IJCSE International Journal of Computer Sciences and Engineering Open Access

Survey Paper Vol.-6, Issue-5, May 2018 E-ISSN: 2347-2693

A Survey on Blockchain Technology- Taxonomy, Consensus Algorithms and Applications

N.S. Tinu

Dept. of CSE, New Horizon College of Engineering, Autonomous college affiliated under VTU, Bangalore, India

[*]*Corresponding Author: tinuns@gmail.com*, Tel.: +9740332141

Available online at: www.ijcseonline.org

Accepted: 21/May/2018, Published: 21/May/20182018

Abstract— Blockchain is a buzzword in the current technology trends. It is usually coupled with the cryptocurrency terms: Bitcoin and Ethereum. Any applications that can be optimized by decentralization and that needs to be highly secured could opt for this technology. Blockchain technology has already entrenched into the finance and banking domains by its unusual transparency, security, and flexibility, that facilitates the control of transactions in a decentralized manner. Its distributed and peer-authentication features empower it to span across auxiliary domains like Contractual Agreements and Real Property, Smart Grids, Gaming and Entertainment, Government public services and Smart Cities with IOT, reputation systems, and security services. This paper provides a description of key characteristics, architecture, and taxonomy of blockchain technology. Moreover, the paper provides an insight into the popular consensus algorithms, technical challenges, and major application areas. Future trends and signs of progress in the blockchain technology were discussed.

.

Keywords—Blockchain, Distributed Ledger, Cryptocurrency

I. INTRODUCTION

Blockchain technology was initially developed to facilitate the digital currency Bitcoin, a powerful concept proposed in the anonymous white paper of Satoshi Nakamoto “Bitcoin: A peer-to-peer electronic cash system” in 2008 and implemented in 2009. But both are two separate technologies, Bitcoin is an encrypted currency, while blockchain is the platform that imparts peer-to-peer payment, supply chain tracking, and many more. In simple words, blockchain can be considered as an operating system upon which applications such as Bitcoins and Ethereum function.

In the simplest words, blockchain is a distributed digital ledger that is open, shared and highly secured, which means, all the records are immutable and verifiable. The term ledger is commonly used in the banking operations as it is the official record keeper used to verify data transactions over time. As the name implies, blockchain allows blocks of data to grow as new blocks are appended to it, with each block containing transaction information stored in a specially designed data storage structure. This enables the transactions in the Bitcoin network to function without any third party assistance, thus empowers it with the potential for building the future of internet systems.

Blockchain implements Asymmetric cryptography for user security and distributed consensus algorithms for ledger consistency. The key characteristics of blockchain technology are decentralization, persistency, anonymity and auditability, which results in reduced cost and improves efficiency [1] [2].

Decentralization avoids single point of failure (smart contract) [3].

Persistency or being immutable capacitates the transactions not to have tampered once it is loaded into the blockchain, thus can be used for applications that require high reliability and integrity. To give an example, consider the hash for “Welcome” is E923F17418D16, the hash for “Welcome” would be 751294185A8D2. The hash value depends on which hash technique is used.

Anonymity solved the trust problem between a node to node in blockchain technologies. The data transfer or even transaction can be anonymous, what is required to know is only the person's blockchain address.

Auditability, otherwise Public Verifiability is another key feature of the blockchain. Compared to a centralized system in which different observers may have different views of the system and the observers are compelled to trust the central authority for verification, blockchain allows anyone to verify the correctness of the state of the system. In this set up each of the state transition is confirmed by verifiers (e.g. miners in Bitcoin), which can be restricted set of participants as well [4]. The change in the state of the ledger according to the protocol can be verified by any observer and all observers will eventually have the same view of the ledger, at least up to a certain length.

A very significant plus of the blockchain technology is that it solves two of the most dreaded problems of currency based transactions, which have so long necessitated the requirement of a third party to validate the transactions. These are popularly known as the Byzantine Generals' Problem (BGP) and the Double Spend Problem.BGP is explained later in the paper [5]. Double Spend Problem is unique to digital currencies. The chance that digital currencies can be counterfeited and becomes worthless was a challenge. Bitcoin (BTC) is the first protocol to solve this. Characteristics of bitcoin as cited by Satoshi Nakamoto in the white paper "Bitcoin: A peer-to-peer electronic cash system" in 2008 can be condensed as[2]

- Enable direct transactions without the need for trusted third parties:
- Enable non-reversible transactions;
- Reduce credit cost in small casual transactions;
- Reduce transaction fees; and
- Prevent double-spending.

The largest impact or application is seen as a multitude of cryptocurrencies that have sprung up. Bitcoin(BTC), Bitcoin cash(BCC), Litecoin(LTC), Ethereum (ETH), Ethereum Classic (ETC), Dash (DASH), Ripple (XRP)[6]. With time blockchain has stretched its arms to other application areas than just the cryptocurrency domain. The advent, fame, and acceptance received by blockchain techniques will potentially transform the way in which digital systems establish, operate and manage. It is required to understand a variety of intricate problems and new requirements, which generate more open issues and challenges for research communities. Being known as the fifth disruptive innovation in computing, it is inevitable to know about the technology. This paper provides an insight on the block chain technology architecture, methodology as well as the major consensus algorithms, challenges and the application areas.

The paper is organized as follows, Section I contains the introduction to block chain technology and Bitcoin. Section II contain the related work of blockchain technology and taxonomy, Section III contain architecture, comparison of blockchain taxonomy and consensus algorithms, Section IV discuss results of blockchain technology in terms of challenges and major application areas, section V concludes the work with some future directions.

II. Related Work

Though blockchain is reasonably new technology, a lot of literature survey is available from various sources like websites, company 'Point of View's (PoVs), whitepapers published by various organizations implementing and experimenting in the blockchain. Conference proceedings, and journal articles are comparatively less.

Zibin et al. has discussed more about consensus, this paper explains different taxonomy also [2].

S.M. Nasti, S.J. Nasti, R.Bashir, M.A. Butt have done work on Bitcoin Mining [4].

Tschorsch et al. has done a technical survey on decentralized digital currencies including Bitcoin. Compared to [6], this paper focuses on blockchain technology instead of digital currencies [6].

III. Methodology

A. Blockchain Architecture

The blockchain is an ordered list of blocks, in which each block holds a complete list of transaction records similar to conventional public ledger. Figure 1 depicts a model of a blockchain. Each block in a blockchain is "chained" back to the previous block, as it contains a hash representation of the previous block. Such an arrangement aids historical transactions in the blockchain not be deleted or altered without invalidating the chain of hashes. This combined with further computational constraints makes blockchain immutable. The first block of a blockchain is called the *genesis block* which has no parent block. Internal details of an individual block are explained below.

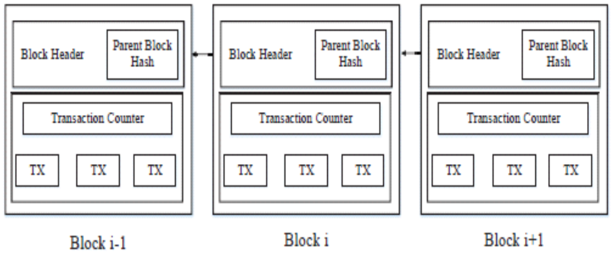


Figure 1. Blockchain model

Block

Each block consists of the block header and the block body as shown in Figure 2. In specific, the block header includes:

(i) Block version: 4-byte long version number that indicates the protocol version used by the node for block validation rules to be followed.

(ii) Merkle tree root hash: contains the hash value of all the transactions in the block.

(iii) Timestamp: stores the current time as seconds in the universal time since January 1, 1970.

(iv) nBits: target threshold of a valid block hash.

(v)Nonce: a 4-byte field that stores a random number which usually starts with 0 and increases for every hash calculation. Any change made to block data (like nonce) will change the entire block hash.

[2] https://bitcoin.org/bitcoin.pdf

(vi) Parent block hash: a 256 -bit hash value that points to the previous block.
The block body consists of a transaction counter and set of transactions. The maximum number of transactions a particular block can contain depends on the block size and the size of each transaction. Authentication and authorization of transactions in blockchain are ensured with the digital signature based on asymmetric cryptography. A brief notion on digital signature is given below.

B. *Digital Signature*

In asymmetric cryptography, each user has a pair of private key and public key. The private key is kept confidential and is used to sign the transactions. These digitally signed transactions are then broadcasted throughout the entire network. The typical digital signature involves two phases: signing phase and verification phase. For instance, consider a user Alice who wants to send a message to another user Bob. As mentioned above both Alice and Bob have their own public and private keys. (1) In the signing phase, Alice signs data with her private key and encrypts it with Bob's public key, and sends Bob the encrypted message. (2) In the verification phase, Bob decrypts the message and validates the value with Alice’s public key, so that Bob could easily check if the data has been tampered or not. The typical digital signature algorithm used in blockchain is the elliptic curve digital signature algorithm (ECDSA) [7].

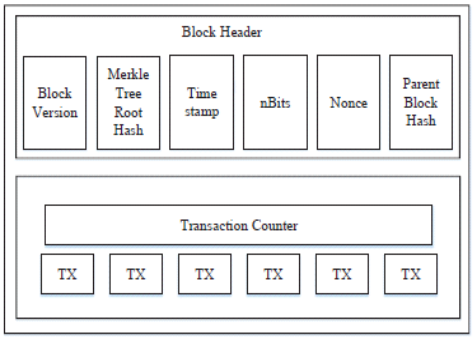


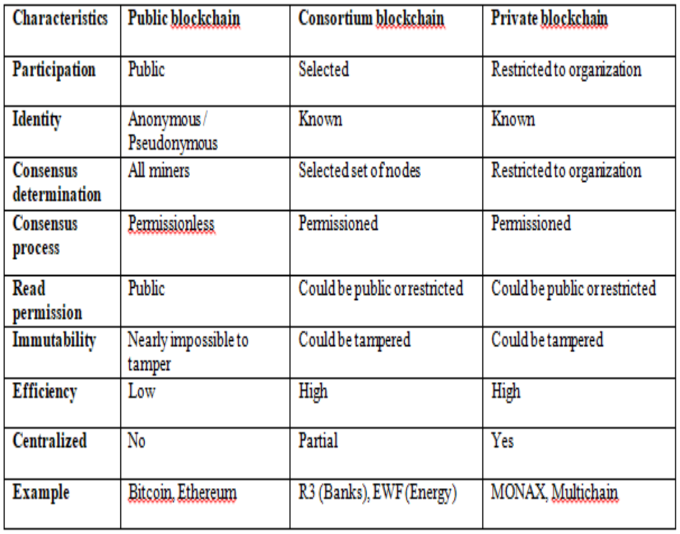
Figure 2. Single Block Structure

C. *Block chain taxonomy*

Based on who can access the blockchain network and how the permissions to write to the blockchain network are consigned, theoretically specifying four types of blockchains can be defined, Permissioned / permissionless Public blockchain, Permissioned / permissionless Private blockchain. A permissioned blockchain restricts the participants who can contribute to the consensus process, whereas a permissionless blockchain does not impose any such restrictions. In this paper, a broader classification of blockchain system is considered and they are of three types: public blockchain, private blockchain and consortium blockchain [8].

In public blockchain all records are public and participation in building a consensus and conducting mining is open to anyone. Proper authentication methods should be adopted in order to eliminate malicious participants. In consortium blockchain consensus are formed under the leadership of a specific group and therefore it is partially decentralized. Building a consensus is easier as participants are all identified. In private blockchain is used only within a specific organization. Building a consensus is quite easy as the mechanism is open only to the relevant organization.it is considered as a centralized network [9]. The comparison among the three types of blockchain is listed in Table 1.

Table 1. Comparison among Public, consortium, Private blockchain



Characteristics	Public blockchain	Consortium blockchain	Private blockchain
Participation	Public	Selected	Restricted to organization
Identity	Anonymous / Pseudonymous	Known	Known
Consensus determination	All miners	Selected set of nodes	Restricted to organization
Consensus process	Permissionless	Permissioned	Permissioned
Read permission	Public	Could be public or restricted	Could be public or restricted
Immutability	Nearly impossible to tamper	Could be tampered	Could be tampered
Efficiency	Low	High	High
Centralized	No	Partial	Yes
Example	Bitcoin, Ethereum	R3 (Banks), EWF (Energy)	MONAX, Multichain

Participation: Determines whether the actors involved are public or restricted.
Identity: Specifies whether participants are known or unknown.
Consensus determination: In public blockchain, all the nodes are allowed to take part in the consensus process. Whereas only a selected set of nodes are responsible for validating the block in consortium blockchain. And for a private chain, it is fully controlled by a particular organization and the organization could determine the final consensus.
Consensus process: Anyone in the world could join the consensus process of the public blockchain. Unlike public blockchain, both consortium blockchain and private blockchain are permissioned.
Read permission: Determines whether everyone can read transactions, which is true in a public blockchain while it depends when it comes to a private blockchain or a consortium blockchain.
Immutability: As public blockchain involves a large number of participants, it is nearly impossible to tamper transactions. Differently, transactions in a private blockchain or a

consortium blockchain could have tampered easily as there is only limited number of participants.
Efficiency: The time required to propagate transactions and blocks is more as there are a large number of nodes on public blockchain network. As a result, transaction throughput is limited and the latency is high. With fewer validators, consortium blockchain and private blockchain could be more efficient.
Centralized: The main difference between the three types of blockchains is that public blockchain is decentralized, consortium blockchain is partially centralized and private blockchain is fully centralized as it is controlled by a single group.
Example: The most popular implementation of the three types of block chains are mentioned.

Blocks are chained together through each block containing the hash of the previous block's header, thus forming the blockchain. If a previously published block were changed, it would have a different hash. This, in turn, would cause all subsequent blocks to also have different hashes since they include the hash of the previous block. This makes it possible to easily detect and reject any changes to previously published blocks. To comprehend the phases involved in the development of blockchain and how it expanded, advancements starting from bitcoin application is considered.

Stage 1: At this stage, the bitcoin blockchain operated as a ledger for the digital currency, bitcoins.

Stage 2: As Bitcoin was developed to be an open source software it acted as a base, and many alternate coins, by modifying various parameters and encryption algorithms, were evolved, from 2009 Bitcoin (BTC), till 2018 Bitcoin Private (BTCP) and still continue.

Stage 3: Various applications started to incorporate blockchain technology to manage assets such as transactions of goods and services, example real estate, automobile, concert coupons, etc.

Stage 4: As blockchain gained trust, the technology started to be used as records of rights in the form of applications guaranteeing the authenticity of the ownership or rights, not only that of transactions, for preserving documents and casting votes, etc.

Stage 5: With the improved capability to embed procedures, triggers, and other program logic, the blockchain technology has already entered the new phase of automation, example possibilities of escrow transactions, smart contracts, automatic processing by IoT devices, etc.

D. Consensus Algorithms

Before understanding consensus algorithm, it is better to know what consensus is and the reason behind using it. Consensus is the process of determining what blocks get added to the chain and what the current state is. Every blockchain follows consensus model that determine how the blocks are validated [9]. Any consensus model has three key elements, find something that:
1. is hard to do
2. is easy to verify
3. enforces a linear history
It is mandatory that every block must be signed, thus block validation becomes the hard thing to do. Once the cryptographic hash is generated it is easy to verify the hash. Blockchain itself enforces the linear history. As it is discussed in the above session blockchain are of different types. So first it is required to decide whether blockchain is permissionless/anonymous or permissioned.In permissionless blockchain, means anyone can participate in forming the chain of blocks, some proof that the validation of a block has been done and is correct is required. In a permissioned blockchain, the validators are known and therefore a proof is not necessary.

Miners are the peers of the blockchain that can validate the blocks in the blockchain. The procedure for validating is known as mining [11]. Every time a new block is added, miners compete with each other to be the first one to validate the block. Every miner can validate the new block and makes a hash. The one who wins this game, they will receive a small payment. In the Bitcoin blockchain whoever wins the validation, the game receives transaction fees and newly issued bitcoins. The number of bitcoins issued is determined by which block is validated. The further the block is in the blockchain the lesser number of new bitcoins one will receive. In the future, there will only be transaction fees.

In blockchain, how the untrustworthy nodes reach consensus among is a metamorphosis of the Byzantine Generals (BG) Problem, which was raised in 1982. In BG problem, a group of generals is leading different parts of Byzantine army. In order to seize the city, all the generals should collaborate and attack at the same time. To communicate the generals have one messenger. The real problem is that one or more generals can be traitors and can communicate misleading messages. However, the attack would fail if only part of the generals attacks the city. The generals need to find a feasible mechanism that allows them to safely seize a city even when traitorous generals are present. Translating this problem to distributed systems: generals are the nodes of the system, traitorous generals are the malicious nodes, and the messenger is the communication channel. How a consensus can be attained in a distributed environment is a challenge. The blockchain is distributed as there is no central node that ensures ledgers on distributed nodes are all the same. Protocols are required to ensure consistency of ledgers in different nodes. Castro and Liskov solved this problem in 1999 with their Practical Byzantine Fault Tolerance algorithm (PBFT) [12]. The first practical implementation was the consensus algorithm of bitcoin: Proof of Work. Several common approaches to reach a consensus in blockchain are discussed below.

E. General Approaches to consensus

PoW (Proof of work) is a consensus strategy used in the Bitcoin network [13]. In a decentralized network, it is easy to validate a block and generate a hash for a new block. In order to avoid rapid generation of new blocks, Bitcoin formulated two characteristics. Only one new block is issued in every 10 minutes and Bitcoin requires the miners to have a proof of work (PoW) means computer calculations. In PoW, each node of the network calculates a hash value of the block header. The nonce in the blockchain header will be changed frequently to obtain different hash values. The consensus requires that this calculated value must be equal to or smaller than a specific given value. Once the node reaches the target value, it would broadcast its block to other nodes and all other nodes must mutually confirm the correctness of the hash value. Other miners would add this validated block to their own blockchains. A lot of computer calculations in PoW, results in too much wastage of resources. Zerocoin is another cryptographic extension of Bitcoin [14]. This can be optimized by incorporating some side applications. An example is, Primecoin that searches for special prime number chains that can be used for mathematical research.

PoS (Proof of stake) is an energy-efficient and security-enhanced alternative to PoW. Blocks need to be generated by someone, which is chosen by Proof of stake algorithm. This algorithm selects the node based on the account balance of the holder in a belief that people with more currencies would be less likely to attack the network. This type of selection is unfair as the richest person would seem to be dominant in the network. The other alternatives are Blackcoin, uses randomization to predict the next generator, Peercoin favors coin age-based selection.

DPOS (Delegated Proof of Stake) Is representative democratic and is an improvement over standard PoS which is direct democratic. In this consensus process, stakeholders elect their delegates to generate and validate blocks. Thus with a fewer number of nodes, blocks and transactions can be confirmed quickly. Deputies can decide upon the block size and block intervals and dishonest stakeholders could be voted out.

PBFT (Practical byzantine fault tolerance) is a replication algorithm that could withstand byzantine faults. Byzantine fault is the scenario when different observers get different symptoms. A Byzantine failure is any kind of system service loss due to a byzantine fault. So PBFT requires every node to be known to all in the network. PBFT could tolerate up to 1/3 malicious byzantine replicas. The new block is determined in a round and the whole process is divided into three phases: pre-prepared, prepared and commit. Each round needs to select a primary based on some rules and it would be responsible for ordering the transaction. If a node has to enter the next phase it needs to acquire votes from 2/3 of all nodes.

Ripple is a consensus algorithm that uses variations of byzantine fault tolerance model, that forms trusted subnetworks within the larger network. Nodes are of two types: a server for participating consensus process and client for only transferring funds. Each server maintains a Unique Node List (UNL). Nodes in the UNL who have received 80% agreements, those transactions would be packed into the distributed ledger

IV. Results and Discussion

As the blockchain technology is becoming prevalent in multidisciplinary applications, flaws and challenges should be a matter of concern. Discussed below were the challenges that the technology itself has spawned and which has resulted in the business domain [15][16].

A. Challenges in terms of technologies

i. Consistency with the real world
ii. Correction of information
iii. Appropriate application of individual technologies that led disruption to existing industry practices
iv. Specific verification of the effects of cost reduction
v. Control security and protection

B. Challenges in terms of business

i. The necessity to ensure the link with transactions in the real world.
ii. Resource wastage
iii. Development of SLAs
iv. Standardization and governance activities for blockchain technologies
v. Clarification of the exchange rate with legal currency
vi. Anonymity, Protection of privacy, and the trade-off with identity verification

C. Applications

Finance and Taxation: Blockchain technology has its roots in finance and banking domain. Large varieties of Cryptocurrencies have been already in use. Other variations are in taxation, the key attributes of blockchain namely provenance, transparency and traceability meet the exact need of modern taxation schemes.

Insurance: A distributed network of multiple parties such as insurers, hospitals, funeral homes, a department of health and the beneficiary can form the nodes of the blockchain. This set up will speed up entire procedure involved and also helps to eliminate frauds.

E-Voting: The requirements of electronic voting such as anonymity, immutability, and public verifiability are suitable for incorporating blockchain technology.

Asset management: Accountability and security features of blockchain, makes it suitable for asset management including house, land registration, precious stone exchange and similar assets.

Smart Cities and IOT: Internet of things along with smart contracts can enable smart cities [17].

Smart contracts: Blockchain can be used as a distributed state machine without a trusted third party, thus the technology is well suited to support smart contracts

Healthcare: Healthcare sector is getting more and more digitalized over time as it aids in getting inter-medical services among countries. Medical data is diverse, vast and needs no alterations [18].Example, Healthcare Data Gateway (HDG).

Commercial distribution management: Blockchain based framework can be used for sharing resources across various services to ensure data immutability, accountability, proper asset utilization and to reduce transaction costs

Non-profit organizations: U.N.'s World Food Programme (WFP) and Bill & Melinda Gates Foundation aims to use blockchain technology in order to provide services faster and cheaper to improve basic amenities for needful people.

V. CONCLUSION AND FUTURE SCOPE

Blockchain technology is still in the phase of development. More research is being conducted in this field so as to overcome the challenges so as to even widespread its acceptance. In this paper, the key characteristics of blockchain technology are discussed. Later section explained the architecture, taxonomy and consensus algorithms. Then the paper discusses the challenges and major application areas of blockchain technology. The limitation of this paper is in not mentioning the advancements in consensus algorithms. Future scope for improvement is exploring more through the advanced consensus concepts and blockchain application trends.

REFERENCES

[1] M. Moser, “Anonymity of bitcoin transactions: An analysis of mixing services,” in Proceedings of Munster Bitcoin Conference, M¨unster, Germany, 2013, pp. 17–18.

[2] Zibin Zheng1, Shaoan Xie1, Hongning Dai2, Xiangping Chen4, and Huaimin Wang3,”An Overview of Blockchain Technology:Architecture,Consensus, and Future Trends”,IEEE 6th International Congress On Big Data, pp. 557-564.

[3] E. B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, “Zerocash: Decentralized anonymous payments from bitcoin,” in Proceedings of 2014 IEEE Symposium on Security and Privacy (SP),San Jose, CA, USA, pp. 459–474, 2014.

[4] S.M . Nasti, S.J. Nasti, R.Bashir, M.A. Butt, “Bitcoin:Surveying First RevolutionaryCryptographic Virtual Currency”, International Journal of Computer Sciences and Engineering, Vol.6, Issue.1, pp. 101-103, 2018.

[5] L. Lamport, R. Shostak, and M. Pease, “The byzantine generals problem,” ACM Transactions on Programming Languages and Systems (TOPLAS), vol. 4, no. 3, pp. 382–401, 1982.

[6] Tschorsch and B. Scheuermann. Bitcoin and beyond: A technical survey on decentralized digital currencies. IEEE Communications Surveys & Tutorials, 18(3):464, 2016.

[7] D. Johnson, A. Menezes, and S. Vanstone, “The elliptic curve digital signature algorithm (ecdsa),” International Journal of Information Security, vol. 1, no. 1, pp. 36–63, 2001.

[8] Xu et al. 2017. A Taxonomy of Blockchain-Based Systems for Architecture Design. 2017 IEEE International Conference on Software Architecture (ICSA), Gothenburg, Sweden, 3-7 April 2017.

[9] Crosby et.al. “BlockChain Technology: Beyond Bitcoin, Applied Innovation Review”, Issue No. 2, June 2016.

[10] D. Kraft, “Difficulty control for blockchain-based consensus systems,” Peer-to-Peer Networking and Applications, vol. 9, no. 2, pp. 397–413, 2016.

[11] C. Decker, R. Wattenhofer, Information propagation in the Bitcoin network. In: Peer-to-Peer Computing (P2P), IEEE Thirteenth International Conference on; p. 1–10,2013.

[12] C. Miguel and L. Barbara, “Practical byzantine fault tolerance,” in Proceedings of the Third Symposium on Operating Systems Design and Implementation, vol. 99, New Orleans, USA, pp. 173–186, 1999.

[13] Peters G.W. Panayi E. 2016. Understanding Modern Banking Ledgers Through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money , Banking Beyond Banks and Money, Springer Sep 2016, pp. 239-278.

[14] I. Miers, C. Garman, M. Green, and A. D. Rubin, “Zerocoin: Anonymous distributed e-cash from bitcoin,” in Proceedings of IEEE Symposium Security and Privacy (SP), Berkeley, CA, USA, 2013, pp. 397–411.

[15] D.Vandervort “Challenges and Opportunities Associated with a Bitcoin-Based Transaction Rating System” vol. 8438. Springer Berlin; Heidelberg; p. 33–42. 2014.

[16] Zheng, Zibin & Xie, Shaoan & Dai, Hong-Ning & Chen, Xiangping & Wang, Huaimin, “Blockchain Challenges and Opportunities: A Survey, International Journal of Web and Grid Services”, 2017.

[17] Sun et.al. 2016. Blockchain-based sharing services What blockchain technology can contribute to smart cities, Springer

[18] Gurpreet kaur, Manreet Sohal, “IOT Survey: The Phase Changer in Healthcare Industry”, International Journal of Scientific research in Network security and Communication, Vol.6, Issue.2, 34-39, 2018.

Authors Profile

Mrs Tinu N.S pursed Bachelor of Technology from Adi Shankara College of Engineering Kalady in 2009, from Mahatma Gandhi University and Master of Technology from Rajagiri School of Engineering in year 2012. She is currently working as an Assistant Professor in Department of Computer Science since 2013. She has 6 years of teaching experience.