International Journal of Engineering & Technology, 7 (1.1) (2018) 667-670

International Journal of Engineering & Technology

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

Research paper

Enhancement of block chain security using re authentication of digital signatures

K Rajasekhar [1], N Raga Rohith [2] *, G N V Krishna Mohan [2], D Divya [2],Ch Jaya Bharathi [2]

[1] *Professor, Department of computer science and engineering, Koneru Lakshmaiah Educational Foundation*
[2] *Student, Department of computer science and engineering, Koneru Lakshmaiah Educational Foundation*
**Corresponding author E-mail: rohithraga.aiesec@gmail.com*

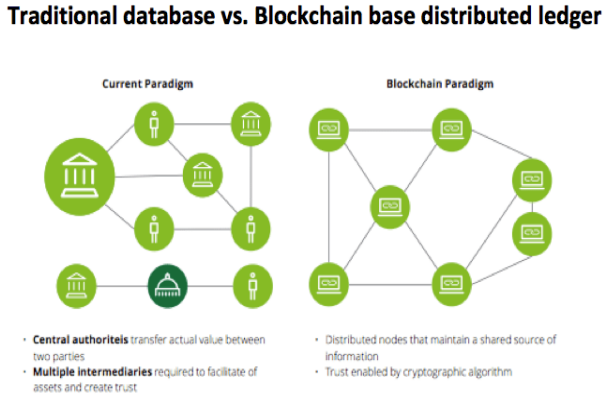
Abstract

Block chain technology first got confined to crypto currencies but later has seen its image in varied applications and hence there is a lot of need to improve its security according to the application. Because of the current digital world revolution there are both the need of its implementation for safe and secure transactions, implementations and at the same time the threats it has been facing day by day. This also could be more efficiently implemented when there is a regulating authority set over for the whole network to whom a particular user can ask to if there is any problem. In this paper we are going to see mainly about the working of block chain technology and security threats of block chain and how can we overcome one of the threats i.e 51% attack. We also are going to see its varied applications in different fields and types of block chains which can be implemented in different applications.

Keywords: *Block chain; Block chain in Banking; Block chain Security; Bit coin; Digital Signature; Proof of Work; Security; 51% attack.*

1. Introduction

Block chain is a decentralized and distributed form of ledger maintenance protocol where every transaction and change made by any other in the system could be seen by each and every one. In simple words it can be said as an open ledger or a leader less application protocol. But when did this application got implemented? This technology was first introduced by Satoshi nakamoto (an anonymous group or could be a person) and got implemented in the year 2008 as a background for bitcoins. The combination of the words block and chain simply explains the chain or series of blocks connected to each other [1].

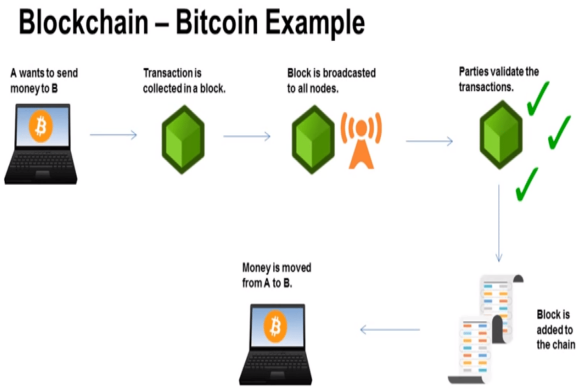


2. Let us also know what actually a bitcoin is?

A bitcoin is a digital currency first released by satoshi nakomoto and later obtained after the miners solve the complex mathematical computations which generally known as Proof of Work and the maximum limit of the number of bitcoins that can be generated is 21 million.

3. How does it work?

The actual working of block chain can be seen perfectly in bitcoin currently. There could be different types of block chains based on its type of use and accessibility to authenticate a transaction.as we know that block chain is a distributed ledger sometimes not everyone gets the accessibility or permission to authenticate a particular transaction[2]. For example let us consider the case of bitcoin transactions. In a bit coin transaction there are the people who could and need to authenticate a particular transaction known as miners. These are the people who has a larger capability of computing the necessary protocols. The process in which the block chain works in case of bitcoin transaction is being explained in the following steps.



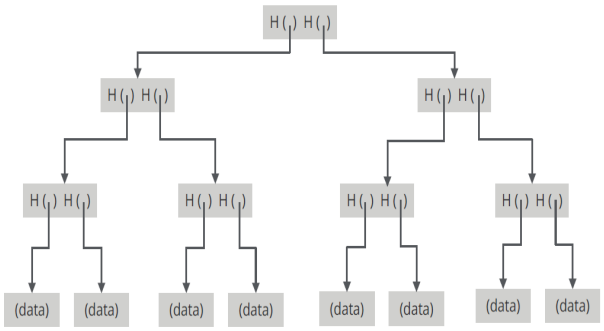
Copyright © 2018 K Rajasekhar et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

1) Let us consider two people A, B who wants to transact bitcoins between each other. So first A releases a request in to the decentralized system. This request is a digital signature formed from the combination of Alice private key, Bobs public key and the bitcoin by a technique called hashing. In bitcoin transactions we generally use hash-256 algorithm.
2) Now this digital signature known as a block is send to all the miners who are in the system. Only these miners can validate any transaction and for that they get incentives.
3) So they validate a particular transaction by the method called Proof of work. This Proof of work is a puzzle to be solved by the miners which require a lot of computation and hence the miners who have a large capacity of computation can solve it faster.
4) Once the Proof of work is done for a block it is broadcasted in the decentralized system and must be validate by at least 51% of the miners.
5) If once the other miners accept this Proof of work then this block will be added to the block chain which contains the hash of the previous block too thus maintaining the continuity.
6) Even if one block is modified it disturbs the chain as every block contains the hash of the previous block and thus it is well secured.
7) Once after the block is added to the chain then that transaction is said to be validated and the bitcoin would be transferred to B.

Here during the addition of every block which has been created by the miner every block consists of mainly few frames i.e. hash of the previous block, hash of the current block. If someone tries to modify the block as it is produced by an algorithm called hash(256) even a slight change in one particular block could disturb the whole hash code which there by breaks the chain. Hence after that it would be very difficult to create the broken chain as they have been created with a lot of computations from lot of miners[3]
The back ground of this block chain is the merkel tree which gets implemented in block chain.

4. Merkel tree

In simple words Merkel tree is nothing but the tree which has the data node and the data of the previous node. This tree generally uses the Hash of the previous data nodes to get constructed.



5. Proof of work

As discussed the miners generally does this proof of work for which they get rewards as in bit coins i.e. 12. 5 bit coins per transaction. This rate actually gets halved for every 4 years in 2009 it used to be 50 bit coins. Miner has to solve a complex mathematical problem for which he/she must show that he has spent significant amount of time and energy [4]. This protocol actually exists by default in the block chain and hence it must be solved by the miners. What exactly is this proof of work is the network generates a difficulty rate (number of prefixed 0's in front of) i.e.

CHALLENGE STRING➔SHA256 (SHA256 (header))
"Challenge string"+<guess the number nonce"=0000000000000000000000000000000000000000" 42 zeroes to be prefixed.

0+ (guess) 0=0000

0+ (guess) 0=0001

0+ (guess) 1=0002

0+ (guess) 2=0003

Miner has to come up with a number when combined with challenge string would produce 42 zeros.This number can be guessed only using brute force method.
Once the number is found the miner claims that he has solved the puzzle and this proof of work must be accepted by the majority of miners in the distributed system i.e. more than 51%.Only then that particular transaction is accepted.
When the miner creates a block or header it consists of 5 main frames.i.e 1)Bit coin version 2)previous block chain 3)Merkel root 4)Time stamp 5)Difficulty target 6)Nonce(answer that miner is trying to solve)

6. Types of block chains

Block chains are majorly classified in 3 types i. e:
1) Private block chain.
2) Permissioned Block chain.
3) Public Block chain.

Private Block chain: In this type of Block chain only one entity has to validate any application or transaction and all the writ authorities' lies with a single person.
Permissioned Block chain: In this type of Block chain only a limited users will have the authority to validate any transaction where these access is given by the main authority.
Public Block chain: In this type of Block chain the authority to validate any transaction can be done by anyone in the block chain this is the type of block chain that we are using in crypto currencies [5].

7. Key features of block chain

There are many important features of block chain, which can be seen from its implementation, and some of them are
1) Information consensus across multiple partners.
2) Time stamping.
3) Security.
4) Authenticity.
5) Resilience.
6) Data loss protection.
7) Data management.
8) Peer to peer connection etc.

Among the above mentioned features the one most important key feature is the information consensus across multiple partners or systems because if the data is lost or manipulated in one system it can be verified through all other systems because it is a distributed ledger and if found that there is a mis-management by any one particular peer that person can be removed from the distributed system easily by authentication of maximum miners and the lost data also can be retrieved easily as it has multiple copies throughout the distributed system [6].

8. Applications of block chain

Block chain technology as discussed is a decentralized system where it is completely transparent and hence more secure. Hence

this technology has a varied type of applications.This technology can be used in areas like E-commerce, global payements,Remittance,P2Plending,Micro finance, Loyalty programs, Supply chain, Ownership, Proof of identity, Intellectual property, Equity, Private markets, Debt, Crowd funding, Derivatives, Digital rights, Banking, Hospitals, Education system etc[7].

But how can this technology be used for varied type of applications is the real challenge. As we know that there are 3 types of block chains i.e. 1) Public block chain 2) Permissioned block chain 3) Private Block chain.

Every application can be implemented using one of these three types of block chain technologies.

The pillar of strength of a block chain is the type of Hash code using for the transactions.As we said there are different types of block chains it depends on the type of application that we choose decides the type of block chain that we use[8]

9. Block chain technology in banking

Block chain technology can be implemented at its best in banking sector which also has its highest need. As we all know that any transaction that we do in ATMs in banking has to be validated both by the account holding bank and the bank through which we are transacting. In this case the problem that we could face is if any of the servers of both the banks are busy the transaction gets delayed [9]. And in the same case if we introduce a Permissioned Block chain i.e. if we allow only banks to have an access so that any bank server could validate the transaction and if it is accepted by at least some other bank servers then the transaction could be done successfully. And this technology especially in banking has a lot of scope because it can avoid any wrong transactions in any bank and it also would be easy to find if there is any fraud that is happening in banking chain. This process also helps to the auditors of the bank to verify the ledgers that bank has undergone. This technology in banking can be implemented not just restricted to one particular country but throughout the world which could help international money transfers to be done at a faster rate. This also helps the current SWIFT system to link with the core banking system.

10. Threat currently facing by block chain

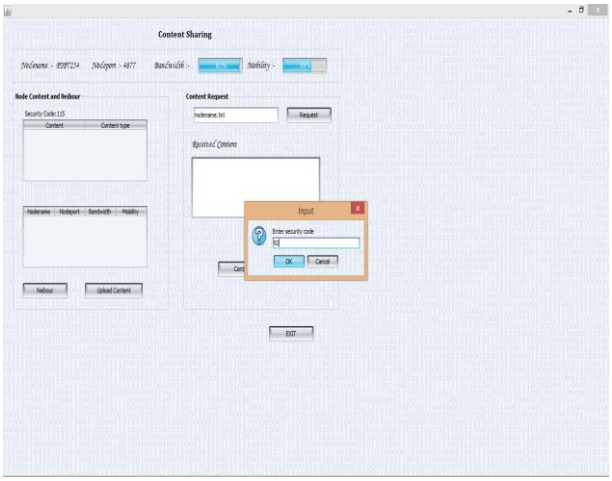
One of the major attacks faced by block chain is the 51% attack. Let us discuss this in detail with an example. Let us say two individuals want to transact the bitcoins. So let's say A has 5 bit coins and he want to send 4 bitcoins to B. The same time say another user C has requested A 3 bitcoins and say A has also sent this request to miners. Say if miners had parallely done the proof of work of both the transactions and then if 51% of the miners has accepted both the proof of works as they see only whether A has enough balance or not but not the number of transactions he has released into the network there could be a possibility of accepting both the transactions by at least 51% of the miners[10].

If both the transactions has got approved by the miners then one of the person i.e. B or C will be a loser. This is the current threat faced by this technology.

11. Recommended view of implementation for the threat and results

In block chain technology when a user wants to do a particular transaction he must first request his transaction which he must distribute in the network and when the nodes receive this request there are nodes which are also miners. Only these miners can validate a request.

So When a person A has 10 bitcoins and he would like to send 7 bit coins to B he sends a request in to the distributed system and at the same time if he sends a request of sending 6 bitcoins to C both the requests would get distributed in the system and if these requests are to be validated they must undergo a process called Proof of work and this proof of work is a process which requires lot of mathematical computations and also require a huge server space. Now what if both the proofs had done parallelly?or what if the proof of work of C is done first and then B where the transaction of B gets denied? [11] So the proposed idea is what if we block a user say A after his first proposal and A can only do another transaction after either his request gets denied or accepted. Then we can rightfully know about a particular transaction whether the transaction is done or not. It also can be done with another way by re authenticating with the digital signature from the beneficiary that he is the rightful owner for a particular transaction by having his public key, senders public key and the request key which gets generated at miner point. Hence by having a re-authentication from B and by blocking A we can improve the security of block chain and we also can avoid attacks like 51% attack or majority attack.



The process goes as follows. Once after the proof of work is done by the miner the miner asks to validate whether the transaction is in between A and B or not for both A and B after blocking A so that no further transactions occur. Now both the users must enter their public keys in order to confirm the transaction that is going to be done between them. Once after both the people sending their public keys the miner checks it and after he doing the proof of work he could validate this transaction.

By this method we are able to maintain the authenticity by having re authentication using digital signatures and also a type of confirmation that transaction is being done between the two right full users.

12. Conclusion

Block chain technology which has got implemented through bitcoins has brought the digital revolution in varied applications throughout the world. It can not only be implemented in crypto currencies but also in each and every application that we use in daily lives. Hence there is a lot more need in order to protect from its vulnerabilities. Here we need to know that the more it gets distributed among the people the more vulnerable it gets because there is every chance of its bad implementation and this technology can be well implemented if there is a particular regulating authority differently according to its field. Block chain also has its implementation at larger scale in creating new business models. As we discussed above the threat currently being faced by the block chain is the 51% attack or the majority attack for which we have proposed a solution i.e. re-authentication of digital signatures which has both the users' public key. If this could be implemented well not just this but it can avoid many other attacks.

References

[1] Juan Garay, Aggelos Kiayias, and Nikos Leonardos. The bitcoin backbone protocol: Analysis and applications. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 281–310. Springer, 2011.

[2] Chapter the block chain security for improving distributionshttp://chimera.labs.oreilly.com/books/ 1234000079/ ch07.html/.

[3] bitcoin/src/chainparams.cpp,https://github.com/bitcoin/bicoin /src/chainparams.cpp#L123.

[4] Why use of bitcoin in near future at every print http://www.coindesk.com/information/why-usebitcoin/ spectrum.ieee.org-static-special-report-block chain-world

[5] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System,"*Www.Bitcoin.Org*, p. 9, 2008.

[6] S. Underwood, "Blockchain beyond bitcoin," *Commun. ACM*, vol.59, no. 11, pp. 15–17, 2016.

[7] Spectrum.ieee.org-computing-networks-blockchains-how-they-work-and-why-theyll-change-the-world.

[8] Banks Look to Block chain To Reduce Fraud In $4 Trillion Trade.

[9] Finance Field at emergence of cryptosystems in blocks, https://www.cryptocoinsnews.com/banks blockchaintrade-Finance-fraud.

[10] Spectrum.ieee.org-tag-blockchain+technology.

[11] A Textbook on Block chain dummies-Manav gupta.