

Digitized and decentralized blockchain technology for banking sector

First Author^a, Second Author^b, Third Author^{a,b,*}

^aFirst affiliation, Address, City and Postcode, Country

^bSecond affiliation, Address, City and Postcode, Country

Abstract

With steadily developing advancements, the banking frameworks can refresh from their customary procedures to an advanced, unchanging, appropriated ledger that can be executed by means of Blockchain. Blockchain Technology is a disseminated friend to peer connected structure which can tackle the issue of keeping up with and keep exchanges in a financial framework. Blockchain gives properties like straightforwardness, auditability, and security. This paper targets giving these functionalities in a disseminated financial framework utilizing blockchain, which will be at standard with the current procedures. It will likewise zero in on the restrictions while carrying out blockchain and future degree.

Keywords: Blockchain, Peer, Ledger;

1. Introduction

This 21st century is about various advances. As innovation is upgrading, individuals are adjusting to the updating advances. From utilizing controller gadgets to utilizing voice notes for providing orders to control gadgets. One of the advanced innovations is Blockchain innovation. Blockchain is a circulated record of a permanent openly available report of computerized exchanges, where recently added record ids are checked across the dispersed organization before it is put away in a square. The data which is added into the record is irrefutable yet not editable. The squares are distinguished by its cryptographic mark. Nonexclusive duplicates of all information are shared on the Blockchain. Members independently approve the information without an amalgamate power. In a place of truth, in the event that one hub is fruitless, the excess hubs will resume to work with no disappointment.

An exchange on blockchain is endorsed provided that every one of the gatherings on the organization all in all support it. Notwithstanding, agreement-based rules can be altered to suit various circumstances. The possibility that disseminated shared organization could be working without depend on believed outsider were given close consideration and were examined heatedly. With the decentralized idea of blockchains, it empowers application without confided in delegate to be running fully supported by cryptography, fair hubs and its agreement component. The benefits of the blockchain innovation meets the fundamental requirements in light of its adaptability and security by laying out a decentralized and secure data organization.

*XYZ.

E-mail address: author@institute.xxx

1.1 Background

The Blockchain Technology has first portrayed by Stuart Haber and W. Scott Sornetta in the year 1991. They presented a computationally useful answer for time-stepping advanced records with the goal that they could be not be harmed. They fostered a framework which is cryptographically secure chain of squares for putting away the time-stepped archives.

In 1992, Merkle trees has planned the framework and named it as blockchain. Merkle trees is utilized to make a got chain of squares. In 2004, Hal Finney presented a framework called 'Reusable verification of work' as a model for computerized cash. Further in 2008, Satoshi Nakamoto conceptualized the hypothesis of circulated blockchains. As of late, Governments are likewise beginning to enter the blockchain market. Blockchain gives better approaches to coordinate cycles and handle data in a more proficient manner.

Need of Blockchain

Blockchain helps in the verification and the traceability of multistep transactions needing verification and traceability. It can provide secure transactions, reduce compliance costs and speed up data transfer processing. Blockchain technology can help contract management and audit the origin of a product.

Block chain has many advantages. For example,

- It is a permanent public computerized record, and that implies when an exchange is recorded, it can't be changed
- Because of the encryption, Blockchain is generally secure
- The exchanges are done straightforwardly in a flash, as the record is refreshed consequently
- As it is a decentralized framework, no mediator expense is required
- The realness of an exchange is checked and affirmed by members

1.2 Area of Work

Blockchain is an appropriated information base that is partitioned a portion of the center points of PC association. as measurements set, a blockchain stores insights electronically in programmed plan. They expect enormous detail in computerized unfamiliar trade structure, as Bitcoin, for taking care of a covered and decentralized document of trades. It makes the accept without the prerequisite for a trusted in untouchable.

Blockchain gathers data as squares. Blocks have specific capacity limit and when filled it connects to the past squares which are as of now full, shaping a chain of information known as the blockchain. The objective of blockchain is to permit advanced data to be recorded and appropriated, yet at the same not altered. In this manner blockchain record of exchanges can't be erased or adulterated. Blockchain is otherwise called dispersed record innovation.

1.3. Existing System

Now a days the transactions are being processed using Cheques, Net Banking and payment Wallets. Payment wallet transactions involves third party of government. These transactions allow centralized platform means power and rights are not to be equally distributed among all the participants in a system. Performing transactions through Cheques, Net banking and payment Wallet the receiver effectively authorizing the seller to “Pull” a payment from their account, passing through several financial intermediates in the process. For this kind of transaction, it is necessary for user to provide personal information such as your name and address.

Table 1. Comparison

	Traditional Banking	Internet Banking	Blockchain Banking
Efficiency	Many Intermediate connections Complex clearing process Low productivity	Many Intermediate connections Complex clearing process Low productivity	Highlight Point transmission Easy clearing process High productivity
Cost	Large measure of manual assessment. Significant expense	Limited quantity of manual assessment. Significant expense	Totally robotized. Minimal expense
Safety	Centralized information capacity can be altered. Simple to spill Users individual Information. Unfortunate Safety	Concentrated information capacity can be altered. Simple to spill Users individual Information. Unfortunate Safety	Dispersed information capacity can't be altered. Personal information is more secure. (Because it uses asymmetric encryption) Good Safety
Customer Experience	Homogeneous service	Personalized service	Personalized service

1.4. Objective

This project aims to create a transaction website using blockchain model which will help a user to transact the huge money in the emergencies and in secure way. As we know, blockchain prevents double spending by timestamping groups of transactions. So, blockchain technology became a major part in banking industry. Accordingly, the system developed will give access to that user if and only if he/she has completed the KYC in the respected bank. The proposed model detects only the Gmail id given at the time of account opening. Users need to enter only the Gmail id as their user id while accessing this platform.

2. Encryption Algorithm

Encryption calculation is utilized to keep up with security and obscurity of the exchange and the client, separately. SHA calculation is an encryption calculation that is utilized to carry out away encryption.

- SHA (Secure hash algorithm)

SHA-256 (secure hash algorithm, FIPS 182-2) is a cryptographic hash function with digest length of 256 bits. It is a keyless hash function; that is, an MDC (Manipulation Detection Code). A message is processed by blocks of $512 = 16 \times 32$ bits, each block requiring 64 rounds.[13]

The algorithm uses the functions:

3. $\text{Ch}(X, Y, Z) = (X \wedge Y) \oplus (X \wedge Z),$
4. $\text{Maj}(X, Y, Z) = (X \wedge Y) \oplus (X \wedge Z) \oplus (Y \wedge Z),$
5. $\Sigma_0(X) = \text{RotR}(X, 2) \oplus \text{RotR}(X, 13) \oplus \text{RotR}(X, 22),$
6. $\Sigma_1(X) = \text{RotR}(X, 6) \oplus \text{RotR}(X, 11) \oplus \text{RotR}(X, 25),$
7. $\sigma_0(X) = \text{RotR}(X, 7) \oplus \text{RotR}(X, 18) \oplus \text{ShR}(X, 3),$
8. $\sigma_1(X) = \text{RotR}(X, 17) \oplus \text{RotR}(X, 19) \oplus \text{ShR}(X, 10),$

and the 64 binary words K_i given by the 32 first bits of the fractional parts of the cube roots of the first 64 prime numbers:

```
0x428a2f98 0x71374491 0xb5c0fbcf 0xe9b5dba5 0x3956c25b 0x59f111f1 0x923f82a4 0xab1c5ed5 0xd807aa98
0x12835b01 0x243185be 0x550c7dc3 0x72be5d74 0x80deb1fe 0x9bdc06a7 0xc19bf174 0xe49b69c1 0xefbe4786
0x0fc19dc6 0x240ca1cc 0x2de92c6f 0x4a7484aa 0x5cb0a9dc 0x76f988da 0x983e5152 0xa831c66d 0xb00327c8
0xbf597fc7 0xc6e00bf3 0xd5a79147 0x06ca6351 0x14292967 0x27b70a85 0x2e1b2138 0x4d2c6dfc 0x53380d13
0x650a7354 0x766a0abb 0x81c2c92e 0x92722c85 0xa2bfe8a1 0xa81a664b 0xc24b8b70 0xc76c51a3 0xd192e819
0xd6990624 0xf40e3585 0x106aa070 0x19a4c116 0x1e376c08 0x2748774c 0x34b0bcb5 0x391c0cb3 0x4ed8aa4a
0x5b9cca4f 0x682e6ff3 0x748f82ee 0x78a5636f 0x84c87814 0x8cc70208 0x90befffa 0xa4506ceb 0xbef9a3f7
0xc67178f2
```

3.Literature survey

Bitcoin: A peer to peer Cash System, by Satoshi Nakamoto is a first white paper and it tells that Blockchain is a transaction database which contains information about all the transactions ever executed in the past and works on Bitcoin protocol. It creates a digital ledger of transactions and allows all the participants on network to edit the ledger in a secured way which is shared over distributed network of the computers. For making any changes to the existing block of data, all the nodes present in the network run algorithms to evaluate, verify and match the transaction information with Blockchain history. [1] When it comes to Bitcoin and cryptocurrency, the manipulation factor is equal to zero, if dealing is done in this system. Using blockchain technology of cryptocurrency means no paperwork, so there will be no waste to manage as well. There are even companies in the world, who are doing eco-friendly tasks, managing waste and accepting payment through cryptocurrency like Bitcoin. [12] Decentralized block chain technology: application in banking sector, by Nikita Rajeshkumar Bagrecha explains about usage of nodes in block chain that is there are two different nodes, verification node belongs to bank and user node for customer. They used rsa algorithm (rivest, shamir, adleman) to create public and private key.[6] Decentralize banking application using block chain technology, by Yash Amesar describes the term block chain and introduces the concept of blockchain frameworks. They have mainly focused on ethereum and web3 uses for implementing block chain decentralized applications(dapp).[7] Blockchain Revolution in Banking Industry, by Thulya Palihapitiya explains that Blockchain technology needs to follow certain standards of modernization. This will be based on the adoption of the latest & advanced technology.[8] A study on blockchain technology in banking sector, by C. Mallesha found that there 4 concepts in blockchain architecture and also outlined about the consensus algorithms. Block chain technology needs to follow certain standards of modernization. This will be based on the adoption of the latest & advanced technology. [9] Blockchain application and outlook in the banking industry, by Ye Guo tells that the promising application prospects are being offered by block chain technology to the banking industry. The interest rate liberalization is to be considered for the said aspect. The study of the systems that are existing to support the banking sector is being carried out. Multi-signature addresses by M. Rosenfeld explains that the confidential keys expected to spend from a wallet can be spread across various machines, dispensing with any of those machines as a weak link, with the reasoning that malware and programmers are probably not going to taint every one of them. The higher the quantity of keys expected to spend the assets (ie the higher M is in M-of-N), the more troublesome it would be for an aggressor to take effectively your assets, but the more bulky really utilizing that wallet becomes. The multisig wallet can be of the mof-n type where any m confidential keys out of a potential n are expected to move the cash.

For instance, a 2-of-3 multisig wallet could have your confidential keys spread across a work area, PC, and cell phone, any two of which are expected to move the cash, yet the split the difference of any one key can't bring about burglary. This can be utilized in combination with equipment wallets. By expecting that keys from various equipment wallets sign exchanges, it can immeasurably diminish the probability that a noxious party that dealt with your equipment wallet could take your assets, since for it to do that, the malignant party would need to think twice about equipment wallets. In the event that every equipment wallet you use in a multisig wallet is made by an alternate organization, it would be inconceivably hard for them to contrive on an assault covertly.

4. Proposed System

The proposed Blockchain exchange framework depends on the deeply grounded Bitcoin approach recognized in "Satoshi Nakamoto, 2008". The framework has been intended to help a financial application in reality climate considering explicit necessities like security, qualification, accommodation, receipt freeness and evidence.

The proposed framework intends to accomplish secure computerized exchanges without undermining its convenience. Inside this specific situation, the framework is planned utilizing an online point of interaction to work with client commitment with measures, for example, computerized mark to safeguard against twofold spending. With a reasonable need to clients an easy-to-use point of interaction is executed to empower straightforward entry. Moreover, the cryptographic hash of the exchange (ID) is messaged to the client as a proof that the exchange has been finished.

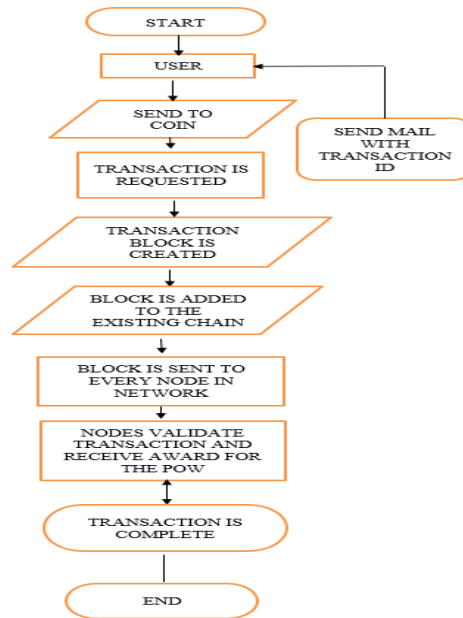


Fig. 1. Architecture of proposed model

5. Results

The result here explains how the model is evaluated and what we used to create this model. It is a web application used to transact money using block chain technology.

5.1 Evaluation of the model

To create a web application, we used Python Programming and Django framework for running the Website in the server. We used SHA 256 algorithm to hashing the data into hash values. The hashing algorithm can be imported from Hash library from Python.

5.2 Modules

Peer Module:

Users also known as peers. In this module user can add themselves by User name. The username can be their own personal mail-id which is already registered while opening bank account in the bank. The user should be completed with KYC verification.

Block Module:

The created peers stored in blocks. We have to add the peers into the block using add peer to block web page. Then the users can have their own transaction block. The transaction block is created separately for every transaction of each user.

Transaction Module:

The users can make transactions after validation of blocks. The transactions can be cross border also, tax collection will be less compared to traditional and internet banking systems. These transaction use coins such as Bitcoin, Altcoin, Dogecoin, and many more.

Chain Module:

After the transaction, the block will be added to the existing chain of blocks. The web page known as view chain can be used to view the previous and present transactions.

5.3 Outputs

First Screen

 Blockchain Transaction

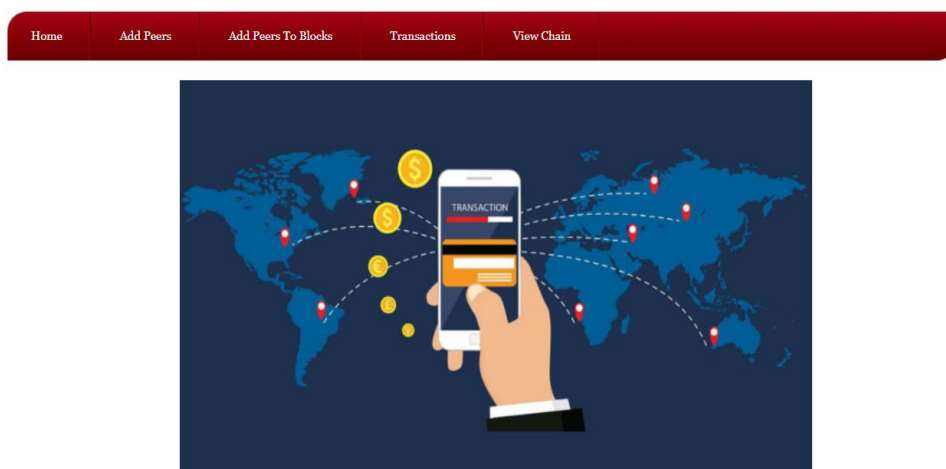
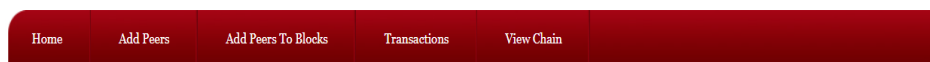


Fig. 2. Home screen

Click on 'Add Peers' link to add new peer details

 Blockchain Transaction



Add Peer Screen

Peer Name

Fig .3. Add peers

Home	Add Peers	Add Peers To Blocks	Transactions	View Chain	
------	-----------	---------------------	--------------	------------	--

Add Peer Screen

Peer Name

Added Peer Details

Fig. 4. Peer details

We are adding new peer as 'sujeevana8@gmail.com' and the entry will be available here till it added to block and after adding to block entry will be deleted from peer screen. Now click on 'Add Peer' button to get below screen.

Home	Add Peers	Add Peers To Blocks	Transactions	View Chain	
------	-----------	---------------------	--------------	------------	--

Add Peer Screen

Peer Name

Added Peer Details
sujeevana8@gmail.com

Fig.5. Added Peer Details

we can see newly added peer details in a table. Now click on 'Add Peers to Blocks' link to add this peer to block chain.

Block No	Block Name	Previous Proof Hash	New Hash	Block Create Time
1	['kaleem.mmd@gmail.com']	9aafedab208fc4b35ca81e510a6926ee4d102f371c583d9266e4ed0210a12	00c3f0cb0d5fe8db139866df997b1333c5a085a344f65bdf39742466ebda9bd	2020-03-26 14:36:26.05727
2	['saleem.mmd@gmail.com']	00c3f0cb0d5fe8db139866df997b1333c5a085a344f65bdf39742466ebda9bd	00931653dd19229666d39310031e945066e7b4f9f9a4d49d40a69317d27c	2020-03-26 14:36:27.58150
3	['himesh@gmail.com']	00931653dd19229666d39310031e945066e7b4f9f9a4d49d40a69317d27c	0085ebec767ae59127b6f7cb3d69a1ef17d787a0b196a8cac48ba1d1eaf8d1	2020-03-26 14:38:25.29263
4	['raju@gmail.com']	0085ebec767ae59127b6f7cb3d69a1ef17d787a0b196a8cac48ba1d1eaf8d1	0096ee96e6d80c5b0b90301b3b2466af1d8782a1c4ec7272c46e4cbbaad43	2020-03-26 14:49:20.07483

Fig. 6. Hash Values

All added peers to block chain will be displayed with their old and new hash value as proof of work. We can see in above screen New Hash of first row is matched with previous hash of second row and goes on till transaction executed successfully with hash validation.

Now we can select new peer name from drop down box and click on 'Add to Block' button to add new peer to new block

Block No	Block Name	Previous Proof Hash	New Hash	Block Create Time
1	['kaleem.mmd@gmail.com']	9aafedab208fc4b35ca81e510a6926ee4d102f371c583d9266e4ed0210a12	00c3f0cb0d5fe8db139866df997b1333c5a085a344f65bdf39742466ebda9bd	2020-03-26 14:36:26.05727
2	['saleem.mmd@gmail.com']	00c3f0cb0d5fe8db139866df997b1333c5a085a344f65bdf39742466ebda9bd	00931653dd19229666d39310031e945066e7b4f9f9a4d49d40a69317d27c	2020-03-26 14:36:27.58150
3	['himesh@gmail.com']	00931653dd19229666d39310031e945066e7b4f9f9a4d49d40a69317d27c	0085ebec767ae59127b6f7cb3d69a1ef17d787a0b196a8cac48ba1d1eaf8d1	2020-03-26 14:38:25.29263
4	['raju@gmail.com']	0085ebec767ae59127b6f7cb3d69a1ef17d787a0b196a8cac48ba1d1eaf8d1	0096ee96e6d80c5b0b90301b3b2466af1d8782a1c4ec7272c46e4cbbaad43	2020-03-26 14:49:20.07483
5	['sujeevana8@gmail.com']	0096ee96e6d80c5b0b90301b3b2466af1d8782a1c4ec7272c46e4cbbaad43	00e06defb94378408751052623f65d32f590373b65eb2991754283d91f1056	2022-04-20 16:40:23.58975

Fig. 7. Add to block screen

New peer also added to block and once it added then that peer will be removed from drop down box. Now click on 'Transactions' link to perform transaction between block chain users.


From Peer: sujeevana8@gmail.com

To Peer: chadakavyasri369@gmail.com

Coins:

Fig. 8. Transactions screen

From peer and to peer choose the user from drop down box and then enter number of coins and click on ‘Submit Transaction’ button to transfer fund.

 Blockchain Transaction

Home Add Peers Add Peers To Blocks Transactions View Chain

Transactions Screen

From Peer

sujeevana8@gmail.com

To Peer

chadakavyasri369@gmail.com


Coins

100

Submit Transaction

Fig.9. Number of Coins

I am sending 100 coins to other user and after transaction completion will display the below screen.

 Blockchain Transaction

Home Add Peers Add Peers To Blocks Transactions View Chain

Transactions Screen

Transaction complete between sujeevana8@gmail.com and chadakavyasri369@gmail.com coins 100

Fig.10. Notification

Now click on ‘View Chain’ tag to view all transaction details

Transaction No	From Peer	To Peer	Coin	Transaction Date
0	kaleem.mmd@gmail.com	saleem.mmd@gmail.com	55	2020-03-26
1	saleem.mmd@gmail.com	kaleem.mmd@gmail.com	23	2020-03-26
2	kaleem.mmd@gmail.com	himesh@gmail.com	40	2020-03-26
3	kaleem.mmd@gmail.com	raju@gmail.com	100	2020-03-26
4	sujeevana8@gmail.com	himesh@gmail.com	9	2022-04-20
5	sujeevana8@gmail.com	chadakavyasri369@gmail.com	5553	2022-04-20
6	sujeevana8@gmail.com	maitridved@gmail.com	77	2022-04-20
7	sujeevana8@gmail.com	chadakavyasri369@gmail.com	22	2022-04-20
8	maitridved@gmail.com	sujeerreddy1@gmail.com	77	2022-05-04
9	sujeevana8@gmail.com	chadakavyasri369@gmail.com	100	2022-05-12

Fig .11. View chain

From view chain we can retrieve all transaction details.

5.4 Performance Analysis

Two public blockchain stages bitcoin and Ethereum were taken a glance at considering their display throughout the limits for instance block time block size no. of exchanges and inconvenience were used to ponder between these two phases too. Bitcoin transaction takes 1 minute of time to complete the process. If we use Ethereum then transaction fee becomes higher. There is a threat of online hacking because Ethereum is the ledger technology and currency, but bitcoin is nothing more than a currency. Both uses Blockchain. Ethereum takes more time to transact currency.

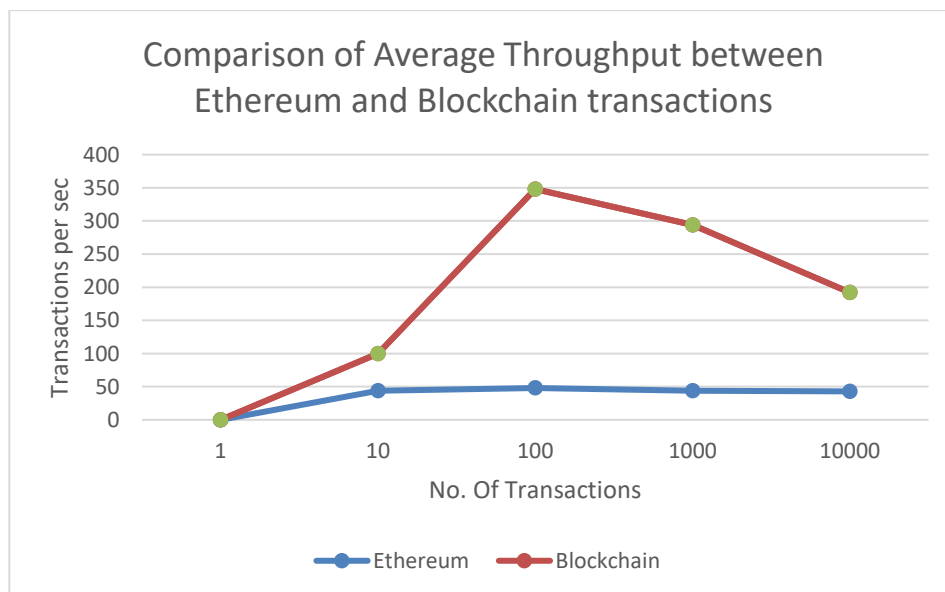


Fig. 12. Comparison between two technologies

6. Conclusion

We have proposed a construction for electronic exchanges without depending upon trust. We began with the standard game plan of coins made using advanced marks, which gives solid control of proprietorship, yet is separated without a procedure for forestalling twofold spending. To address this, we proposed a scattered affiliation utilizing affirmation of-work to record a public history of exchanges that rapidly turns out to be computationally crazy for an assailant to change tolerating fair focus focuses control a bigger part of CPU power. The affiliation is great in its unstructured straightforwardness. Focuses work all the while with little coordination. They shouldn't stress over to be seen, since messages are not directed to a specific spot and just should be totally completed a best exertion premise.

References

- [1] S. Nakamoto, Bitcoin: "A Peer-to-Peer Electronic Cash System"-2008.
- [2] S. Sargolzaei, B. Amaba, M. Abdelghani, and A. Sargolzaei, "Cloud based Smart Health-care Platform to tackle Chronic Disease," vol.4863, no. August, pp. 30-32, 2016.
- [3] S. Underwood, "Blockchain beyond bitcoin," Commun. ACM, vol. 59, no. 11, pp.15-17, 2016.
- [4] Salah albeshr, Haitham nobanee , "Blockchain application in banking industry: A mini-review",2020
- [5] G. Engaged, J. Tobe, G. Your, C. Computing, C. Dellorso, E. Apps, E. Reggie, R. Coughlan, and M. S. Fernandes, "Annual Conference - May 6-7, 2013-Kingsmill Resort ` The Value of Values: Linking Strategy and Decision Making" - 2013 Annual Conference Educational Sessions," 2013.
- [6] Nikita Rajeshkumar Bagrecha¹, Ishaq Mustafa Polishwala², Pragya Abhai Mehrotra³, Rishabh Sharma⁴ "Decentralized Block Chain Technology: application In Banking Sector" INCET, June-2020
- [7] Yash Amesar, Yash Nerkar, Nitesh Mali, Ashwin Nitnaware, Dr. Prashant Yawalkar "Decentralize Banking Application Using Block Chain Technology" IJSREM, sep-2020
- [8] Thulya Palihapitiya "Blockchain Revolution in Banking Industry" 2020.
- [9] C.Mallesha, S.Haripriya, " A Study on Blockchain technology in banking sector" IJACR,2019.
- [10] Ibrar Ahmed, Shilpi, Mohammad Amjad "Blockchain Technology A Literature Survey" IRJET, Oct-2018
- [11] Ye Guo, Chen liang, "Blockchain application and outlook in the banking industry.", Springer open,2016
- [12] Jackson, M. (2018). How Bitcoin and blockchain technology can benefit the waste management industry. Retrieved February 1, 2019
- [13]Lucey, B., & Corbet, S. (2018). Why Bitcoin proves regulation is the biggest issue facing cryptocurrency. Retrieved February 1, 2019, from
- [14]DHAR, S. (2016). Smarter banking: Blockchain technology in the Indian banking. *Asian Management Insights*, 46.
- [15] Gupta, A. (2018). Blockchain Technology Application in Indian Banking Sector. *Delhi business Review*
- [16] Khadka, R. (2020). The impact of blockchain technology in banking. *Centria*.
- [17] Patki, A. (2020). Indian banking sector: blockchain implementation, challenges and way forward. *Journal of Banking and Financial Technology* , 1.
- [18] Rega, F. G. (2018). Blockchain in the banking industry: an Overview. , 1-8.

[19] Wattana Viriyasitavat (2018). Blockchain characteristics and Consensus in modern business process. JIII,1.

[20] Thomas Kitsantas (2019). A review of blockchain technology and its applications in the business environment.