Evolutionary Transformation of Blockchain Technology

Santosh Kumar Singh[1], Vikas Rao Vadi[2]
Assistant Professor, Department of Computer science, BTTS, Don Bosco Technical School, New Delhi, India[1]
Professor, Director, Bosco Technical Training Society, Don Bosco Technical School, New Delhi, India[2]

***Abstract*—Blockchain technology plays an important role in the business development. Several businesses can possibly advantage from the revolutions blockchain decentralization technology and confidentiality protocols proposal with regard to safeguarding, records access, auditing and handling dealings inside digital platforms. Blockchain is founded on distributed and protected decentralized protocols in which no single point of control, and there is no single authority, the data blocks are generated, added, and validated by the nodes of the network themselves. This article provides understandings into the recent developments within blockchain technology. We first provide the chronological background of this swift and prompt technology. The major prominence of this article is to present a wide learning of the consecutive developments in Blockchain Technology by emphasizing the fundamentals of all generations in detail.**

Keywords*— *Blockchain, Decentralized network, Distributed ledger, Security.

I. INTRODUCTION

Blockchain technology that turned into first projected as strength for carrying out the primary virtual money and is now being organized in several application areas due to its exclusive characteristics that guarantee the protected, translucent and trustworthy dealings of information in a peer2peer mode inside a distributed system.

Blockchain Technology initially got here into recognition with the beginning of Bitcoin introduced by Santoshi Nakamoto [1]. The foremost generation of Blockchain is Bitcoin [2] which was based on distributed peer2peer virtual money that removed the existence of any dominant power like banks or any intercessors. To enhance the belief concerns among the users, carry out the model of consensus [3] to guarantee the genuineness and truthfulness of the customers. Because of the restricted utilization of the 1st generation in simply monetary segment, additional developments were prepared to implement Blockchain for other areas too. Ethereum is known for [4], the 2nd generation machinery has massive application through its dependable smart contact sections for crowdsourcing. A smart contract [5] is an internally self-assured agreement where the compliance amid purchasers and merchants are straight rehabilitated into lines of codes across a distributed blockchain system. New advancement is Hyperledger due to its Permissioned architecture [6] it delivers advanced modularity and adaptability than Ethereum. The 3rd generation Blockchain has innate confirmation machinery and extra well-organized quicker and inexpensive than earlier types. Uniting Blockchain Technology with AI i.e. artificial intelligence has at present cemented the way for the 4th generation of blockchain also.

The rest of the paper is prepared as follows. In section II we will explain fundamental of blockchain, in section III focuses on to demonstrate a detailed study of the sequential developments in Blockchain Technology by emphasizing the essentials of each generation in detail, in section IV we demonstrate a parameter wise transformations among the numerous generations, finally we conclude the paper in section V.

II. FUNDAMENTALS OF BLOCKCHAIN

A. *Historical Background*

Beginning of crypto guaranteed signatures transformed interchange of information between the transmitter and receiver in 1980. Digi Cash [6-7] exchange through email became widespread in 1989. Further practice of virtual papers became public and main highlighting is positioned on guaranteeing their verification, competence and dependability. In 1991, the idea of time stamping a virtual document to guarantee that cannot be retrospective and are alter proof suggested by Haber and Storenetta [9–11]. In following years, combination of Merkle Trees permitted gathering of numerous virtual papers into a block that enriched their safety. Usage of virtual currencies became fairly leading in the late 90s, [12]. Virtual exchanges are immaterial and simply accessible electronically. Szabo [13] presented the idea of “bit gold”, distributed virtual money in 2005 grounded on dissimilar cryptographic components.

Finney [14] submitted a scheme called “Reusable Proof of Work, RPoW” that functioned by attaining a non-replaceable Hashcash [15] centered proof of work token. In complementation, a RSA-signed token is generated that is interchangeable amid the customers.

Drawing philosophies from the present virtual exchange idea and basics of cryptography, Satoshi Nakamoto carried the idea of Blockchain Technology into attention by applying the first blockchain as the open ledger for transactions prepared with “Bitcoin in 2008[1]”. Since its beginning, Blockchain has been gaining the consideration of numerous scholars for its immeasurably protected structures.

B. *Structure of Blockchain*

The design of a block could be supposed to be partitioned into two segments, one containing of the heading with altogether data about data i.e. metadata and the other containing of entirely the transaction particulars. Figure 1 demonstrates the structure of blockchain

At the outset, the metadata be made up of Preceding Hash that is utilized to sequence the existing block through its previous block in the blockchain. The 2nd part of metadata includes the data relating to mining races for example

Timestamp, Difficulty and Nonce. Mining [16] is accomplished by extraordinary computers which resolve multifaceted mathematical glitches to obtain payments in return, hence concluding the confirmation processes. Timestamp provides the design time particulars for a specific block so removing the rejection of service consequences. Difficulty provides the complication that was used to generate this block. In cryptography, nonce [17] is a random numeral utilized simply once in the whole communication. Nonce is the quantity which miners are challenging for. Positively mining is that the persuasive miner was the former to predict the nonce that is a string of arbitrary quantities attached to the hashed matters of the block that is once more time rehashed.

The last metadata comprises the Merkle Tree root that is a data arrangement to précis whole the business particulars in the equivalent block in a well-organized way.

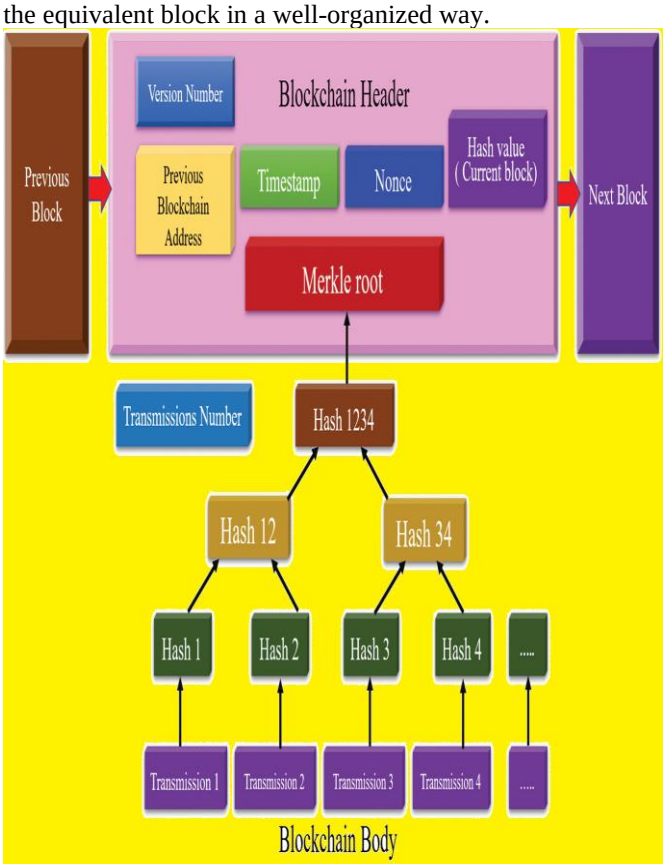

Fig. 1 Structure of Blockchain

C. *Types of Blockchain*

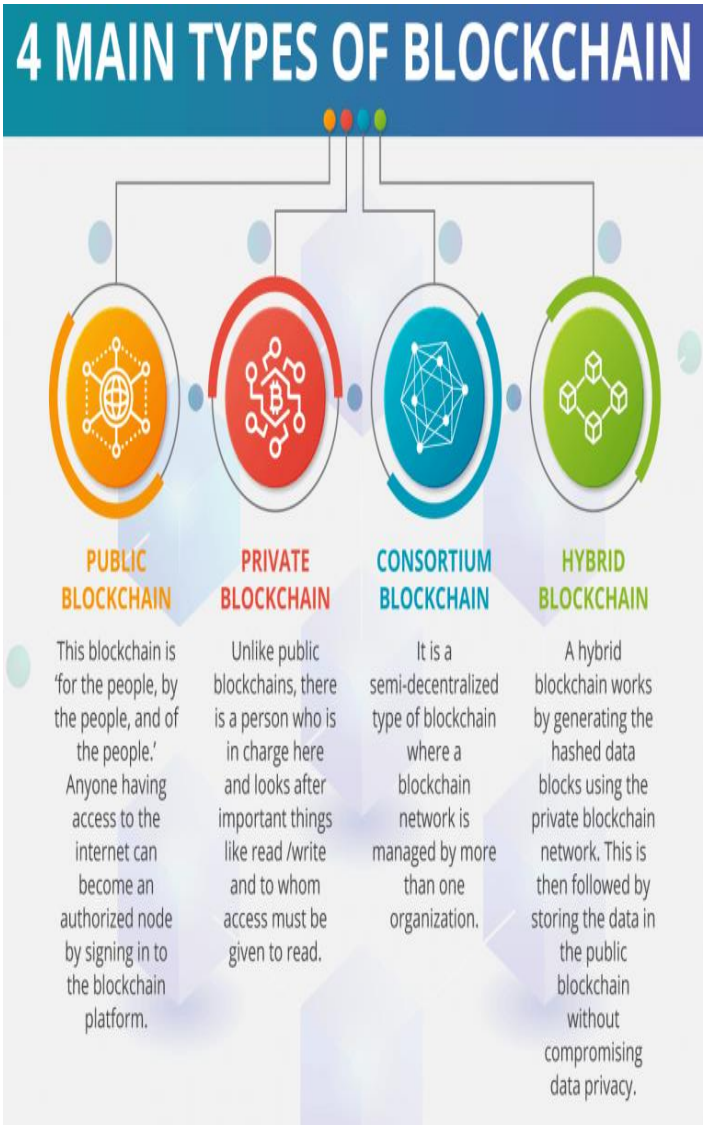

Fig. 2 Types of Blockchains

The different categories of Blockchain are characterized on the base of their applications.

- Predominantly the two comprehensive kinds of Blockchain are Public and Private Blockchain.
- Two variant correspondingly exist like the Consortium and Hybrid Blockchain. Figure 2 demonstrates the kinds of Blockchain in a shell.

We are comparing the best projecting categories of blockchain as shown in table1.

Table 1 Comparison of three projecting types of Blockchain

Parameter	Public	Private	Consortium
Speed	Slow	Fast	Fast
Agreement	PoS / PoW	Multiparty agreement	Multiparty agreement
Writing Privileges	Anybody	Approved Users	Approved Users
Reading Privileges	Anybody	Requested users	Rest on situation
Authority	Anybody	Particular central power	Many central power

Contributors	Anyone	Permissioned and identified entities	Permissioned and identified entities
Decentralization	**Entirely decentralized**	**Centralized**	**Fewer centralized**
Permission	No	Yes	Yes

III. THE EVOLUTIONARY TRANSFORMATION OF BLOCKCHAIN

Blockchain technology has gone through four predominant developments and each of those has been deliberated inside the subsequent subdivisions.

A. Blockchain 1.0

The 1st generation of Blockchain i.e. 1.0, initiated from the idea of decentralized Ledger machinery [18]. Decentralized ledger is a databank that is consensually pooled among numerous applicants hence allowing public eyewitnesses to remove double spending consequences. The greatest noticeable application of Decentralized ledger was cryptocurrency where Bitcoin [19] played an essential part and therefore became the "currency on the web" [20]". Bitcoin launched in 2009 and showed its constancy, dependability, competence, straightforwardness, independency and safety to preserve a path of transaction details and handover power of these details from one consumer to another directly. It essentially utilizes consensus and mining mechanisms to exchange cryptocurrencies. Figure 3 provides the general functioning of Bitcoins.

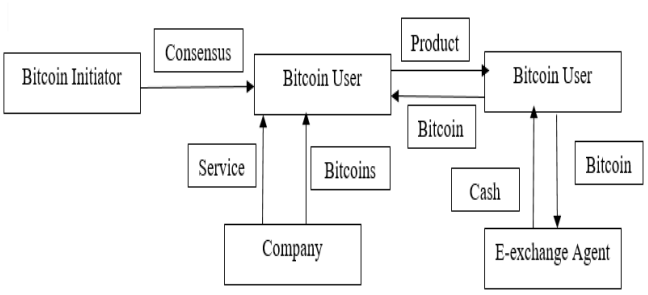

Fig. 3 Bitcoin model

Swan [21] emphasized the usefulness of Bitcoin presence installed as a cryptocurrency in applications affecting to money transfer, payment and virtual expenditures based on encryption machineries and works autonomously. So Bitcoin has the prospective to substantiate to be a proposal of an innovative monetary strategy. Narayanan et al. [22] particularized the procedure of Bitcoin, their mining and guidelines in their work. Decker and Wattenhofer [23] examined the data circulation in Bitcoin network by using multi-hop distribution to inform the ledger. Bitcoin is mainly established on mining machineries which includes resolving algo-puzzles to confirm financial dealings to obtain cryptocurrencies as payments. Böhme et al. [24] systematically deliberate the Bitcoin scheme philosophies, its fundamental machineries and procedures, the numerous usages of Bitcoin for customer disbursements in addition to the possible dangers related with it. O' Dwyer and Malone [25] deliberate energy depletion in Bitcoin mining and recommended extraordinary hardware changes to attain extreme profits.

The detail that inconspicuousness and decentralization of Bitcoin declares it a possible game changer in e-commerce was suggested by Grinberg [26]. Velde supported the practical and theoretical happenings of Bitcoin to be instilled in current monetary segments due to its liberty from any central power involvement [27].

Blockchain 1.0 therefore has varieties of benefits above the customary disbursement machineries for example little transactional charges and comparative secrecy in transactions. Due to sufficient supply Bitcoins will not ever be out of marketplace. Bitcoins eradicating double spending as well as also eliminate forging by allowing protected trackable and translucent dealings.

Among all its accomplishments, Bitcoins too have some drawbacks. Blockchain 1st generation fundamentally employs the (Proof of Work) consensus machinery that requires the calculation of difficult calculated puzzles. Because of the complication involved, (Proof of Work) is timewasting and utilize huge quantities of energy than the total incomes made as well having a considerably slow throughput. One more drawback of Satoshi's knowledge of Blockchain 1.0 is that it uses simply 1 megabyte (MB) blocks of material on bitcoin dealings. The most distinguished limitations of Blockchain 1.0 are their incapability to backing Smart Contracts and other application regions in its place of monetary services.

B. Blockchain 2.0

The extravagant mining and reduced accessibility of the Blockchain 1st generation encouraged Buterin [28] to spread the idea of Blockchain further than money. This directed to the beginning of the Blockchain 2nd generation i.e. Ethereum that is constructed on innovative ideas of smart contracts together with using Proof of Work consensus machineries. "A smart contract is an agreement between two people in the form of computer code".

Smart Contracts [29] are independent self-handling computer programs that run spontaneously on the ground of predefined sections amid two parties. This is not possible to be damaged or altered hence [30] fundamentally decrease the charge of confirmation, run, and deception avoidance and allow translucent contract description.

Fig. 4 Smart contract on blockchain

Figure 4 shows smart contracts on blockchain. Few steps involved in its working, the 1st stage is preparation of the agreement in the middle of two customers. Guidelines and circumstances of the contract has to be acknowledged by the two corresponding person and transformed into a code. Without the permission of the concerned people no

alterations can be done into the agreement. Real-world example can be termination of an insurance rule or distribution of belongings. As soon as the code implementation is ended, the contracts will spontaneously handover the value to the appropriate receiver. The clearance is as a result finished promptly, firmly and professionally. This handover is also note down into the blockchain.

Ethereum [31-33] employs the application of smart contracts in Blockchain. Ether has number of applications in practical almost every region for example, real estate, electronic voting, and trading. In the Ethereum, miners race for Ether. That is applied to prize miners for containing dealings in their block, known as gas.

Dannen provided a detailed understanding of (Solidity - high level programming language) to carry out smart contracts. Antonopoulos and Wood [34] provided the bit by bit guide to form a smart contract using Solidity like, about Solidity version, installing it, smart contract writing, compiling and lastly installing it into the Blockchain.

On the other hand, smart contracts also impose numerous troubles on the consumers since they are very complicated to write [35]. Slightly errors while scripting the agreement can lead to unintentional hostile effects [36]. Consequently to attain extreme profits of Ethereum, it is necessary to express and install the smart contract properly.

C. *Blockchain 3.0*

The main obstacle of Blockchains 1.0 and 2.0 are not scalable of any kind, typically established on Proof of Work and require about 60 minutes to approve transactions. This entire permit to the beginning of the contemporary technology of Blockchain called Blockchain 3.0 that purposes to create cryptocurrencies worldwide workable. The 3rd generation of Blockchain commonly includes Decentralized Apps (dApps) [37]. Blockchain 3.0 too uses Proof of Stake and Proof of Authority [38] consensus machineries to allow improved quickness and calculating control for smart contracts without any extra operation fees. Blockchain 3.0 removes the dependence on Miners to confirm and validate transactions and in its place usage innate machineries for the same, therefore extremely fast to permit thousands of dealings per second.

Blockchain 3.0 cemented way for numerous stages with their distinctive benefit to inspire Blockchain practice in day to day life. For example ICON projects [39] IOTA [40] Cardano [41] Aion [42].

The qualities of Blockchain 3.0 have extremely high transaction speed and consist of no single regulatory power in this manner no particular point of letdown. DApps don't belong to a specific IP address therefore challengers cannot damage information and safety is improved.

On the other hand, the Blockchain 3rd generation also has numerous drawbacks like updating or bug fixing because of their distributed environment.

D. *Blockchain 4.0*

Another forthcoming favorable development in the advancement of Blockchain is the Blockchain 4.0 the main goals to provide a business-operating platform to generate and execute applications hence transforming the machinery to completely middle-of-the-road. It has the probability of imparting other flourishing machineries such as (AI) with Blockchain. Blockchain 4.0 allows production of a continuous addition of dissimilar platforms to work underneath a single umbrella in consistency to achieve commercial and manufacturing demands. The preliminary platform to keep advancing Blockchain 4.0 practicalities is Unibright [43] that allows a combination of a number of blockchain business simulations. One more instance is SEELE Platform [44] which allows cross communication among dissimilar protocols across several facilities harmonically. The 4th generation has the prospective to permit the transactional speed up to (1 M/sec) transactions.

IV. COMPARISION OF DIFFERENT GENERATIONS

This segment compares all the generations and shown in Table 2. For cryptocurrency exchange, Blockchain 1.0 stills evidences to be a naiver alternative. Further non-monetary areas like Agriculture, Healthcare, Smart Homes, and Education etc. employ smart contracts with the Ethereum platform to express the rules and guidelines amid the service provider and consumers. The 3rd and 4th generation is more be in the majority where Blockchains workings into backend for a number of business models. Both generations are still in its beginning and experiencing numerous alterations to become possible enough to oblige manhood.

Table 2 Comparison among dissimilar generations of blockchain

Parameter	**Blockchain 1.0**	**Blockchain 2.0**	**Blockchain 3.0**	**Blockchain 4.0**
Application	Monetary region	Non-monetary region	Commerce platforms	Industry 4.0
Instance	Bitcoin	Ethereum	Cardano, IOTA, Anion	Unibright, SEELE
Energy utilization	Maximum	Reasonable	Power Competent	Very well-organized
Price	Costly	Inexpensive	More Cheaper	Cost efficient
Speed	7 TBS	15 TBS	1000 TBS	1M TBS
Inter communiqué	Not approved	Not approved	approved	approved
Inter operation	No	No	Yes	Highly
Scalability	No	Poor	Scalable	Highly
Verification	Via miners	Via smart contracts	In-built confirmation Via dApps	Sharding Automated confirmation
Consensus mechanism	PoW	Assigned PoW	Proof of stake, authority	Proof of integrity
primary theory	Distributed Ledger	Smart contracts	dApps	Blockchain with AI

V. CONCLUSION

Blockchain is gifted machinery that has harvested massive attention of scholars. By joining cryptographic philosophy with distributed, immutability and clarity it principally impacted the one-to-one data exchange. The 1st generation, Bitcoin removed the existence of every middle power for

example banks or mediators. Bitcoin uses consensus models to guarantee the genuineness and truthfulness of the consumers. 1st generation is only useful in monetary region. Further Ethereum, the 2nd generation machinery used a smart contract in which decision amid purchaser and sellers are written as lines of codes across decentralized blockchain system. The 3rd generation has innate confirmation machinery.

The primary plan of this article was to offer a complete learning of the succeeding evolutions in Blockchain machinery by emphasizing the fundamentals of every generation. Joining A.I with Blockchain has by now made ready way for the 4th generation of blockchain also.

REFERENCES

[1] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, 21260.
[2] Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation*, *2*(6-10), 71.
[3] Baliga, A. (2017). Understanding blockchain consensus models. *Persistent*, *4*, 1-14.
[4] Dannen, C. (2017). Cryptoeconomics survey. In *Introducing Ethereum and Solidity* (pp. 139-147). Apress, Berkeley, CA.
[5] Mohanta, B. K., Panda, S. S., & Jena, D. (2018, July). An overview of smart contract and use cases in blockchain technology. In *2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)* (pp. 1-4). IEEE.
[6] Cachin, C. (2016, July). Architecture of the hyperledger blockchain fabric. In *Workshop on distributed cryptocurrencies and consensus ledgers* (Vol. 310, No. 4).
[7] Abrar, W. (1900). Untraceable electronic cash with digicash.
[8] Friis, J. B. (2003). "Digicash mplementation. *University of Aarhus*.
[9] Haber, S., & Stornetta, W. S. (1990, August). How to time-stamp a digital document. In *Conference on the Theory and Application of Cryptography* (pp. 437-455). Springer, Berlin, Heidelberg.
[10] Bayer, D., Haber, S., & Stornetta, W. S. (1993). Improving the efficiency and reliability of digital time-stamping. In *Sequences Ii* (pp. 329-334). Springer, New York, NY.
[11] Singh, S. K., Manjhi, P. K., & Tiwari, R. K. (2021). Cloud Computing Security Using Blockchain Technology. In *Transforming Cybersecurity Solutions using Blockchain* (pp. 19-30). Springer, Singapore.
[12] https://en.wikipedia.org/wiki/Digital_currency
[13] Szabo, N. (2008). Bit gold, unenumerated. blogspot. com (Mar. 29, 2006) Internet Archive. *Retrived from http://unenumerated. blogspot. com/2005/12/bit-gold. html*.
[14] Ølnes, S., & Jansen, A. (2017, September). Blockchain technology as s support infrastructure in e-government. In *International conference on electronic government* (pp. 215-227). Springer, Cham.
[15] Back, A. (2002). Hashcash-a denial of service counter-measure.
[16] Leonardos, N., Leonardos, S., & Piliouras, G. (2020). Oceanic games: Centralization risks and incentives in blockchain mining. In *Mathematical research for blockchain economy* (pp. 183-199). Springer, Cham.
[17] https://en.bitcoin.it/wiki/Nonce
[18] Mills, D. C., Wang, K., Malone, B., Ravi, A., Marquardt, J., Badev, A. I., ... & Baird, M. (2016). Distributed ledger technology in payments, clearing, and settlement.
[19] Antonopoulos, A. M. (2014). *Mastering Bitcoin: unlocking digital cryptocurrencies*. " O'Reilly Media, Inc.".
[20] Antonopoulos, A. M., & El Hariry, S. H. (2016). *The internet of money* (Vol. 1). Columbia, MD: Merkle Bloom LLC.
[21] Swan, M. (2015). *Blockchain: Blueprint for a new economy*. " O'Reilly Media, Inc.".
[22] Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2017). Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction.
[23] Decker, C., & Wattenhofer, R. (2013, September). Information propagation in the bitcoin network. In *IEEE P2P 2013 Proceedings* (pp. 1-10). IEEE.
[24] Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, technology, and governance. *Journal of economic Perspectives*, *29*(2), 213-38.
[25] O'Dwyer, K. J., & Malone, D. (2014). Bitcoin mining and its energy footprint.
[26] Grinberg, R. (2012). Bitcoin: An innovative alternative digital currency. *Hastings Sci. & Tech. LJ*, *4*, 159.
[27] Velde, F. (2013). Bitcoin: A primer.
[28] Buterin, V. (2014). A next-generation smart contract and decentralized application platform. *white paper*, *3*(37).
[29] https://en.wikipedia.org/wiki/Smart_contract
[30] Macrinici, D., Cartofeanu, C., & Gao, S. (2018). Smart contract applications within blockchain technology: A systematic mapping study. *Telematics and Informatics*, *35*(8), 2337-2354.
[31] Buterin, V. (2016). Ethereum: Platform Review. *Opportunities and Challenges for Private and Consortium Blockchains*.
[32] Katsiampa, P. (2019). Volatility co-movement between Bitcoin and Ether. *Finance Research Letters*, *30*, 221-227.
[33] Bouoiyour, J., & Selmi, R. (2017). Ether: Bitcoin's competitor or ally?. *arXiv preprint arXiv:1707.07977*.
[34] Antonopoulos, A. M., & Wood, G. (2018). *Mastering ethereum: building smart contracts and dapps*. O'reilly Media.
[35] Delmolino, K., Arnett, M., Kosba, A., Miller, A., & Shi, E. (2016, February). Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab. In *International conference on financial cryptography and data security* (pp. 79-94). Springer, Berlin, Heidelberg.
[36] Chen, T., Li, X., Luo, X., & Zhang, X. (2017, February). Under-optimized smart contracts devour your money. In *2017 IEEE 24th International Conference on Software Analysis, Evolution and Reengineering (SANER)* (pp. 442-446). IEEE.
[37] https://www.investopedia.com/terms/d/decentralized-applications-dapps.asp
[38] De Angelis, S., Aniello, L., Baldoni, R., Lombardi, F., Margheri, A., & Sassone, V. (2018). PBFT vs proof-of-authority: Applying the CAP theorem to permissioned blockchain.
[39] Santosh Kumar Singh, P.K.Manjhi, Dr. R.K. Tiwari "Cloud Computing Security using Blockchain Technology" ISBN: 978-81-950136-2-3, TIPSCON 2020, 10th National Conference on "Society 4.0: A Futuristic Perspective on Nature of Work, Jobs and Skills – Post COVID-19", 5thDecember 2020, Trinity Institute of Professional Studies, Affiliated to Guru Gobind Singh Indraprastha University, New Delhi. https://www.journalpressindia.com/website/proceedings.php?cid=30
[40] Divya, M., & Biradar, N. B. (2018). IOTA-next generation block chain. *Int. J. Eng. Comput. Sci*, *7*(04), 23823-23826.
[41] https://tradingstrategyguides.com/cardano-cryptocurrency-strategy/
[42] Spoke, M. (2017). Aion: The third-generation blockchain network. *Whitepa-per*, *2017*.
[43] Schmidt, S., Jung, M., Schmidt, T., Sterzinger, I., Schmidt, G., Gomm, M., ... & Emig, B. (2018). Unibright-the unified framework for blockchain based business integration. *White paper, April*.
[44] https://icodrops.com/seele/