Blockchain Technology – A New Technology for Creating Distributed and Trusted Computing Environment

Amit Kumar Tyagi[1][0000-0003-2657-8700], Terrance Frederick Fernandez[2][0000-0002-7317-3362],

Deepti Goyal[3], Shashvi Mishra[4]

[1, 4] School of Computer Science and Engineering, Vellore Institute of Technology, Chennai, 600127, Tamilnadu, India.

[2]Department of Information Technology, Rajiv Gandhi College of Engineering & Technology, Puducherry, India

[3]Department of Computer Science and Engineering, Lingaya'sVidyapeeth, Faridabad - 121002, Haryana, India

amitkrtyagi025@gmail.com, frederick@pec.edu, deeptigoyal1994@gmail.com, shashvimishra@gmail.com

Abstract. Over the past decades (1950 to 2018), the world has moved from wired things to wireless devices with the advancement of electronics devices/technology. Such increment or development in networking technology faces plethora of incidents like issues in leaking privacy of users and that of surveillance and security breaches in systems. This paper canvasses about compromising users' privacy as various issues, challenges and questions which were raised in existing models. Be mindful that due to these issues, breaches or loopholes, unknown users/ third-parties collect and control large amounts of personal information; also they might misuse this gained data against respective user, for example, for financial use, blackmailing, etc. Hence, this article discusses about a novel technology (i.e., Blockchain), upon which every industry is trusting upon. How this new technology has grown to be fastest technology since the past decade among users and organization? Answers to such queries are given in this manuscript. Blockchain provides decentralized, distributed personal data management system which ensures that user can own, control and protect their data against any kind of breach. In last, this work provides current trends of blockchain technology in many sectors/ applications and also includes few future challenges for this distributed ledger technology

Keywords: Blockchain Technology, Bit Coin, Crypto-currency, Security, Trust, Real-World applications.

1 Introduction about Blockchain

The Blockchain is a concept of sharing information/ data in a distributed and decentralized manner. This concept was used previously in buying lands, but technically it was sued in 2008 in a cryptocurrency called 'Bitcoin' [1]. From 2008 till date, this concept had seen multitudinous enhancements and a rapid growth to employ this technology/ concept in several real worlds' applications, in creating distributed and

trusted environments. In general, Blockchain concept grows as a chain-like structure via constructing different blocks. In which, each block consists of the information regarding previous (the block that comes before it in a chain) and next block (that comes after in a chain). The details are stored as cryptographic hash which acts as a significant ID which is created by taking into account the mentioned variables:

- The latest block timestamp,
- The phase series,
- A previous block identifier, and a variable called nonce.

Now here an argument arises "What is a nonce"? Nonce represents a highly arbitrary number which helps monitor and supervise the toughness of the puzzle in the cryptographic form. In other terms, it possesses a modifiable value which is altered autonomously to ensure the minimum time limit of 10 minutes' work force for the addition of a novel block into the Blockchain network. For example, Thousands of nodes store copies of the relevant content in a shared blockchain, like Bitcoin, forcing a cap on transaction volumes to retain decentralization. On the other hand, only nodes with a direct interest in the efficient processing of transactions are added / executed in private block chains. Blockchain environments are not only technologically decentralized, but they also provide a highly decentralized decision-making framework.

In general, the Bitcoin Blockchain was the first commonly used Blockchain, and it serves as a de-facto example of how Blockchain systems might work. Bitcoin Blockchain is the primogenitor of public Blockchain, or plainly called as 'permission less' Blockchain, just by running some free software, and without signing up, anyone could write data into it. It should be noted that the Bitcoin Blockchain file includes a list of all Bitcoin transactions that have occurred since January 2009. In simple words, Bitcoin is an electronic currency utilizing Blockchain technology [1].

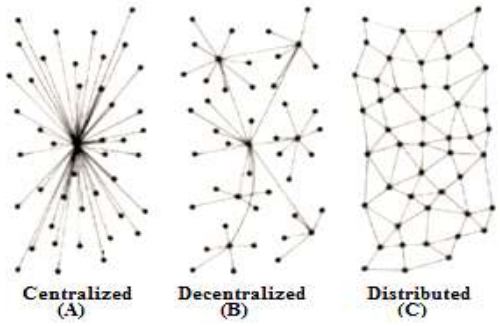

Fig.1. Explanation of Centralized, Distributed and Decentralized Database/ Application

Figure 1 shows that the structure of Centralized, Distributed and Decentralized Database.Hence, some characteristics of Blockchain technology are:

- **Consensus:** The validity of the successful completion of a transaction depends on the agreement of the participants.
- **Provenance:** Participants are aware of the fact that the assets have been derived from a source and know that its' ownership is prone to change with time.

- **Immutability:** None of the participants have the authority to modify or alter the transactions after it has been upheld to the ledger. If a transaction is errored, it must be reversed and rectified with the commencement of a new one, such that both are recorded.
- **Finality:** A single, distributed ledger provides a source to approach the ownership of an asset or a successful transaction.

Hence, this section discusses about introduction about Blockchain, uses of Blockchain technology in several applications (in today's era). Now, the organization of remaining work in this manuscript is discussed as: section 2 discuss about evolution of Blockchain technology. Further, section 3 discusses structure of Blockchain, and then necessity of Blockchain is being discussed in section 4. Furthermore, section 5 discusses "How Blockchain technology build trust in computing environment" and where it is more useful in near future. Then, several issues and challenges in Blockchain concept is being discussed in section 6. Finally, section 7 concludes the work flashing future scope in brief.

2 Evolution of Blockchain

As the old adage goes, necessity is mother of invention. Most of the best innovations of the century have been done in last few decades because there was a necessity in it. All these happened because of development in technology and availability of resources. An invention could never be instantaneous, it arises or is fetched up from a long time ago, but most of us do not know about its history. Blockchain concept had been used since 1900s. For example, in buying or selling of lands, everyone is aware of the previous seller or entire history of a sold land. Today this concept is enabled with technology and changing the growth of industry/ organisation/ practical applications. In this section, we will understand about the evolution of Blockchain technology. Hence, figure 2 reveals the history of Blockchain from its birth year. We can find out that that many applications have been shifted towards Blockchain and using Blockchain to provide trusted secured and reliable service to users.

2.1. Blockchain 1.0: Launching of Bitcoin - a New Cryptocurrency

The first Blockchain was conceptualized by a common man named Satoshi Nakamoto in the year 2008-2009 [1, 29, and 33]. It represents the technology of Bitcoin. The whistle-blower introduced decentralization of data and information storage through a distributed and decentralized database. He declared the fact that there was no need to verify financial transaction for "trusted third parties" and a method or structure was employed to develop the structure of the internet, i.e., TCP/IP suite. Bitcoin created a drastic change to the internet itself, so it needed to act as a platform and have its own application layer to be built on-top of its core protocols.

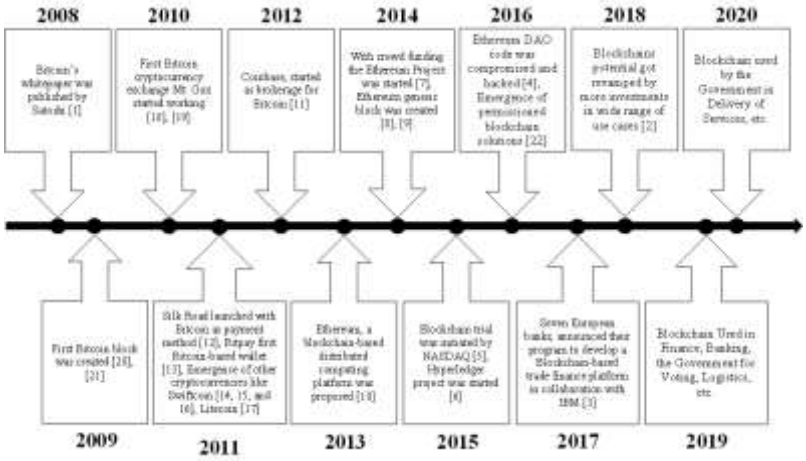

Fig.2. Evolution of Blockchain Year by Year

2.2. **Blockchain 2.0: Ethereum Rise - Smart Contracts**

Vitalik Buterin (a Russian-Canadian programmer), co-founder of Ethereum and Bitcoin magazine, contributed the Bitcoin codebase [28]. He wanted Blockchain technology to allow for zenith level of scripting and thus Ethereum project was instituted in 2014. The Ethereum technology pioneered Blockchain 2.0 which saved money and did pronominal improvement to the Blockchain. It allows Blockchain as a platform and this is achieved through the concept of distributed virtual machine. Ethereum and other platform projects are known as distributed virtual machine because of their ability to run decentralized application top of their own Blockchain. It also allows micro payments so it can handle small value transactions. It also includes the concept of token digital assets and finally it also christened the idea of decentralized organisation called Decentralized Autonomous Organizations (DAO). It would govern finances and policy on Blockchain.

2.3. **Blockchain 3.0**: **Next Generation Technology without Mining- DApps**

Generally, Distributed Applications (DApp) means decentralized applications or services which are produced without the involvement of centralized infrastructure. DApps use decentralized storage and decentralized communication. Due to this unique nature, DApps are using Blockchain technology, or have their backend code running on a decentralized Peer-to-Peer (P2P) network. Whereas on the other side, a traditional application consists storage and execution (or running code on blackened) on centralized servers. Such services are not involved in DApp. Note that, like a traditional App, a DApp can have frontend code and user interfaces written in any language that can allow calls to its backend [30]. But, when a DApp spears a frontend, it transforms into new technologies such as Ethereum Swarm (placed on decentralised storages). It can therefore be written as: DApp = frontend + (running, i.e., on Ethereum) contracts.

2.4. Blockchain 4.0: Making Blockchain usable in Industry 4.0

Due to rapid development and requirement of security and trust together, Blockchain is moved to new level, i.e., it (Blockchain) is used by industries or firms. Blockchain

4.0 uses solutions and concepts to make useful Blockchain technology in (with) business demands, for example, Industry 4.0 demands. The definition of Industry 4.0 is: automation, preparation of business capital, and convergence of various execution systems [23]. Notice that this industrial revolution needs a massive/ higher degree of confidence and protection of privacy against malicious users outside the world. Blockchain fulfill these needs of rendering higher degree of trust and privacy protection in industry. One ends up with business integration when incorporating Blockchain to IT structures, allowing Cross-System / Cross-Blockchain business processes, i.e. machines to securely and autonomously place an order for their replacement parts to arrive [23]. Management of the supply chain, approval workflows, financial transactions and condition-based payments; data collection, health management and asset management of the Internet of Things (IoT) are few applications that in the near future will be run by Blockchain technology. Today every organization is looking for distributed and trusted environment and this can be achieved by Blockchain technology. Hence, precisely, in real-life market cases, Blockchain 4.0 makes Blockchain 3.0 even more accessible (with providing higher trust among human being and machines). With satisfying Industry 4.0 demands by Blockchain technology in (with) industries, we move one step forward in making of a human experience (life) better.

Hence, this section discusses about evolution of Blockchain technology (from past to present scenario). Now in the forthcoming section, we will put some light upon the structure of Blockchain and will discuss how blocks are getting fabricated and added in a Blockchain (of a transaction).

3. Structure of Blockchain

A Blockchain is a decentralized, distributed public or private ledger to exchange some values (called value-exchange protocol) through blocks (in a Peer to Peer network.), also without modification/ alteration of all next blocks [1, 33]. Blockchain is the fifth evolution of computing. A block is a packaged data structure (uses linked lists and pointers). It is a framework for container data that clusters transactions known as the Blockchain for inclusion in the public ledger. The block header contains structure of blocks in a well–ordered form (very block contains data of previous bock and next block) called metadata (i.e., Data about data) (refer figure 3). Note that the first block is referred to as the genesis block (built in 2009) in the Blockchain. It is a universal parent of all the blocks in the Blockchain. There are some other core components of Blockchain architecture, which can be included as:

- Node: This is a user or machine (each has an independent copy of the entire Blockchain ledger) inside the Blockchain architecture.
- Transaction: The intent of the Blockchain is the smallest building block of a Blockchain system (records, data, etc.).
- Block: It is a data structure used to manage a transaction collection that is distributed to all network nodes.
- Chain: It is a block series in a particular order.
- Miners: Before adding anything to the Blockchain framework, it has some unique nodes that perform the block verification process.
- Consensus (consensus protocol): a collection of guidelines and arrangements for the implementation of Blockchain activities.

Adding Blocks to Blockchain: To understand the process of adding a new block to the Blockchain in depth, a group of users select a miner at the beginning to deal with transactions submitted. There is a voting deadline. Any consumer in the group has the right to vote before this time. One protocol states, however, that anyone can only vote once. Then a miner who has authority to mine in the next period of time becomes the consumer who has the largest number of votes. Some transactions are contained in a new block. The new block is related by its hash value to the Blockchain (refer to figure 3). That is, we must read the block header if we want to obtain the former block. It was possible to get the preview hash value from the block header. The value is the former block 's current hash value. The newly added block is also signed with its key by the miner, so we know the identity of the miner who completed the work of adding the new block and could therefore reward him. The machine will eventually broadcast the news that a new block has been added. The new block needs to be checked by all the other users. The new block must be recreated and added to the block by other miners at the same time.

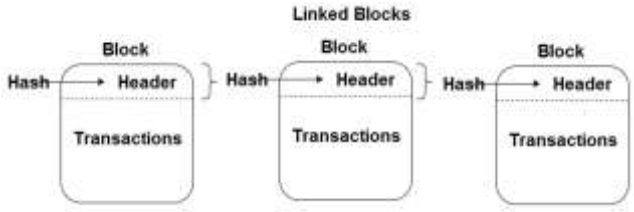

Fig.3. Structure of a Blockchain Network

In summary, there are various components of a Blockchain structure which are included as:

- Nodes within Peer to Peer (P2P) network
- Block and Genesis Block Properties
- Transactions inside the ledger
- The validation or mining method
- The "consensus" within the design of Blockchain
- Proof-of-labor

Hence, this section discussed about a detailed explanation of creating blocks, and adding of respective blocks in a Blockchain. Also, discusses how it builds trust on a public network. Now in next section, this work will discuss about necessity of Blockchain technology in current or for today's applications.

4. Necessity of Blockchain Technology

In the near future, popularity of Blockchain might be uncertain, but the concept of distributed networking will take the driver's seat as there is always a special need. It is necessitous not because it is avaricious, cost–saving or tighter data security but due to its distributed nature. Blockchain is essential because it provides peer to peer networks with confidence (using primarily data structure like linked list and pointers in a network). A primary reason banks exist is for transactions to serve as a Trustworthy Third Party (TTP). In simple terms, bringing trust to a decentralized network is

ground-breaking. In short, by adopting Blockchain, people can remove intermediary across the world. Some necessities of Blockchain include:

- Enhances reach of a businesses
- Ensures swift transactions
- Restricts frauds
- Reliability and transparency
- Immutability
- Cost effective

Blockchain technology provides new tools for authentication and authorization in this smart era/ digital world, i.e., provides a tough competition to several centralized administrators. Today, Blockchain applications can useful to consumers via several benefits, i.e., from business perspective, it is a game changing technology, and in near future, it will be used in many applications like finance, bank, land reforms, etc. In this section, we discussed about necessity of Blockchain technology in early stages and in current era or several applications. Now next section will explain on how the trust is built in several (real-world's) applications using Blockchain concept, and upon applications this technology can be employed in near future.

5. How Blockchain Technology Builds Trust and where?

In a Blockchain network, each block carries a transaction value between places. Considering data structure with hash function, (also cryptographic puzzle to solve) makes Blockchain tamper-proof, i.e., via providing higher (tight) security and anonymity among larger quantity of users, we build trust using Blockchain.

5.1. Building Trust among Peers using Blockchain Technology

Blockchain protection is based on the principle of proof of work, and a transaction is considered valid only until proof is obtained by the framework that adequate computational work has been done by approving nodes. In the form of a hash calculation, the miners (responsible for making blocks) are constantly trying to solve cryptographic puzzles (called Proof of Work (PoW)). The method of adding a new block is called mining to the Blockchain. The robustness against failure and exposure to data is given by blockchain technology. A decentralized data system responsible for preserving all transactional history is the Blockchain. In the form of a chain, the blocks refer to each other. The chain's first block is known as Genesis. A block header, transaction counter, and transaction are composed of each block. To record the data, it acts as a decentralized architecture. In the header, each block in the chain is marked by a hash. The hash is special and the Stable Hash Algorithm (SHA-256) produces it. SHA takes plaintext of any size and calculates a 256-bit cryptographic hash of a fixed size. Each header contains the previous block 's address in the chain.

A Blockchain is a decentralized transaction ledger through a network of peer-to - peer (P2P) operations. A transaction ledger is just a place where something can be recorded. We say Blockchains are decentralized ledgers because everyone on the network has their own synchronized copy. They can all see and confirm that a transaction has occurred and has been recorded, all at the same time. This occurs on a peer-to-peer computer network. So, instead of connecting to a central authority through a hub-and-spoke model, every participant has a computer linked to other participants. The data flow from organizations to the third party and back can be replaced with ease using

Blockchain technology. Data, instead, travels between anonymous organizations and comes to a final assent within a short span of time, which clearly implies the combined efforts of all parties from a set of events. Data encoding assures the privacy of data, digital signatures, etc. and assures validation, data consolidation and much more. As a result, Blockchain is able to address the issue of having to trust third parties. In general, Blockchain varies widely in configuration and functionality, whether public or private; like any network that is open to the public, but mostly needed to protect a private network for defense / secure technology. Depending on if they require someone to be able to write to them (public or permission less Blockchain) or whether the participant pool is restricted (private or authorized Blockchain), Blockchain systems have various frameworks or protocols. In general, Blockchain public-write is far more limited than private ones. There are actually thousands of public and private blockchains working at the moment, but many of them do not have a large uptake. Ripple, NXT, and Ethereum, etc., are today's public networks developed with blockchain technology that have gained popularity in the last several years.

Now we're talking about adding new blocks to the outgoing Blockchain, and then there's a chance across a network that two different blocks will be added by different nodes at the same time, causing a chain fork. There is a 'consensus law' in this case that helps nodes find out the block they can assume is the block. The rule is called the 'longest chain rule' in Bitcoin, i.e., each node recognizes the validity of both contending blocks, and when the next block is built on one of the contenders, the situation resolves. The longer chain becomes part of the Block-chain de-facto. In this, validation of new added blocks is done based on ledgers/ consensus mechanism. It takes us back to the technology, which is based on applied cryptography, i.e., If we take the case of a certain party who intends to top up the ledger with some items. This particular transaction process is encrypted with the help of famous algorithms, and all members of the team are notified about this as well. Each Blockchain has its own “consensus mechanism” [1, 5, and 7]. Everyone uses the same, defined process to confirm that transactions are valid. Once they agree, the information is added to the permanent record. The new ledger entry has become one more block of data in a chain of related transactions. Because everyone is working from the same data, the transaction record cannot be challenged, and it cannot be changed.

It is to be observed that Consensus Function is a mechanism that urges a majority of the Blockchain nodes to come into an agreement on a certain message along with ensuring that the recent blocks have been correctly added to the existing chain, and assure that event like “fork attack” or other malicious intrusions do not occur. Here, *Proof of Work (PoW)* is useful on a public Blockchain, such as the one used for Bitcoin, but it demands for large amounts of power, and electricity, thus leading to the jingle of loose coins in the server’s pockets. Such expensive measures are to be avoided and hence, using Consensus Mechanism, Blockchain helps in the propagation of trust and ensures that the users remain anonymous. In other words, it builds trust among peers based on proof work and consensus mechanism and also preserves the privacy of existed peers available in a blockchain network. Hence in summary, a Blockchain in simple term called the ‘chain of trust’. Blockchain technology preserves privacy of users during making transaction by providing anonymity among all users. Apart from anonymity, there are six major keys to Blockchain Technology i.e., Decentralized character, Flexibility and Openness, Automation, Unchangeable, and

Anonymity. Notice that the variables that make Blockchain technology common and useful are: SHA256 Hash Function, Public Key Cryptography, Distributed Ledger, Peer to Peer Network, Proof of Work and Validation Incentives.

Hence, components or services like Distributed, Decentralized, Tighter Security, Transparency, and Flexibility are the major merits of Blockchain [24, 26, and 27]. Now using Blockchain technology, future industries or business enhancements can be extracted or included.

5.2. Future with Blockchain

As discussed above, Bitcoin is just the premiere application of Blockchain. Blockchain provides the facility of recording and storing Bitcoin transactions, but Blockchain has various implementations apart of Bitcoin. For example, Big Data (term coined in early 20's century) with Blockchain network is enabling to solve several problems/ objectives/ goals, discussed in [27]. Blockchain has a highly resilient architecture inherently distributed, which makes it an interesting platform to deliver trusted services for society. In this section, we will address Blockchain applications for identity and protected data. Blockchain technology can provide a way to solve this issue, i.e. identity authentication, without the need for a trusted central authority, by providing a stable solution. With Blockchain, participants in the network will communicate as follows:

- The government regulator establishes and populates the Blockchain registration for the new vehicle and passes the vehicle ownership to the manufacturer.
- Within the conditions permitted by the smart contract (a digital agreement or collection of rules governing a transaction), the manufacturer attaches the make, model, and vehicle identification number to the vehicle prototype.
- The dealer will see the new stock availability, and after a smart contract is performed to verify the transaction, ownership of the vehicle can be transferred from the seller to the dealership.
- The leasing firm is able to see the inventory of the supplier. After a smart contract is executed to confirm the sale, ownership of the car can be shifted from the dealer to the leasing company.
- The lessee will see the vehicles available for rental and fill out any form needed to execute the lease agreement.
- The leasing process continues between different leaseholders and the leasing company until the leasing company is prepared to remove the car.

In the above-mentioned small contract using Blockchain technology, the ownership of the asset is passed to the scrap dealer, who has the authorization to dispose of the vehicle under another smart contract. Hence, we have discovered several applications of Blockchain apart monetary applications like with the case of Bitcoin. Generally, any sort of knowledge can be included in Blocks on the Blockchain network, making Blockchain technology very flexible and useful. In the Blockchain database, car names, medical papers, land records, and more can be saved. In virtually any situation where it is necessary to keep a stable, open, and tamper-proof record in a decentralised manner, blockchains can be useful. Some other applications are making voting more transparent, keeping record of physical products, Digital identity systems and creating different financial instruments

In 2018, Japan has tried to use Blockchain concept in election/ voting to make it more transparent and trusted [25]. In future, some other countries will also implement such concept in their election – process.

5.3 Possible uses of Blockchain Technology in the Finance Sector

In addition to its role in money transactions, there are several additional applications that Blockchain technology brings to the financial sector. Blockchains can be used to store deeds, leasing agreements, equities, bonds, contracts, and titles since it can be used to record any sort of information. Technologies based on blockchains such as Ethereum make it possible for everyone to tokenize any physical asset. Tokens may be used to represent ownership in the same way that a stock's shares represent a company's ownership. For example, if many people share a restaurant's owner-ship, they might choose to tokenize the restaurant using Blockchain technology. By doing so, without even having to meet in person, they could vote on significant matters. In addition, physical goods can be tokenized as part of the supply chain of manufacturing, gold, silver, and other properties. Blockchain is touted as a technology that in the near future will revolutionize the finance sector. But slow transaction speeds and a lack of standardization, on the other hand, threaten to limit development.

5.4. A Use Case with Hyper-ledger

Privacy is a key problem within "traditional" Blockchain technology, as addressed in [22, 32 and 33] in Enigma. On the other hand, Storj is a network of peer-to-peer cloud storage and claims to be the' most stable and private cloud.' Hyper-ledger is an open source Blockchain platform, released by the Linux Foundation in December 2015, to support Blockchain-based distributed ledgers. Factom is the first functional Blockchain technology to include an unalterable record-keeping system [23, 24]. With the aim of enhancing many aspects of efficiency and reliability, it focuses on ledgers designed to facilitate multinational business transactions, including major technical, financial, and supply chain organizations. The purpose of the project is to put together a range of independent initiatives to build open protocols and standards by offering a modular platform to support various components for different uses. This will involve a range of Blockchains with their own agreement, identity, access control, and contract services, storage models, and services. Enigma is yet another example of decentralised network simulation. This is a decentralised, privacy-guaranteed computing network and an extension of Blockchain technology. The objective of Enigma is to allow developers without using a Trusted Third Party (TTP) to create a 'privacy by design', end-to-end decentralised application. Enigma is generally an extension of Blockchain technology, since computation and data storage are not done within the Blockchain, however the Blockchain is a "operating framework" for safe multi-party computations performed by network participating storage and computing nodes. Data is split between different nodes, and different nodes collaborate without leaking information to the other nodes to compute functions together. In summary, “no single party ever has access to data in its entirety; instead, every party has a meaningless (i.e., seemingly random) piece of it.”

Hence, this section discusses about building trust in several domains. Also, this section discussed how Blockchain can be useful in building trust, i.e., how it can be a

bullet proof (any attack-proof) technology in near future. Now in next section, we will discuss about several issues with respect to Blockchain technology in brief.

6. Issues and challenges with the Blockchain Technology

While Blockchain technology has tremendous potential for building future Internet systems, there are numerous technological demurrals facing it. In creating distributed web, distributed cloud, etc., Blockchain is becoming reposeful than any others. Yet, using Blockchain technology in applications is not free from challenges due to raised critical issues. These loopholes can be discussed as follows. Firstly, scalability is a huge concern. Larger blocks, however, mean greater storage capacity and that results in slower network propagation. In millions of blocks, massive data storage leads to a slower processing speed. Notice that a tough challenge has been the trade-off between block size and protection. Secondly, by selfish mining policy, it has been proven that miners could gain greater revenue than their fair share. For more revenue in the future, miners are hiding their extracted blocks. Branches could occur frequently in that way, which hinders the growth of Blockchain. Thirdly, wastage of electrical energy in mining block is sky-high. Proof of work, for example, wastes too much energy, while in the proof of stake consensus process the phenomenon that the rich get richer could occur. To sum up, there are five big challenges that Blockchain technology needs to resolve (to get worldwide acceptance by industrial stakeholders), these difficulties are: Increased performance, Interoperability, Reduced complexity, Cost, Supportive regulation and more collaboration.

6.1. Current Critical issues and Limitations of Blockchain Technology

Miners are getting incentive in verifying new blocks, but this incentive hit the rock bottom, whereas the computation power is increasing or so the requirement of electrical energy to mine new blocks or any transaction. Note that a user contains all of the transaction of Blockchain whatever has been created or generated so far. Some critical issues have been raised (rectified) in Blockchain (during making a transaction or creating a block), which are included as:

Complexity: An entirely new language is involved in blockchain technology. It has made cryptography more popular, but jargons are full of chock-full of the highly specialised industry. Thankfully, there are many attempts to include detailed and easy to understand glossaries and indexes.

Network size: Blockchains are not strangely immune to bad actors (like all distributed systems) as they are 'anti-fragile,' i.e. they respond to attacks and grow stronger. However, this calls for a wide network of users. If a Blockchain is not a stable network with a widely dispersed node grid, the complete advantage becomes more difficult to harvest. For certain approved Blockchain ventures, there is some discussion and debate over whether this is a fatal flaw.

Transaction costs, network speed: After being touted as 'near free' for the first few years of its existence, Bitcoin actually has notable transaction costs. As of late 2016, only about seven transactions per second can be processed and each transaction costs about $0.20 and can store only 80 bytes of data. The politically charged aspect of using the Bitcoin Blockchain is still there, not for transactions, but as a data store.

This is the topic of 'bloating' and is frequently frowned upon because it causes miners to reprocess and re-record the data continuously.

Human error: If a Blockchain is used as a database, the data going into the database must be of high quality. The data stored on a Blockchain is not necessarily trustworthy, so events need to be correctly registered in the first place. In a Blockchain record system similar to a centralised database system, the expression 'garbage in, garbage out' holds valid.

Unavoidable security flaw: In Bitcoin and other block chains, there is one notable security flaw, i.e., if more than half of the computers operating as network service nodes say a lie, the lie will become the truth. This is called a '51 percent attack' and when he introduced Bitcoin, Satoshi Nakamoto[1] illustrated it. For this purpose, the community closely tracks Bitcoin mining pools, ensuring that no one unknowingly gains such network power.

Politics: Since Blockchain protocols provide an opportunity to digitise models of governance, and since miners are essentially creating another type of incentivized model of governance, there have been sufficient opportunities between various sectors of the community for public disagreements.

In summary, other limitations of Blockchain technology includes: Lack of Technical knowledge, fewer people available with proper certification, Scalability, shoestring privacy, Security concerns, Complexity, Himalayan transaction cost and manual errors**.**

6.2. Challenges Occurring in Blockchain

In Blockchain, a transaction usually takes 10 minutes to update/ complete. Another goal of our system is to ensure the scalability of the system/ database (because requests may grow to large number or ~1 million per day in a system), and also ensuring the security of all generated data. As we discussed, many countries are trying to use Blockchain concept in the election process, yet opposition ones worry about cloud threatening. Only few threats like 51% attack on cloud computing are possible when Blockchain technology is being used there [31]. In summary, some other **c**hallenges in Blockchain technology are: Initial Costs for Setup, Consumption of energy, Integration with the legacy system, Security and Privacy and Public awareness.

Note that not all Blockchain ecosystems need to have the same mechanisms, especially if participants can be identified and trusted to behave.

- **The problems with peer-to-peer:** With peer-to-peer models, even if all peers are ‘trusted’, there can be a problem of agreement or consensus, i.e., if each peer is updating at different speeds and have slightly different states, how do we determine the “real” or “true” state of the data? In an ‘untrusted’ peer-to-peer network where we can not necessarily trust any of the peers, how do we ensure that the system cannot easily be corrupted by bad peers?
- **How do we make it hard for dishonest miners to create blocks?** Remember, this is only a problem for ledgers where block-makers are not trusted. A common conflict is when multiple miners create blocks at the same time, roughly. Because blocks take time to be shared across the network, which one should count as the legit block?

Hence, we find two important provisional conclusions with respect to using Blockchain network technology in our work, i.e., Mostly / empirically, blockchain technol-

ogy is often linked to trust, but it should be linked to power. Empirical evidence indicates that no confidence is required if full control is possible in Blockchain. This chapter addresses in depth many problems and issues with regard to blockchain technology. Now, with some future work, the next segment will conclude this work in brief (related to Blockchain technology).

7. Conclusion and Future work

A Blockchain is a network of blocks, i.e., contains a structure of mesh network (of computers) which are distributed and de-centralized in nature (for making a communication). Also, we discussed above (in sections) that Blockchain is a crying-out or most needed technology for providing secure, transparent and trusted services. But we should not neglect the fact that we are still in the early stages as the technology is still immature and (completely) has not yet been proven on scale. For this technology, for example, to illustrate this, we can look into this in several situations / scenarios, data volume, transmission speed, and consensus speed, i.e. useful provided that Bitcoin adds only up to 1 megabyte (MB) of data every ten minutes. Finally, we demonstrate that, instead of trust, Blockchain technology should be more linked to power. In addition, due to the inherent character of decentralized decision making, we argue that full autonomy of Blockchain systems is not always feasible and thus trust is still a factor in some Blockchain environments. We conclude that block-chain technology is a technology that, from a device perspective, increases control over counterparties in a transaction, but decreases control. The future research gaps are to be sorted out upon which we are going to witness the integration of Blockchain with Internet of Things, Artificial Intelligence and Cloud/ Edge Computing. In next decade, Blockchain will be majorly implemented in sectors like Banking, transportation, agriculture, healthcare, logistics, energy, in government schemes/ services, etc. for serving trusted, secured and privacy preserved services or their users.

References

1. S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf
2. us-fsi-2018-global-blockchain-survey-report.pdf. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-fsi-2018-global-blockchain-survey-report.pdf. (Accessed on12/17/2018).
3. IBM news room - 2017-06-26 seven major European banks select IBM to bring blockchain-based trade finance to small and medium enterprises - United States. https://www-03.ibm.com/press/us/en/pressrelease/52706.wss. (Accessed on 12/04/2018).
4. Sergei Tikhomirov. Ethereum: state of knowledge and research perspectives. In International Symposium on Foundations and Practice of Security, pages 206–221. Springer, 2017.
5. Huasheng Zhu and Zach Zhizhong Zhou. Analysis and outlook of applications of blockchain technology to equity crowdfunding in china. Financial innovation, 2(1):29, 2016.
6. Ori Jacobovitz. Blockchain for identity management. The Lynne and William Frankel Center for Computer Science Department of Computer Science. Ben-Gurion University, Beer Sheva Google Scholar, 2016.

7. Liudmila Zavolokina, Mateusz Dolata, and Gerhard Schwabe. Fintech transformation: How it-enabled innovations shape the financial sector. In International Workshop on Enterprise Applications and Services in the Finance Industry, pages 75–88. Springer, 2016.
8. Kazım Rıfat O¨ zyılmaz and Arda Yurdakul. Integrating low-power iot devices to a blockchain-based infrastructure: work-in-progress. In Proceedings of the Thirteenth ACM International Conference on Embedded Software 2017 Companion, page 13. ACM, 2017.
9. Launching the ether sale. https://blog.ethereum.org/2014/07/22/ launching-the-ether-sale/. (Accessed on 12/05/2018).
10. History of ethereum ethereum homestead 0.1 documentation. http:// ethdocs.org/en/latest/introduction/history-of-ethereum.html. (Accessed on 12/05/2018).
11. Coinbase. https://www.investopedia.com/terms/c/coinbase.asp. (Accessed on 12/05/2018).
12. Joshua R Hendrickson, Thomas L Hogan, and William J Luther. The political economy of bitcoin. Economic Inquiry, 54(2):925–939, 2016.
13. bitpayapi-0.3.pdf. https://bitpay.com/downloads/bitpayApi-0.3.pdf. (Accessed on 12/06/2018).
14. Cryptocurrencies timeline: a history of digital money. https://www.telegraph.co.uk/technology/digital-money/ the-history-of-cryptocurrency/. (Accessed on 12/17/2018).
15. Bnak launches swiftcoin, electronic currency that is safer than cash — business wire. https:// www.businesswire.com/news/home/20121119005937/en/BNAK-Launches-Swiftcoin-Electronic-Currency-Safer-Cash. (Accessed on 12/17/2018).
16. Daniel B Bruno. System and method for providing a cryptographic platform for exchanging debt securities denominated in virtual currencies, July 27 2017. US Patent App. 15/483,190.
17. Yingjie Zhao. Cryptocurrency brings new battles into the currency market. Future Internet (FI) and Innovative Internet Technologies and Mobile Communications (IITM), 91, 2015.
18. Dorit Ron and Adi Shamir. Quantitative analysis of the full bitcoin transaction graph. In International Conference on Financial Cryptography and Data Security, pages 6–24. Springer, 2013.
19. David Yermack. Is bitcoin a real currency? an economic appraisal. In Handbook of digital currency, pages 31–43. Elsevier, 2015.
20. Luqin Wang and Yong Liu. Exploring miner evolution in bitcoin network. In International Conference on Passive and Active Network Measurement, pages 290–302. Springer, 2015.
21. Bitcoin's quirky genesis block turns eight years old today - bitcoin news. https://news.bitcoin.com/bitcoins-quirky-genesis-block-turns-eight-years-old-today/. (Accessed on 12/06/2018).
22. Zibin Zheng, ShaoanXie, Hong-Ning Dai, and Huaimin Wang. Blockchain challenges and opportunities: A survey. Work Paper, 2016.
23. https://medium.com/@UnibrightIO/blockchain-evolution-from-1-0-to-4-0-3fbdbccfc666
24. https://blockchaintechnologycom.wordpress.com/2016/11/21/advantages-disadvantages/
25. https://cointelegraph.com/news/japanese-city-tsukuba-trials-blockchain-based-voting-system
26. Sawal, Neha and Yadav, Anjali and Tyagi, Dr. Amit Kumar and Sreenath, N. and G, Rekha, Necessity of Blockchain for Building Trust in Today's Applications: An Useful Explanation from User's Perspective (May 15, 2019). Available at SSRN: https://ssrn.com/abstract=3388558 or http://dx.doi.org/10.2139/ssrn.3388558
27. BikramadityaSinghal, GautamDhameja and PriyansuSekhar Panda, A Beginner's Guide to Building Blockchain Solutions, book. Apress, 2018.

28. https://www.forbes.com/sites/bernardmarr/2018/02/02/blockchain-a-very-short-history-of-ethereum-everyone-should-read/
29. https://www.coursera.org/learn/cryptocurrency
30. https://bitcointalk.org/index.php?topic=5026914.0
31. JinHo Park and Jong Hyuk Park, Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions, MDPI, doi:10.3390/sym9080164, 2017.
32. Tyagi, Amit Kumar; Nair, Meghna Manoj; Niladhuri, Sreenath; Abraham, Ajith, "Security, Privacy Research issues in Various Computing Platforms: A Survey and the Road Ahead", Journal of Information Assurance &Security . 2020, Vol. 15 Issue 1, p1-16. 16p.
33. Amit Kumar Tyagi, G. Aghila, N Sreenath, "AARIN: Affordable, Accurate, Reliable and INnovative Mechanism to Protect a Medical Cyber-Physical System using Blockchain Technology" Scalable Computing: Practice and Experience, December 2020.