

Evolution of Blockchain Technology in Business Applications

Saugata Dutta

Research Scholar, Galgotias University,
Greater Noida, Uttar Pradesh, India

Dr. Kavita

Galgotias University,
Greater Noida, Uttar Pradesh, India

Abstract: Blockchain technology is an invention where digital transactions refer to distributed database without the need of third party intervention and authentication. In present time several organizations in various disciplines are adopting this technology which has transparency, integrity, efficiency in cost and time. Its unique technology is being adopted in various industries like banking, legal, healthcare, rentals, education and many more. The intention of this paper is to outline the Blockchain technology and its function in various domain.

Keywords—Blockchain, bitcoins, cryptocurrencies, smart contracts, decentralization, encryption.

I. INTRODUCTION

A Blockchain is a chain of blocks of information which are hashed and distributed making it more secured and transparent. With the advent of hashing in individual block it becomes nearly impossible to change or tamper with any of the block. If any of the block is changed then the entire chain of block becomes invalid because each block stores the hash of the previous block, the security mechanism uses a term called "Proof of work" which actually slows down the creation of new block. If any of the block is tampered, then all following blocks needs to be recalculated. The security of Blockchain technology comes with the combination of hashing and proof of work. But there is another technology behind it which makes it unique and that is data distribution. It uses P2P rather than a centralized server which is more prone for tampering. Every individual who joins the network gets a copy of the block chain. If a new block is created, then everyone in the network gets a copy of the new block and each node verifies that none of the block is tampered with and then the new block is added to the Blockchain of new node.

In the primitive use of Blockchain, it was first designed by Ralph Merkle in 1979. This design of tree structure came to be known as Merkle tree where series of records are connected with the previous record using hashing such that no records is altered and a proof of integrity.

The history of Blockchain started from 1991, when two research scientist named Stuart Haber and W. Scott Stornetta introduced a computational theory for time stamping digital documentation such that it cannot be made backdated or tampered.

In 1992, Merkle tree was incorporated by putting several digital documents in one block, but however the technology went unused.

In 2004, Hal Finney a cryptographic activists introduced a system named RPoW which is known as Reusable Proof of Work (RPoW) which used non exchangeable hashcash based proof of work token and in return creates a RSA based signed token that can be transferred from person to person. It also consists of a trusted server which users can verify the

correctness and integrity in real time. It is considered to be the early step for crypto currencies.

In 2008, the blockchain was first theoretically conceptualized by Satoshi Nakamoto. The design was then improved in a significant way using a hash cash like method in order to add blocks to the chain without the involvement or signed by a trusted party. [1]

In 2008, Satoshi Nakamoto introduced the Blockchain technology with bitcoins a digital cryptocurrency. A decentralized, peer to peer and electronic cash system. Rather than using a hardware trusted computer system, the underlying layer of crypto currencies used the Blockchain mechanism which practices decentralized, peer to peer protocol for verifying transactions. This Blockchain technology thus has a secured history of exchanges, uses peer to peer network for timestamp as well as verification and without the need of third party authority intervention.

On 3rd Jan 2009, bitcoin came to existence using the Blockchain technology when the first bitcoin block was mined by Satoshi Nakamoto with 50 bit coins The first recipients of bitcoin was Hal Finney who received 10 bitcoins from Satoshi Nakamoto and it is said to be the first official transaction underlying the technology with Blockchain.

The Blockchain size file size has increased to an exponential level since 2014 which was 20 GB [13]. The size was 30 GB in 2015 and in next 2 years the size increased to 100 GB for Bitcoin Blockchain [1].

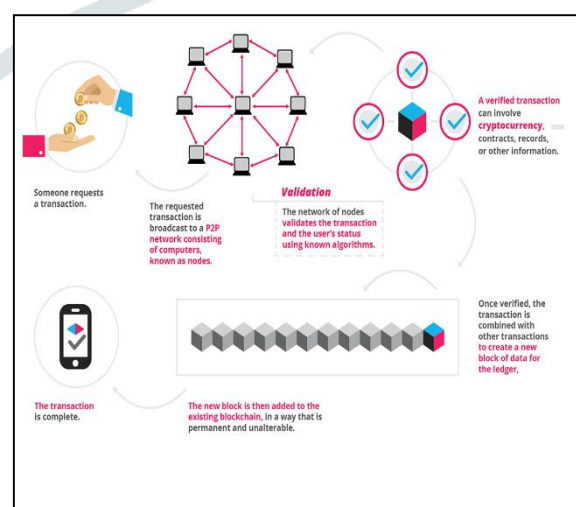


Fig 1: Basic Blockchain transaction model [2]

The basic model of Blockchain technology states that when a transaction request is initiated, the requested transaction is broadcasted to a network of computers in a peer to peer network. Nodes in the network validates the transaction with

a predefined algorithm. The transaction can be of any nature starting from banking, cryptocurrencies, contracts or any other type of information. The transaction once verified is then added to other transactions to create a new block of data for ledger. This new block is then added to the existing Blockchain with a set of predefined rules which is unalterable and transparent. The transaction is said to be completed.

II. REVIEW LITREATURE

Pascal Mehrwald et al. suggested a conceptualized model in combining Blockchain technology and smart contracts which can advance trust in sharing economy suggesting moderating effects in online settings [4].

A Muthanna et al. proposed an algorithm to use a Blockchain mechanism in IOT devices for decentralization in a trustful manner [5].

Florian Glaser et al. outlines the use of Blockchain technology as a platform where the transparent, autonomous and distributed nature will reduce the security risk. [6].

Xiwei Xu et al. applied a Blockchain mechanism in a project called originChain. When this technology is used it provided transparent and tamper proof traceable data which included high availability. There is a large impact on the quality of the system with the structural design of the system [7].

Paula fraga-lamas et al. suggested an approach of using Blockchain technology in automotive industry putting emphasize on cybersecurity. The exploration raised an opportunity to create new business model and can even create a disruption in car sharing. SWOT analysis has been done for the same with some recommendation and future developments [8].

D Dujak et al. outlines the use of Blockchain in logistics and supply chain using distributed ledger technologies. This paper also discusses about the future applications of Blockchain in logistics and supply [9].

Asad Ali et al. discusses the advent of Blockchain technology in healthcare industry which has changed the model of traditional health care system with effective diagnosis and secure data sharing. This paper also discusses with the Blockchain applications in healthcare domain with challenges and future aspects. [10].

Axin Wu et al. outlines the attribute based encryption where Blockchain technology is used to guarantee the integrity and non-repudiation of data. When a secret key is abused the source can be audited where it shows the proposed system is efficient and secured [11].

Cao, Y et al. discussed the feasibility of using Blockchain technology in energy industry and also discussed the applied methodology by the pioneers. This paper also discusses the application practices of Blockchain technology in domestic and over-seas and also the challenges [12].

Olga Labazova et al. demonstrates various Blockchain based systems contributing new technical dimensions and linking applications. This paper also presents an overview of current Blockchain based system [13].

III. BLOCK CHAIN TECHNOLOGY

A Blockchain is basically a distributed ledger that is transparent to everyone. If any transaction is recorded in Blockchain, it is difficult and nearly impossible to alter the data. Combination of block forms Blockchain.

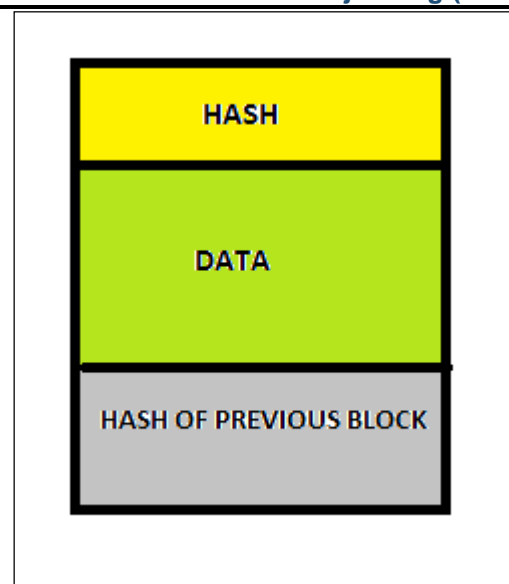


Fig 2: Blockchain Block

A block contains hash, data and hash of the previous block refer Fig (2). Type of data may be depending on the type of Blockchain application. A hash may be considered to be a fingerprint and it always a unique. When a block is created, its hash value is created. If there is a change in the block, the hash value also changes. Data entity is information that is stored. In case of bitcoin, it may store the information like sender, amount and receiver. Previous hash consists of the hash value of the previous block which is attached to the following block and thus creating a chain of block and this is the unique feature that makes it secured.

Each block is connected with the following and previous block. In this case as per fig (3), block 3 is points to block 2 and block 2 is points to block 1. The first block is known as the genesis block as it is the first one and cannot point to the previous block.

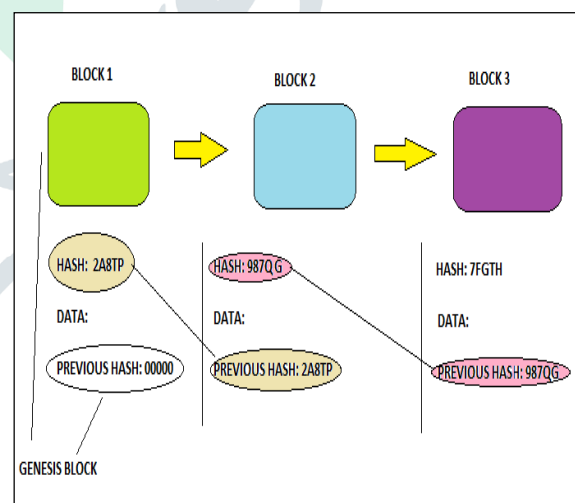


Fig 3: A Blockchain architecture

Now if block 2 is tampered, then the hash value of block 2 will change and make all following blocks invalid. Since hashing layer is not only the protection shield because the technology and hardware has greater resources which can calculate humongous number of hashes per second and recalculate hashes of following blocks and make valid again. There is a mechanism which is known as the proof of work which slows down the process of block creation. If we take the example of bitcoin, it takes ten minutes to recalculate the proof of work and in context to add a new block to the chain. So it makes nearly impossible to tamper a block

because the proof of work then needs to be calculated for all following blocks. Apart from this feature, there is another layer which makes it more secured is the distributed network. Rather than depending on a central entity to manage, Blockchain depends on the P2P network. In this network everyone allows to join where each one which may be precisely call a node gets a copy of the Blockchain. Each node can verify the integrity. When a new block is created by a node, each node verifies the integrity of the block such that the same is not tampered with. Once the verification is done, each node then adds the new block to its chain. Tampered blocks will be rejected by the nodes in the Blockchain network. in order to successfully tamper a Blockchain, one needs to tamper all the blocks then recalculate the proof of work of all blocks and take control of more than 50% of the nodes in the P2P network which is nearly impossible to perform.

IV. BLOCKCHAIN FUNCTIONS IN BUSINESS APPLICATIONS

There are various segmentation of business lines where blockchain being or can be used with great prospects which is resilient, secured, authentic and tamper free. These are some of the areas where Blockchain has been used and in some areas Blockchain technology research and study is still in process.

1. Smart Contracts: Smart Contracts are just like contracts as in a real world but are digital in form. A tiny computer program stored in a Blockchain. Both the parties can agree to a certain terms and condition which are digitally embedded and when certain rules are met the agreement is automatically enforced. The smart contract resides in Blockchain and hence cannot be tampered. The smart contracts eliminate the need for any centralized authority.

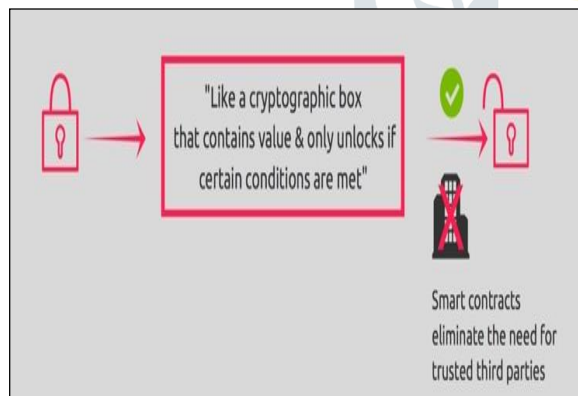


Fig 4: Smart contracts [14].

However smart contracts should not be compared with the legal contracts in the present time but there is a future possibility to become legal contracts provided some criteria are met. Once some legal standards are specified and followed, we may experience a widespread usage of legal contracts in form of smart contracts accepted by court of law [14].

2. Cryptocurrencies: are virtual and digital currencies that uses cryptography and Blockchain to secure and a medium to exchange. There are limits of units that can exists. With Blockchain technology the transfer of funds is easily verifiable. There is no central authority and works in a

decentralized manner. Allow new units to be added when certain conditions are met. Blockchain acting as a public ledger where every user can see each other's transactions and balance. The reason it is known as currency because it uses private and public key for encryption and decryption. The public key is the wallets address. The miners get rewards when they confirm the transactions and that's how the nodes add the block to the database. The most common cryptocurrencies are Bitcoins, Ripple, Litecoin, Ethereum, NEM and IOTA.

3. Sharing Economy: The sharing economy is a concept where an individual lease outs its assets to be used by others. But there had been issues in terms of cost effectiveness and privacy.

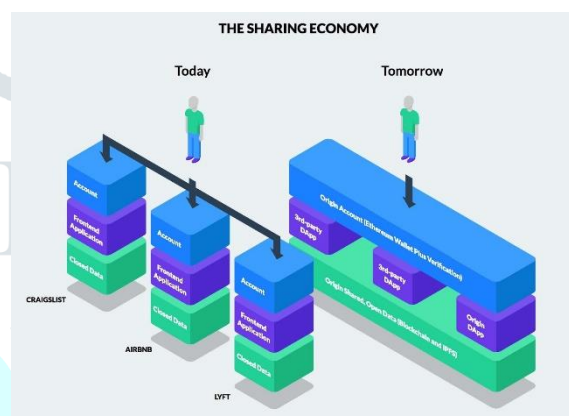


Fig 5: Sharing economy [15]

With the advent of Blockchain technology it eliminates the need of various transaction fees which makes it more convenient to use with transparency. Involvement of any third party authority is not required. In context to the above some of the organization started developing the Blockchain network where buyers and sellers can meet, browsing the menu of products and payments. Blockchain is making way creating decentralized trust on sharing economy providing transparency and security with its peer to peer network. The paradigm will change the outlook of the customers and sellers with this technology.

4. Crowd funding: There are several traditional methods such as funds through bank, self and ventures. There are several pre-requisites in each of the examples like limited funding, good revenues from existing business and lastly demanded product. Existing crowdfunding still has jargons in the model with not reaching the target goals. With the advent of Blockchain technology and digital cryptocurrencies, this has facilitated companies to create their own stock in order to get funded from the public in the form of cryptocurrencies for investments and some assured returns. The transparency and security of Blockchain technology is helping to augment in this line of business.

5. Governance and Control: Blockchain technology being transparent and secured, public data can be easily published with the help of this technology naming a few like public opinions, polls, shares, election, results and surveys. This actually means company governance becomes more verifiable and transparent.

6. Supply chain management: In the supply chain management, once the product is passed from different movement, the transactions are recorded with full product history that cannot be changed from manufacturing to sales. This will help in recording, assigning, sharing, linking and tracking.

7. Digital Storage: Blockchain in digital storage is however a recent invention. The blockchain technology which is decentralized is consuming less bandwidth as the downloading are done from different nodes which can be a financial benefit. The data is distributed to various nodes without compromising the security with minimum cost. It's an advantage in terms of scalability as well where encrypted data is stored on network of decentralized nodes.

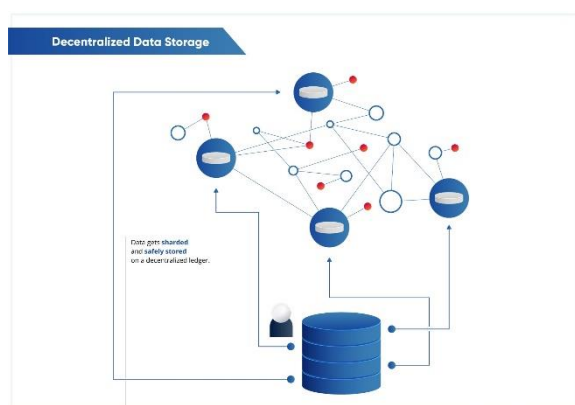


Fig 6: Decentralized Data Storage [16]

8. Protection of intellectual property: There is actually no guarantee of online contents to be stolen especially if it is designed and created by the originator. These medias are stolen without the consent and perhaps no one knows the actual owner. There is no enforcement that is hard enough to protect the same. With the help of Blockchain technology, there are no stones unturned to protect the intellectual property. The smart contracts are the best way to automate the sales without compromising the security and intellectual property of the media through blockchain based service. Any media can be sold directly to the customers through blockchain technology with smart contracts and micropayments.

9. Internet of Things (IOT): However, there are actually various challenges to incorporate full-fledged to Blockchain. There are various surveys which has questioned about the security of IOT devices. Blockchain technology can overcome the issue. In an IOT Blockchain network, the records are immortal with its history. This will enable smart devices which can exchange data and even carry on a financial transaction without any third party authority. With the help of IOT blockchain technology, smart devices can provide a complete report of the failures of parts which requires replacement. For industrial IOT applications, the capability of Blockchain technology in context to distributed ledger and decentralization which enables many regulatory and compliance.

10. Know your customer and Anti-money laundering: KYC costs can be minimized through cross institution client verification. Fraudulent can be minimized or in fact be stopped with this blockchain technology. With

the distributed ledger, any suspicious transactions can be detected. there are certain apps which takes the snapshot of the identification and key documents like passport, identification card etc. and after verification from the concern body, data is then stored in Blockchain with encryption.

11. Stock Trading: Blockchain technology can make the stock industry more optimal through its decentralization and automation. This will help in settlements, processing post trade with paperwork which is ease of use and ownership transfer. This will also eliminate the use of any third part authorities as with the help of smart contracts to register the transactions. This will help in fairness and transparency, post trade automation, higher liquidity, reduced transaction costs.

12. Land title registration: With the use of Smart contracts, land registration title is permanently fixed with the system, tamper free, authentic and can be seen by any party. The buyer will this be assured that the land document is forge free and the owner of the land is genuine including the history of the land details with real time traceability and transparency in property.

13. Health care: Blockchain technology has more potential for health information exchange with efficiency and security. However, this is still under review for a nationwide blockchain network for medical records of patients. There are various medical institutions which does medical research on drugs or diseases which can be stored in a blockchain which is transparent, genuine and tamper free. Insurance fraud can also be detected with the use of Blockchain.

V. CONCLUSION

Blockchain technology with its distributed ledger, smart contracts and decentralized nodes offers great future and revolutionary technology as against the traditional technology in various lines of business. Bitcoin or crypto currencies is one of the revolutionary product using the technology has attracted audiences across the world. Not only restricted to crypto-currencies, Blockchain mechanism has great future scope which can be used in more sectors.

ACKNOWLEDGEMENTS

My sincere thanks to my professor and guide who has supported me enormously for accomplishing.

REFERENCES

- [1]<https://en.wikipedia.org/wiki/Blockchain>
- [2]<https://blockgeeks.com/guides/what-is-blockchain-technology>
- [3]<http://www.ledgerprojects.com/how-a-blockchain-works-lets-make-one/>
- [4] Mehrwald, Pascal., Treffers, Theresa., Titze, Maximilian., and Welp, M. Isabell., "Application of Blockchain Technology in the Sharing Economy: A Model

of Trust and Intermediation”, Hawaii International Conference on System Sciences, 2019, pp. 4585-4594.

[5] Muthanna, A., A. Ateya, A., Khakimov, A., Gudkova, I., Abuarqoub, A., Samouylov, K., & Koucheryavy, A. (2019). Secure and Reliable IoT Networks Using Fog Computing with Software-Defined Networking and Blockchain. *Journal of Sensor and Actuator Networks*, 8(1), 15. doi: 10.3390/jsan8010015

[6] Glaser, F., Hawlitschek, F., & Notheisen, B. (2018). Blockchain as a Platform. *Business Transformation through Blockchain*, 121–143. doi:10.1007/978-3-319-98911-2_4

[7] Xu, X., Lu, Q., Liu, Y., Zhu, L., Yao, H., & Vasilakos, A. V. (2018). Designing Blockchain-based applications a case study for imported product traceability. *Future Generation Computer Systems*. doi:10.1016/j.future.2018.10.010.

[8] P. Fraga-Lamas and T. M. Fernández-Caramés, "A Review on Blockchain Technologies for an Advanced and Cyber-Resilient Automotive Industry," in *IEEE Access*, vol. 7, pp. 17578-17598, 2019. doi: 10.1109/ACCESS.2019.2895302

[9] Dujak, D., & Sajter, D. (2018). Blockchain Applications in Supply Chain. *EcoProduction*, 21–46. doi:10.1007/978-3-319-91668-2_2

[10] Siyal, A., Junejo, A., Zawish, M., Ahmed, K., Khalil, A., & Soursou, G. (2019). Applications of Blockchain Technology in Medicine and Healthcare: Challenges and Future Perspectives. *Cryptography*, 3(1), 3. doi:10.3390/cryptography3010003

[11] Wu, A., Zhang, Y., Zheng, X., Guo, R., Zhao, Q., & Zheng, D. (2019). Efficient and privacy-preserving traceable attribute-based encryption in Blockchain. *Annals of telecommunications*. doi:10.1007/s12243-018-00699-y

[12] Cao, Y. (2019). Energy Internet Blockchain technology. *The Energy Internet*, 45–64. doi:10.1016/b978-0-08-102207-8.00003-5

[13] Lavazova, Olga and Dehling, Tobias and Sunyaev, Ali, From Hype to Reality: A Taxonomy of Blockchain Applications (2018). *Proceedings of the 52nd Hawaii International Conference on System Sciences (HICSS 2019)*, January 8-11, 2019, Wailea, Maui, HI, USA.

[14] <https://blockchainhub.net/smart-contracts/>

[15] <https://hackernoon.com/blockchain-is-the-infrastructure-for-a-new-decentralized-sharing-economy-f715da32bece>

[16] <https://lisk.io/academy/blockchain-basics/use-cases/blockchain-data-storage>