International Journal of Engineering & Technology, 7 (1.1) (2018) 401-405

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Redactable blockchain and it's implementation in bitcoin

Krovi Rajasekhar [1] *, Sri Harshini Yalavarthy [1], Sravani Mullapudi [1], M.Gowtham [1]

[1] Koneru Lakshmaiah Educational Foundation
**Corresponding author E-mail: harshini.asr@gmail.com*

Abstract

A Blockchain is a ledger of records. It originally came from the digital currency bitcoin. Its main features are transparency and accountability. For this we use chameleon hashing concept which uses a trapdoor key. Unless the trapdoor is used it is hard to find collisions. We can create collisions only if we know the trapdoor and can rewrite the block of data with the new redacted stored files in blocks are permanently recorded and cannot be modified. To overcome this, we use the new redaction capability and expand its usefulness for enterprises and also in financial sector. This could limit uses in financial sector for the services because this must require data to be changed or smashed, coding and transaction mistakes might happen, which can be undone through redaction. An unchangeable record is not useful for the applications that area used for blockchain. Wherever the blockchain is used, either for a code or data there should be a way to redact it in unavoidable situations. The constraints for redacting a blockchain should be strict and can be done with whole block. We use this redaction concept with the bitcoin technology, which is a person-to-person digital cash system.

Keywords: *Blockchain; Bitcoin; Chameleon Hash Functions; Redaction; Transactions.*

1. Introduction

In late 2008, Satoshi Nakamoto who was brilliant in mathematics has come across a concept called Bicoin, a peer-to-peer Electronic cash system. In that he introduced bitcoins as a virtual currency that could essentially work as online cash [3]. The word – Bitcoin is made up of bit and coin that literally stands for digital/virtual currency. Implemented as an open source code, the Bitcoin technology is the world's first ever completely decentralized digital payment system. The technology soon became an interesting affair for the developers across the globe. Bitcoin technology being a decentralized system allows banks and other organizations to settle transactions without depending on the centralized systems.

Bitcoin depends on digital signatures, proofs of work and peer-to-peer networking to make a blockchain ledger of transactions. Digital currency called bitcoin is the simplest implementation of the blockchain technology [2]. Bitcoin uses a language which is used to build blocks such as smart contract, which are locked by digital signatures and can only be opened under certain verified conditions. The blockchain technology challenges our normal way of transactions and blockchain start-ups have received more than $1 billion of venture capital money to exploit this technology for various applications such as voting, record keeping, etc. Normal daily services are centralized and will not hold up well. Blockchain allows the services to be decentralized completely. We need not depend on a third single trusted party for our daily services if we use blockchain. It is revolutionary technology that challenges the current day transactions that are being done in a conventional manner. Smart contract are becoming popular in business agreements since the constraints can execute themselves leading to perfect execution and by reduces costs by providing transparency [5].

Block chain is considered vey revolutionary these days. Because, blocks are mined every 10 minutes on average, and the Bitcoin scripting language is not Turing complete [1]. The bitcoin scripting technology helps in solving the limitations of digital currency which makes it hard to hack. Other than blocks approach we can build alternate blockchains not which guarantees desired features and full decentralization. It allows a high degree of automation in smart contracts.

2. Blockchain

The blockchain is a ledger of records stored in a file structure called block, or a distributed database of records, or a public ledger of all transactions that have been executed and shared among the parties which have been participated in the transaction. Transactions that are stored in the block are immutable i.e. the information can never be modified or vanished [4]. These transactions that are executed during a given period of time are recorded into file called a block. The blocks are added to the blockchain in a linear or chronological order [6]. Each a time a block gets completed a new block is generated. The blockchain contains a certain and verifiable record block of every single transaction that has been ever made.

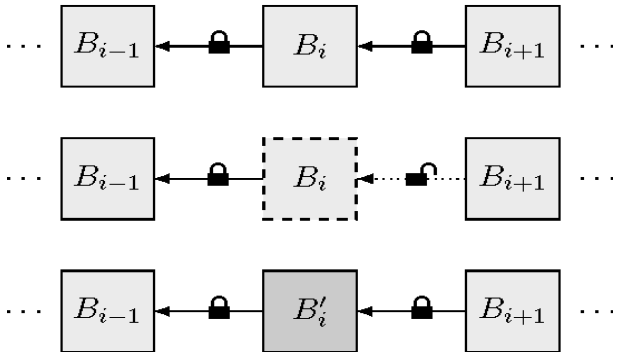

Fig. 1: Block in A Blockchain Being Redacted.

Copyright © 2018 Krovi Rajasekhar et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The blockchain eliminates the risk of data loss by storing data across its network. Blockchain security methods use encryption technology. This encryption methodology is based on public and private keys [7]. A public key is user's address on the blockchain and consists of a string of randomly generated numbers. The blockchain eliminates the risk of data loss by storing data across its network. Blockchain security methods use encryption technology. This encryption methodology is based on public and private keys. A public key is user's address on the blockchain and with a string of randomly generated numbers [14].

2.1. Public and private blockchains

In blockchain technology, Private Blockchain and Public Blockchain happen when enterprises financially started exploring the various blocks in the Blockchain technology. These two Blockchain technologies are arising up with the various businesses dealt models to know the major difference between these two blockchains [8]. The private blockchain produces at a less cost and faster than the public blockchain. At the initial stage of development, the blockchain has been an interesting topic to deal globally. At present, it is being a united part in the financial sectors of the digital world. The major differences between the blockchains are whether to identify its private or public blockchains [9]. As of now, many analyzers are arguing that the private blockchains are not the blockchains because the nature of blockchains changes because they reduce the third party persons to know the effect of transactions.

2.1.1. Public blockchain

Ethereum and Bitcoin are blockchains that are easy to be accessed to everyone. The public blockchain has the major factor that no one can access the information which is on the blockchain or the laws of the blockchain. According to users, no one will have access to change the protocols of the blockchain and also the information that is on the blockchain. Therefore, the persons who uses the public blockchain can wholeheartedly have trust in a third party to use the blockchain. Since it is a decentralized party, every miner in the network knows about the blockchain but can access it only with the private key.

The major drawback in public blockchain is that the computers and miners involved in the network require a large amount of computational power to maintain a ledger distributed to all the miners at a very large scale. Every node involved in the network should go through proof of work which involves solving a consensus integrity crypto graphical problem in synchronization with the other miners.

Other disadvantage is that public blockchain will not guarantee the privacy and security notion. Being a public blockchain it is too open to the other miners which makes it prone to the eavesdropping or thwart hacking [4].

2.1.2. Private blockchains

The private blockchains are handled by an organisation. This blockchain has access only to the individuals who has the permission to handle the blockchain by having its proof. Private blockchains are generally databases which can be regarded as a distributed record [7]. The transactions in private blockchain are easy and feasible compared to the public bitcoin blockchain. Since the public transactions has slow processing of the transaction records compared to the private blockchain, the transaction ledger with more data prefers a private blockchain. Depending on their respective advantages both the blockchains are used in different industries of the blockchain. The financial institutions prefer to promote both the blockchains in order to get enough profits for the investment of the finances in both the blockchain developments.

2.1.3. Similarities

Even though they differ in some aspects, both the blockchains do share some similarities

- Both are peer-to-peer networks which only allow the transactions signed digitally using a crypto graphical complex problem.
- Both assure the parties that even when some malicious users are present in the network, the ledger remain unchanged.
- Both the blockchains use a consensus algorithm which records the consensus of all the parties in the network [10].

Private blockchains are like shared databases and they are used to solve efficiency issues like fraud and security. If we add public node to the private blockchain it is no different than the public blockchain.

3. Redaction

Blockchain being an immutable cannot be changed. This could limit uses in financial sector for the services because this must require data to be changed or smashed, coding and transaction mistakes happen, and capacity and costs for retaining data need to be controlled. An unchangeable record is not appropriate for some applications. Once the record or block is created in blockchain it cannot be changed but in some situations changes should be done to remove or modify the content. Redactions should be performed only under strict constraints, and with full transparency and accountability. For redaction we use advanced chameleon hash function. This is different than the original chameleon hash function. In strandard chameleon hash function the trapdoor key is not shown publicly. But redaction technique uses collisions to find the redactable blocks .In order to generate the collisions we need trapdoor. A chameleon hash is a cryptographic hash function [11]. We integrate this hash function with the bitcoin technology making it more feasible for changes.

The concept of redactable blockchain is to associate the secret key to every link of the blockchain. Absence of secret key leads to immutable blockchain and makes it hard to find the collisions. By considering secret key, it is possible to easily find the collisions and re-write the content in the blockchain. Redaction can also be done with deletion, modification and insertion of multiple blocks with the help of secret key. If the secret trapdoor key is lost or destroyed, the new blockchain changes to immutable blockchain.

The main reasons for using a redactable blockchain for bitcoins are improper content being stored as arbitrary messages and rewritable storage in bitcoin [12]. Some miners who want to compromise the bitcoin system associate the improper content blocks with records. Therefore, so many users will not download and participate in the mining, since the blockchain with improper content is visible to all the miners. So, adding new block will not do any good if the old improper content blocks are still visible to all the miners and they take up so much space. The redactable technique helps us overwrite the improper content in the blockchain.

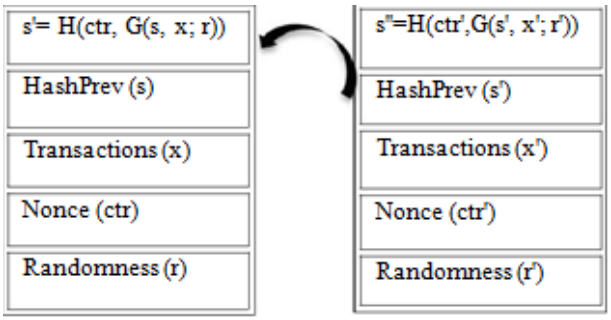

Fig. 2: Every Block Points to Its Previous Block.

4. Bitcoin

Bitcoin is a decentralized system in which the economic value is assigned. Bitcoin is a computer network software protocol used to do the digital transactions. In bitcoin network the currency is digital and the transactions are also done digitally. Blockchain is a public ledger and is an instance of bitcoin. It is assumed that for every five or ten minutes a new block is added to the blockchian. It checks the chain for every ten minutes for the new transactions. It gives information on how many bitcoins are there in the assigned public address [8]. Generally public address comprises of 27 to 34 character uppercase strings, digits from 0 to 9, lowercase letters that is base 58. Every public address maintains a private key, so the person in the possession of the private key can spend the bitcoins. Private keys have 51 characters more than the public address but the format is same Private Key is necessary for the transaction because b using the private key you sign the digital transaction cryptographically. Thus, the bitcoins are sent to other addresses. Then the change in amount of your bitcoins is broadcasted to the whole network and the ledger records that your bitcoins are now sent to the other address in 10 minutes as mentioned above.

4.1. Processing - mining

Mining enforces sequential order of blocks and protects the neutrality of the network. It prevents the adding of blocks by any miner easily. If the blocks are added irrespective of rules then then the blocks that follow the newly added blocks get invalid. All the computers that participate in the bitcoin network are called miners. These miners get competitive about sensing a change and writing a new block because the computer that solves the puzzle and writes a new block will be awarded a new bitcoin. The reward associated with each block began at 50 in 2009, is now 25, and will halve every 4 years, until an ultimate quantity of 21 million bitcoin are created. Transparency plays a large role in bitcoin maintenance. All confirmed transactions are appended in the block chain. By this the transactions and the amount possessed by every miner is noted. The integrity, authentication and the chronological order of the blocks can be protected through cryptography [12].

5. Related work

5.1. Blockchain using hashing

To understand blocks we need to understand hash function. A hash function mapping a set of inputs will result to another output set. We use hashing for different applications for storing of data and lookup by logging into any password oriented protected systems. It is also used in verifying the data integrity.
To redact the blockchain, we undergo the following actions:

- Rewriting the blocks
- Compression of any number of blocks
- Adding the blocks.

The redaction technique can be done by only specific authorized miners since un-experienced miners will not be showcased with these particular skills and this could lead to the blockchain disruption. Among these above actions, redaction technique is mostly used in rewriting the blocks to overcome the improper content in the blockchain [10].

5.1.1. Chameleon hash function

A Chameleon hash is a cryptographic hash function that contains a trapdoor. This hash function computes the hash value of the given message m. After hashing, signature follows. It uses a trapdoor function to generate the collisions efficiently .We can recreate algorithms that link two separate blocks through the use of secure private keys.

Once a change has been made, the standard hash is broken, leaving evidence of the change. The chameleon hash stays intact and maintains the link between the edited and existing blocks.

For any m, m', r r'$\leftarrow h^{-1}$ (td, m, r, m') (1)

From finding r', we can prove the following equation:

h^{-1} (ek, m, r) = h (ek, m', r'), Where

m, m' are Two messages r, r' are Two numbers

ch (m, r) = ch (m', r') where m$\neq$ m' (2)

Here the two messages m and m' use the same hash function but different random numbers as in (1). When we apply the chameleon hash function on both of messages as in (2) it leads to collision. With the help of a secret key we find collisions. And then we replace the changed or modified block with the old block in the chain.
The evolution of the chameleon hash function is special hash function. This special hash function is collision-resistant unless a secret key is known. The main difference between the standard hash and special hash is that in the improved design it is okay to reveal the number of collisions unlike standard hash in which the collision is kept secret because it can reveal the secret key.

5.1.2. Trapdoor function

A trapdoor function is referred as one-way function that is very easy to compute, but has a secret key which helps us to calculate the inverse operation i.e. if 'f' is trapdoor function, then y=f(x) is easy to compute without some key K. For the given K, it is to very easy to compute $y=f^{-1}$ (x, K). A hash function and trapdoor function are bit different as the hash function is not reversible. Instead it is called a one-way function. The trapdoor function can be inversed using the knowledge K. A one-way function is very similar to trapdoor function as it is very easy to compute but very hard to reverse as there is no general key that allows you to inverse the above one-way function.

6. Proposed work

6.1. Key management

The management of trapdoor key for the chameleon hash function is entirely application dependent. To explain this we quote the following three types of blockchains which explains us how the trapdoor key being managed among the different authorities. In the each case below, we clearly explained about the trapdoor key management [2].

- Private blockchain: This blockchain, is widely used in the financial sector. The central authority is only given write permissions, and the read permissions may be public or restricted. In this organized way, the key management becomes simple in this blockchain, the trapdoor key will be authorized with a specific person who has the right to compute collisions and therefore redact blocks.
- Private blockchain: This blockchain, is widely used in the financial sector. The central authority is only given write permissions, and the read permissions may be public or restricted. In this organized way, the key management becomes simple in this blockchain, the trapdoor key will be authorized with a specific person which has the right to compute collisions and therefore redact blocks.
- Public blockchain: This type of blockchain is completely decentralized, and all parties are allowed to send transactions to the network and have the transactions included in the blockchain as long as the transactions are valid. The

consensus process is independent and not controlled by any party. The best example of a public blockchain is Bitcoin.

6.1.1. Using private blockchain

Promisingly, re-writing the content of the old block is possible when the hash function finds a collision, in the cases when the hash function is same and the content is different, without modifying the outer hash function H. Here, we explain the idea in the simple way where only a trusted central authority is able to redact the blockchain.

A block is a triple of the form B = (s, x, ctr), where $s \in \{0, 1\}^k$, $x \in \{0, 1\}^*$ and $ctr \in N$. Block B is valid if

validblockDq (B):= (H (ctr, G (s, x)) < D)∧ (ctr < q) = 1

A block is a tuple B: = s, x, ctr, (h, ξ), where the components s, x and ctr are the same as above explained, and the new component (h, ξ) is the check pair for the chameleon hash function. The function G is defined as a secret-coin chameleon hash CH = (HGen, Hash,HVer, HCol), and the validation predicate for a block will now equal to

validblockDq (B) := (H(ctr, h) < D) ∧ (HVer(hk, (s, x), (h, ξ))) ∧ (ctr < q) = 1.

Here we do not need to store the hash value h, because this value is computed as a deterministic function's input and randomness of the chameleon hash. Here, in this case, a block has a type B: = s, x, ctr, r, where r is the randomness for the chameleon hash. The predicate of validation for a block becomes

validblockDq (B) := (H (ctr , Hash(hk, (s,xz); r)) < D) ∧ (ctr < q) = 1.

6.1.2. Re-writing blocks

Input : The input for the rewriting the blocks consists a chain C with length n, block indices denoted with I where I should be the subset of the blocks n , and the chameleon hash function and a trapdoor key tk which is shared to the miners.
Description: The main idea behind this algorithm is when a block is to be redacted a hash is computed to see if there are collisions for that hash of the block in which the new content or the rewritable content is present x'. The old chain is replaced by the new chain C', which has the modified block to replace the old one. After the new chain is created in place of old one it is broadcasted to the every node. This process is done for every transaction implying that every miner of the system should use this new redacted chain in favor of the old chain, even longer ones.
Algorithm:

C' ← C;

Parse the chain C_ as (B1 to Bn); for i: = 1 to n do

if i ∈ I then

Update the i-th block of C1as

Bi: = _si, xi, ctr i, (hi, ξi) _;

ξ' ← HCol(tk , (hi, si||xi, ξi), (si||x'i));

B':= si, xi, ctr i, (hi, ξi);

C' ← Cn−i+1||Bi||i1C1;

End

End return C'

Output: By applying this algorithm we obtain a redacted block chain of length n.
Every time a block is redacted using the above algorithm a collision for the underlying chameleon hash function is given away. Hence, it is important that collisions do not expose the secret trapdoor key because the exposure leads unauthorized users rewrite the blocks. This can disrupt the whole bitcoin system. For example, when changes occur it is enough to just broadcast the modified blocks and telling the blocks to do modification in their old copy of the blockchain. In this instance the list of changes can be identified by the digital signatures for correct authentication. In this way the user need not download the whole blockchain.

7. Literature survey

The blockchain technology is already used in the bitcoin protocol. The protocol has some supporting algorithms. For individual companies the blockchain technology may seem as a threat even though it presents promising economic growth. In financial industries there are some regulatory requirements that are demanded by the customers like keeping their information private. This can be solved through homomorphic encryption which allows the transactions done on encrypted data. One of the many drawbacks of blockchain is network latency, since the bitcoin strategy allows you to check for every 10 minutes. If there is no transaction in the 10 minutes it affects the network latency. The other drawback is throughput since the retail industries now allow 10000 transactions per second [3].
Chain validation:
The chain validation algorithm generally validates the properties of the chain C. This algorithm contains some input values and a hash function to take that input values. The algorithm using these parameters performs the content validation V for each block. The algorithm checks the validation of the work properly done and that the previous block's hash is properly added in the current block for each block of the chain. In this way the input parameters are given to the hash function and the validation is done if the result is failed then the whole chain is rejected. The predicate value V is not determined at first.
Chain comparison:
This algorithm is responsible for comparing the chains of bitcoin or blockchain and orders them in priority. This algorithm uses a function for the ordering the space of the chains. It is a straight forward algorithm and is parameterized by a max ( ) function which applies to the chains. In the max ( ) function two chains let C1 and C2 then the max function returns the longest of the two chains. If the length of the C1 and length of the C2 then other than the length some other characteristics will be applied to the chains to break the tie. Other alternatives like picking chain at random or using the lexicographical order. This will be performed independently to the tie breaking rule [13].
In block chain the chains with the longest order is used in most cases. Because the latest transactions in bitcoin which are stored in the form of the blocks are appended to the existing chain or the previous transaction blocks are added to the new blocks making it the largest. Blockchain is the biggest or greatest innovation of the bitcoin. In bitcoin the transactions are visible to all the miners. To make this possible the blockchain is broadcasted to all the nodes or the miners by using flooding algorithm.

8. Conclusion

Since an immutable blockchain would not be editable, the redactable blockchain which has been proposed in this paper, helps us in re-writing the subject of many number of blocks in decentralized services using the blockchain technology. To implement this we have used chameleon hashing along with private blockchain method. We used a public hash key and a secret trapdoor

key as inputs for the hash verification algorithm in chameleon hash function to find collisions. This modified chameleon algorithm's main purpose is to find the collisions unlike the normal chameleon algorithm, which intends to hide the collisions. Thus, the current blockchain is replaced with the redacted blockchain. The redacted blockchain is integrated with the bitcoin transaction.

References

[1] S. Nakamoto. Bitcoincorehttps://github.com/bitcoin/bitcoin,
[2] OpenSSL project. http://www.openssl.org/.
[3] M. Andrychowicz, S. Dziembowski, D. Malinowski, and L. Mazurek. Secure multiparty computations on Bitcoin. In IEEE Symposium on Security and Privacy. https://doi.org/10.1109/SP.2014.35.
[4] M. Andrychowicz, S. Dziembowski, D. Malinowski, and L. Mazurek. On the malleability of bitcoin transactions. InFinancial Crypto, pages 1-18, 2015. https://doi.org/10.1007/978-3-662-48051-9_1.
[5] AdambackHashcash.http://www.cyphers pace.org/hashcash, 1997.
[6] Krawczyk, H. Rabin, T: Chameleon signatures.In Proceedings of NDSS 2000. (2000) 143–154.
[7] https://spectrum.ieee.org/computing/networ ks/the-future-of-the-web-looks-a-lot-like-bitcoin/four-cool-things-you-can-do-with-the-blockchain.
[8] https://newsroom.accenture.com/news/accen ture-debuts-prototype-ofeditable-blockchain-for-enterprise-and-permissioned-systems.html. Accenture debuts prototype of editable blockchain for enterprise and permissioned systems.
[9] J. A. Garay, A. Kiayias, and N. Leonardos. The Bitcoin backboneprotocol: Analysis and applications. In EUROCRYPT, pages 281– 310, 2015.
[10] G. Ateniese and B. de Medeiros. On the key exposure problem in chameleon hashes. In SCN, pages 165–179, 2004.
[11] S. I. of Technology. Blockchain just got much more powerful. https://www.stevens.edu/news/blockchain-just-got-much-more-powerful.
[12] V. Buterin. On public and private blockchains https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/.
[13] http://www.coindesk.com/bitcoinventure-capital Coindesk. Bitcoin venture capital.
[14] K. Petrasic and M. Bornfreund. Beyond bitcoin:The blockchain revolution in financial services: http://www.whitecase.com/publications/insi ght/beyond-bitcoin-blockchain-revolution-financial-services.