IJCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.-7, Special Issue-10, May 2019 E-ISSN: 2347-2693

Improving Security of Blockchain Through Authorisation

Vivek Sharma[1*], Nagendra Kumar[2]

[1,2]SRIST, Jabalpur, Madhya Pradesh, India

[*]*Corresponding Author: viveksrgi99@gmail.com, Tel.: +919981946482*

DOI: https://doi.org/10.26438/ijcse/v7si10.111114 | Available online at: www.ijcseonline.org

Abstract— Blockchain is the chain of blocks and each block consists a time stamp, transaction data and a cryptographic hash of previous block. It is a decentralized distributed network in which each peer node connected with each other and shares history of all the transactions. Each new block added to blockchain whenever a transaction occur need to be verified by all the peer node and transaction executed successfully if more that 50% allows. There are some vulnerabilities which are present in Blockchain because of its publicly open network and lack of security certification. We tried to modify the Blockchain with the use of smart contracts with the existing blockchain network and using X.509 Certification for specifying the permission allotted to each peer node at the time it is added to the network.

Keywords—Blockchain,Block,Node,X.509Certificate,Cryptographic,Hash,Vulnerabilities

I. INTRODUCTION

The blockchain is a distributed database containing records of transactions that are shared among participating members. Each transaction is confirmed by the consensus of a majority of the members, making fraudulent transactions unable to pass collective confirmation. Once a record is created and accepted by the blockchain, it can never be altered or disappear. [1] Blockchain technology enables distributed, encrypted and secure logging of digital transactions. It is the underlying technology of Bitcoin and other cryptocurrencies. Blockchain is expected to revolutionize computing in several areas, particularly where centralization was unnatural and privacy was important.[2] Since its introduction in the early 1980s (Chaum, 1982), the design of e-cash has always been one of the main research topics in the field of cryptography. However, the one without any trusted third party remained an open problem till Bitcoin(Nakamoto) launched in 2009. Due to its decentralization, unforgeability, double-spending resistance and pseudonymity, this brand new e-cash system has brought a remarkable culmination of cryptocurrency research and its applications. Based on its main framework, many new cryptocurrencies including decentralized (such as (Litecoin), Nxtcoin (Nxt)) and centralized ones (such as RScoin (Danezis and Meiklejohn, 2016)) have been proposed. The market value of these cryptocurrencies has increased more than 30 times during 2017 (from about $17 billion on 1st Jan. to $591 billion on 31st Dec.) (Coinmarketcap). As the core technology behind Bitcoin, the blockchain has demonstrated its capability of innovation and infiltration in many domains, including finance, insurance, industry, healthcare, agriculture and so on (Romano and Schmid, 2017; Tasca et al., 2017). For example, the blockchain technology, combined with the cloud computing and Intel® SGX (Software Guard Extensions), would give us an opportunity for alleviating cost and risk caused by trust third parties (Romano and Schmid, 2017), which will have a pervasive impact on the future of our society (Tasca et al., 2017). However, Bitcoin is not yet an ideal e-cash system. The privacy leakage is one of the main problems. For instance, anyone can see the payer's bitcoin address, payee's bitcoin address, and the content of each transaction in the bitcoin blockchain. To solve this issue, many advanced cryptographic primitives, such as ring signature (van Saberhagen, 2013), zero-knowledge proof (Miers et al., 2013; Ben-Sasson et al., 2014a) have been adopted in blockchains.[3]

II. RELATED WORK

1) Title: S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, 2008.

Problem Statement: Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for nonreversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

Objectives: A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.[4]

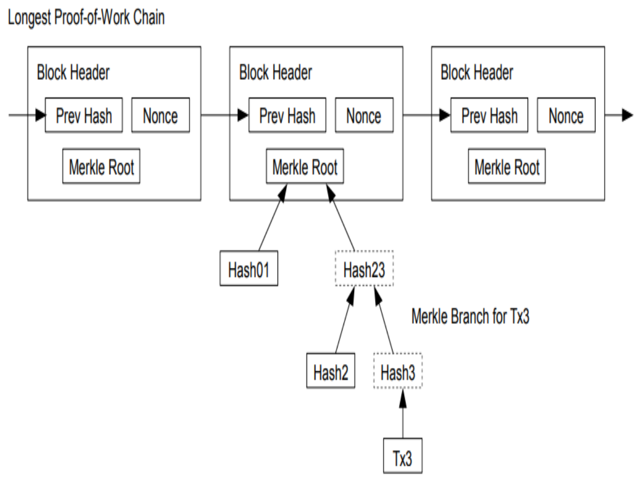


Figure 1. Working Of BLOCKCHAIN[3]

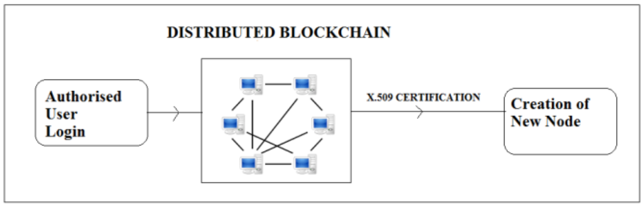
An algorithm that enables a set of processes to reach a common decision is called a consensus algorithm. In this case, that common decision is agreement on the current configuration by a set of operational replicas. Given our problem context, we'll call the participants replicas instead of processes. But the algorithm we describe works for general consensus, not just for deciding on the current configuration. One problem with such consensus algorithms is that multiple replicas may be trying to drive a common decision at the same time. It's important that different replicas don't drive the replicas toward different decisions.[5]

Cryptocurrencies have seen a massive surge in popularity and behind these new virtual currencies is an innovative technology called the blockchain: a distributed digital ledger in which cryptocurrency transactions are recorded after having been verified. The transactions within a ledger are verified by multiple clients or "validators," within the cryptocurrency's peer-to-peer network using one of many varied consensus algorithms for resolving the problem of reliability in a network involving multiple unreliable nodes. The most widely used consensus algorithms are the Proof of Work (PoW) algorithm and the Proof of Stake (PoS) algorithm; however, there are also other consensus algorithms which utilize alternative implementations of PoW and PoS, as well as other hybrid implementations and some altogether new consensus strategies. [6]

Algorithm Of BLOCKCHAIN:
Step1: Initiating transaction, blockhash, previous hash in the system.
Step2: For addition of new block in the system, it need to satisfy mathematical equation through Poof Of Work(PoW) algorithm.
Step 3: If current blockhash doesn't be supported by more than 50% of block nodes in the network, new node cannot be added to the network.
Step 4: Each block node in the network of blockchain shares transaction to verify the reliability of block node.
Step 5: Each node updated whenever new one added in the network.

III. METHODOLOGY

We are using SSH certificate creation in consensus peer-peer decentralized network along with authorized user login:



X.509 certificates enable to affirm the distinguishing proof of the parties involved in the communication. As of now, majority of individuals and communities are using X.509 certificates to demonstrate their ID during on-line exchanges.[7] One of the most engaging aspects in managing distributed systems is the complexity of security management, mainly access control. The traditional Access Control List (ACL) cannot always be able to provide the desired level of security in large scale infrastructures. Many different access control techniques are available today, but Role Based Access Control (RBAC) and Attribute Based Access Control (ABAC) prevail. In the case of RBAC, access privileges are allocated to roles rather than to individual users. Therefore, RBAC has the advantage that it can significantly simplify the management of access controls for large numbers of users. ABAC, as a replacement for or adjunct to RBAC, performs decisions relying on attributes of requestors and resources, being more suitable for distributed systems. ABAC assigns attributes to users, which can be certified by specific authorities and later verified against access control policies. ABAC uses labeled objects and user attributes instead of permissions to provide access control. We can say that a role in ABAC can be regarded as a group of mixed attributes rather than representing an unitary group of permissions as in RBAC. The Privilege Management Infrastructure (PMI) is a concept that manages user authorizations by using the ITU-T X.509 Attribute Certificates (ACs) This was introduced in the 2001 version of X.509, and in 2005 a delegation service was added to improve the PMI. In 2009, an interdomain authorization was also added to enhance the current version of PMI. Using an analogy[8]

Algorithm:

Step 1: Creating a admin frame to login the blockchain network .

Step 2: Generation of generis block if not exist in the network.

Step 3: X.509 Certificate generation for improving the reliability of the system.

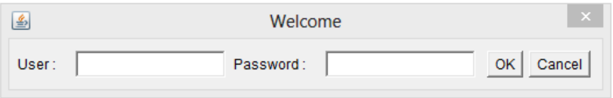
Step 4: Once smart contract condition satisfies the certification requirement, new block node added to system.

Step 5: All Block node hash history be updated along with the previously generated Block node.

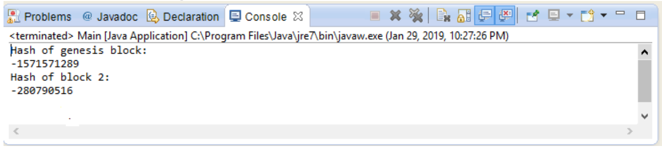
IV. RESULTS AND DISCUSSION

	Blockchain	Modified Blockchain
Permission	No need	Needed
Trust on 3rd Party	No	Yes
Voting System	Yes	Restricted to few
Consensus Algorithm	Proof Of Work	Proof Of Authority
Computation Power	HIGH	LESS
Node Participation	All presented nodes	Choosen ones
Smart Contract	No	Yes

1. Login Admin Frame

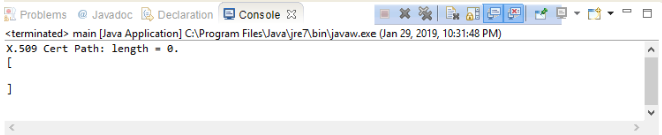


2. Existing Blocknodes



```
<terminated> Main [Java Application] C:\Program Files\Java\jre7\bin\javaw.exe (Jan 29, 2019, 10:27:26 PM)
Hash of genesis block:
-1571571289
Hash of block 2:
-280790516
```

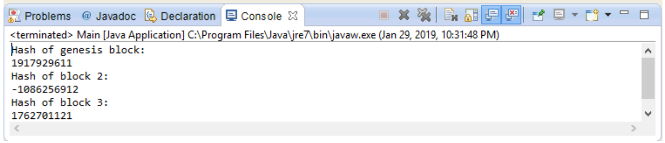
3. Certificate Generation for verifying trustability



```
<terminated> main [Java Application] C:\Program Files\Java\jre7\bin\javaw.exe (Jan 29, 2019, 10:31:48 PM)
X.509 Cert Path: length = 0.
[

]
```

4. New Hash Of Block 3 is added to Blockchain network



```
<terminated> Main [Java Application] C:\Program Files\Java\jre7\bin\javaw.exe (Jan 29, 2019, 10:31:48 PM)
Hash of genesis block:
1917929611
Hash of block 2:
-1086256912
Hash of block 3:
1762701121
```

V. CONCLUSION AND FUTURE SCOPE

Blockchain at present works on open network which enable anyone to access it by solving mathematical equation which requires lots of computational power and energy. Changes which we recommend reduces the need of large computational power as it is limited to accessed by authorised nodes only which will do all the transactions through it as participation of nodes be restricted to trusted individual who satisfies the requirement of smart contracts based on trusted X.509 certificate make it reliable to do only legal transactions which will restrict the use of blockchain network in any transaction for illegal work.

There is vast scope of blockchain , it can be used as backend application to manage resources perfectly, as changes need to be done by authorised individual which provide control over the resources which is not present because of anonymous use of network. By authorising , particular organisation need to manage all resources and it requires less computational power to secure the resources of the application.

ACKNOWLEDGMENT

Assistant Professor Nagendra Kumar, thanks for guiding me. H.O.D. Prateek gupta, Principal Biplab Paul, thanks for giving this golden opportunity for showcasing my Research Work in the "NATIONAL CONFERENCE ON RECENT TRENDS IN INTELLIGENT COMPUTING" conducted at

Shri Ram Group Of Institution, Jabalpur, Madhya Pradesh, India.

Sponsored By: AICTE/CSIR/DST/DRNOMPCOST

REFERENCES

[1]DMITRY EFANOV, PAVEL rOSCHIN, ALL-PERVASIVENESS OF THE BLOCKCHAIN TECHNOLOGY, PROCEDIA COMPUTER SCIENCE ,VOLUME 123, 2018, PAGES 116-121

[2] ZIGA TURK, ROBERT KLINC, POTENTIALS OF BLOCKCHAIN TECHNOLOGY FOR CONSTRUCTION MANAGEMENT,PROCEDIAENGINEERING,VOLUME 196, 2017, PAGES 638-645

[3]LichengWang,XiaoyingShen,JingLi,JunShao,YixianYang Cryptographic primitives in blockchains,Journal of Network and computerApplicationsVolume127, 2019, Pages 43-58

[4] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, 2008.

[5] Philip A. Bernstein, Eric Newcomer, in Principles of Transaction Processing (Second Edition), 2009

[6] L. M. BACH ; B. MIHALJEVIC ; M. ZAGAR , COMPARATIVE ANALYSIS OF BLOCKCHAIN CONSENSUS ALGORITHMS,IEEE,2018

[7]V.Y.Kulkarni,R.A.Rane,P.Mestr,S.Panchal, Risk Rating System of X.509 Certificates, Procedia Computer Science, Volume 89, 2016, Pages 152-161

[8] Adam MihaiGergelyBogdanCrainicu, The Concept of a Distributed Repository for Validating X.509 Attribute Certificates in a Privilege Management Infrastructure Procedia Technology,Volume 22, 2016, Pages 926-930

[9]R.C. Merkle, "Protocols for public key cryptosystems," In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, pages 122-133, April 1980.

[10]S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In Journal of Cryptology, vol 3, no 2, pages 99-111, 1991.

[11]H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In 20th Symposium on Information Theory in the Benelux, May 1999.

[12] Farrell S, Housley R., An Internet Attribute Certificate Profile for Authorization, Request for Comments: 3281, Network Working Group, Standards Track, IETF, 2002.

focuses on An Introduction to Methods of Backup and Disaster Recovery for Cloud Computing .

.