2023 International Conference on Intelligent Systems for Communication, IoT and Security (ICISCoIS) | 979-8-3503-3583-5/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICISCOIS56541.2023.10100456

Evolution of Blockchain and Smart Contracts

A State of the Art Review

Christina K.
UG Scholar
Department of Computer Science and Engineering
CMR Institute of Technology
Bengaluru, India
chk21cs@cmrit.ac.in

Dr. R. Kesavamoorthy
Associate Professor
Department of Computer Science and Engineering
CMR Institute of Technology
Bengaluru, India
kesavamoorthy.r@cmrit.ac.in

***Abstract*— Over the years, the methods of transaction have changed swiftly although the trading process had a dynamic increase and decrease. Passing over a trajectory of greater assets in the financial world we now have Blockchain technology that determines decentralization and monetary values. Smart Contracts are generally referred as digital contracts that allow two parties to take on some form of exchange and that could be anything such as a cash transfer to property transfers such as homes, objects, NFTs, crypto currencies and a lot more. This will definitely disturb several industrial sectors around the world, which includes trade, marketing, medical, real estate. Evolving in every shape and form from the very beginning, most certainly blockchain and smart contract will take over every aspect of the future paving the way for a conservative world that ultimately yearns decentralized system. This paper will be one stop destination for understanding the evolution of blockchain and smart contracts.**

Keywords*— *Blockchain; smart contracts; decentralised network; transactions; peer-to-peer network;

I. INTRODUCTION

The concept of blockchain technology and smart contract applications will undeniably revolutionize the way we live our lives and will remain long after. Blockchain enabled smart contracts are powerful enough to redeem us from the hands of any third-party institutions for safety. An amazing derivative of this technology is that it makes our transactions and trade completely democratic. Services will grow rapidly since one can use them to exchange credits and even simpler transactions. Every individual in this network would have equal power and dominion. The most important advantage of blockchain and smart contracts will help us increase transaction time, reduce costs, and even ease the complex processes.

Blockchain is a system wherein a report of transaction is made using bitcoin or any other crypto-asset and is maintained throughout several computer systems which are linked in a peer-to-peer network. It is nothing but a distributed ledger for bitcoin transactions. This technology has been taken over by many businesses, governments and corporations to fulfil numerous needs. The number one motive of Block chain is to provide protection, immutability, traceability and transparency in an allotted community.

Generally, Block chain is considered as a public ledger used to file transactions. Blockchain consists of blocks that subsequently add each other, and a sequence of chain is formed that is permanent and can't be tampered. To further provide an explanation for this chain of blocks, the preliminary block is named as Genesis block that is a file of the very first transaction. And this block is allotted with an alphanumeric string known as a "hash" which is calculated using the timestamp. Now in a sequential chain of blocks, the hash of a particular Block is created by the use of the preceding block's hash. The computers on this network are called the "miners", they evaluate the transactions and test if they are legitimate through various mathematical calculations. For Similar verification, the idea "consensus" is performed, in other words a Settlement is made among 51% of the partakers, to decide a selected block's originality and agree if the brand-new block's hash has been effectively calculated, before it's delivered to the chain.

Bitcoin [1, 2] is one of the very first protocols to use this technology. Bitcoin white paper was first published by pseudo anonymous Satoshi Nakamoto. This white paper outlined how bitcoin can make peer-to-peer transactions in a decentralized network, which was powered by cryptography. This allowed people to do decentralized finance and started calling it "digital gold". Furthermore, decentralized transactions using bitcoin was upgraded to decentralized agreements called as smart contracts which were a set of instructions executed. To be more specific, these set of instructions are written in code and embodied on decentralized blockchain platforms. Bitcoin was viewed only as a store of value, but Ethereum was viewed both as a store of value and as a utility to facilitate the decentralized agreements.

This paper has been organized in the following way. Section 1 set the introduction for the paper. Section 2 will focus on the history of blockchain technology [3,4] along with a timeline. Section 3 will focus on the history of smart contracts along with a timeline at the end. Section 4 highlights the applications of the blockchain and smart contracts followed by section 5 that explains the future scope of the technology. Concluding remarks are mentioned in Section 6 followed by Acknowledgment and References.

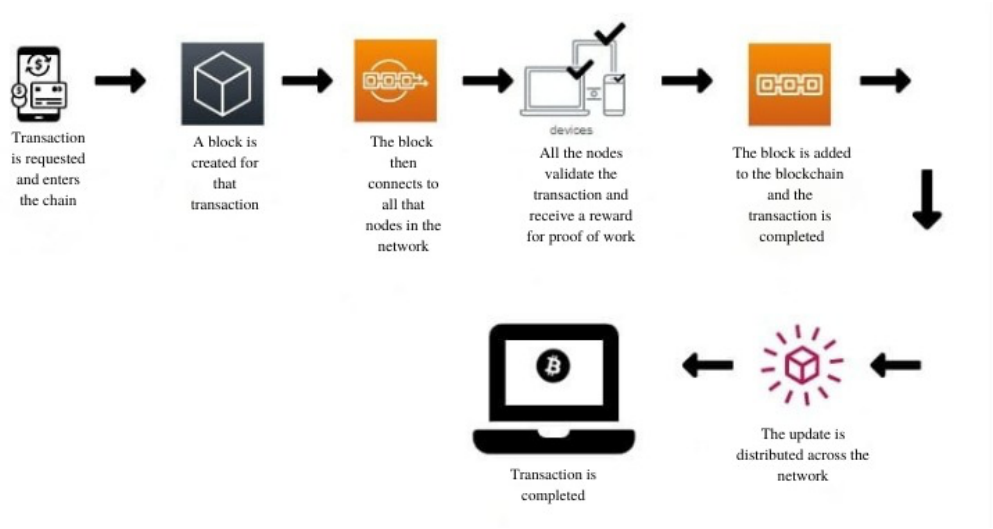

Fig. 1. Working of Blockchain

II. HISTORY OF BLOCKCHAIN TECHNOLOGY

A. 1979-2007: Introduction of block chain in the early years

- Even before bitcoin was regarded, various blockchain based technologies were being used [5]. These types of technologies were based on the Merkle tree data structure, named after the scientist Ralph Merkle. He observed a technique of public key distribution and virtual signatures known as "tree authentication".
- In 1991: Stuart Haber and W. Scott Stornetta posted an article about time stamping digital documents.
- In 1992: Haber and Stornetta upgraded the pattern to include Merkle trees, which permitted multiple document certificates to remain on a single block. The idea of proof-of-work (POW) also turned into an addition to verify Computational attempt.

B. 2008-2009: Bitcoin and blockchain get their jump

- In 2008: A white paper publication was released by Satoshi Nakamoto explaining bitcoin and blockchain Ideas. He also brought the idea of "chain of blocks" which meant adding of blocks sequentially. Transactions enter the chain of block for which data is created [6]. The block connects to all the nodes within the network. Every node chooses to approve or deny the new block. if accepted, the new block is introduced to the chain. There is no requirement of any third party.
- In 2009: bitcoin grew from a mere idea to an actual reality.
- Jan 3, 2009: Satoshi Nakamoto mined the very first bitcoin block that contained 50 bitcoins and was referred as the Genesis block.
- Jan 8, 2009: Release of Bitcoin version 0.1.
- Jan 12, 2009: the first bit coin transaction with 10 bitcoins was done.
- Oct 12, 2009: A channel for bitcoin builders called #bitcoin-dev was initiated on Internet Relay Chat.
- Oct 31, 2009: the foremost change of paper cash for bitcoin -- Bitcoin Market – was established.

C. 2010-2012: Bitcoin and cybercurrency

- Nov 22, 2009: A platform called the “Bitcoin talk” was launched by Satoshi Nakamoto to share bitcoin associated news and facts.
- May 22, 2010: Bitcoin created history when 10,000 bitcoin for two Papa John's pizzas was paid by Laszlo Hanyecz. After that incident, bitcoin exchange Mt. Gox that was tokyo-based, was launched. This handled greater than 70% of all Bitcoin transactions.
- January 2011: Mining of one-sector of the 21 million bitcoin.
- February 2011: the price of bitcoin became identical to the U.S. dollar.
- By 2012, crypto-currencies were well mounted but went through price fluctuations.

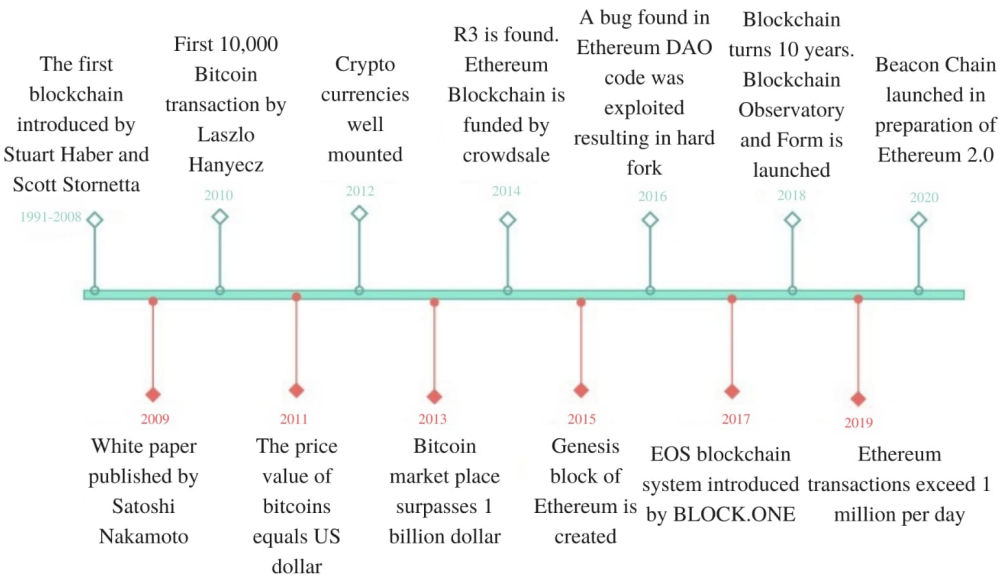

Fig. 2. Timeline of Blockchain Tehnology

D. 2013-2015: Upward push of Ethereum and blockchain to distinction.

- February 2013: [7]Coinbase reported that $1 million worth of bitcoin at more than $22 each was sold in a single month. A decentralized application platform leading to the creation of Ethereum foundation was proposed by a white paper publication. This definetely made a way for Blockchain technology, and also for the use of numerous purposes. It introduced smart contracts and supplied creators, a platform for building decentralized programs.
- 2014: It was the year of turning point, as economic establishments and other businesses started to understand and discover the capability of blockchain. And fixed their eyes on the development of blockchain technology . Later numerous Corporations accepted bitcoin, inclusive of the Chicago SunTimes, Overstock.Com, Microsoft, PayPal and Expedia.
- 2015: Ethereum Frontier network enabled developers to put in writings, the decentralized apps that might be sited to a network. Ethereum became the largest utility of blockchain era.

E. 2016-present: Blockchain goes mainstream Blockchain is a valuable technology, but not limited to finance or other cybercurrencies.

- 2016: The blockchain gained acceptance all over the world.A project called The CDC and the Hyperledger proclaimed a corporation to reinforce trade advocacy and education. A hard fork was found in the Ethereum network when a bug in the Ethereum was exploited.
- *2017: The highest record of nearly $20,000 of bitcoin was acheived. And was recognised as legal currency by japan. The EOS blockchain OS was introduced by Block.one company,*
- 2019: A supply chain based on the hyper ledger system was launched by Walmart. Amazon declared it's wide-range accessibility on AWS. Ethereum transactions surpassed 1 million per day. Research and development of blockchain took the spotlight as establishments accepted this technology.
- 2020: Approximately 40% of defendants unified blockchain to production and 55% observed blockchain as a deliberate significance. Beacon Chain was released in the research for Ethereum 2.0. Stable coins went through a substantial growth for the reason that they assured more stability than the conventional cyber currencies. A budding curiosity for the emerging blockchain and AI enhanced corporate progressions.

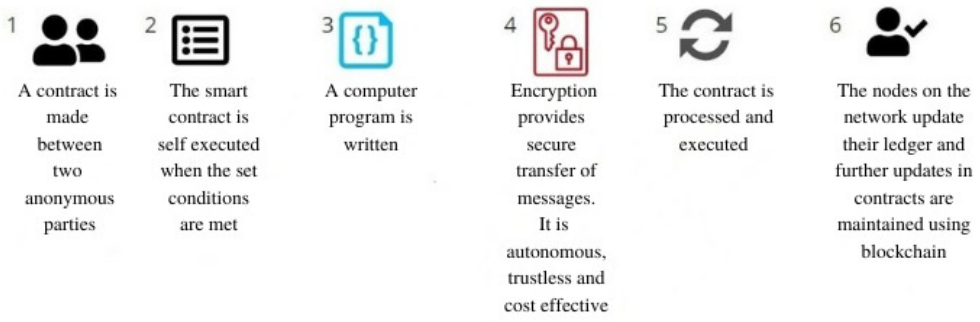

Fig. 3. Working of Smart Contracts

Blockchain technology proceeds into 2021 and 2022 as administrations and initiatives depend on blockchain to get a hold of variety of applications. Over the years, an increase in interest for using blockchain for applications other than cyber currency has rose, which comprises voting, supply chain, real estate, web 3, intellectual rights, DAOs, the internet of things, and many more.

III. History Of Smart Contracts

Smart contract was introduced by Nick Szabo in 1994. Exchange of money, goods, stocks, or anything of a value in a translucent and tampered way while avoiding a middleman, is supported by smart contracts [8]. They function on blockchain. They permit parties to approve of specific terms or enter into a specific pact, which once accomplished, triggers the smart contracts to initiate a deed such as transferring supply chain management money and many more. They are generally referred as digital contracts that allow two parties to take on some form of exchange and that could be anything such as a cash transfer to property transfers such as homes, objects, NFTs, crypto currencies and a lot more [9,10].

1) Smart contract was specifically used to refer to the idea of a computation of general purpose that occurs on a blockchain or a distributed ledger. A "smart contract" in the words of the US NIST, is a collection of code and data that is employed using cryptographically signed transactions.

2) The Ethereum blockchain was introduced in the year 2015. A smart contract is way too different from the usual contracts with respect to it's protocols, patterns and methods. A transaction with specified information about the contract is recorded in a blockchain or distributed ledger.It cannot be altered after that point.The legal system typically resolves disagreements over contracts and upholds conditions, but it is also usual to have alternative arbitration process, especially for cross-border business.

Smart contracts, well known as self-executing contracts are eccentric digital protocols that benefit us to deal with valuable digital assets quickly and easily. They are used well for the deep transformations brought about by the disruptive technologies like IoT, AI, and mechanization. To explain the interface between blockchain and smart contracts, we consider various conventions. Firstly, Security and excellent dependability of smart contracts on blockchain .High dependability while performing the transactions provides excellent security because it is fully encrypted.

Smart contracts are independent on blockchain, third-party middlemen to carry out transactions are not certainly required. Due to the fact that, everyone using the public blockchain network can see the information included in the contract, it fosters an interconnected atmosphere. Since all parties in the cycle can see the updates made to the contract's content, this intensifies transparency[11,12].

Contracts on blockchain are programmed using software code. Additionally, they deliver instantaneous changes quickly and accurately. Transactions made using smart contracts do not need human supervision. Thus, it lowers the jeopardies associated with the contract execution process. Smart contracts also offer speed and effectiveness since they initiate to work right away when a convinced condition is satisfied. Besides, smart contracts are digital and automated and they do not require any paperwork or forms to be filled out manually.

IV. Applications

A. Supply Chain management using Blockchain

Transactions on supply chain are traced by means of blockchain technology in a highly safe and transparent way that empowers traceability all over supply chain. Farm storage is one of the main applications of blockchain [13,14]. Blockchain qualifies permanent record-keeping, transparency and validation of transactions shared by several supply chain participants. This can be used to check the acceptability or the current state of the distributed merchandise .

B. Blockchain in Cyber security:

The existing internet structure is vulnerable to cyber-attacks owing to the centralized network that is being used. This can certainly cause fraud and data theft [15]. The transaction details are stored in the cloud, which is easily accessible to anyone. Blockchain in this case is a gamechanger. The transaction details are permanently stored and the data is encrypted which makes it simple to prevent harmful attacks since peer-to-peer connections ensure that data is safe and unchangeable.

C. Ballot system using blockchain:

With the assistance of a decentralized network vulnerabilities are avoided [16,17]. Voting processes can function in total transparency by doing away with the need for third-party systems using blockchain.

D. Blockchain in Financial Services:

Blockchain can improve financial services and settlement systems by increasing the efficiency to diminish costs. Banks like UBS, have decided to use tokens for international trades. Whereas the Chamber of Digital Commerce was recognized to edify and support Blockchain technology in the economic service areas and beyond.

E. Blockchain in medical industry:

Maintaining extremely sensitive data such as patient records and reports, that could be relocated between sectors or research centers is laid-back now. Numerous patient details that often wish to remain private are entered as new individual blocks to the blockchain. These blocks keep the records secure and encrypted. Similarly, medical research firms would also want their data to be stored securely [18]. Test results and new drug formulas are to be kept away from technical modifications. Thus, blockchain plays a vital role in preserving valuable medical data.

V. RESEARCH GAPS

A. Slow transaction speed

Blockchain can conceivably replace all the banks, credit and debit cards. For example, Visa can handle thousands of transactions per second whereas Bitcoin can only handle 7-8 transactions per second as it uses proof-of-work as it's algorithm for consensus. Thus, it is extremely slow compared to the traditional transaction methods we use.

B. Harmful to the environment

Bitcoin and Ethereum that works on proof-of-work consume a large amount of energy to solve any mathematical computation. As a significant amount of power is required miners around the world who are into crypto mining purchase an entire power plant that apparently consumes more energy than most of the smaller countries.

C. Minimum security on public blockchain

The very first reason why Blockchain was invented was for security and transparency. But in reality, public blockchain is available for everyone on the network. Even if the data on blockchain is safe and un-tampered, it is clear that the data is exposed to all the nodes on the network.

VI. FUTURE SCOPE

The future of Blockchain is all about decentralized applications or protocols. We have observed various applications of blockchain, be it buying or selling bitcoin, crypto currencies, NFTs tokens and many. But apart from the above decentralized applications, this technology would also be used for supreme security like tracking illegal weapons around the world. Illegal arms that are bought or sold by anyone can be tracked by the record of transactions on the blockchain.

Blockchain is bringing about a massive change to the developments across various platforms. Apparently one main technological revolution that is on the move includes Web3. The evolution of internet from Web 1.0 that is the read only state to Web 2.0 which is stated as social driven. e are gradually moving towards the next phase of the internet, Web 3.0 which promises people to own things digitally in a whole new world. Blockchain and crypto ecosystems already have working products for Web3 [19]. This can rewrite the entire conceptualized protocols of the internet.

Decentralized autonomous organizations (DAOs) permit people to organize around a shared interest without a central decision-making authority. DAOs can drive Web3 to be more decentralized, transparent and community centered [20]. Web3 can also solve majority of problems faced by internet and reduce the power of the tech giants. Therefore, blockchain is unquestionably a major driving force in the expansion of Web3 development in the future.

Furthermore, regarding centralized financial services blockchain introduced De-Fi known as the Decentralized Finance [21,22]. There are variety of services today such as loans, saving plans, insurance and stock markets that are built around centralized system. This financial system is prone to fraud, corruption and mismanagement. The solution to this kind of unreliable system would be decentralized blockchain technology.

Metaverse can simply digitize our everyday world providing a marketplace for physical things in the digital world [23,24]. This world turns physical to digital whereas virtual turn into reality. Gaming, entertainment, business, goods service and everything that we do these days will be put into metaverse. Crypto is fundamentally the currency used in this world [25]. This brings us to something called the NFTs also known as non-fungible tokens. NFTs are digital entities that are minted, bought or sold in the world of metaverse. It can be owned by

any individual without the control of any centralized body. These entities include audios, images, files, artworks, gaming items etc. Particularly gaming is going to be taken to another level where people can sense things just like they do in the real world.

VII. Conclusion

Although Blockchain is not being much of a bargain in majority of the organizations present today, it has outgrown the customary traits which would certainly bring about a massive change in the centralized system. Bitcoin stepping in as the very first successful implementation of blockchain technology has had many other assets follow through. Ultimately, the intended purpose of decentralization would permeate furthermore in all possible sectors.

Acknowledgment

We thank the Cyber Security Centre of Excellence - CCoE, Department of Computer Science and Engineering, CMR Institute of Technology, Bengaluru, India. This paper and the research work behind it would not have been possible without it.

We would also like to show our gratitude to the Management, Principal, Vice Principal, HoD-CSE, CMR Institute of Technology, Bengaluru, India for their constant support and encouragement towards continuous research and development.

References

[1] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, 2008

[2] The Bitcoin's Network Effects Paradox—A Time Series Analysis
Ioanna Roussou, Chaido Dritsaki, Emmanouil Stiakakis Theoretical Economics Letters Vol.9 No.6, August 27, 2019 DOI: 10.4236/tel.2019.96126

[3] Kesavamoorthy, R., Guptha, A., Gupta, A., Gahlot, A., Pandey, A. (2022). A State of Art Review on Blockchain Technology. In: García Márquez, F.P. (eds) International Conference on Intelligent Emerging Methods of Artificial Intelligence & Cloud Computing. IEMAICLOUD 2021. Smart Innovation, Systems & Technologies, vol 273. Springer, Cham. https://doi.org/10.1007/978-3-030-92905-3_55

[4] M.A. Khan, K. Salah, IoT security: Review, blockchain solutions, and open challenges. Futur.Gener.Comput.Syst.(2018). https://doi.org/10.1016/j.future.2017.11.022

[5] 101blockchains.com/history-of-blockchain-timeline

[6] www.blockchain-council.org/blockchain/a-detailed-history-of-blockchain-from-the-establishment-to-broad-adoption/

[7] Detailed history of blockchain: From the Establishment to Broad Adoption. https://www.blockchain-council.org/blockchain/a-detailed-history-of-blockchain-from-the-establishment-to-broad-adoption

[8] K. Saini, A. Roy, P. R. Chelliah and T. Patel, "Blockchain 2.O: A Smart Contract," 2021 International Conference on Computational Performance Evaluation (ComPE), 2021, pp. 524-528, doi: 10.1109/ComPE53109.2021.9752021.

[9] Bhalla, A. (2021) A detailed history of Blockchain: From the establishment to broad adoption, Web3 & Blockchain Certifications. Available at: https://www.blockchain-council.org/blockchain/a-detailed-history-of-blockchain-from-the-establishment-to-broad-adoption (Accessed: January 9, 2023).

[10] Z. Zhu, J. Su, Z. Jiang, M. Ye and Z. Zheng, "Making Smart Contract Classification Easier and More Effective," 2022 IEEE International Conferences on Internet of Things (iThings) and IEEE Green Computing & Communications (GreenCom) and IEEE Cyber, Physical & Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics (Cybermatics), 2022, pp. 228-230, doi: 10.1109/iThings-GreenCom-CPSCom-SmartData-Cybermatics55523.2022.00067.

[11] M. Suvitha and R. Subha, "A Survey on Smart Contract Platforms and Features," 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS), 2021, pp. 1536-1539, doi: 10.1109/ICACCS51430.2021.9441970.

[12] A survey on Smart Contract Platforms and features | IEEE conference Available at: https://ieeexplore.ieee.org/abstract/document/9441970

[13] R. R. Konapure and S. D. Nawale, "Smart Contract System Architecture for Pharma Supply chain," 2022 International Conference on IoT and Blockchain Technology (ICIBT), 2022, pp. 1-5, doi: 10.1109/ICIBT52874.2022.9807744.

[14] Smart Contract System Architecture for Pharma Supply Chain (no date). Available at: https://ieeexplore.ieee.org/document/9807744/ (Accessed: January 9, 2023).

[15] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han and F. -Y. Wang, "Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends," in IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 49, no. 11, pp. 2266-2277, Nov. 2019, doi: 10.1109/TSMC.2019.2895123

[16] S. T. Alvi, M. N. Uddin, L. Islam and S. Ahamed, "A Blockchain based Cost effective Digital Voting System using SideChain and Smart Contracts," 2020 11th International Conference on Electrical and Computer Engineering (ICECE), 2020, pp. 467-470, doi: 10.1109/ICECE51571.2020.9393081.

[17] Alvi, S.T. et al. (1970) Classification of blockchain based voting: Challenges and solutions: Semantic scholar, 2020 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE). Available at: https://www.semanticscholar.org/paper/Classification-of-Blockchain-based-Voting%3A-and-Alvi-Uddin/3c2cc4f6b5c4637b90fe7ef6364a7967569601c0

[18] Z. Liu et al., "Make Web3.0 Connected," in IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 5, pp. 2965-2981, 1 Sept.-Oct. 2022, doi: 10.1109/TDSC.2021.3079315.

[19] Make Web3.0 connected | IEEE Journals & Magazine | IEEE Xplore (no date). Available at: https://ieeexplore.ieee.org/document/9428608/ (Accessed: January 9, 2023).

[20] Walch, Angela. "Blockchain Applications to International Affairs: Reasons for Skepticism." Georgetown Journal of International Affairs, vol. 19, 2018, pp. 27–35. JSTOR, http://www.jstor.org/stable/26567524. Accessed 8 Jan. 2023.

[21] Dekker, B., Hühn, A., Korsten, P., & Okano-Heijmans, M. (2022). The emergence of decentralized finance. In The geopolitics of digital financial technologies: A chance for Europe? (pp. 6–7). Clingendael Institute. http://www.jstor.org/stable/resrep40265.6

[22] Makarov, I. and Schoar, A. (2022) Cryptocurrencies and decentralized finance (DEFI), Brookings. Brookings. Available at: https://www.brookings.edu/bpea-articles/cryptocurrencies-and-decentralized-finance-defi/ (Accessed: January 9, 2023).

[23] UNDERSTANDING THE METAVERSE. (2022). US Black Engineer and Information Technology, 46(2), 60–61. https://www.jstor.org/stable/48697592

[24] Metaverse-2022: The 2022 IEEE conference on metaverse (no date) Metaverse-2022 | The 2022 IEEE Conference on Metaverse. Available at: http://www.ieee-smart-world.org/2022/metaverse/ (Accessed: January 9, 2023).

[25] Person, Kavita, P. and Saini, C. (2021) Essential enterprise blockchain concepts and applications: Kavita Sai, Taylor & Francis. Taylor & Francis. Available at: https://www.taylorfrancis.com/books/edit/10.1201/9781003097990/essential-enterprise-blockchain-concepts-applications-kavita-saini-pethuru-chelliah-deepak-saini (Accessed: January 9, 2023).