International Journal of Healthcare Information Systems and Informatics
Volume 16 • Issue 2 • April-June 2021

Blockchain:
The Perspective Future of Technology

Riya Sapra, Manav Rachna University, Faridabad, India
Parneeta Dhaliwal, Manav Rachna University, Faridabad, India

ABSTRACT

Many applications are being built using the immutability and robustness of blockchain. Blockchain is a new class of information technology that combines cryptography and a distributed ledger that already exists. The model is composed of a group of computers that collaborate towards maintaining a secured database without storing the data at any central unit. It is the technology behind all the crypto currencies like Bitcoin, Litecoin, Ethereum, and now finding its way to record everything possible. This paper focuses on the basic framework of blockchain model, its pre-requisites, and challenges of blockchain. Various current real-time applications of the technology are also discussed. Finally, an application area has been proposed that can be used to create a huge database of the citizens of the country and facilitate them with ease of access to their personal data. It will open new ways of data analysis at a nationwide scale.

KEYWORDS

Applications, Bitcoin, Blockchain, Challenges, Consensus, Distributed Ledger, Merkle Root, Pre-Requisites

INTRODUCTION

Blockchain has become a buzzword in IT sector. The technology behind blockchain has become so powerful that applications are being built on top of it, making them decentralized, block based and resistant to censorship. The increasing number of people handling bitcoin digital currency has resulted in launch of various new initiatives based on blockchain principle. Bitcoin is a digital money ecosystem where users transfer bitcoins for buying or selling of goods (Nakamoto, 2008). Unlike traditional currencies, bitcoins are entirely virtual i.e. no physical coins. The digital coins only signify a transfer value from a sender to a receiver (Antonopoulos, 2014). Various other cryptocurrencies came to market after the success of Bitcoin. Success of bitcoin that were based on blockchain, providing highly robust and secure system is being adopted widely by both academia and industry facilitating enterprises, healthcare market, manufacturing industries and much more.

Apart from cryptocurrencies, blockchain is being implemented in a variety of application areas because of its robustness and data security features. In the field of Internet of Things, blockchain can be used for providing security and privacy to the users for their data within the network (Khan & Salah, 2018). In the area of Big Data, blockchain can be used in increasing data security and improving the quality of data (Azaria et al., 2016). Blockchain is also being used in machine learning, to create smart contracts for trustless machine learning (Kurtulmus & Daniel, 2018). Also in the area of Cloud Computing, blockchain is used to provide user privacy and data security (Park & Park, 2017). For data security, blockchain is also used in the area of fog computing and edge computing (Tuli et al., 2019).

DOI: 10.4018/IJHISI.20210401.oa1

Our Contributions

The main objective of the article is to define the concepts of blockchain technology and to highlight the huge number of real time applications available. The major contributions of our work include detailed understanding of Blockchain technology and describing the underlying concepts. We identified the pre-requisites and challenges involved in adopting blockchain technology. Also, new application areas have been proposed where blockchain technology is being adopted. Finally a novel blockchain system BirthChain, has been proposed for automating the process of generating Birth certificates by the government body and hospitals which will ease the work flow and reduce parent's hassle. This article will be highly beneficial for the academicians, the researchers and the people from industry who want to start working in the area of Blockchain. They can incorporate blockchain technology in various new application areas that have been identified. The proposed system will motivate the readers and give them a direction to use blockchain technology in their application domains.

Organization of the Paper

The structure of the paper is as follows. The current section describes in detail the blockchain architecture and its features. The types of nodes and various categories of blockchain are also discussed in this section. The working of blockchain and various other important concepts like smart contract, consensus protocol etc. are also explained to provide better understanding of the technology. The authors have also identified various pre-requisites and challenges involved in adopting the technology. In Background section, the detailed literature of the various consensus protocols and other application based techniques of blockchain are discussed. The article also lists the various applications areas where blockchain has been implemented and projected some novel areas that can be benefited from the technology. A new application area to automate the process of generation of birth certificate has been proposed along with detailed step wise implementation of blockchain. In the end, the article is concluded along with the scope of future work.

Blockchain Architecture

Blockchain is a chain of blocks which include all the valid transactions happening in the chronological order to be maintained in public ledgers, secured by hashes and validated through distributed consensus (Sapra & Dhaliwal, 2018). The technology behind blockchain works by maintaining the transaction ledger with all the members in the blockchain. Whenever there is a new transaction, the transaction ledger is updated without any involvement of third party. Transaction may denote a transfer of financial value as in case of cryptocurrencies like Bitcoin, Dodgecoin (Antonopoulos, 2014), Litecoin (Swan, 2015) etc. or execution of an arbitrary code as in case of Ethereum (Buterin, 2014) blockchain or data transfer from one device to another device in IBM ADEPT (Makhdoom et al., 2018).

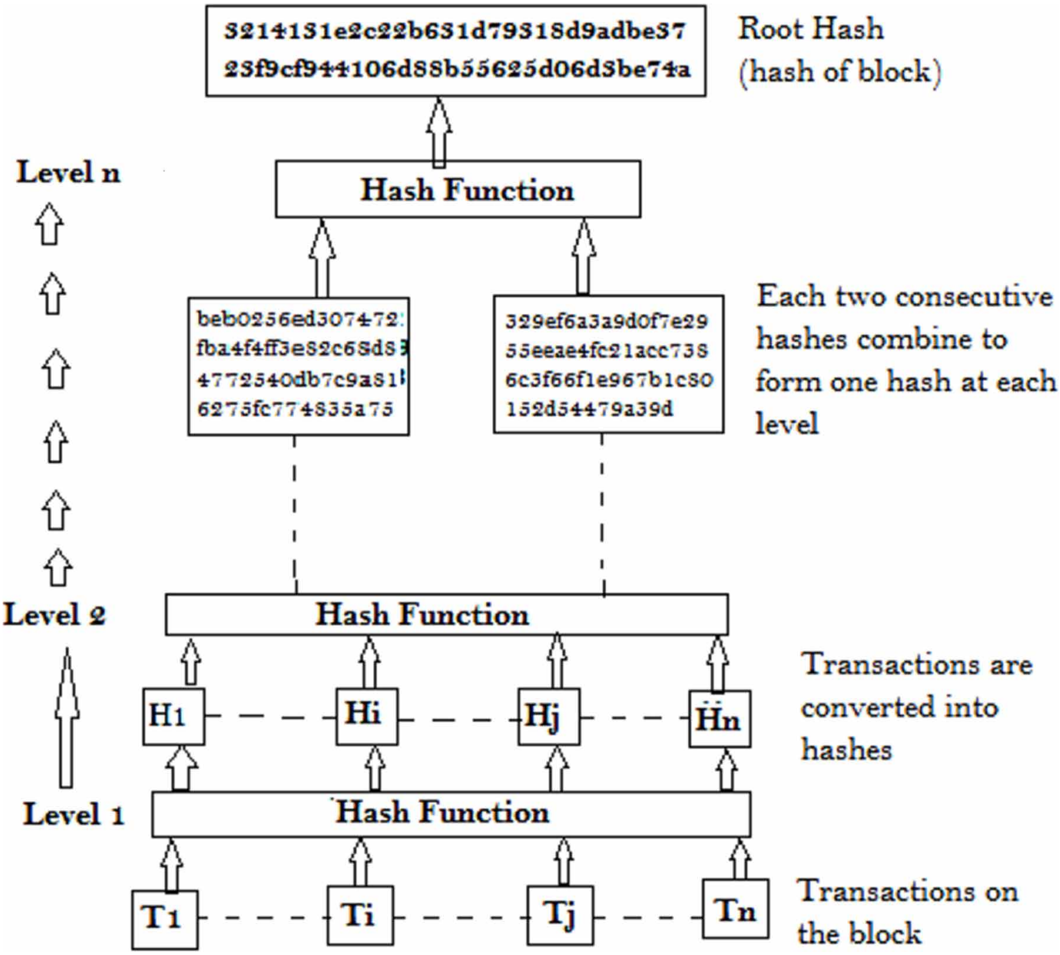
Ledger is a book or a computer file for recording and totaling all economic transactions as debit/credit transactions, a starting and ending monetary balance for each account as shown in Table 1 (Hamida et al., 2017). Blockchain ledger is decentralized so it does not have to rely on the centralized server (Lin & Liao, 2017). It is replicated to many network participants, who collaborate in its maintenance. Also the information in blockchain is append-only, which guarantees that if a transaction is added to the ledger, no one can modify it (Niranjanamurthy et al., 2018).

Each block is represented by a hash value called the merkle root of the block as shown in Figure 1 (Nakamoto, 2008). The root hash is evaluated by converting all the transactions into a hash value using a hash function. The hash function takes any length string as input and provides a unique fixed length output known as hash of that transaction (Singh &Singh, 2016). For example if we have 4 transactions in a block, at Level 1, every transaction will be converted into its unique hash. For level 2 to level n-1, two hashes will be converted into one unique hash and so on till we get one single hash for all the transactions in the block as shown in Figure 1.

Table 1. Ledger

Ledger				
Date	**Description**	**Debit**	**Credit**	**Balance**
11-Aug-19	Balance Forwarded			3,00,000
11-Aug-19	Goods Purchased	1,00,000		2,00,000
12-Aug-19	Machinery Purchased	50,000		1,50,000
13-Aug-19	Goods Sold		80,000	2,30,000
14-Aug-19	Travelling Expense	10,000		2,20,000
15-Aug-19	Goods Sold		30,000	2,50,000

Figure 1. Merkle root evaluation

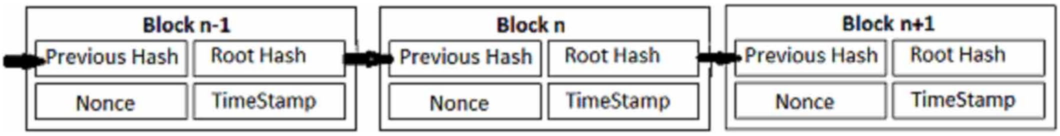


Each block stores its own root hash, nonce, timestamp and hash of previous block as shown in Figure 2 (Nakamoto, 2008). Nonce is a unique random number in every block which is used as an authentication protocol so that no old transactions are redone. The timestamp is the time when block is created (Niranjanamurthy et al., 2018). The blocks in blockchain are connected via hashes to form a chain. If anyone attempts to tamper any transaction in the block, its hash will change and so will the root hash. This will make the blockchain invalid and hence the changes will be reversed using the valid blockchain available on the network.

The decentralized and immutable behavior of blockchain makes it suitable for many applications like supply chain (Brown, 2018), financial trading (Zhao et al., 2016), banking (Singh & Singh, 2016), cross border payments (Olleros & Zhegu, 2016), health care (Rouhani et al., 2017) and many more.

Features of Blockchain

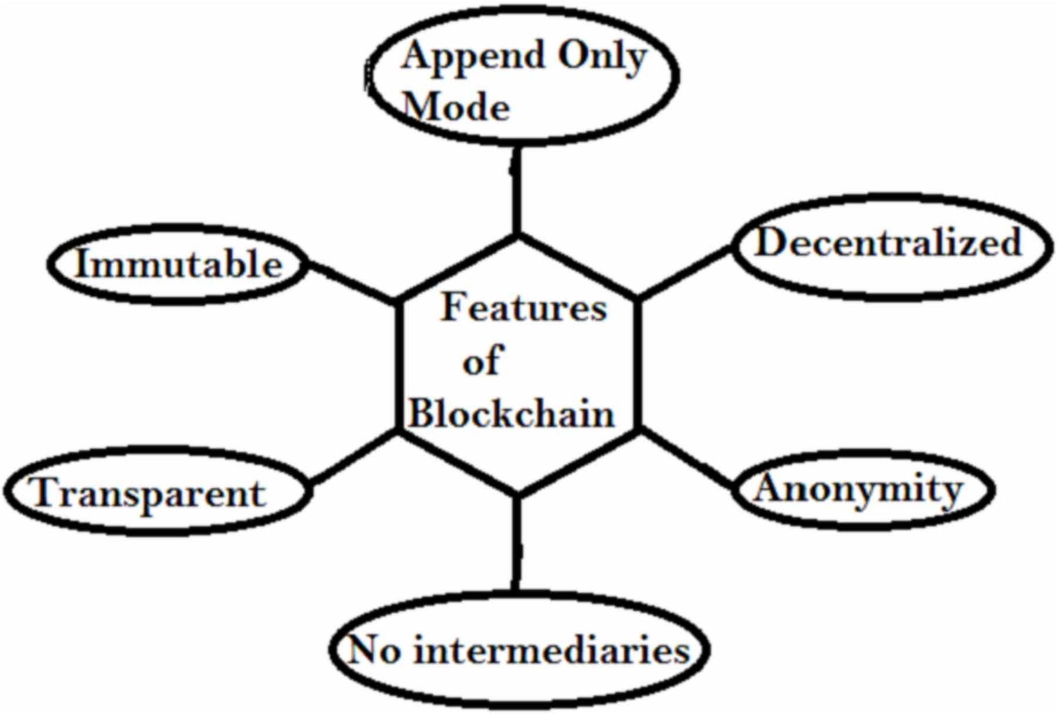
Figure 2. Blockchain architecture



The blockchain is an emerging technology being adopted by both private and government organizations. The technology and concepts behind blockchain make it apt for data storage, financial transactions, secure data transfer, copyright management etc. Figure 3 gives some of the key features of blockchain.

- **Append Only Mode**: Blockchain only allows appending of transactions or blocks as every block and transaction is time stamped and ordered according to time. Due to append only behavior of blockchain, the transaction once written on blockchain cannot be edited or manipulated.
- **Decentralized**: In blockchain, the nodes works in decentralized fashion. All the full nodes and miner nodes have the complete copy of the blockchain. Any attacker cannot successfully manipulate a transaction or block as the correct copy of the blockchain will be available with other nodes and no node will validate the malicious transaction. This will result in failure of propagation of malicious transaction or block.
- **Immutable**: Transactions in blockchain cannot be altered in any way as transactions are just appended to the block with time stamping mentioned for every transaction. This makes blockchain immutable and secure for sensitive data and transactions also.
- **Transparent**: In blockchain, the transactions happening are publically visible by all the parties which make blockchain transparent. Also in public blockchain anyone can join the network and participate in blockchain mining. This adds to the transparency of blockchain.
- **Anonymity:** The identity of the user is hidden in blockchain as every node is represented by an address generated using cryptographic function using the public key of the node called its Blockchain address. This brings in privacy and user anonymity to blockchain.
- **No Intermediaries**: The working of blockchain brings trust to the network as every transaction before getting committed is verified by a number of nodes. So there is no requirement of any third party like banks, lawyers to validate the transaction.

Figure 3. Features of Blockchain



Working of Blockchain

Blockchain is a decentralized peer to peer network where anyone in the trustless network can communicate or do business with another without involvement of any third party. Any communication or financial transfer is a transaction in blockchain. Figure 4 shows the detailed working of blockchain.

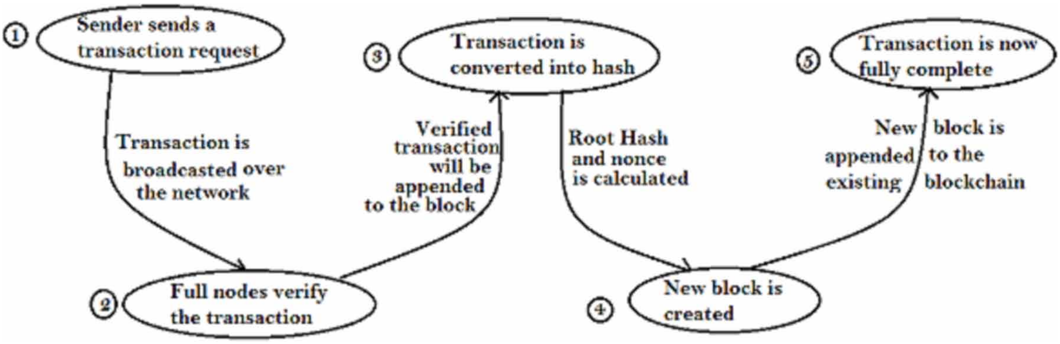
For any transaction, sender initiates a transaction request after signing his/her digital signature within the transaction (Nakamoto, 2008). This requested transaction gets broadcasted to the peer to peer network of computers, also known as nodes. The nodes (full nodes) of network validate the transaction by verifying whether the sender is eligible for the transaction or not. The verified transaction is then linked or appended to previous transactions. After specified interval or specified number of transactions, the verified transactions are used to create a new block. In the new block all the transactions are converted into hashes using a hash algorithm based on the consensus protocol (Nguyen, 2018). The hashes of all the transactions combine to evaluate the root hash of the block. Nonce for the block is computed by the miner node by solving the difficult puzzle of the consensus protocol. The new block gets appended to the existing blockchain connected via previous block root hash. The transaction is now finally complete. The transactions become valid only after it is added to blockchain.

Types of Nodes in Blockchain

In blockchain, the users/peers are generally classified in three categories according to their computing capability and tasks assigned:

- **Simple Node:** These nodes neither store the complete copy of the blockchain nor mine the block. They can only send or receive transactions.

Figure 4. Working of blockchain


① Sender sends a transaction request
Transaction is broadcasted over the network
② Full nodes verify the transaction
Verified transaction will be appended to the block
③ Transaction is converted into hash
Root Hash and nonce is calculated
④ New block is created
New block is appended to the existing blockchain
⑤ Transaction is now fully complete

- **Full Node:** The complete copy of blockchain is maintained by a full node. It validates the transactions and propagates them. It checks for the malicious transactions in the network and stops it from routing. These nodes don't mine the block but are essential for the security of blockchain.
- **Miner Node:** These are the full nodes of blockchain with the additional capability of mining the blocks and adding them to the blockchain. These nodes are selected on the basis of consensus protocol (Nguyen, 2018) used for the blockchain.

Consensus Protocol

In blockchain, all the transactions are propagated within the network before being added to the new block. These transactions are validated by full nodes. Miner nodes add these validated transactions to a new block using an algorithm called consensus protocol. Moreover, all the work is done in a decentralized scenario, a mechanism needs to be followed such that every node in the network has the same and correct copy of the blockchain. Proof of Work (PoW) (Nakamoto, 2008) is the first consensus protocol which originated the concept of blockchain. Various consensus algorithms have been proposed for improved efficiency and better performance. Details of these algorithms will be discussed in the background.

Smart Contract

Smart contract is a new version of blockchain (Makhdoom et al., 2018). It is a computer program with set of rules encoded in it. These programs run on blockchain and can execute transactions like automatic financial transfers on certain events or data transfer after authentication. The major application areas include mortgage loans (Kosba et al., 2016), supply chain management (Olleros & Zhegu, 2016), insurance (Niranjanamurthy et al., 2018), protecting copyrighted content (Buterin, 2014), online voting (Buterin, 2014) etc. Smart contract is represented by an address whose code resides on blockchain. These contracts are invoked by sending transactions to the address of contract. Smart contracts are also called DApps (Decentralized Applications) as they are deployed on blockchain. Ethereum (Buterin, 2014), Rootstock (Lerner, 2015), CounterParty (Christidis & Devetsikiotis, 2016) are some of the popular smart contract platforms.

Types of Blockchain

Blockchain can be categorized either on the basis of mining rights or access rights of the nodes present in blockchain. Figure 5 shows the different types of blockchain. The main task of miner nodes involved in the blockchain network is to mine the block i.e. create a new block that includes all the verified transactions happening in the blockchain. This block is then be appended to the existing blockchain network. According to the mining rights i.e. how the miner node of the network is selected, two types of blockchain exist:

- **Permissioned Blockchain:** In permissioned blockchain, miner nodes are selected for mining of block. Anyone without permission cannot mine the block. There can be different ways of selecting the miner. For Example: PoS (Lin & Liao, 2017) selects miner on the basis of stake the miner has whereas PoET (Chen, 2017) uses lottery for selecting the miner.
- **Permissionless Blockchain:** Permissionless blockchains are open to all. Anyone can join the network, validate the transaction and mine the block. Bitcoin (Nakamoto, 2008) and Ethereum (Buterin, 2014) are permissionless blockchains.

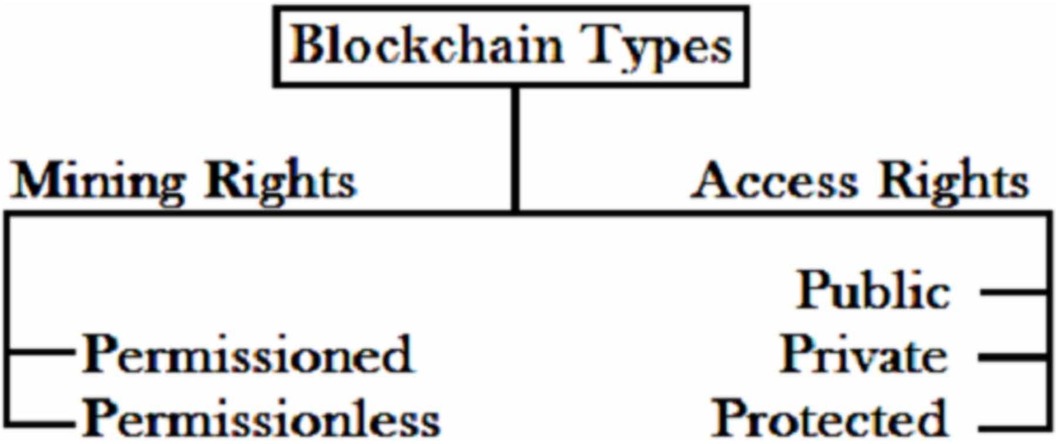
Categorization of blockchain can also be done on the basis of permission of joining the network, reading or writing the transactions. There are blockchains in which anyone can join or leave the network e.g. Cryptocurrencies. In other blockchain, there might restriction/permissions associated with joining or leaving the network. Also every blockchain network defines who is allowed to read and do the transactions. According to these access rights, three types of blockchain are:

- **Public Blockchain:** In public blockchain such as Bitcoin (Nakamoto, 2008), Dash (Duffield & Diaz, 2015), Ethereum (Buterin, 2014) transactions are transparent. Anyone can execute transactions via network and can read the transaction on public block explorer (Singh & Singh, 2016). Hence the transactions can be audited by anyone. These blockchains (Lin & Liao, 2017) are preferable in cryptocurrencies.
- **Federated or Consortium Blockchains:** Consortium Blockchains (Sheetal & Venkatesh, 2018) are partly decentralized blockchain as they don't allow anyone to participate in the verification of transactions. They are faster, provide better transaction privacy and have higher scalability as compared to public blockchain. These blockchains are preferable in the banking sector. Corda (Brown, 2018) is a partly decentralized federated blockchain.
- **Private Blockchain**: In private blockchains such as Ripple (Olleros & Zhegu, 2016), write permissions are only meant for an individual or an organization and read permissions may be public or restricted to few authorized persons. Private or permissioned (Niranjanamurthy et al., 2018) blockchains provides different access rights to people in the same network for providing privacy of data. This makes it useful for collecting, storing or sharing of sensitive information, auditing, database management etc.

Pre-Requisites of Blockchain

- **Transaction Verification and Validity Checking:** Whenever someone is doing a transaction, there must be a protocol for commitment of transaction so that the transaction is fully committed or discarded. The Proof of Work (PoW) (Nakamoto, 2008) or Proof of Stake (PoS) (Lin & Liao, 2017) algorithms are needed to create blocks of transactions by verifying by legitimacy of transactions.
- **Consistency Maintenance:** As all the nodes on the network holds a copy of public ledger, the consistency of the data needs to be maintained. Consensus algorithm (Sheetal & Venkatesh, 2018) is required so that an identical and updated copy of the data is maintained.
- **Security and Integrity of Data:** Data distributed in public ledgers cannot be hacked or manipulated as it is append-only data. In case of permissioned Blockchain, methods need to be designed for accessing the sensitive data by only authorized users of the Blockchain.
- **Hashing Algorithm:** Transactions in Blockchain are stored as hash values. Various hashing algorithms like Secure Hash Algorithm (SHA) -256 (Zyskind et al., 2015), SHA-1 (Rouhani

Figure 5. Types of bl ockchain



et al., 2017), The Algorithm X11(Duffield & Diaz, 2015), Scrypt (Fernandez & Fraga-Lamas, 2018) should be used to hash the transactions of Blockchain.

- **Decentralized Network:** One of amazing feature of blockchain is decentralization of the data which secures it from any single point of failure. Decentralization brings designing of lots of rules and protocols for information exchange and update. These protocols should be defined and tested before implementation.
- **No Double Spending:** Double spending is using the same digital money in more than one transaction. The risk of double spending is very common in digital currencies. Protocols need to be defined for the verification and authentication of each transaction and digital currency used.

Challenges

Decentralization brings a lot of challenges. As there is no central authority so every participating node needs to process every transaction, maintain a copy of the system and update it as and when required.

- **Storage:** All the data in blockchain needs to be stored on every participating node in the network, there is high requirement of data storage and as the size of block or blockchain grows, storage requirement will increase many folds. Various storage optimization techniques need to be devised for handling this issue.
- **Processing Speed:** All the transactions are happening in real time and need to be updated at every node. Moreover as users of blockchain increases, the number of transaction per second will increase, resulting in requirement of high processing speed.
- **Security:** Blockchain has a 51% attack problem (Pinno et al., 2018). If someone has a control of 51% of the block, he/she will be able to manipulate the block. This problem needs to be addressed.
- **Scalability:** As the size of blockchain increases, storage requirements may increase many folds. Faster computations and higher power will be required.
- **Environment Impact:** To run blockchain, high amount of electricity is required. Environmental friendly means need to be designed to cater the high power demand of blockchain.

BACKGROUND

The concepts of distributed computing, public ledgers, cryptography are decades old but blockchain gained popularity just recently after the release of Bitcoin (Nakamoto, 2008). In blockchain no one is allowed to change the previous transaction which makes it immutable. This feature of time stamping every transaction came from the concept of time stamping digital documents so that no user can back-date or forward-date the document (Haber & Stornetta, 1990). This helps identify the user making changes in the shared document. Also the transactions are digitally signed by the sender as a purpose of verification of the transaction. Digital signature along with the transaction helps in non-repudiation (Niranjanamurthy et al., 2018) of any transaction. This brings trust in the network. The first consensus algorithm was designed on the principle of digital time stamping the document with the introduction of nonce, block size, nodes, miners etc. The literature of blockchain technology can be studied in two aspects: blockchain's consensus algorithms and blockchain's applications/techniques. Various consensus protocols have been proposed to meet the requirement of different applications. The details of these applications/techniques and the consensus protocols are defined below.

Consensus Protocol

Working of blockchain is defined by the consensus algorithm used for the blockchain. Various consensus protocols have been proposed by different authors. A comparison study of these algorithms is given in Table 2.The first consensus protocol Proof of Work (PoW) (Nakamoto, 2008) requires the miners to find the value of nonce by solving a tough puzzle with certain level of difficulty. The difficulty is updated after every 2016 block. Average speed of adding new block in PoW is approximately a block every 10 minutes. PoW uses SHA-256 (Zyskind et al., 2015) algorithm as their hash function. PoW requires a lot of computation power and specialized hardware for solving the puzzle.

A variant of PoW is proposed which uses Cuckoo hash function (Tromp, 2004) in place of puzzle work. It resolves the limitation of PoW as it requires fewer efforts than PoW to create a new block. In this variant, a hash table with two different hash functions is used to create a graph and multiple nonces to be broadcasted as a block. Another variant of PoW proposes miners to find the longest chain of primes (Nguyen, 2018) instead of finding nonces. The chain of primes must be larger than a given value and should be like a Cunningham chain (King, 2013). Primecoin (King, 2013) uses this variant of PoW as its consensus protocol. PoW has a high transaction latency of around 10 minutes i.e. a transaction will be confirmed only after the creation of the block. To combat this, Bitcoin-NG (Next Generation) (Eyal et al., 2016) was proposed to separate the block into micro block and key block. When a miner (leader) finds a nonce, he/she can broadcast the key block and till the time another miner broadcast the next key block, he (leader) can publish micro blocks. The transactions will be verified quicker with micro blocks and hence transactional latency is reduced.

PoS (Proof of Stake) (King & Nadal, 2012) is another popular consensus algorithm which does not require powerful machines to find the nonce for the block. It uses the concept of staking their coins for win the chance of mining the block. Miner with more stakes will be more trustful as he/she would not want anyone to attack the blockchain. Nextcoin (Li et al., 2017) uses pure PoS for mining of blocks.

A variant (Bentov et al., 2016) of PoS chooses miner on the basis of the state of the block. It uses a procedure called follow-the Santoshi to find Santoshi index and Santoshi value. This Santoshi value will act as a reward for the miner of the new block. Another variant of PoS elects leader (miner) randomly by calculating an entropy value (Kiayias et al., 2017) which is secure enough and difficult to predict so that no manipulation is possible in leader election. Another variant of PoS called Delegated Proof of Stake (DPoS) (Larimer, 2014) uses stake as well as voting of delegates to get the chance of mining. For high stake, more number of delegates needs to be produced. Also the list of delegates is always shuffled.

Proof of Activity (Bentov et al., 2014) combines the approaches of PoW and PoS to combat the double spending (Niranjanamurthy et al., 2018) problem of blockchain. In this algorithm, a block with initially no transaction but a suitable nonce is created. A pool of nodes with their respective stake is also created. N nodes are selected randomly and the last node will be selected to mine the block i.e. add transactions to the block.

In Proof of Born (PoB) (P4Titan, 2014) consensus the miners needs to send their coins to an unspendable address in order to burn them i.e. these coins cannot be used then. Miner with highest number of the coins burnt will get the chance to mine the block. In Proof of Space (PoS) (Dziembowski et al., 2015) miners

needs to invest in hard disks. Investing in hard disk is less expensive as compared to PoW's high computing power devices. In this consensus algorithm the miner is supposed to create large datasets on hard disk called as plots. Higher the plots more are the chances of miner to be selected for mining the block.

Proof of Elapsed Time (PoET) (Chen,2017) has been proposed by Intel for their blockchain platform Sawtooth Lake (Nasir, 2018). This algorithm works in TEE (Trusted Execution Environment) on Intel's XGS (Software Guard Extension). All the miners send a request for a wait-time to the trusted function of XGS hardware. The miner receiving shortest wait time will get the chance to mine the block. Another consensus protocol Proof of Luck (PoL) (Milutinovic et al., 2016) also requires XGS and TEE for its execution. Each miner creates a new block to be appended to his/her current chain. A lucky number in the range 0 to 1 is assigned to each new block. Chain with the largest lucky value will be selected as the main chain.

In Practical Byzantine fault Tolerance (PBFT) (Castro & Liskov, 1999) a leader node is selected from the miner nodes. Simple nodes also called clients requests transactions, full nodes validates them and after the threshold number of transactions, the leader order them and creates block. This block is then broadcasted and peers store them locally. To double-check the correctness of block, it is broadcasted again to all the peers.

Other Methodologies/Techniques

Bitcoin is the first implementation of the concept of blockchain (Nakamoto, 2008). It is a cryptocurrency which uses PoW to bring consensus in the network. It brought revolution to way of doing financial transactions. Various cryptocurrencies originated after the rise of Bitcoin. Litecoin is identical cryptocurrency to Bitcoin (Swan, 2015). The consensus protocol used by Litecoin has better storage and reduced transaction confirmation time. Ethereum is another cryptocurrency which later became the first blockchain platform to include smart contracts (Buterin, 2014). In the beginning Ethereum used PoW as its consensus protocol but later shifted to PoS in order to reduce the power consumption.

Hyperledger is a blockchain specifically designed for companies to allow them to deploy their components according to their needs (Nasir, 2018). Quorum is a permissioned private blockchain meant for privacy of sensitive data by using cryptography on Ethereum platform (Chase, 2016). Rockchain is another Ethereum based platform for preserving data privacy by using distributed file system for the data-centric approach through smart contracts (Chase, 2016).

(Azaria et al., 2016) proposed MedRec, a novel and decentralized record management system which uses blockchain to handle electronic medical records (EMRs). It provides the patients a comprehensive and immutable log of medical records with an easy access to the treatment sites. Through blockchain, MedRec manages the confidentiality and authenticity of the information.

(Singh & Singh, 2016) proposed Sia, a blockchain based decentralized cloud storage system where various peers rent their storage spaces. It provides agreements/smart contracts between the clients and storage provider by using Bitcoin protocol.

(Kosba et al., 2016) proposed Hawk, as a decentralized system for smart contracts to retain transactional privacy by designing a compiler which automatically implements cryptography on the smart contract written by the programmer The contractual parties interact with each other using cryptographic primitives like zero-knowledge proofs and thereby defining a formal model for applications design atop decentralized blockchains (Feige et al., 1988).

Table 2. Comparison study of consensus protocols of blockchain

Algorithm	Description	Application	Limitation
PoW (Proof of Work)	Miners compute cryptographic hash with some level of difficulty called nonce	Bitcoin, Litecoin, Dogecoin	Slow throughput, High computation, High energy demand
PoS (Proof of Stake)	People stake their tokens to bet on which blocks are valid.	VCash, BitBay, Peercoin, Qtum	Blockchain Forks
DPoS (Delegated Proof of Stake)	Token holders elect delegates to do validation.21–100 elected delegates are shuffled periodically to deliver the block.	EOS, BitShares	Partially centralized
PoA (Proof of Authority)	Authorities are assigned a fixed time slot for block generation	Parity	High degree of centralization
PoET (Proof of Elapsed Time)	Lottery based protocol to select miner on the basis of least waiting time.	HyperLedger Sawtooth	Need specialized hardware
PoB (Proof of Burn)	Miners send coins to an unspendable address to be eligible for mining. Has no energy cost	Slimcoin	High risk. Rich get richer
PoS (Proof of Space)	Miner creates large datasets called plots on big hard disks. Higher the number of plots, higher is the chance of node getting selected as miner.	Burstcoin Spacemint Chia	Huge sized hard disk are required
Proof of Activity	Combines PoW and PoS. A block with a nonce but no transaction is created. N nodes will be chosen randomly. The last one will add transactions to the block.	Decred, Espers	Heavy resource utilization
Proof of Luck	All miner nodes make their own block. A number is assigned to every block. The chain with largest total value will be the accepted blockchain.	Luck	Need specialized hardware
Practical Byzantine Fault Tolerance (PBFT)	After a block is created, it is double checked that all the nodes have appended the same block.	Hyperledger Fabric	Partially centralized

(Yli-Huumo et al., 2016) explained the technical perspective of challenges, features and future directions of blockchain technology. It provided review of various research papers to define the current scenario and applicability of blockchain in industry and academia.

(Rouhani et al., 2017) used blockchain to build Medichain, as a decentralized platform for managing and controlling personal data like medical records. A mobile application provides fine grained access control to the user to monitor how and where its data is used. The access rights are stored in blockchain and users can alter the permissions any time.

(Yuan et al., 2017) used an aggregate signature for blockchain transactions to improve security of the transactions by hiding the amount involved in it. The proposed scheme also improves the performance as the size of signature every time remains constant for any amount of transaction. This scenario is implemented in blockchain based transactions on Big data to check the performance of transaction for privacy preserving behavior.

(Seebacher & Schüritz, 2017) provided extensive literature review of various peer reviewed article of blockchain technology. It defined the various characteristics of blockchain and how they are influencing industry and academia.

Blockchain is being used effectively for storing and exchanging information over internet. (Meng et al., 2018) gave a design scheme for securing copyright information is proposed by integrating blockchain with digital watermarking, perceptual hash function, Inter Planetary File System (IPFS) and Quick Response (QR) code. A peer to peer network is used to integrate copyright management and its distribution without the need of any centralized authority.

(Yakubov et al., 2018) defined blockchain technology to build secure public key infrastructure (PKI) systems to replace certificate authorities for issuing, validating and cancelling X.509 certificates. Ethereum smart contracts and restful services are used to provide verification of digital certificates issued (Buterin, 2014).

(Jain et al., 2018) defined a scheme to store sensitive data in blockchain as it prevents unauthorized access and make data tamper-proof by using secured cryptographic algorithms like Secure Hash Algorithm (Rouhani et al., 2017), Scrypt (Fernandez & Fraga-Lamas, 2018).

(Li et al., 2018) proposed an energy blockchain for the security of energy trading system. It proposes a credit-based payment system for fast energy trading to be used in P2P energy eliminating the need of any trusted intermediary.

(Partala, 2018) used Blockchain Covert Channel (BLOCCE) for covert communication. Covert communication channels are used in military communication or in authoritarian government for secret communications. Covert messages are securely embedded to the blockchain using steganography and cryptography.

(Pinno et al., 2018) proposed ControlChain, a blockchain-based architecture for managing IoT access authorizations. The proposed architecture is fully decentralized, fault tolerant, user transparent, scalable, user friendly and compatible with a many access control models of IoT. It establishes a secure relationship between a group of users and devices providing high privacy and confidentiality among them.

(Turkanović, 2018) designed a decentralized education platform for credit transfer and grading system. This platform is built as per the guidelines of Higher Education Institutes (HEIs) in European countries. The motive of this platform is to create a global ubiquitous learning environment for students and HEIs which is beyond administrative and language barriers.

Blockchain is being used in a variety of applications using Internet of Things (IoT) to remove the hurdles of security and privacy in the IoT network. (Makhdoom et al., 2018) gave the systematic study of IoT environment showcasing the two big limitations: security and privacy in IoT network and how blockchain can be used to resolve these issues.

(Khan & Salah, 2018) also surveyed the major security issues involved with IoT network by defining the current problems faced while transmitting data in IoT communications and the present solutions available for them. It also identified the blockchain based solutions for the security issues of IoT.

(Nizamuddin et al., 2019) proposed a unique concept for sale of digital assets using smart contracts to facilitate authors and publishers. It uses Ethereum blockchain platform to implement smart contract and Ether cryptocurrency for the payments by the customers.

(Iqbal et al., 2019) defined trust management model for Internet of vehicles and explains how the new technologies like fog computing and blockchain can be used for implementing trust management with higher efficiency by using distributed computing for dynamic nature of Internet of vehicles.

(Rathee et al., 2019) provided a security framework for IoT heathcare using blockchain technology. It use the concept of encrypting all the data whether it be medicines or health reports by using hash algorithm so that no data is manipulated by anyone in the blockchain network. The results achieved for this framework, when compared with the conventional approach provided better simulated results.

APPLICATIONS

Blockchain is being used in various public and private sector organizations. There has been various start-ups adopting and providing Blockchain related services. In fact, in some countries, blockchain is being adopted by the governments also. The various areas where blockchain has its applications can be broadly classified in following categories:

Financial Services

- ICICI bank became the first bank to perform banking transactions using Blockchain to provide electronic and paperless financial transactions within the country and abroad (Sheetal & Venkatesh, 2018).
- Bajaj Finserv is also using blockchain to fasten its services of settling claims and travel insurances (Sheetal & Venkatesh, 2018).
- A blockchain based platform “chain.com” uses Blockchain for private equity exchange (Zhao et al., 2016).
- Corda is an open source Blockchain platform that connects supply chain to global network, insurance providers to their authoritative record and much more (Olleros & Zhegu, 2016).

Smart Healthcare

- The NITI Aayog, India is trying to solve the issue of fake medicines using blockchain technology (Balsari et al., 2018).
- Medichain is building a blockchain based platform for health information exchange for hospitals (Rouhani et al., 2017).

Smart Property

- Microsoft and Ernst & Young (Xu et al., 2017) are developing blockchain project for content rights and management of royalties.
- Ujo Music (Mattila, 2016) is a music platform which uses blockchain for music licensing.
- ChromaWay (Kshetri and Voas, 2018) is using blockchain for land registry to track property ownership.
- Everledger (Mattila, 2016) is a blockchain based diamond certification database to keep track of original, owner, VAT charges etc.

Smart Government

- BitID, Onename, Bithandle are various blockchain based digital identity (Olleros & Zhegu, 2016) verification platforms.
- Estonia, Europe (Sullivan & Burger, 2017) is the first nation to use blockchain to provide e-residency to anyone by issuing e-ID which allows them to do any commercial activity within the nation.

Smart Contracts

- Eris Industries (Mattila, 2016) provides a platform to create smart contracts by writing their own programs which can be executed in a distributed manner.
- Ethereum (Buterin, 2014) uses smart contracts to provide a platform to build decentralized application on top of it.

Data Storage and Protection

- Emercoin (Olleros & Zhegu, 2016) is a provider of blockchain based IT services like data storage security, data protection and creation of various distributed services.
- Storj (Wilkinson et al., 2014) is a decentralized cloud storage platform which allows user to share and transfer data without having third party reliance.

Commerce

- Bitcoin (Nakamoto, 2008) was the first real application of blockchain. Various other crytocurrencies (Singh & Singh, 2016) like Ripple (Olleros & Zhegu, 2016), Litecoin (Swan, 2015), Dodgecoin (Antonopoulos, 2014) etc. originated after Bitcoin's success.
- HomeSend which is meant for cross border payments is also finding its use case in Blockchain (Olleros & Zhegu, 2016).
- Six international banks joined Utility Settlement Coin (USC) blockchain based project, which will streamline the inter-bank settlements (Meyer, 2017).

PROPOSED APPLICATION AREAS

Blockchain technology provides user privacy by encrypting user identities and at the same time provides transparency of data as anyone can check for historic as well as recent transactions of the network. Also, the data in a blockchain network is immutable as no editing is possible once the data is written to the blockchain. Moreover a large number of users can participate and different set of roles or responsibilities can be attached to each individual in the network. This makes blockchain appropriate for managing tasks for different hierarchy of employees within one or many organizations. In this way Blockchain can be used to create a platform for Birth certificates generation.

In the present scenario, the birth certificate is generated in Municipal Corporations and Tehsildar's office after filling birth records in the registration form provided by them. These offices take 7-10 days to verify birth records from the hospitals and then issue the certificate. There can also be some additional personal delays in the existing system. Also, one of the parents needs to visit the office to submit the registration form and collect the certificate. In the proposed blockchain system, BirthChain, the hospitals and the government officials will act as nodes of the network. The tasks of both of the nodes will be as follows:

- **Hospitals**: Every hospital in the country will be connected on the blockchain platform. Whenever a child is born in any of the hospital across any of the cities, it needs to update the details on the blockchain platform giving birth details of the child as well as the parents' details. This will create a request to the Municipal corporation or Tehsildar office to generate birth certificate for the newly born child.
- **Government Body**: The officials of Municipal corporation or Tehsildar will first verify the details submitted by the hospitals. After the validation process of the officials, the birth certificate will be generated and sent to the parents' address. An e-Birth certificate will also be emailed to parents' email address.

Figure 6 depicts the scenario of blockchain platform BirthChain. The process starts after a child is born. Hospital authorities have to update child's and parents' details on the blockchain platform. This information will be verified by the assigned government officials who will act as miners of the blockchain network. Once the validation is done by the miners, the information is shared with Municipal Corporation to generate birth certificates. A simple smart contract will be used to generate and e-mail Birth certificates to the parents' email address. The officials at Municipal Corporation will then post the certificate to parents' postal address.

BirthChain will ease the process for the parents by issuing them birth certificates at home as well as an e-birth certificate to their e-mail id. The complete process will take less time if compared to the current process as BirthChain does not involve filling of registration form or hospital verification. Figure 7 shows the flow chart for the activities involved in the whole process of BirthChain. For any issues, an online grievance handling system will also be incorporated.

In this system, few selected municipal corporations will be made full nodes to store the complete blockchain ledger for new borns. So the hospitals and other government offices need not store any data related to new births as a distributed blockchain ledger is being maintained. Also no paper records need to be maintained by any offices. It will also help in analysis of data like evaluating birth rate on a daily or yearly basis in the specified location or nation as a whole, population count of a particular age group, population count who is eligible for voting etc.

Figure 6. BirthChain- The proposed Blockchain platform for Birth Certificate generation

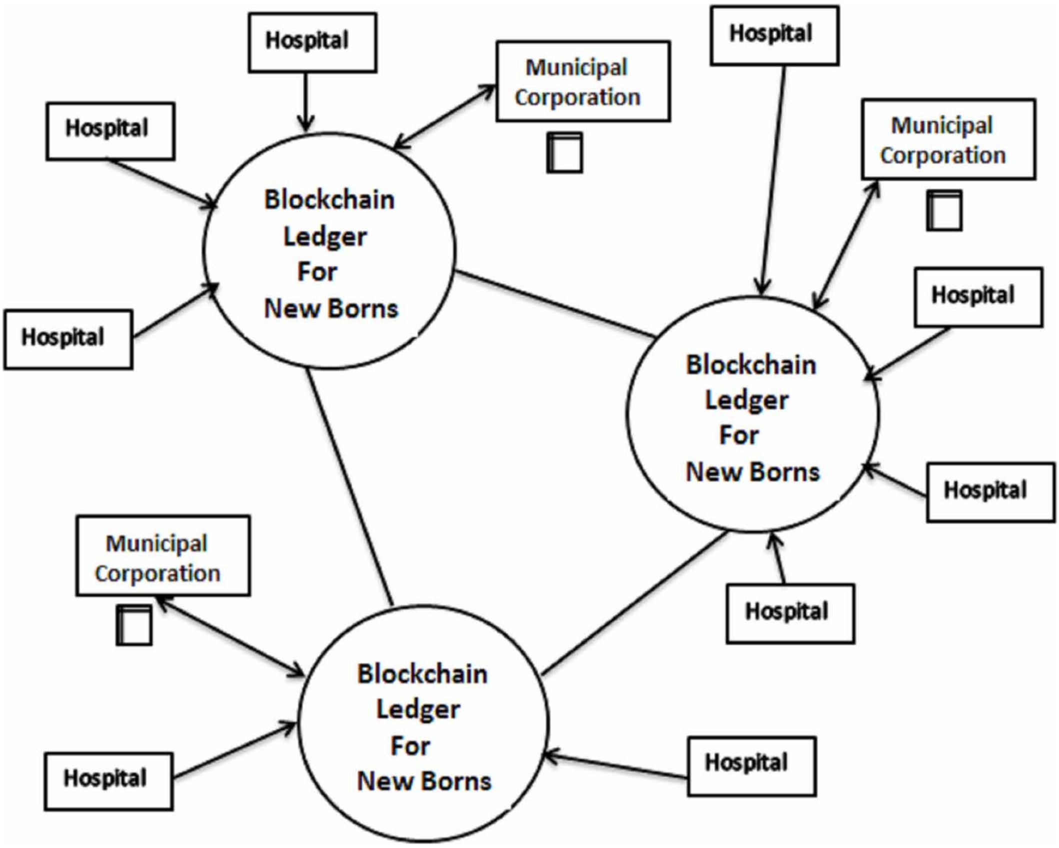
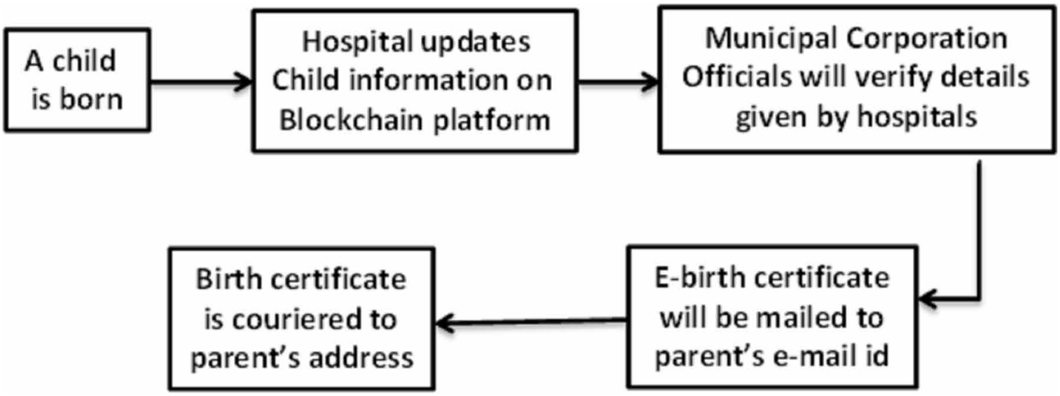


Figure 7. Flow chart for the activities involved in BirthChain


A child is born
Hospital updates Child information on Blockchain platform
Municipal Corporation Officials will verify details given by hospitals
E-birth certificate will be mailed to parent's e-mail id
Birth certificate is couriered to parent's address

CONCLUSION AND FUTURE WORK

Blockchain technology is going to transform the internet era. It is addressing the major privacy and security concerns of the new age technologies like cloud computing, Internet of Things etc. In fact, various businesses are using smart contracts for their transactions as they enforce strict laws and automate transactions involving various parties. Industries and organizations are embracing the technology and looking for use cases and usage of the technology for their work. Apart from private organizations, the technology is getting accepted by the government in various countries like Europe for e-residency and India in land registry.

The proposed application BirthChain will act as a trusted ledger of birth records for the nation. It will ease the current process of generating birth certificates. Nobody will be able to forge any information in present or future. As copy of blockchain ledger will be available with the municipal corporations, it can be used by other government bodies like PAN card office, passport office, schools to verify the birth certificate authenticity. In future, BirthChain can be extended to store details of person's demise and generate death certificates. It will help to evaluate population count, death rate, reasons of death, average death age etc.

The technology is still in very early phases. A lot of research and development is going on to optimize its working algorithms for cleaner and greener environment. Many blockchain platforms are testing its applicability and efficiency over other technologies for existing processes. Blockchain is also being integrated with other technologies to get the best use of various technologies. It surely has much more to deliver in the years to come.

REFERENCES

P4Titan. (2014). *Slimcoin a Peer-to-Peer Crypto-Currency with Proof-of-Burn*. Academic Press.

Antonopoulos, A. M. (2014). *Mastering Bitcoin: unlocking digital cryptocurrencies*. O'Reilly Media, Inc.

Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016, August). Medrec: Using blockchain for medical data access and permission management. In *Open and Big Data (OBD), International Conference on* (pp. 25-30). IEEE.

Balsari, S., Fortenko, A., Blaya, J. A., Gropper, A., Jayaram, M., Matthan, R., & Mandl, K. D. et al. (2018). Reimagining Health Data Exchange: An application programming interface–enabled roadmap for India. *Journal of Medical Internet Research*, *20*(7), e10725. doi:10.2196/10725 PMID:30006325

Bentov, I., Gabizon, A., & Mizrahi, A. (2016, February). Cryptocurrencies without proof of work. In *International Conference on Financial Cryptography and Data Security* (pp. 142-157). Springer. doi:10.1007/978-3-662-53357-4_10

Bentov, I., Lee, C., Mizrahi, A., & Rosenfeld, M. (2014). proof of activity: Extending bitcoin's proof of work via proof of stake. *Performance Evaluation Review*, *42*(3), 34–37. doi:10.1145/2695533.2695545

Brown, R. G. (2018). *The Corda Platform: An Introduction*. Academic Press.

Buterin, V. (2014). *A next-generation smart contract and decentralized application platform*. White Paper.

Castro, M., & Liskov, B. (1999, February). Practical Byzantine fault tolerance. In OSDI (Vol. 99, pp. 173-186). Academic Press.

Chase, J. M. (2016). *Quorum white paper*. Available: https://github. com/jpmorganchase/quorumdocs/blob/master/QuorumWhitepaper v0.1.pdf

Chen, L., Xu, L., Shah, N., Gao, Z., Lu, Y., & Shi, W. (2017, November). On security analysis of proof-of-elapsed-time (poet). In *International Symposium on Stabilization, Safety, and Security of Distributed Systems* (pp. 282-297). Springer. doi:10.1007/978-3-319-69084-1_19

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. *IEEE Access: Practical Innovations, Open Solutions*, *4*, 2292–2303. doi:10.1109/ACCESS.2016.2566339

Duffield, E., & Diaz, D. (2015). *Dash: A PrivacyCentric CryptoCurrency*. Self-published.

Dziembowski, S., Faust, S., Kolmogorov, V., & Pietrzak, K. (2015, August). Proofs of space. In *Annual Cryptology Conference* (pp. 585-605). Springer.

Eyal, I., Gencer, A. E., Sirer, E. G., & Van Renesse, R. (2016, March). Bitcoin-NG: A Scalable Blockchain Protocol. In NSDI (pp. 45-59). Academic Press.

Feige, U., Fiat, A., & Shamir, A. (1988). Zero-knowledge proofs of identity. *Journal of Cryptology*, *1*(2), 77–94. doi:10.1007/BF02351717

Fernández-Caramés, T. M., & Fraga-Lamas, P. (2018). A Review on the Use of Blockchain for the Internet of Things. *IEEE Access: Practical Innovations, Open Solutions*, *6*, 32979–33001. doi:10.1109/ACCESS.2018.2842685

Haber, S., & Stornetta, W. S. (1990, August). How to time-stamp a digital document. In *Conference on the Theory and Application of Cryptography* (pp. 437-455). Springer.

Hamida, E. B., Brousmiche, K. L., Levard, H., & Thea, E. (2017, July). Blockchain for enterprise: overview, opportunities and challenges. *The Thirteenth International Conference on Wireless and Mobile Communications (ICWMC 2017).*

Iqbal, R., Butt, T. A., Afzaal, M., & Salah, K. (2019). Trust management in social Internet of vehicles: Factors, challenges, blockchain, and fog solutions. *International Journal of Distributed Sensor Networks*, *15*(1), 1550147719825820. doi:10.1177/1550147719825820

Jain, A., Jain, A., Chauhan, N., Singh, V., & Thakur, N. (2018). *Seguro Digital storage of documents using Blockchain*. Academic Press.

Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, *82*, 395–411. doi:10.1016/j.future.2017.11.022

Kiayias, A., Russell, A., David, B., & Oliynykov, R. (2017, August). Ouroboros: A provably secure proof-of-stake blockchain protocol. In *Annual International Cryptology Conference* (pp. 357-388). Springer. doi:10.1007/978-3-319-63688-7_12

King, S. (2013). *Primecoin: Cryptocurrency with prime number proof-of-work*. Academic Press.

King, S., & Nadal, S. (2012). *Ppcoin: Peer-to-peer crypto-currency with proof-of-stake*. Academic Press.

Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016, May). Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In *2016 IEEE symposium on security and privacy (SP)* (pp. 839-858). IEEE.

Kshetri, N., & Voas, J. (2018). Blockchain in Developing Countries. *IT Professional*, *20*(2), 11–14. doi:10.1109/MITP.2018.021921645

Kurtulmus, A. B., & Daniel, K. (2018). *Trustless machine learning contracts; evaluating and exchanging machine learning models on the ethereum blockchain*. arXiv preprint arXiv:1802.10185

Larimer, D. (2014). *Delegated proof-of-stake (dpos)*. Bitshare whitepaper.

Lerner, S. D. (2015). *Rootstock: Bitcoin powered smart contracts*. Academic Press.

Li, W., Andreina, S., Bohli, J. M., & Karame, G. (2017). Securing proof-of-stake blockchain protocols. In *Data Privacy Management, Cryptocurrencies and Blockchain Technology* (pp. 297–315). Springer. doi:10.1007/978-3-319-67816-0_17

Li, Z., Kang, J., Yu, R., Ye, D., Deng, Q., & Zhang, Y. (2018). Consortium blockchain for secure energy trading in industrial internet of things. *IEEE Transactions on Industrial Informatics*, *14*(8), 3690–3700.

Lin, I. C., & Liao, T. C. (2017). A Survey of Blockchain Security Issues and Challenges. *International Journal of Network Security*, *19*(5), 653–659.

Makhdoom, I., Abolhasan, M., Abbas, H., & Ni, W. (2018). Blockchain's adoption in IoT: The challenges, and a way forward. *Journal of Network and Computer Applications*.

Mattila, J. (2016). *The blockchain phenomenon*. Berkeley Roundtable of the International Economy.

Meng, Z., Morizumi, T., Miyata, S., & Kinoshita, H. (2018, July). Design Scheme of Copyright Management System Based on Digital Watermarking and Blockchain. In *2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC)* (pp. 359-364). IEEE. doi:10.1109/COMPSAC.2018.10258

Meyer, D. (2017). *More Banks Join UBS-Led Blockchain Scheme to Speed Up Settlements*. Retrieved from https://fortune.com/2017/08/31/banks-ubs-blockchain-settlements/

Milutinovic, M., He, W., Wu, H., & Kanwal, M. (2016, December). Proof of luck: An efficient blockchain consensus protocol. In *Proceedings of the 1st Workshop on System Software for Trusted Execution* (p. 2). ACM. doi:10.1145/3007788.3007790

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. Academic Press.

Nasir, Q., Qasse, I. A., Abu Talib, M., & Nassif, A. B. (2018). Performance analysis of hyperledger fabric platforms. *Security and Communication Networks*.

Nguyen, G. T., & Kim, K. (2018). A Survey about Consensus Algorithms Used in Blockchain. *Journal of Information Processing Systems*, *14*(1).

Niranjanamurthy, M., Nithya, B. N., & Jagannatha, S. (2018). Analysis of Blockchain technology: Pros, cons and SWOT. *Cluster Computing*, 1–15.

Niranjanamurthy, M., Nithya, B. N., & Jagannatha, S. (2018). Analysis of Blockchain technology: Pros, cons and SWOT. *Cluster Computing*, 1–15.

Nizamuddin, N., Hasan, H., Salah, K., & Iqbal, R. (2019). Blockchain-Based Framework for Protecting Author Royalty of Digital Assets. *Arabian Journal for Science and Engineering*, *44*(4), 3849–3866. doi:10.1007/s13369-018-03715-4

Olleros, F. X., & Zhegu, M. (Eds.). (2016). *Research handbook on digital transformations*. Edward Elgar Publishing. doi:10.4337/9781784717766

Park, J., & Park, J. (2017). Blockchain security in cloud computing: Use cases, challenges, and solutions. *Symmetry*, *9*(8), 164. doi:10.3390/sym9080164

Partala, J. (2018). Provably Secure Covert Communication on Blockchain. *Cryptography*, *2*(3), 18. doi:10.3390/cryptography2030018

Pinno, O. J. A., Gregio, A. R. A., & De Bona, L. C. (2017, December). ControlChain: Blockchain as a Central Enabler for Access Control Authorizations in the IoT. In *GLOBECOM 2017-2017 IEEE Global Communications Conference* (pp. 1-6). IEEE.

Rathee, G., Sharma, A., Saini, H., Kumar, R., & Iqbal, R. (2019). A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology. *Multimedia Tools and Applications*, 1–23. doi:10.1007/s11042-019-07835-3

Rouhani, S., Butterworth, L., Simmons, A. D., Humphery, D. G., & Deters, R. (2018, July). MediChain TM: A Secure Decentralized Medical Data Asset Management System. In *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)* (pp. 1533-1538). IEEE.

Sapra, R., & Dhaliwal, P. (2018, December). Blockchain: The new era of Technology. In *2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC)* (pp. 495-499). IEEE. doi:10.1109/PDGC.2018.8745811

Seebacher, S., & Schüritz, R. (2017, May). Blockchain technology as an enabler of service systems: A structured literature review. In *International Conference on Exploring Services Science* (pp. 12-23). Springer. doi:10.1007/978-3-319-56925-3_2

Sheetal, M., & Venkatesh, K. A. (2018). *Necessary requirements for Blockchain Technology and its Applications*. Academic Press.

Singh, S., & Singh, N. (2016, December). Blockchain: Future of financial and cyber security. In *Contemporary Computing and Informatics (IC3I), 2016 2nd International Conference on* (pp. 463-467). IEEE.

Sullivan, C., & Burger, E. (2017). E-residency and blockchain. *Computer Law & Security Review*, *33*(4), 470–481. doi:10.1016/j.clsr.2017.03.016

Swan, M. (2015). *Blockchain: Blueprint for a New Economy*. O'Reilly Media.

Tromp, J. (2014). Cuckoo Cycle: a memory-hard proof-of-work system. *IACR Cryptology ePrint Archive, 2014*, 59.

Tuli, S., Mahmud, R., Tuli, S., & Buyya, R. (2019). Fogbus: A blockchain-based lightweight framework for edge and fog computing. *Journal of Systems and Software*, *154*, 22–36. doi:10.1016/j.jss.2019.04.050

Turkanović, M., Hölbl, M., Košič, K., Heričko, M., & Kamišalić, A. (2018). EduCTX: A blockchain-based higher education credit platform. *IEEE Access: Practical Innovations, Open Solutions*, *6*, 5112–5127. doi:10.1109/ACCESS.2018.2789929

Wilkinson, S., Boshevski, T., Brandoff, J., & Buterin, V. (2014). *Storj a peer-to-peer cloud storage network*. Academic Press.

Xu, R., Zhang, L., Zhao, H., & Peng, Y. (2017, March). Design of network media's digital rights management scheme based on blockchain technology. In *Autonomous Decentralized System (ISADS), 2017 IEEE 13th International Symposium on* (pp. 128-133). IEEE. doi:10.1109/ISADS.2017.21

Yakubov, A., Shbair, W., Wallbom, A., & Sanda, D. (2018). A Blockchain-Based PKI Management Framework. In *The First IEEE/IFIP International Workshop on Managing and Managed by Blockchain (Man2Block) colocated with IEEE/IFIP NOMS 2018*. doi:10.1109/NOMS.2018.8406325

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology? A systematic review. *PLoS One*, *11*(10), e0163477. doi:10.1371/journal.pone.0163477 PMID:27695049

Yuan, C., Xu, M. X., & Si, X. M. (2017). Research on a new signature scheme on blockchain. *Security and Communication Networks*, *2017*, 2017. doi:10.1155/2017/4746586

Zhao, J. L., Fan, S., & Yan, J. (2016). *Overview of business innovations and research opportunities in blockchain and introduction to the special issue*. Academic Press.

Zyskind, G., & Nathan, O. (2015, May). Decentralizing privacy: Using blockchain to protect personal data. In Security and Privacy Workshops (SPW), 2015 IEEE (pp. 180-184). IEEE.

Riya Sapra has completed her B.Tech and M.Tech in Computer Science & Technology in 2011 and 2013 respectively. Currently she is a Ph.D scholar at Manav Rachna University, India. She is interested in technologies like Blockchain and Internet of Things. Her current work focuses on using blockchain in the existing and new application areas to ease the process of work. She has authored few research papers and book chapters.

Parneeta Dhaliwal has received her Ph.D. in Computer Science from University of Delhi. Dr. Dhaliwal is currently working as an Associate Professor in Department of Computer Science & Technology,ManavRachna University, Faridabad. She has guided many M.Tech and Ph.D. students in their research work.Her research interests include Data Mining, Machine Learning, Big Data and Blockchain. She is an author and co-author of many research papers in reputed International Journals and Conferences. Dr. Dhaliwal is a life member of CSI (Computer Society of India).