Volume 4 || Special Issue 1 || ICCEME 2019-2020 || ISSN (Online) 2456-0774
INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH
AND ENGINEERING TRENDS

BLOCKCHAIN IN BANKING SYSTEM

Prof. Dipti A. Gaikwad[1] ,Mrunal S. Tupe[2], Ameya S. Kulkarni [3],
Vedant M. Kulkarni[4], Suraj B. Kolekar [5]
Department of Information Technology Jayawantrao Sawant College Of Engineering Pune, India[1,2,3,4,5]
diptisawant12@gmail.com[1],mrunal.tupe@gmail.com[2] ,ameyakulkarni56@gmail.com[3],
vedant.m.kulkarni371999@gmail.com[4] ,surajkolekar16@gmail.com[5]

Abstract- **In 2018, on September 23, the North Korean programmers had created and embedded malware to take instalment data from Indian ATMs and banks. The malware, known as ATMDtrack, started showing up on systems and is believed to be owing to Lazarus Group, a hacking bunch that has focused on banks, ATMs, and digital currency trades. Ransomware assaults have been there since 2005, it is a kind of pernicious programming that accesses documents or frameworks and squares client access to those documents or frameworks. Then, all documents, or even whole gadgets, are held prisoner utilizing encryption until the casualty pays a payment in return for an unscrambling key. The key permits the client to get to the records or frameworks scrambled by the program. Ransomware costs organizations more than 75 billion dollar for each year and the normal expense of a ransomware assault on organizations was 133,000 dollar. Damages from ransomware are required to ascend to 11.5 billion dollar this year, and another association has succumbed to ransomware at regular intervals in 2019, and at regular intervals by 2021. These attacks lead to the stealing of the customer's details and data, i.e. their data is insecure. For the security purpose of the banks and customers' accounts, our system entitled "Blockchain in Banking System" focuses on the security of the data of the customer using block chain technology. Utilization of encryption algorithm SHA-256 in banking system to store its transaction details on blockchain database instead of dealing with common database. Basically it uses a peer-to-peer network of computers to validate transactions, to make it more secure and decentralized, to avoid different cyber-attacks that happen on bank. We have implemented blockchain in banking system to make it more secure, corruption free and fast by using blockchain's encryption (hashing) and decentralized feature.**

Keywords –*Blockchain, Encryption, Ransomeware*

I INTRODUCTION

The blockchain is a powerful technology that allows Bit- coin, and instead hands control back to the individual user. Here we will examine how this system works, what it means for our future and why it is so useful.

To date, blockchain technology is applicable in all Altcoin, Dogecoin, and other virtual currencies to be open, anony-mous, and secure. The blockchain essentially is a database about every Bitcoin transaction in detail. Usually known as a "public ledger," the log contains metadata about when and how each transaction took place. The ledger is publicly accessible through APIs and torrent sites. To prevent tinkering with current and also past transactions, the database is cryptographically secured ,Because of Cryptography can edit only the parts of the blockchain that they "own" - by possessing the private keys required to write into the file. It also keeps everyone's copy of the distributed blockchain is kept in sync. One of the most exciting aspects of blockchain technology is that it is entirely decentralized, instead of storing at single location. This removes the need for powerful central authorities areas and the banking system is not an exception. New technologies, such as blockchain technology should be introduced in the modern banking system, since they provide control over crypto currency that will help in counteracting money-laundering and financing of terrorism in the country and around the world. Since today's banking framework is based on centralized databases, it is simple for an attacker to enter in any such databases which will effortlessly understand all the data and information of the clients of the bank. This unprotectedness of the present financial framework can be decreased by re- constructing the financial systems over blockchain innovation, which will remove the unified database design and decentralize the information over the blockchain and in this way, the hacking of the database can be decreased. Since the exchanges over the blockchain innovation is verified by every single hub of the chain, it will make the exchanges increasingly more secure along these lines making the general banking framework quicker and secure. Smart contracts are used to exchange money or ownership, store data, make decisions, and interact with other contracts. We are using smart contract for sending confirmation message to bank client that their transition is successfully done. Block chain facilitates smart contracts as they facilitate storage of any kind of digital information, including computer code that can be executed once two or more parties enter their keys. Contracts could be created and financial transactions executed when this code is programmed, according to the set criteria.

A. Need

The major question that arises is to why use blockchain when already the market has thriving excess of other databases. What substantial importance it holds against the competing products. For this let's understand the problem with the current systems. They could be summed up as follows: (i) Difficult to monitor and assess asset ownership and its transfer in a trusted business network. (ii)Some factors like inefficient, expensive, vulnerable etc. extremely obstruct the performance and thereby destroying the progress.

B. Solution offered by Blockchain

Blockchain not at all like conventional frameworks is sufficiently dynamic to turn into a pioneer in execution in a fluctuating business sector situation. In a block chain the preeminent favourable position it guarantees is that each gathering has a record which is kept up in a record accessible to everyone. It is a record broadly went between various clients in this way making a mutual database which is imitated to these clients and who can get to it simply after they have the entrance directly for it. Accord, provenance, unchanging nature, certainty are the different perspectives into which it works, ensuring that every one of these features cooperate into a sensible amalgamation.

Utilization of encryption technique in banking system to store its transaction details on block chain database instead of dealing with common database, basically it uses a peer- to-peer network of computers to validate transactions, to make it more secure and decentralized, to avoid different cyber-attacks happens on bank. A Blockchain is a digital, immutable, distributed ledger that record the transactions. It maintains continuously-growing list of records generally known as" blocks" which are secured from tampering and revision. Each block contains a timestamp and a link to a previous block is provided by the secure hash algorithm like SHA256.

II WORKING FLOW OF SYSTEM IS AS FOLLOWS

1. Transaction request

A person may perform transactions through different ways like visiting the bank, ATM or an online transaction. The transaction can be of any type like depositing or withdrawing money to or from the bank. The person requests for a transaction to the bank.

Block

A new block is created which consists of the data, hash and the hash value of the previous block. The formation of the new block represents that the transaction is created. Here the hash algorithm SHA-256 is applied for the security of the data within the newly created block.

Nodes

The new block with the transaction data is sent to each and every node where the details about the person's account are stored, i.e. it is distributed over the network.

Validation

Now after the data in the new block reaches every node over the network, each node validates the transaction performed by the individual.

Chain

After the validation of the transaction by the nodes over the network, now the new block is added to the chain of blocks. This new block contains the hash value of the previous block.

Transaction complete

As soon as the new block is added to the chain of blocks the conformation message goes to the person or individual that the transaction is completed.

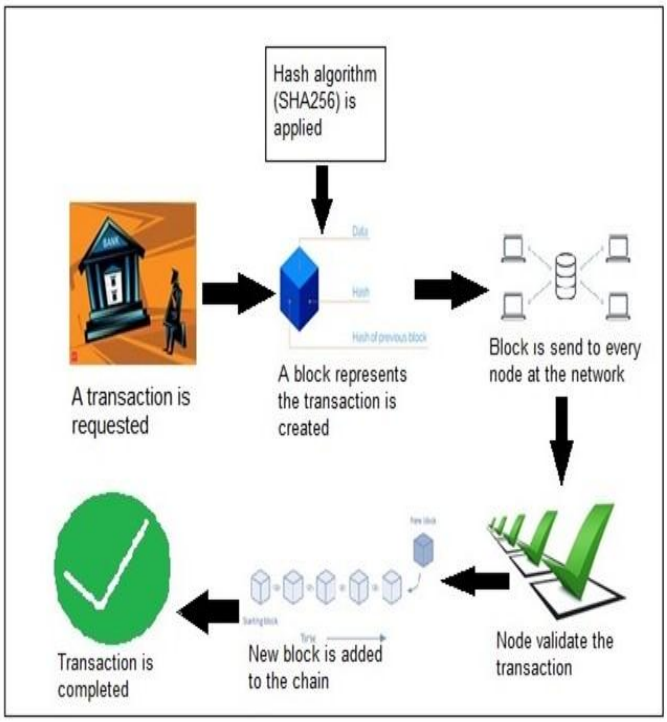

Figure 1. System Architecture

III ALGORITHM

Secure hash algorithmic an encryption algorithm which is used to create hash of strings. It is a cryptographic hash also called as digest, it is a kind of signature for a text or data file. SHA-256 generates an unique 256-bit (32 byte) signature for a text. A hash is not encryption it cannot be decrypted back to the original text, i.e. it is a one-way cryptographic function. The larger the number of possible hashes, the smaller the chance that two values will create the same hash. The hash functions of SHA do not need a key, they just calculate a hash-value from any input. SHA-256 is one of the successor hash functions and is one of the strongest hash functions available. SHA-256 is used in several different parts of the bitcoin network: -

•Mining uses SHA-256 as the proof of work algorithm

•SHA-256 is used in the creation of bitcoin addresses to improve security and privacy.

A.Steps for hashing with SHA-256

1. Padding

If we note Mthe message to be hashed, and L its length in bits where L ¡264, then as a first step we create the padded message M, which is message plus a right padding, such that M is of length L, a multiple of 512.

2.Blocks

M' is parsed into blocks of size 512 bits, M1 to MN, and each block is expressed as 16 input blocks of size 32 bits, M0 to M15.

3.Hash Initialization

The initialization hash value H0 of length 256 bits, i.e. 8 input blocks of 32 bits, is set by taking the first 32 bits of the fractional parts of the square roots of the first eight prime numbers: - • H0(0) = 6a09e667 • H1(0) = bb67ae85 • H2(0)= 3c6ef372 • H3(0) = a54ff53a • H4(0) = 510e527f • H5(0) = 9b05688c • H6(0) = 1f83d9ab • H7(0) = 5be0cd19

Input:- Hello Bank

Hash:- bb603091bf1b9abc1c2da8aeab6a23e0e15b0b979 fe0df14b9a94cadded0fbb1

IV FUTURE SCOPE

This system can be used in the real banking sector, for cashless transactions and for fast international transactions.

V CONCLUSION

We have implemented blockchain in banking system to make it more secure, corruption free and fast by using blockchain's encryption (hashing) and decentralized feature.

REFERENCES

[1]S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash Sys- tem,"www.Bitcoin.Org, p. 9, 2008.

[2]J.Simom, "The End of Big Banks," Project sandicate, the world' opinion page. Febuary 2016.

[3]S. Underwood, "Blockchain beyond bitcoin," Commun. ACM, vol. 59, no. 11, pp. 15–17, 2016.

[4]Kim S.Nash, "Major Banks Complete 'Modest' Blockchain Test," The Wall Street Journal. January 2016.

[5]B. Libert, M. Beck, and J. Wind, "How blockchain technology will disrupt financial services firms," Knowledge@Wharton, pp. 2–7, 2016.

[6]] WSJ Staff, "The Blockchain Is Hot, But for How Long?," The Wall Street Journal. Febuary 2016.

[7]Telis Demos, "Blockchain Start-up Gets Big-Bank Backing," The Wall- Street Journal. January 2016.