]*

[1]*Dept. of Computer Science, Graduate School, Sungshin Women's University*
[2]*School of Information Technology, Sungshin Women's University,*
[1]*kyongjin@sungshin.ac.kr,* [2]*philhong@sungshin.ac.kr*
**Corresponding author*

Abstract

The blockchain is new revolutionary paradigm for the world, but the privacy and confidentiality are still issues. This study is focused on the technical securities to provide a blockchain service on a foundation of trust. We suggested the rule-based data protection system that is to provide authorize rules used in mechanism, to control an access users without intermediaries on the blockchain. We have developed a scenario of an application a smart contract based on the suggested system and simulated it.

Keywords*: Blockchain, Data Protection System, P2P Distributed Networks*

1. Introduction

A number of global companies have begun to expand the full-scale research and investment about the blockchain that is the most recognizable trend technique today. The definition of this technique is being mentioned in many ways, and in short it is distributed digital legders that make the contents public to every dealings participant.

Applying technology operates by the blockchain, distributed trading ledger without particular dealing management agency, unlike the existing dealing way of storing the records at central server, so private enterprises as well as financial authorities has begun to research to the full-scale introduction of the blockchain technology for its advantage that could cut off hacking with low system maintenance costs. In other words, when users request for a transaction in a P2P distributed environment, it creates a block with dealing records and sends the block to all participants on network, and after it completes the transaction as adding the dealing records on the existing blockchain[1,4].

So it is likely to be safer relatively since it is impossible for the hackers to hack the blockchain of network participants from all over the world at the same time to modify or operate memory hacking with this kind of process. Business wise it is presumed to be able to reduce the costs since safe financial transactions at low costs without having center network like before when it is applied to the real environment, because it operates by P2P distributed mode. Also consumers using the service could expect many advantages such as speed improvement, reduced fee as well as more convenient service for published dealing information. As compared with this trend, however, there coexists many kinds of problem with the blockchain technique yet[2,8,10]. First, quite amount of time, source and efforts are needed to use the advantage of the blockchain, especially in institutional terms, an active support for the application of the blockchain technique from regulatory agency would be necessary. That is to say that the application level of the blockchain may be different according to the law and regulation of each country. It is one of the reason that our technique of reaction to the blockchain is at an early stage yet compared to overseas country. Besides institutional issues, transactions with the blockchain technique need to review in advance about ways to provide steady service as compatible to the existing computer system. The key functional role of the blockchain is providing

ISSN: 1738-9976 IJSIA

distributed books as a kind of financial book with the new database technique that records digital records [7,11]. Of course it is difficult to operate the dealing records in a block effectively, issues about possibilities of double payment based on 51% of attack, triggering branching on purpose, DoS attack to certain transaction or address, *etc*. still exist in posse due to the structural characteristics of the blockchain, although it carries high security level as cutting off memory hacking.

In the research purpose, we propose a secure system for data sharing using smart contract on the blockchain. The rest of this paper is organized as follows. In Section 2, we briefly describe the background of the blockchain and outline some related works and technologies. Section 3 discusses security concerns related to the blockchain. Section 4 introduces our system for sharing and accessing securely on the blockchain, which incorporates three mechanisms for data protection, and we present a complying protocol-based scenario by leveraging the usability of our system. For performing this idea, Section 5 represents a simulation. Finally, in Section 6 we conclude and discuss some ideas for future research work.

2. Background and Related Technologies

The blockchain data structure is a secure record of historical transactions in distributed environment, so it should be applied to be various techniques. This research introduces the most representative technologies, chaning and consensus mechanism[6,9].

The chaning technology is an ordered, linked list of blocks of transactions, each block is chained to the next block, using a cryptographic hash function, each referring to the previous block in the chain. And this technology ensures tamper proof mechanism of the blockchain. It is important to verify to assemble a chain by connecting the block to the existing blockchain. The chaning technology would be connected through a number of different consensus mechanisms. There are a lot of ways to corroborate the accuracy of a ledger for selecting the greatest-difficulty chain. The consensus mechanism is the assembly of blocks into chains and the selection of the chain with the Proof of Work (PoW), the Proof of Stake (PoS) and the consensus by bet. These technologies ensure that valid transactions are propagated across the network, and the distributed ledgers could has the potential to improve the speed and transparency.

Table 1. Typical Transaction Algorithms for Blockchain

Method	Concept	Type	Coin
PoW	- Nodes are required to solve a computationally difficult problem to ensure the validity of the newly mined block. - So the computational power can win the reward and create a block, - And the new block is linked that chain.	Public	Bitcoin, Etereum
PoS	- Probability to create a block and receive the associated reward is proportional to a user's ownership stake. - Individuals who has probability fraction of the total number of coins in circulation creates a new block	Public	Ethereum, Blackcoin, Peercoin
Consensus by bet	- Protocol offers opportunities for validators to bet against the protocol on which blocks are going to be finalized.	Consortium or Private	Tendermint, Casper

3. Security Concerns on Blockchain

The blockchain technology is suggested as solving to the security problems in banking especially. All transfers (and events) are recorded in a secure and verifiable form using mathematical techniques based on cryptography algorithms. And these records are permanent with copies of the blockchain scattered all over the global infrastructure. It is to protect the integrity.

However recent events in the world have shown that the blockchain technology is vulnerable to security problems. For example, the DAO, the Decentralized Autonomous Organization, was stolen $55 million in June[14]. The attackers exploited a weakness in the program code in the DAO underlying the blockchain. As a matter of fact, it was not hacked, just a bad design. In August attackers also hacked $72 million worth of Bitcoin from accounts at the Hong Kong cryptocurrency exchange Bitfinex[13]. Ethereum network was recently attacked by the EXTCODESIZE opcode, that is a computational DDoS[5]. The attack transactions were calling this opcode roughly 50,000 times per block. Because of this, miners and nodes needed to take as long as 60 seconds to validate processing some blocks. These situation raises questions about the extent to which the blockchain can improve security and privacy. As shown in Table 2, it represents security exposures inherent in applying the blockchain technology.

Table 2. Potential Risk Factors on Blockchain Technology

Category	Risk factors	Seriousness	Vulnerability
Managerial issues	Private key leakage caused by the management insufficiency	Very high	Very high
Technological issues	Forged or falsified record	High	Low
	Malware	High	High
	DDoS attack	High	Low
	51% cartel attack	Low	Low
Physical issues	Cracking the digital currency exchange	Very high	Very high
	Stolen or lost private key	Very high	Very high

According to the study survey[15] about the distributed ledger security concerns, interested parties including bankers and financial execs were worried first about other banks seeing their transactions, then about the security of the transactions themselves. That is because the blockchain is not considered to be confidential. Anyone is keen on releasing all of transactions onto a public ledger without restrictions. So this environment is easier to be threatened to expose and hack them.

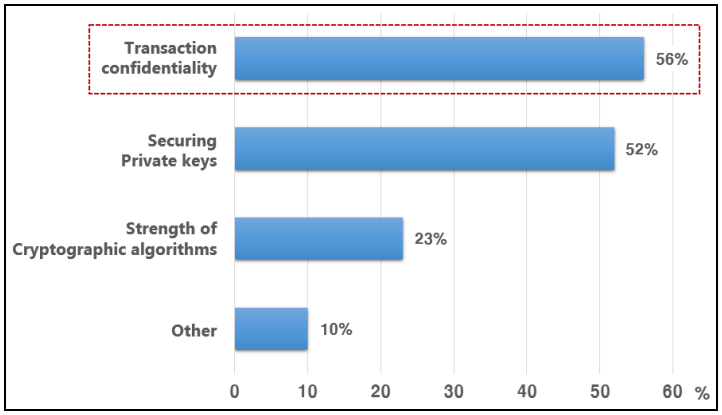

Figure 1. Security issues on Blockchain Technology

In this paper, we suggest to the idea using a smart contract[12] that the system on the blockchain will solve security issues.

4. Rule-based Data Protection System on Blockchain

4.1. Overview Architecture

The blockchain is a network-based open record system, and the information does not converge on certain server, instead the same data, that is called block, is saved in the computers of network participants, the node. This study makes sure to dualize the public record and classified information, and the link to exchange data in secured environment with encoded communication environment, namely the application, in order to provide safe the blockchain service on a foundation of trust as shown in Figure 2. In this kind of structure, once **Owner-A** creates data to use the service and agrees to share his/her own data, the classified information such as private information is removed from the information, and the pseudonymous address is added to record it as encoded information. After this system is on the blockchain, a third party besides **Owner-A** gets the access. Given the right to access the shared data in certain condition, the **Requestor-B** can have access to the owner's data, and all of these access event is recorded publically on the blockchain as occurring transaction.

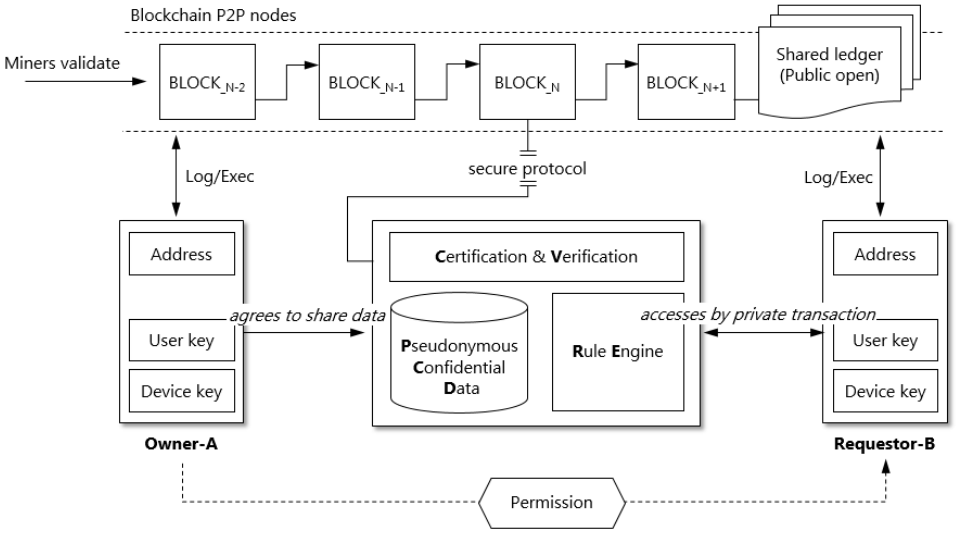

Figure 2. Overview Architecture

This kind of mechanism process guarantees individual rights as well as data integrity by allowing **Owner-A** him/herself to see how his/her data is being processed. In other words, it guarantees privacy of Owner-A as well as protection for the shared information as providing them the right to control his/her own data. More specific mechanisms are shown below.

1) Certification & Verification Mechanism (CVM)

When the participants of the blockchain creates wallet or access to make an account, *address* is created as well as *userKey*/*deviceKey* as a pair. This system can figure out whom this information belongs to through the *address*, and CVM identifies who is accessing. Then it verifies that the identifier is correct with *user's private key*. *Private key* is the only value that verify the owner or requester, and it checks the validity of accessor as being verified by many nodes of the blockchain as signing with *private key*.

Verification of device is also performed integration work in case of owner. **Owner-A** tightens up access security to protect his/her privacy with multi-factor identification that selectively uses authentication methods such as certificate verification, biometric recognition, ID/PW, *etc*. that he/she could own, as well as encrypted code of device identification number(*e.g.,* UUID, Mac Address) in use. This could generate *device's private key* and *public key* for owner. In this process, all the authentication and access attempts by **Requestor-B** for information are recorded as transaction of the blockchain, and they go through integrity verification from majority nodes of the blockchain network to guarantee not being forged.

2) Rule Engine Mechanism (REM)

When user authentication is valid, they receive a permission entry to the information as Role-based Access Control (RBAC) through REM. The definition of roles here is used to identify user's right to have access to the certain information or service as considering occupation, position, field, *etc.* of the ordinary user. This mechanism is constructed as role-based access control[3] that applies to the network environment, and it gives right to access the information as identifying the accessor to the information, namely users, with role. In order to identify role, CVM allocates user's role after identifying who it is through verification. It prevents dark-side hacker primarily as identifying the role like this. The structure of RBAC consists of the elements of $\{u, r, s\}$ and the relationship of $\{(u, r) \in UA$ and $(r, s) \in SA\}$. A user u could be accessor through the blockchain network as elements such as user, who is trying to access to the information, computer, agent, *etc*. r stands for role, and allocating u to r can be expressed as $(u, r) \in UA$, and at this, r is classified as user, requestor (by accessing level), and a third party with no permission to access. Next, a service s is the data that owner put on with the information saved in ledger, including information about protected private data as well as public data that could be shown. Also it includes a permission p, which is the right to access. At this, r getting access to s could be expressed as $(r, s) \in SA$. In addition, a constraints c is included as an element of RBAC, and it allows to use information after identifying the conditions of purpose, limitation, *etc*. in approach to the information. r allocates users as classifying with hierarchy, and allows s to have access in line with condition c. In other words, $(r, c_i) \in RC_i$, *where* $c_1, ..., c_n$ defines role after what the limited condition is in allocating users to role, and $(u, r, c_i) \in UAC_i$ means allocating users to appropriate roles. Also it provides access control between users and service according to the limited condition as $(r, c_i, s) \in SAC_i$ when allocated users to the role trying to use the service. In this kind of relationship, allowable authority is given to user after owner receiving an agreement by opt-in about use of information, and it assigns user authority in limited time, and makes sure to have access with authority granted when trying to use it again when the information is need, even if it was used in the past.

3) Pseudonymous Confidential Database

Users own digital wallet that accounts for saving and creating private key as well as public address. Digital wallet, means of using among network users, send blocks from encoded a protocol, and all the events originating such as transmission, creation, remittance, *etc*. are recorded as distributed books that anyone can see in the blockchain as safe transactions. But in case of information being uploaded that is private and not to go public, the information is encoded through user's address and it is recorded in Pseudonymous Confidential Database with the encoded address. This allows one to gain ownership of user's data as it controls use of data through access control of REM, putting one's own information as assets.

4.2. Proposed Approach Flows and Algorithms

Figure 3 shows the overall structure of the proposed model to protect the asset. In this case, the blockchain would record registering the asset and the proposed model could provide protecting it against any unauthorized user who attempt to watch.

As can be seen, in this scenario example, the owner has registered a property on the blockchain. And then owner has developed the pseudonymous address and key pairs for protecting registry of a property. The proposed system establish the rules based on set of owner's constraints. When a user *u* wants to access the asset, it will only be granted access to the asset if owner allow it.

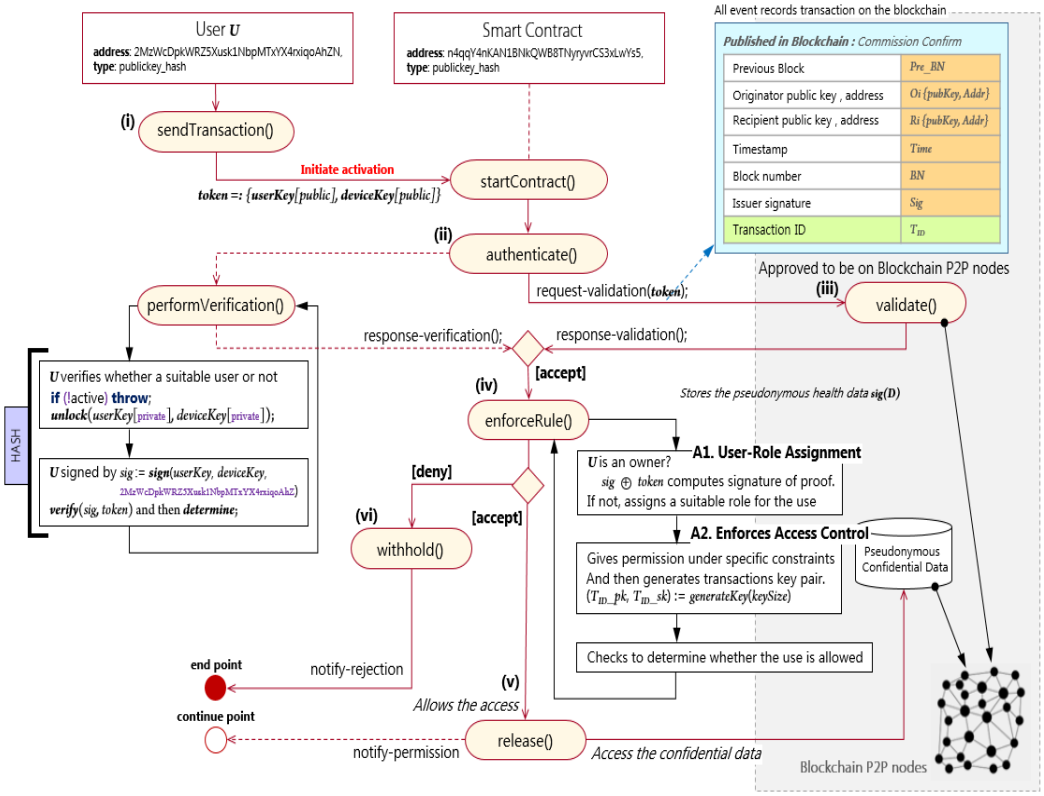

Figure 3. Complying Proposed System based Scenario

i) *u* carry out CVM to the proposed smart contract by sending digital currency as a start event. After CVM verifies u that could use smart contract as an identification mechanism, ii) contract provides strengthened certification by carrying out device verification as well as user verification. iii) All verification and/or access attempts from requestor for the information as well as events originating are recorded as transaction of the blockchain. Once they know who this is through this process, iv) it provides Role-based authority to give users limited use after operating REM for granting information use. If the information being accessed is general or public information, v-vi) all the blockchain network participants have access to it, but in case of sensitive information included in assets, only limited ones get the access to it through a strong access control. Information on the existing blockchain could guarantee its integrity as it goes public, even the transactional information, but it was an issue not to assure confidentially. To redeem this, giving ownership that provides information access authority about private and/or sensitive information included in asset information to users can provide the blockchain-based stability of privacy. Access control makes it only possible for owner to modify, add and delete the defined rules.

A1: User-Role-Assignment for REM

```
Input: A user u_i, and a constraint of user c_i
Output: A role, r_j
/* u's userKey and deviceKey */
if u_i ∉ U then
    throw;
else
    if u_i is verified and u_i owns Sign(u_i.userKey, u_i.deviceKey) then
        r_j ← Role-Assign(u_i, OWNER);
    else
        if c_i = R_Ci then
            r_j ← Role-Assign(u_i, GROUP);
        else
            r_j ← Role-Assign(u_i, ANONYMOUS);
return r_j;
```

Mechanisms mentioned above shows the algorithm **A1**. After verifying primarily through user identification, user-role assignment algorithm allocates *u* to OWNER role with all authorities if *u* is the owner of asset, and if *u* is not the owner, it examines constraints *c* and allocates them to the appropriate roles such as $GROUP_{1..N}$, ANONYMOUS. In other words, role assignment can protect the information as control the access primarily the private or sensitive information that is not to be public on the blockchain, which opens all the information to the network participants or accessors.

A2: Role-Service-AccessControl for REM

```
Input: A user u_i, a constraint of user c_i, and a service s_j
Output: A constant variable, access-result
/* access-result can involve ACCEPT, RESTRICT, DENY */
/* userKey[public] and deviceKey[public] are owner's data relate to general and public */
/* userKey[private] and deviceKey[private] are owner's data relate to individual and sensitive */
if C = ∅ or User-Role-Assignment(u_i) = OWNER then
    access-result ← ACCEPT;
else
    foreach c_i ∈ C do
        if c_i = R_Ci then
            if u_i owns s_j.userKey then
                access-result ← Role-Right-Check(u_i, RESTRICT);
                With owner's informed consent, s_j(userKey[private], deviceKey[private]) can
                    permissions(access, read);
            else
                access-result ← DENY;
                But s_j(userKey[private]) can permissions(access, read);
        else
            access-result ← DENY;
return access-result;
```

In **A2** shown, after assigning *u* to *r*, role-service access control examines constraints to verify if *u* is accessible, and allocates the appropriate to the calculation that fits to accessibility, if the information includes sensitive ones to the data on the blockchain when *u* trying to access it. If *u* is OWNER when using asset, it guarantees the integrity that allows *u* to see all the information, and gives the owner the ownership to their private information.

5. Prototype and Simulation

As we mentioned earlier, security and privacy on the blockchain are a major issue as it deals with confidential data or operative. The blockchain with various security technologies such as some biometrics, token-based, or password system should be considered as the important factors that affect the performance. In this paper, we have

proposed a security method to protect the assets and we have indicated a practice using a smart contract.

In order to simplify the testing environment, we could install a private testnet on a blockchain and develop a proposed application using a smart contract. For operating in a simulated environment, the major server, which could be installed and developed, is implemented in the Windows 10 operating system, and the development language of server is Go 1.4 based on Geth 1.4. And then the proposed system, which provides to protect for the assets, is used to implement an application using Solidity.

This process involves ***transaction*** that is generated and updated on a blockchain. With this the performance method can be useful for calculating the response time through log messages and transaction blocks.

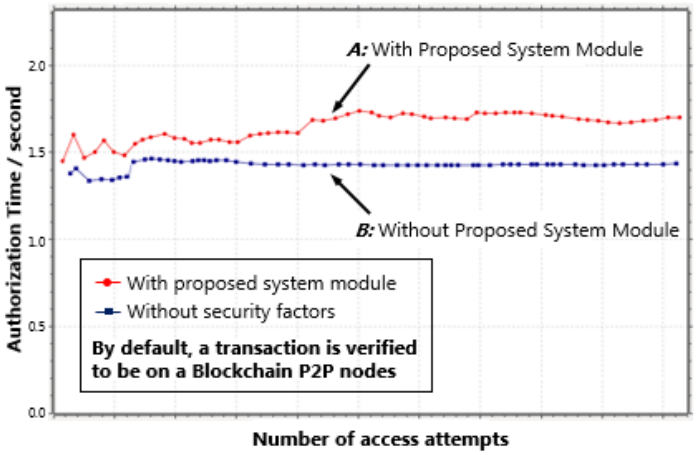

Figure 4. Comparison and Simulation Graph

The Figure 4 represents the results of the time taken depending on the users' authentication overhead. Two systems both graph A and B are performed by the same simulation environment using a smart contract, so all generated transactions are verified by default to be on the blockchain P2P nodes. Instead, there are a difference between applying security factors and nothing. Graph A is using the proposed system, and graph B is the general system including a basic process. As shown in the graph, there is a slight difference in time performance. Through this performance result, the proposed system could ensure not only enhanced security but also performance. It will be really not much different from the change in the blockchain even if enough resources are available. Thus, the proposed system is a very effective way to protect assets and to reduce threats.

6. Conclusion

Distributed ledger technology, also called the blockchain, is new trend in finance area. This trend can lead to be apparent in the growth of the less formal sharing economy. The good thing can be to achieve data and transaction transparency, but privacy and confidentiality are important issues.

This study is focused on the technical securities from among these to provide the blockchain service on a foundation of trust. We introduce the rule-based data protection system to share and access data safely on the blockchain. The proposed system should perform consolidated authentication for verifying users or accessors, and it support the access control for protecting confidential data. We suggested a scenario based on proposed system that can upload Smart Contract that shares asset information to the blockchain to operate safely. And we have prototyped and performed the simulation to find out the impact. The result showed that our system could ensure not only enhanced

security but also performance. Future research will focus on the smart contract because it will be very useful in the realm of various industry.

Acknowledgments

This work was supported by the Sungshin University Research Grant of 2016.

References

[1] J. P. Cruz and Y. Kaji, "The Bitcoin Network as Platform for Trans-Organizational Attribute Authentication", Proceedings of the International Academy, Research, and Industry Association, **(2015)**, pp. 29-36.
[2] T. Hardjono and N. Smith, "Cloud-Based Commissioning of Constrained Devices using Permissioned Blockchains", Proceedings of the International Workshop on IoT Privacy, Trust, and Security, **(2016)**, pp.29-36.
[3] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-based access control models", IEEE Computer, vol. 29, no. 2, **(1996)**, pp. 38–47.
[4] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," URL: https://bitcoin.org/bitcoin.pdf, **(2008)**.
[5] J. Young, "Ethereum is Under DDoS Attack, Miners are Alerted", URL: https://cointelegraph.com/news/ethereum-is-under-ddos-attack-miners-are-alerted, **(2016)** September 25.
[6] D. Mazie'res, "The Stellar Consensus Protocol: A Federated Model for Internet-level Consensus," Draft URL: http://citeseerx.ist.psu.edu/, **(2016)**.
[7] J. Young, "Ethereum Classic Attack Pool Under DDoS Attacks", URL: http://www.livebitcoinnews.com/ethereum-classic-attack-pool-under-ddos-attacks/, **(2016)** August 1.
[8] C. Decker, J. Seidel and R. Wattenhofer, "Bitcoin meets strong consistency", Proceedings of the 17th International Conference on Distributed Computing and Networking, **(2015)** December.
[9] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf and S. Capkun, "On the Security and Performance of Proof of Work Blockchains", Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, **(2016)** October, pp.3-16.
[10] G. Karame, "On the Security and Scalability of Bitcoin's Blockchain", Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, **(2016)** October, pp.1861-1862.
[11] S. Underwood, "Blockchain beyond bitcoin", Communications of the ACM, vol. 59, no. 11, **(2016)**, pp. 15-17.
[12] L. Luu, D.-H. Chu, H. Olickel, P. Saxena and A. Hobor, "Making Smart Contracts Smarter", Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, **(2016)** October, pp.254-269.
[13] S. Gibbs, "Bitcoin worth $78m stolen from Bitfinex exchange in Hong Kong", URL: https://www.theguardian.com/technology/2016/aug/03/bitcoin-stolen-bitfinex-exchange-hong-kong, **(2016)** August 3.
[14] K. Dotson, "Ethereum DAO attacked, over $55 million of Ether cryptocurrency stolen", URL: http://siliconangle.com/blog/2016/06/17/ethereum-dao-attacked-over-55-million-of-ether-cryptocurrency-stolen/, **(2016)** Jun 17.
[15] P. Crosman, "Does Blockchain Tech Solve Security Problems or Cause New Ones?", URL: http://www.americanbanker.com/news/bank-technology/does-blockchain-tech-solve-security-problems-or-cause-new-ones-1090801-1.html, **(2016)** August 18.

Authors

Kyong-jin Kim, she graduated with a B.S. in 2007, with a M.S. in 2009 and with a Ph.D. in 2013 from the Sungshin Women's University. She joined the Information Security lab as a postdoctoral fellow in March 2013. Her research interests focus on privacy protection, security framework, and access control.

Seng-phil Hong, he received his BS degree in Computer Science from Indiana State University, and MS degree in Computer Science from Ball State University at Indiana, USA. He researched the information security for Ph.D at Illinois Institute of Technology from 1994 to 1997, He joined the Research and Development Center in LG-CNS Systems, Inc since 1997, and he received Ph.D. degree in computer science from KAIST University in Korea. He is actively involved in teach and research in information security at Sungshin Women's University, Korea. His research interests include access control, security architecture, Privacy, and e-business security.