International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 05 | May 2020 www.irjet.net p-ISSN: 2395-0072

SECURITY SCHEME FOR KEY MANAGEMENT BASED ON BLOCKCHAIN CONSENSUS AGREEMENT

Balamurali A[1], Harini V[2], Prahelika V[3] , Sneka I[4]

[1]*Professor, Dept. of Computer Science Engineering, SRMIST college, Tamil Nadu, India*
[2,3,4]*Student, Dept. of Computer Science Engineering, SRMIST college, Tamil Nadu, India*

Abstract - *With the consistent advancement and wide use of blockchain innovation, the issue of security breach is turning out to be increasingly conspicuous and must be completely paid attention to. This paper proposes a blockchain security scheme for key management based on blockchain consensus agreement Compared with related schemes which uses Secret Encryption Algorithm we propose a security scheme using the Secret value generation algorithm which provides multi-layer protection to the blockchain system. This algorithm incorporates a scheme for protection of privacy which reduces the problem of computational overhead that is caused during the process of verification by using the concept of consensus agreement. This use of algorithm in the blockchain reduces it's problems caused due to storage overhead as well. The communication within the blockchain and nodes improves a great amount thereby providing an environment that is efficient and the implementation in this environment is made tamper proof.*

Key Words: Blockchain, consensus agreement, security scheme, Secret value generation algorithm.

1.INTRODUCTION

Blockchain technology is an ongoing achievement in performing secure transactions in an open network without the presence of centralised control or authority supervising it. The blockchain manages the data by acting like a decentralised database which keeps account of the ongoing transactions in the open network in an organised manner. With the help of crowd computing techniques and the distributed usage of cryptographic methods the blockchain is secured with digital intelligence where the blocks in the blockchain network are mostly connected in a peer-peer fashion which is proved to be an easy way to set up and also less expensive. Concretely, the blocks involved in a blockchain maintains the unique hash value assigned to each of the other blocks participating in the network and also keeps account of the details involved in the transactions taking place.Each block encodes the hash value of other blocks with the help of cryptographic methods and by maintaining the hash value of the previous block it ensures that all the blocks in the network are cryptographically linked.In this security scheme the network uses a consensus procedure so as to provide a generalised agreement and is verified which plays a major role in controlling the addition of recently developed blocks in the open network of blockchain, Each block in the blockchain carrying detailed information about the transaction records is maintained consistently and also helps in controlling the security measures undertaken to maintain the records securely which are then verified upon consensus agreement. Subsequently, all the blocks involved maintains the detailed information about the ongoing transactions occurring in the blockchain and the recently developed blocks which are permitted to be added to the blockchain network cannot reframe or alter the information contained by each block in the hindsight of other blocks,the security and probity of each block involved in the network will not be compromised at any cost,thus assuring a tamper proofed environment for the blockchain network even after permitting the addition of newly developed blocks. Thus, with the proposed scheme the blockchain is loaded with multi layer protection and verification with the help of consensus aggregation which ensures secure transaction of data from one node to another (sender and receiver) in an open network much more efficiently compared to the existing system.

Studies that deals with privacy and security issues of blockchain are based on two important points .First it is necessary to look for drawbacks and vulnerabilities of the existing systems and the next step is to develop a new model which promises to eradicate all the discovered drawbacks in the proposed system. This paper presents a comprehensive view of a security scheme using secret generation algorithm based on blockchain consensus agreement to maintain privacy of blockchains.

2. EXISTING SYSTEM

A major limitation when using Conventional security schemes like biometric-based signature schemes index-hidden PriKey designs and post-quantum block-chain schemes is that they provide lesser efficient environment to work with. As in the case of using biometric based signature schemes it breaks the anonymity of users in blockchain as the terms in between the users and biometrics are one to one totally not suitable for not in real time. In other approaches like lattice based signature scheme it involves private and public keys in small sizes and the related research of this technique is still less for practical implementation, in the case of post quantum blockchain the use of it always or mostly leads to computational overhead problems and index hidden PriKey designs require new block chain architectures in telecommunications and digital signatures, Considering the method of identity based approach it involves mulitple authority approach which leads to mutliple authentications resulting in heavy burden on the system. decreasing compatibility and extensibility of current blockchains which leads to highly complex and lesser efficiency environments because it proves to be too inefficient to complete the user's real-time requirements which threatens the security of blockchain in an open network.

3. PROPOSED SYSTEM

The establishment of blockchain using a consensus scheme among systems having decentralized infrastructures over the internet emerged when comparing this mechanism with systems having inrasturcutres that are centralized. Consensus is a group-based convention for arriving at a dynamic conclusion in a group. Contrasted with the voting scheme based on majority, the consensus mechanism accentuates the process in which the whole group taking part will get benefited by arriving at a consensus that is agreed upon. The issues that arise when arriving at a consensus progressively in a group mainly depends on the co-ordination among the members of the group. A list of transactions are put into blocks by the validators. Each block contains a blockheader, and the information contained within the blockheader are a merkle root hash, an additional secret value that is generated and added to the merkle root hash so that the integrity of the transactions can be maintained and an additional layer of security can be provided as well, each block's identity depends on the order of generation of the block which is given by the timestamp that is generated during the generation of the block and this is included in the blockheader as well, the previously generated block produces a hash which is included in the blockheader so that the architecture of the chain can be maintained and validated, and so on. Validators need to be selected at fixed intervals and this can be done using Consensus algorithms., and this validator links the generated block to the previous one. Some examples of Consensus algorithms are Proof-ofoWork, Proof-of-Stake and Delegated Proof of Stake. These Consensus algorithms eliminate the overhead caused due to double spending transcations, protects the transactions from Distributed Denial of Service attacks and ensures that the transactions are visible and reliable so that no one can manipulate the transactions. These algorithms are also helpful in locating and tracing back the lost private keys with the help of the additional secret value that is generated and added along with the merkle root hash. This generation and addition of the secret value is much more efficient when compared with the existing systems. All participants taking part in any transaction in blockchain will have the same copy of the data sets. An example of this could be the same copy of the account book of their cryptocurrency. Thus due to this transparency in data sets, it assures that the transactions are undenaible and irreversible.

4. ARCHITECTURAL DESIGN OF SECURITY SCHEME BASED ON CONSENSUS AGREEMENT

The Architectural design for the security scheme for key management based on consensus agreement first requires system initialization which gathers information and resource required for building a blockchain and the initialised system data undergoes basic level of encryption using Secret Value Generation Algorithm. The keys are generated to maintain the confidentiality and security of the transacted information. Using hash functions and keys the system information is digitally signed using default signature algorithm. The users in the system are verified by requesting certain proofs and on providing that, the consensus agreement of 2/3 of total nodes guarantee the proofs and allows the users to actively participate and access the information within the blockchain network without compromising the security or privacy policies of the blockchain.

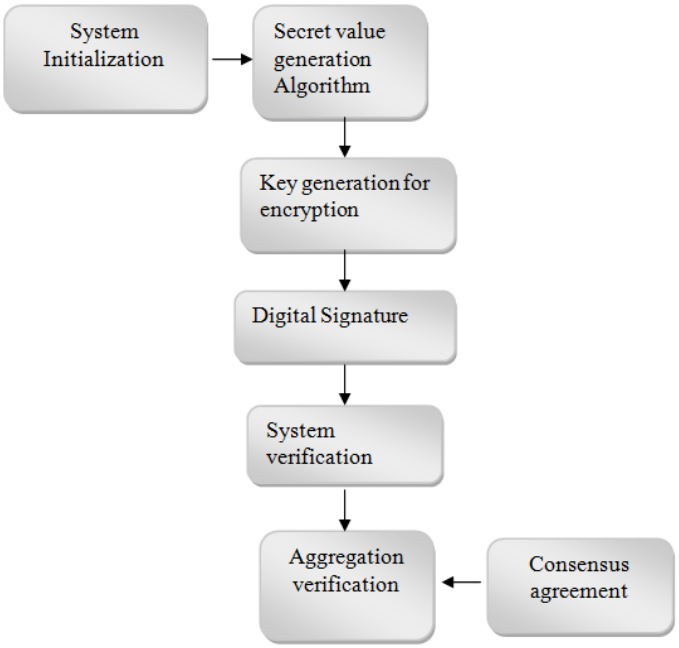

Fig -1: Experimental Framework

5. EXPERIMENTAL PROCEDURE

a) SYSTEM INITIALIZATION

System is initialized by gathering information and resources to construct a blockchain. Firstly the sender and receiver in the supply chain is identified and is sufficed by the authentication of the same. Then the information to be transacted from one node to another are put into records and is contained by the corresponding blocks involved .A database is then created to maintain and secure transaction logs which keeps account on all the transactions made.

b) GENERATION OF SECRET VALUE AND KEYS USED FOR ENCRYPTION

A secret value is generated by using the secret value generation algorithm apart from the merkle root hash which helps in providing multi layer protection to the system and takes the security parameter of the system to the next level when compared to the existing systems and the generation of secret value is used to map the data of arbitrary size to data of fixed size also helps in tracing the lost private keys during transactions.

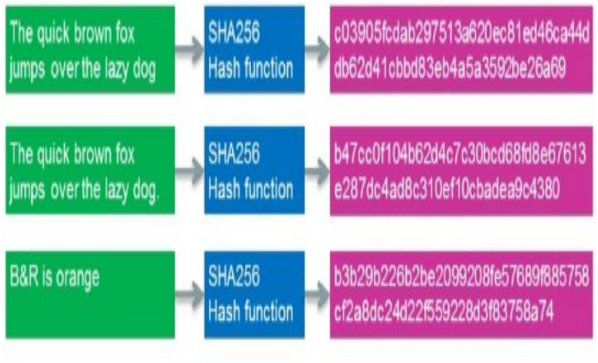

Fig -2: Secret value generation

The ciphering key involved is generated for encrypting and decrypting the data transacted in the block chain network. The generated keys should be known by both sender and intended receiver to retrieve information from the network successfully.

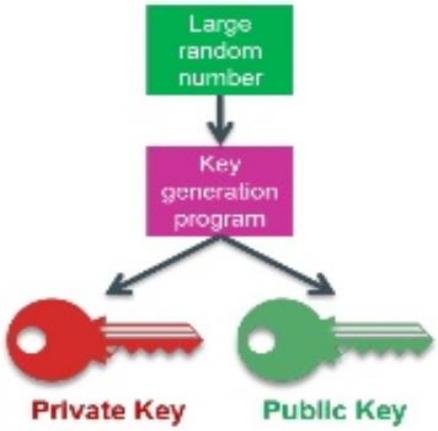

Fig -3: Key generation

The information about the keys must be exchanged between the nodes in a secure manner. There are two keys involved namely private and public where the public key information can be disclosed or be known to everyone but the private key will remain a secret for everyone except the intended recipient who can decode the private key with details the user has been given access to.Key generation in the case of generating a public key can be done by randomly selecting large prime numbers which is then fed into a key generation program that generates the public key needed, whereas in the case of private key the key generator program generates a much longer complex prime number which can't be reversed even when the user has access to the public key

c) DIGITAL SIGNATURE

Digital Signature is used to maintain the security and prove that the given information is valid by using algorithms and calculations that deal with cryptography. The information that is protected with a digital signature can be checked to make sure that it hasn't been tampered with. The procedure involved in generating a digital signature includes three main segments. The beginning segment includes the generations of keys, in this case two keys, involved namely private and public where the public key information can be disclosed or be known to everyone but the private key will remain a secret for everyone except the intended recipient who can decode the private key with details the user has been given access to. The second segment is the process of digitally signing data. It delivers a signature for the information message generated by using the private key that is generated in the first step. The verification process is the third segment in the generation of the digital signature.

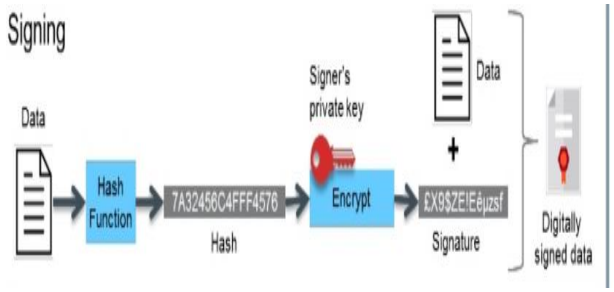

Fig -4: Digitally Signed Data

The verification process verifies the digital signature by taking the public key, the concealed message and the produced signature as inputs. The signature produced for the corresponding message is verified using the public key from the input and a boolean value is generated as a result. The process of digital signing can be considered secure and the generation of the digital signature can be well defined if it follows two properties. The first one is making sure that the various signatures can be verified by using the corresponding message to make sure they are valid. The second one is that the signatures must be unforgeable, meaning any other user excluding the valid participant who gained access to the public key must not be able to tamper with the produced digital signature and make forged signatures on the private messages.

d) SYSTEM VERIFICATION,AGGREGATION AND CONSENSUS AGREEMENT

Consensus is the process that involves groups making decisions and arriving at dynamic conclusions. Contrasted with the process of voting based on majority, the consensus agreement includes the group and the group as a whole arrive at a consensus that benefits all the members of the group. The issues that arise with arriving at consensus progressively in a group can be solved based on the co-ordination among all the members of the group. Thus co-operation among all members of the group can lead to good consensus.

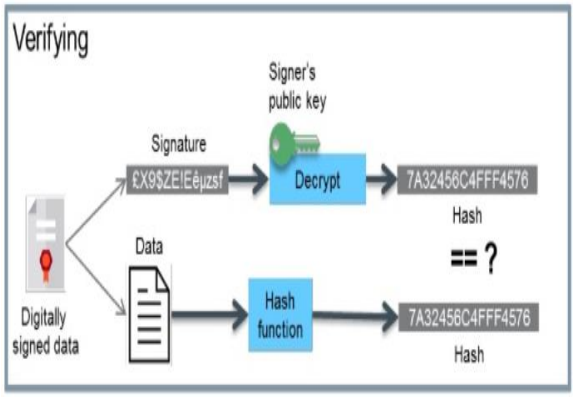

Fig -5: Verification

The job of the consensus node is to verify the client's identity and then send the results of the verification i.e if the client is a valid client or not to all the other nodes. The process of consensus is where each consensus node will cast it's vote into a ballot. The votes are then counted and if the total number of votes casted by the consensus nodes is greater than 2/3rd of the total number of nodes that are present in the network, then the verification of the client is passed i.e the client is considered as a valid client and the message provided by the client can be then undergone for encryption. This encoded or encrypted message is then inserted into the blockchain as a block and connected into the network. The verified client's information regarding his/her identity is then sent to user or customer.

6. EXPERIMENTAL RESULT ANALYSIS

The experimental results on developing a security scheme for key management based on blockchain consensus agreement are better when compared with the existing systems. The verification process is

basically divided into two steps. The production of the proof and the verification of the proof. It is usually difficult and takes up a lot of time for the person the person to generate and provide a proof that falls into and meets all the given criteria and requirements. Once this is done, the process of verifying the proof produced by the person is opposite to that of generation of the proof as this process can be done quickly by the members and it is easy for the members to do this verification step. In the verification process, the correctness of the proof is the measure used to verify the produced proof. The main property of the hash function that is used in this algorithm is that it is collision resistant. This means that the hash value that is generated by the hash function of this property is hard to tamper. Thus providing a very high layer of security for the associated message. This hash is really difficult to tamper with even if the messenger got caught. When a message has been tampered with, there would be a drastic and obvious difference between the hash generated previously before it has been tampered and the hash developed from crypting the indigenous message the senders intended to send to the recipient thus making it time consuming and computationally costly. Irrespective of that if the adversary plan on tampering he may have to undergo the process of proof of work verification which is again much more expensive and leads to longer waiting hours before he could tamper into the system successfully, and again if the adversary tries to reframe the hashes of previous block linked with each block that again will fail due to the collision resistant property of the linked structure of hash and it is time consuming to trace out every past block and changing the hash of it until he reaches the first block.During these situations the tamper resistant property come in hand to secure the blockchain in an open network. The double characteristics of Proof of work ensures that it is a compex deal to find the perfect nonce for the hash created by the secret value generation algorithm which offers multi-layer protection.

7. CONCLUSION

The proposed security scheme for key management provides and additional and improved layer of security by limiting the network's rate at which a new block is created and added to the blockchain. It limits this by a rate at one every 10 mintues. i.e it creates and adds a new block to the blockchain once every ten minutes. This rate control is implemented by the algorithm. It monitors the amount of time that is spent on solving each of the proof of work challenges that are generated and adjusts the level of difficulty of the various challenges automatically. This algorithm generates the proof of work successfully at high costs. On doing so the level of difficulty in predicting which particular miner in the provided network will be the one that is going to generate the next new block that is to be added to the blockchain is increased. It also provides an efficient tamper proof environment and offers multi layer protection to the network by adding secret value which helps in tracing the lost private keys .Thus it can be concluded that a security scheme based on consensus agreement provides an an optimally secure,highly scalable environment for the transactions occurring within the blockchain.

REFERENCES

[1] S. Jarecki, A. Kiayias, H. Krawczyk, and J. Xu, ``Highly-efficient and com- posable password-protected secret sharing (or: How to protect your bitcoin wallet online),'' in Proc. IEEE Eur. Symp. Secur. Prsivacy (EuroSP), Saarbrucken, Germany, Mar. 2016, pp. 276291.

[2] C.-Y. Li, X.-B. Chen, Y.-L. Chen, Y.-Y. Hou, and J. Li, ``A new lattice- based signature scheme in post-quantum blockchain network,'' IEEE Access, vol. 7, pp. 20262033, 2019.

[3] X. Liang, S. Shetty, D. Tosh, Y. Ji, and D. Li, ``Towards a reliable and accountable cyber supply chain in energy delivery system using blockchain,'' in Security and Privacy in Communication Networks (Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering), vol. 255. Cham, Switzerland: Springer, 2018, pp. 4362.

[4] P. Urien, ``Crypto terminal based on secure element for consumer trusted blockchain transactions,'' in Proc. 16th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC), Las Vegas, NV, USA, Jan. 2019, pp. 12.

[5] Z. Gao, X. Lei, L. Chen, X. Zhao, Y. Lu, and W. Shi, ``CoC: A unified distributed ledger based supply chain management system,'' J. Comput. Sci. Technol., vol. 33, no. 2, pp. 237248, Mar. 2018.

[6] S. Chen, R. Shi, Z. Ren, J. Yan, A. Shi, and J. Zhang, ``A blockchain- based supply chain quality management framework,'' in Proc. IEEE 14th Int. Conf. E-Bus. Eng. (ICEBE), Shanghai, China, Nov. 2017, pp. 172176.

[7] Y. Cui and H. Idota, ``Improving supply chain resilience with establishing a decentralized information sharing mechanism,'' in Proc. 5th Multidisci- plinary Int. Social Netw. Conf. (MISNC), Saint-Etienne, France, Jul. 2018, Art. no. 23.

[8] Y.Wang, J. H. Han, and P. Beynon-Davies, ``Understanding blockchain technology for future supply chains: A systematic literature review and research agenda,'' Supply Chain Manage., vol. 24, no. 1, pp. 6284, Jan. 2019.