Blockchain Technology in Cloud Computing : A Systematic Review

Ms. Ketki R. Ingole [1], Ms. Sheetal Yamde[2]

[1] *Head Department of Computer Science and Engineering, Computer Science and Engineering, Sipna COET Amravati, Maharashtra, India*
[2] *Student, Computer Science And Engineering , Sipna COET Amravati, Maharashtra, India*

---***---

Abstract : *A blockchain is essentially a distributed database of records or public ledger of all transactions or digital events that have been executed and shared among participating parties. Each transaction in the public ledger is verified by consensus of a majority of the participants in the system. And, once entered, information can never be erased. The blockchain contains a certain and verifiable record of every single transaction ever made. Bitcoin, the decentralized peer to peer digital currency, is the most popular example that uses blockchain technology. The digital currency bitcoin itself is highly controversial but the underlying blockchain technology has worked flawlessly and found wide range of applications in both financial and nonfinancial world. The main hypothesis is that the blockchain establishes a system of creating a distributed consensus in the digital online world. This allows participating entities to know for certain that a digital event happened by creating an irrefutable record in a public ledger. It opens the door for developing a democratic open and scalable digital economy from a centralized one. There are tremendous opportunities in this disruptive technology and revolution in this space has just begun. This white paper describes blockchain technology and some compelling specific applications in both financial and nonfinancial sector. We then look at the challenges ahead and business opportunities in this fundamental technology that is all set to revolutionize our digital world.*

***Key Words*: Blockchain; Computer Security; Bitcoin; Authentication; Cloud computing.**

1. INTRODUCTION

The blockchain is a quite novel technology, 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. Looking across these technological developments in cloud computing. 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 subjective 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. Since the improvement of the Internet and encryption technology Using blockchain can provide higher security compared to storing all data in a central database. The use of these technologies in Bitcoin "mining" was ground-breaking 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.

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. 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, and authentication, access control, and so on.

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.

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.

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).

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 logically 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 secrecy since there is no way of finding information pertaining to the owner. 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.

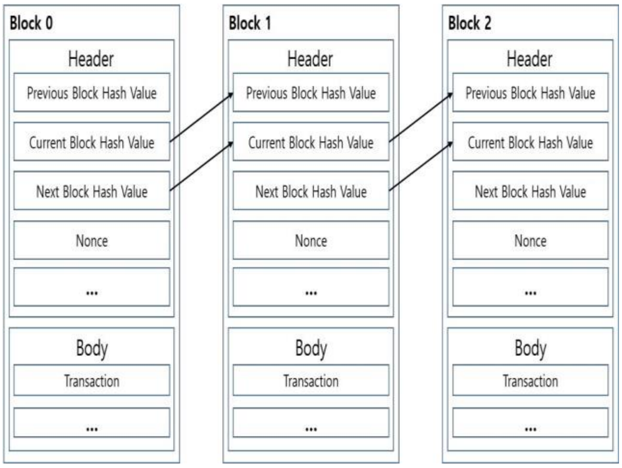

Fig -1. Blockchain connection structure

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.

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. 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 cryptcurrency in 1998. 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.

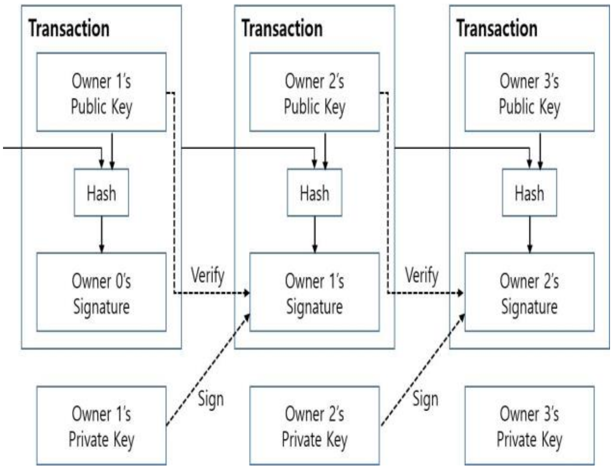

Fig -1. A bitcoin transaction.

3. CONSIDERATION FOR BLOCKCHAIN SECURITY:

Regulatory challenges underlying cryptocurrencies like bitcoin has attracted significant interest from both private businesses and governments for its many other possible applications.

3.1. 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.

3.2. 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 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.

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. 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 smart phone in order to hack the bitcoin. The attacker will install malware on the computer or smart phone 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.

5. SECURE BLOCKCHAIN SOLUTIONS IN CLOUD COMPUTING.

The security factors for using bitcoin with blockchain were introduced and security cases of bitcoins using blockchain were reviewed . 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 secrecy. 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.

6. CONCLUSIONS

This book has tried to demonstrate that blockchain technology's many concepts and features might be broadly extensible to a wide variety of situations. 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 smart phone in order to hack the bitcoin. There are studies on using a secure token or saving it securely to protect the personal key. While blockchain's best-known, most used and highest-impact application is Bitcoin, the potential impact of the *technology* is much greater and wider than ... 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.

REFERENCES

1. Y Gilad, R Hemo, S Micali, G Vlachos, N Zeldovich : Algorand: Scaling Byzantine Agreements for Cryptocurrencies
2. A. Kiayias, I. Konstantinou, A. Russell, B. David, R. Oliynykov. : Ouroboros: A provably secure proof-of-stake blockchain protocol.
3. Atzei N., Bartoletti M., Cimoli T., A Survey of Attacks on Ethereum Smart Contracts, 6th International Conference on Principles of Security and Trust (POST), (2017)
4. Dimitri N., Bitcoin Mining as a Contest, Ledger, 2, 31-37.
5. Evans D., Economic Aspects of Bitcoin and other Decentralized Public-Ledger Currency Platforms, Coase-Sandor Institute for Law and Economics Working Paper 685, (2014)
6. Eyal I., Emin G., Majority is Not Enough: Bitcoin Mining is Vulnerable, in Financial Criptography and Data Security, Springer, (2014)
7. Houy N., The Bitcoin mining game, Ledger, 1, 53-68, (2016)
8. Narayanan A., Bonneau J., Felten E., Miller A., Goldfeder S., Bitcoin and Cryptocurrency Technologies, Princeton University Press, (2016)
9. Szabo N., Smart Contracts: Building Blocks for Digital Markets, www.fon.hum.uva.nl (1996)
10. Tapscott D.,- Tapscott A., Blockchain Revolution, Portfolio Penguin, (2016).