symmetry

MDPI

Article

# Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions

**Jin Ho Park [1] and Jong Hyuk Park [2,*]**

[1] Department of Computer Science, School of Software, SoongSil University, Seoul 06978, Korea; j.park@ssu.ac.kr

[2] Department of Computer Science and Engineering, Seoul National University of Science and Technology, (SeoulTech) Seoul 01811, Korea

* Correspondence: jhpark1@seoultech.ac.kr; Tel.: +82-2-970-6702

Received: 29 June 2017; Accepted: 1 August 2017; Published: 18 August 2017

**Abstract:** Blockchain has drawn attention as the next-generation financial technology due to its security that suits the informatization era. In particular, it provides security through the authentication of peers that share virtual cash, encryption, and the generation of hash value. According to the global financial industry, the market for security-based blockchain technology is expected to grow to about USD 20 billion by 2020. In addition, blockchain can be applied beyond the Internet of Things (IoT) environment; its applications are expected to expand. Cloud computing has been dramatically adopted in all IT environments for its efficiency and availability. In this paper, we discuss the concept of blockchain technology and its hot research trends. In addition, we will study how to adapt blockchain security to cloud computing and its secure solutions in detail.

**Keywords:** blockchain; computer security; bitcoin; authentication; cloud computing

## 1. Introduction

With the need for next-generation financial technology recently increasing, there have been active studies on blockchain for the secure use of electronic cash by communicating solely between peers and without the involvement of third parties. A blockchain is the public ledger for transactions and it prevents hacking during transactions involving virtual cash. As a type of distributed database and a data record list that continuously grows, it is designed to disable arbitrary tampering by the operator of distributed peers. Transaction records are encrypted according to a rule and operated in computers that run the blockchain software. Bitcoin is an electronic currency using blockchain technology [1].

Using blockchain can provide higher security compared to storing all data in a central database. In the data storage and management aspect, damage from attacks on a database can be prevented. Moreover, since the blockchain has an openness attribute, it can provide transparency in data when applied to an area requiring the disclosure of data. Due to such strengths, it can be utilized in diverse areas including the financial sector and the Internet of Things (IoT) environment and its applications are expected to expand [2–6].

The blockchain finalizes a transaction record through the work authentication process, when a person who loans electronic cash forms a block by combining the transactions over the network. The hash value is then generated by verifying it and connecting the previous block. This block is periodically updated and reflected on the electronic cash transaction details to share the latest transaction detail block. This process provides security for the transaction of electronic cash and allows the use of a reliable mechanism [7–9].

Cloud computing has been applied to many IT environments due to its efficiency and availability. Moreover, cloud security and privacy issues have been discussed in terms of important security elements: confidentiality, integrity, authentication, access control, and so on [10].

In this paper, we seek to investigate the definition and base technology of blockchain and survey the trend of studies to date to discuss areas to be studied, considering cloud computing environments. In addition, we discuss the considerations for blockchain security and secure solutions in detail.

This paper studies the blockchain technology and surveys the blockchain by analyzing generic technology and research trends and discusses the solution for using bitcoin safely as well as future study areas. The results of this research can serve as important base data in studying blockchain and will aid in understanding the known security problems thus far. We can foster the development of future blockchain technology by understanding the trend of blockchain security.

The rest of this paper is organized as follows. In Section 2, we discuss related works including the basic concept of blockchain and bitcoin as a use case. Section 3 presents a detailed discussion and survey on the security considerations for blockchain including the settlement of blockchain, the security of transaction, the security of wallet, and the security of software. In Section 4, we discuss blockchain security case studies—authentication, security incidents, and 51% attack—and improve the blockchain. Section 5 proposes secure solutions for the blockchain in cloud computing in detail. Finally, we conclude our study in Section 6.

## 2. Related Works

In this section, we discuss the basic concept of blockchain and the existing research. We also study the specific use of blockchain in bitcoin.

### *2.1. Blockchain*

A blockchain is the technology that allows all members to keep a ledger containing all transaction data and to update their ledgers to maintain integrity when there is a new transaction. Since the advancement of the Internet and encryption technology has made it possible for all members to verify the reliability of a transaction, the single point of failure arising from the dependency on an authorized third party has been solved.

The blockchain has broker-free (P2P-based) characteristics, thereby doing away with unnecessary fees through p2p transactions without authorization by a third party. Since ownership of the transaction information by many people makes hacking difficult, security expense is saved, transactions are automatically approved and recorded by mass participation, and promptness is assured. Moreover, the system can be easily implemented, connected, and expanded using an open source and transaction records can be openly accessed to make the transactions public and reduce regulatory costs [11].

The blockchain is a structured list that saves data in a form similar to a distributed database and is designed to make arbitrarily manipulating it difficult since the network participants save and verify the blockchain. Each block is a structure consisting of a header and a body. The header includes the hash values of the previous and current blocks and nonce. The block data are searched in the database using the index method. Although the block does not contain the hash value of the next block, it is added as a practice (Figure 1) [12].

Since the hash values stored in each peer in the block are affected by the values of the previous blocks, it is very difficult to falsify and alter the registered data. Although data alteration is possible if 51% of peers are hacked at the same time, the attack scenario is realistically very difficult.

Public, key-based verification and a hash function that can be decrypted are both used to provide security in the blockchain. The ECDSA (Elliptic Curve Digital Signature Algorithm) electronic signature algorithm, which verifies the digital signature generated during a transaction between individuals, is used to prove that the transaction data have not been altered.

Although using an anonymous public key as account information enables one to know who sent how much to another peer, it still ensures anonymity since there is no way of finding information pertaining to the owner [13–15].

The hash function is used to verify that the block data containing the transaction details are not altered and to find the nonce value to get a new block, as well as to guarantee the integrity of

transaction data during a bitcoin transaction. The integrity of the transaction details can be verified through the public key-based encryption of the hash value of the transaction data. Moreover, using the root hash value, which accumulates the hash value of each of the transaction details, enables easy determination of whether the bitcoin data were altered since the root hash value is changed when the value is changed in the process [16,17].

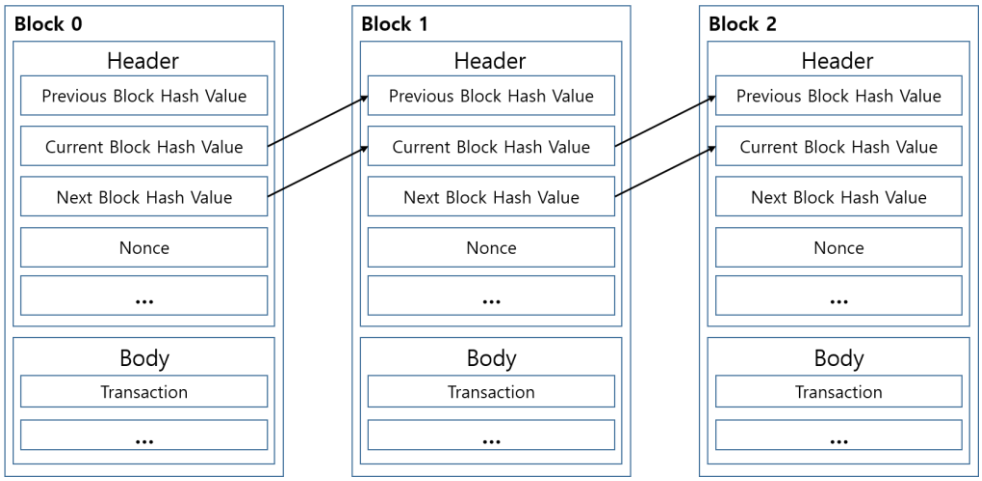


**Figure 1.** Blockchain connection structure.

There are many ongoing studies to strengthen security using these characteristics of blockchain. The most important part of the blockchain is security related to the personal key used in encryption and there are studies on how to protect the personal key. An attacker attempts a "reuse attack" and other attacks to obtain the personal key stored in a peer's device in order to hack the bitcoin. The attacker can hack the bitcoin since the data may be leaked if the attacker can obtain the personal key. To solve this problem, studies on applying both hardware and software securities for approving transactions are ongoing [18].

Bitcoin is very vulnerable to infection by malware since it is often traded in widely used devices such as peers' PCs or smartphones. The malware penetrating through various paths such as e-mail, USB, or apps with poor security must be detected and treated since it can infect a peer's device. The need for security is growing, particularly in trades of items used in games since many of them use bitcoins. As such, there have been studies on detecting and treating malware in the game environment [19].

One of the strengths of bitcoin is that it is difficult to falsify and alter the ledger because so many peers share the transaction ledger. Since it takes the data recorded in the majority of ledgers, hacking is practically impossible unless the attacker alters and falsifies 51% of all peers' ledgers, even if the data of some ledgers are altered. Still, there are concerns that 51% of the ledgers can be falsified and altered simultaneously considering increasing computing power and there are studies suggesting the intermediate verification process or design of the verification process in order to solve the problem.

### *2.2. Bitcoin*

Bitcoin is the digital currency proposed by Satoshi Nakamoto in 2009 to allow transactions between peers without a central authority or a server to issue and manage the currency. Bitcoins are traded with the P2P-based distributed databases based on public-key cryptology. Bitcoin is one of the first implementations of cryptocurrency in 1998 [20].

The bitcoin transaction information is disclosed over the network such that all peers can verify it and so currency issuance is limited. The peers participating in the network have the same blockchain and the transaction data are stored in blocks in the same way as the distribution storage of transaction

data. Although there are many threats involved in electronic transactions, bitcoin can be technically implemented to cope with them. For example, a person attempting to generate a falsified receipt record from another person's account to his or her own account can be blocked by verifying it with the sender's personal key. If multiple parties intend to use a bitcoin at the same time, the chain that loses in the competition between peers will be eliminated.

The most basic components of a bitcoin are the bitcoin address where the bitcoin belongs, the transaction showing the flow of bitcoin between the addresses, and the block where the transaction is confirmed by the bitcoin peers. The key to the bitcoin process is the bitcoin transaction, which shows the input containing the bitcoin and the bitcoin address as the output. While banking is the process wherein some of the money in an account moves to another account, a bitcoin transaction requires all bitcoins in an input to be transferred to the output and the inputs and outputs need not be singular.

The electronic currency used in bitcoins consists of a chain of electronic signatures (Figure 2). The coins of an owner are transferred to the next chain with the hash value of the previous transaction and the electronic signature is transmitted to the public key of the next owner. The recipient can check the signature to confirm the ownership chain. In the process, a problem arises: the recipient is not able to ensure that one of the owners has not used the coin(s) multiple times. A reliable central authority is introduced to check all transactions of double use to address this problem [21].

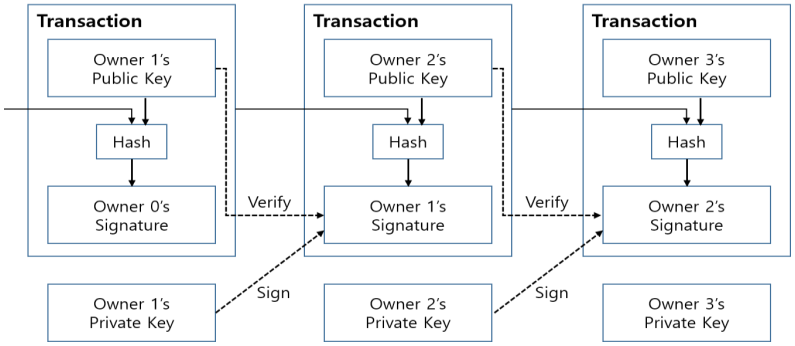


**Figure 2.** A bitcoin transaction.

## 3. Consideration for Blockchain Security: Challenges

Blockchain technology has been implemented or realized as cyber money and is actually used. Note, however, that various security issues occurring in blockchain agreement, transaction, wallet, and software have been reported. This paper checks the trends of security issues raised to date and the security level of the current blockchain. We think this attempt is very important as the results can serve as base data for developing future blockchain technology and supplementing security.

### *3.1. Settlement of Blockchain*

Although there should only be one blockchain since it is the sequential connection of generated blocks, a blockchain may be divided into two because the two latest blocks can be generated temporarily if two different peers succeed in mining the answer for generating the block at the same time. In such case, the block that is not chosen as the latest block by the majority of peers in the bitcoin network to continue mining will become meaningless. In other words, the bitcoin will follow the majority of peers who have 50% or more mining capability (operating capability). Therefore, if an attacker has 51% mining capability, a "51% Attack", wherein the attacker has control of the blockchain and he/she can include falsified transactions, can be a problem. According to a study, an attacker can realize illegal gain with only 25% operating capability through a malicious mining process instead of 51%. Since the current operating capability of the whole bitcoin network is already high gaining meaningful operating capability is considered to be difficult. Nonetheless, mining pools—the associations of

mining peers—have been actively mining to increase the probability of mining. Thus, this risk has become an issue. Recently, GHash, a leading mining pool, temporarily exceeded the 50% threshold, forcing the bitcoin community to go through internal and external adjustments to cope with the risk. In particular, the possibility of dominating the blockchain is related to the basic security of the bitcoin and such security threats have temporarily affected the economic factors because of the characteristics of the bitcoin, which is always closely related to the market price [22,23].

### 3.2. *Security of Transaction*

Since the script used in inputs and outputs is a programming language with flexibility, different transaction forms can be created using such. A bitcoin contract [11] is a method of applying bitcoin for the existing authentication and financial service. A widely used method involves creating the contract using the script that includes a multiple-signature technique called multisig. Although the scripts are used to solve a wide range of bitcoin problems, the possibility of an improperly configured transaction has also increased as the complexity of the script increases. A bitcoin using an improperly configured locking script is discarded since nobody can use it as the unlocking script cannot be generated. To this end, there are studies that suggest models of bitcoin contract-type transactions to verify the accuracy of a script used in a transaction [24].

### 3.3. *Security of Wallet*

The bitcoin address is the hash value of a public key encoded with a pair of public and personal keys. Therefore, the locking script of a bitcoin transaction with an address as output can be unlocked with an unlocking script that has the value signed with the public key of the address and the personal key. The bitcoin wallet stores information such as the personal key of the address to be used for the generation of the unlocking script. It means that loss of information in the wallet leads to a loss of bitcoin since the information is essential for using the bitcoin. Therefore, the bitcoin wallet has become the main subject of bitcoin attack through hacking [25].

To assure the security of the bitcoin wallet, services have introduced multisig for multiple signatures. Since multisig only allows a transaction when there is more than one signature, depending on the setting, it can be used as the redundant security feature of the wallet. For example, if multisig is set in an online bitcoin wallet and is configured to require the owner's signature in addition to the signature of the online wallet site whenever a transaction is executed from the wallet, malicious bitcoin withdrawal can be prevented since the owner's personal key is not stored, even when the online wallet site is taken over by a hacking attack. Moreover, multisig is evolving into services that allow withdrawal from the bitcoin wallet only through biometric data or separate equipment using a two-factor authentication and other measures [26].

As the fundamental solution to hacking attacks of a bitcoin wallet, offline, cold storage-type wallets such as a physical bitcoin coin or a paper bitcoin wallet that is not connected to the Internet, are available. Similar approaches include the hardware-type bitcoin wallets to reduce the risk associated with online transactions. The hardware wallet, such as Trezor, stores the key in a tamper-proof storage unit connected to the computer through USB, that is, only when used and the signed transaction is transferred using the internally stored key and only when the user is authenticated. In other words, the storage unit is connected only when there is a need to establish a bitcoin transaction, remaining in cold storage-like status the rest of the time. Although it is more secure than cold storage because there is one more authentication process, problems such as loss of cold storage and lack of user-friendliness also plague the hardware wallet [27].

### 3.4. *Security of Software*

The bug of the software used in bitcoin can be critical. Although the official Bitcoin Developer Documentation [28] site clearly explains all bitcoin processes, the bitcoin core software is still effective

as the reference since the detailed processes of the early bitcoin system have been determined through the software implemented by Satoshi Nakamoto.

Nonetheless, even the bitcoin core software, which must be more reliable than anything, is not free from the problem of software malfunction such as bug. The most famous software bug is the CVE-2010-5139 vulnerability that occurred in August 2010. Due to the bug caused by integer overflow, an invalid transaction wherein 0.5 bitcoin was delivered as 184 trillion bitcoin was included in a normal block, and the problem was not resolved until 8 h later. Moreover, there was a bug where a block processed in version 0.8 was not processed in version 0.7 as the database was changed from BerkeleyDB to LevelDB since the bitcoin version of the bitcoin core was upgraded from 0.7 to 0.8. It caused the peers of version 0.7 and peers of version 0.8 to have different blockchains for 6 h. Both of these problems are cases showing that the general confidence in the security of bitcoin transactions of a block as having significant depth after a period of time and can be threatened by a software bug [29].

## 4. Blockchain Security Case Studies

The demand for the security of bitcoins based on blockchain has increased since hacking cases were reported. Mt. Gox, a bitcoin exchange based in Tokyo, Japan, reported losses of USD 8.75 million due to hacking in June 2011 and bitcoin wallet service InstaWallet reported losses of USD 4.6 million due to hacking in April 2013. In November of the same year, anonymous marketplace Sheep Marketplace was forced to shut down after somebody stole USD 100 million worth of bitcoins. Mt. Gox, which had already suffered losses due to hacking, again reported losses of USD 470 million due to hacking in February 2014 and subsequently filed for bankruptcy. The problems continued, with the Hong Kong-based bitcoin exchange Bitfinex reporting losses of USD 65 million due to hacking in August 2016. These problems have raised awareness of the need for security.

There have been academic studies on the security of blockchain to overcome such security problems and many papers have been published [30]. In particular, since blockchain is the generic technology of cyber money, the damages can be serious in cases of misuse and attempts to steal cyber money occur frequently. Therefore, it seems very meaningful to understand the attack cases known so far and to carry out investigations to draw up countermeasures.

### *4.1. Authentication*

An important part of blockchain security is security related to the personal key used in encryption. An attacker carries out various attempts to access a user's personal key stored in the user's computer or smartphone in order to hack the bitcoin. The attacker will install malware on the computer or smartphone to leak the user's personal key and use it to hack the bitcoin. Some studies have proposed a hardware token for the approval of a transaction to protect the personal key.

Other studies suggested strengthened authentication measures for the storage unit containing the bitcoin. A two-factor authentication is considered to be the leading method for strengthening authentication. For bitcoin, the two-party signature protocol by ECDSA can be used for authentication (Figure 3) [31,32].

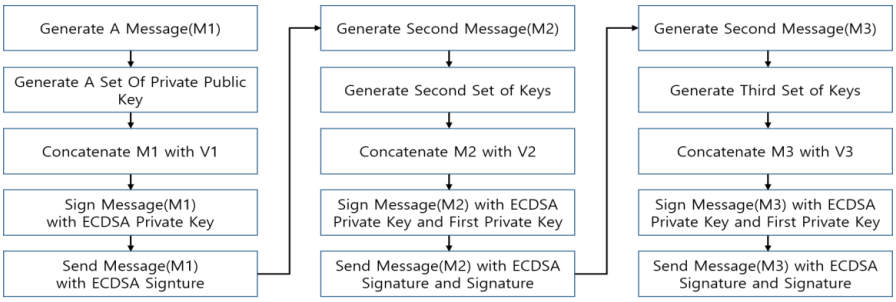


**Figure 3.** ECDSA two-party signature.

### 4.2. *Security Incidents*

With more people using bitcoins, cases of malware and malicious codes targeting bitcoins have also been reported. Malware can hack the bitcoins by infecting computers. To solve such a problem, a PC security solution must be installed to detect malicious code [17]. One recently found malicious code looted game accounts and can be applied for looting the bitcoin accounts. With more bitcoins being used for the cash transaction of online game items, security measures to cope with it are needed [33].

The Distributed Denial of Service (DDoS) attack floods the targeted server with superfluous requests to overload the system and prevent the provision of normal service to other users. Thus, it can prevent the users of blockchain from receiving the service. DDoS attacks include the bandwidth-consuming attack that exceeds the bandwidth of all systems using the same network and the PPS (Packet Per Second)-consuming attack that causes internal system failure or the denial of service to other servers in the same network. The http-flooding attack transfers a large amount of http packets to a targeted server to cause the denial of service. Since the bitcoin service must be continuously provided to the users, countermeasures to DDoS attacks are needed [34].

#### 4.2.1. 51% Attack

In a bitcoin environment, a 51% attack alters and falsifies 51% of the ledgers simultaneously. Thus, it is a very difficult attack to coordinate. The attacker must have 51% or more calculating capability of all users, intentionally generate two branches, and set the targeted branch as the legitimate blockchain. To solve the problem, an intermediate verification process must be provided to prevent such tampering [35,36].

In a bitcoin environment, a 51% attack consists of five steps.

1. Publish mining software with a higher EV (Expected Value).
    - *(1)* Mine on new headers (but validate it as soon as possible)
    - *(2)* More “flexible” 2-h rule
    - *(3)* Decide on fork with own block version number
    - *(4)* Make miner aware of the “Goldfinger” reward
    - *(5)* “Members only” functionality
2. Create a pool with stickiness.
    - *(1)* New members will receive only 90% of shares in the first 2 weeks and 110% after 2 weeks (Ponzi scheme)
3. Create unwanted coalitions (timestamp attack).
4. Attack other pools with cannibalizing pools.
5. Eventually switch to members only.

A race attack generates hundreds of transactions and sends them to multiple users when a legitimate transaction is sent. Since many users are likely to presume the transferred transaction to be legitimate, losses can be sustained if 51% of users change the ledger.

In a Finney attack, an attacker generates a block containing altered data and carries out the attack with it. Such attacks can be prevented when the attack target sets the transaction in standby mode until block confirmation.

#### 4.2.2. Improved Blockchain

Since the current payment system is very complex and transaction facilitators are scattered, the points targeted by security attacks are increasing. A user intending to trade money will pay an annual membership fee to receive a card and use it to purchase goods or use services. The customer’s

bank and the merchant's bank interact with each other to settle the fee and a shop intending to use the card receives it from a bank and uses it for the purchase of goods and services. A simplification of transaction is required since more people use smartphones to purchase goods or services (Figure 4) [37].

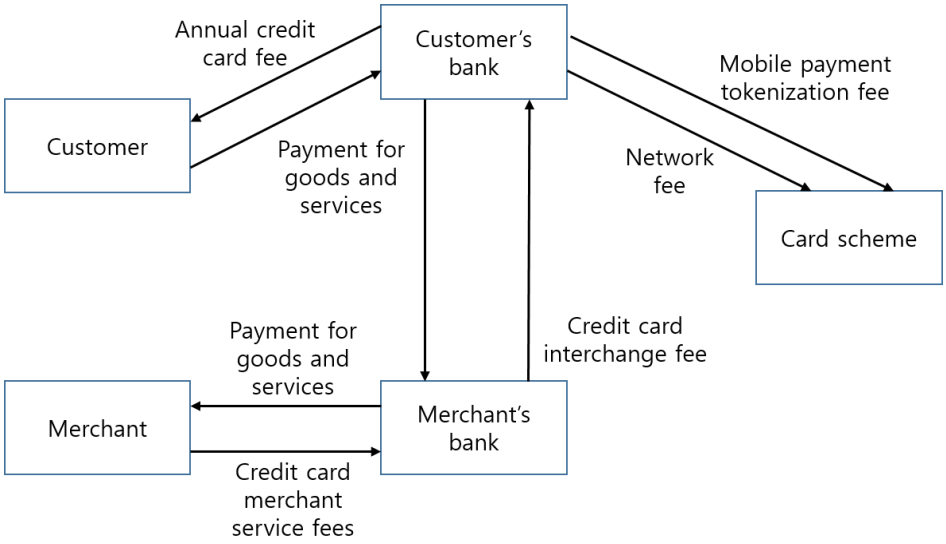


**Figure 4.** General payment process system.

As for the benefits of executing a conventional transaction as a peer-to-peer transaction using blockchain, the transaction is not only reliable and verifiable but also cost-efficient since there are no third parties involved. In addition, a transaction using blockchain can be completed very quickly since physical distance does not affect the transaction, whereas conventional transactions across the border can be very slow. Moreover, conventional, centrally managed transactions are vulnerable to leaks of important data when the managing server is hacked since all the valuable data is managed in the central server. In contrast, it is very difficult to attack blockchain-based transactions since all important data is distributed and an attacker must hack and alter 51% of the peer-to-peer transactions. Therefore, the improved blockchain must be used for transactions to solve the problems of conventional transactions [1].

One of the biggest problems of bitcoin using the blockchain is the possibility of a double transaction. A double transaction is the act of sending the bitcoin to two or more accounts for malicious purposes and "total currency" and "longest chain wins" are used as mechanisms for preventing it. The total currency mechanism means that the transaction can be terminated if the total currency exceeds 21 million by double transaction. The longest chain wins mechanism creates the next block first when a blockchain is forked by double transaction and the longest chain with the most work will always win.

If a user double-spends a bitcoin and the transaction details are consequently sent to two different peers, two blocks will be generated. The peers will generate the next blocks using two blocks in competition. As a result, the chain that loses in the competition, such as the red block in the Figure 3, is naturally eliminated and the longer chain wins. The double spending problem can be addressed through such a mechanism (Figure 5) [38].

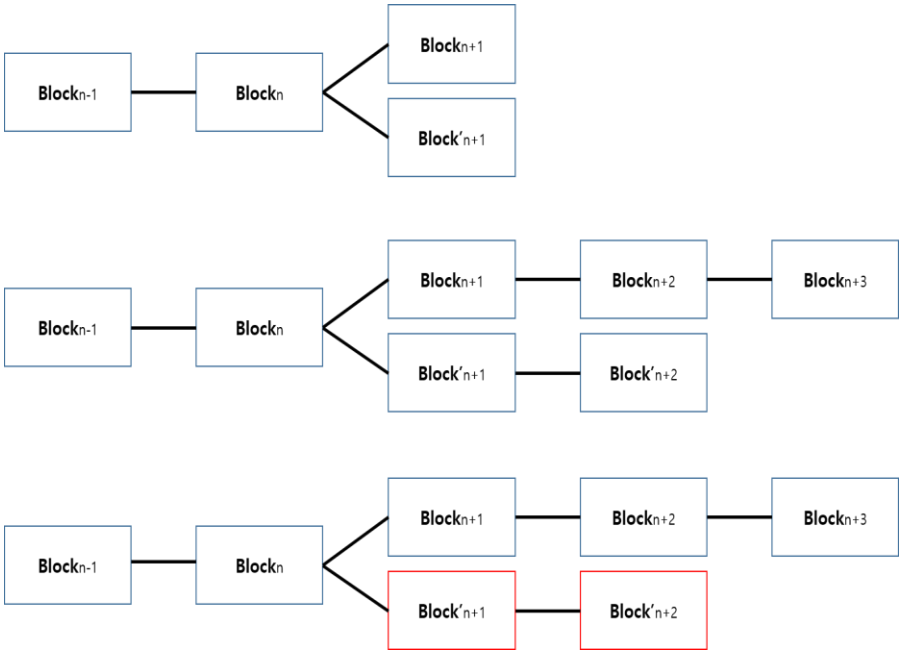


**Figure 5.** Double-spending prevention mechanism.

## 5. Secure Blockchain Solutions in Cloud Computing

The security factors for using bitcoin with blockchain were introduced in Section 3 and security cases of bitcoins using blockchain were reviewed in Section 4.

If the user data is disclosed in the cloud computing environment, monetary and psychological damages can occur due to the leak of users' sensitive information. The security of the saving and transmitting data, such as confidentiality and integrity, in the cloud computing environment is mainly studied. Note, however, that studies on privacy protection and anonymity are not sufficient. Blockchain is a representative technology for ensuring anonymity. If combined with the cloud computing environment, blockchain can be upgraded to a convenient service that provides stronger security. User anonymity can be ensured if the blockchain method is used when saving the user information in the cloud computing environment. An electronic wallet is installed when using the blockchain technology. If the electronic wallet is not properly deleted, the user information can be left behind. The remaining user information can be used to guess the user information. To solve this problem, we propose a solution that installs and deletes the electronic wallet securely.

Cases of falsifying the ledger or bitcoin and double transactions of blockchain pose the biggest problem. A secure wallet is needed to solve such security problems. Although the electronic wallet installed in the PC is generally used, the security of electronic wallets in mobile devices must be verified as mobile devices have become very popular. Since a transaction occurs based on the time value of a mobile device, the security of a transaction can be confirmed only when both the integrity and accuracy of a time stamp generated in a mobile device are guaranteed [28].

Moreover, the base technology must also be verified since vulnerabilities differ according to the programming language and platform used for the development of the electronic wallet environment. A secure electronic wallet must be developed by minimizing and verifying problems that can occur at each step of planning, requirement analysis, implementation, QA (Quality Assurance), and maintenance.

The electronic wallet must have measures for secure restoration if infringed by an attacker, verification of a binary installed for self-protection, and protection of the remaining data for restoration. It must provide security for the data stored in the electronic wallet as well as the settings needed for

the utilization of the electronic wallet. It must also be able to delete the remaining data securely when the electronic wallet is no longer used and must consequently be discarded.

To use an electronic wallet securely, a user installs it on his or her PC and the platform sends the electronic wallet and data to establish a secure environment. The user downloads and installs the electronic wallet software to use the bitcoin with blockchain and the public key of the platform is sent to the electronic wallet when the installation is completed. The electronic wallet sends the certificate distributed during development to the platform, which then verifies the validity of the certificate in the electronic wallet. The platform and the electronic wallet exchange the key using the Diffie–Hellman method, with each owning the shared key. When a user requests a transaction involving the use of a bitcoin, the ledger data containing the time stamp data between the electronic wallet and the platform are encrypted with the shared key and sent. When a request for disposal is executed, the user's certificate is found and deleted from the electronic wallet and the finished message is sent to confirm that it has been securely discarded. In addition, all the relevant files are deleted so that the remaining data are securely removed (Figure 6).

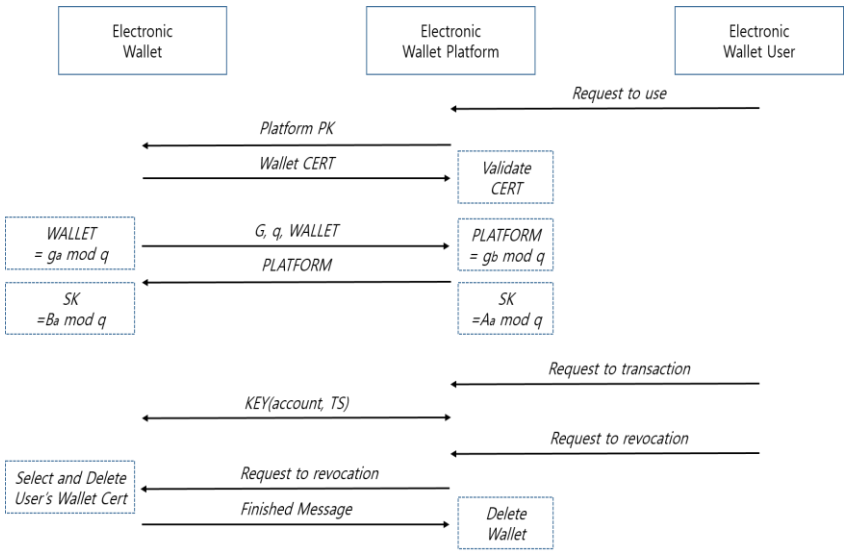


**Figure 6.** Secure bitcoin protocol.

This method uses a blockchain-based electronic wallet in the cloud computing environment. The blockchain method is used to remove the information of the user who uses cloud computing. This method installs and uses an electronic wallet and removes it normally. The electronic wallet is securely removed by sending the finished message. Leak of user information can be prevented only when the electronic wallet is completely removed. Even though many existing studies have been performed on the blockchain protocol, a method for removing the electronic wallet completely is presented to ensure user anonymity and privacy protection.

We compared the method with existing studies in terms of confidentiality, integrity, anonymity, privacy protection, and residual information protection (Table 1). Confidentiality checks if the information is leaked to unauthorized peers, whereas integrity checks if the data used in transactions are altered or falsified without sanction during transfer or storage. Anonymity must assure that the peer involved in a transaction is not identifiable. Privacy protection protects the personal information of peers participating in the transaction, whereas residual information protection checks the safe removal of user data at the time of transaction termination and program removal.

**Table 1.** Comparison of related studies.

| | Authentication Case [31] | Security Incidents Case [34] | 51% Attack Case [35] | Improved Blockchain Case [38] | Secure Blockchain Solution |
|---|---|---|---|---|---|
| Confidentiality | | √ | √ | √ | √ |
| Integrity | √ | √ | | | √ |
| Anonymity | √ | √ | √ | √ | √ |
| Availability | √ | | | | √ |
| Privacy Protection | √ | √ | √ | √ | √ |
| Residual Information Protection | | | | | √ |

The authentication case [31] does not provide integrity since it has the problem of leaking the key by hacking the personal key to attack the blockchain. Also, it does not provide residual information protection since it does not verify the complete removal of the electronic wallet. The security incidents case [34] does not provide availability since the service becomes unavailable due to infection by malware and does not provide residual information protection since it does not verify the complete removal of the electronic wallet. The 51% attack case [35] can have problems of infringed integrity of the transaction ledger and unavailability following an attack that alters 51% of the transaction ledger. Additionally, it does not provide residual information protection since it does not verify the complete removal of the electronic wallet. The improved blockchain case [38] neither assures integrity nor provides availability since the vulnerability of double transaction remains. Moreover, it does not provide residual information protection since it does not verify the complete removal of the electronic wallet. The secure blockchain solution improves security by providing residual information protection since it encrypts the data using a public key and verifies the complete removal of the electronic wallet.

## 6. Conclusion

A blockchain has done away with the server to exclude the involvement of the central authority and has facilitated transactions through the participants who jointly store the transaction records and, finally, approve the transactions using P2P network technology. The blockchain has a distributed structure and utilizes the peer network and the computing resources of peers. Technical measures such as proof of work and proof of stack have been implemented to improve the security of blockchain.

Although the security of blockchain is continuously enhanced, problems have continued to be reported and there are active studies on security. An attacker makes various attempts to access a user's personal key stored in the user's computer or smartphone in order to hack the bitcoin. There are studies on using a secure token or saving it securely to protect the personal key.

In this study, we discussed the blockchain technology and related core technologies and surveyed the trend of studies to date to discuss further areas to be studied. Various current issues should be taken into account to use blockchain in the cloud computing environment. Blockchain gives rise to many problems even now, such as the security of transactions, wallet, and software and various studies have been conducted to solve these issues. The anonymity of user information should be ensured when using blockchain in the cloud computing environment and the user information should be completely deleted when removing the service. If the user information is not deleted but instead left behind, the user information can be guessed from the remaining information. Therefore, this study discussed the method of providing security by presenting a method of secure blockchain use and removal protocol. It seems that studies on efficiency are also needed beside security, considering the environment wherein a massive amount of information is transmitted.

**Acknowledgments:** This research was supported by MSIP (Ministry of Science, ICT, and Future Planning) Korea under the ITRC (Information Technology Research Center) support program (IITP-2017-2014-0-00720) supervised by IITP (Institute for Information & communications Technology Promotion).

**Author Contributions:** Jin Ho Park: Research for related works, analysis, design, amelioration of the proposed model and drafting of the article. Jong Hyuk Park: Total supervision of paperwork, review, comments, assessment, etc.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References


1. Il-Kwon, L.; Young-Hyuk, K.; Jae-Gwang, L.; Jae-Pil, L. The Analysis and Countermeasures on Security Breach of Bitcoin. In Proceedings of the International Conference on Computational Science and Its Applications, Guimarães, Portugal, 30 June–3 July 2014; Springer International Publishing: Cham, Switzerland, 2014.
2. Beikverdi, A.; JooSeok, S. Trend of centralization in Bitcoin's distributed network. In Proceedings of the 2015 16th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), Takamatsu, Japan, 1–3 June 2015.
3. Bonneau, J.; Miller, A.; Clark, J.; Narayanan, A.; Kroll, J.A.; Felten, E.W. Sok: Research perspectives and challenges for bitcoin and cryptocurrencies. In Proceedings of the 2015 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 17–21 May 2015. [CrossRef]
4. Christidis, K.; Michael, D. Blockchains and Smart Contracts for the Internet of Things. *IEEE Access* **2016**, *4*, 2292–2303. [CrossRef]
5. Huang, H.; Chen, X.; Wu, Q.; Huang, X.; Shen, J. Bitcoin-based fair payments for outsourcing computations of fog devices. *Future Gener. Comput. Syst.* **2016**. [CrossRef]
6. Huh, S.; Sangrae, C.; Soohyung, K. Managing IoT devices using blockchain platform. In Proceedings of the 2017 19th International Conference on Advanced Communication Technology (ICACT), Bongpyeong, Korea, 19–22 February 2017.
7. Armknecht, F.; Karame, G.; Mandal, A.; Youssef, F.; Zenner, E. Ripple: Overview and Outlook. In *Trust and Trustworthy Computing*; Conti, M., Schunter, M., Askoxylakis, I., Eds.; Springer International Publishing: Cham, Switzerland, 2015; pp. 163–180.
8. Vasek, M.; Moore, T. There's No Free Lunch, Even Using Bitcoin: Tracking the Popularity and Profits of Virtual Currency Scams. In Proceedings of the International Conference on Financial Cryptography and Data Security, San Juan, Puerto Rico, 26–30 January 2015; Springer: Berlin/Heidelberg, Gemany, 2015.
9. Zhang, J.; Nian, X.; Xin, H. A Secure System For Pervasive Social Network-based Healthcare. *IEEE Access* **2016**, *4*, 9239–9250. [CrossRef]
10. Singh, S.; Jeong, Y.-S.; Park, J.H. A survey on cloud computing security: Issues, threats, and solutions. *J. Netw. Comput. Appl.* **2016**, *75*, 200–222. [CrossRef]
11. Kaskaloglu, K. Near zero Bitcoin transaction fees cannot last forever. In Proceedings of the International Conference on Digital Security and Forensics (DigitalSec2014), The Society of Digital Information and Wireless Communication, Ostrava, Czech Republic, 24–26 June 2014.
12. Ziegeldorf, J.H.; Matzutt, R.; Henze, M.; Grossmann, F.; Wehrle, K. Secure and anonymous decentralized Bitcoin mixing. *Future Gener. Comput. Syst.* **2016**. [CrossRef]
13. Aitzhan, N.Z.; Davor, S. Security and Privacy in Decentralized Energy Trading through Multi-signatures, Blockchain and Anonymous Messaging Streams. *IEEE Trans. Dependable Secur. Comput.* **2016**, *99*. [CrossRef]
14. Heilman, E.; Foteini, B.; Sharon, G. Blindly signed contracts: Anonymous on-blockchain and off-blockchain bitcoin transactions. In Proceedings of the International Conference on Financial Cryptography and Data Security, Christ Church, Barbados, 22–26 February 2016; Springer: Berlin/Heidelberg, Gemany, 2016.
15. Natoli, C.; Gramoli, V. The blockchain anomaly. In Proceedings of the 2016 IEEE 15th International Symposium on Network Computing and Applications (NCA), Cambridge, MA, USA, 31 October–2 November 2016.
16. Shi, N. A new proof-of-work mechanism for bitcoin. *Financ. Innov.* **2016**, *2*, 31. [CrossRef]
17. Swan, M. *Blockchain: Blueprint for a New Economy*; O'Reilly Media, Inc.: Sebastopol, CA, USA, 2015.
18. Tschorsch, F.; Scheuermann, B. Bitcoin and beyond: A technical survey on decentralized digital currencies. *IEEE Commun. Surv. Tutor.* **2015**, *18*, 2084–2123. [CrossRef]
19. Wressnegger, C.; Freeman, K.; Yamaguchi, F.; Rieck, K. Automatically Inferring Malware Signatures for Anti-Virus Assisted Attacks. In Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security, Abu Dhabi, UAE, 02–06 April 2017.
20. Decker, C.; Roger, W. Information propagation in the bitcoin network. In Proceedings of the 2013 IEEE Thirteenth International Conference on Peer-to-Peer Computing (P2P), Trento, Italy, 9–11 September 2013.

21. Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. Available online: https://bitcoin.org/en/bitcoin-paper (accessed on 29 June 2017).
22. Bozic, N.; Guy, P.; Stefano, S. A tutorial on blockchain and applications to secure network control-planes. *SCNS IEEE* **2016**. [CrossRef]
23. Bradbury, D. The problem with Bitcoin. *Comput. Fraud Secur.* **2013**, *11*, 5–8. [CrossRef]
24. Paul, G.; Sarkar, P.; Mukherjee, S. Towards a more democratic mining in bitcoins. In Proceedings of the International Conference on Information Systems Security, Hyderabad, India, 16–20 December 2014; Springer International Publishing: Cham, Switzerland, 2014.
25. Bamert, T.; Decker, C.; Wattenhofer, R.; Welten, S. BlueWallet: The Secure BitcoinWallet. In *Security and Trust Management*; Mauw, S., Jensen, C., Eds.; Springer International Publishing: Cham, Switzerland, 2014; pp. 65–80.
26. Anceaume, E.; Lajoie-Mazenc, T.; Ludinard, R.; Sericola, B. Safety analysis of Bitcoin improvement proposals. In Proceedings of the 2016 IEEE 15th International Symposium on Network Computing and Applications (NCA), Cambridge, MA, USA, 31 October–2 November 2016.
27. Upadhyaya, R.; Jain, A. Cyber ethics and cybercrime: A deep dwelved study into legality, ransomware, underground web and bitcoin wallet. In Proceedings of the 2016 International Conference on Computing, Communication and Automation (ICCCA), Noida, India, 29–30 April 2016.
28. Haber, S.; Stornetta, W.S. How to time-stamp a digital document. In Proceedings of the Conference on the Theory and Application of Cryptography, Sydney, NSW, Australia, 8–11 January 1990; Springer: Berlin/Heidelberg, Gemany, 1990.
29. Eyal, I.; Emin, G.S. Majority is not enough: Bitcoin mining is vulnerable. In Proceedings of the International Conference on Financial Cryptography and Data Security, Christ Church, Barbados, 3–7 March 2014; Springer: Berlin/Heidelberg, Gemany, 2014.
30. Petersen, K.; Feldt, R.; Mujtaba, S.; Mattsson, M. Systematic Mapping Studies in Software Engineering. In Proceedings of the 12th International Conference on Evaluation and Assessment in Software Engineering (EASE), Bari, Italy, 26–27 June 2008.
31. Mann, C.; Loebenberger, D. Two-factor authentication for the Bitcoin protocol. In *International Workshop on Security and Trust Management*; Springer International Publishing: Cham, Switzerland, 2015.
32. Yuan, Y.; Wang, F.-Y. Towards blockchain-based intelligent transportation systems. In Proceedings of the 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC), Rio de Janeiro, Brazil, 1–4 November 2016.
33. Kogias, E.K.; Jovanovic, P.; Gailly, N.; Khoffi, I.; Gasser, L.; Ford, B. École Polytechnique Fédérale de Lausanne (EPFL). Enhancing bitcoin security and performance with strong consistency via collective signing. In Proceedings of the 25th USENIX Security Symposium (USENIX Security 16), Austin, TX, USA, 10–12 August 2016.
34. Vasek, M.; Thornton, M.; Moore, T. Empirical analysis of denial-of-service attacks in the Bitcoin ecosystem. In Proceedings of the International Conference on Financial Cryptography and Data Security, Christ Church, Barbados, 3–7 March 2014; Springer: Berlin/Heidelberg, Gemany, 2014.
35. Bastiaan, M. Preventing the 51%-Attack: A Stochastic Analysis of Two Phase Proof of Work in Bitcoin. Available online: http://referaat.cs.utwente.nl/conference/22/paper/7473/preventingthe-51-attack-a-stochastic-analysis-of-two-phase-proof-of-work-in-bitcoin.pdf (accessed on 29 June 2017).
36. Kroll, J.A.; Davey, I.C.; Felten, E.W. The economics of Bitcoin mining, or Bitcoin in the presence of adversaries. *Proc. WEIS.* **2013**, *2013*.
37. Eyal, I.; Gencer, A.E.; Sirer, E.G.; van Renesse, R. Bitcoin-ng: A scalable blockchain protocol. In Proceedings of the 13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16), Santa Clara, CA, USA, 2 February 2016.
38. Karame, G.O.; Elli, A.; Srdjan, C. Double-spending fast payments in bitcoin. In Proceedings of the 2012 ACM Conference on Computer and Communications Security, Raleigh, CA, USA, 16–18 October 2012.