2021 Second International Conference on Secure Cyber Computing and Communication (ICSCCC)

Divergent applications of Blockchain Security: A Survey

Vakul Sharma
Dept. of Comp. Science & Engineering
Dr. B R Ambedkar National Institute of Technology Jalandhar,
Punjab-144011, India
vakulsharma50@gmail.com

Lalit Kumar Awasthi
Dept. of Comp. Science & Engineering
Dr. B R Ambedkar National Institute of Technology Jalandhar,
Punjab-144011, India
director@nitj.ac.in

2021 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC) | 978-1-6654-4415-6/20/$31.00 ©2021 IEEE | DOI: 10.1109/ICSCCC51823.2021.9478094

Abstract— **The way people communicate and share information is changed with the use of the internet. Almost everything is digitalized from communication, payments, shopping, and learning. Due to which a massive amount of data is generated and stored on centralized servers making a single point of failure and a single point to attack. Through this paper, we discuss and analyze how blockchain is not only used for cryptocurrency transactions but can also provide DLT (decentralized ledger technology) and security services in other fields. The way blockchain technology finds its applications in emerging fields like IoT, autonomous vehicles, smart toll, energy trading, games, decentralized video streaming, their future research directions, and limitations are discussed by us in this paper.**

Keywords— Blockchain, Data Integrity, Authentication, Verification, Cryptocurrency, Hash, DLT, DDOS, Digital Fingerprint, Consensus Algorithm.

I. Introduction

A blockchain is a kind of database that makes it different from a traditional database in the way it stores data. In blockchains, data is stored in blocks, which are then linked together forming a chain of blocks. The most popular application of blockchain is to use blockchain as a transaction ledger but it can also store other types of data as well. If it is a cryptocurrency blockchain, a ledger can represent any record, including transaction records [1]. Blockchain technology has the capability to entirely transform the world. It completely mitigates the disadvantages of a centralized system. In a centralized system, every participating entity follows one network owner. The central owner keeps data that other users can access as well as user information. A centralized framework is simple to set up and can be built quickly. Every transaction on Blockchain is checked and verified by the node, which is a computer that is a participant in the specific Blockchain network. Blockchain rose to prominence after ‘Satoshi Nakamoto' published his research on ‘Bitcoin'. It began as a distributed storage technology that provided services to largely decentralized registers while also providing security mechanisms for authentication, authorization, and verification of created data. Ethereum and Bitcoin are the best implementations of blockchain technology to date, but there is still much room for improvement and we cannot say that Bitcoin and Ethereum are the final and only applications of Blockchain technology [1][2].

In this paper, we discuss the most recent stages in development practices involving blockchain technology. The following section will present an overview of blockchain technology, its architecture followed by the literature survey in section 3. In Section 4, we discuss an analysis of the literature survey, and finally, we examine the research gap including risks, threats, and varied security issues related to it, and provide solutions in these regards in Section 5.

List of Abbreviations	
POS	Proof of Stake
POW	Proof of Work
POE	Proof of Energy
DDOS	Distributed Denial of Service
P2P	Peer-To-Peer
DLT	Distributed Ledger Technology
PBFT	Practical Byzantine Fault Tolerance
IoT	Internet of Things

II. Overview of Blockchain Technology

A. Components of Blockchain architecture

Node: A node can simply be a computer system in the network. Blockchain uses a p2p network so every node in the network is connected forming a distributed network of nodes having equal privileges. The work of every single node is to process and verify the transactions [3].

Transactions: Transactions are the most basic and smallest component of blockchain. These are the only reasons we are using blockchain technology so that we can store, assess, and retrieve the already happened transactions. A transaction can simply be a payment record that contains the sender's address, recipient’s address, a time-stamp when the transaction happened, and the amount [3].

Block: A single block in the blockchain contains a block version number that indicates the policies utilized for block validation. A timestamp that indicates when that particular block was created. nBits, this gives the threshold target for a valid block hash. Nonce, a 4-Bytefield that usually starts with 0 and increases with every subsequent hash calculation. So, before verifying the block the nonce is calculated and the node which calculates the nonce first is rewarded when all other participating nodes verify this work. Merkle tree root hash: This is computed from all the transactions present in the block. It acts as a condensed digital fingerprint for the block. Any modification to any of the transactions present in the block results in the root hash being modified. Previous block hash, in this field the hash of the previous block which is already a verified block in the blockchain is written. This helps the blocks to form a chain of blocks and provides integrity to the chain. For example, block 'n' would contain the hash of block 'n-1' in this field where 'n' is an integer sequence number. The current block hash is the hash calculated from all the transactions that block holds including the hash of the previous block [3].

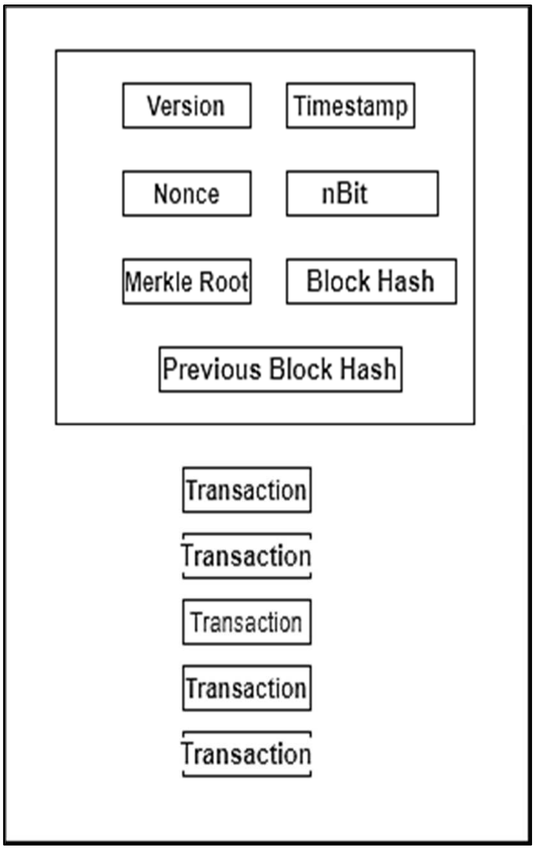

Fig. 1. Block Structure

B. How does blockchain work?

Let us consider an example to elaborate the working of Blockchain, suppose one person wants to send money to another person, now sending money involves a simple transaction, now this simple transaction is stored in a block along with the other transactions in the block, this block has a specific size. The size of the block in Bitcoin is fixed to 2 Mega Byte. When the block is completely filled, it gets distributed to every other node on the network [4]. When the other nodes on the network receive a new node, they verify it with the help of some consensus algorithm. In bitcoin-related terminology, this is referred to as "Proof of work" and "Proof of stake" in the context of Ethereum 2.0. The time taken for the entire process depends upon the blockchain (approx. 10 minutes for bitcoin and few minutes for Ethereum) [3]. In the case of the bitcoin blockchain the miners are provided with a mathematical problem like a puzzle and whichever node or miner is able to solve that puzzle first verifies the transaction which aids that particular miner to mine a block. As more and more blocks are mined this puzzle gets tough. The mined block is then appended to the main chain of blocks. As soon as the block gets placed on the main network's chain, it is then impossible to change it providing data integrity.

C. Types of Blockchain

There are primarily three types of blockchain technologies listed below:

Public blockchain: In this type of blockchain anyone interested to be a part of the network can participate and can become a validator node. Example: Bitcoin.

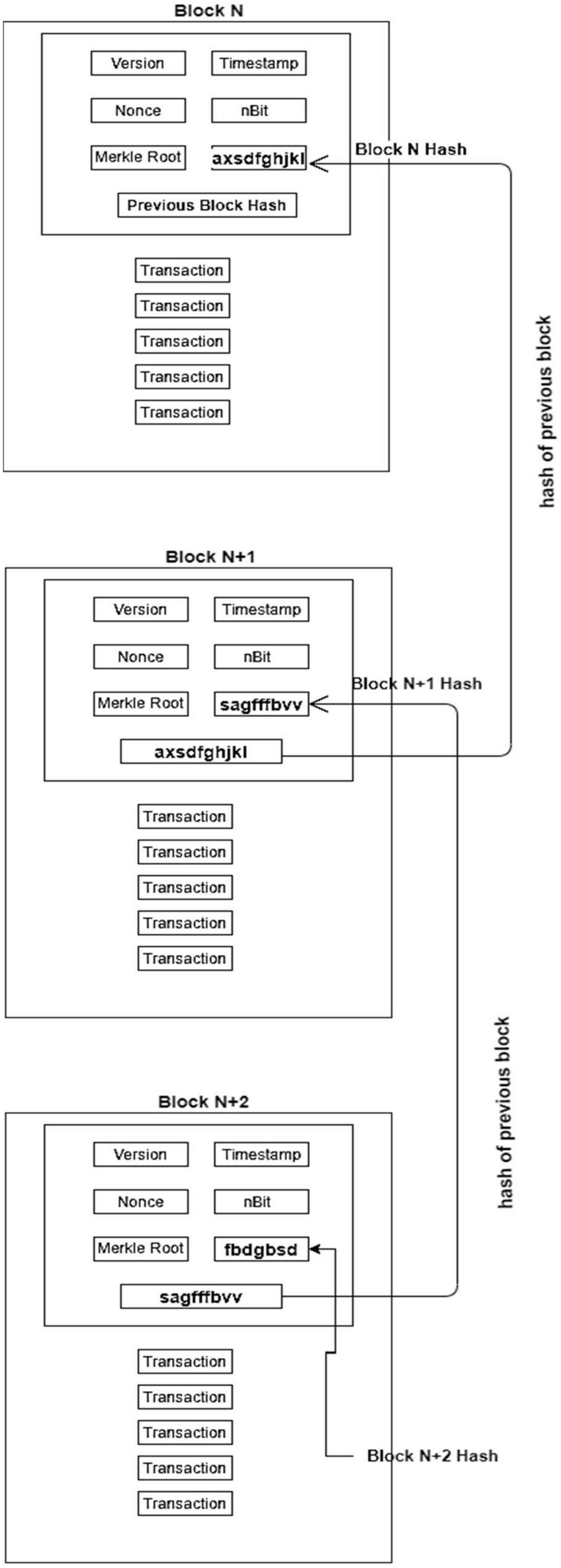

Fig. 2. Chain of Blocks showing how a block is linked to its previous block

Consortium blockchain: This type lies between the public and private blockchains where the group or the organization who created the network has control over the nodes and can choose to keep the blockchain open or private. Example: Hyperledger.

Private Blockchain: In this type of blockchain not all nodes are allowed to take part in the consensus or verification process. The blockchain is kept private within the organization and a central authority has control. Example: Ripple.

III. LITERATURE SURVEY

In this section, we discuss the latest advancements in blockchain technology over traditional methods. The study is divided into subcategories based on the recent use-cases of blockchain. Also, how and where the blockchain technology fits best in 2019 and 2020.

The first subcategory will discuss how blockchain can remove the middlemen from any real-world transaction and save the fee. Then, next, we discuss how the energy generated from the solar panels can be shared efficiently and incentives can be earned from it. Then, how the blockchain network can be prevented from DDOS attacks. IoT based distributed applications are next discussed. In the next subcatageory we discuss how autonomous vehicles can share their data securely, then decentralized games, streaming platforms, and lastly decentralized certificate verification system.

A. Smart Toll

Since now we have seen the use of autonomous toll systems equipped with RFID cards (Radio Frequency Identification) which collect the toll amount when a vehicle is passed through the toll booth, the sensors sense the RFID card automatically or a person scans the FT (FASTag) using a scanner device [1]. The data of any vehicle passing through the toll plaza is stored in a centralized database. With the Smart Toll [2], a decentralized, scalable, and secure way to share data in an intelligent vehicular network is discussed by using blockchain technology as a reliable way for toll payments. Using blockchain for storing the transactions of vehicle passing and paying the toll at the booth, and also removing the middlemen (debit and credit card) fee of about 2% - 3% [2].

B. Energy Trading

The traditional method of storage and supply of power is from power grids but by combining IoT (internet of things) and DLT (distributed ledger technology) we can have decentralized power generation and supply. The electrical power generated and stored with the help of solar panels mounted on roofs of houses can be used for trading the saved energy and the owner can earn incentives. Every house participating in trading will be like a peer on the network and the network formed using blockchain technology will be a p2p network [3]. The energy wastage and low utilization of the network are there but with the use of blockchain and smart contracts collectively we can do asynchronous settlements [4]. This will improve the trust, better price of energy, and a more reliable energy internet system.

C. Anti-D Chain: DDOS detection in blockchain

The traditional DDOS detection methods and algorithms were mainly for the detection in a centralized environment but the blockchain works on the decentralized network thus previously known methods fail here. Even the machine learning approaches for DDOS attack detection fail.

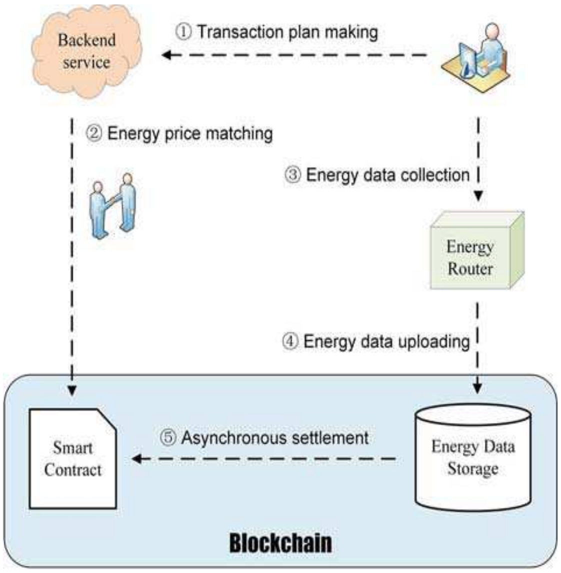

Fig. 3. Asynchronous Transaction Settlement [9]

Anti-D Chain [5] a new approach for detection of DDOS attacks is discussed which is based on ensemble learning. Here, RF (Random Forest) and AdaBoost for ensemble learning strategy along with lightweight classifiers like ID3 and CART is used. So, in P2P networks Anti-D chain improves the efficiency and correctness for detecting a DDOS attack by giving better results in some important indicators (such as ROC curve, Recall, F-Score, FPR, TPR, and Precision).

D. Edgence: IoT based distributed application

The traditional IoT network works on a centralized server, where all the data is collected and processed to gain insights. This makes the IoT network vulnerable to cyber-attacks like DDOS to disrupt the network, or to gain unauthorized access, or to steal and modify the recorded data. With Edgence (EDGe + intelligENCE) [6] where edge clouds are used to access the IoT devices and then using the blockchain to provide security by making the data tamper-proof, encrypted, transparent as previous IoT data transactions can be reviewed, increased trust as it will follow consensus before finalizing any data on the blockchain and is decentralized.

E. Intelligent Vehicular Network (IVN)

The autonomous vehicles [6] have taken over the conventional vehicles, the so-called intelligent autonomous self-driving vehicles are there which let the passenger reach his destination without any driver driving the car i.e driverless vehicles. The problem lies in the network they use to share such information any change in the information can cause serious issues. Intelligent vehicular network (IVN) [7] uses the tri-blockchain concept to share and communicate with other autonomous vehicles. Different blockchain servers are used which provides dynamic information and thus forming a reliable network in case of emergencies.

F. Discover DaVinci

Games we play are centralized and many security issues are there, using blockchains the money or the tokens can be stored on the smart contracts instead of giving it to any untrusted middlemen. Discover DaVinci [8] is a game built on blockchain technology that takes the trust and security of its players to a new level. Its focus is on teaching blockchain technology using games.

G. Dtube: Decentralized Video Streaming

The way we have been using the video streaming platforms like Youtube, NetFlix, Hotstar, and many more, there is always a central authority who is the in-charge of anything we see and what we can upload i.e lack of open internet. In this system lack of incentives, trust, security, and limited access capacity can be seen. Dtube [9] helps to make this network decentralized and uploading videos using InterPlanetary File System (IPFS), so no one can remove your content and you have full control over your videos. You can make your uploaded videos private or public but once uploaded it can't be erased.

H. SkillCheck: A Certification System

The verification of documents and certificates is a major issue even today. It takes a couple of days to verify and validate documents. The staff at educational institutes and even recruiters at multinational companies usually take days for verifying the certificates of the appliers whether they are fake or genuine. It is so time-consuming and wastage of human labor and in return the validators get nothing. With SkillCheck [10], incentives are provided to the validators in the form of tokens. They validate the certificates and documents and put a verified copy over the blockchain. The problem of decentralizing the data was already solved before incorporating the blockchain but the idea of giving incentives was still limited.

IV. Analysis Of Literature

The literature referred to study the recent advancements and different approaches of blockchain technology in various recent publications we analyze that most of the advancements are implementing 'proof of work' (POW) and 'proof of stake' (POS) consensus.

The subcategory A, D, E, and F uses proof of work consensus and the remaining subcategories use POS and proof of energy consensus. The Smart Toll [2] uses POW to validate the toll fee transactions. Energy Trading [4] uses proof of energy to reach a consensus. EDgence [6] uses proof of work consensus to validate whether the DDOS attack happened or not.

A comparative analysis is shown in Table 1 which shows the problems addressed, consensus algorithms used, and the limitations in the work done. The table shows referred literature that uses many other consensus algorithms like Proof of Identity, Proof of Existence, Proof of Honesty, Delegated Proof of Contribution, Proof of Knowledge, and Proof of Replication and Retrievability. Some of these consensus algorithms do not ensure decentralization and some of them are still not implemented.

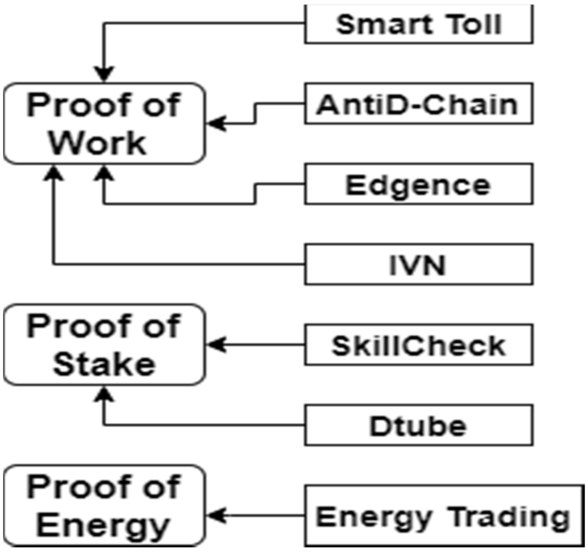

Fig. 4. Different Consensus Algorithms used in recent blockchain use-cases.

V. Research Gaps

After reviewing and establishing a survey of blockchain technology and its recent use cases, we arrive at a position where we can demonstrate some gaps in building up of the referenced literature, the gaps noticed are as follows:

- In most of the referred researches, proof of work consensus is used which makes the efficiency of the whole system low as in the proof of work to validate every block a computation is needed to be done by every node on the network thus wasting system resources and time of validators.
- Validation of nodes and adding them to the blockchain is taking more than 5 minutes.
- Both public and private clouds are used together, making the system less efficient.
- Such consensus algorithms are used which does not guarantee decentralization.
- No fundamental study is performed before implementing permissioned or permissionless blockchains. Thus, reducing efficiency.
- Consensus like proof of energy, proof of concept, proof of identity is still having security issues.
- Due to low validators in the network, the systems are vulnerable to 51% attacks.
- Using pubic blockchains trust issues and user personal data leakage is still an issue.

TABLE 1. Comparison of related work based on recent applications of blockchain technology.

Work	Publisher	Problem Addressed	Consensus Algorithm	Limitation
(Tanveer,Hasnain Javaid, 2019)	Springer	Debit card and credit card (middlemen) fee.	Proof of Work	No incentives are given to the validators and users.
(Ting Li, Wei Zhang, 2019)	IEEE	P2P energy trading, a distributed scheme with grid control.	Proof of Energy	Energy wastage and less reliable in energy transaction settlements.
(S. Ai, D. Hu, T. Zhang, 2020)	IEEE	Energy Internet, a transaction settlement system.	Proof of Energy	Higher processing time of asynchronous transaction settlement
(B.Jia and Y. Liang, 2020)	IEEE	DDOS attack detection with ensemble learning.	Proof of Work	Implemented only on an artificial blockchain.
(M. Singh, 2020)	IEEE	Intelligent vehicular network for trust issues in autonomous cars.	Proof of Work	Costly, as camera, mic, and other sensors need to be installed on every turn on the road.
(T. V. Doan, T. D. Pham, 2020)	IEEE	Content and Traffic Centralization in video streaming services.	Proof of Stake	More IP hops due to distant servers which makes it slow and less reliable.
(Regio A. Michelin, Ahmed, 2020)	IEEE	Integrity establishment of video from untrusted sources.	Proof of Integrity	Increasing more cameras per gateway increases latency.
(Ajay Kumar, Sandhya, 2020)	IEEE	Making payments private, privacy issues, and incentives.	Proof of Existence	Overhead of accessing both private as well as a public blockchain.
(Syed, Danish, Kaiwen, 2020)	IEEE	Intelligent Privacy-Preserving electric vehicle (EV) charging station.	Proof of Work	No implementation of Proof of Concept, no use of Smart Contracts, and not implemented on Ethereum network.
(Shitang Yu, Kun Luv, 2018)	IEEE	Node Mapping in intelligent devices using PBFT-DPOC.	Delegated Proof of Contribution	Used consensus algorithm has low efficiency and doesn't always allow decentralization.
(P. Urien, 2020)	IEEE	Securing Crypto Wallets by managing keys.	Based on Secure Smart Cards	No Consensus Algorithm is used and also the cost of hardware used is high.
(I. Makhdoom, F.Tofigh, 2020)	IEEE	Making Consensus attack-proof and reducing transaction latency.	Proof of Honesty	Currently implemented for only consortium blockchains, not for public blockchains.
T. Salman, R. Jain, and L. Gupta, 2019)	IEEE	Reducing and detecting malicious node's effect on the probabilistic blockchain's consensus process.	AI (agents) based collective decision	Consensus calculations and removing malicious nodes from the network needs still to be implemented.
(K. Wang, H. S. Kim, 2019)	IEEE	Reducing block propagation time and increasing throughput and scalability of the system.	Proof of Work	Shows efficiency only when the nodes have different mining power and POW is still time and resource-consuming.
(D. Chen, H. Yuan, S. Hu, 2020)	IEEE	Proof of retrievability and data replication with incentives given	Proof of Replication and Retrievability	The Server is still vulnerable and open to server-side attacks.
(M. Singh, G. S. Aujla, A. Singh, 2020)	IEEE	Securing a software-defined industrial network using a deep learning-based blockchain framework	Voting Based, Proof of Identity, Proof of Knowledge	Efficient for a small number of nodes, as the nodes increase throughput decreases sharply.

VI. Conclusion And Future Scope

In this paper, we present a review of recent researches in the field of blockchain technology approaches. We review and establish a comparative analysis based on the research studies towards advancements in blockchain techniques. Blockchains can revolutionize the "blockchain as usual" practice to "blockchain as a service". Through the literature referred we conclude that use cases of this technology, in sectors such as healthcare, supply chain, business and industry, data management, financial, prediction market, and governance are shifting towards blockchain technology.

Future researches can be done to address the issues found like:

- To validate the transactions done on the bitcoin blockchain takes 10 minutes and the transactions done on the Ethereum blockchain take up to 2 minutes, a more efficient approach is needed.
- Instead of using both public and private clouds together, the use of Hyperledger will be efficient which is a consortium blockchain.
- New consensus algorithms are needed to be developed to guarantee decentralization.
- Before implementing permissioned or permissionless blockchains their fundamentals are needed to be studied to increase the overall performance and utilization of blockchain.
- POS instead of POW needs to be implemented.
- More incentives are needed to be given to attract more validators and 51% attack can be prevented.

References

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

[2] A next-generation smart contract and decentralized application platform, V Buterin - white paper, 2014.

[3] Singh, Balpreet & Sharma, Krishna & Sharma, Nonita. (2020). Blockchain Applications, Opportunities, Challenges, and Risks: A Survey. SSRN Electronic Journal. 10.2139/ssrn.3565930.

[4] Szabo N. (1997)," The Idea of Smart Contracts".

[5] Neeharika Bakhla, Abhishek Kumar, Fanilal, Jayparkash. RFID technology in automatic toll collection. Recent Trends in Sensor Research & Technology. 2018

[6] Tanveer, Hasnain & Javaid, Nadeem. (2019). Using Ethereum Blockchain Technology for Road Toll Collection on Highways.

[7] T. Li, W. Zhang, N. Chen, M. Qian, and Y. Xu, "Blockchain Technology Based Decentralized Energy Trading for Multiple-Microgrid Systems," 2019 IEEE 3rd Conference on Energy Internet and Energy System Integration (EI2), Changsha, China, 2019, pp. 631-636, doi: 10.1109/EI247390.2019.9061928.

[8] S. Ai, D. Hu, T. Zhang, Y. Jiang, C. Rong, and J. Cao, "Blockchain-based Power Transaction Asynchronous Settlement System," 2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring), Antwerp, Belgium, 2020, pp. 1-6, DOI: 10.1109/VTC2020-Spring48590.2020.9129593.

[9] B. Jia and Y. Liang, "Anti-D chain: A lightweight DDoS attack detection scheme based on heterogeneous ensemble learning in blockchain," in China Communications, vol. 17, no. 9, pp. 11-24, Sept. 2020, DOI: 10.23919/JCC.2020.09.002.

[10] M. V. Rajasekhar aIoTA. K. Jaswal, "Autonomous vehicles: The future of automobiles," 2015 IEEE International Transportation Electrification Conference (ITEC), Chennai, 2015, pp. 1-6, DOI: 10.1109/ITEC-India.2015.7386874.

[11] M. Singh, "Tri-Blockchain Based Intelligent Vehicular Networks," IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Toronto, ON, Canada, 2020, pp. 860-864, DOI: 10.1109/INFOCOMWKSHPS50562.2020.9162692.

[12] M. Suvajdzic, J. Oliverio, A. Barmpoutis, L. Wood and P. Burgermeister, "Discover DaVinci – A Gamified Blockchain Learning App," 2020 IEEE International Conference on Blockchain.

[13] Cryptocurrency (ICBC), Toronto, ON, Canada, 2020, pp. 1-2, DOI: 10.1109/ICBC48266.2020.9169470.

[14] T. V. Doan, T. D. Pham, M. Oberprieler and V. Bajpai, "Measuring Decentralized Video Streaming: A Case Study of DTube," 2020 IFIP Networking Conference (Networking), Paris, France, 2020, pp. 118-126.

[15] P. Urien, "Crypto Terminal: A New Open Device For Securing Blockchain Wallets," 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Toronto, ON, Canada, 2020, pp. 1-3, doi: 10.1109/ICBC48266.2020.9169410.

[16] I. Makhdoom, F. Tofigh, I. Zhou, M. Abolhasan and J. Lipman, "PLEDGE: A Proof-of-Honesty based Consensus Protocol for Blockchain-based IoT Systems," 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Toronto, ON, Canada, 2020, pp. 1-3, doi: 10.1109/ICBC48266.2020.9169406.

[17] T. Salman, R. Jain and L. Gupta, "A Reputation Management Framework for Knowledge-Based and Probabilistic Blockchains," 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 2019, pp. 520-527, doi: 10.1109/Blockchain.2019.00078.

[18] K. Wang and H. S. Kim, "FastChain: Scaling Blockchain System with Informed Neighbor Selection," 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 2019, pp. 376-383, doi: 10.1109/Blockchain.2019.00058.

[19] D. Chen, H. Yuan, S. Hu, Q. Wang and C. Wang, "BOSSA: A Decentralized System for Proofs of Data Retrievability and Replication," in IEEE Transactions on Parallel and Distributed Systems, vol. 32, no. 4, pp. 786-798, 1 April 2021, doi: 10.1109/TPDS.2020.3030063.

[20] M. Singh, G. S. Aujla, A. Singh, N. Kumar and S. Garg, "Deep-Learning-Based Blockchain Framework for Secure Software-Defined Industrial Networks," in IEEE Transactions on Industrial Informatics, vol. 17, no. 1, pp. 606-616, Jan. 2021, doi: 10.1109/TII.2020.2968946.