BLOCKCHAIN – An Overview

[1]Mohd Shahique Qamar Siddiqi

[1]Student
[1]Department of Computer Science and Engineering, School of Engineering Sciences & Technology,
[1]Jamia Hamdard, Delhi, India.

Abstract: Blockchain technology works on the distributed ledger pattern wherein the peers' follow-up the chaining approach to maintain a cryptographic hash; mostly considered for cryptocurrencies it has various other applications in terms of supply chain management, smart contracts, decentralized systems and many more. As of the advancement in the field of science, working remotely has now become a trend to maintain the redundancy and privacy of the system; thus the diversified applications of Blockchain technology make it simple and worth it. It can add-on to the IoT sections with the mapping of various devices within a decentralized network. An overview of the blockchain can open-up varied perspectives and increase its future scope in terms of implementation.

The purpose of this research is to understand the blockchain technology, its applications, and challenges faced on getting it functional.

IndexTerms **– blockchain, distributed ledger technology (DLT), blockchain diversity, supply chain, smart contracts, cryptocurrencies.**

I. Introduction

A blockchain, originally block chain, a distributed digital ledger is nothing but a growing list of records, called blocks, that are linked using cryptography. Blockchain ensures traceability, transparency, and security. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data (generally represented as a Merkle tree). [1] Broadly it can be subdivided into three categories:

- Blockchain 1.0 – focusing on cryptocurrencies
- Blockchain 2.0 – smart contracts
- Blockchain 3.0 – applications

Blockchain 4.0 is expected to leverage the implementation of the decentralized network into the industry, enterprise resource planning, and integration of systems.

Characteristics of blockchain technology being:

1.1 Decentralization

Blockchain does not store any of its information in a central zone. Rather, the entire blockchain is replicated and spread over a system of computing devices. At whatever point another block is added to the blockchain, each computing device on the framework revives its blockchain to reflect the change. By spreading that data over a system, as opposed to putting away it in one focal database, blockchain turns out to be increasingly hard to alter. On the off chance that a duplicate of the blockchain fell under the control of a programmer, just a solitary duplicate of the data, as opposed to the whole system, would be undermined.

1.2 Persistency

Exchanges can be approved rapidly and invalid exchanges would not be conceded by genuine excavators. It is difficult to erase or rollback exchanges once they are remembered for the blockchain. Blocks that contain invalid exchanges could be found right away.

1.3 Anonymity

Each customer can coordinate with the blockchain with a created address, which does not uncover the certifiable character of the customer. Note that blockchain cannot ensure the ideal security protection on account of the trademark prerequisite.

1.4 Auditability

Bitcoin blockchain stores information about client adjusts dependent on the Unspent Transaction Output (UTXO) model: Any trade needs to suggest some past unspent trades. At the point when the current trade is recorded into the blockchain, the state of those implied unspent trades changes from unspent to spent. So trades could be adequately verified and followed.

Blockchain technology (Distributed ledgers) have numerous applications in the leading industries based upon the criteria of work, mostly where the central authority is not defined. But as blockchain much more relies on the security and privacy its pre-eminent use lies in the financial sector. In short, when it comes onto maintaining the anonymity of the client-vendor relationship where the retracing of ownership over a hierarchy/chain has to be in such a way that there aren't any loopholes and tracks for hackers to penetrate in; the reason being digital cryptocurrencies (Bitcoin, Ripples, Ethereum, etc.) are the most considered implementation. This technology (merkle tree) was founded back in 1991 by Stuart Haber and W. Scott Stornetta, on the basic idea of preventing the tampering of documents within a timestamp. Afterward, it was conceptualized as blockchain in 2008.

The blockchain is structured so that it is impervious to any further alterations than the default. It is "an open, disseminated record that can record exchanges between two gatherings proficiently and in a certain and perpetual manner". For use as an appropriated record, a blockchain is normally supervised by a circulated framework all things considered sticking to a show for between center point correspondence and endorsing new squares. At the point when recorded, the data in some irregular square cannot be changed retroactively without the modification of each and every resulting square, which requires the understanding of the framework lion's offer. Regardless of the way that blockchain records are not unalterable, blockchains may be seen as secure by structure and exemplify a circled enlisting system with high Byzantine adjustment to non-basic disappointment. The decentralized understanding has thusly been ensured with a blockchain.

Blockchain was created by an individual (or social event of people) under the name entitled, "Satoshi Nakamoto" in the year 2008 to fill in as the open trade record of the cryptographic cash bitcoin. The development of the blockchain for bitcoin made it the chief modernized money to deal with the twofold spending issue without the prerequisite for a trusted in influence or central server. The bitcoin design has breathed life into various applications, and blockchains that are perceivable by general society are extensively used by advanced monetary standards. Blockchain is seen as a sort of portion rail. Private blockchains have been proposed for business use. Sources, for instance, Computerworld called the exhibiting of such blockchains without a genuine security model "snake oil".

II. Related Work/Literature Review:

Blockchain innovation has been anticipated by industry and research networks as a problematic innovation that is ready to assume a significant job in overseeing, controlling, and in particular, making sure about industry adoptions, and measures in businesses. Introduced over a decade, this technology has in numerous applications in terms of distributed ledgers. Popularized with its digital currency's implementation in the year 2008, Bitcoin to be precise, [11] has proven to be revolutionary. This grants cash related trades subject to blockchain development or DLT (for straightforwardness routinely saw as reciprocals) to be executed with Bitcoin being the most observable model in this piece. It is being used as "cash for the Internet", a propelled portion system, and can be seen as the enabling impact of an "Internet of Money". At that point around the year 2013, the innovation saw its second form which was predominantly centered around savvy contracts, little PC programs that "live" in the blockchain. They are self-deciding PC programs that execute subsequently and conditions described already (the help, affirmation, or necessity of the show of an understanding). One significant great position this innovation offers is the blockchain making it hard to change or hack Smart Contracts. So Smart Contracts diminish the cost of affirmation, execution, attestation, and coercion evasion and license clear understanding definition vanquishing the moral danger issue.

Generally noticeable in this field is the Ethereum Blockchain — with its target permitting the execution of Smart Contracts.

Later in the year, 2015 the blockchain adaptation 3.0 was presented with DApps as its major concerned territory. DApp is a shortened structure for decentralized application avoiding united establishment. It uses decentralized limit and decentralized correspondence, so most DApps have their backend code running on a decentralized shared framework, a blockchain. On the other hand, a standard application has its backend code running on brought together servers. [11] A Decentralized Application can have frontend code and UIs written in any language that can make calls to its backend, like a regular App. In any case, a DApp can have its frontend encouraged on decentralized stores, Ethereum Swarm.

Decentralized Application = frontend + contracts (running for instance on Ethereum)

With the foundations laid by the past structures, Blockchain 4.0 depicts plans and approaches that set blockchain advancement usable to business desires. Especially Industry 4.0 solicitations. Industry 4.0 centrality in short terms computerization, adventure resource organizing, and blend of different execution systems. In any case, this cutting edge uprising demands a growing degree of trust and security confirmation — this is the spot blockchain gets to takeover.

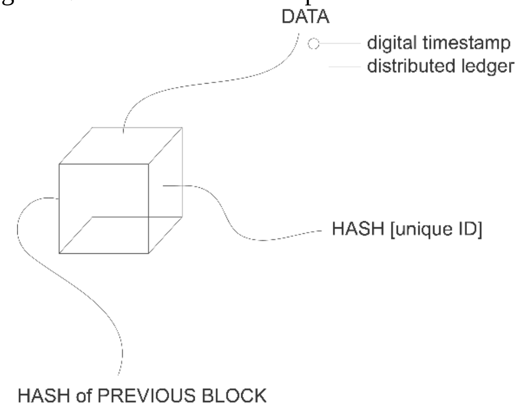
While adding blockchain to IT frameworks one enhances up with business joining, allowing Cross-System/Cross-Blockchain business structures (machines safely and self-administering placing in a solicitation for their new parts to appear). Gracefully chain the administrators, underwriting work forms, money related trades, and condition-based portions, IoT information assortment, wellbeing the board and resource the executives are only a couple of instances of zones that can be enabled by blockchain innovation.

Blockchain 4.0 methods, making Blockchain 3.0 usable considering all the facts, business situations. Fulfilling Industry 4.0 requests by making blockchain guarantees spring up.

III. Structure

A blockchain is a decentralized, distributed digital ledger used for maintaining the transactional records over a changed scope of computing devices so that any included record cannot be adjusted retroactively, without the modification of all the resulting blocks. The authenticity of the blocks must be verified within the network cryptographically. The block structure comprises a block hash value which serves as the unique id, timestamp, data, and hash of the previous block. Probably it is the linked-list that constitutes the blocks and the formation of block-chain. The integrity of the blockchain has been maintained through genesis block by a factor, nonce; it generates a random number for verifying the hash. Since hash values are unique, changes made in any of the blocks will immediately update the hash values thus increasing the reliability factor and making it more secure. According to Swanson (2015), this consensus mechanism ‘‘is the process in which a majority (or in some cases all) of network validators agree on the state of a ledger. It is a set of rules and procedures that allows maintaining a coherent set of facts between multiple participating nodes’’. [2]

Figure 1: Architecture of a simple block



IV. Algorithm

Adding onto the security measures if any of the nodes breakdown, the chain becomes harder to crack thus enhancing the security of the measures. Overall we can conclude that blockchain is highly enforced towards the integrity of data-binding and security thus perfect to implement in the distributed networks. The algorithm it follows is consensus wherein either proof of stake (PoS) [8] or proof of work (PoW) methods can be considered. [4]

For the production and record-establishment of a decentralized network without centralized authority blockchain protocols have to keep the measure by a community of dispersed record keepers, with reduced manipulation and tampering. In a way, that the decentralized consensus must collide-in to a majority to derive meaningful standalone outcomes, with varying and suitable algorithms (swarm optimization techniques, bankers' algorithm over the decentralized channel, ant-colonization, turtle-pattern traceback, etc.) based upon the projected application. To be precise, proof-of-work (PoW) and proof-of-stake (PoS).

Challenges faced are financial risk and security thefts (malware attacks, accidental loss), timelining issues, communication failures, time delays, data loss.

V. Applications

5.1 Blockchain 1.0

Blockchain structures the bedrock for cryptographic forms of money like Bitcoin. Money related measures like the U.S. dollar are overseen and affirmed by a central force, commonly a bank or government. Under the central force structure, a customer's data and money are in reality at the motivation of their bank or government. On the off chance that a customer's bank breakdown or they live in a country with a touchy government, the estimation of their cash may be in harm's way. These are the worries out of which Bitcoin was borne. [5] By spreading its exercises over an arrangement of PCs, blockchain grants Bitcoin and distinctive cryptographic types of cash to work without the necessity for a central force. This decreases chance just as takes out countless the taking care of and trade costs. It also gives those in countries with unsafe fiscal structures continuously consistent cash with more applications and an increasingly broad arrangement of individuals and establishments they can work with, both locally and all around (regardless, this is the goal).

5.2 Blockchain 2.0

Smart Contract was a concept that combines computer protocols with user interfaces to execute the terms of a contract. [5] That is somewhat serving the purpose of digital signing and authenticating the documents globally via the blockchain technology; enhancing the outreach and bypassing the barrier of disconnection is what it surpasses. Smart contracts can be used to control the ownership of properties, stamping of confidential documents digitally, issuing of certificates, two-factor authentication, notary, and bonds.

To an advent, the blockchain technology provides the functionality of establishing smart contracts via cryptographic methods, which embeds the previous history for integrity. In the upcoming era, there is a possibility that the industrial sector might adapt to blockchain technology as the main concern always relies upon the secure and stable system of networks (decentralized is considered to be the safest as for functioning, though cost-effective). Although, financial sectors will be amongst the first to advance to blockchain technology considering the measures of payment settlements, loans, user-privacy, and end-to-end encryption. If once opted for blockchain payment methods would work in real-time mode by adjusting the ledger, which will overrule the market slowdown and the payee settlement considering the bank-vendor scenario.

5.3 Blockchain 3.0

Supply chain management has numerous implementations too; Suppliers can use the blockchain to record the origin of materials that they have purchased. This would allow associations to check the realness of their things, close-by prosperity, and ethics names like "Normal," "Neighborhood," and "Sensible Trade.". The nourishment business is moving into the utilization of blockchain to progressively follow the way and security of nourishment all through the homestead to-client venture.

Block-chain supply chain managements are potential, disruptive technology for design, organization, operations, and general management of supply chains. Blockchain's ability to guarantee the readability, traceability, and authenticity of information along with smart contractual relationships for a trustless environment all portend a major rethinking of supply chains and supply chain management.

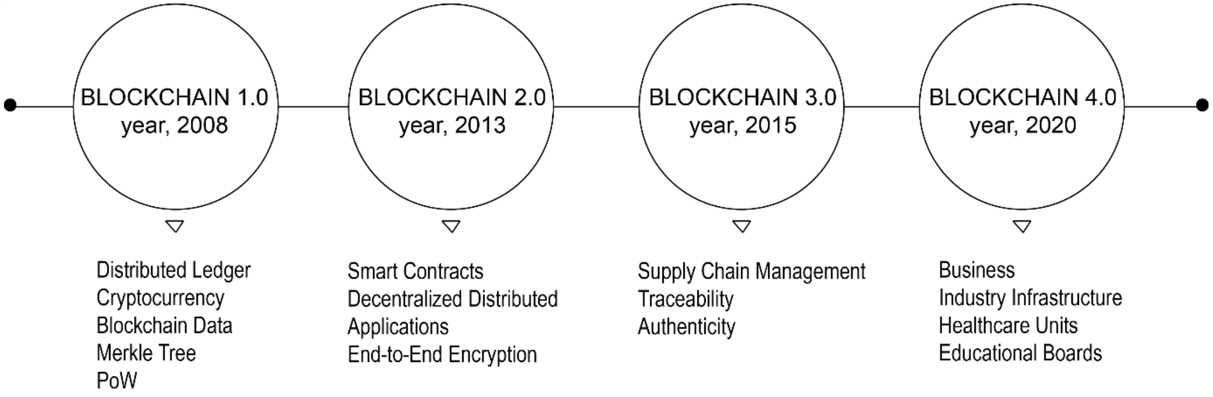
5.4 Blockchain 4.0

Blockchain 4.0 is another age of blockchain innovation. It vows to convey blockchain as a business-usable condition for making and running applications, bringing the innovation completely standard. With the foundations laid by past interpretations, Blockchain 4.0 depicts courses of action and approaches that set blockchain development usable to business desires. Industry 4.0 significance in short terms computerization, adventure resource organizing, and compromise of different execution frameworks. In any case, this mechanical insurgency requests an expanding level of trust and security assurance which can, in turn, be fulfilled by blockchain.

While adding blockchain to IT frameworks one winds up with business reconciliation, permitting Cross-System/Cross-Blockchain business forms, for example, machines securely and self-governing submitting a request for their new parts to show up. Production network the executives, endorsement work processes, monetary exchanges, and condition-based installments, IoT information assortment, wellbeing the board and resource the board are only a couple of instances of territories that can be enabled by blockchain innovation. Blockchain 4.0 strategies, making Blockchain 3.0 usable in genuine business circumstances. Satisfying Industry 4.0 specification by making blockchain ensures come to presence.

Few other implementations can be considered as, car vehicle history (Boch's IoT lab), Notary (digital signing), Insurance, Digital voting (identification, threat-free), tracking package shipment (to maintain integrity) medicines, food industry (tracking, manufacturing - consuming), decentralized system, IoT.

Figure 2: The blockchain timeline



VI. Security

Blockchain and the related advancements offer no immediate and effective solution for cybersecurity issues. In the event that anything, they just reinforce existing endeavors for secure systems, interchanges, and information. [6] Blockchain uses encryption and hashing to store changeless records and a large number of the current cybersecurity arrangements use fundamentally the same as innovation too. Most of the existing safety efforts depend on a solitary believed power to check data or store scrambled information. This leaves the framework powerless against assault, and numerous awful entertainers could concentrate their endeavors on a solitary objective to submit refusal of administration assaults, infuse vindictive data, and coerce information through robbery or shakedown. Blockchains have the high ground overcurrent safety efforts in that obvious blockchains are decentralized and don't require the position of trust of an individual from the gathering or system. The framework doesn't require trust because every hub or part has a total duplicate of all notable data accessible and simply through accomplishing agreement of the lion's share will more information be added to the chain of past data.

The decentralized consensus is maintained by the designs, being proof-of-work (PoW), and proof-of-stake (PoS). [10] PoW rewards record-attendants who illuminate muddled cryptographical riddles to approve exchanges and make new squares (i.e., mining). It forestalls attacks, for example, a denial-of-service(DoS) attack, and guarantees that once one watches a substantial condition of the record, exchanges of a specific age cannot be nullified, because doing so requires the noxious element to have to figure power that can rival the whole system. [7] Therefore, the blockchain accomplishes a carefully designed agreement of the legitimacy of these exchanges. In contrast to PoW, in PoS the maker of the following square is picked dependent on his/her holding of the local cryptographic money (i.e., the stake). Other conspicuous plans incorporate down to earth byzantine adaptation to internal failure calculation (PBFT) and the assigned verification of-stake calculation (DPoS). Instead of contrasting specific structures, we will show decentralized agreement calculation in the reflection to reveal insight into most surviving structures.

Many algorithm designs in their current forms are imperfect, but they have improved quickly and substantially. For instance, several hacking incidents have occurred on blockchains, and Bitcoin has been criticized for wasting electricity, but multiple proposals to address these issues by improving the protocol design and furthering decentralization have been made. Practitioners are actively researching another problem: the lack of consensus when modifying blockchain protocols, which generally leads to forking and temporary confusion about which blockchain users should follow.

VII. Issues

With Proof of Work, the probability of mining a block depends upon the work done by the excavator (for instance CPU/GPU cycles spent checking hashes). Because of this segment, people should combine in order to mining more blocks, and become "mining pools", a spot where holding most figuring power. [10] When it holds 51% preparing power, it can assume responsibility for this blockchain. It causes security issues. In the event that somebody has over 51% processing power, at that point, he/she can find Nonce esteem speedier than others, implies he/she has the position to choose which square is allowable. What it can do is:

- Modify the exchange information, it might cause a double-spending assault.
- To stop the square confirming exchange.
- To stop excavator mining any accessible square.

A greater part assault was progressively plausible in the past when most exchanges were worth significantly more than the square prize and when the system hash rate was a lot of lower and inclined to rearrangement with the approach of new mining advancements.

Another issue is the fork issue. Fork issue is identified with decentralized hub rendition, understanding when the product redesign. It is a critical issue since it is keeping track of a wider range for the Blockchain.

VIII. Pros And Cons

For all its multifaceted nature, blockchain's ability as a decentralized kind of record-keeping is about unbounded. Albeit each innovation accompanies a superior end and with some basic underlying facts that pulls it back, explicitly discussing Blockchain.

Table 1: Pros and cons of blockchain technology

ADVANTAGE	DISADVANTAGE
Improved exactness by evacuating human inclusion in check.	Noteworthy innovation costs are related to mining bitcoin.
Cost decreases by dispensing with outsider confirmation.	Low transaction rate per second.

Decentralization makes it harder to alter.	History of utilization in illegal exercises.
Exchanges are secure, private, and effective.	The vulnerability of being hacked.
Straightforward innovation.	

IX. Conclusion And Future Scope

To conclude, blockchain or distributed ledger technologies can benefit IT industry operations, markets, and consumers. They offer disintermediation, transparency, and tamper-proof transactions. The aforementioned paperwork exhibits the basic functioning of the blockchain technology, the structure of a block, algorithm, and the security measures faced on implementation. Considering the issues, and market adoption with the varying version of technology it exhibits. Blockchain has a high adoption rate due to its property of anonymity and its upcoming integration in the industrial infrastructures are to be awaited.

With the upcoming enhancement in the blockchain technology, introduction and adoption of the measures of its very fourth generation of version, there is a high probability of its acceptance in industry and businesses. The decentralized government can be the very first to ensure its adaptability. Other sectors can be PSUs, healthcare units, and educational sectors as well.

References

[1] Sara Saberi, Mahtab Kouhizadeh, Joseph Sarkis & Lejia Shen (2019) Blockchain technology and its relationships to sustainable supply chain management, International Journal of Production Research, 57:7, 2117-2135, DOI: 10.1080/00207543.2018.1533261

[2] Michael Nofer • Peter Gomber • Oliver Hinz • Dirk Schiereck, “Blockchain”

[3] Blockchain by Melanie Swan, Published by O’Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472.

[4] “Blockchain Disruption and Smart Contracts” Lin William Cong Booth School of Business, University of Chicago and Zhiguo He Booth School of Business, University of Chicago Booth School and NBER

[5] NISTIR 8202 Blockchain Technology Overview by Dylan Yaga Peter Mell Computer Security Division Information Technology Laboratory, Nik Roby G2, Inc. Annapolis Junction, MD and Karen Scarfone Scarfone Cybersecurity Clifton, VA

[6] A systematic literature review of blockchain cyber security by Paul J. Taylor, Tooska Dargahi, Ali Dehghantanha, Reza M. Parizi, Kim-Kwang Raymond Choo

[7] A blockchain based decentralized data security mechanism for the Internet of Things by Chunpeng Ge, Zhe Liu*, Liming Fang

[8] Blockchain without waste: Proof-of-Stake by Fahad Saleh

[9] A Survey of Distributed Consensus Protocols for Blockchain Networks Yang Xiao, Student Member, IEEE, Ning Zhang, Member, IEEE, Wenjing Lou, Fellow, IEEE, Y. Thomas Hou, Fellow, IEEE

[10] A Survey of Blockchain Security Issues and Challenges by Iuon-Chang Lin1,2 and Tzu-Chun Liao2

[11] IoT security: Review, blockchain solutions, and open challenges by Minhaj Ahmad Khana, *, Khaled Salahb