Blockchain Technology: Research and Applied

Subjects: Computer Science, Software Engineering
Contributor: Sumaira Johar, Arjun Somanathan

Blockchain being a leading technology in the 21st century is revolutionizing each sector of life. Services are being provided and upgraded using its salient features and fruitful characteristics. Businesses are being enhanced by using this technology. Countries are shifting towards digital currencies i.e., an initial application of blockchain application. It omits the need of central authority by its distributed ledger functionality. This distributed ledger is achieved by using a consensus mechanism in blockchain. A consensus algorithm plays a core role in the implementation of blockchain. Any application implementing blockchain uses consensus algorithms to achieve its desired task.

Keywords: blockchain ; applications ; consensus mechanisms

1. Introduction

The 21st century is all about revolutionizing technology. One of the leading technologies that have changed many aspects is blockchain. It impacted different businesses from the very first step. Blockchain provides decentralized, transparent, and secure systems. It is a distributed ledger technology that maintains a transaction ledger and secures it by using cryptography. The transactions are recorded in blocks and these blocks are connected to each other through hashes. Initially, it was used by Satoshi Nakamoto in 2008 for public transactions of bitcoins. Bitcoin [1] digital currency was the first application of blockchain [2][3].

Blockchain came as a solution to the longstanding user's trust problem. With its emergence with the renowned cryptocurrency Bitcoin, it provided an architecture to allow the user to trust a decentralized system instead of trusting a third party. Operating a peer-to-peer network, it keeps records of the ledger of transactions. This helps to avoid any center party. The whole process is done through a consensus. A ledger is shared between multiple entities, allowing everyone to inspect it. No single user can control it. It is a distributed cryptographically secured database that keeps the record of every transaction from the very initial one.

2. Types of Blockchain

There are three main types of blockchain. These do not often confuse traditional databases or distributed ledger technology (DLT) with blockchains. These types of blockchain are:

- Public/Permissionless Blockchains for example Bitcoin and Ethereum etc.
- Private/Permissioned Blockchains for example Hyperledger and R3 Corda etc.
- Hybrid Blockchains for example Dragonchain etc.

3. Applications of Blockchain

Blockchain has now being deployed in not only cryptocurrency but its underlying technology is used in various applications [4]. We tried to discuss a few applications of blockchain which includes cryptocurrencies as well as other potential areas where blockchain has emerged. **Figure 1** shows different applications of blockchain.

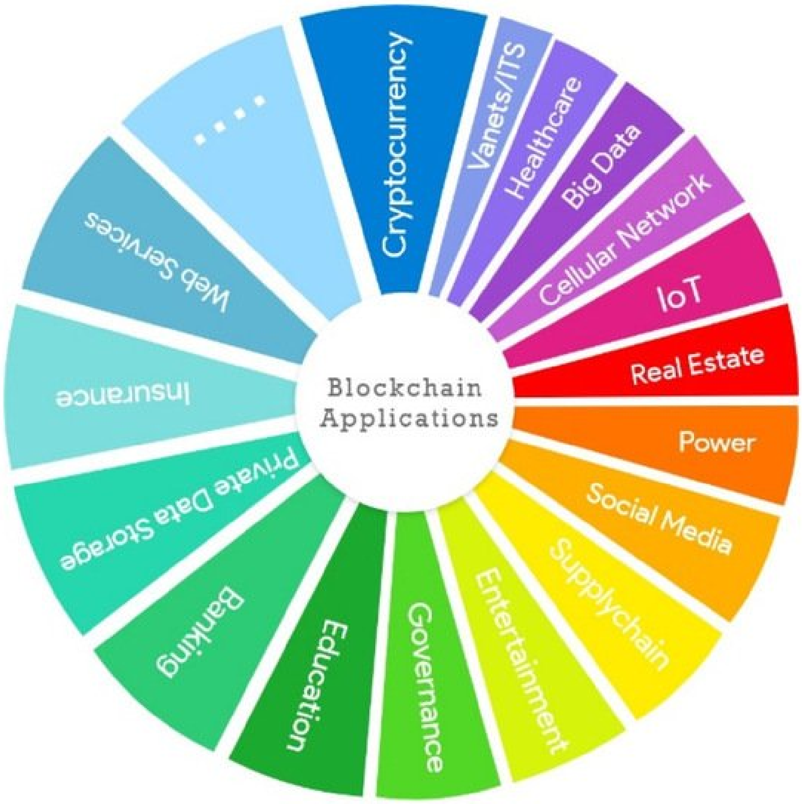

Figure 1. Applications of blockchain.

4. Blockchain's Architecture

Figure 2 shows a general view of a blockchain. A block contains the transactions, the hash of the previous block, and a hash of the next block [5]. This information is stored in a block using a cryptographic mechanism. A block in the chain can come from any miner. While creating the chain of blocks, the hash of the previous block is added to the current block. Thus a miner creates a new block by using the hash of the previous block, combines it with its own set of messages, and creates a new hash out of it. This way a new block is formed. This recently formed block now turns out to be the new end for the chain. By this mechanism, the chain grows as more blocks are added by the miners.

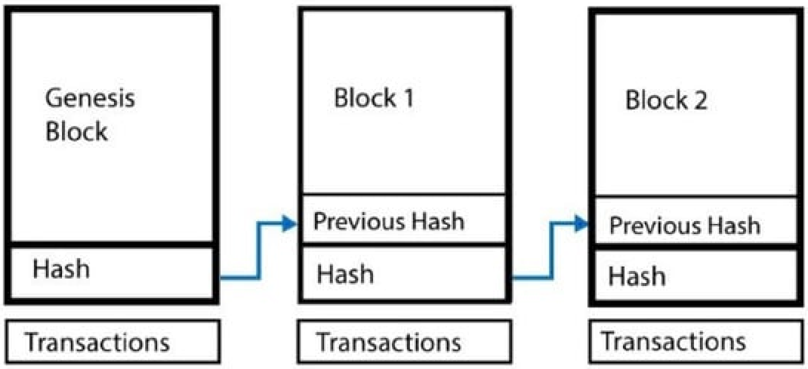

Figure 2. Blockchain architecture [6].

Double-spending is the problem where the sender uses the same money at more than one place for gaining goods or services from multiple dealers. The use of centralized authority solves the double-spending problem, but another main issue arises which is the cost of maintaining and creating the centralized authority itself. Blockchain however prevents double-spending by grouping the transactions and timestamping them and then broadcasting them in the network to all the participant nodes. The transactions are mathematically related to previous ones and are timestamped, hence impossible to tamper with.

There are also some other fields in the block header which are shown in **Figure 3**. We explain each of them.

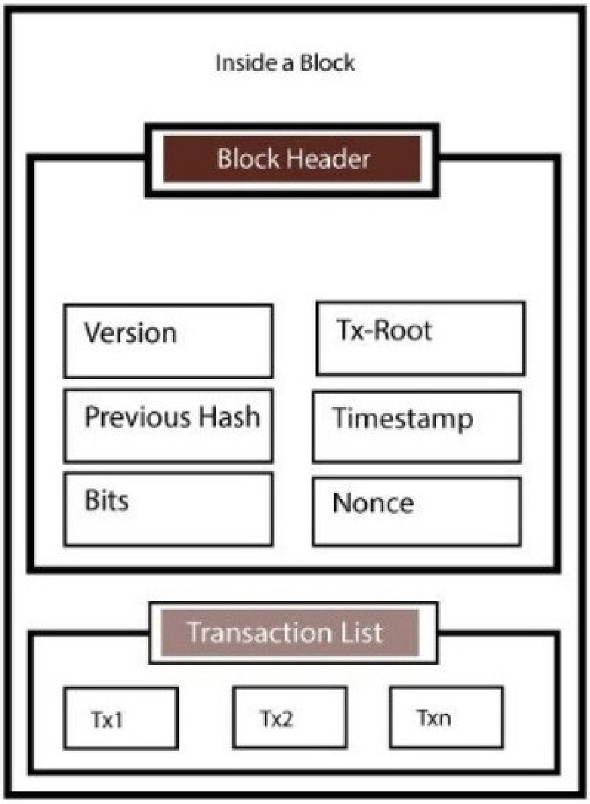

Figure 3. Structure of a block [7].

5. Consensus Algorithms

We know that blockchain is a decentralized distributed network that provides security, immutability, transparency, and privacy. There is no concept of centralization to verify and validate the transactions, but still, transactions in the blockchain are considered to be completely verified and secured. This is the result of a core algorithm present in every blockchain network called a consensus protocol.

A consensus algorithm is a technique through which all the peers of the blockchain network reach a common agreement about the current state of the distributed ledger. Therefore, consensus algorithms provide trust and reliability among unknown peers in a distributed environment. A consensus mechanism ensures that every new block added to the blockchain is the only truth that is agreed upon by all the blockchain nodes [8].

The blockchain consensus protocol comprises some specific aims that are coming to an agreement, cooperation, collaboration, mandatory participation of each node in the consensus process, and equal rights to every node. Hence, a consensus algorithm targets finding a common agreement that is a win for the whole network. The above-discussed applications are categorized and consensus algorithms based on these categories are further discussed below. **Figure 4** shows a categorical diagram of the consensus and their distribution.

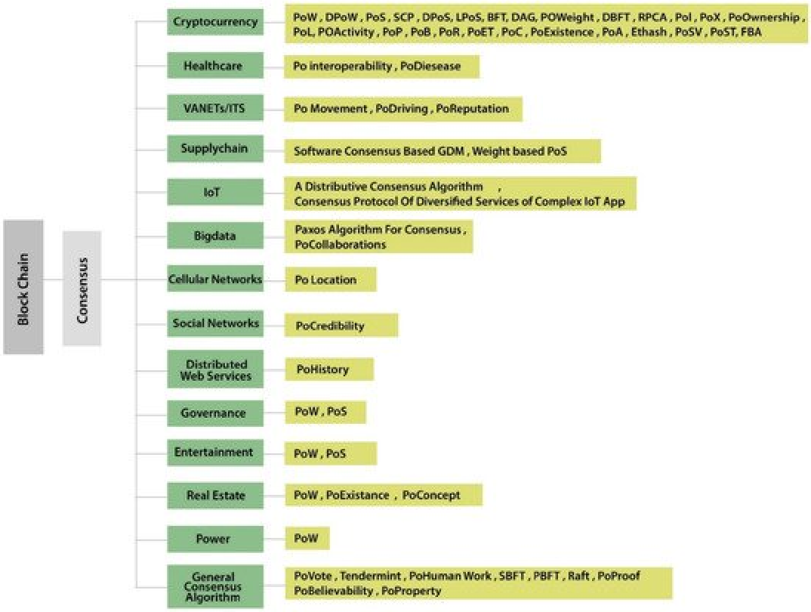

Figure 4. Categorization of the consensus algorithms.

6. Development Platforms

Table 5 describes some of the important features of the development environments.

Table 5. Comparison of blockchain technologies.

Comparison Parameters	Ethereum	Cosmos	Cardano	EOS	Bitcoin	Hyperledger	Corda
Token	ETH	ATOM	ADA	EOS	Bitcoin	n/a	SDK
Public/Private	Public	Public/Private	Public	Public/Private	Public	Public/Private	Private
Programming Languages	Solidity	Java, C++, Python, Go	Haskell	JavaScript, Python, Ruby	Golang	Java, Golang, Node	Kotlin, Java
Consensus Algorithms	Proof of Work (Currently used), Proof of Stake (In Future)	Tendermint (Byzantine Fault-Tolerant, Proof of Stake)	Proof of Stack	Delegated Proof of Stack	Proof of Work	Practical Byzantine Fault Tolerance	Pluggable Consensus
Transactions Per Second	25	10,000	n/a	Millions (theoretically)	1/3 to 1/7	More than 1000	Between 15 and 1678 TPS
Transaction Size	1 MB	250 bytes	n/a	n/a	1 MB	Changeable (depending on framework)	Maximum size in bytes
Open Source	True	True	True	True	True	True	True
Pros	Anyone can write smart contract and anyone can view that contract	Works like a hub for blockchains, based on Tendermint	Scalability, Sidechain which reduces the risk of hacks.	Parallel processing, low latency, free usage (claimed not proven).	Safe and secure, High token value.	Don't use cryptocurrency so it is ideal for business networks.	Designed specifically for financial applications
Cons	Scalability issue, 25 transactions per second is very slow	Complex technology may have compatibility issues with the latest technologies and new blockchains	Maintaining a side chain is complicated and it will require its own miners.	Never actually free, not fully decentralized, the free transaction fee are imposed on everyone who has EOS.	Very slow, not ideal for programming while there are other faster technologies.	There are a lot of frameworks to choose from and they all have different requirements to implement and setup.	Partially decentralized, not much suitable for IoT resource constrained networks

7. Blockchain Challenges

Although blockchain has improved a lot of applications and has a fault-tolerant peer-to-peer network blockchain always comes up with its vulnerabilities. We discuss the possible attacks on a blockchain ledger.

7.1. Denial of Service (DoS) Attacks

The attacker crash a node by flooding a large amount of traffic in a denial of service (DoS) [9]. It prevents authorized users from retrieving the service or resource. Similarly, a distributed denial of service (DDoS) is another type of attack where a node is flooded with malevolent requests. In DDoS multiple attackers attack a single node.

7.2. Sybil Attacks

Multiple identities attacking a larger portion of the network is called a Sybil attack. The invaders can launch numerous false nodes that seem to be honest to their peers. These false nodes take part in falsifying the network to authenticate illegal transactions and to modify valid transactions. They can use virtual machines, several devices, or internet protocol (IP) addresses as bogus nodes for the attack. The peer-to-peer (P2P) network assumes that every participating node contains only one identity. Thus, numerous forged nodes give attackers the ability to repudiate transmitted blocks and to outvote authentic nodes. When an attacker controls a large number of nodes in the network, it increases the chances of double-spending [10].

7.3. Eclipse Attacks

In an eclipse attack [11], specific nodes are isolated from the peer-to-peer network by the attacker. Similar to Sybil attacks, it does not attack the entire network. Once the target node is isolated, the attacker controls all outgoing connections of the node [12]. From there on, the attacker can abuse the target network and dispatch distinctive sorts of attacks on blockchain mining power and agreement components. These attacks include double-spending, engineering block races, selfish mining, and splitting mining power.

7.4. Routing Attacks

In routing attacks [13], a message is intercepted by the attacker in the blockchain network. The attack alters the message and sends it to its neighbors. Furthermore, this attack is divided into a partitioning attack and a delay attack. In a partitioning attack, the entire blockchain network is divided into two or more portions. In a delayed attack, the attacker captures the message and tampers with it. Then, it redirects the tampered message to another blockchain network portion.

Different consensus mechanisms are used by blockchain to develop trust among blockchain peers. However, there are some possible attacks on these consensus mechanisms.

7.5. The 51% Attacks

A miner, having 51% or more hashing power, can initiate a 51% attack in the blockchain network [14]. The 51% attack, enables the attacker to stop the confirmation of a new block. Additionally, the attacker can reverse transactions already confirmed by the blockchain.

7.6. Double Spending

In double-spending, multiple transactions with the same cryptocurrency are performed by a user [15][16]. This transaction is broadcast to each node in that network. This transaction needs to be confirmed by the nodes, this confirmation is time consumable [15]. This time, between two transactions' initiation and confirmation can be a window for the attacker to quickly launch his/her attack [17][18].

7.7. Alternative History Attacks

In an alternative history attack, a transaction is sent to the merchant by the attacker [19][20]. In addition, a double-spending transaction is included by the attacker in an alternative blockchain fork [21][22]. The merchant sends the product after n blocks confirmation. Therefore, the attacker tries to find more than n blocks. If the attacker succeeds, he gains his coins by releasing the fork.

References

1. Velde, F. Bitcoin: A Primer; Essays on Issues the Federal Reserve Bank of Chicago Dec; Federal Reserve Bank of Chicago: Chicago, IL, USA, 2013.
2. Shoker, A. Sustainable blockchain through proof of exercise. In Proceedings of the 2017 IEEE 16th International Symposium on Network Computing and Applications (NCA), Cambridge, MA, USA, 30 October–1 November 2017; pp. 1–9.
3. Brito, J.; Castillo, A. Bitcoin: A Primer for Policymakers; Mercatus Center at George Mason University: Fairfax, VA, USA, 2013.
4. Sun, J.; Yan, J.; Zhang, K.Z. Blockchain-based sharing services: What blockchain technology can contribute to smart cities. Financ. Innov. 2016, 2, 26.
5. Basden, J.; Cottrell, M. How utilities are using blockchain to modernize the grid. Harv. Bus. Rev. 2017, 23, 1–8.
6. Syed, T.A.; Alzahrani, A.; Jan, S.; Siddiqui, M.S.; Nadeem, A.; Alghamdi, T. A comparative analysis of blockchain architecture and its applications: Problems and recommendations. IEEE Access 2019, 7, 176838–176860.
7. Wang, W.; Hoang, D.T.; Hu, P.; Xiong, Z.; Niyato, D.; Wang, P.; Wen, Y.; Kim, D.I. A survey on consensus mechanisms and mining strategy management in blockchain networks. IEEE Access 2019, 7, 22328–22370.
8. Lucas, B.; Páez, R.V. Consensus Algorithm for a Private Blockchain. In Proceedings of the 2019 IEEE 9th International Conference on Electronics Information and Emergency Communication (ICEIEC), Beijing, China, 12–14 July 2019; pp. 264–271.
9. Dinh, T.T.A.; Liu, R.; Zhang, M.; Chen, G.; Ooi, B.C.; Wang, J. Untangling blockchain: A data processing view of blockchain systems. IEEE Trans. Knowl. Data Eng. 2018, 30, 1366–1385.
10. Li, X.; Jiang, P.; Chen, T.; Luo, X.; Wen, Q. A survey on the security of blockchain systems. Future Gener. Comput. Syst. 2020, 107, 841–853.
11. Sayeed, S.; Marco-Gisbert, H. Assessing blockchain consensus and security mechanisms against the 51% attack. Appl. Sci. 2019, 9, 1788.
12. Wüst, K.; Gervais, A. Ethereum Eclipse Attacks; Technical Report; ETH: Zurich, Germany, 2016.
13. Nayak, K.; Kumar, S.; Miller, A.; Shi, E. Stubborn mining: Generalizing selfish mining and combining with an eclipse attack. In Proceedings of the 2016 IEEE European Symposium on Security and Privacy (EuroS&P), Saarbruecken, Germany, 21–24 March 2016; pp. 305–320.
14. Sahay, R.; Geethakumari, G.; Mitra, B. A novel blockchain based framework to secure IoT-LLNs against routing attacks. Computing 2020, 102, 2445–2470.
15. Saad, M.; Cook, V.; Nguyen, L.; Thai, M.T.; Mohaisen, A. Partitioning attacks on bitcoin: Colliding space, time, and logic. In Proceedings of the 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS), Dallas, TX, USA, 7–10 July 2019; pp. 1175–1187.
16. Natoli, C.; Gramoli, V. The blockchain anomaly. In Proceedings of the 2016 IEEE 15th International Symposium on Network Computing and Applications (NCA), Cambridge, MA, USA, 31 October–2 November 2016; pp. 310–317.
17. Pilkington, M. Blockchain Technology: Principles and Applications. In Research Handbook on Digital Transformations; Edward Elgar Publishing: Cheltenham, UK, 2016; Available online: https://www.elgaronline.com/ (accessed on 16 May 2021).
18. Lee, H.; Shin, M.; Kim, K.S.; Kang, Y.; Kim, J. Recipient-oriented transaction for preventing double spending attacks in private blockchain. In Proceedings of the 2018 15th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), Hong Kong, China, 11–13 June 2018; pp. 1–2.
19. Rosenfeld, M. Analysis of hashrate-based double spending. arXiv 2014, arXiv:1402.2009.
20. Pérez-Solà, C.; Delgado-Segura, S.; Navarro-Arribas, G.; Herrera-Joancomartí, J. Double-spending prevention for bitcoin zero-confirmation transactions. Int. J. Inf. Secur. 2019, 18, 451–463.
21. Malik, A.; Gautam, S.; Abidin, S.; Bhushan, B. Blockchain Technology-Future of IoT: Including Structure, Limitations and Various Possible Attacks. In Proceedings of the 2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT), Kannur, India, 5–6 July 2019; Volume 1, pp. 1100–1104.
22. Mechkaroska, D.; Dimitrova, V.; Popovska-Mitrovikj, A. Analysis of the possibilities for improvement of BlockChain technology. In Proceedings of the 2018 26th Telecommunications Forum (TELFOR) IEEE, Belgrade, Serbia, 20–21

7.8. Race Attacks

In the race attack, the attacker creates two transactions. The first transaction is sent to the merchant by the attacker [23][24]. This product is sent by the merchant without confirmation. Meanwhile, the second transaction is broadcast by the attacker to invalidate the first transaction.

7.9. Finney Attack

In the Finney attack [25], two similar transactions i.e., one crediting the target and the other crediting the attacker are used by the attacker [26][27]. This attack mines a block that including the first transaction and delays publishing it. Meanwhile, the attacker mines the second transaction. When the attacker succeeds, he purchases goods with the first transaction. Then, he releases the pre-mined block which includes the first transaction. The attacker receives both goods and coins whereas the merchant finds their transaction invalid [28][29].

8. Blockchain Research Issues

8.1. Blockchain-Based Research Issues in Healthcare

Blockchain has improved the medical and smartphone applications but there are still some security issues as blockchain comes with potential problems. Any industry including healthcare that needs to use blockchain and its devices should train themselves in these areas to improve it. Such education can improve patient-centered data [30][31]. The blockchain experiments in this research need a patient to authorize himself before transferring a record and this could lead to threats. Key leakage and management is another issue that is not addressed. If a key is lost by a patient the data is difficult or impossible to be authenticated or recovered. A mechanism should be discovered for recovering data. Traditional blockchain cannot be enough in the case of a large amount of patient's storage and sharing data so a double blockchain solution is presented by Lejun Zhang [32].

8.2. Blockchain-Based Research Issues/Future Work in Intelligent Transportation System (ITS) and Internet of Things (IoT)

An ITS aims to improve road safety and traffic management [33][34]. Vehicles share information regarding their position, speed, and direction, etc. with other vehicles [35][36] as they carry sensing data via dedicated short-range communication [37]. In ITS, nodes can communicate with each other via different blockchain apps at a large scale autonomously forming decentralized autonomous organizations (DAOs) or decentralized autonomous systems (DASs). Research is needed at the microscopic level of these autonomous agents. Concrete work is also needed in system modeling of self-adaptive, self-evolving, and self-organizing DAOs and DASs. Moreover, mechanisms should be designed for crowd-sourcing incentives. There are more interesting issues in ITS such as credit evaluation of ITS assets and trust-based management which needs more effort of research. Further study needs to be undertaken in smart-contract-based ITS and data security and privacy issues to prevent the easier 51% attack in ITS. Blockchain can be explored more to incorporate with IoT [38] for improving security and privacy in various domains of smart application [39]. G. Ali [40] suggested a blockchain-based framework for access delegation in IoT which produces high throughput in the case of a large number of concurrent requests. Therefore, further investigation needs to be undertaken in such scenarios.

8.3. Blockchain Research Issues/Future Work in Real Estate

Private blockchain using smart contracts can be the best solution for recording transactions of real estate having high transaction fees [41]. Using resource information by a customer can lead to a conclusion about the business work of other customers. So a hybrid blockchain that includes both private and public best features can be deployed to audit the access of data as it provides the most authoritative system for the participating nodes [42].

9. Future Work

In the future, studies can explore more consensus algorithms as in IoT, machine learning, intelligent transportation systems, etc. Applications are not specific to those mentioned in this paper for example banking [43] or related applications can be explored and added. Open blockchain-based research issues in academic subjects like software engineering, databases, and networks, etc must be considered.

November 2018; pp. 1–4.

23. Morganti, G.; Schiavone, E.; Bondavalli, A. Risk Assessment of Blockchain Technology. In Proceedings of the 2018 Eighth Latin-American Symposium on Dependable Computing (LADC), Belgrade, Serbia, 20–21 November 2018; pp. 87–96.
24. Alkhalifah, A.; Ng, A.; Kayes, A.; Chowdhury, J.; Alazab, M.; Watters, P.A. A taxonomy of blockchain threats and vulnerabilities. In Blockchain for Cybersecurity and Privacy; CRC Press: Boca Raton, FL, USA, 2020; pp. 3–28.
25. Dasgupta, D.; Shrein, J.M.; Gupta, K.D. A survey of blockchain from security perspective. J. Bank. Financ. Technol. 2019, 3, 1–17.
26. Alizadeh, M.; Andersson, K.; Schelén, O. A Survey of Secure Internet of Things in Relation to Blockchain. J. Internet Serv. Inf. Secur. 2020, 3, 47–75.
27. Saad, M.; Spaulding, J.; Njilla, L.; Kamhoua, C.; Shetty, S.; Nyang, D.; Mohaisen, A. Exploring the attack surface of blockchain: A systematic overview. arXiv 2019, arXiv:1904.03487.
28. Kaushik, A.; Choudhary, A.; Ektare, C.; Thomas, D.; Akram, S. Blockchain—Literature survey. In Proceedings of the 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Bangalore, India, 19–20 May 2017; pp. 2145–2148.
29. Vokerla, R.R.; Shanmugam, B.; Azam, S.; Karim, A.; De Boer, F.; Jonkman, M.; Faisal, F. An Overview of Blockchain Applications and Attacks. In Proceedings of the 2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN), Vellore, India, 30–31 March 2019; pp. 1–6.
30. McGhin, T.; Choo, K.K.R.; Liu, C.Z.; He, D. Blockchain in healthcare applications: Research challenges and opportunities. J. Netw. Comput. Appl. 2019, 135, 62–75.
31. Lunardi, R.C.; Michelin, R.A.; Neu, C.V.; Nunes, H.C.; Zorzo, A.F.; Kanhere, S.S. Impact of consensus on appendable-block blockchain for IoT. In Proceedings of the 16th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, Houston, TX, USA, 12–14 November 2019; pp. 228–237.
32. Zhang, L.; Peng, M.; Wang, W.; Su, Y.; Cui, S.; Kim, S. Secure and Efficient Data Storage and Sharing Scheme Based on Double Blockchain. CMC Comput. Mater. Contin. 2021, 66, 499–515.
33. Ali, Q.E.; Ahmad, N.; Malik, A.H.; Ali, G.; Rehman, W.U. Issues, challenges, and research opportunities in intelligent transport system for security and privacy. Appl. Sci. 2018, 8, 1964.
34. Ali, Q.E.; Ahmad, N.; Malik, A.H.; Rehman, W.U.; Din, A.U.; Ali, G. ASPA: Advanced Strong Pseudonym based Authentication in Intelligent Transport System. PLoS ONE 2019, 14, e0221213.
35. Taleb, T.; Sakhaee, E.; Jamalipour, A.; Hashimoto, K.; Kato, N.; Nemoto, Y. A stable routing protocol to support ITS services in VANET networks. IEEE Trans. Veh. Technol. 2007, 56, 3337–3347.
36. Taleb, T.; Ochi, M.; Jamalipour, A.; Kato, N.; Nemoto, Y. An efficient vehicle-heading based routing protocol for VANET networks. In Proceedings of the IEEE Wireless Communications and Networking Conference, 2006, WCNC 2006, Las Vegas, NV, USA, 3–6 April 2006; Volume 4, pp. 2199–2204.
37. Qi, W.; Landfeldt, B.; Song, Q.; Guo, L.; Jamalipour, A. Traffic differentiated clustering routing in DSRC and C-V2X hybrid vehicular networks. IEEE Trans. Veh. Technol. 2020, 69, 7723–7734.
38. Alghamdi, N.S.; Khan, M.A. Energy-Efficient and Blockchain-Enabled Model for Internet of Things (IoT) in Smart Cities. CMC Comput. Mater. Contin. 2021, 66, 2509–2524.
39. Alamri, M.; Jhanjhi, N.; Humayun, M. Blockchain for Internet of Things (IoT) Research Issues Challenges & Future Directions: A Review. Int. J. Comput. Sci. Netw. Secur. 2019, 19, 244–258.
40. Gauhar, A.; Ahmad, N.; Cao, Y.; Khan, S.; Cruickshank, H.; Qazi, E.A.; Ali, A. xDBAuth: Blockchain based cross domain authentication and authorization framework for Internet of Things. IEEE Access 2020, 8, 58800–58816.
41. Ahmad, I.; Alqarni, M.A.; Almazroi, A.A.; Alam, L. Real Estate Management via a Decentralized Blockchain Platform. CMC Comput. Mater. Contin. 2021, 66, 1813–1822.
42. Li, M.; Shen, L.; Huang, G.Q. Blockchain-enabled workflow operating system for logistics resources sharing in E-commerce logistics real estate service. Comput. Ind. Eng. 2019, 135, 950–969.
43. R. Arjun; K. R. Suprabha; Innovation and Challenges of Blockchain in Banking: A Scientometric View. *International Journal of Interactive Multimedia and Artificial Intelligence* **2020**, *6*, 7-14, 10.9781/ijimai.2020.03.004.