IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

BLOCKCHAIN: AN OVERVIEW

[1]Hitesh Sharma, [2]Yogesh Kumar,[3]Deepak Agrawal, [4]Dr.Nitin Arya

[1]Assistant Professor, [2]Assistant Professor, [3]Assistant Professor, [4]Assistant Professor,

[1]MBA Department

[1]Engineering College Jhalawar, Jhalawar , India

Abstract: Blockchain is the most promising technology of last decade. With features such as decentralisation, persistency, anonymity and auditability, it revolutionised the trade and industries. Blockchain are distributed databases which is unified collection of databases in which information is stored electronically in a digital formation multiple, interconnected computers. Though blockchain technology is outlined in 1991; only after the invention of bitcoin in 2009, it gained prominence and extensive application; due to the important role it plays to maintain a secure and shared recording crypto currency systems. The innovative technology of block chain ensures the integrity and security of the data records and removes the need for a trusted third party to facilitate the transactions. This study focuses on understanding the blockchain and its evolution in real-world.

***Keywords*:** blockchain, distributed-ledger technology (DLT),smart contracts, consensus model; proof of work; proof of stake; crypto currency;

Introduction

Termed as the technology of the future, Blockchain is most discussed technologies in industries nowadays. It has wide range of application in banking and financial-services industries. Blockchain technology was first proposed by, two researchers Stuart Haber and W. Scott Stornetta in 1991 in a quest to build a system in which the timestamps in the digital document could not be tampered. In 2009; a programmer or a group of programmers, who used a pseudonym Satoshi Nakamoto;introduced bitcoin- a decentralized digital currency, which was the first widespread use of block chain technology (1). Blockchain systems have unique characteristics for the banking and financial-services industries. Since blockchain systems operate as decentralized networks, they do not require a central server; all the transactions are recordedby a community of users in a shared ledger within that community. Thus,they do not have a single point of failure. The use of distributed open source protocols ensuresintegrity in the transactions and eliminatesthe needof trusted third party such as a bank, company, or governmentfor the execution of transactions. Once published, transactions arevisible to all parties, they are unchangeable andirreversible;also. It ensures transparency andbuildshigh degree of confidence among contracting parties.

Need of the Study

The block chain technology;though in infancy;is maturing day by day. It is ushering in technological disruptions in the various fieldssuch as cryptocurrency, healthcare. Banking, cybersecurity, intellectualproperty, logistics and supply chain. It is the need of the hour to study the evolution and use of the block chain technology in real-world.

Objectives of the Study

The objectives of this study are as follows:

1. To understand the block chain technology.
2. To study the evolution and adoptionof block chain technology.

Review of Literature

The literature investigated for the present study is focused on two broad areas. In the first area, the studies are based on understanding the block chain and its underlying technology. The second area included studies on the evolution and adoption of block chain technology.

A. Understanding the block chain

Blockchain; though it is conceptualised in 1991, it only gained popularity after its use in cryptocurrencies;the unique features of blockchain technology possesswide-rangingpotential in various areas. To understand the blockchain and its potential, it is important to it is important to understand the fundamental aspects of blockchain technology.

Blockchain: Blockchains are distributed digital ledgers of cryptographically signed transactions that are grouped into blocks. Each block is cryptographically linked to the previous one (making it tamper evident) after validation and undergoing a consensus

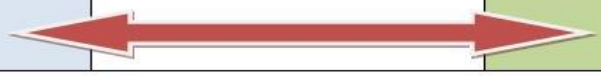
decision. As new blocks are added, older blocks become more difficult to modify (creating tamper resistance). New blocks are replicated across copies of the ledger within the network, and any conflicts are resolved automatically using established rules (2).

Deloitte's Richard Bradley explained the blockchain in a simple and innovative way as "You (a "node") have a file of transactions on your computer (a "ledger"). Two government accountants (let's call them "miners") have the same file on theirs (so it's "distributed"). As you make a transaction, your computer sends an e-mail to each accountant to inform them. Each accountant rushes to be the first to check whether you can afford it (and be paid their salary "Bitcoins"). The first to check and validate hits "REPLY ALL", attaching their logic for verifying the transaction ("proof of work"). If the other accountant agrees, everyone updates their file.This concept is enabled by the "Blockchain technology"(3).

Distributed-ledger technology (DLT): Distribute- ledger is a shared record of data across different parties, sites, locations, countries, institutions and Distributed ledger technology (DLT) is a computerized framework for keeping the record of the transactions wherein the transactions and their details are recorded in numerous places on multiple nodes simultaneously in an accurate and secure manner with the use of cryptography. Dissimilar to conventional databases, Distributed-ledger records doesn't use centralised data stores and central administrator. In it the data records are shared, replicated, and synchronized amongst the members of decentralised network.

'Distributed ledgers' (DLs) are a specific implementation of the broader category of 'shared ledgers', which are simply defined as a shared record of data across different parties. A shared ledger can be a single ledger with layered permissions or a distributed ledger which consists of multiple ledgers maintained by a distributed network of nodes, as defined above. In this document, we are commonly using the term distributed ledgers (DLs), and specifically use the term blockchain only when referring to DLs that use a blockchain data structure (4).

Collomb, A & SOK, K. ,sums up the key differences between the standard transactional model (so far quasi-unique and certainly prevalent) and the decentralized approach that DLT provides (the so-called blockchain transactional model) with the help of following table (5) .

Standard	Model	Block chain
Trusted third-party/Central Coordinator	Paradigm	Trustless System/ Pseudonymous Participants
Centralized Server/Many Clients	Architecture	Peer to Peer Network
Single copy	Database	Multiple Access
Controlled Access/ Firewalls	Security	Cryptography
Intermediation	Price/Cost	Consensus/ Proof of work
PRIVATE		PUBLIC

Standard vs Blockchain transactionalmodel: Collomb, A & SOK, K. (5)

Smart contracts: As defines by Cong, L W & He, Z "Smart contracts are digital contracts allowing terms contingent on decentralized consensus that are tamper-proof and typically self-enforcing through automated execution"(6). Smart contracts are computer programs stored on a blockchain which are supposed to run when the pre- agreed conditions are met. Usually smart contracts are used to automate the execution of an agreement and at the same time participants can be made certain of the outcome, in spite of involvement of any intermediary's or time loss.A smart contract comprises the standards that members have altogether settled upon to oversee the development of facts in the distributed ledger. Smarts contracts guarantees that all exchanges consent to the basic lawful arrangements and that the records oversaw by DLT are legitimate. With the potential to automate laws and protocols, Smart contracts improve accuracy, efficiency and transparency thus extensively used inGovernment voting system, Healthcare, Supply chain and financial services.

Consensus Model: Consensus models forms the core of the blockchain networks.It is a method through which every one of the peer nodes of the Blockchain network comes to common agreement about the current situation of the distributed ledger. Thus, agreement calculations accomplish reliability and ensure trust between obscure peer nodes in adistributed computing environment. Basically, the agreement convention ensures that each new block that is added to the Blockchain is the unique version of truth that is settled upon by every one of the peer nodes in the Blockchain.The Blockchain agreement convention comprises of a few explicit goals like coming to an arrangement, joint effort, co-activity, equivalent freedoms to peer node, and required support of every peer nodes in the agreement interaction. These mechanisms aim to ensure that all participants deal with identical copies of the distributed database files in immutable, private, secure, and transparent manner.

Currently most common consensus algorithms used by blockchain projects are: Proof of Work (PoW), and Proof of Stake (PoS).

Proof of work: The term "proof of work" was first used by Markus Jakobsson and Ari Juels in a paper in 1999 (7).It is the original consensus algorithm in a blockchain network which is used to confirm the transaction and creates a new block to the chain. This algorithm uses competitive validation model, inwhich minors (agroup of people who participates in blockchain transactions) compete against each other to complete the transaction on the network and add new blocks to the blockchainand also verifying the transactions and ensures that these additions are accurate.

Proof of stake: Proof of stake is a cryptocurrency consensus mechanism for processing transactions and creating new blocks in a blockchain.Proof of stake decreases the computational work required to verify blocks and transactions in the blockchain. To become a validator; it requires participants to have high level of technical knowledge as well has they have to put some minimum amount of cryptocurrency as collateral which is called "stake" for the chance to successfully approve transactions and earn a reward in return. The amount of return is in proportion to the amount of crypto each validator has in the pool and the length of time they've had it there.

Cryptocurrency: Cryptocurrency or Digital money is assortment of binary data which is designed to work as a medium of exchange. It is a type of payment that can be done digitally, which doesn't require any third party such as a government or bank to facilitate the transaction.It uses cryptography that empowers individuals to purchase, sell or exchange crypto safely.D S Soegoto and I Ramadhan in their paper discussed that any cryptocurrency is encrypted information in the form of a cryptographically protected record designating a certain value and certifying the possessor's ability to use this value at his own discretion. From this position, cryptocurrency is similar to non-documentary securities that certify property rights. Since cryptocurrency itself embodies the value that comes from the economic costs of using the computing power of computers in the blockchain network, it can also be considered as a commodity. However, by its functions, cryptocurrency is closest to money (8).

B. Evolution and adoption of block chain technology

Like some other innovations, the Blockchain Technology, also evolved with time. The advent of advancement in the technology revolutionised the way of doing business in diverse fields. The blockchain innovation was depicted in 1991 by the researcher Stuart Haber and W. Scott Stornetta. They needed to present a computationally pragmatic answer for time-stepping computerized records with the goal that they couldn't be antedated or altered. They foster a framework utilizing the idea of cryptographically tied down chain of blocks to store the time-stepped records.

In 1992, Merkle Trees were introduced into the design, which makes blockchain more effective and productive by permitting many documents to be gathered into one block. Merkle Trees are utilized to make a chain of block which is safe and secure. It stores a series of information records, and every information records associated with the one preceding it. The most current record in this chain contains the historical backdrop of the whole chain. Nonetheless, this innovation was not utilised by anyone, even its patent got expires in 2004.Blockchain, however new, has evolved into three generations. Each of the three generations proceeded to develop and make their own space in the business and attempting to arise as victors in the profoundly intertwined space. The three blockchain ages are:

First - generation blockchain (Bitcoin and Digital Currencies): The blockchain technology was in existence since many years, but it got prominence;only after its use in bitcoin network ;as proposed by developer Satoshi Nakamoto, at this stage it exhibited the capability of the innovation in the proliferation of cryptocurrencieswhere it is used to develop shared-ledgers which support cryptocurrency networks. It also faced significant difficulties such as, slow transactionconfirmation, delayed final settlement, privacy issues and high energy utilization in mining.

Second - generation blockchain (Smart Contracts):With the passes of time the developers realised numerous intrinsic benefits other than merely documenting and keeping the record of transactions.This generationof blockchain, as envisioned by the founders of Ethereum by developing smart contracts, were centred around building a versatile ecosystem that could be utilized to help the development of decentralized applications. The significant difficulties were Interoperability between different platforms, Limited protection, Limited throughput or efficiency.

Third - generation blockchain: The third - generation of Blockchain is focused on discovering and implemented the new applications of blockchain technology by addressing the issue of scalability as well as overcoming the challenges faced by previous generations of blockchain. It is based on premises of providing higher throughput by enabling faster Interoperability, industry-wide implementations, better security, more cost-effectiveness, lower energy consumption and better sustainability.

Blockchain real-world use cases: Firms across the diverse business areas are realising the numerous benefits and potential of the blockchain innovations. The blockchain technology suppliers are also constantly developing customised solutions for them. Blockchain has been proposed to be used in different applications and use cases across diverse industries.

A brief overview of each domain can be presented using the following table (9).

Sector	Use-cases
Financial Services	Trade finance , Securities issuance , Derivatives settlement, Dispute management , Forex trade , Fund processing ,Risk management , Secure record keeping , Identity management
Banking	Asset certification , Trade finance , Cross-border payment , Client on boarding ,Audit trail , Inter-bank payments , KYC , Syndicated loans , Identity management
Insurance	Claims management , Reinsurance , Contract authentication , Customer data-sharing, Insurance marketplace , Insurance records ,KYC ,P2P Insurance
Government and Non-Profit	Asset registration, Asset tracking , Digital land and vehicle registry, Digital currency , Digital identity , Digital voting , Food distribution ,Secure travel for refugees
Healthcare and Life Science	Cold chain tracking ,Drug provenance , Health records , Organ registry, Pharma track-and-trace , Physician recertification , Provider data management
Manufacturing Supply Chain	3D design records , Anti-counterfeiting ,Digital provenance ,Preventive maintenance , Supply chain management ,Warranty and payments
Retail and CPG	Distributed marketplace ,Food auditing ,Inventory control, Loyalty programs , Procurement optimization , Supply chain traceability
Travel and Transportation	Cargo track and trace , Damage tracking , Preventive maintenance ,Ticketing , Customer data sharing , Shipping documentation
Technology, Media and Telecom	Product provenance , IP management , Fraud detection, Micropayments , Media IP protection ,Loyalty programs
Utilities and Resources	Electricity grid management,Energy trading,Shared equipment , Green certification , Produce logistics ,Wholesale energy supply

Conclusion

Blockchain technology is definitely one of the greatest innovations of man. The recognition of its advantages and adoption in diverse fields, resulted in, exponential and disruptive growth in the Blockchain technology. As the computerized and actual physical worlds converge, the practical pragmatic uses of Blockchain bound to develop and grow by leaps and bounds. The business value added by blockchain will grow to billions in the coming years, and to trillions in near future. This paper has briefly presented the overview of Blockchain and its different emerging applications and use cases.

References

1. Nakamoto, S. (2008) "Bitcoin: A Peer-to-Peer Electronic Cash System," October 2008, Online:https://bitcoin.org/bitcoin.pdf
2. Yaga, Det al.(2018),“Blockchain Technology Overview”, NISTIR 8202.NIST,Online:Blockchain Technology Overview (nist.gov).
3. Bradley, R, (2018): Blockchain explained... in under 100 words, Online : https://www2.deloitte.com/ch/en/pages/strategy-operations/articles/blockchain-explained.html
4. Natarajan, H et al. (2017), Distributed ledger technology (dlt) and blockchain,FinTech Note - No. 1, International Bank for Reconstruction and Development / the World Bank, Online:https://openknowledge.worldbank.org/bitstream/handle/10986/29053/WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf?sequence=5
5. Collomb, A &SOK, K. (2016):“Blockchain / Distributed Ledger Technology (DLT): What Impact on the Financial Sector”,Digiworld Economic Journal, No. 103, 3rd Q. 2016, p. 93.
https://www.investopedia.com/terms/b/blockchain.asp
6. Cong, L W &He, Z (2018): Blockchain Disruption and Smart Contracts,NBER Working Paper Series, National Bureau of Economic Research, Online :https://www.nber.org/papers/w24399
7. Jakobsson , M & Ari Juels, A (2000): Proofs of work and bread pudding protocols, Springer Science+Business Media Dordrecht 1999, Online: https://link.springer.com/content/pdf/10.1007/978-0-387-35568-9_18.pdf
8. Bolotaeva O S et al (2019). “The Legal Nature of Cryptocurrency”, IOP Conf. Ser.: Earth Environ. Sci. 272 032166 Online: https://iopscience.iop.org/article/10.1088/1755-1315/272/3/032166/pdf
9. Rawat, D.B.et al (2019) : Blockchain: Emerging Applications and Use Cases, Online:arXiv:1904.12247v1 [cs.CR] 28 Apr 2019