International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 02 | Feb 2019 www.irjet.net p-ISSN: 2395-0072

A REVIEW ON IMPLEMENTATION TECHNIQUES OF BLOCKCHAIN ENABLED SMART CONTRACT FOR DOCUMENT VERIFICATION

M. HamithaNasrin[1], S. Hemalakshmi[1], Prof G. Ramsundar[3]

[1]B.E, Dept of Computer Science and Engineering, KPR Institute of Engineering and Technology
[3]Asst. Prof, Dept of Computer Science and Engineering, KPR Institute of Engineering and Technology, Coimbatore.

Abstract - *Blockchain is essentially a decentralized distributed database or a ledger. Decentralization in simple term means that the application or service continues to be available and usable even if a server or a group of servers on a network crashes or are not available. Basically a blockchain is a distributed database which monitors continously increasing data structure into blocks which contains details of individual transactions. The integrity and the chronological order of the blockchain are enforced with cryptography. Transactions that take place are computationally impractical to reverse. The existing system uses blockchain in various fields including smart contracts i.e, smart contract for document verification. We have chosen blockchain for implementing smart contracts for digital degree verification System. This project outlines the concept, characteristics and need of blockchain. The project mainly works with the implementation of blockchain in Ethereum environment with focus on smart contract for digital degree verification.*

Key Words: Blockchain, Cryptography, Ethereum, Smart contracts, Digital degree verification.

1. INTRODUCTION

Blockchain means having multiple blocks chained together and each block stores transactions in a way that it impossible to modify these transactions. Not being able to change and modify past transactions makes blockchain solution purely trustworthy, transparent and incorruptible. It is most important to understand that blocks and its chain is just one of the facets of blockchain. There are also other important concept like mining, miners, consensus and protocol that works along with chain of blocks to make blockchain work without flaws. Ethereum is extending its functionality with the help of smart contracts. With the implementation of blockchain in smart contract a function for digital degree verification can be developed and with the function the user can able to validate the degree and the data is stored in the block so that anyone can view the certificate which avoids the duplication or fraud attempt. Section 2 explains the need of blockchain section 3 explains the cryptographic techniques, section 4 explains about blockchain and Ethereum architecture, section 5 explains about the mining nodes, section 6 briefly explains about the process of mining in blockchain section 7 is for glimpse about smart contracts, section 8 covers the related work and finally section 9 is given for conclusion.

2. NEED OF BLOCKCHAIN

The primary objective of Ethereum is to accept transactions from accounts, update their state and maintain the updated state as current state untilanother transaction updates it again. The entire process of accepting, executing and writing transactions can be divided into two phases in Ethereum. There occurs a decoupling when a transaction is accepted by Ethereum and when the transaction is executed and written to the ledger. This decoupling concept is quite important for decentralization and distributed architecture to work as expected. Blockchain helps significantly in three different ways.

2.1 Trust

Blockchain helps in creating different applications that are decentralized and collectively owned by multiple number of people. Nobody in this group has the power to change or delete previous transactions. Even if someone tries to do modifications, it will not be accepted by other stakeholders.

2.2 Autonomy

There is no single owner for Blockchain based application systems. No one controls the blockchain system, but everyone participates into its activities. This helps in creating complete solutions that cannot be manipulated or induce corruption.

2.3 Integrity

The state and transactions are secured cryptographically and cannot be modified easily by intruders.

2.4 Intermediaries

Blockchain based application can help in removing the intermediaries from existing processes.

3. CRYPTOGRAPHY

3.1 Symmetric Encryption and Decryption

Symmetric cryptography refers to process of using a single and same key for both encryption and decryption. It means

that, the same key is be available to multiple people if they want to exchange messages using this form of cryptography.

3.2 Asymmetric Encryption and Decryption

Asymmetric cryptography refers to process of using two different keys for encryption and decryption. Any key can be used for encryption and decryption. Messages encrypted with public key can be only decrypted using private key and messages encrypted with private key can be decrypted using public key. Suppose, if user A is using B's public key to encrypts messages and sends it to B. Now B can use its private key to decrypt the message and extract contents out of it. Messages encrypted with B's public key can only be decrypted by B as B holds its private key and no one else. This is the general use case of Asymmetric keys. There is another use case which is discussed in Digital signature.

3.3 Hashing

Hashing is the process of transforming string data of any length into another fixed length string data and it is not possible to regenerate or identify the original data from resultant string data. Hashing ensures that even a slight change in the input data will completely change the output data and no one can ascertain the change in the original data. There is another important property of using hashing is that no matter the size of input string data the length of its output is always fixed. For example, using SHA256 hashing algorithm, a function with any length of input will always generate 256-bit output data in return. And this property especially becomes useful when large amount of data can be stored as 256-bit output data. Ethereum uses hashing quite extensively. It hashes all the transaction data, hashes multiple transaction hashes to generate single root transaction hash and in fact the blocks in Ethereum are also represented as hash. Another important property of hashing is that it is mathematically infeasible to identify two different input strings that will output the same hash value. Similarly, it is impossible to computationally and mathematically find the input from the hash itself.

3.4 Digital Signature

One of the most important use case of using Asymmetric keys is in creation and verification of Digital signature. Digital signature is very similar to signature done by an individual on a piece of paper. Similar to the paper signature, digital signature helps in identifying an individual. It also helps in ensuring that messages are not tampered during transit. For example, If A wants to send a message to B. How can B identify and ensure that the message has come from A only and that the message has not been changed or tampered with in transit? Now 'A' takes the message it wants to send to Band generates a hash of it and then using its private key encrypts the hash and appends the resultant cipher data to the original message. Once the resultant message reaches to B, it segregates the messages into the original message and cipher data. It decrypts the cipher data using A's public key and extracts the hash out of it. It further hashes the original message and compares both the hashes obtained. If the hashes are same, it means that the message is not tampered within transit. It also establishes the fact that the message is originated by A only since A can encrypt the hash with its private key. Digital signature is mainly used to sign transaction data by the owner of asset or crypto-currency like ether.

4. BLOCKCHAIN AND ETHEREUM ARCHITECTURE

Blockchain is an architecture which comprises of multiple components that are interconnected and what makes blockchain unique is the way these components functions and interact with each other. Following are some of the important Ethereum components, it includes Ethereum virtual machine, Miner, Blocks, Transactions, Consensus algorithm, Accounts, Smart contracts, mining nodes, Ether and GAS. A Blockchain network consists of multiple number of nodes belonging to miners and some nodes that do not mine but helps in execution of smart contracts and transactions. These nodes are known as Ethereum virtual machines. Each node is connected to another node in the network. These nodes use peer-to-peer protocol to talk to each other within the network. They use 30303 port number to interact among themselves. Each miner maintains an instance of ledger. Ledger contains all blocks in the chain. With multiple miners it is quite possible for miners to have their ledger instance might have different blocks than other. The miners synchronize their blocks on an on-going basis to ensure that every miner's ledger instance is same as other.

The EVM also hosts smart contracts. Smart contracts helps in extending Ethereum by writing custom business functionality into it. These smart contracts can be executed as a part of transaction and it follows the process of mining that is discussed in Section V

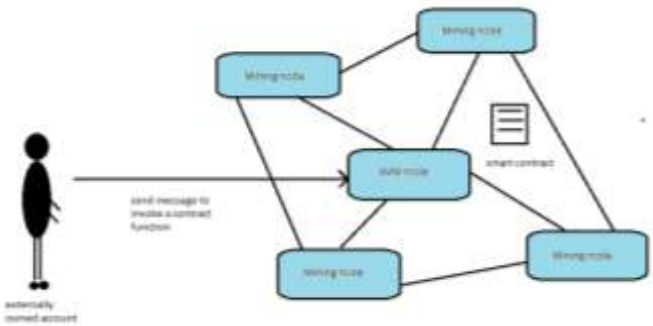

Fig -1: Account invokes smart contract function

A person who is having an account on network can send a message for transfer of Ether from his account to another or he can send a message to invoke a function within a contract. Ethereum do not differentiate them as far as transactions are considered. The transaction must be digitally signed with the account holder's private key. This is to ensure that identity of the sender can be established while validating the transaction and changing balances of multiple accounts.

4.1 Relationship between block and transaction

Ethereum stores transactions within Blocks and each block has a upper Gas limit and each transaction needs certain amount of Gas to be consumed as a part of its execution. The cumulative gas from all the transactions that are not yet written in ledger cannot surpass the Block Gas limit. This ensures that all transactions need not get stored within a single Block. As soon as the Gas limit is reached, other transaction is removed from the block and mining begins thereafter.

The transactions are hashed and it is stored in the block. The hashes of two transactions are taken and hashes further to generate another hash value. This process eventually provides a single hash from all transactions stored within the block in a blockchain. This hash is known as Merkle root hash and stored in Block's header. A change in any one of a transaction will result in change in its hash and eventually change in root transaction hash.

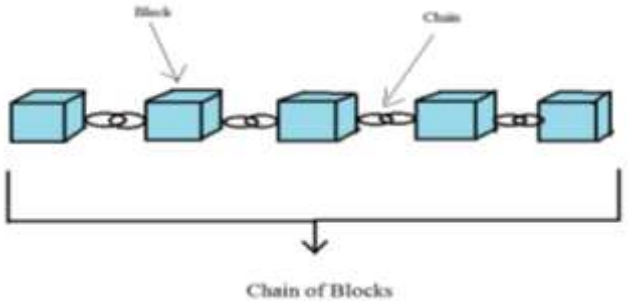

Fig -2: Chain of blocks

It will have cumulative effect because if the hash of the block is changed then the child block has to change its hash because it stores its parent hash. This helps in making whole transactions immutable. This is also shown in FIGURE 3.

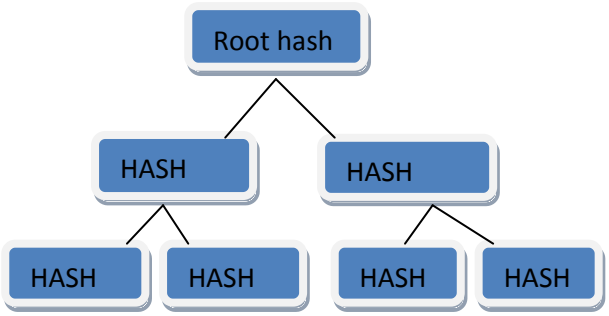

Fig -3: Block Hash

5. MINING NOGES

5.1 Nodes

There are two types of nodes in Ethereum.

- Ethereum virtual machines
- Mining Nodes

It is to be noted that this distinction is made to clarify concepts of Ethereum. In most of the scenarios' there is no dedicated EVM machines instead all nodes acts as miner as well as EVM node in the network.

5.2 Ethereum virtual machines (EVM)

Consider EVM as the execution runtime for Ethereum network. EVM's are primarily responsible for providing a runtime that can execute code written in smart contracts as well. It can access contracts of account holder and externally owned accounts. It does not have access to ledger but has limited information about current ongoing transaction.

EVM are the execution component in Ethereum. The purpose of EVM is to execute the code in smart contract line by line. However, when a transaction is submitted, the transaction is not executed immediately at the time of submission instead is it pooled in a transaction pool. These transactions will not be executed and not yet written to the Ethereum ledger. EVM nodes are similar to mining nodes but they do not do mining.

5.3 Mining Nodes

A miner is solely responsible for writing transactions to the Ethereum chain. A miner job is similar to that of an accountant. An accountant is responsible for writing and maintaining the ledger similarly, a Miner is solely responsible for writing transaction in the Ethereum ledger. A miner is interested in writing transactions to ledger because of the reward associated with the process. Miners get two types of reward, reward for writing a block to the Ethereum chain and cumulative gas fees from all transactions in the block. There are generally many number of miners available within a blockchain network each trying and competing to write transactions. However only one miner node can write the block to the ledger and rest will not be able to write the current block and determination of a miner who will write the block happens using a challenge. The challange is given to every miner and every miner tries to solve the puzzle using its compute power. The miner who solves the puzzle first within the time write block containing transactions to ledger and also receives five ether as reward. Every Mining node maintains its own instance of Ethereum ledger and the ledger is same ultimately across all the other miners. It is the job of miners to ensure that their ledger is updated with latest blocks. There are primarily three important functions performed by Miners or Mining Nodes.

- Mine or create a new block with the transaction and write the same to Ethereum Ledger
- Advertise and send a newly mined block to other miners in the network.
- To accept new blocks mined by other miners and keep its own ledger instance updated.

Mining Nodes refers to the nodes that belong to Miners. These nodes are part of the similar network where EVM is hosted. At some point of time, the miners would create a new Block, collect all transaction from transaction pool and add all

the transaction to the newly created block. Finally, this Block is added to the blockchain. There are additional concepts like consensus, solving of target puzzle before writing the block and those will be explained in section VI.

6. MINING BLOCKS IN A BLOCKCHAIN

Miners always looks forward to mine new block and are also listening actively to receive new blocks from other miners. As mentioned before, at some point of time, the miner collects all transactions from the transaction pool. This activity is done by all node in the network. The miner constructs a new block and adds all transactions to the block. Before adding these transactions, it will check if any of the transaction is already written in a block that it might receive from other miners. If so, it will eliminate those transactions. The miner will add his own coin base transaction for getting plunder of mining the block. The next task for the miner is to generate the Block header and performs following task. The miner hashes all the transactions in the block, these hashes are further combined in pairs to generate a new hash value. The process continues until there is just one root hash for all transactions in the block. The hash is referred as Merkel Root transaction hash. This hash is thenadded to the block header. The miner also identifies the hash value of the previous block. The previous block will become parent to the current block and its hash will also be added to the current block header. The miner in similar way calculates the State and Receipts transaction root hashes and add them to the block header as well. A nonce and timestamp value is also added to the block header. The mining process starts where the miner keeps changing the nonce value and try to find a hash value that will satisfy as an answer to the given target puzzle. It is to be kept in mind that everything that is mentioned here is executed by every miner in the network. Eventually, one of the miner would be able to solve the target puzzle and advertise the same to other miners in the network. The other miners can verify the answer and if found correct would further verify every transaction while accept the block and append the same to their own ledger instance.

This entire process is also known as Proof of Work (PoW) wherein a miner provides proof that is worked on computing the final answer for the target puzzle that could satisfy as solution to the puzzle. There are other algorithms like Proof of Stake (PoS) and Proof of Importance (PoI) and such algorithms are summarized in the following.,

6.1 Proof of Work

POW is the mining technique used in bitcoin and is currently used by many other blockchain technologies in various fields. It requires the mining nodes to solve a hard mathematical puzzle that is changed frequently and has been agreed by all miners. Once the node validates the transactions and solves the targetpuzzle, the block is submitted to the blockchain network. Other mining nodes will also validate the block to make sure that the submitter is not falsifying. Once it is agreed among all the miners that the block is legit, it will be added to the blockchain and the submitter will be rewarded as per the norms. The agreement here is based on the majority consensus protocol. Thus it is difficult to fake unless the attackers compromise more than 50% of the mining nodes.

6.2 Proof of Stake

Unlike PoW, PoS does not require the mining nodes to solve ahard mathematical puzzle which is computationally expensive. The chance of a node being chosen to create a new block depends on the node's wealth or stake.

6.3 Proof of Importance

PoI is a mining technique that calculates the significance of an individual node based on the transaction amount and the balance of the mining node. It assigns a priority with the hash value calculation to the more significant nodes. Further a node with the highest priority is chosen for the next block creation

7. SMART CONTRACT

A smart contract is a contract implemented, deployed and executed within Ethereum environment. Smart contracts are digitization of the traditional legal contracts. Smart contracts are deployed, stored and executed within the Ethereum Virtual machine. The data stored in smart contract can be used to record information, fact, associations, balances and any other information needed for the implementation logic for real world contracts. Smart contracts are closely related to object oriented classes. A smart contract can call another smart contract just like an Object-oriented class to create and use objects of another class. Think of smart contract as a small program that consist of functions. You can create aninstance of the contract and invoke functions to view contract and update the data along with execution of some logic.

8. RELATED WORK

With the current growing interest in the blockchain technology and smart contract implementation, many new platforms and applications have been proposed.Several survey papers have been written to highlight the benefits of this technology for current applications. Examples of such survey includes the bockchain technology for IOT, Bitcoin mining and health care etc.

Proposed system

This paper investigates the use of blockchain technology in a different set of applications which is not discussed in prior surveys. We aim to provide a comprehensive survey on the use of blockchain technology in digital degree

verification.

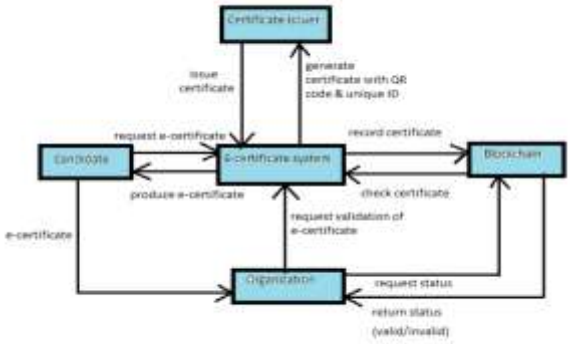

Fig -2: Proposed system architecture

9. CONCLUSION

We have analysed that our work for implementing blockchain in smart contract for digital degree verification system works better when compared to traditional verification system Data security is one of the major features of blockchain technology. Blockchain is a large and open-access online ledger in which each node saves and verifies the same data. Using the proposed blockchain based system reduces the likelihood of certificate forgery. The process of certificate application and automated certificate granting are open and transparent in the system. Companies or organizations can thus inquire for information on any certificate from the system. In conclusion, the system assures information accuracy and security.

REFERENCES

[1] S. King and S. Nadal, "Ppcoin: Peer-to-peer crypto-currency with proof- of-stake," self-published paper, August, vol. 19, 2012.

[2] V. Buterin et al., "A next-generation smart contract and decentralized application platform," white paper, 2014.

[3] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in 2016 IEEE symposium on security and privacy (SP). IEEE, 2016, pp. 839–858.

[4] C. Udokwu, A. Kormiltsyn, K. Thangalimodzi, and A. Norta, "An exploration of blockchain enabled smart-contracts application in the en- terprise," Technical Report, DOI: 10.13140/RG.2.2.36464.97287, Tech. Rep.

[5] M. Knechtand B. Stiller, "Smartdemap: A smart contract deployment and management platform," in IFIP International Conference on Au- tonomous Infrastructure, Management and Security. Springer, 2017, pp. 159–164.

[6] C. Dannen, Introducing Ethereum and Solidity. Springer, 2017.

[7] Xiuping Lin, "Semi-centralized Blockchain Smart Contracts: Centralized Verification and Smart Computing under Chains in the EthereumBlockchain", Department of Information Engineering, National Taiwan University, Taiwan, R.O.C., 2017.

[8] T. Bocekand B. Stiller, "Smart contracts–blockchains in the wings," in Digital Marketplaces Unleashed. Springer, 2018, pp. 169–184.

[9]Solidity, https://solidity.readthedocs.io/en/latest/index.html

[10] G.-T. Nguyen and K. Kim, "A survey about consensus algorithms used in blockchain."Journal of Information Processing Systems, vol. 14, no. 1, 2018.

[11] Gong Chen, Development and Application of Smart Contrats.