IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727, Volume 20, Issue 3, Ver. IV (May. - June. 2018), PP 40-48
www.iosrjournals.org

Blockchain-Bitcoin Transaction Management System for Current Banking System

Hemalatha T, S. Rohini, D Vivekananda Reddy
Department of CSE S V U College of Engineering, Tirupati.
Department of ECE, Annamacharya Institute of Technology and Sciences, Tirupati, India.
Department of CSE S V U College of Engineering, Tirupati. India
**Corresponding author: Hemalatha T, S. Rohini*

Abstract: *Now-a-days Blockchain and Bitcoin are some of the trendiest keywords as part of the today's technology and even those who are not familiar with Cryptocurrency are quite impressed in the same. The Blockchain is been used highly for Transaction Management and it is replacing the current existing Transaction Management System. If a technology is replacing the existing system there must be a certain problem. To overcome such problems Blockchain Concept is used. In this paper, the Blockchain-Bitcoin Transaction Management System is proposed to overcome the issues with current Banking Systems like, Transactional charges, Financial Crises and Financial Depression and Net Banking Frauds. Bitcoin Blockchain solve these issues with the Centralized, Private ledgers/Distributed ledgers with Peer-to-Peer Networks , Prone to Hacks by using Digital Signatures and Double Spending.*

Keywords: *Blockchain; Bitcoin; Transaction Management; Cryptocurrency;Transaction Management System; Banking System; Peer-to-Peer Networks;*

Date of Submission: 09-06-2018 Date of acceptance: 03-07-2018

I. Introduction

A blockchain is a chain of blocks that has taken from an ancient. This technique was visually described in 1991 by the group of researchers and was reasonably intended into timestamp digital documents. So that it was not possible to pack their than or to tamper with them(like notary). However, it depend by mostly on used by and deputed by "Satoshi Nakamoto" in 2009 to create a digital Cryptocurrency "Bitcoin".

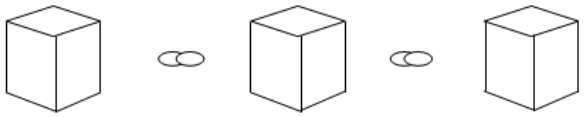

Fig. 1. Blockchain Structure

Blockchain technology promises to be enormously in troublesome and empowering in both public and private sector computing applications. As a way to order transactions in a distributed ledger, blockchains offer a record of consensus with a cryptographic audit trail that can be maintained and validated by multiple nodes. It lets contracting parties dynamically track assets and agreements using a common protocol, thus streamlining and even completely collapsing many in-house and third-party verification processes[1].

Blockchain systems possess a number of attractive attributes for the banking and financial-services markets. Such systems are resilient and can operate as decentralized networks that do not require a central server and do not have a single point of failure. Because they operate using distributed open source protocols, they have integrity and do not need to trust a third party to execute transactions. Public blockchain systems are also inherently transparent, because all changes are visible by all parties. The blockchain functionality also allows applications and users to operate with a high degree of confidence because transactions are unchangeable they cannot be reversed or resequenced. In general, blockchain systems are uniquely able to ensure that contracting parties all have accurate and identical records[1].

Currency transactions between persons or companies are often centralized and controlled by a third party organization. Making a digital payment or currency transfer requires a bank or credit card provider as a middleman to complete the transaction. In addition, a transaction causes a fee from a bank or a credit card company. The same process applies also in several other domains, such as games, music, software etc. The transaction system is typically centralized, and all data and information are controlled and managed by a third party organization, rather than the two principal entities involved in the transaction. Blockchain technology has

been developed to solve this issue. The goal of Blockchain technology is to create a decentralized environment where no third party is in control of the transactions and data.

In this paper, we propose a Blockchain-Bitcoin Transaction Management System in Current Banking System to overcome the issues that occur at the time of transaction between two persons/end-systems like Transactional Charges, Financial crises and Financial depression, double spending and Net Banking frauds. This problem can be solved by using the Blockchain concept Bitcoin transactions as Centralized, distributed ledger, private ledgers, Prone to hacks etc. Here to solve these issues private key cryptography, peer-to-peer network , distributed ledger and digital signatures are used.

The remainder of this paper is organized as follows. Section II describes the related work of this paper and the concept of Blockchain technology discussed in Section III. We describe our system model, including the issues in banking system and Bitcoin transaction management in Section IV. Section V concludes this paper and presents some future plans.

II. Related Work

Blockchain, mostly known as the technology running the Bitcoin cryptocurrency, is a public ledger system maintaining the integrity of transaction data [7]. Blockchain technology was first used when the Bitcoin cryptocurrency was introduced. To this day, Bitcoin is still the most commonly used application using Blockchain technology [8]. Bitcoin is a decentralized digital currency payment system that consists of a public transaction ledger called Blockchain [9]. The essential feature of Bitcoin is the maintainability of the value of the currencywithout any organization or governmental administration in control. The number of transfers and users in the Bitcoin network is constantly increasing [10]. In addition, the conversions with traditional currencies, e.g. KRW, EUR and USD, occur constantly in currency exchange markets [11][12]. Bitcoin has therefore gained the attention of various communities and is currently the most successful digital currency using Blockchain technology [11].

The Bitcoin blockchain in its simplest form is a database or ledger comprised of Bitcoin transaction records. database is distributed across a peer-to-peer network and is without a central authority, network participants validity of transactions before they can be recorded. This agreement, which is known as "consensus," is achieved called "mining."[6].

III. Blockchain Technology

A. Blockchain

Blockchain is the technology behind Bitcoin. A block is a collection of all the recent transactions that have happened and verified. In simple terms, the technology handles blocks uniquely identified, linked transaction records in a chain. A blockchain is a continuously growing, distributed, shared ledger of such blocks, which are sealed cryptographically with a digital fingerprint generated by a hashing function.

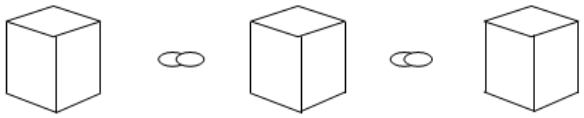

Fig 2. Blockchain

By grouping all the transactions details at pre hash code for this and then store it in a block. Once the transaction is verified, then the block becomes permanent part of the blockchain and chain keeps growing. So, it is believed that for every 10 minutes a new block is created and blockchain keeps growing accordingly. So, how many transactions happened to that all can be grouped as part of the block and then stored in to the blockchain block.

B. Bitcoin

Bitcoin is the first decentralized digital currency that came into the market and was introduced in 2009 by " Satoshi Nakomoto".

Fig 3. Bitcoin

Bitcoins use various cryptographic and mathematical problems that ensure that the creation and management of bitcoins is restricted.
Now the blockchain is a distributed ledger that is completely open to anyone , they have an interesting property, once in there is coded inside the blockchain it becomes very difficult to change it.
Lets take a block

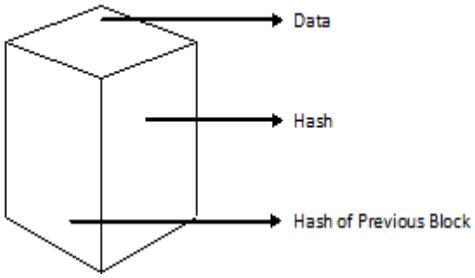

Fig 4. Bitcoin block

The bitcoin block example consists of three elements: One is the data which stores the data inside the block in the present type of blockchain.
For example , the bitcoin blockchain stores the details about transactions, such as sender and receiver and the number of points.

Fig 5. Bitcoin Block example

The Second is Hash, where the hash can be compared with a Fingerprint. It identifies a block and all of its contents and it is always unique just as a fingerprint.

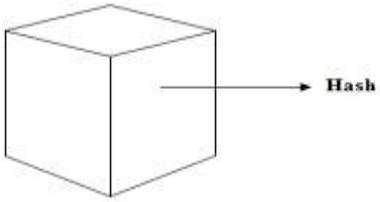

Fig 6. Block

Once a block is created, its hash is been calculated, changing something inside the block will cause hash to change. So, another words Hash is a failure one, When you wants to check the changes of the block. If the figure print of the block changes it no longer is the same block.

The third element inside of the each block is the Hash of the previous block. This effectively creates a chain of blocks and this technique is used to keep this blockchain so secure.

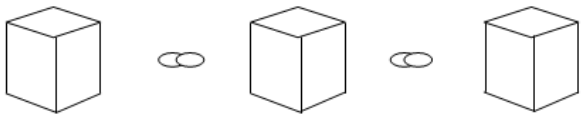

Fig 7. Creates the chain

Let us take an example, here we have a chain of three blocks, as we can see each block has Hash and Previous hash.

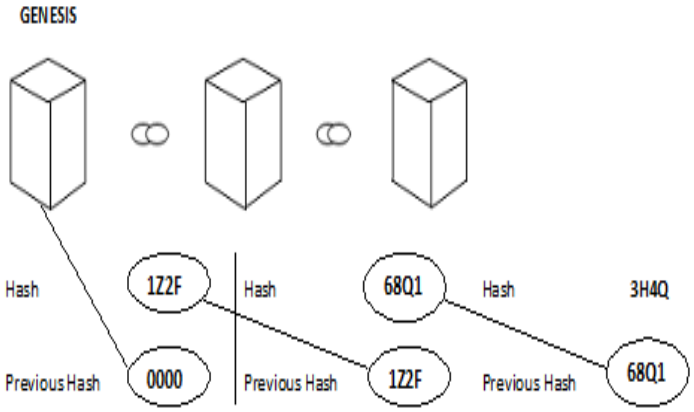

Fig 8. Genesis Block

Now the block No.3 points the block No.2 and bock No.2 points to No.1. The first block is a bit special, it can point to previous blocks, because well it's the first one, we call this block the "Genesis block".

Now coming to the second block , it causes the hash of the block to changes well in turn the block 3 and all the following blocks invalid, because they no longer store a valid hash of the previous block. So change in the single block will make all following blocks invalid. But using hash is none enough to prevent tempering.

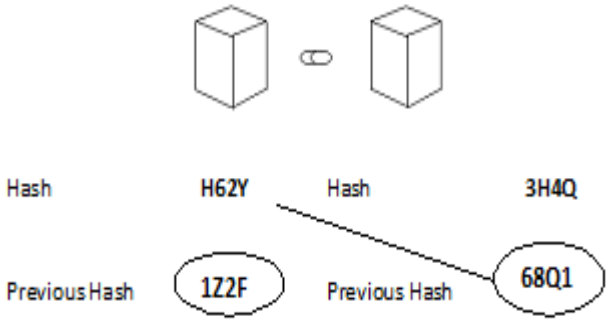

Fig 9. Tampering

Computing these days are very fast and can calculate 100's of, 1000's of hashes per second , we could effectively tamper with the block and we calculate all the hashes of the other blocks to make the blockchain family again.

So, to mitigate this blockchain are something that are called Proof-of-Work. It is a mechanism that slows down the creations of new blocks.

Fig 10. Slow and steady

In Bitcoins case it takes about 10 minutes to calculate the coin Proof – of – Work and add a new block to the chain.

Fig 11. Adding new chain

This mechanism makes a very hard to tamper with the blocks , because if we tamper with one block we need to calculate the proof –of-work for all the following blocks.
So, the security of a blockchain comes from the creatives of the hashing and the proof-of-work mechanism. There is one more way, Blockchains secured themselves, that is being distributed.

IV. Bitcoin Transaction Management

Now Blockchain and Bitcoin are some most of trendy keywords as part of the today's technology and even those who are not familiar with crypto currency are quite impressed in the same. Blockchain is been used highly for transaction management and it is replacing the current existing transaction management system. If a technology is replacing the existing system, there must be a certain problem.

C. Issues with Current Banking Systems

For example, When Host A wants to send $100 to Host B, due to transaction fee $2, Host B is getting only $98, now it may not seem a huge amount but lets assume that there are every day 10 thousand transactions are happen, and in that 10 thousand transactions and if 2% commission and it's a huge amount. Some of the issues like, Net Banking Frauds, Transactional Charge with everything and Financial crises etc.,

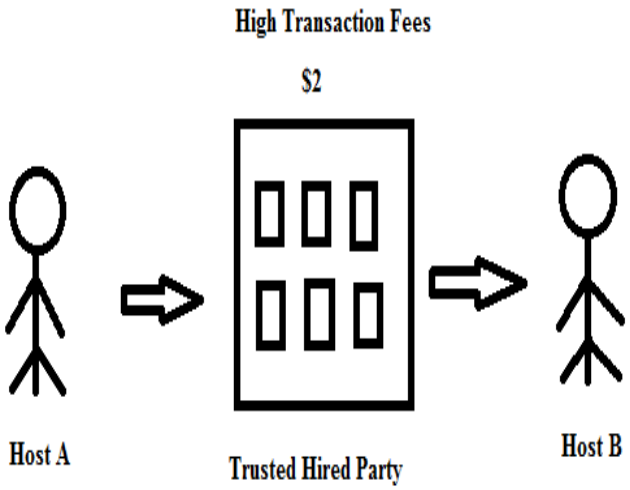

Fig 12. Transaction System

In the year 2015 JP Morgan Chase, Bank of America and Wells Fargo alone earned more than $6 billion from ATM and overdraft fees (SNL Financial and CNN Money Report).

Host A is having $500 in his account and at the same time he is sending $500 to Host C and $400 to Host B. Now , if the both transactions takes at the same time then it becomes a problem to identify which is valid, because the Digital Signature attached to digital transaction can be to an extent falsified and copied as well this makes double spending quite possible and something that is of a challenge. This is one challenge that most of the banking systems or digital financial solutions had faced across when they were working with online payment transactions. Apart from this the financial crises and financial depression.

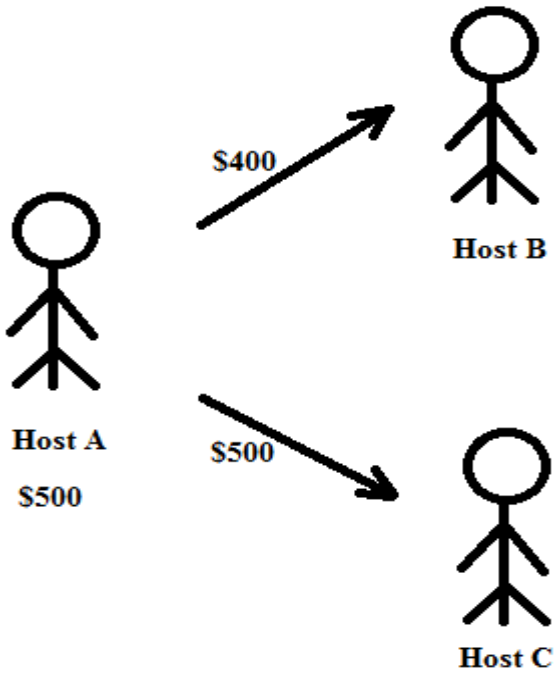

Fig 13. Transaction of Host A, B, C

D. How Bitcoin Solves These Issues

Bitcoin solved the issue we had with Centralized banks

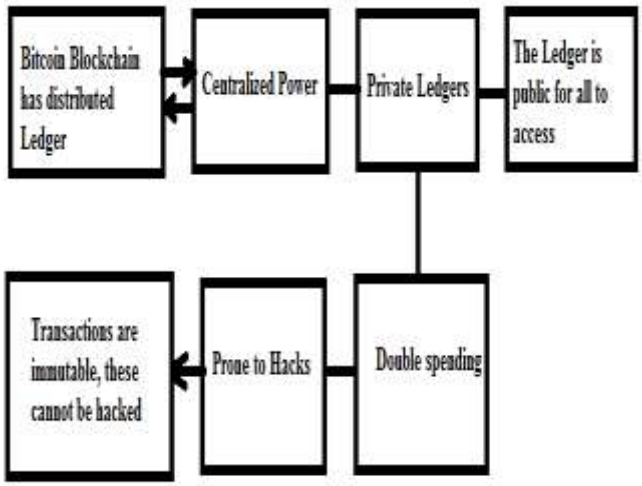

Fig 14 . Sructure of Bitcoin Sloutions

In Centralized power every monitoring system is controlled by a government authority. It could be a central body anonymous personality and so far almost all currency is out there today are actually controlled by the central authority.

However, with Bitcoin this system got decentralized and distributed among everyone of the bitcoin system.

Most of the financial institutions are private ledgers. However with the blockchain system the ledger in itself is public. Everyone who becomes the part of this blockchain network gets a complete copy of the entire blockchain as soon as the signup, so immediately when we signup for the bitcoin blockchain ,we get the list of complete transactions that has happened from the start of the bitcoin Bitcoin Transaction that's a huge amount of transaction, but blockchain makes it very easy as well as completely secure and store all the transaction details at the same time , it ensures that none of it get manipulated.

The blockchain systems cannot be hacked in Prone to Hacks.

Double spending is not allowed because of the basic structure of the block transactions.

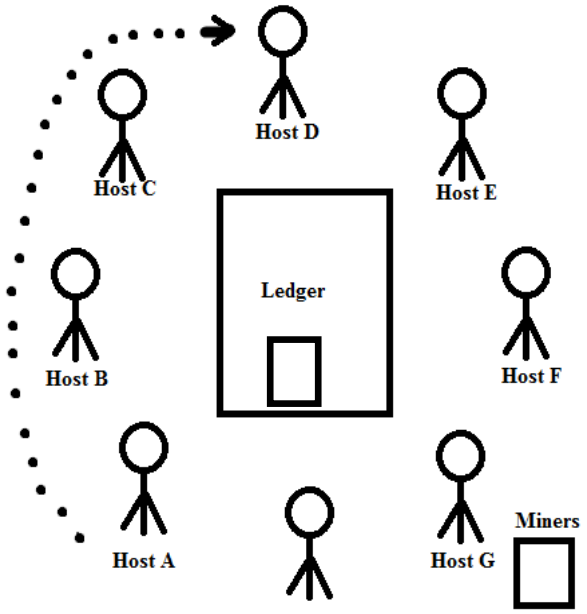

Fig 15.(a) Bitcoin Transaction Management

- Let us take a bitcoin transaction where Host A wants to transfer $500 to Host D.
- The transactions is a part of the new block that will be validated at Miners F and G.

Miners – They have to check whether Host A is having a sufficient balance are not.

Account Number	Balance	
Xxxxxxxxxxxx	40	Ledger
Xxxxxxxxxxxx	52.67	
Xxxxxxxxxxxx	1482	
Xxxxxxxxxxxx	12.00	
Xxxxxxxxxxxx	673	
Xxxxxxxxxxxx	100.65	

Fig 16. Ledger

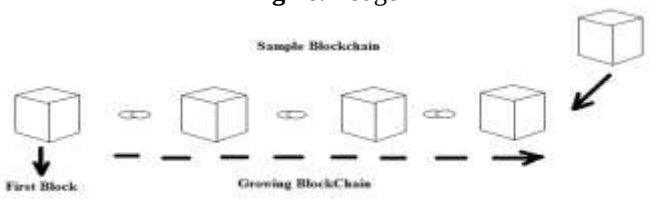

Fig 17. Sample Blockchain

Every transaction holds details of the transfer of currency from one account to the other. The balance of any account is not stored explicitly. It is always calculated by adding up all the blockchain transactions ever recorded. This balance gets updated for every time when transaction takes places and the ledger gets updated itself for every transaction.

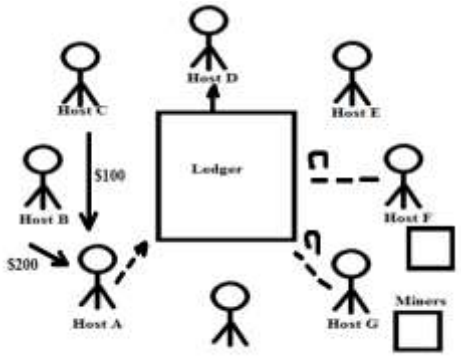

Fig 18.(b) Bitcoin Transaction Management

- Host F and G are Miners who use, they resources to validate the block containing the transaction.
- Once the block is validated, money is deducted from Host A's account and is transferred to Host D's bitcoin account.
- This solves the problem of Double spending.
- The Miners who validate the transaction as well as complete the next block of the blockchain get as(12.5) BTC as incentive which becomes the first transaction for the next(new) block.

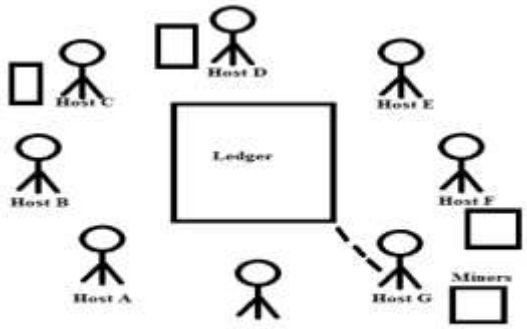

Fig 19.(c) Bitcoin Transaction Management

- The current block becomes a permanent part of the blockchain.

E. Flow Diagram of Bitcoin Transaction Management

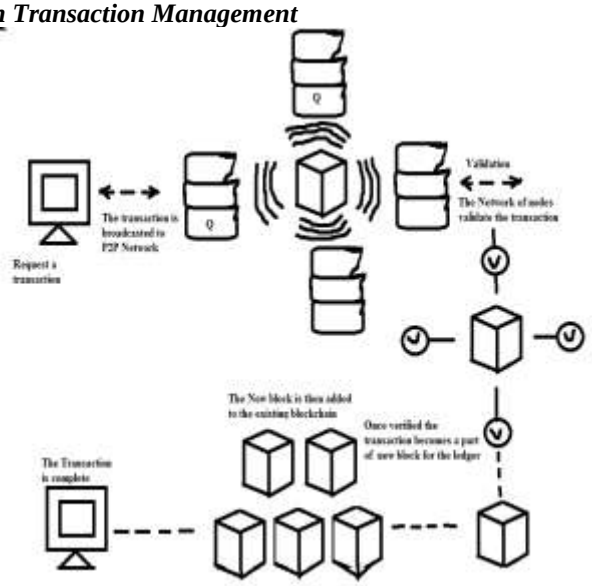

Fig 20. Flow Diagram

V. Conclusion

In this paper, the blockchain concept is used to overcome the issues with banking systems by proposing the bitcoin transaction management system for current banking system. The issues are like transactional charges, financial crises and net banking frauds etc., These are overcome by the centralized, private ledgers and double spending etc. In the Future work this work will be implemented on real systems.

References

[1]. Jesse Yli-Huumo1, Deokyoon Ko2, Sujin Choi4*, Sooyong Park2, Kari Smolander3Michael Crosby "Where Is Current Research on Blockchain Technology?—A Systematic Review "a research article.

[2]. (Google) Nachiappan (Yahoo) Pradan Pattanayak (Yahoo) Sanjeev Verma (Samsung Research America) Vignesh Kalyanaraman (Fairchild Semiconductor in" BlockChain Technology: Beyond Bitcoin" in AIR Applied Innovative Review. Issue no.2, June 2016.

[3]. Youtube videos of Edureka " Blockchain Tutorials".

[4]. Youtube video " How does a Blockchain work".

[5]. "What is Blockchain Technology? A Step-by-Step Guide For BeginnersAn in-depth guide by BlockGeeks – http//blockgeeks.com.

[6]. The difference between Bitcoin and blockchain for business Blockchain Unleashed: IBM Blockchain Blog.

[7]. Swan M. Blockchain: Blueprint for a New Economy. ª O'Reilly Media, Inc.º; 2015.

[8]. Coinmarketcap, Crypto-Currency Market Capitalizations; 2016. Accessed: 24/3/2016. https://coinmarketcap.com/.

[9]. Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. Consulted. 2008; 1(2012):28.

[10]. Kondor D, PoÂsfai M, Csabai I, Vattay G. Do the rich get richer? An empirical analysis of the Bitcoin transaction network. PloS one. 2014; 9(2):e86197. doi:10.1371/journal.pone.0086197 PMID: 24505257

[11]. Herrera-Joancomart J. Research and Challenges on Bitcoin Anonymity. In: Garcia-Alfaro J, Herrera- Joancomart J, Lupu E, Posegga J, Aldini A, Martinelli F, et al., editors. Data PrivacyManagement,Autonomous Spontaneous Security, and Security Assurance. vol. 8872 of Lecture Notes in Computer Science.Springer International Publishing; 2015. p. 3±16. Available from: http://dx.doi.org/10.1007/978-3-319-17016-9_1.

[12]. Bitcoincharts; 2016. Accessed: 24/3/2016. https://bitcoincharts.com.

IOSR Journal of Computer Engineering (IOSR-JCE) is UGC approved Journal with Sl. No. 5019, Journal no. 49102.

Hemalatha T, S. Rohini " Blockchain-Bitcoin Transaction Management System for Current Banking System." IOSR Journal of Computer Engineering (IOSR-JCE) 20.3 (2018): 40-48.