International Journal of Latest Trends in Engineering and Technology
Special Issue April-2018, pp. 048-051
e-ISSN:2278-621X

BLOCK-CHAIN TECHNOLOGY ADOPTED IN RECONCILIATION SYSTEM AND PAYMENT GATEWAYS

Ms. Vaishnavi. M[1], M, Ms. Archana C.S.[2], Ms. D.N. Vijith Niranjana [3], Mrs.S.Aarthi[4]

Abstract —The extent of the unraveling fraud at India's s could rise beyond the nearly $2 billion mark (Rs. 12,998) so far outlined by the lender, according to sources .If there was a rule that only transactions recorded in block-chain will be honored for Credit to the beneficiary instead of just SWIFT messaging, the transaction would have been audited at source and these scams would have been prevented.

This Paper is aimed the adoption of block-chain by India's banks that could help avert frauds and enforce the disaggregated and transparent nature of the technology, which updates information across all users simultaneously, alert to the creation of the letters of undertaking (LoUs), and other such documentations. 'Immediate notification' is sent to the parties involved in the transaction.

Keywords: Block –chain, LoUs,Bitcoins

1. INTRODUCTION

Block-chain is a type of distributed financial statement for maintaining a permanent and dabble-proof record of transactional data. A block-chain functions as a decentralized database that is managed by computers which belong to a peer-to-peer network.

A block-chain register(basically also called as ledger) contains of two types of records: Individual transactions and Blocks.

The first block consists of a header and data that affects the transactions taking place within a set time period.the first block is called as the genesis block. The block's timestamp is used creates an alphanumeric string which is claimed also as hash. After the first block was created, each subsequent block in the ledger uses the previous block's hash to calculate its own hash. Before a new block can be added to the chain, its authenticity must be checked by a computational process called validation .Also every block stores the hash value of the previous block. At this point of the block-chain process, a majority of nodes in the network must accept the new block's hash was calculated correctly. Validation ensures that all copies of the distributed ledger share the same state. Once a block has been added, it can be referenced in subsequent blocks, but it cannot be changed. If someone attempts to swap out a block, the hashes for previous and subsequent blocks will also change and disrupt the ledger's shared state.

In our paper , we would walk the audience through the following:1.Present Financial Transaction Infrastructure.2. Explanation of what a block chain is.3.Key Areas of Application of block chain in Banking.4. Points on how Block Chain Disrupts the present industry practices.

2. PRESENT SYSTEM

Over the following 30 years most banks moved to core banking applications to support their operations creating a Centralized Online Real-time Exchange . This meant that all the bank's branches could access applications from centralized data centers. Deposits made were reflected immediately on the bank's servers, and the customer could withdraw the deposited money from any of the bank's branches.

Lou: Stands for "Letter of Undertaking". The bank in India stands guarantee for the borrower who borrows money from a foreign bank by giving a LoU. Usually LoU is given only on collateral security from the borrower. A security in the form of immovable assets or shares or business premises to the value of 110% of the amount in the LoU is usually taken.

In the present system:

1. SWIFT messages are independent of the Core Banking System.
2. The CBS does not validate any SWIFT messages. That is it is not mandatory for recording of SWIFT messages in CBS.
3. SWIFT messaging is honored by all banks all over the world.

[1] UG Student, Department of Computer Science & Engineering, Meenakshi Sundararajan Engineering College, Chennai, Tamil Nadu, India

[2] UG Student, Department of Computer Science & Engineering, Meenakshi Sundararajan Engineering College, Chennai, Tamil Nadu, India

[3] UG Student, Department of Computer Science & Engineering, Meenakshi Sundararajan Engineering College, Chennai, Tamil Nadu, India

[4] Assistant Professor, Department of Computer Science & Engineering, Meenakshi Sundararajan Engineering College, Chennai, Tamil Nadu, India

4. The Lou Transaction was not recorded in the CBS of the bank

5.Access control – Grant/revoke-Access control limits actions on objects to specific users. In database security, objects pertain to data objects such as tables and columns as well as SQL objects such as views and stored procedures.

Once a role has been created, the format for implementing RBAC follows the pattern:

GRANT privilege_name
ON object_name
TO role_name;

Privilege_name identifies the rights to be granted. These include such rights as selecting data,
modifying data, or manipulating the database structure. [1]

6.Encryption of data-in-motion / data-at-rest-Start with a Secure Configuration , Stay Patched , Stay on top of all the security alerts and bulletins , Implement the Principal of Least Privilege , Review User Rights to ensure all access is appropriate , Defense in Depth / Multiple Levels of Security. [4]

7.Data Encryption -A data encryption is a random string of bits created explicitly for scrambling and unscrambling data. Data encryption is designed with algorithms intended to ensure that every key is unpredictable and unique. Cryptography uses two types of keys: symmetric and asymmetric. Symmetric keys have been around the longest; they utilize a single key for both the encryption and decryption of the ciphertext. This type of key is called a secret key [2].

.8.SQL Injections-Database systems are used for the backend functionality. User supplied data as input is often used
to dynamically build sql statements that affect directly to the databases. Input injection is an
attack that is aimed at subverting the original intent of the application by submitting attacker –
suppliedsql statements directly to the backend database. [3]

Issues in core banking system

Risk and complexity - A typical universal bank runs more than 180 badly-documented applications, restricting flexibility but also creating thousands of points of failure

Scalability - Banking systems can't keep up with the exponential growth in volumes brought about by the digitization of banking, and soon the Internet of Things

High expenditure and opportunity cost -The cost of maintaining ageing legacy banking systems eats up more than 75% of banks' IT budgets, leaving little for value-enhancing expenditure

An expectations gap - Customers want financial institutions to perform the role of infomediaries , helping them to make better financial and commercial decisions. To achieve this, banks need real-time, integrated systems.

Sophisticated attacks that exploit un-patched vulnerabilities , Double or triple encrypted SQL-injection attacks that render web-application firewalls virtually useless ,Insider attacks , Insider mistakes , Advanced identity theft via database rootkits , Increasingly sophisticated social engineering leading to full-blown database disclosures.

2. PROPOSED SYSTEM

2.1. Motivation

We know a lot about fraud and money laundering, and also about amassive scam worth Rs. 11,400 crore by a Bank to benefit a billionaire jeweler and others.

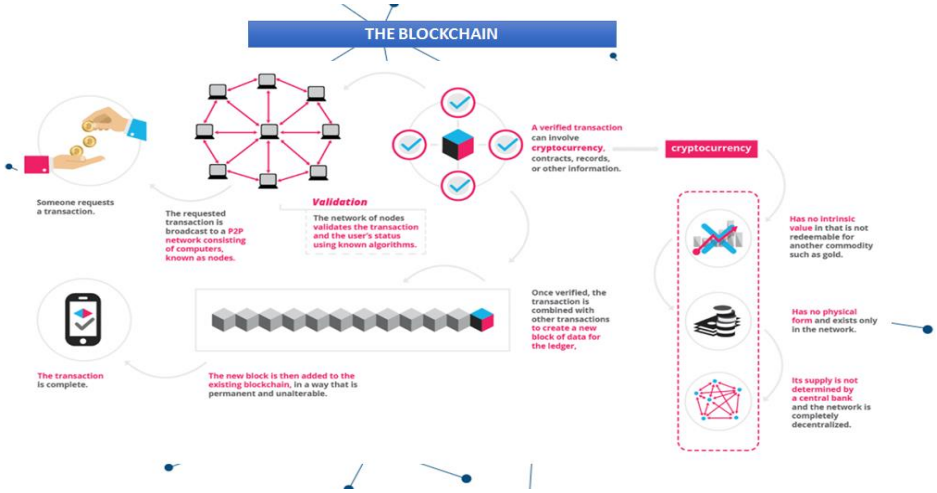
If there was a rule that only transactions recorded in block-chain will be honored for Credit to the beneficiary instead of just SWIFT messaging, the transaction would have been audited at source and the scam would have been prevented. Block chain has not yet been implemented in India and if this could be implemented as part of government project to ensure security of recorded transactions in these nationalized banks and all private organizations, this could serve the society for future use.

The acceptance of block-chain by India's banks could help avoid frauds such as the one at the bank as the disaggregated and clear nature of the technology, which updates information across all users instantaneously, would have ensured that various officials would have instantly been alerted to the creation of the letters of undertaking (LoUs). Bloch chain provides Immediate notification ,Transaction reconciliation systems at present do not result in immediate notification .Using block-chain, all parties on the chain will be immediately notified about a transaction. Block-chain, a distributed ledger technology originally developed as an accounting system for the crypto currency (Bitcoin) technology.

2.2. Execution at SBI

SBI committed block-chain's utility, can improve internal fraud monitoring, and can be implemented in reconciliation systems and in several cross-country payment gateways, If the LoUs were on the block-chain, then they would have been there for everybody to see, and every entry into the chain leaves a clear record of who made that entry, and where .Which means that anything documented on them cannot be changed or deleted, and is instantly uploaded to all users on that block-chain. "If a person of a bank wants to lend to a borrower, he /she needs to know what all he has borrowed from other institutions as well. For that, we have the CIBIL score at present, but that data is prone to human error. The modus operandi of the fraud as it appears right now is that somebody used all the authentication methods and it was compromised at the user level. If that is the case, then any technology can be hoodwinked. Here, what was given into the system is not in doubt, the one who gave it into the system is in doubt. Still, block-chain's technology is such that even human error can be greatly mitigated by Block-chain can fix this by having everything linked.

2.3. Architecture



2.4 Working:

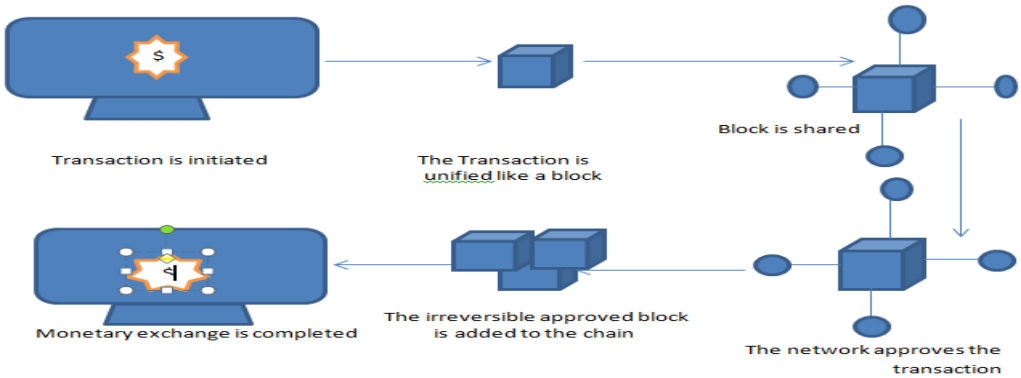
There are three principal technologies that combine to create a block-chain.

1) private key

2) A distributed network and

3) An incentive to service the network's transactions, record-keeping and security.

When two people want to transact over the internet. Each of them holds a private key and a public key. The main purpose of this component is block-chain technology which is easy to create using a secure digital identity reference. Identity is based on possession of a combination of private and public cryptographic keys. The combination of these keys can be seen as a dexterous form of consent, creating an extremely useful digital signature. This digital signature provides strong control of ownership. The approving of transactions and permissions (authorisation),for block-chains, this begins with a distributed network. When cryptographic keys are combined with this network, a super useful form of digital interactions emerges. The process begins with person A taking their private key, making an announcement of some sort -- in the case of bitcoin, that you are sending a sum of the cryptocurrency -- and attach it to B's public key. A block - containing a digital signature, timestamp and relevant information - is then broadcast to all nodes in the network. [8]



Block- Chain Technology should cover the following transactions to be recorded and stored in Block:

1. All Bank Guarantees, Letter of Credits, Bill of Ladings and Letter of Undertakings.
2. All Collateral security valuation and their charging to the Loan account of the customer.
3. MOD (Memorandum of Deposit of Title Deeds) which is usually done in Registration offices.
4. All Credit Analysis, Risk Exposure Assessment of the Customer, Credibility scores (like CIBIL scores) periodically done on the Borrower customer.
5. All repayment schedules and periodic repayment of loan by the customer.
6. All Investment banking operations like Road Shows, Initial Public Offerings, Initial sale of shares of the companies and subsequent secondary market transactions on a company's shares.

As all the credit history of customers are stored in the Blocks of the block-chain, all stakeholders like foreign banks offering loans, credit card companies, Insurance companies, Investment bankers can read all information regarding the customer to assess their risk of financially supporting the customer.
If the foreign bank which lent money to the offender had known that the borrower has not shown enough collateral security and the transaction has not been vetted in the Core Banking system, they would not have lent money to the borrower. Complete information about the borrower has not been shared to the concerned stake holders. Block Chain Technology can facilitate information gathering and assimilation to all stake holders.

3. CONCLUSION

Block-chain has emerged as one of the most disruptive technologies and has minimized the prevailing security issues in financial transactions. By implementing block-chain for the financial and banking industry, we get transformation in various fields by fraud reduction ,that is 45% of financial intermediaries ,suffer from economic crime .Knowing the customers can be done in an exemplary way. Smart contracts which is a code could be programmed to create contracts .Block-chain could enable higher security and lower cost for banks to process payment. The risk of operational errors and fraud can be dramatically reduced .

4. REFERENCES

[1] Database Security: What Students Need to Know Meg Coffin Murray Kennesaw State University, Kennesaw, GA, USA
[2] A research Paper on Cryptography Encryption and Compression Techniques SaritaKumari Research Scholar
[3] DATABASE SECURITY - ATTACKS AND CONTROL METHODS Mubina Malik and Trisha Patel
[4] Database Security and Auditing: Leading Practices Rob Barnes Director, Enterprise Auditing Solutions Application Security, Inc
[5] https://blockgeeks.com
[6] ieee-future-directions-blockchain-white-paper.pdf
[7] Ieeexplore.ieee.org/document/7966963
[8] https://www.coindesk.com/information/how-does-blockchain-technology-work
[9] www.icicibank.com/blogs/banking-innovation/blockchain-infographic.page
[10] BlockChain: A Distributed Solution to Automotive Security and Privacy Article