Open Access Article

A SURVEY OF THE BLOCKCHAIN CONCEPT AND MITIGATION CHALLENGES IN DIFFERENT NETWORKS

Wed Kadhim Oleiwi
wsci.wed.kadhum@uobabylon.edu.iq

Alharith A.Abdullah
alharith@itnet.uobabylon.edu.iq

Abstract
Blockchain is an important technology that is considered to be a hot research subject for its perfect performance in terms of distributed systems and security. Networks are the backbone of life today, and it is found in different aspects such as military, industry, health, scientific works, and monitoring. However, networks tend to suffer from a number of issues (such as threats and attacks) which cause them to fail and prevents them from performing properly. This work presents an introduction to the blockchain technology, followed by the explanation of its distinct features which help in dealing with the aforementioned network issues, enhancing the network performance, and eventually increasing its overall security.

Keywords: Blockchain, Network, Wireless network, IOT network, Wireless Sensor Network (WSN), Ad-hoc network.

抽象的

区块链是一项重要技术，因其在分布式系统和安全性方面的完美表现而被认为是热门研究课题。 网络是当今生活的支柱，它存在于军事、工业、健康、科学工作和监控等不同方面。 然而，网络往往会受到许多问题（例如威胁和攻击）的影响，这些问题会导致它们出现故障并阻止它们正常运行。 这项工作介绍了区块链技术，然后解释了其独特的功能，这些功能有助于处理上述网络问题，提高网络性能，并最终提高其整体安全性。

关键词：区块链、网络、无线网络、IOT 网络、无线传感器网络（WSN）、Ad-hoc 网络。

I. Introduction

Networks play an essential role in making human life easier and more convenient through providing safety and security when deployed in different approaches. In their earlier forms, networks were nothing more than two computers connected together across the world for storing and transmitting information. Today, this technology tends to offer support in different approaches, as new forms of network appear according to their deployment after the connection of a large number of non-traditional devices to the internet [2] [3]. Despite the great progress in the field of networking, it still suffers from some problems that make it vulnerable to various attacks and malfunctions [2] [3].

Received: August 12, 2021 / Revised: September 08, 2021 / Accepted: September 30, 2021 / Published: October 10, 2021
About the authors：Wed Kadhim Oleiwi
Corresponding author- Email: wsci.wed.kadhum@uobabylon.edu.iq

Blockchain technology has slowly started to invade the network as a guaranteed substitution digital model that utilizes cryptography and mathematics. Blockchain has a distributed Peer-to-Peer (P2P) technology deployment to deal with the problem of maintaining the order of transactions [1]. A number of several basic properties are found in Blockchain such as decentralization, transparency, shared ledger based on consensus, immutability, and privacy. These eventually realize the features needed for authentication and authorization like security, decentralization and anonymity [5]. The blockchain technology seems to be a revolution in terms of computer protocols employed to record and store information digitally on multiple devices or multiple nodes. The sharing property is considered to be an important aspect of it: in case the data is only to be used within an organization's own computer network, then the existing technologies and security protocols are sufficient enough to meet that purpose. However, when the data needs to be distributed through security borders, then the blockchain is found to be a more convenient solution [2]. Blockchain is applied for securing and distributing data in a new and unique manner. Eliminating the central entity in the distributed network indicates a major shift to direct transaction between non-intermediaries. This implies that the update of blockchain takes place only by consensus among participants within the system, and a transaction can never be altered or deleted. No hacking, manipulation or disruption can occur to the distributed database as is the case with classic centralized databases with user-controlled access systems [2].

In the networking space, the research's effort continues to solve various problems and issues that have arisen with networks of various structures, eventually leading to their disruption and prevents them from performing their duties in an ideal manner. One of the most recent developments involves the integration of the latest blockchain technology. There are a number of characteristics found in blockchain which suggest that it may help in solving a range of network issues. These characteristics include: data integrity and immutability, automation, reliability, decentralization, security, high availability, and accessibility, as is explained in Table (1) [4].

The present work surveys the current works that deploy the blockchain technology for solving issues in different network types. As compared to other works, this paper offers a comprehensive discussion of the integration and deployment of the new technology blockchain with different kinds of networks, and explains the manner in which such a deployment contributes to the improvement of networks.

The present study can be outlined in the following way: The second section discusses the basic concept of block chain and its structure. The third section displays some of today's networks and their issues, whereas the fourth section surveys the works wherein blockchain is used to solve the aforementioned issues discusses in the previous section. Finally, section V states the conclusions of the study. Figure (1) shows the main outline of the present work.

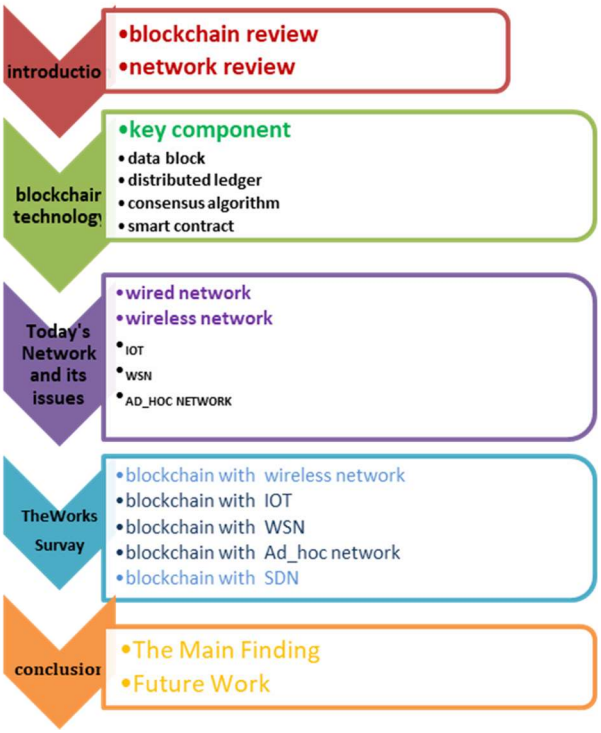

Figure (1) The main body of the work.

II. Blockchain Technology

This technology changes the vital factors so as to resolve key issues like trust within a network, employ innovative security that matches other platforms or record-keeping systems, and deploy hashing and asymmetric encryption. Its core concept is the decentralization of data management system to obtain a great distribution. Every node within the network has an equivalent role to the other nodes and shared the same privileges. In addition, due to its p2p transaction, there is no need for a trusted third party [3]. A number of properties are found in blockchain, like security, immutability, robustness, transparency, and auditability [4]. Therefore, it is used in a number of common software applications including file sharing applications like Ethereum, Napster, and BitTorrent [5] [6], and the messaging application Skype. The most famous application is Bitcoin [7]. Figure (2) shows how blockchain works and processes.

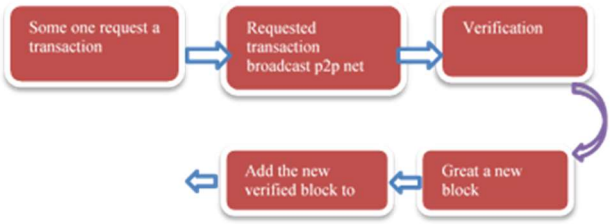

Figure (2): Overview of the blockchain concept.

The main components of Blockchain are listed below:

a- Data block: The blockchain is realized in form of a chain of blocks. When data needs to be transmitted in the system, it undergoes a number of processes to be put in the block format. Then, this block is joined to the blockchain by deploying the hash label, as illustrated in Figure (3). In this way, any transition in the system can be found within this chain, and with no ability of modification [7] [8].

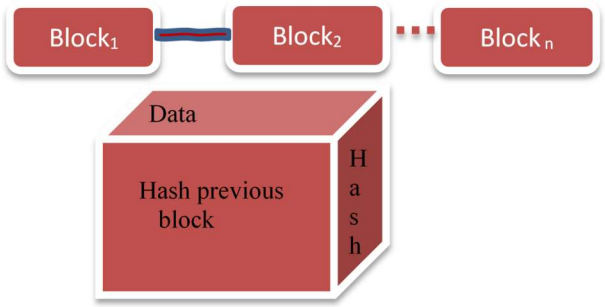

Figure (3): The data block structure

The data block structure mainly includes the block header and block body. The block body is used for storing the transactions after verification, whereas the block header is used to specify meta-data, such as the hashes of the previous and current blocks, the time stamp, nonce, and Merkle root [7].

b- Distributed ledger: A distributed ledger is one of the digital systems used for the footage of

transactions at various places. It is a database that is consensually shared and synchronized across many locations, institutions or layouts. The distributed database used in blockchain is a kind of shared database, whereby every member of the blockchain system has authentication to reach it. The ledger play involves peer-to-peer complete visibility in the system, which is necessary to ensure a auditable and transparent transfer process, as shown in Figure (3) [8] [9].

c-Consensus algorithm: Due to the distributed system, there is no central management for the transition process in the system among its peers. Some security issue appear as fraud issues, which require a mechanism to build trust and reliability among members. This is achieved through the consensus algorithm, which involves a procedure through which all the peers of the Blockchain network reach a corporate contract around the present state of the distributed ledger. Examples of consensus algorithms include the Proof of Work (PoW) and Proof of Stake(PoS) [9].

d- Smart contract: It can be described as a transaction protocol or computer program intended to run in the blockchain system. It functions as a regulator or legally significant transition and takes action according to the rules of a contract or arrangement. Ethereum is the first platform for smart contracts [9].

Table (1) shows the main properties of blockchain technology that make it appropriate to be dealt with.

Table (1): The main advantages of Blockchain Technology

Advantage/service	Description
Data integrity and Immutability	It reduces fraud while strengthening regulatory compliance
Automation	Smart Contracts which are self-executed code commands can be stored and executed on Blockchain
Reliability	It is regulated by a single control center and there is no single point of failure
Decentralization	It removes the need for a third-party to intermediate, avoiding all the additional overhead cost and transaction fees
Security	All transactions will be digitally time stamped with a cryptographic hash code. A unique 64-digit alpha-numeric signature is recorded corresponding to every single transaction.
High availability and Accessibility	Due to decentralized networks, Blockchain Technology data would be complete, timely and accurate

III. Today's Network and its Issues

Since the Internet is used all around the world, its increasingly expanding access involves a huge number of attacks which are not covered current secure communication protocols. Possible attacks include hacking attempts, viruses, worms, cyber bullying, theft of identity, DoS, and Distributed DoS (DDoS). There are several mechanizations suggested to deal with such attacks such as identity management and encryption schemes for the confidentiality of communication channels. In this section, a number of network categories will be discussed, as well as the issues that appear with each category [10] [11].

A network can be categorized based on the links that form the connection among devices [10] :

a- Wired Network: This type of network requires a kind of physical medium which consists of a cable. It can be made up of fiber optics, twisted pair, or copper. In this kind of network, there is only one device attached to a single cable, and the data is mutual among the different devices by using this same concept of wire network.

There ae a number of issues with this kind of networks. First, the connection: Cables can be easily damaged after some time and there is no freedom of movement for users. Second, it is expensive: When expanding the network, there are more cables needed. Therefore, it will be more costly and it takes lots of time to re-start the network. Third, It is not suitable for openly public usage [10] [12].

b- Wireless Network: The revolution of wireless networks brought ultimate modifications to data networking and telecommunication. The users became completely free within their personal communication networks, as the wireless LAN's, mobile radio networks and cellular systems all provide fully distributed mobile communications wherever and whenever wanted. Various technologies have arisen with wireless networks [10]. Wireless NET is the unguided data communication network within the borderline area, offering flexibility to the administrations and users, increased productivity, portability, and lower installation costs, as it is networked without infrastructure. Wireless Network portable/mobile devices are the most established forms today [10]. The most commonly used wireless devices are smart phones, mobile phones, laptops, PDAs, and TVs [11] [12] [13].

The issues found in this kind of network can be stated as follows. First, hardware architecture and firmware: This problem arises due to the insufficient number of access points or having outdated firmware. Second, physical object interference: The design and placement of the crucial network elements affect the reliability of the network. Third, RF interference could be affected by devices which release electro-magnetic signals. Fourth, incorrect antenna configuration: their location can create a huge difference [12] [13].

b.1- Internet of Things (IoT) Network: It is a network of different kind of objects with unique identity that have the ability to communicate with each other without any human-to-human or human-to-computer interaction [14]. The IoT is a structure of consistent computing, mechanical, digital objects, people, or animals which can transfer and deliver data over a network. The fundamental characteristics of the IoT network include its interconnectivity, heterogeneity, dynamic changes, and its enormous scale [15][16].

There are several issues related to the use of IoT networks. First, device management: Its devices are often placed in inaccessible locations are, meanwhile making remote updates and diagnostics are a must. Second, connectivity: Managers must be sure that their access points can deal with a large number of IoT devices [16][17]. Third, the cyber security venture should use exclusive and secure, password-protected wireless networks to confirm the data encryption. Fourth, data management: IOT networks generate extraordinary volumes of data which require sufficient management. Fifth, power management: Given the increasing number of devices, it is necessary to keep the power managing criteria compatible with it [18] [19] [20].

b.2-Wireless Sensor Network: These are networks of sensor devices and nodes that sense their environment through which they are spread, so as to gather information about the surrounding area and send the information through wireless channels. Multiple hops are involved to forward the information, to a pool which is locally used or is connected to another network through gateways [20]. Sensor nodes can be either stationary or moving [20]. There are many applications and situations that require such kinds of network, such as environmental monitoring, medical applications, military applications, industrial applications, and security applications [20] [21].

The main issues faced in this type of networks are as follows. First, Fault-tolerant communication is common where one or more the sensor nodes are faulty or of no reliability. Second, low latency: The events need to be detected from the context as speedily as possible. Third, the number of sensor nodes used within the environment could reach hundreds or even thousands. Fourth, the transmission media: The traditional complications associated with wireless channel may affect the sensor network. Fifth, the coverage problems reflect the (QOs) to be provided. Sixth, power and resource managements: The deployment of sensor nodes in harsh environment leads to limitations in resources [21] [22] [23].

b.3- Ad-hoc Network: These can be defined as decentralized wireless networks without any infrastructure. The network connectivity determines in a dynamic way which nodes are to forward the data. Different forwarding protocol like OLSR, AODV, and DSR are deployed to supply the paths to all nodes participating within the routing to forward the data to other nodes. This pattern of communication creates the phenomenon of multiple hops [22] [23]. The in-between nodes act as routers to route packets to the target nodes, where the nodes makes the decision to choose the appropriate path to direct or forward the packet.

There are several issues and challenges when realizing the benefits of Ad-hoc networking [23], as follows. First, routing: The paths between the nodes actually contain multiple hops, which increase the difficulty of communication, unlike the single hop directive. Second, security: Security issues appear due the self-organization behavior and membership, attacked wireless links, and roaming in harsh areas. Third, Quality of Service (QoS): The resource limitation and self-organization topology cause issues in terms of deferred information or services. Fourth, TCP variants: TCP cannot adapt fully with multi-hop networks [24] [25]. Table (2) show the contribution of blockchain to deal with several different network issues.

Table (2): Blockchain contribution to the management of different networks issues [8][9].

Issues	Network	How blockchain can deal with it
security	All	1- Digital signature (public key, private key) infrastructure. 2-Immutable ledger. 3- Cryptographically.
Power and resource management	IOT, WSN, ad-hoc	1-Smart contract . 2-Distributed leger.

Data storage and management	IOT, WSN	1- Immutable distributed ledger.
Data integrity	ALL	1-Immutable distributed ledger. 2-Consensus algorithm.
Point of Failure	IOT, WSN, central SDN	1-Distributed nature of blockchain (p2p network)
Authenticatio n	all	1-Smart contract 2-Identity management 3-Distributed ledger
Scalability and flexibility	IOT, WSN	1-Distributed nature of blockchain (p2p network)

IV. A- The deployment of blockchain to deal with network issues

This section displays the role that blockchain plays in different kind of network, as well as its contribution to solving various issues, as shown in Figure (4).

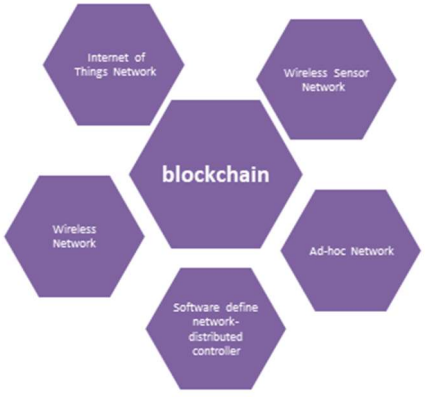

Figure (4): Contribution of Blockchain to different types of networks.

a- Blockchain for Wireless Network

Blockchain plays an effective role in enhancing the RF spectrum utilization in wireless network. A public ledger-based scheme for creating VWNs is used whereby primary wireless resource-owners (PWROs) sublease their wireless resources. The distributed Blockchain-based scheme will provide security as well as the desired QoS requirements [31]. A blockchain consensus-based scheme is used for verifying the authenticity of channel state information (CSI), and adding the users who intentionally advocate a higher CSI value within the fraud chain. This improves the network performance by powerfully controlling the use access in mobile applications [32]. Blockchain Radio Access Network (B-RAN) architecture with an advanced distribution and secure and well-organized apparatuses are used to manage network access and authentication among essentially trustless network units. Large self-organized RAN can be advanced by virtually linking several entities without relying on powerful information-aware and resource-rich network centers [33]. Another work that deploys blockchain in energy consumption with wireless network is [34] whereby the blockchain is presented for recording power data which is collected through the wireless network, which in turn enables the smart contract to reasonably decide upon trading aspects.

b- Blockchain for IoT Networks

A wide deployment of the emerging blockchain technology is found in IoT networks, especially in terms of energy consumption. The high resource devices form an overlay network for implementing a publicly available decentralize

BC in order for guaranteeing privacy and security to end-to-end networks. The proposed design uses decentralize confidence to reduce the time that is required to block validation [35]. The blockchain technology concept is chosen to increase the security of IoT network, and provide flow tables within a distributed blockchain network. The updated scheme of flow rule tables using the blockchain techniques is proposed for the secure verification, validation and download of flow rule tables for IoT forwarding devices. The security of systems depend on monitoring and parsing incoming packets [36]. The study in [37] takes into account the scalability of IOT network, and proposes a design for the organization of IoT devices. The architecture offers a distributed access control scheme that is connected to geologically spread network of the sensor. A blockchain-enabled architecture of high security and energy-efficiency for SDN controllers in IoT networks is presented in [38], whereby a cluster structure is used with a routing protocol. Both public and private blockchains are used for P2P connections among IoT devices and SDN controllers, thereby eliminating the need for PoW. The adopted authentication method of distributed trust makes blockchain a sufficient technique to be used with devices of resource constrain in IoT.

c- Blockchain in Wireless Sensor Network

This section reviews the contribution of blockchain to WSN networks. The design depends on the structure of blockchain used to store decentralized authentication and node trust info. This model is evaluative, adaptive and certifies the reliability over time. The work in [39[addresses the issues security and privacy on one hand, and those of authentication and trust management on the other hand. Another work that deals with data storage with blockchain in WSNs is [40], whereby blockchain is employed for constructing the first incentive node mechanism as per data storage. The data storage machine is salaried with digital money. The work in [41] proposed a model of malicious nodes to deal with the security issues in wireless sensor network. It involves a blockchain trust model (BTM) with the WSNs quadri-lateral measuring localization method. In addition, the blockchain smart contract, detection of malicious nodes in 3D, and voting consensus results are recorded within the blockchain distribution. As for [42], a management model was proposed based on blockchain in order to develop an association between eradicate malicious nodes and beacon nodes. The model rejects the beacon with minimum trust value in order to provide the consistency and reliability of localization in WSNs.

d-Blockchain with Ad-hoc Networks

In this kind of networks, the blockchain contributes to its improvement and development through the integration of different IT systems and different technologies. The study in [43] implements Smart Energy Grid, whereby the blockchain granting ledger is used to connect the Grid, exchange information, and trade energy among the convoluted nodes. Blockchain plays a significant role in aiding communications, security and transaction amongst the stakeholders involved with a Smart Energy Grid [43]. In the context of security, the authors in [44] worked on preventing the mislead of the whole communication by malicious users within the internet of vehicles, whereby malicious ploy intruders compromise smart devices. The technique offers secrecy and safety in real time conditions to the control system between the

customers via blockchain, so as to ensure the clearness and security between customers and drivers by the blockchain [44]. Another work that deals with the message consistency and identity legitimacy is [45], whereby vehicle nodes segment data with further vehicle by allowing vehicles to upload sensor data to a reliable center for storage, so that it is susceptible to security dangers like data leakage and malicious tampering. This is necessary to limit the triggering conditions for prenominated nodes when storing and transmitting data for the apportioning of data coins to vehicles in of data smart contracts. In [46], a key derivation algorithm is associated with the blockchain technology in order to recognize an operative documentation management so as to decrease the necessity for participating vehicles to supply a large number of private keys.

B-Blockchain with SDNs:

This section addresses the contribution of blockchain to in the promising network type of software define networks (SDNs). These can be define as "the decoupling of control and packet forwarding planes within the network". The network is directly connected to the API, bolstering application performance and security. This creates an architecture of high flexibility and dynamicity which could be altered according to the demands [24] [25].

There are two aspects involved in the application of blockchain with Software Define Networks. The first is related to the central SDN. In the field of security of central SDN, the work in [47] focuses on the security of the central controller, whereby the controller plane escapes the false flow rules in the forward of layer devices and the injection of the attacker. As for the authentication issues, the work in [48] proposes a different method in authentication whereby the blockchain and SDN-based technique is used for re-authenticating heterogeneous entities, and the repetitive exchange of private and public keys that are supplied through the developed blockchain module. The second side involves the deployment of blockchain with decentralize (distributed) SDN control plane The study in [49] employs blockchain with distributed SDN controllers. The blockchain connects all controllers is a distributed way using various control domains and master-slave roles. The smart contracts apply to the consistent data operation within the distributed ledger for providing the customized network function. As for the work in [50], they propose a uniform security mechanism for SDN using Blockchain. The mechanism involves the decentralization of the control plane to treat the problem of single-point failures, whereas the maintenance of a network-wide view depends on the blockchain layer that is recorded. The authenticity, traceability, and accountability of application flows are hereby guaranteed, so that the programmable configuration is secured using the authentication algorithm to access control among controller-app. Moreover, secure controller-switch channels are applied for further protecting the resources and communications within SDN using the security protocol.

Through this approach, an integrated system of blockchain-based SDN is suggested which obtains a number of advantages via both technologies of SDN and blockchain. These include how adaptable, available, reliable, scalable, and secure the system is. Such an integration addresses several security issue found in SDN controllers using blockchain and distributed architecture. As for the scalability issue of blockchain, it can be solved through the

use of the distributed SDN, in addition to the reconfiguration protocol that retrieves the setup of SDN controllers, as shown in Figure (5).

Table (3) shows the forms of contribution that the blockchain technology provides within different types of networks. It presents the role that the blockchain technology plays in improving and addressing some of the networks issues including security, scalability, data storage, energy consumption, and the authentication, as explained in Figure (6).

V-Conclusion

The essential features for which the blockchain technology is really valued are its decentralized infra-structure and its ability of including secure chains of historical exchanged data through the verification of all data exchanges using timestamps in P2P networks. This implies that exchanging data does not require a central authority. Moreover, the applications of blockchain extend to a number of fields, as it could realize trust and security through the use of software programs for verifying and validating consensus in new infra-structures. This paper provides a comprehensive overview of blockchain and addresses different aspects like transactions, consensus algorithm, and distributed ledger. It then presents an overview of the basic issues faces in different types of networking, and how the blockchain technology might contribute to solving them, especially in terms of security, scalability, data integrity, data storage, power and resource management, authentication and authorization spectrum management, interference management, and data sharing. Future re4search might include the comprehensive investigation of blockchain in light of its applications and its use in smart contracts.

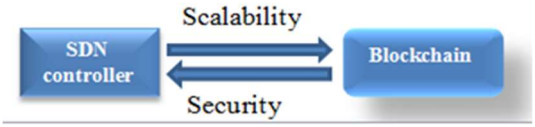

Figure (5) The integration between SDN and blockchain

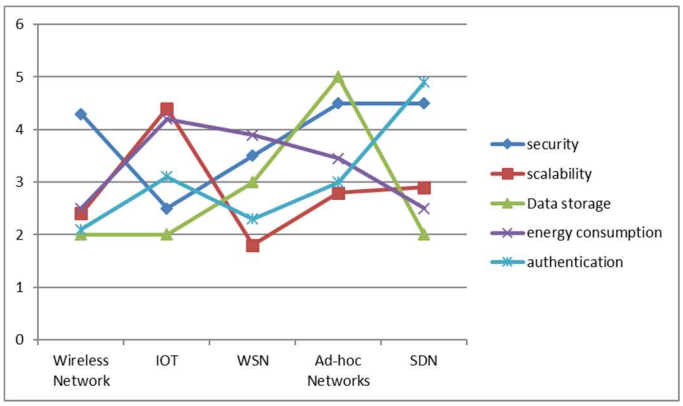

Figure (6): The Blockchain technology contribution in enhancing networks issues.

Table (3):The contribution of Blockchain technology to different types of network

Proposed work	***Network type***	***The benefit of employing the blockchain in the network***	***Description***
[28] Zhang, G.	Wireless Network	Security Data Shared	It is a system that is based on smart contracts whereby the supervision and fine-grained data access control are combined.

			This creates an environment of high security to share data.
[29] Jiang, Xin & Liu	Wireless Network	User's Authentication	All authentication records within the network are considered to be the public ledger, and therefore tends to realizes an efficient observation of malicious aspects.
[30] Ren, Y. & Leng,	Wireless Network	Store Data	It increases the security of the collected data through proposing a sequential aggregate signature scheme using designated verifiers for ensuring that only the designated users have access to the user data.
[31] D. B. Rawat,	Wireless Network	Enhance RF Spectrum Utilization	It is a distributed Blockchain-based scheme for providing security in addition to the aimed QoS criteria.
[32]Lin, Di, and Yu Tang	Wireless Network	Authenticity Of Channel	It is a blockchain consensus-based scheme for verifying the authenticity of CSI and the addition of users that perform an intentional advocating of higher CSI values within the fraud chains
[33]Ling, Xintong,	Wireless Network	Secure and Well-Organized	It is a B-RAN architecture with an advance distribution
[34]Z. Liu, D. Wang,	Wireless Network	Energy Consumption	The blockchain records power data that is collected through the wireless network so that smart contract can reasonably decide upon the trading.
[35] Dorri, Ali,	Internet Of Things Network	Privacy and Security	The decentralized confidence is used for reducing the time needed for validating the block.
[36] P. K. Sharma	Internet Of Things Network	Security Of IoT	The scheme is updated to flow rule tables using the blockchain technique for the secure verification of the latest flow rule table versions.
[37]Novo, Oscar	Internet Of Things Network	Scalability Of IoT	The architecture offers a distributed access control scheme connected to geologically spread network of the sensor
[38]A. Yazdinejad	Internet Of Things Network	Secure and Energy-Efficient	Both public and private blockchains are used in P2P communication among IoT devices and SDN controllers

[39] Moinet, Axel	Wireless Sensor Network	Authentication and Trust Management	It is a design that depends on the structure of blockchain used to store decentralized authentication and node trust information
[40] Ren, Yongjun	Wireless Sensor Network	Data Storage	The blockchain is employed to construct the first incentive node mechanisms as per data storage
[41] She, Wei,	Wireless Sensor Network	Security	It proposes a model for Malicious Node, whereby a blockchain trust model (BTM) is used for WSNs
[42] Kim, Tai-Hoon,	Wireless Sensor Network	Consistency and Reliability	The management model was proposed based on blockchain in order to develop an association between eradicate malicious nodes and beacon nodes
[43] Pieroni, Alessandra	Ad-Hoc Network	Security	Blockchain is used for the connection of the Grid, the exchange of information, and the trade of energy among the convoluted nodes
[44] Rathee, Geetanjali	Ad-Hoc Network	Prevent a Mislead	The technique offers secrecy and safety in real time conditions to the control system among the customers using blockchain.
[45] X. Zhang and X. Chen	Ad-Hoc Network	Message Consistency and Identity Legitimacy	Dangers like data leakage and malicious tampering are addresses for limiting the triggering conditions in prenominated nodes when storing and transmitting data for apportioning data coins to vehicles to contribute to data smart contracts
[46] C. Lin, D. He, X. Huang	Ad-Hoc Network	Recognize an Operative Documentation Management	The key derivation algorithm is associated with the blockchain technology in order to recognize an operative documentation management due to decreases the necessity of vehicles to supply a huge number of private keys.
[47]S. Boukria,	Software Define Network-Central Controller	Security	The attacker enters through escaping the false flow rules that in forwarding layer devices.
[48] A. Yazdinejad	Central Software Define	Authentication	Blockchain and SDN based techniques are used in ejecting the re-authentication in heterogeneous

	Network-Central Controller		
[49] H. Yang and Y. Liang	Software Define Network-Distributed Controller	Consistent Data Operation	It employs blockchain with distributed SDN controllers, whereby all of the latter are linked via blockchain in a distributed manner in various control domains
[50] Jiasi, Weng and Jian	Software Define Network-Distributed Controller	Single-Point Failure	It proposes a uniform security mechanism for SDN in light of the blockchain technique, whereby the control plane is decentralized to treat the problem of single-point failures.

References

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

[2] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in 2017 IEEE International Congress on Big Data (BigData Congress), 2017, pp. 557-564.

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

[4] X. Xu, I. Weber, M. Staples, L. Zhu, J. Bosch, L. Bass, et al., "A taxonomy of blockchain-based systems for architecture design," in 2017 IEEE International Conference on Software Architecture (ICSA), 2017, pp. 243-252

[5] N. Andrade, M. Mowbray, A. Lima, G. Wagner, and M. Ripeanu, \Inuenceson cooperation in bittorrent communities," in Proceedings of the 2005 ACM SIGCOMM workshop on Economics of peer-to-peer systems. ACM, 2005, pp.111{115.

[6] G. Fox, \Peer-to-peer networks," Computing in Science & Engineering, vol. 3,no. 3, pp. 75{77, 2001.

[7] S. Guha and N. Daswani, \An experimental study of the skype peer-to-peer voipsystem," Cornell University, Tech. Rep., 2005. Reviews, vol. 100, pp. 143-174, 2019.

[8] W. Yang, S. Garg, A. Raza, D. Herbert, and B. Kang, "Blockchain: trends and future," in Pacific Rim Knowledge Acquisition Workshop, 2018, pp. 201-210.

[9] H. F. Atlam and G. B. Wills, "Technical aspects of blockchain and IoT," Role of Blockchain Technology in IoT Applications, vol. 115, p. 1, 2019.

[10] G. W. Peters and E. Panayi, "Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money," in Banking beyond banks and money, ed: Springer, 2016, pp. 239-278.

[11]F. Alaba, M. Othman, I. Hashem and F. Alotaibi, “Internet of Things security: A survey”, Journal of Network and Computer Applications, 88, pp.10-28, 2017.

[12] H. Kim and E. A. Lee, "Authentication and Authorization for the Internet of Things," in IT Professional, vol. 19, no. 5, pp. 27-33, 2017. doi: 10.1109/MITP.2017.3680960

[13] Jurcut, A., Coffey, T., Dojen, R. and Gyorodi, R., “Analysis of a key-establishment

security protocol", Journal of Computer Science and Control Systems, Vol. 2008, ISSN 1844-6043, pp. 42-47, 2008.

[14] Jurcut, A.D., Liyanage, M., Chen J., Gyorodi C., He, J., "On the Security Verification of a Short Message Service Protocol", 2018 IEEE Wireless Communications and Networking Conference (WCNC), Barcelona, Spain, April 2018. DOI: 10.1109/WCNC.2018.8377349

[15] J. Deogirikar and A. Vidhate, "Security attacks in IoT: A survey," 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, 2017, pp. 32-37, DOI: 10.1109/I-SMAC.2017.8058363

[16]K. Lee, D. Kim, D. Ha, U. Rajput and H. Oh, "On security and privacy issues of fog computing supported Internet of Things environment," 2015 6th International Conference on the Network of the Future (NOF), Montreal, QC, 2015, pp. 1-3, doi: 10.1109/NOF.2015.7333287.

[17] I.F. Akyildiz, E.P. Stuntebeck, Wireless underground sensor networks: research challenges, Ad-Hoc Networks 4 (2006) 669–686.

[18] M. Li, Y. Liu, Underground structure monitoring with wireless sensor networks, in: Proceedings of the IPSN, Cambridge, MA, 2007.

[19] I.F. Akyildiz, D. Pompili, T. Melodia, Challenges for efficient communication in underwater acoustic sensor networks, ACM Sigbed Review 1 (2) (2004) 3– 8.

[20 J. Heidemann, Y. Li, A. Syed, J. Wills, W. Ye, Underwater sensor networking: research challenges and potential applications, in: Proceedings of the Technical Report ISI-TR-2005-603, USC/ Information Sciences Institute, 2005.

[21] I.F. Akyildiz, T. Melodia, K.R. Chowdhury, A survey on wireless multimedia sensor networks, Computer Networks Elsevier 51 (2007) 921–960.

[22] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, 2002 Wireless sensor networks: a survey, Computer Networks, vol 38, no. 4, pp. 393-422, (March 2002.)

[23] Pirmez, L., Delicato, F., Pires, P., Mostardinha, A., de Rezende, N.:2007 Applyingfuzzy logic for decisionmaking on wireless sensor networks. In: Fuzzy Systems Conference '07, Proc., IEEE (2007).

[24] J. Duato, "A necessary and sufficient condition for deadlock-free routing in cut-through and store-and-forward networks," IEEE Trans Parallel and Distrib. Systems, vol. 7, no. 8, pp. 841-854, Aug. 1996.

[25] Barakabitze, Alcardo & Ahmad, Arslan & Hines, Andrew & Mijumbi, Rashid. (2019). 5G Network Slicing using SDN and NFV: A Survey of Taxonomy, Architectures and Future Challenges. Computer Networks. 167. 106984. 10.1016/j.comnet.2019.106984.

[26]Chuck Black and Paul Goransson . "Software Defined Networks: A Comprehensive Approach." (2014).

[27] Yustus Eko Oktian, SangGon Lee, HoonJae Lee, JunHuy Lam, Distributed SDN controller system: A survey on design choice, Computer Networks, Volume 121, 2017, Pages 100-111, ISSN 1389-1286.

[28] Zhang, G., Li, T., Li, Y. et al. Blockchain-Based Data Sharing System for AI-Powered Network Operations. J. Commun. Inf. Netw. 3, 1–8 (2018). https://doi.org/10.1007/s41650-018-0024-3

[29] Jiang, Xin & Liu, Mingzhe & Yang, Chen & Liu, Yanhua & Wang, Ruili. (2019). A Blockchain-Based Authentication Protocol for WLAN Mesh Security Access. Computers,

Materials & Continua. 58. 45-59. 10.32604/cmc.2019.03863.
[30] Ren, Y., Leng, Y., Zhu, F., Wang, J., & Kim, H. J. (2019). Data Storage Mechanism Based on Blockchain with Privacy Protection in Wireless Body Area Network. Sensors (Basel, Switzerland), 19(10), 2395. https://doi.org/10.3390/s19102395
[31] D. B. Rawat and A. Alshaikhi, "Leveraging Distributed Blockchain-based Scheme for Wireless Network Virtualization with Security and QoS Constraints," 2018 International Conference on Computing, Networking and Communications (ICNC), Maui, HI, 2018, pp. 332-336, doi: 10.1109/ICCNC.2018.8390344.
[32]Lin, Di, and Yu Tang. "Blockchain consensus based user access strategies in D2D networks for data-intensive applications." IEEE Access 6 (2018): 72683-72690.
[33]Ling, Xintong, et al. "Blockchain radio access network (B-RAN): Towards decentralized secure radio access paradigm." IEEE Access 7 (2019): 9714-9723.
[34]Z. Liu, D. Wang, J. Wang, X. Wang and H. Li, "A Blockchain-Enabled Secure Power Trading Mechanism for Smart Grid Employing Wireless Networks," in IEEE Access, vol. 8, pp. 177745-177756, 2020, doi: 10.1109/ACCESS.2020.3027192.
[35] Dorri, Ali, Salil S. Kanhere, and Raja Jurdak. "Towards an optimized blockchain for IoT." 2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI). IEEE, 2017.
[36] P. K. Sharma, S. Singh, Y. Jeong and J. H. Park, "DistBlockNet: A Distributed Blockchains-Based Secure SDN Architecture for IoT Networks," in IEEE Communications Magazine, vol. 55, no. 9, pp. 78-85, Sept. 2017, doi: 10.1109/MCOM.2017.1700041
[37]Novo, Oscar. "Blockchain meets IoT: An architecture for scalable access management in IoT." IEEE Internet of Things Journal 5.2 (2018): 1184-1195.
[38]A. Yazdinejad, R. M. Parizi, A. Dehghantanha, Q. Zhang and K. -K. R. Choo, "An Energy-Efficient SDN Controller Architecture for IoT Networks With Blockchain-Based Security," in IEEE Transactions on Services Computing, vol. 13, no. 4, pp . 625-638, 1 July-Aug. 2020, doi: 10.1109/TSC.2020.2966970.
[39]Moinet, Axel, Benoît Darties, and Jean-Luc Baril. "Blockchain based trust & authentication for decentralized sensor networks." arXiv preprint arXiv:1706.01730 (2017).
[40] Ren, Yongjun, et al. "Incentive mechanism of data storage based on blockchain for wireless sensor networks." Mobile Information Systems 2018 (2018).
[41] She, Wei, et al. "Blockchain trust model for malicious node detection in wireless sensor networks." IEEE Access 7 (2019): 38947-38956.
[42] Kim, Tai-Hoon, et al. "A novel trust evaluation process for secure localization using a decentralized blockchain in wireless sensor networks." IEEE Access 7 (2019): 184133-184144.
[43] Pieroni, Alessandra, et al. "Smarter city: smart energy grid based on blockchain technology." Int. J. Adv. Sci. Eng. Inf. Technol 8.1 (2018): 298-306.
[44] Rathee, Geetanjali, et al. "A blockchain framework for securing connected and autonomous vehicles." Sensors 19.14 (2019): 3165.
[45] X. Zhang and X. Chen, "Data Security Sharing and Storage Based on a Consortium Blockchain in a Vehicular Ad-hoc Network," in

IEEE Access, vol. 7, pp. 58241-58254, 2019, doi: 10.1109/ACCESS.2018.2890736.
[46] C. Lin, D. He, X. Huang, N. Kumar and K. R. Choo, "BCPPA: A Blockchain-Based Conditional Privacy-Preserving Authentication Protocol for Vehicular Ad Hoc Networks," in IEEE Transactions on Intelligent Transportation Systems, doi: 10.1109/TITS.2020.3002096.
[47]S. Boukria, M. Guerroumi and I. Romdhani, "BCFR: Blockchain-based Controller Against False Flow Rule Injection in SDN," 2019 IEEE Symposium on Computers and Communications (ISCC), Barcelona, Spain, 2019, pp. 1034-1039, doi: 10.1109/ISCC47284.2019.8969780.
[48] Yazdinejad, Abbas, et al. "Blockchain-enabled authentication handover with efficient privacy protection in SDN-based 5G networks." IEEE Transactions on Network Science and Engineering (2019).
[49] H. Yang, Y. Liang, Q. Yao, S. Guo, A. Yu, and J. Zhang, “Blockchain based secure distributed control for software defined optical networking,” China Communications, vol. 16, no. 6, pp. 42–54, 2019
[50] Jiasi, Weng & Jian, Weng & Jia-Nan, Liu & Zhang, Yue. (2019). Secure Software-Defined Networking Based on Blockchain