RESEARCH ARTICLE OPEN ACCESS

Research of a Possibility of Using Blockchain Technology without Tokens to Protect Banking Transactions

C.Mani MCA., M.E.*, S.Arul**
*Associate Professor, Department of CSE, Nandha Engineering College (Autonomous), Erode, Tamilnadu, India.
Email: cmanimca@gmail.com
** Final MCA, Department of MCA, Nandha Engineering College (Autonomous), Erode, Tamilnadu, India.
Email: aruljones20@gmail.com

****

ABSTRACT

This paper discusses the utilization of Blockchain technology without tokens to shield information about banking transactions, namely, transfer amounts, card details, names of participants, etc. this subject has relevancy, since the digital economy is becoming an integral a part of modern life. The processed information passes through the database of banks and payment systems, which potentially makes it available to the attacker. The article analyzes the protection mechanisms of distributed databases, proposes an answer to the matter of maintaining the individuality of data in them supported Blockchain technology without tokens and provides recommendations on the introduction of Blockchain technology into modern banking systems.

Keywords — **distributed database, mining, token, Blockchain, transaction.**

****

I. INTRODUCTION

Commercial banks, because the most significant establishment of the fashionable world, must adhere to certain rules of data security and be ready to withstand destructive factors. Banking information has always raised the interest of intruders to that, so each bank must organize the protection of the info it stores, control the boundaries of the inner information space to safeguard against information leakage. This task within the nowadays is complicated by the territorial distribution of banking infrastructure: the presence of branches, automated teller and other services with which the top office conducts information interaction. Geographically-distributed database structures should even be shielded from internal failures resulting in data loss and disruption of the complete system. the aim of the work is that the analysis and development of recommendations for the protection of data in geographically-distributed structures, typical of recent banks, supported the Blockchain technology.

II. PROBLEM FORMULATION

Confidential information about bank customers, the state of their accounts, transaction history: - all of this is often stored, processed and transmitted by the banking information systems inside their infrastructure. one amongst the most tasks of the bank is to make sure information security of information, confidentiality, to ensure their safety and integrity, within the process of exchange and processing of knowledge. There are four kinds of failures in distributed databases [1], transaction failure, node failure, media failure, communication line failure. the matter of system failures is additionally expressed within the incontrovertible fact that the failed node can't participate in transactions. supported the foregoing, the matter of maintaining the distinctiveness of data in distributed databases of banking infrastructures is

an urgent task that must be addressed. Thus, it's necessary to search out how to make sure the individuality and integrity of knowledge circulating during a distributed banking infrastructure, using the capabilities of innovative information technologies, particularly, the Blockchain technology

III. CENTRALIZED AND DISTRIBUTED DATABASES

Currently, all information about cards and transactions is stored on banking servers in their centralized databases. they supply stability, simple implementation, flexibility, scalability, performance.

because of the very fact that within the present time more and more applications are working under heavy loads, special requirements for network servers are required. One server cannot do, such machines will need dozens, while the requirement to transfer large amounts of knowledge. From this it follows that distributed databases (DDB) are increasingly finding their use. Distributed database - a collection of copied, shared and synchronized digital data, geographically distributed in numerous places by country and / or institution.

A distributed database may be a decentralized database that's controlled by an outsized number of participants and remains available. Computers of a distributed database are called “nodes”; they're full-fledged and passive participants. so as to update the database, it's necessary to validate the total nodes, the reconciliation is achieved employing a special consensus mechanism.

To arrange competitive access, each node will have its own distributed schedule for the interaction of elements

(Fig. 1). Ti - subtransactions;

1 - generating transactions;

2 - data transfer

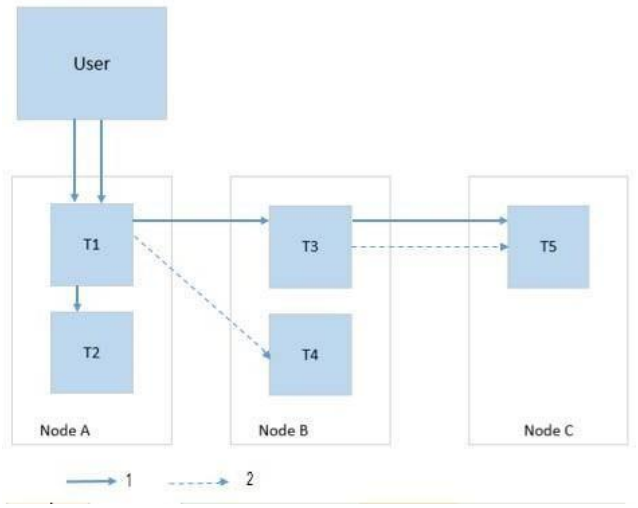

Fig. 1 Distributed Transaction Model

DDB includes a number of important advantages:

- reliability;
- availability;
- processing efficiency;
- data replication;
- economic benefits;
- system modularity;
- productivity increase.

Along with the benefits of DDB have their disadvantages:

- data compatibility;
- storing the system catalog;
- ensuring data integrity;
- disaster recovery problem
- competitive access;
- the distributed impasses (when two or more transactions at the identical time are in wait state, and for work each of transactions expects the termination of execution of other transaction).One possible solution to those problems could also be Blockchain technology.

IV. ANALYSIS OF THE MECHANISM OF THE BLOCKCHAIN

A Blockchain may be a chain of blocks, each block stores information on addresses, transactions, account balances, and therefore the structure itself is totally decentralized. From here you'll be able to trace the whole transaction history. The Blockchain is additionally characterized by complete openness of

knowledge and therefore the impossibility of fixing the stored information. Competitive access issues are resolved within the Blockchain by consensus protocol. After creating a brand new block, all transactions that claim to be included in it are checked by this protocol for legality, and therefore the transactions that violate the balance conditions are discarded. The hash value of the header is termed the hash value of the block, therefore, the transactions that are within the block don't directly participate within the hashing. The header includes such parameters because the block version, the hash value of the previous block, the hash value of all transactions within the new block, the date and time of the block creation and therefore the varied accessory nonce parameter. The hash value of transactions calculated by the algorithm named the Merkle tree, and this hash value is employed for block hashing. additionally it's wont to check the integrity of the info and acquire a singular identifier. Regarding, the Blockchain Merkle tree is built as follows:

1) Calculation of the hash values of all transactions within the block – hash;

2) Calculation of the hash values of the sum of the transaction hash values;

3) Calculation of hash valuesтfrom the sum of the resulting hash values; Further process goes on a recursion. The hash value tree is binary, which implies there must be an excellent number of elements at each step. That is, if there are only three transactions, the last one are going to be duplicated.

4) the method continues on recursion until the instant when the sole hash value is obtained. Such a hash value is termed merkle_root, the identical field that's per the specification and employed in the block header. This structure, merkle_root protects all transactions within the block and provides the so-called “non-formability”, as if a minimum of one transaction changes, the merkle_root changes and, therefore, the title and therefore the entire block change. This ensures that the transaction within the block can't be changed by the attacker, because of which the data remains confidential and reliable.

In fig. 2 shows the algorithm of the Blockchain with mining. For hashing, SHA-256 is employed [2], let's briefly take a look at its algorithm.

SHA-256 uses 64 constants (32-bit words) and 6 nonlinear functions:

Ch (x, y, z) = (x AND y) XOR (NOT x AND z)
Maj (x, y, z) = (x AND y) XOR (x AND z) XOR (y AND z)

Sigma0 (x) = ROTR(x, 2) XOR ROTR(x, 13) XOR ROTR(x, 22) 1766

Sigma1 (x) = ROTR(x, 6) XOR ROTR(x, 11) XOR ROTR(x, 25)

Delta0 (x) = ROTR(x, 7) XOR ROTR(x, 18) XOR SHR(x, 3)

Delta1 (x) = ROTR(x, 17) XOR ROTR(x, 19) XOR SHR (x, 10)

where

ROTR - right shift by n bits

ROTR(x, n) = (x >> n) | (x << (32-n))

SHR - right shift by n bits (x, n) = x >> n

After which there are four stages of hashing. At the primary stage, the message is transformed from 16 words with a size of 32 bits to 64 words with a size of 32 bits. within the second stage, the variables are initialized for the hash function. At the third stage, the most loop of the compression function is performed, after which it calculates the intermediate hash value and therefore the result.

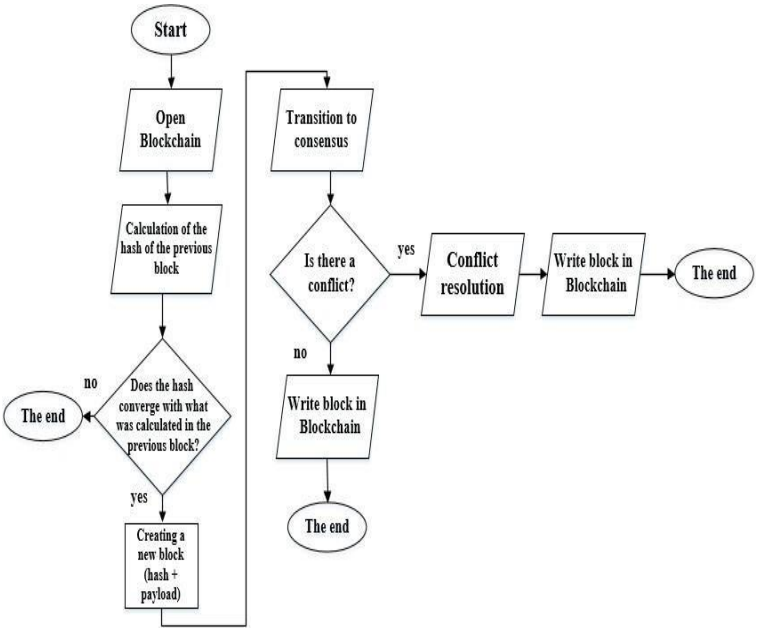

Fig. 2. Scheme of the block addition algorithm in the Blockchain with mining

Figure 3 shows an example of the operation of the consensus mechanism. The Blockchain technology database is found in many nodes (six during this example). Each node stores its own copy of the chain of transactions, which is updated whenever new data about transactions is received. within the first two transactions, the info and signatures were properly validated by all six nodes, i.e. matching hash values were obtained. In transaction № 3 at point № 5, the hash value didn't coincide with the others and can be corrected by other parties using the consensus mechanism.[3]

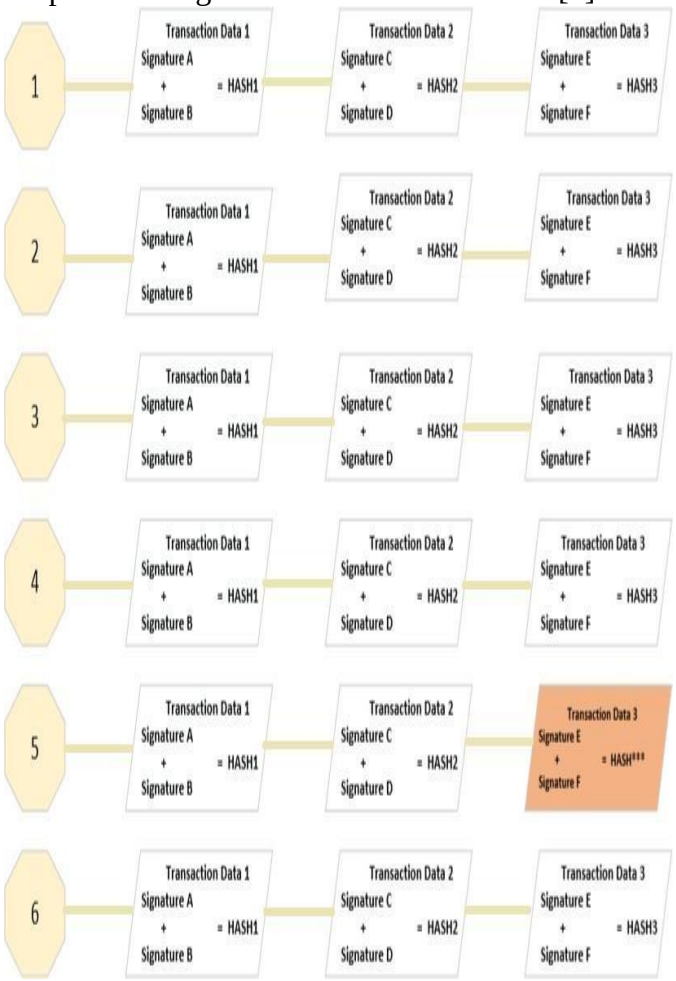

Fig.. 3. An example of using the mechanism of consensus

The mechanism of consensus ensures that the info stored on each node are exact copies. The protocol of consensus represents a rule set which are coordinated by nodes in network. These rules guarantee that the network will work to destination and to stay synchronized. The consensus protocol defines: - how blocks should be added to the Blockchain; - when blocks are considered valid; - how conflicts are resolved. [4] the appliance of the mechanism of consensus may be considered on the instance of Bitcoin cryptocurrency. the most mechanism in it's the Proof of the work done (PoW) Bitcoin. a brand new block within the Bitcoin network is mined in a mean of 10 minutes. To do this, the pc must solve a posh math problem. This process is named mining. After the matter is solved, the block is added to the chain, and also the miner is rewarded by the network with a specific number of tokens. on balance the nodes have checked the block and added it to their copy of the Blockchain, the blocks are considered valid. Each node has software that checks the legitimacy of the block. Validation rules are established by consensus mechanism. If two miners attempt to simultaneously add a true block, a conflict arises - the chain is split into two. All consensus protocols Bitcoin, solve this problem simply: that chain wins, which is longer. I.e. where it's more miners, the chain will quicker grow. The analysis of the blockchain mechanism shows that its main characteristics, as a transaction management tool, don't depend upon the utilization of tokens. within the process of making a blockchain, tokens are accustomed motivate the work of miners to form the blockchain network workable. This work are often evaded tokens, if we are talking a few corporate blockchain, as an example, banking.

V. THE BANK SYSTEM WITH THE BLOCKCHAIN WITHOUT TOKEN

Consider a system which will work on the premise of the Blockchain, but without mining (i.e., without tokens) using the instance of a bank with its branches and users. However, only the bank can create new blocks, therefore, mining and tokens are missing. If, for instance, Peter wants to transfer money to Alyona, then this transfer must bear the bank or its branch so as for it to be confirmed, record the transaction within the block and make a brand new one. The algorithm for creating a block within the system into account is presented in fig. 4. this method has one owner - the bank, and he, in

turn, can represent a limiteless number of nodes in numerous places. At the identical time, the structure into consideration requires complete trust and also the degree of decentralization is minimized, but the territorial distribution of the system remains and also the use of Blockchain remains relevant. An example of the employment of such a system may additionally be a digital property rights platform. This structure of import accounting requires complete trust within the organization, in our case, the bank. The owner of the system can create several nodes with auditor rights which will verify that each one changes are applied correctly, and if something goes wrong, the auditors will notice. one among the benefits of such a structure is that it doesn't require large computing power, but with each change in 1768 the state of the system, data is synchronized, copying occurs in real time, as a results of which the system becomes proof against denial of service.

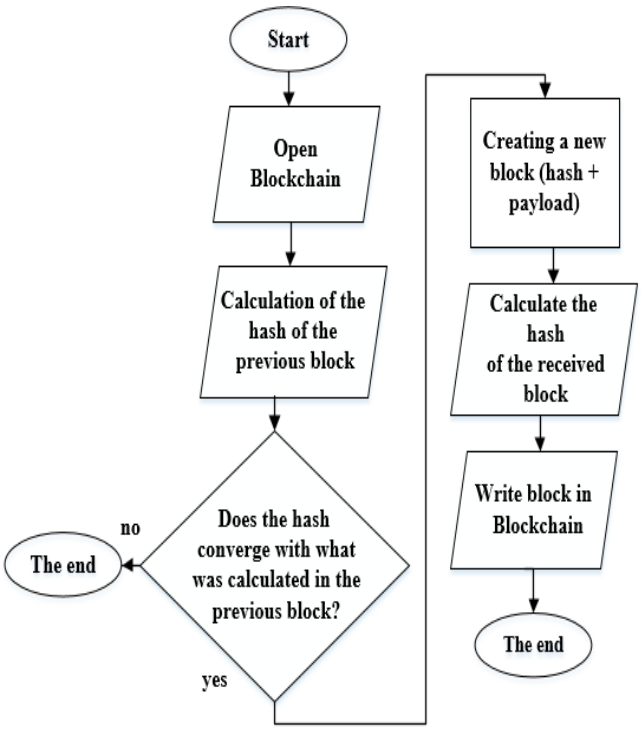

Fig.. 4. Diagram of the block creation algorithm in Blockchain without mining

A varied accessory parameter (nonce) is employed, within the blockchain with mining, when hashing a replacement block within the process of its creation. Changing the numerical parameter, miners attempt to pick a hash value, but the given number, which determines the speed of finding the required nonce. Since its search is finished by brute force, success depends directly on the computing power. This process determines the viability of the common use blockchain and makes the blockchain completely decentralized. a company blockchain, a banking one in our case, can exist without mining, connecting the whole infrastructure with a peer-to-peer network. The network is controlled by the bank, while the blockchain technology retains its mechanism and every one its advantages. • Transparency: all legitimate users have the power to create entries, while it's impossible to vary previously registered data. • Reducing transaction costs: the blockchain allows you to independently conduct transactions to affiliates and other services of the structure. • Decentralization: there's no central point of data gathering. Information about specific blocks scattered across all servers of the company structure. thanks to structural hashing on the Merkl Tree, all transactions within the block are shielded from changes, information remains confidential and reliable. additionally, using merkleroot, you'll be able to create simplified verification nodes only by block headers, while two interacting nodes can make sure that transactions are correct only by their headers. The Blockchain technology also makes it possible to scale back the amount of intermediaries between participants in a very transaction through the introduction of smart contracts. a wise contract is an electronic protocol that's written using code. Its purpose is to transfer information and to enforce the terms of a contract by both parties. [5] The Blockchain manages transactions and upon the occurrence of conditions specified by a contract, the program code of the contract recorded in blocks of the chain is automatically executed. Moreover, the obligations that the parties must fulfill are automatically fulfilled.

VI. CONCLUSION

The development of data technology and electronic business each day has an increasingly significant impact on all spheres of the trendy life. Blockchain technology is meant to vary the standard perception of how people interact through a network. the most advantage of the Blockchain technology is that the complete synchronization of processes, integrity and uniqueness of all processed information, no matter mining and tokens. Blockchain technology helps to boost distributed databases in terms of storage, synchronization, loss and integrity of information. Thus, the Blockchain may be a tool which at implementation within the banking industry without mining and tokens will considerably simplify processes of maintenance of integrity and uniqueness of data on bank transactions, and its implementation within the processes of smart contracts will allow to scale back number of participants at commission of some transactions.

VII. REFERENCES

[1] Komkov D.K. «Features, applications and directions for the development of distributed databases». [Electronic resource]. URL https://cyberleninka.ru/article/v/osobennosti-sfery-primeneniya-inapravleniya-razvitiya-raspredelennyh-baz-dannyh

[2] Butakova N.G., Fedorov N.V. Kriptograficheskiye metody i sredstva zashchity informatsii: uchebnoye posobiye. – SPb.: ITS «Intermediya», 2016 - 384 p

[3] Maas T. «The Quick, 3-Step Guide to Blockchain Technology» [Electronic resource]. URL: https://hackernoon.com/3-steps-tounderstanding-blockchain-8a285572daa3

[4] Dobkina L. «5 advantages of the blockchain and one trap for the investor» [Electronic resource]. URL https://ru.ihodl.com/investment/2017-12-13/5-preimushestvblokchejna-i-odna-lovushka-dlya-investora/

[5] Osmolovskaya A. S. «Smart Contracts: Functions and Applications» own [Electronic resource]. URL https://cyberleninka.ru/article/n/smartkontrakty-funktsii-i-primenenie