International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 04 | Apr 2019 www.irjet.net p-ISSN: 2395-0072

# Block Chain Based Banking Application

**Miss. Patil Snehal A.[1], Mr.Mohire Abhishek S.[2], Miss. Vibhute Aishwarya Ulhas[3], Miss. Shaikh Rabana Sharif[4], Miss. Mali Jyoti Ashok[5]**

*[1,2,3,4,5]BE Student of Department of Computer Science and Engineering, AGTI'S Dr. Daulatrao Aher College of Engg, Karad, Maharashtra, India*

---

***Abstract—*** *Blockchain technology is a core, underlying technology with promising application prospects in the banking industry. To date, blockchain technology is relevant in all areas and the banking system is not an exception. blockchains could revolutionize the underlying technology of the payment clearing and credit information systems in banks, thus upgrading and transforming them. block chain 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*

***Keywords***— *lockchain, Benefits from Blockchain, Decentralized consensus, Features of Blockchain, Security Aspects of Blockchain, Smart contracts, Trusted Computing,*
*Banking.*

## I. INTRODUCTION

The blockchain is the public ledger of all Bitcoin transactions that have ever been executed. It is constantly growing as miners add new blocks to it (every 10 minutes) to record the most recent transactions. The blocks are added to the blockchain in a linear, chronological order. Each full node (i.e., every computer connected to the Bitcoin network using a client that performs the task of validating and relaying transactions) has a copy of the blockchain, which is downloaded automatically when the miner joins the Bitcoin network. The blockchain has complete information about addresses and balances from the genesis block (the very first transactions ever executed) to the most recently completed block. The blockchain as a public ledger means that it is easy to query any block explorer (such as https://blockchain.info/) for transactions associated with a particular Bitcoin address—for example, you can look up your own wallet address to see the transaction in which you received your first Bitcoin.

### 1.1 Need of Reserch

•*Blockchain is Reshaping the Banking Sector*

The banking industry is strictly regulated in all jurisdictions, while banking sector representatives are distinguished by their conservative attitudes. But the wide dissemination of blockchain in the recent years, the overwhelming popularity of cryptocurrencies, and the ICO boom have contributed to the fact that the management of many banks and financial organizations no longer deny the potential of blockchain technology.

• Cost Savings

At its most basic, blockchain can be a useful and efficient way for financial institutions to manage the books and involve the customer in the process. For example, banks can use blockchain technology to give customers granular details of where their money is invested and when interest payments come through. Instead of encoding and issuing ATM cards, banks can create and use securely encrypted apps based on blockchain. By adopting this technology, financial institutions can save money and grant customers more safety, power and control over the money they entrust in those institutions.

• *Accountability*

It's rarely discussed, but computerization and software have done wonders to reduce both external fraud and internal misuse of company assets. It's much harder for an employee to fudge the books when those books are digitally generated, and you can check who last logged into the computer to change them, after all. But blockchain promises to further reduce increasingly rare incidents of fraud for financial institutions who adopt the technology. Blockchain technology makes all transactions easy to check and makes it impossible to change every backup of the books. Therefore, fraud attempts can be stopped before money leaves the bank and customer accounts will be protected.

• *Blockchain is virtually impossible to hack*

While hackers can break into traditional networks and find all the data in a single repository and exfiltrate it or corrupt it, the blockchain makes this unfeasibly hard. The data is decentralized, encrypted, and cross-checked by the whole network. Once a record is on the ledger it's almost impossible to alter or remove without it being noticed and invalidating the signature.

## II. LITERATURE SURVEY

Androulaki, E., Karame, G.O., Roeschlin, M., Scherer, T. and Capkun, S., 2013. Evaluating user privacy in bitcoin. In Financial Cryptography and Data Security (pp. 34-51). Springer Berlin Heidelberg The world has globalized and so are the operations and the business carrying out in the market of this world. As suggested by TReid and Harrigan (2013), world is now a global village. The importance of economy and currency cannot be neglected. Where there raised a situation where the business is taking place without any consideration of boundaries and walls, there should be easy availability of currency as well. Several approaches have been made towards making the payment method easier and faster. The concept of e-money and e-commerce has long been used in the market (Mkiers et al. 3013). Contemporary situation has witnessed the importance of mobile wallet and transfer of money using applications in mobile phones. All these things are welcoming an approach towards a kind of money that could be used in the business. One such concept is the introduction of Bitcoin. Barber, S., Boyen, X., Shi, E. and Uzun, E., 2012. Bitter to better—how to make bitcoin a better currency. In Financial cryptography and data security (pp. 399-414). Springer Berlin Heidelberg The Bitcoin operates in the manner as the ATM that includes a string of numbers or letters attached in a particular fashion. A pin is often offered to the user of the Bitcoin account for carrying out any kind of monetary transaction with any person throughout the world (Androulaki et al. 2013). However, in the year 2014, IRS declared that all digital currencies are to be charged with certain amount of transaction charges. Any gain or loss suffered in the Bitcoin will b considered as the gain or loss of the country as a whole. Thus, the transaction is to be included in the GDP of the country. This created an alarm among the users of the digital money system. The miners were the main users of this currency.

## III. METHODOLGY

### A) Blockchain Technology: How does it work?

We explain the concept of the blockchain by explaining how Bitcoin works since it is intrinsically linked to the Bitcoin. However, the blockchain technology is applicable to any digital asset transaction exchanged online. The blockchain is a decentralized distributed ledger. Speaking in a human language — it is a network of computers having an identical copy of the database and changing its state (records) by a common agreement based on pure Mathematics.

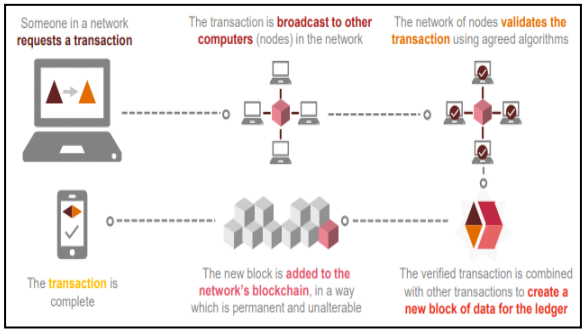


*Fig.3.1 Modules*

### B) Implementation Details

i) *UI Module*

This module provides Front end UI of our system without blockchain support/storage. It shows banking transactions without blockchain i.e. using simple database storage.It allows to client signup with system and makes transactions, request fund from trusted party by exchanging currency with DC coins. Trusted party has rights to transfer fund on request.System generates account identifier using SHA256 algorithm and uses GUID to differentiate transactions from each other. In addition of that, it provides interfaces for login, dashboard, send fund, receive fund and request fund etc. To make system more secure it uses OTP during login process.

*ii) Block Generator and Web Miner Module*

In previous module, we have created required UI for customers for sending and receiving DC coins without support of Block Chain Platform.In this module we are going to create blockchain on a single node/server and a simple proof of work (mining) System.Blockchain is a chain/list of blocks. Each block has their own hash/digital signature. Once blockchain is formed then we will check its integrity by looping through blocks in blockchain i.e. checking current block previous hash is same as previous block hash and current hash with newly calculated hash. This is called as "Proof of Work". Any tampering with old block – requires to create whole block chain again.

*iii) Transactions and wallet Module*

In module 2, we have stored only plain transaction message as data. In this module we are going to replace data with Transaction details and customer's wallet with public and private keys generated using Elliptic-curve ryptography

For our DC coin, public key will acts as sender address hence it is OK to send share public key with others to receive payment. Our private key is used to sign our transactions so that nobody can spend/use our coins

other than owner of private key. During transaction, public key will be sent and can be used to verify that our signature is valid and data is not tampered. Because signature consists of Sender+To+NoofCoins The private key is used to sign the data we don't want to be tampered with. The public key is used to verify the signature i.e. its integrity.

*iv) Peer to Peer Networks to Node*

In Module 2, we have created only one node/server. In this we are going to create 2/3 nodes which will form P2P networks.Each node will maintain their copy of Blockchain and web miner will verify integrity throughout network. Here we are going to use Proof-of-Authority (PoA) is a consensus algorithm which can be used for permissioned ledgers. It uses a set of 'authorities', which are designated nodes that are allowed to create new blocks and secure the ledger. Ledgers using PoA require sign-off by a majority of authorities in order for a block to be created.And Block Storage is nothing but ledger and database to store details of blockchain

## IV. SOFTWARE DESIGN

### A) Data flow diagram:

A data flow diagram (DFD) is a graphical representation of the "flow" of data through an information system, modelling its process aspects. A DFD is often used as a preliminary step to create an overview of the system without going into great detail, which can later be elaborated. A context diagram is a top level (also known as "Level 0") data flow diagram. It only contains one process node ("Process 0") that generalizes the function of the entire system in relationship to external entities. DFD Layers.... Draw the context diagram first, followed by various layers of data flow diagrams. DFD Levels.

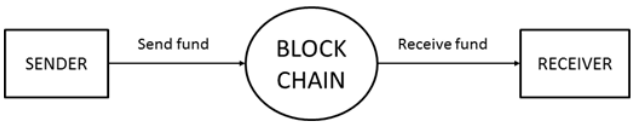


*Fig. DFD Design*

1st Level DFD:

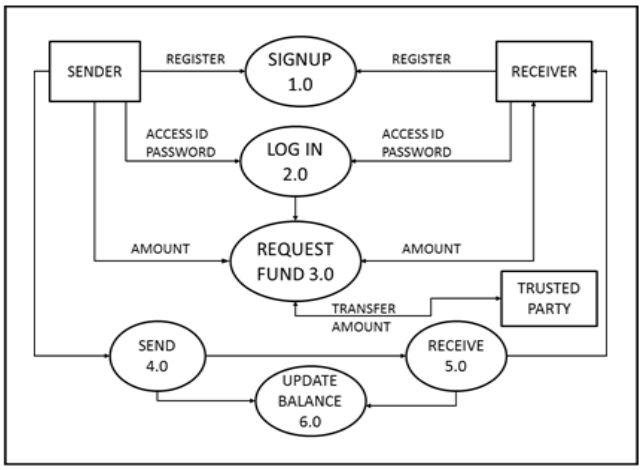


*Fig.1st Level DFD*

2nd Level DFD:

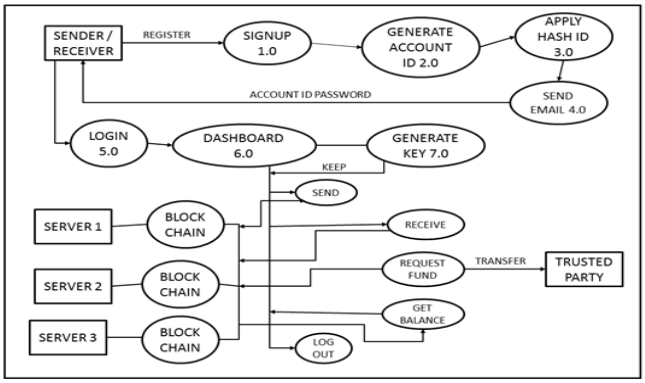


*Fig.2nd Level DFD*

### B) Flow Chart:

A **flowchart** is a type of diagram that represents an algorithm, workflow or process. The **flowchart** shows the steps as boxes of various kinds, and their order by connecting the boxes with arrows. This diagrammatic representation illustrates a solution model to a given problem. Flowchart diagram for sender side:

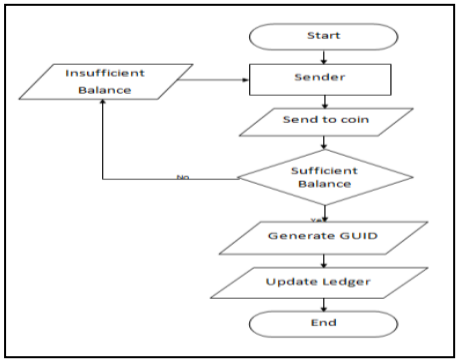


*Fig.Flow Chart*

## V. THE SCOPE OF BLOCKCHAIN TECHNOLOGY IN THE BANKING SECTOR

As banks need to make numerous transactions every day, Blockchain technology could be of enormous significance by bringing in security and genuineness in transactions. Endorsing an idea of trust economy, Blockchain can give financial institutions an opportunity to win the faith and confidence of their customers. Blockchain is a technological advancement that will transform the financial services provided by banks. The global financial system serves billions of individuals and businesses, bringing in trillions of dollars in circulation every day

### A) Benefits of Blockchain:

- Speeding up transactions
- Blockchain's verification system has the potential to enable near to or real-time processing and settlement of transactions.
- Cutting costs and complexity
- Blockchain can be used to orchestrate and automate interactions with external parties, as well as within your own processes.
- Reducing data duplication
- Blockchain provides a single shared view of the truth in your network, reducing data entry duplication and reconciliation.
- Increasing resilience
- Due to the distributed nature of blockchain, there is no single point of failure. This makes it significantly more resilient than current systems.

### B) Existing System:

Traditional systems tend to be cumbersome, error-prone and maddeningly slow. Intermediaries are often needed to mediate the process and resolve conflicts. Naturally, this costs stress, time, and money. In contrast, users find the blockchain cheaper, more transparent, and more effective.

### C) Proposed System:

Trusted Third Party[ Has sufficient amount of fund] DCoins

Customer will first register with bank. Bank will provide UserName and Password[Hash Code] and will send via mail to customer account- Customer will request fund to TTP and TTP will assign no of coins to customer

Steps
======
1. Register customer
Email : jaishwarya9996@gmail.com
Password: admin123
Confirm Password: admin123
Register ====> Send Mail [ Account Identifier]
2. Login ===> Enter Account identifier and password
3. Request Fund
---
Amt:
<Next> ===> Request submitted to Third Party

## VI. FUTURE SCOPE

Currently we are going to implement blockchain system for banking online transfer transactions. But it is equally applicable for following domains with few changes
•- Password or any personal identification
•- Healthcare
•- Government Services
•- IOT
•- Financial Service

## VII.CONCLUSIONS

- It is useful to understand blockchains in the context of bitcoin, but you should not assume that all blockchain ecosystems need bitcoin mechanisms such as proof of work, longest chain rule, etc. Bitcoin is the first attempt at
- maintaining a decentralised, public ledger with no formal control or governance. There are significant challenges involved.
- On the other hand, private distributed ledgers and blockchains can be deployed to solve other sets of problems. As ever, there are tradeoffs and pros and cons to each solution, and you need to consider these individually for each individual use case.

## VIII. ACKNOWLEDMENT

We would like to give the special thanks to the computer science engineering department of the college DACOE HOD Prof. Ashish N. Patil and Project guide Prof. Sayali P. Shinde to have their guidance. We are also thankful to the technologies that we have used to have such format of paper.

## REFERENCES

1. Anonymous Post-Quantum Cryptocash [pdf, cached pdf, bib] Huang Zhang, Fangguo Zhang, Haibo Tian, Man Ho AuIn Proc. of: Proceedings of the 22nd International Conference on Financial Cryptography and Data Security (FC). Springer, 2018,
2. A Taxonomy of Blockchain-Based Systems for Architecture Design [pdf, cached pdf, bib]Xiwei Xu, Ingo Weber, Mark Staples, Liming Zhu, Jan Bosch, Len Bass, Cesare Pautasso, Paul RimbaIn

Proc. of: Software Architecture (ICSA), 2017 IEEE International Conference on, 2017,

3. Proof of Luck: An Efficient Blockchain Consensus Protocol [pdf, cached pdf, bib]Mitar Milutinovic, Warren He, Howard Wu, Maxinder KanwalIn Proc. of: SysTEX '16 Proceedings of the 1st Workshop on System Software for Trusted Execution, 2016, ACM
4. A first look at the usability of bitcoin key management [pdf, cached pdf, bib]Shayan Eskandari, David Barrera, Elizabeth Stobert, Jeremy ClarkIn Proc. of: Workshop on Usable Security (USEC), 2015,
5. On Decentralizing Prediction Markets and Order Books [pdf, cached pdf, bib]Jeremy Clark, Joseph Bonneau, Edward W Felten, Joshua A Kroll, Andrew Miller, Arvind NarayananIn Proc. of: WEIS, 2014,
6. Zerocoin: Anonymous distributed e-cash from bitcoin [pdf, cached pdf, bib]Ian Miers, Christina Garman, Matthew Green, Aviel D RubinIn Proc. of: Security and Privacy (SP), 2013 IEEE Symposium on, 2013,
7. Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace [pdf, cached pdf, bib] Nicolas ChristinIn Proc. of: Proceedings of the 22nd World Wide Web Conference (WWW'13), 2013.