The Future of Blockchain Technology

Arshiya Sharma*

Student, Class 12th, Welham Girls School

Abstract- Blockchain, the next generation of the Internet, has already made a significant impact in the real-time operations of the financial sector over the past decade. Cryptocurrency, the Internet of Things (IoT), financial services, etc. all benefit from its robust set of tools, which facilitate the cross-pollination of these and other technologies. Decentralization & long-term reliability are the two most crucial aspects of Blockchain technologies. Despite the fact that Blockchain & Bitcoin technologies are both beneficial, they are nonetheless often confused with one another. In addition, this article distinguishes between the two with the help of the smart contract's development & highlights the potential advantages of blockchain technology. While several research have focused on how blockchain can be used in specific contexts, neither the technology nor its potential uses have been systematically surveyed. We undertake an extensive assessment of blockchain technology, architecture, analyzes blockchain applications, & technical problems to address this knowledge gap.

Keywords- Blockchain, Bitcoin, Application, Architecture, Limitation

- X -

INTRODUCTION

A blockchain is simply one kind of distributed ledger; not all DLTs use blocks or chains to record transactions. The blockchain is an unalterable digital ledger that records transactions in an economy. It may be used to keep track of anything of value, not only money. The 2016 book "Blockchain Revolution" by Don & Alex Tapscott. A blockchain (from the two words "block chain") is a growing list of digital records stored in connected & encrypted blocks. These "blocks" of information are stored sequentially in a digital format [G. Eason 1955]. Each block in the chain is timestamped, hashed cryptographically, and contains data (such as a Bitcoin transaction). To ensure that no data in the entire "blockchain" has been altered, each block of hashed data relies on the one that came before it in the chain [I. S. Jacobs 1963], [Shuai Wang 2018], [ZainabAlhadhrami 2017].

Blocks of data are linked together in a blockchain. Data mining collects & organizes data into blocks, each of which has a certain amount of data. A cryptographic hash and time stamp serve as unique identifiers for each block. Each new block in the blockchain includes a hash of the prior block in the chain, creating an immutable record of all transactions since the creation of the first block, known as the Genesis Block. To expand and sustain the network, this procedure is continuously revived. This means that no bank or government can censor transactions on this distributed ledger. Everyone with a reliable internet connection can actually get to it. In addition to cryptocurrencies, blockchain is being implemented by a wide variety of industries, from messaging apps & critical infrastructure protection to ride sharing and cloud storage.

BLOCKCHAIN ARCHITECTURE TYPE

Numerous blockchain architectures, each with its own unique structure & design.

A. Public Blockchain

Everyone in the organization can agree to the trade in this kind of blockchain, and everyone can take part in the discussions that lead to the consensus. By establishing a square of dispersed trades, it ensures decentralization. Before every transaction is added to the framework, it is integrated with the blockchain. As a result, it may be verified and fine-tuned with each department. Any participant with a computer and network access can act as a central node and view the whole blockchain record. It specifies that any interested party may observe the exchange, check its legitimacy, and even take part in the bargaining. Client confidentiality and complete transparency in the public organization's record are two of its advantages.

B. Private Blockchain

Access to data on this blockchain is strictly controlled by a central authority, & participation by nodes is limited. When it comes to controlling who can access what data on a private blockchain, things are strictly monitored. Nodes in the network cannot take part in the process of validating and verifying financial transactions. Each transaction, on the other hand, is started, verified, and validated by a third-party corporation or organization. As a result, the process of confirming & validating financial transactions is streamlined. When opposed to public blockchains, private blockchains offer a greater level of anonymity because they allow the organization to choose the access rights to individuals. A private blockchain works well for a conservative company with a well-established management structure. Bringing the company into the 21st century through the use of a private blockchain. Private blockchains are more likely to be used by private companies or government agencies since they allow for the presence of a central authority with improved security, efficiency, & speed.

C. Consortium Blockchain

Consortium blockchain can be thought of as semi-decentralized because it combines public & private blockchains. While anyone can join one of these blockchains, not all participants will have access to the same data. Access permissions are context-dependent, and blocks are checked against a set of rules. As a result, consortium blockchains are only "semi-decentralized." Consensus in consortium blockchains is managed by a group of trusted nodes chosen in advance. After a group of nodes reaches consensus through transaction validation, a new block is appended to the chain. The ability to read the blockchain in a consortium Blockchain can either be made public or restricted to participants. Consortium Blockchains, in contrast to private Blockchains, are only partially decentralized. Corporations prefer the decentralized nature of a consortium blockchain architecture over that of private Blockchains.

THE ARCHITECTURE OF BLOCKCHAIN

The names of the sender and the recipient of a Bitcoin transaction, for example, are stored in a block that is connected to the one before it. Genesis Block refers to the initial block chain that is liked with subsequent blocks. Because of cryptography & distributed ledger, integrating financial transactions is challenging. Many businesses are increasing their spending on this cutting-edge technology in an effort to speed up their operations and cut costs. The widespread adoption of cryptocurrencies has spurred the development of blockchain technology. Ledger entries can be viewed but not altered once recorded [Satoshi Nakamoto, 2017].

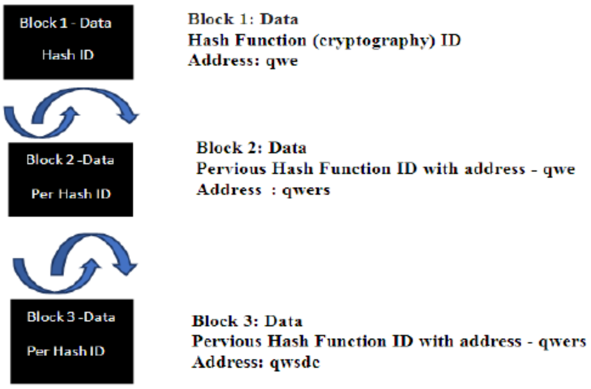

Figure 1: Blockchain Technology Architecture

Since no centralized server is required and all transactions can be safely hidden, this system is known as decentralized technology. The software is inoperable if Blockchain is not available through the internet. Blockchain is a term that defies precise explanation. Many people are confused by the widespread use of the term "blockchain" to refer to a variety of diverse concepts, from smart contracts to virtual currency. The primary idea underlying Blockchain is decentralization. The easiest way to describe blockchain is as a decentralized system or distributed digital ledger in which transactions are recorded anonymously among many users using the same hash algorithm as the previous hash. It's a permanent document that can't be changed or removed.

A. Importance of Blockchain

The blockchain has the potential to revolutionize data management, storage, & dissemination. Information uploaded to the chain cannot be altered or removed, which is one of the technology's strongest features. The blockchain has the potential to outperform existing technologies in terms of efficiency, security, & speed. Since Bitcoin's introduction in 2008, cryptocurrencies have been all the rage. However, in recent years, interest in blockchain's potential has skyrocketed. Know Your Customer, Anti-Money Laundering, Trade Surveillance, Smart Contracts, Collateral Management, Settlement, & Clearing, and the Capturing of Current Ownership of High-Value Items are only a Few of the Potential Applications Being Explored with Blockchain Technology. The definition of "smart contracts" When predetermined conditions are met, the terms of a smart contract are carried out mechanically by the computer. The obvious benefits of smart contracts include lower prices, higher quality, and faster speeds for executing contracts. The blockchain can be used to store smart contracts. From permission blockchains "where the verification blockchain is preselected by a central authority or consortium" to permission less blockchains "where anyone can participate in the verification process," the authority over blockchain varies depending on the type of blockchain used. The permission less blockchain that underpins Bitcoin is currently the subject of greater media interest [B.E.Dixon, 2016]. However, regardless of who is in charge, the core concepts of a technology that captures events securely remain unchanged. There has been a lot of hype about how blockchain will revolutionize the banking sector, but the technology still has a ways to go before it is generally adopted. Some of the uses of blockchain still need to be refined before they become widely adopted, as recent exploits of badly written smart contracts demonstrate. Blockchain currently has practical applications in Bitcoin, provenance, & land registry. Still in development are applications in fields as diverse as digital business, corporate operations, insurance, healthcare, supply chain management, logistics contract administration, and smart execution.

B. Blockchain – Future Applications

Blockchain's popularity has skyrocketed recently. Theoretically, the technology can traverse borders and do away with inefficiencies brought on by intermediaries, logistics, and other such factors. Since the blockchain has such promising applications, prominent financial institutions are banding together to invest & advance the technology. Financial institutions in other countries are funding pilot programs & studies to investigate the potential of blockchain technology. Legal, regulatory, & political hurdles are to be expected with the introduction of any cutting-edge technology. To integrate blockchain technology into a management setting involving more than just exchange and proof of value, the financial services industry relies on malware Security to provide high security & secure service [J. Richardson 2017]. Blockchain technology is based on a philosophical framework that combines networks, algorithms, & cryptographic methods. This concept incorporates characteristics like automation, security, & decentralization into its distributed decentralized algorithms & peer-to-peer network. Blockchain data may be saved, updated, & distributed with the help of asynchronous database synchronization. With this technology, information can be sent from one node to another, and the only thing individuals need to access it is the address of that node. Due to the absence of desirable regulations, this technology has no central authorities or central system for linking the employees who are transforming their data through nodes.Smart contracts allow the Blockchain to socially function in accordance with the norms established by its panel members [Walid, 2017].

C. Smart Contract

Is a form of system software that can be used to automatically carry out this technology & ensure that the stack holders adhere to any rules and regulations that have been set up for it. All of the programming for smart contracts has already been agreed upon & approved by all parties involved in the relevant blockchain. When clients approve of a transaction with a stack holder, the transaction is encrypted and linked to the address of the prior transaction, providing an extra layer of security provided by blockchain technology.

Since no records of transactions are kept centrally, using peer-to-peer networks makes it more challenging for hackers to compromise any given set of information. As a result, more capital is flowing into smart contract programs, in which each node block contains the immutable, publicly accessible data of a single stack holder. The security of this decentralized system relies heavily on the usage of a consensus algorithm. The nonce is the error generated by the proof-of-work security method, which is a random process. It verifies the legitimacy of the new user & confirms which miners are responsible for filling up the block. This forces miners to guard against hacker attacks on the proof of stack [A. Gervais, 2016].

BLOCKCHAIN LIMITATIONS

As a relatively new technology, blockchains have yet to overcome a number of hurdles that could limit their use beyond the financial industry:

a) **Scalability**: Currently, a new block of transactions can be added to the Bitcoin blockchain every ten minutes or so. As a result, the number of transactions processed per second is quite low (less than five) compared to that of more conventional transaction networks (S. Mitra, 2017).

b) **Block size**: All of this stems from the fact that the Bitcoin protocol was designed with a relatively modest block size. Each block can be up to one megabyte in size, which means that 2,200 transactions can be processed at once. There has been some talk about increasing the size of individual blocks, but no decision has been made as of yet [Iuon-Chang 2017].

c) **High costs:** Proof-of-work algorithms are run by miners using high-end hardware. Although in theory all nodes have the necessary software to mine the network, in practice only select nodes can effectively compete in this process. Since hardware and electricity costs prevent most nodes from participating in this process, Nakamoto's "one-CPU-onevote" concept is obsolete [Dusko K., 2018].

d) **Cryptography**: The widespread use of cryptographic technologies is still in its infancy, and it is unrealistic to anticipate it from the average Internet user in the near future.

e) **Complexity**: The technical jargon around blockchain technologies makes them seem even more foreign to the layperson. Somehow, only a chosen few are able to grasp this new technology.

f) **Environmental impact:** The inefficiency of work in terms of the energy it consumes is also demonstrated by the foregoing. Bitcoin's annual electricity demand may have been equivalent to that of 280,000 US households in the spring of 2017, according to some estimates.

g) **Bandwidth**: Active full nodes require sufficient Internet bandwidth in order to function properly in the network. With the blockchain's current size at around 120

Gigabytes [Roger W 2017], slow, unstable connections are not desirable.

h) **Centralization:** The majority of mining power is now concentrated in only a few nodes.

i) **Usability**: Users & nodes in a blockchain network must exercise extreme caution when handling public & private keys. While improvements have been made to wallet software, losing private keys is still a major concern. Few existing technologies can safeguard n users against malware, and none can withstand physical theft.

j) **Immutability as liability**: The immutability of a blockchain could be a weakness if it were compromised by hackers or if a security flaw in the underlying technology made a particular exploit possible. For instance, last year's Ethereum breach allowed a single malicious node to steal $64 million [George C., 2017].

The community behind blockchain technology is proactive, and they're already trying to fix these problems. The availability of the source code to the public is a major factor. In contrast, consensus or a majority of nodes agreeing on a course ahead are required to make modifications to the code & blockchain operations [Atul K 2017].

Ancient (2008-2013)

The emergence of bitcoin

Bitcoin (BTC) was the first blockchain-based application. Since its inception in 2009, it has remained the most popular and expensive kind of digital currency. Satoshi Nakamoto's whitepaper provided a thorough explanation of the system as a digital peer-to-peer network. Nakamoto generated the genesis block, which subsequent blocks were mined from, resulting in one of the longest chains of blocks carrying a variety of data & transactions. Since the introduction of Bitcoin, a blockchain application, many other apps have emerged, each with the same goal: to make use of the features and concepts offered by distributed ledger technology. As a result of this evolution in technology, a plethora of use cases for blockchain have surfaced.

Middle (2013-2015)

Ethereum development (THE BITCOIN 2.0)

To grow material consumption by an infinite amount on a finite world is impossible, as E. F. Schumacher put it. Therefore, Vitalik Buterin set out to create what he considered to be a malleable blockchain that can do more than just act as a P2P network. Buterin thought Bitcoin had untapped potential and was not making full use of the blockchain's features. When Ethereum was released in 2013 as a new public blockchain with greater functionalities than Bitcoin, a major turning point in blockchain history occurred.

Buterin developed Ethereum different from the Bitcoin Blockchain by offering a feature that allows users to store assets other than contracts, such as catchphrases. The new function expanded Ethereum's functionality beyond that of a coin and into that of a platform for the development of decentralized applications.

The Ethereum blockchain, which debuted in 2015, has become one of the most significant applications of blockchain technology due to its ability to facilitate smart contracts. Ethereum's blockchain technology has also been able to attract a thriving developer community, which has been important in the development of a genuine ecosystem for the cryptocurrency. Ethereum's blockchain processes the most daily transactions because of its ability to run smart contracts & decentralized apps. The company's bitcoin market cap has also surged significantly.

Future (2018-present) the rubbing of minds

It's no surprise that various people have built alternative blockchain technologies since 2018 to address the limitations of bitcoin and Ethereum. One of the newest blockchain systems is NEO, which is described as the top open-source, distributed, and blockchain platform developed in China. Despite the ban on cryptocurrencies, the country is nevertheless actively involved in blockchain technology. NEO, backed by Alibaba CEO Jack Ma, bills itself as "the Chinese Ethereum" and aims to challenge Baidu's dominance in the country.

Some engineers used blockchain technology to construct IOTA in an effort to speed up the expansion of the IoT. The cryptocurrency platform is designed for the IoT ecosystem & seeks to provide free transactions and unique verification processes. It also addresses some of Bitcoin's scaling issues that plagued Blockchain 1.0.

In addition to IOTA & NEO, several second-generation blockchain systems are also creating waves in the industry. The Monero, Zcash, and Dash blockchains were developed as attempts to ameliorate the early blockchain's lack of security and scalability. The three blockchain apps, known as privacy Altcoins, are designed to protect users' anonymity & funds during transactions.

Previous discussions of blockchain history have focused on open blockchain networks, where any user is able to access its data. But as technology has advanced, more and more companies and organizations have been adopting this strategy to boost operational efficiency.

Big companies are spending a lot of money to hire experts so they can get a head start on technology. Companies like Microsoft appear to have led the charge in the hunt for blockchain technology platforms, which has resulted in the hybrid, private, & federated blockchains that are in use today.

To the future

Based on blockchain's progress, we can see that it has a promising future. So, here are some forecasts for the future of blockchain based on my cursory investigation:

By 2022 & beyond, the blockchain industry is expected to generate more than $10 billion in valuation, creating a strong demand for blockchain professionals & increasing the number of available jobs in the sector. The research firm projects that the company's value will increase to more than $175.9 billion by 2025 and more than $3.1 trillion by 2030, based on their findings from the Blockchain Digital Transformation study. Therefore, blockchain-based startups will enjoy more financial success.

- Blockchain technology will find far more uses, well beyond the current ones in the financial sector, the property market, insurance, and so on.
- Its widespread adoption in the financial sector bodes well for the future success of blockchain-based businesses like Petra.
- Deloitte predicts that by 2020, more than 60% of businesses will have adopted blockchain technology.
- Blockchain technology is being used by companies like Walmart to enhance and modernize their supply chain operations.
- According to Goldman Sachs, by 2027, the technology might contribute as much as $300 billion to global GDP.
- In collaboration with Stellar.org, JP Morgan is building a blockchain-based securities settlement platform.
- Large financial institutions including Citigroup, JPMorgan Chase, and Wells Fargo are investigating how blockchain technology could benefit their business.

CHALLENGES OF BLOCKCHAIN

A challenge is an openly stated request for evidence. Here are some of blockchain technology's most pressing problems right now.

A. Scalability

The blockchain's size continues to balloon out of control as the number of users & volume of daily transactions both continue to rise. Each node stores a copy of all transactions for further verification. Prior to validating any other transactions, the current transaction must be verified. The inability to handle millions of transactions simultaneously in real time is mostly attributable to the limited block size & time interval utilized to construct another block. In the meantime, the size of the blocks in blockchain could provide a problem with transaction delay in the case of low transaction volume, since miners prefer to validate transactions in exchange for transaction fees. According to, the proposed remedies for the blockchain adaptability problem fall into two broad categories: storage optimization & blockchain redesign. The remaining non-null addresses would be maintained by the database. It is also possible to use a lightweight consumer as a substitute to address the mobility issue. When implementing changes, the blockchain can be split into a larger "key block" and a smaller "micro block," with the larger block handling elections for new leaders & smaller block storing individual transactions.

B. Privacy Leakage

Due to the fact that all public key information and balances are accessible to the whole network, the blockchain is especially susceptible to privacy leaks during transactions.

Mixing solutions & anonymous solutions are two broad categories that describe the methods recommended for achieving anonymity in blockchains. Anonymity can be achieved with the use of mixing, a service that moves assets across many information deliveries and various yield locations.

C. Selfish Mining

Blockchain also has to deal with the problem of selfish mining. If only a small fraction of available hashing power is employed, a block can be tampered with. Selfish miners do not share their newly mined blocks with the network, but instead construct a separate branch that only shares their blocks once certain conditions are met. In this scenario, honest miners lose a lot of time and energy while greedy miners focus on the private chain.

D. Personal Identifiable Information

The term "personally identifiable information" (PII) refers to any piece of data that can be used to determine the specific identity of an individual.

E. Security

Confidentiality, integrity, & availability are three aspects of security that are explored in [J.Mendling 2018]. It is difficult in general with public networks like blockchains.

Distributed systems that relay fake data over their network have poor confidentiality. Blockchains are built on a foundation of trust, but they face a number of obstacles. Blockchains have great readability in comparison to writing because of their widespread replication. Due to these characteristics, the 51%

majority attack becomes more theoretical in a vast blockchain network.

F. Merit & Demerit of Blockchain Technology

Blockchain's primary benefits are its decentralized nature, transparency, reliable chain, immutability, & resistance to destruction. In contrast, the key drawbacks of the Blockchain are its high energy consumption, its complicated integration procedure, and its expensive implementation costs.

G. Future of Blockchain Technology

By 2022, at least one new blockchain-based enterprise will be worth $10 billion, claims York Solutions. The value blockchain brings to businesses will increase to almost $3.1 trillion by 2030, from just over $360 billion in 2026.One groundbreaking blockchain-based company will be worth $10 billion by 2022. The value blockchain brings to businesses will increase to almost $3.1 trillion by 2030, from just over $360 billion in 2026.

CONCLUSION

Even though Blockchain technology is relatively new and its widespread deployment is a little-studied issue in practice, it has quickly become one of the world's most beneficial & flexible concerns due to the extensive facilities in most systems across industries. Some advantages of Blockchain technology give us hope for a future in which information technology is secure & trustworthy. Distributed ledger technology, which includes the blockchain, is a decentralized digital database that is maintained in real time by a network of computers rather than a single, centralized server. All of these unique computers are referred to as nodes, and they are linked together in an entirely haphazard fashion. It's an almost impossible-to-make academic journal. Because of its decentralized, peer-to-peer nature, it enjoys widespread acclaim & praise from its users. However, Bitcoin protects a wide range of blockchain-related research.

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to Ms. Sapna Sharma, Head of Department, Computer Science, Welham Girls' School for her invaluable support throughout the research.

REFERENCES

1. Atul K., Arpit G., 2017, " BLOCKCHAIN: An analysis on next-generation internet ", available : http://dx.doi.org/10.26483/ijarcs.v8i8.4769
2. B.E.Dixon and C. M. Cusack, ―Measuring the value of health information exchange,‖ in Health Information Exchange. Elsevier 2016, pp. 231–248.
3. Dusko K., 2018, " Impact of Blockchain Technology Platform in Changing the Financial Sector and Other Industries " , available :http://repec.mnje.com/mje/2018/v14-n01/mje_2018_v14-n01-a18.pdf
4. G. Eason, B. Noble, and I. N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955. *(references)*
5. George C ., 2017, " Bitcoin – A Brief Analysis of the Advantages and Disadvantages ", available: http://www.globeco.ro/wpcontent/uploads/vol/split/vol_5_no_2/geo_2017_vol5_ no2_art_008.pdf
6. Gervais, G. O. Karame, K. W¨ust, V. Glykantzis, H. Ritzdorf, and S. Capkun, ―On the security and performance of proof of work blockchains,‖ in Proceedings of ACM SIGSAC Conference on Computer and Communications Security (CCS'16), pp. 3–16, New York, NY, USA, 2016.
7. https://101blockchains.com/history-of-blockchain-timeline/
8. https://insidetelecom.com/is-blockchain-the-future-of-finance/#:~:text=The%20potential%20of%20block-chain%20to,the%20contract%20in%20real%2Dtime
9. https://timesofindia.indiatimes.com/readersblog/raghib-blogs/opportunities-and-the-future-of-blockchain-technology-43325/
10. https://www.infoworld.com/article/3657635/why-blockchain-is-the-future-of-the-internet.html
11. https://www.robertwalters.com.au/hiring/hiring-advice/Blockchain-technology-and-the-future-of-banking.html
12. S. Jacobs and C. P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.
13. Iuon-Chang L., Tzu-Chun L., 2017, " A Survey of Blockchain Security Issues and Challenges " , available : http://ijns.jalaxy.com.tw/contents/ijns-v19-n5/ijns2017-v19-n5- p653-659.pdf
14. J. Richardson, Ethereum vs. Hyperledger, [Online] http://goo.gl/64a3Gg [26] Wall Street Firms to Move Trillions to Blockchains in 2018, IEEE Spectrum, Sept. 2017, [Online] http://goo.gl/bhr3Ck (Erişim: 1 Şubat 2018).
15. J.Mendling, I. Weber, W. V. D. Aalst, J. V. Brocke, C. Cabanillas, F. Daniel, S. Debois, C. D. Ciccio, M. Dumas, S. Dustdar et al., Blockchains for business process management-challenges and opportunities, ACM Transactions on Management Information Systems (TMIS), 9 (2018), Article No. 4

16. Roger W., Christian D., Conrad B., 2017, " Scalable Funding of Blockchain Micropayment Channel Networks " , available : http://drops.dagstuhl.de/opus/volltexte/2017/7363/ pdf/dagrep_v007_i003_p099_s17132.pdf
17. S. Mitra, B. Jana and J. Poray, "Implementation of a Novel Security Technique Using Triple DES in Cashless Transaction," 2017 International Conference on Computer, Electrical & Communication Engineering (ICCECE), Kolkata, India, 2017, pp. 1-6.doi: a10.1109/ICCECE.2017.8526233
18. Satoshi Nakamoto, ―Bitcoin: AHou, ―The application of blockchain technology in e-government in china,‖ in ICCCN. IEEE, 2017, pp. 1–4
19. Shuai Wang , Jing Wang, Xiao Wang , Member, IEEE, TianyuQiu, Yong Yuan , Senior Member, IEEE,LiweiOuyang, YuanyuanGuo, and Blockchain Powered Parallel Healthcare Systems Based on the ACP Approach2329-924Xc 2018 IEEE.
20. Walid A., Nicolas S., 2017, " Blockchain technology for social impact: opportunities and challengesahead",available: HTTPs 10.1080/23738871.2017.1400084
21. ZainabAlhadhrami, Salma Alghfeli, Mariam Alghfeli, Introducing Blockchainsfor Healthcare2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA).

Corresponding Author

Arshiya Sharma*

Student, Class 12th, Welham Girls School