ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(A High Impact Factor, Monthly, Peer Reviewed Journal)*

*Website: www.ijircce.com*

**Vol. 6, Issue 4, April 2018**

# Transaction Confirmation in Bitcoin Blockchain

Rajani Kodagali, Prof.Anand Pashupathimath

M. Tech, Student, Dept. of Computer Science and Engineering, SDMCET Dharwad, Dharwad, Karnataka, India

Asst Professor, Dept. of Computer Science and Engineering, SDMCET Dharwad, Dharwad, Karnataka, India

**ABSTRACT:** One of the basic appliances for useful system of the money is remuneration. Information pertaining to the amount of compensation awarded to various individuals can often to consider sensitive, commanding an assured degree of the privacy. As Bitcoin and crypto currencies evolve same design into a recognized of exchange for larger money of the world economy, a rising number of persons will earn profits in form of block-chain-based on payments. This Bitcoin transaction waits tens of minutes for transactions to commit in each and every block to confirm the transaction and it consists more than 6 blocks for one complete transaction. Exact confirmation of transactions in an each block is proposed in this system. In between dealer and sender bilinear diffie hellman a key exchange protocol is used. Every transaction has a hash associated with it by Merkle root method.

**KEYWORDS:** Diffie Hellman Key Exchange, Hash code and Merkle Root

## I. INTRODUCTION

Block-chain is a technology which is based on digital currency based on the network and cryptographic tools. The bit-coin is generated a trust less environment, the users are transfer the money to other user with no relying on trusted mints like payment services or bank System [14]. This block chain will provide a kind of append only the information stock of transaction which can replicated between users. Many back sectors are involved tests of block-chain technology which can include through the global consortium and applying the block-chain to trades the finance also across the border of payments. Financially, transaction is first but not the case of investigating the block-chain technology. This will implement the distributed the ledger is in general verification and stored any kind of transactions.

A block-chain is mainly supportable list of data by cryptographically. The enthusiasm around the block-chain is one of the reason of database that do not has any cryptographic guarantee of an integrity, guarantees which is necessary for any operating database in environment. Where the field of the security system and privacy is enhance the method has been learned thus Snowden revelations. This for all databases is possibly operating in environment. Some of hype around the block chain is for good reason. First occasion in decades is sustainable database by replacing the block chain [9] [10]. However, there is a more block chain than only integrity of data. The primary advantage of block-chain is that the information is decentralized. The public circulated ledger build a block-chain when all users has same information, which necessary for high value of use cases like currency is clear invasive of privacy for multiple users. Privacy and security on blockchain is emerging the field that needs for further investigation.

Many enterprises, governments and startups [1] are discovering its application in area of diverse as supply electronic helth record, energy, voting, supply chain, protecting critical civil infrastructure and ownership management. Then wide array if an intrest in blockchain technology which is underlined by fast evolution includes simple deployement through the blockchain service fron Microsoft, IBM3 orAzure2. This chain becomes publicly available in infrastructure for build the decentralised application also achieves interoperability [12].

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

## II. LITERATURE SURVEY

S. Matthew et.al [1] proposes the model of blockchain remuneration. They provide the foundation for creation of device that may search blockchain for behaviour of evidence remuneration takes place that cryptocurrencies that is bitcoin. The consideration of the ethic of anonymity that does not overlook the importance reasons for anonymity which can take for granted by traditional currencies. This is still the case that people are uncomfortable divulging the information of them salaries with co-workers or friends. Then relative ease with an individual address in bitcoin chainblock is associated by salary from heuristics are presented which can demonstrates the host of novel challenges also opportunities. This represents the initial step in determination of what paradigm is ultimately stored and interact each other from one of the old social technologies or money.

Petra Isenberg et.al [2] proposes the visual exploration system for studying the behaviour of each entities exchanging the bitcoins. This bit coin can be crypto currency, more popular for permitting the financial pseudonymous of transaction. The blockchain is the public ledger of bitcoin system which holds the data based on millions of each transaction between the pseudonymous address. This address is belongs to each entity like serviced, enterprises or people. Understanding how the bitcoin system is employed, it is difficult because the unclear address which belongs to similar entity. Proposed tool address is the problem by clustering the address as well as displaying the transaction details for each entity.

Marco Cognoscenti et.al [3] proposed the systematic survey to study the use cases of block chain and which factor is affected integrity, adaptability and anonymity of bitcoin technology. The goal of them research work is to leverage that block chain and peer to peer methods for private by IoT Design where the information produced the mechanisms that are not entrusted to centralize the companies. They reported some uses of bitcoin. If some of them explicitly thought for internet of things. They found some use cases for private and decentralized of data management which is in way by them goal. Regarding that the adaptability and integrity, they found that the more bitcoin systems which is more secure but at the same time blockchain of scalability issues make it suitable for IoT. Regarding an anonymity that they found in bitcoin is guaranteed.

Xiwei Xu et.al [4] proposes the taxonomy of block-chain also block-chain based system. This taxonomy is used when compare the block-chains also assists in design then performance of software architecture is uses the technology of block-chain. The taxonomy captures the main architectural descriptions of block-chain and impact of various decisions. This is planned to help with significant architecture consideration about the quality of attributes and performance of the block chain based system (For example availability, performance and security). Then other than patterns, taxonomies are classified and organize the exits solution.

Joseph Bonneau et.al [5] proposes the first systematic exposition of bitcoin then many crypto currencies is related or alcoins. Drawing from a scattered body knowledge that identifies 3 keys components old bit-coin design which decouple. This enables more insight analysis of bitcoin properties further stability. They map the design gap for various changes in proposed system, provides the comparative analysis for other consensus methods, currency allocation methods, computational puzzle and key management tool. They survey anonymity issues in bitcoin then provide an evaluation framework for studying the variety of privacy which is enhanced. Finally they provide the novel insights in term disintermediation models which absolve the requirement for trusted intermediaries in set of application. They identify the 3 general disintermediation methods and provide detail comparison.

Harry Halpin et.al [6] proposes the block-chain has fueled that one of the most enthusiastic burst of activity in cryptography in years. But outstanding problems in privacy and security should solve for block-chain technology to reach their potential. They presented this concept bringing together industry and academia to study the problems for ranging from deploys new cryptographic primitives on bit-coin to enable privacy preserving file storage. They overviewed that not only for large problem but also outstanding unsolved issues that require further cooperation of block-chian community.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

## III. METHODOLOGY

In this proposed system for exact confirmation of transactions in a block chain from dealer to sender is shows in Fig. 1. Sender sends the bit coin to the Receiver via Dealer and miners validate transaction it to block chain. Receiver gets bit coin from sender and gives the confirmation information. During Every transaction inside the block paired and then hashed together by Merkle root method which is the efficient method of making transaction into block. Each key-value is stored in database which looks up previous transaction. Stored information updates sender bank information and is checked by the dealer for further process. In between dealer and sender bilinear diffie hellman a key exchange protocol is used.

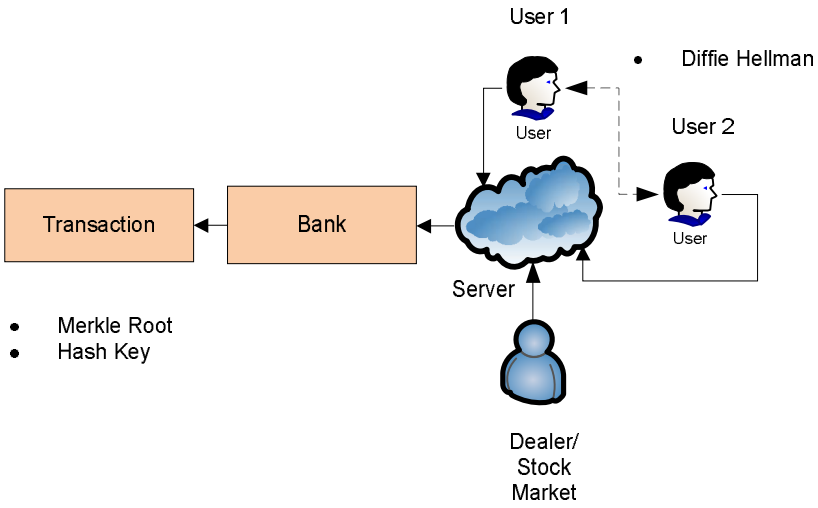


Fig 1: Operational Diagram of Proposed System

### 3.1 Diffie Hellman

Diffie-Hellman is not encryption method which normally thinks that would not typically use Diffie Hellman to encrypt information. This method is employed for secure key exchange that encrypts data. This can be accomplishes to secure exchange by generating the shared key (known as KEK or Key Encryption Key) in between two devices [15]. The shared key is encrypts the symmetric key for transmittal secure. The symmetric key is also named as Data encryption key or traffic encryption key.

This Diffie Hellman key exchange method solves following problem. For example, Alice and Bob are two users; they want to share the secret key foe cipher symmetric process, but only when communication is insecure. Every bit of data that exchange can be noticed by their adversary Eve. We can observe that how these two parties are to share the key without making it accessible to Eve. Firstly the glance appears that Alice and Bob face an impossible task. This is great job insight of Diffie and Hellman that the complexity of discrete logarithm mistakes for $\mathbb{F}^*_p$ gives a possible solution.

The first step of DH is to agree large prime number (p) and a nonzero integer i.e g modulo of p. Alice and Bob create the values of g and p knowledge publicly for example they may post the values on their web sites so Eve knows Alice and bob. For many reasons, this is best when they choose g its order in $\mathbb{F}^*_p$. $\mathbb{F}^*_p$ represents the large prime number.

Then next step is, Alice is pick some secret integer value that she do not reveal to others, similarly the Bob picks secret integer value of b that he can make as secret key. Alice and Bob calculated by their secret keys, is shows below.

$$\underbrace{A \equiv g^a \pmod p}_{\text{Alice computes this}} \text{ and } \underbrace{B \equiv g^b \pmod p}_{\text{Bob computes this}}$$

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

Next they computed the exchange values; Alice (A) sends the key to Bob and Bob (B) sends to Alice. Eve get both the values of A and B, since they send the keys by insecure communication channel.

Finally, Alice and Bob are use their secret keys is to calculate

$\underbrace{A' \equiv B^a \pmod p}_{\text{Alice computes this}}$ and $\underbrace{B' \equiv A^b \pmod p}_{\text{Bob computes this}}$

Then calculated the values of $A'$ and $B'$ respectively which are in same, depicts that

$$A' \equiv B' \equiv (g^b)^a \equiv g^{ab} \equiv (g^a)^b \equiv A^b \equiv B' \pmod p$$

This frequent value is there in exchanged key.the flow of this algorithm is a show in Fig. 2.

Third party of Diffie Hellman key agreement is lends to decisional form. The DBDH, DDH needs participants to decide if target element were either special combination of random element or input parameter.

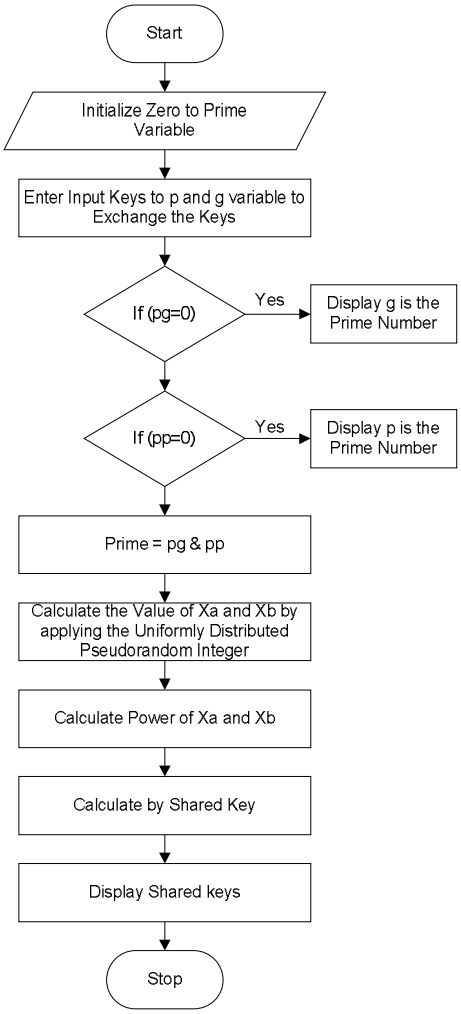


Fig. 2: Flow chart diagram of Diffie Hellman Key Exchange

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

The idea of this Hellman exchange is followed when two parties are wishing to share the secret.

Algorithm : Diffie Helman Key Exchange

*Step.1:* Alice and Bob are agree on transformation of encryption

*Step.2:* Alice and Bob each creates two keys such as $pk_A$, $sk_A$ and $pk_B$, $sk_B$:

$$D_{sk}(\varepsilon_{pk}(x)) = x$$

*Step.3:* $pk_A$ and $pk_B$ are Both made as public key when $sk_A$ and $sk_B$ become secret.

*Step.4:* When Alice encrypts m then Alice using Bobs public key agreed on encryption method.

$$c = E_{pk_B}(m)$$

*Step.5:* Alice sends an information c to Bob through the channel.

*Step.6:* Bob will decrypts $D_{sk_B}(c) = m$ by using Bob private key.

### 3.2 Transaction

The main importance of the blockchain technology can consequently that the fact, which can obtainable for all but still possesses or controlled by without any user [8]. This will helps that the operation of every participant enhance together also continues the blockchain by obeying the strict rules. In general agreement, participants were agreeing the chain which can be updated. This agreement is known as consensus machine.

This technology function, which can on thousands of nodes for example computer, worldwide etc. these nodes are come and go as they want in network. The new block starts with the process which known as mining by specialize nodes or other miners. These miners are operating secretly by working together and trying to find out the puzzles which can be created as a new blocks in bit coin [7]. This creation is not an easy to make a sound. It will take some steps to complete and confirm new blocks.

In currency transaction, more than two miners are verifies the transitions also supervise that everything is in order. Then the people making a transaction actually have money that what he wants to spend. Suppose this is a true transaction, the miners are confirms the changes. Later, the transactions were in chronological order which can bundle in same block, which is in longer execution form chain blocks [11]. The chain consists all accepted transactions that can occurred since a birth of blockchain and the data is obtainable to all which given by time. Some of them explained that it is referred to blockchain as a chronological ledger, or knowledge base in which transactions can be recorded by network. Fig. 3 depicts the example of two users are transferring the money from one user to other user and third party (dealer) observe that the money is transferred or not.

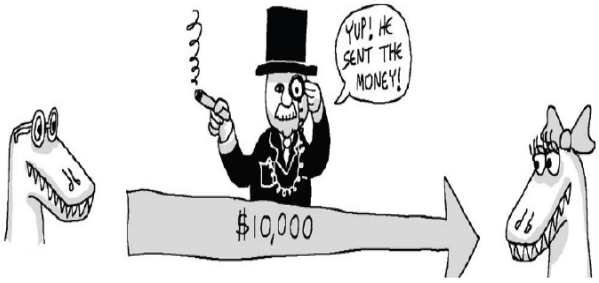


Fig. 3: Traditional online financial transactions using third trusted party

### 3.3 Merkle Root

Every transactions has an identified code known as hash, it consists the original piece of data of transaction. The transaction of hash values are bundled together in each block which can combined in the system known as Merkle tree. The combined hash value is put into the header of next block with some other data is shows in Fig. 4. The past hash in new blocks are ensures that blocks does not tampered and hinder cheating [2]. The timestamp proves that the information exists for time being.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

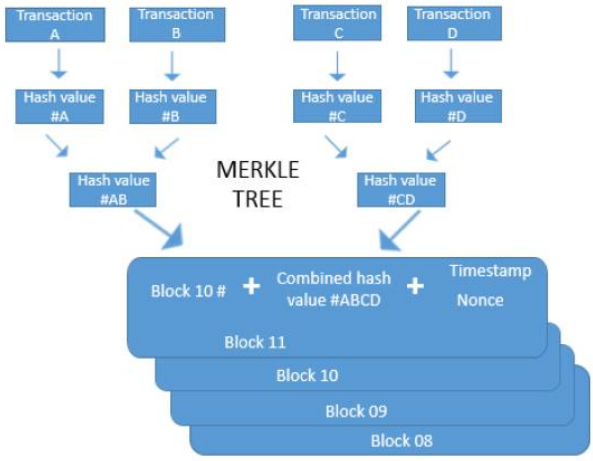


Fig. 4: Merkle root

The header becomes one of the parts of mathematical puzzle, where the miners found by manipulating the some number named as nonce. Miners are going through the trillions of potential solution to calculate the puzzle and also when correct solution is found, the miner finds it, announced it into other network. The miners are checks the solution and confirm it if it is correct then update the block correspondingly. This is a beauty of bit coin block-chain where the puzzle is very hard to crack the problem but so simple to check. The header hash is identifying the string of new block which is called as block-chain [13].

In return the maintaining and mining the new blocks of block-chain, miners were receives the rewards of some amount of recently mined bitcoin. This is an incentive why the miners are wants to update the block-chains by resolving the complex puzzles. The payment is postponed until a few amount of block is mined. This may secures the miners which is more resourceful to maintain the block-chain. Another reward is adding the transaction fees into transactions. 97% of the transactions are included a transaction fee which currently <0.1% of transaction value. This system is necessary because it is more sufficient to incentive for miners to continue for preserve the block-chain when final bitcoin are mined also no more bitcoins were received as reward. These transactions are marginal in differences to new transaction cost, but those are tends to rise when last bit coin has been mined.

When last transaction in a coin can be buried with enough blocks, before spent the transaction is removed to keep the disk. Without breaking any block hash, transactions hashed in Merkle Tree to facilitate with only a root which can included in block hash. The previous blocks are compressed by stubbing off the branches of Merkle root. The inner hashes are no need of storing it.

### 3.4 Hash key

Hash trees are employed to prove the information which is stored, controlled and exchanged between the computers. The main usage of hash tree is make sure that information block is received from other which is unaltered and undamaged. Even for check the other peers and sends fake blocks. For example the sun Microsystems are used Hash Trees in ZFS system. similarly, Hash Trees are used in Google wave protocol, Git distributed control system, Bit coin peer-to-peer network, Tahoe-LAFS backup system and so on are made used hash trees in trusted computer systems.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

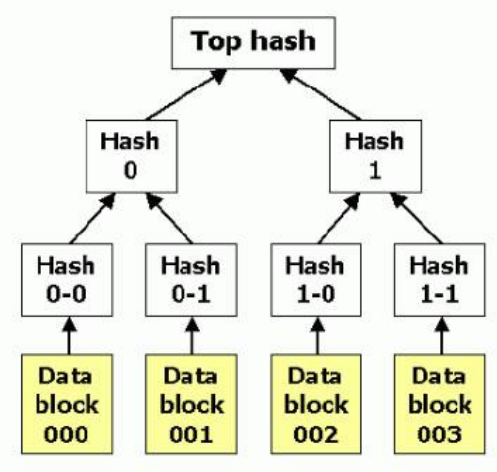


Fig. 5: Binary Hash Tree

Hash Tree defines as tree of hashes in which leaves the hashes of information blocks for a file, set of files or instance. Further nodes are hashes with respective children in the tree. For example, about Fig. 5 shows that hashes 0 is result of hashing hash 0-0 and then hash 0-1. Thus, hash 0= (hash 0-0 || hash 0-1) where || represents that concatenation.

The hash tree implementations were in binary (that is two child nodes are in each and every node) but those are used only for more child nodes under each node. The cryptographic hash function is Whirlpool, Tiger or SHA-1 used for hashing. The hash tree requires defending against to unintentional damage, is less secure for check the sums like CRCs used. In top of the hash tree there is a master hash or root hash. In all cases top hash is attained from trust source before downloading a file on network. For example, web site or friend is called as good recommendation of file to download. The hash tree is received from non trusted source when top hash is available. The received hash tree can be checked against top trusted hash and if the hash tree fake or damaged, other hash tree from other source is tried until the program which can finds to match the top hash.

## IV. RESULTS

In proposed system, we should exchange the keys with the help of diffie hellman algorithm. Initially users should give the prime keys to exchange then hash code will generate the hash value in the form of hexadecimal. The experimental result is shows below, user1 enters the prime number of 2 and user2 enters the prime number of 7. Then shared key is generated. Once shared key is generated we need to pass this value to transaction. This transaction block is creates the hash code in three iteration is shows below table.

| Key Exchange |
|---|
| ***Input:*** Masukkan Nilai g: 2<br>Masukkan Nilai p: 7 |
| ***Output***: shared key: 1<br>Transaction<br>First Iteration<br>Hash A: B9DEBF7D<br>Hash B: 52F36E64<br>Hash C: 68A54817<br>Hash D: C1FA0711<br>Hash E: 66C3A63D<br>Hash F: 384850E1<br>Hash G: 575B42F7 |

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

Hash H: 02DC5AA1
---
Second Iteration
Hash AB: B9DEBF7D52F36E64
Hash CD: 68A54817C1FA0711
Hash EF: 66C3A63D384850E1
Hash GH: 575B42F702DC5AA1
---
Third Iteration
merkle Root of Hash(AABCDEFGH)
B9DEBF7D52F36E6468A54817C1FA071166C3A63D384850E1575B42F702DC5AA1

## V. CONCLUSION

The speed at which payments in block chain based crypto currencies can be performed in each block generation interval, which in Bit coin is fixed to 10 minutes .This paper presents a new system model in block chain for implementing exact confirmation of transaction between owner and sender by using bilinear diffie hellman key generation. During Every transaction inside the block paired and then hashed together by Merkle root method which is the efficient method of making transaction into block. Integrate scheme into block chain analyze the security of it and evaluate its performance.

## REFERENCES

1. English, S. Matthew, and Ehsan Nezhadian, "Conditions of Full Disclosure: The Blockchain Remuneration Model", Security and Privacy Workshops (EuroS&PW), IEEE, pp. 64-67, 2017
2. Isenberg, Petra, Christoph Kinkeldey, and Jean-Daniel Fekete, "Exploring Entity Behavior on the Bitcoin Blockchain", IEEE, Visualization, 2017.
3. Conoscenti, Marco, Antonio Vetro, and Juan Carlos De Martin, "Blockchain for the Internet of Things: A systematic literature review", Computer Systems and Applications, IEEE, pp. 1-6, 2016
4. Xu, Xiwei, Ingo Weber, Mark Staples, Liming Zhu, Jan Bosch, Len Bass, Cesare Pautasso, and Paul Rimba, "A taxonomy of blockchain-based systems for architecture design", Software Architecture, IEEE, pp. 243-252, 2017
5. Bonneau, Joseph, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua A. Kroll, and Edward W. Felten, "Sok: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies", Security and Privacy (SP), IEEE, pp. 104-121, 2015
6. Halpin, Harry, and Marta Piekarska. "Introduction to Security and Privacy on the Blockchain." Security and Privacy Workshops, IEEE, pp. 1-3, 2017
7. Conoscenti, Marco, Antonio Vetro, and Juan Carlos De Martin. "Peer to Peer for Privacy and Decentralization in the Internet of Things." Software Engineering Companion, 2017 IEEE, pp. 288-290, 2017
8. Bocek, Thomas, Bruno B. Rodrigues, Tim Strasser, and Burkhard Stiller, "Blockchains everywhere-a use-case of blockchains in the pharma supply-chain", Integrated Network and Service Management (IM), IEEE, pp. 772-777, 2017
9. Zyskind, Guy, and Oz Nathan. "Decentralizing privacy: Using blockchain to protect personal data." In Security and Privacy Workshops (SPW), 2015 IEEE, pp. 180-184. IEEE, 2015
10. Ateniese, Giuseppe, Bernardo Magri, Daniele Venturi, and Ewerton Andrade. "Redactable blockchain–or–rewriting history in bitcoin and friends." In Security and Privacy (EuroS&P), 2017 IEEE European Symposium on, pp. 111-126. IEEE, 2017
11. Göbel, J., and A. E. Krzesinski, "Increased block size and Bitcoin blockchain dynamics", In Telecommunication Networks and Applications Conference (ITNAC), IEEE, pp. 1-6, 2017.
12. Chen, Po-Wei, Bo-Sian Jiang, and Chia-Hui Wang, "Blockchain-based payment collection supervision system using pervasive bitcoin digital wallet", In Wireless and Mobile Computing, Networking and Communications (WiMob), IEEE, pp. 139-146, 2017.
13. Buchmann, Nicolas, Christian Rathgeb, Harald Baier, Christoph Busch, and Marian Margraf, "Enhancing Breeder Document Long-Term Security Using Blockchain Technology", In Computer Software and Applications Conference (COMPSAC), IEEE, Vol. 2, pp. 744-748, 2017.
14. Xu, Xiwei, Ingo Weber, Mark Staples, Liming Zhu, Jan Bosch, Len Bass, Cesare Pautasso, and Paul Rimba, "A taxonomy of blockchain-based systems for architecture design", In Software Architecture (ICSA), IEEE, pp. 243-252, 2017.
15. Jin, Tong, Xiang Zhang, Yirui Liu, and Kai Lei, "BlockNDN: A bitcoin blockchain decentralized system over named data networking", In Ubiquitous and Future Networks (ICUFN), IEEE, pp. 75-80, 2017