Digital Communications and Networks xxx (xxxx) xxx

Contents lists available at ScienceDirect

Digital Communications and Networks

journal homepage: www.keaipublishing.com/dcan

Can blockchain link the future?

Liang Qiao [a], Shuping Dang [b], Basem Shihada [b], Mohamed-Slim Alouini [b], Robert Nowak [c], Zhihan Lv [a,*]

[a] College of Computer Science & Technology, Qingdao University, Qingdao, 266071, China
[b] Computer, Electrical and Mathematical Sciences and Engineering Division, King Abdullah University of Science and Technology, Thuwal, 23955-6900, Saudi Arabia
[c] Institute of Computer Science, Warsaw University of Technology, Nowowiejska 15/19, 00-665, Warsaw, Poland

ARTICLE INFO

Keywords:
Blockchain
Consensus algorithm
Scalability
Smart contract
Internet of things
Digital twins

ABSTRACT

Recently, decentralization has been extensively explored by researchers. Blockchain, as a representation of decentralized technology, has attracted attention with its unique characteristics, such as irrevocability and security. Consequently, herein, we introduce cutting-edge blockchain technologies from four directions: blockchain system, consensus algorithms, smart contract, and scalability. Subsequently, we analyze the current lack of consensus mechanism, fault tolerance, and block capacity of the blockchain, and the integration of blockchain into 5G/6G mobile communication. Furthermore, we discuss the possible applications of blockchain in intellectual property protection, the Internet of Things, digital twins, standardization, and epidemic prevention and control. Finally, explore the impacts and solutions of blockchain on human society beyond technology.

1. Introduction

Since Satoshi Nakamoto published a paper called Bitcoin: A Peer-to-Peer Electronic Cash System in 2008, blockchain, a decentralized ledger and database technology, has been extensively discussed among researchers because of its irrevocability, collective maintenance, traceability, and other promising characteristics [1,2]. With the development of big data, distributed storage, and 5G/6G network, blockchain has been widely applied in various fields, such as governments, finances and supply chains [3–7].

In this perspective, we consider the opportunities and challenges of blockchain by reviewing the recent research in key technologies of bitcoin and Ethereum (i.e., two representatives of blockchain in cryptocurrency) considering consensus algorithms, smart contracts, scalability, and other applications. To expand, blockchain must upgrade from blockchain 1.0, which is simply a programmable cryptocurrency system, to blockchain 2.0, a programmable financial system, or blockchain 3.0, i.e., a programmable social system [8]. Fig. 1 shows the evolution of blockchain. However, to enable, the following problems must be solved. First, a new consensus mechanism that does not rely on computing power must be urgently developed to save energy sources and break the monopoly of “big computing power” institutions on the recording right. In addition, the storage capacity of the blockchain must be substantially improved to facilitate its application in big data scenarios that rely on extremely heavy data transmission. Furthermore, transactions on these blocks should become transparent and visible, and a black box data verification mechanism must be developed to protect the user's digital privacy. Fortunately, 5G/6G mobile communication technology and edge computing provide opportunities for achieving the above blockchain development [9–12].

To this end, we provide a comprehensive and systematic framework in this perspective. In particular, we discuss the challenges and opportunities associated with blockchain. Then, we then anticipate and subdivide the potential applications of blockchain and explore issues beyond technology that can significantly affect the research and deployment of blockchain.

2. Background

To justify our blockchain vision, we begin by providing the background of key blockchain technologies that cover the blockchain system, consensus algorithms, smart contracts, and scalability.

2.1. Blockchain system

Blockchain is the key technology of the digital cryptocurrency system represented by bitcoin. It is a model based on distributed ledgers, asymmetric encryption, consensus mechanism, smart contracts, and

* Corresponding author.
E-mail address: lvzhihan@gmail.com (Z. Lv).

https://doi.org/10.1016/j.dcan.2021.07.004
Received 3 November 2020; Received in revised form 9 July 2021; Accepted 12 July 2021
Available online xxxx

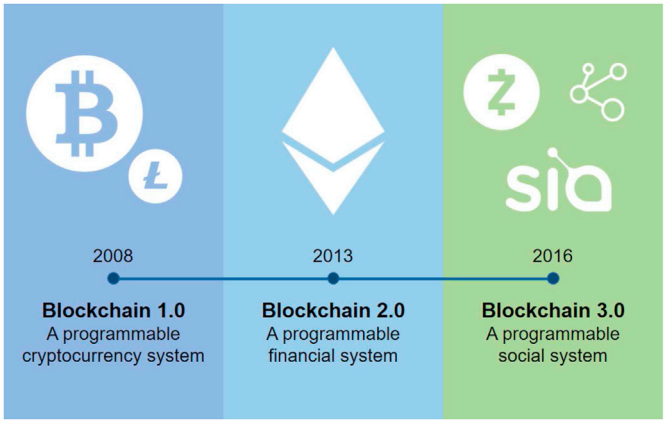

Fig. 1. Evolution of blockchain.

other core technologies independent of any third party that achieves decentralization with security and anonymity. With the development of blockchains, digital cryptocurrency, consensus mechanism, and distributed storage technology, block chains provide effective solutions for the trust in the open networks and the security of data storage in centralized institutions [13–15].

Blockchains usually do not directly save original data or transaction records; instead, they save their hash values by encoding the original data into a string of numbers and letters of a specific length. These encoded strings are then recorded in the blockchain. Hash functions have many excellent characteristics suitable for storing blockchain data. Through such a unidirectional process, the input value can barely be reversed by the hash output. Additionally, the process of converting different length inputs data to hash values takes an equal amount of time, guaranteeing the in-time processing of the input data. Moreover, it produces a fixed output length that facilitates processing later. Notably, even with a one-bit input difference, the hash process produces a significantly different output value and ensures its randomness [16].

2.2. Consensus algorithms

Because no centralized organization managing and controlling blockchain exist, blockchain implementation encounters trust problems. To reach a consensus among users, peers in blockchain networks must abide by the same protocol. This mutual trust mechanism used in the blockchain is constructed based on consensus. Members of the blockchain make codecisions using consensus algorithms [17]. A consensus must satisfy the following necessities.

- **Consistency.** The prefix of the blockchain saved by all honest nodes is the same.
- **Effectiveness.** The information published by an honest node is eventually recorded in its blockchain by all other honest nodes.

Currently, blockchain consensus algorithms satisfying the above necessities can be divided into five categories [18–20].

Proof-of-Work (PoW). PoW is one of the earliest consensus algorithms. Before a group of transactions (i.e., a block) is recorded into the blockchain, nodes perform SHA256 calculations on the block and make the first *target* bit of the block's hash value become zero by modifying the value of the random number *nonce* in the blockhead. Consequently, the node that first discovers the random number obtains the accounting right and receives rewards. However, PoW utilizes considerable computing power when scrambling for the accounting right, and substantial resources and time are wasted before reaching a consensus. Thus, PoW is unsuitable for commercial applications.

Proof-of-Stake (PoS). Instead of having the validators perform some of the computation, PoS uses an election process in which one node is randomly chosen to validate the next block. To become a validator, a node must deposit a certain number of coins into the network as a stake. The size of the stake determines the possibility of a validator being chosen to forge the next block. As a reward, the node receives the fees associated with each transaction.

Delegated Proof-of-Stake (DPoS). DPoS is designed as an implementation scheme for digital democracy. A fixed number of delegates between 21 and 101 are voted by relevant stakeholders. These elected delegates will validate transactions and are rewarded accordingly. Each stakeholder receives several votes proportional to the number of coins owned, or they delegate these stakes to another stakeholder on the network. Therefore, compared with PoW; however, this improved transaction speed weakens the degree of decentralization in DPoS.

Raft. Raft is a typical consensus algorithm used in distributed systems that divide nodes in distributed systems into three roles: Leader, Follower, and Candidate. It transmits heartbeats to other nodes through the Leader node for log synchronization and uses the election mechanism to deal with the downtime of some nodes in the distributed system. However, Raft only tolerates (N - 1)/2 faulty nodes and not malicious nodes. Thus, it is generally used in private chain scenarios [21,22].

Practical Byzantine Fault Tolerance (PBFT). Unlike Raft, PBFT can tolerate (N - 1)/3 malicious nodes. It is commonly used in alliance chains. In PBFT, the client sends a request to the Leader node, and the Leader node responds by sending a *pre-prepare* message to other nodes. After receiving this message, other nodes conduct a consensus check. Every node that accepts the request sends a *prepare* message to other nodes. When the *prepare* messages are received from more than 2f nodes, each 2f node broadcasts the *commit* message to other nodes. For each 2f + 1 *commit* message received, most nodes have reached a consensus, and the nodes execute the request and write data. Additionally, PBFT designs an impeachment mechanism to ensure the safety of the Leader node [23].

For clarity, we summarize the pros and cons of different consensus algorithms in Table 1.

Although these five consensus algorithms have certain advantages over conventional consensus algorithms, they also have disadvantages, such as the inverse proportionality between efficiency and degree of decentralization (i.e., efficiency decreases as the degree of decentralization increases, and vice versa).

2.3. Smart contract

Bitcoin is simply a distributed ledger used to record cryptocurrency transactions without any other functions. Ethereum has applied smart contract technology in its blockchain, making it applicable to several scenarios. A smart contract is a piece of code running on the blockchain that controls digital assets and specifies the rights and obligations agreed upon by the contract participants; a smart contract is automatically executed in the blockchain. No one can intervene in the execution of a smart contract once it goes online and keeps running without any intermediaries [24]. Ethereum develops smart contracts based on solidity (similar in syntax to Javascript).

Table 1
Pros and cons of three commonly utilized consensus algorithms.

Consensus Algorithm	Advantage	Disadvantage
PoW	Full decentralization Antiattack property	Low energy efficiency Inefficient wire transfer
PoS	Efficient wire transfer High energy efficiency	Easy to monopolize Threat to security
DPoS	High-energy efficiency	Vulnerability Less decentralization
Raft	High efficiency	Limited applications Does NOT tolerate malicious nodes
PBFT	High efficiency High safety and activity	High-communication complexity Rely on network quality

Owing to the irrevocable nature of the blockchain, a smart contract submitted to the blockchain cannot be modified; hence, the code is repeatedly debugged for errors before submitting. The Decentralized Autonomous Organization (DAO) is a decentralized autonomous venture fund based on Ethereum. Users on Ethereum can use Ether to participate in investment projects on the DAO and invest in blockchain projects through collective-decision based on the voting mechanism. If some users do not wish to participate in the investment projects approved by most people, they build a child DAO by splitting the existing DAO. This further reflects the democratic system. However, in the past, a tiny process mistake occurred in splitting the DAO code, allowing hackers to steal 50 million Ether [25,26]. This also caused the Ethereum team to hard fork Ethereum to Ethereum Classic (ETC) and Ethereum (ETH).

2.4. Scalability

All transaction records in the bitcoin blockchain are stored in the Merkle tree (a tree structure based on Hash pointers), wherein only full nodes can save transaction information; the root Hash of the Merkle tree is subsequently stored in the blockhead. Therefore, considering the network propagation delay, the bitcoin blockchain was initially designed with a capacity limit of 1 MB per block. Each transaction or smart contract of Ethereum consumes the fee *GasUsed*, which controls the size of the block through the *GasLimit* field of each block, and allows the validator of each block to adjust the *GasLimit* of the last block by adding or subtracting 1/1024. However, with an increasing number of users, the amount of data in each block will reach the upper limit, and the block capacity limit makes it impossible to apply Ethereum to some scenarios involving big data storage [28,29] (c.f. Fig. 2 for more details). Expanding the information capacity under the premise of ensuring the transmission efficiency for applications in big data is an open problem that requires further investigation. Currently, the key technologies for blockchain capacity expansion include two schemes as shown in Fig. 3: layer-1 (on-chain scaling) and layer-2 (off-chain scaling) [30,31].

On-chain scaling proposals recommend directly modifying the block capacity cap to accommodate more transactions. In Bitcoin Improvement Proposal (BIP) 101, the upper limit of block capacity was increased to 8 MB through a hard fork in January 2016 and has since doubled every two years. In BIP102, it is recommended to increase the block capacity from 1 to 2 MB. Although these two proposals expand the block capacity, they are limited by network bandwidth. When the network propagation delay is large, the risk of solitary block increases.

The key to off-chain scaling is to allow transactions to be completed off-chain. This usually requires building a second layer network on the blockchain network, e.g., the lightning network. The lightning network is mainly composed of Revocable Sequence Maturity Contract (RSMC) and Hashed Time Lock Contract (HTLC), in which RSMC allows users to create two-way off-chain micropayment channels and achieve unlimited quick off-chain transfers within the limit. HTLC allows users who do not directly establish channels to transfer through other cooperative users while ensuring that funds are not lost through forwarding errors or malicious behaviors of the cooperative users.

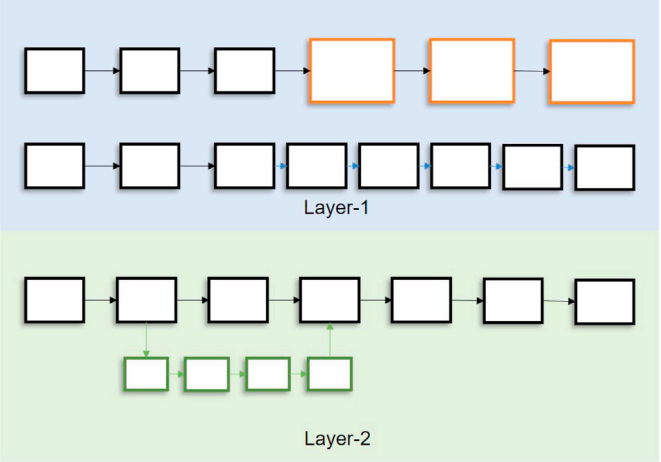

Fig. 3. Key technologies of blockchain capacity expansion.

3. Challenges and opportunities

Although the bitcoin blockchain was proposed in 2008, its audience is still small until 2017. Even with the increased awareness regarding bitcoin blockchain now, many technological improvements are still required. To accelerate technological progress on the blockchain, we discuss the potential opportunities and challenges of blockchain by analyzing the limitations of canonical blockchain technology and the impacts of other technological developments on the blockchain.

3.1. Increasingly centralized blockchain

The PoW consensus algorithm adopted by bitcoin wastes computing power and energy. Each transaction consumes approximately 657.39 kWh, which is equivalent to the average power consumption of

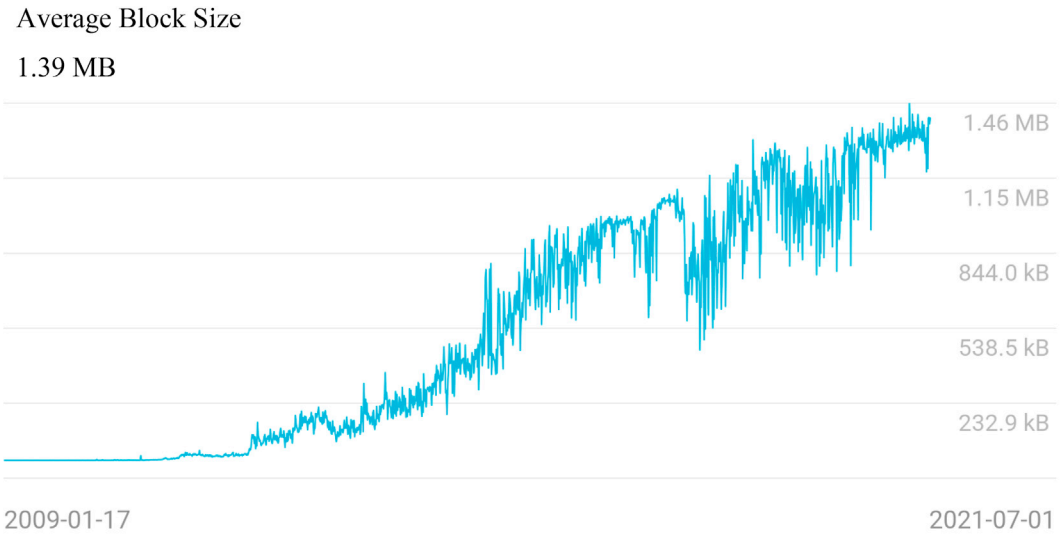

Fig. 2. Average block size of bitcoin over the last 12 years [27].

59 days per household in the United Kingdom. Bitcoin mining generates 10.71 kilotons of e-waste every year, which is equivalent to the amount of waste generated by the country of Luxembourg in a year [32,33]. Moreover, the scrambling for accounting rights is entirely dependent on computing power. Therefore, computing nodes use Application Specific Integrated Circuit (ASIC) chips, which can only be used for mining, to build mining pools. These nodes use a majority of the computing power in the blockchain network. In 2014, GHash.IO large mining utilized more than half of the available computing power to launch 51 % attacks [34–37]. As shown in Fig. 4, the current distribution of computing power in major mining pools is spread out across numerous categories.

However, several large mining pools account for a considerable proportion of the computing power, and thus face the risk of united attacks [38]. Consequently, ordinary users find it difficult to obtain accounting rights, and hence, users are divided as consumers and recorders. This contradicts the principle of decentralization and deviates from the main purpose of blockchain design; this does not support the development of blockchain. Although Ethereum adopts different consensus mechanisms, it also relies on memory, and the shared authorization-certification mechanism does not eliminate its dependence on tokens. Thus, a new consensus mechanism that is independent of hardware and money needs to be developed urgently [39,40].

3.2. Zero fault tolerance

Owing to the irreversibility of blockchain, users are required to be highly cautious in every step of operation; nevertheless, users inevitably face some of the following issues.

- Loss of the private key, which cannot be recovered. Consequently, the money in the blockchain account is permanently frozen.
- Misoperations, such as mistransfer, cannot be reversed.
- It is difficult to dispose of increasing bad debts in Unspent Transaction Outputs (UTXO).

Similarly, once the smart contract in Ethereum is written into the blockchain, it cannot be modified. A loophole in the smart contract can cause irreparable loss [41,42]. Therefore, the code review of the smart contract must be strengthened. Moreover, easier software tests for smart contracts were different. Currently, we need to build a local test blockchain network that simulates user behavior.

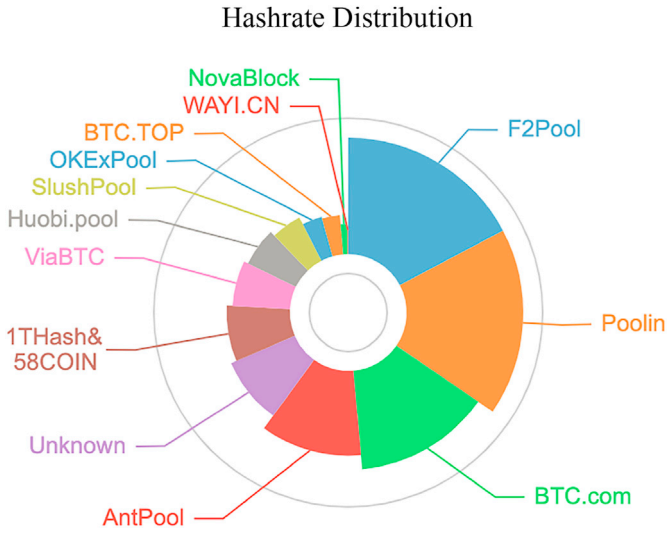

Fig. 4. Current distribution of computing power in major mining pools [27].

3.3. Parameters of bitcoin

When bitcoin design began in July 2010, Nakamoto set an adjustment cycle for mining difficulty spanning 2016 blocks, with each block size being limited to 1 MB. Consequently, the block time can be configured to about 10 min [43]. These parameters were set to prevent the whole node from being limited by the physical conditions of both the network and hardware. These physical limitations result in delayed verification and an unsynchronized ledger in the time domain. Additionally, the set-up by Nakamoto following the network conditions at that time, without rigorous mathematical derivation and reasoning. With the development of 5G/6G mobile communication technology, the block time can be reduced, and the parameters can be optimized using various mathematical methods.

3.4. High threshold

Unlike traditional centralized architectures, most blockchain applications do not have clients, and when they do have clients, it is more difficult to start the execution of the blockchain. For example, Ethereum, which currently has the most users and is the most widely used client *geth,* also uses command-line operations. Smart contracts written in programming languages may be unreadable for ordinary users, let alone participate in and publish smart contracts. Therefore, ordinary users typically find it difficult to participate in the blockchain. Currently, most users manage blockchain accounts through wallet software, which is also centralized, thereby risking the user's account security. Thus, the blockchain audience is limited to computer-related professionals and enthusiasts, and this does not support the universal development of blockchain. To resolve this dilemma, the decentralized client based on peer-to-peer technology was released by the blockchain application development team, allowing users to conduct blockchain transactions using the traditional centralized system interaction habits. This software classifies clients as light nodes, full nodes, and mining clients based on their needs and provides a formally verified smart contract template for users to use. In this manner, the development of blockchain technology is expedited.

3.5. IPv6

An IPv6 address is 128 bits. Theoretically, the IPv6 protocol assigns an IP address to any electronic device. As a direct consequence, all networked devices can obtain a unique public network IP and can bind the IP address to the Mac address as necessary. Combining IPv6 addresses with the public key to the blockchain for identity mapping purposes will help promote the identity of the blockchain and ensure the security and reliability of the Internet. Additionally, network operators can apply the blockchain to manage IP addresses, thereby achieving spontaneous management and organization of network access devices; the blockchain can be used to build a decentralized IPv6 distribution mechanism to break the monopoly of network operators on IP addresses.

3.6. Policy support

As mentioned in the previous article, the development of blockchain technology should follow three stages. Typical applications exist for the first two stages: the programmable currency stage (blockchain 1.0), represented by encrypted electronic currency with payment and circulation currency functions such as Bitcoin and Litecoin, and the programmable financial stage (blockchain 2.0) that supports smart contracts, as represented by Ethereum. In the blockchain 3.0 stage, the application scenarios of blockchain are expected to grow from the financial attributes of payment to the programmable society stage. Currently, our research goal is to realize blockchain 3.0, which is strongly supported by various countries and governments because it will provide great opportunities for the development of blockchain at the application level.

4. Potential applications

Blockchain aims to achieve a decentralized ledger. Because of its decentralization, security, and irrevocable characteristics, blockchain is widely used in cryptocurrencies and other fields such as smart grids, data management, and military [44–47]. The potential applications of blockchain are illustrated in Fig. 5.

4.1. Intellectual property protection

There is no concept of balance in bitcoin. All legitimate bitcoin transactions can be traced to the outputs of previous transactions. All unspent transaction outputs are stored in UTXO. In the case of the loss of private keys and other problems, bitcoin can be permanently stored in UTXO, leading to a continuous expansion of UTXO. Bitcoin users can permanently nullify bitcoin through transparent unsuspended/prunable outputs and fill in the information after executing RETURN to realize digital commitment. Thus, bitcoin will always be locked in the bitcoin blockchain. This feature can be used to put the hash value of intellectual property information after RETURN. When intellectual property disputes arise, they can be proved by publishing the original content to protect the above intellectual property.

4.2. Internet of Things (IoT)

With the help of low-cost computing, cloud computing, big data analysis, and mobile technology, IoT interconnects embedded devices using sensors through private or public networks, reduces human intervention as much as possible, and realizes seamless communications among people, processes, and goods [48–50]. However, most current applications of IoT are related to smart homes and the Internet of vehicles, which contain considerable private information. In addition, IoT devices may be simultaneously managed by multiple managers; thus, the centralized network architecture faces the risk of privacy disclosure [51–54]. Moreover, because of its automaticity, most IoT devices automatically perform information transmission without information screening and cannot determine the reliability of information sources [55]. Blockchain provides a new idea and solution to IoT challenges considering scalability, cooperation ability, trust relationship, security, and privacy protection [56,57]. In particular, the decentralization characteristics of blockchain reduce the load of the centralized architecture and reduce the high operation and maintenance costs [58]. All data transmitted through blockchain are encrypted, and user data and privacy are more secure [59]. Identity rights management and multi-party consensus help to identify illegal nodes and prevent malicious nodes from accessing the system [60]. As long as the data is written into the blockchain, tampering with it is difficult. The chain structure helps build a verifiable and traceable electronic storage [61]. The distributed architecture of blockchain and the characteristics of peer-to-peer transmission help to break the existing multiple information islands of the IoT, establish a mutual trust mechanism at low cost, and promote the horizontal flow of information and inter-network cooperation [62–64].

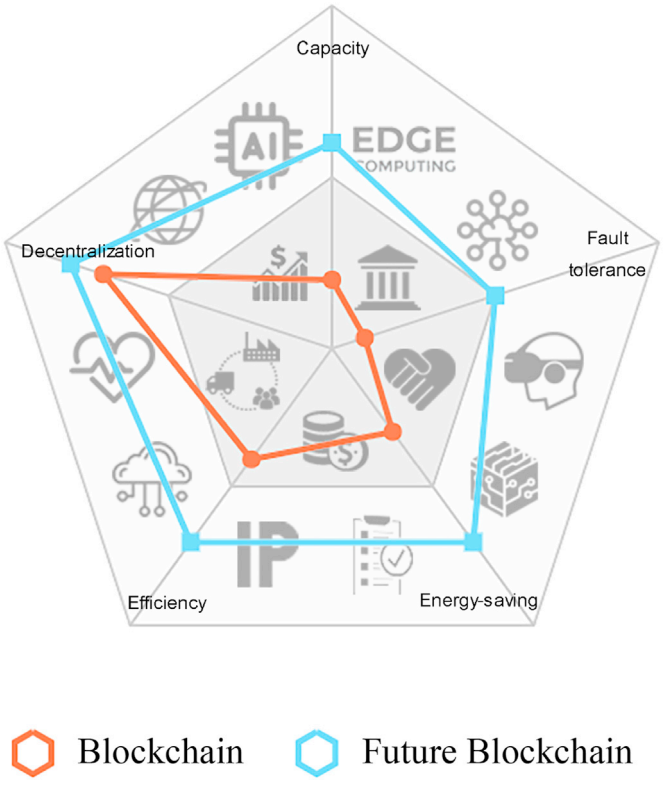

Fig. 5. Potential applications of blockchain and future blockchain.

4.3. Digital twins

Digital Twins describes a physical object and its relationship with each other digitally. It links the digital simulation image with the physical world. The digital world can judge the result in advance using prediction, trial and error, and automatic feedback to the physical world to adapt the production or operation mode [65]. It requires high reliability of data sources as well as high consistency between digital and real data. Blockchain is used to improve system security because of its data transparency, nontemporality, and other characteristics [66,67]. Reliable transmission of the data mapping process using blockchain is conducive to improving the accuracy and reliability of the prediction results [68,69]. It has similar applications in virtual reality scenes. Research on spatial information systems requires spatial data visualization for real data [70]. The process of extracting real-world information and mapping it to the virtual world using geographic blocks is a nontrivial task. In this process, data interpretation errors and data tampering may occur. We believe that blockchain technology can be applied to data organization to achieve safe and reliable data mapping, but when organizing spatial data, we generally use Hash Geo Code to perform two-dimensional table-like indexing [71] and traditional blockchains are unsuitable for storing tabular geographic information data. Therefore, the blockchain propagation method can change from a one-way Hash linked list to a central point radiation propagation to represent two-dimensional data with location information. It provides a multidimensional, reliable experimental environment that fits the real layer for theoretical research using the virtual layer.

4.4. Standardization

With the development of the economy and technology, to achieve the best production and operation orders together with economic benefits, most industries should formulate, issue, and implement unified standards to break trade barriers and promote technological cooperation. However, the formulation of these standards is often monopolized by leading enterprises or vested interest groups in the industry. To maximize their interests, the standards are designed to conform to their production conditions, unfavorable to the development of small- and medium-sized enterprises in the same industry. Considering this, blockchain technology can help maintain fairness for a standardization process [72].

4.5. Blockchain provides a reliable data source for Artificial Intelligence (AI)

Artificial Intelligence (AI) technology has become one of the most popular technologies recently. This technology performs data statistics on numerous training sets and extracts models from data for predictions [73]. The prediction quality depends on the quality of the training sets.

For practical applications of AI, the most difficult part is not model building, but feature engineering, including cleaning abnormal data. The data on the blockchain is open and transparent and thus cannot be tampered with. Hence, these data show high reliability. A high-quality training set can break the "data island," promote data flow for sharing, and form a free and open data market. In turn, AI can empower the blockchain. In particular, AI can enhance the consensus algorithm using optimized neural networks, improve the efficiency and scalability of the transfer process and smart contracts, and achieve the self-regulation of the public chain.

4.6. Federated learning

With the continuous development of AI, many scenarios applying AI technology will improve the user experience or production efficiency [74]. However, most AI computing tasks are currently concentrated on the central server of the enterprise. AI applications collect user data and upload it to the central server for training, causing the risk of privacy leakage. Federated Learning is committed to solving such problems [75] by delegating AI training tasks to the terminal for execution. Each terminal should only train on its local data, and then upload the trained gradient to the server, which uses the Federated Averaging algorithm to integrate these gradients and then publishes them to each node. Two issues must be considered in this process. One issue is the influence of network propagation delay on training speed. However, with research on 6G mobile communication technology, the characteristics of high reliability and low delay have brought new development opportunities to federated learning [76,77]. The second problem is that the server deduces the characteristics of the user's data through the gradient, and the user's data face the risk of leakage. In response to this problem, blockchain technology can be used to link each terminal node in federated learning to achieve a decentralized federated learning system that ensures data consistency while protecting user data privacy [78].

4.7. Epidemic prevention and control

The COVID-19 outbreak occurred worldwide in 2019, killing hundreds of thousands of people. Not only has human life been drastically affected, but the global economy has also been severely damaged, particularly the import and export trade [79]. The traditional supply-chain management system relies on centralized records, making it difficult to trace the origin of goods, and the suppliers cannot prove their innocence. Because of a chain structure, blockchain is suitable for supply chain tracking. First, its multiparty common maintenance features build a trust mechanism among users. Second, operators at all levels must record their electronic signatures on the blockchain, which supports epidemic identification and tracking. While realizing the prevention and control of epidemic situations, it also guarantees the normal progress of international trade.

In addition to supply chain tracking, numerous material donations were made during the outbreak of the epidemic. Owing to the relevant funds or regulatory authorities, problems such as inefficient material distribution and opaque information appeared. Blockchain technology can be used to build an epidemic public welfare information transfer and publicity platform to improve efficiency while enhancing information transparency. Additionally, during the epidemic, various rumors spread on the Internet, causing serious social panic. Current information on the Internet lacks credibility, making it difficult for citizens to identify relevant and real information. Blockchain technology can be used to build online public opinion releases. Such a platform can accurately track the spreaders of rumors while reducing supervision costs.

5. Beyond the technologies

Since the rise of bitcoin in 2017 and 2019, people are more and more concerned about blockchain because of the impact of its decentralized structure on human society. In this section, we discuss the problems brought by blockchains and their solutions from the two directions of standards and supervision.

5.1. Blockchain standard

Owing to the rapid development of bitcoin, many people regard blockchains as a financial tool but do not understand the blockchain technology itself. Some companies obtain investment through the speculation of blockchain, and even some Multi-Level Marketing (MLM) institutions disguise virtual currency as blockchain electronic currency for sale. Many applications claim to be based on blockchain technology, but it is difficult for nonprofessional users to judge their underlying technology; hence, third-party certification bodies must develop standards and specifications to evaluate and authenticate the blockchain system, which supports the wide application of blockchain.

5.2. Blockchain supervision

Blockchain can be used for illegal transactions because of its anonymity, as it makes tracking the identity of criminals more difficult. However, the transaction data stored on the block, including the public keys of both sides of the transaction, are transparent and open. Therefore, as long as the trader participates in offline transactions, its anonymity can be easily destroyed. The centralized database maintained by the regulatory department can be used to map accounts on the blockchain through tracking transactions and via other supervise the blockchain.

6. Conclusions

In this perspective, we introduced key technologies of blockchain, discussed the current problems and opportunities of blockchain in combination with the development of other technologies. We also studied the combination of blockchain and other academic fields and proposed several potential application scenarios. Finally, we discussed the impact of blockchain on human social life and future development directions.

We propose that future blockchain technology should be scalable, and efficient consensus mechanisms that do not rely on computing power should be the main research direction. Editable blockchain technology broadens its application scenarios and effectively integrates blockchain with AI, IoT, and other fields. The effective combination of other fields has realized the transformation of most traditional centralized applications to becoming decentralized, and now, blockchain can "link" the future.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

This work was supported in part by the National Natural Science Foundation of China (NSFC) under Grant No. 61902203, Key Research and Development Plan - Major Scientific and Technological Innovation Projects of ShanDong Province (2019JZZY020101).

References

[1] S. Nakamoto, Bitcoin: a peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf, 2008.

[2] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, F.-Y. Wang, Blockchain-enabled smart contracts: architecture, applications, and future trends, IEEE Trans. Syst. Man Cybern. Cybern.: Systems 49 (11) (2019) 2266–2277.

[3] A.S. Musleh, G. Yao, S. Muyeen, Blockchain applications in smart grid–review and frameworks, IEEE Access 7 (2019) 86746–86757.
[4] S. Jangirala, A. K. Das, A. V. Vasilakos, Designing secure lightweight blockchain-enabled rfid-based authentication protocol for supply chains in 5g mobile edge computing environment, IEEE Transactions on Industrial Informatics.
[5] W. Viriyasitavat, L. Da Xu, Z. Bi, V. Pungpapong, Blockchain and internet of things for modern business process in digital economy—the state of the art, IEEE.Trans.Comput.Soc.Syst. 6 (6) (2019) 1420–1432.
[6] J. Xie, H. Tang, T. Huang, F.R. Yu, R. Xie, J. Liu, Y. Liu, A survey of blockchain technology applied to smart cities: research issues and challenges, IEEE.Commun. Surv. Tutorials. 21 (3) (2019) 2794–2830.
[7] Z. Guan, G. Si, X. Zhang, L. Wu, N. Guizani, X. Du, Y. Ma, Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities, IEEE Commun. Mag. 56 (7) (2018) 82–88.
[8] Y. Yuan, F.-Y. Wang, Blockchain and cryptocurrencies: model, techniques, and applications, IEEE Trans. Syst. Man Cybern. Cybern.: Systems 48 (9) (2018) 1421–1428.
[9] Y. Dai, D. Xu, S. Maharjan, Z. Chen, Q. He, Y. Zhang, Blockchain and deep reinforcement learning empowered intelligent 5g beyond, IEEE Network 33 (3) (2019) 10–17.
[10] J. Xu, S. Wang, B.K. Bhargava, F. Yang, A blockchain-enabled trustless crowd-intelligence ecosystem on mobile edge computing, IEEE Transactions on Industrial Informatics 15 (6) (2019) 3538–3547.
[11] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, Z. Han, When mobile blockchain meets edge computing, IEEE Commun. Mag. 56 (8) (2018) 33–39.
[12] G. Singh, A. Singh, M. Singh, S. Sharma, N. Kumar, K.-K. R. Choo, Blocked: blockchain-based secure data processing framework in edge envisioned v2x environment, IEEE Trans. Veh. Technol..
[13] M.C.K. Khalilov, A. Levi, A survey on anonymity and privacy in bitcoin-like digital cash systems, IEEE.Commun. Surv. Tutorials. 20 (3) (2018) 2543–2585.
[14] A. Dorri, M. Steger, S.S. Kanhere, R. Jurdak, Blockchain: a distributed solution to automotive security and privacy, IEEE Commun. Mag. 55 (12) (2017) 119–125.
[15] W. Yang, E. Aghasian, S. Garg, D. Herbert, L. Disiuta, B. Kang, A survey on blockchain-based internet service architecture: requirements, challenges, trends, and future, IEEE Access 7 (2019) 75845–75872.
[16] M. Wang, M. Duan, J. Zhu, Research on the security criteria of hash functions in the blockchain. Proceedings of the 2nd ACM Workshop on Blockchains, Cryptocurrencies, and Contracts, 2018, pp. 47–55.
[17] Y. Xiao, N. Zhang, W. Lou, Y.T. Hou, A survey of distributed consensus protocols for blockchain networks, IEEE.Commun. Surv. Tutorials. 22 (2) (2020) 1432–1465.
[18] D. Huang, X. Ma, S. Zhang, Performance analysis of the raft consensus algorithm for private blockchains, IEEE Trans. Syst. Man Cybern. Cybern.: Systems 50 (1) (2019) 172–181.
[19] V. Gramoli, From blockchain consensus back to byzantine consensus, Future Generat. Comput. Syst. 107 (2020) 760–769.
[20] W. Wang, D.T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, D.I. Kim, A survey on consensus mechanisms and mining strategy management in blockchain networks, IEEE Access 7 (2019) 22328–22370.
[21] D. Ongaro, J. Ousterhout, In Search of an Understandable Consensus Algorithm (Extended Version), 2018. Retrieved July 20 (2016).
[22] R. Shi, Y. Wang, Cheap and available state machine replication, in: 2016 USENIX Annual Technical Conference (USENIX ATC 16), USENIX Association, Denver, CO, 2016, pp. 265–279.
[23] M. Castro, B. Liskov, Practical byzantine fault tolerance and proactive recovery, ACM Trans. Comput. Syst. 20 (4) (2002) 398–461.
[24] L. Thomas, Y. Zhou, C. Long, J. Wu, N. Jenkins, A general form of smart contract for decentralized energy systems management, Nat. Energy. 4 (2) (2019) 140–149.
[25] A. Mavridou, A. Laszka, Designing secure ethereum smart contracts: a finite state machine based approach, in: International Conference on Financial Cryptography and Data Security, Springer, 2018, pp. 523–540.
[26] M.I. Mehar, C.L. Shier, A. Giambattista, E. Gong, G. Fletcher, R. Sanayhie, H.M. Kim, M. Laskowski, Understanding a revolutionary and flawed grand experiment in blockchain: the dao attack, J. Cases Inf. Technol. 21 (1) (2019) 19–32.
[27] BlockchainInfo, Blockchain charts. https://www.blockchain.com/charts, 2020.
[28] Q. Zhou, H. Huang, Z. Zheng, J. Bian, Solutions to scalability of blockchain: a survey, IEEE Access 8 (2020) 16440–16455.
[29] J. Xie, F.R. Yu, T. Huang, R. Xie, J. Liu, Y. Liu, A survey on the scalability of blockchain systems, IEEE Network 33 (5) (2019) 166–173.
[30] S. Kim, Y. Kwon, S. Cho, A survey of scalability solutions on blockchain, in: 2018 International Conference on Information and Communication Technology Convergence (ICTC), IEEE, 2018, pp. 1204–1207.
[31] J. Poon, T. Dryja, The bitcoin lightning network: scalable off-chain instant payments. https://lightning.network/lightning-network-paper.pdf, 2016.
[32] Telegraph, Bitcoin using more electricity per transaction than a british household in two months. https://www.telegraph.co.uk/science/2020/03/01/bitcoin-using-electricity-per-transaction-british-household/, 2020.
[33] V. Sharma, I. You, F. Palmieri, D.N.K. Jayakody, J. Li, Secure and energy-efficient handover in fog networks using blockchain-based dmm, IEEE Commun. Mag. 56 (5) (2018) 22–31.
[34] M. Conti, E.S. Kumar, C. Lal, S. Ruj, A survey on security and privacy issues of bitcoin, IEEE.Commun. Surv. Tutorials. 20 (4) (2018) 3416–3452.
[35] T. Neudecker, H. Hartenstein, Network layer aspects of permissionless blockchains, IEEE.Commun. Surv. Tutorials. 21 (1) (2018) 838–857.
[36] M. Saad, J. Spaulding, L. Njilla, C. Kamhoua, S. Shetty, D.H. Nyang, D. Mohaisen, Exploring the attack surface of blockchain: a comprehensive survey, IEEE Communications Surveys & Tutorialsdoi (2020), https://doi.org/10.1109/COMST.2020.2975999.
[37] A.K. Fedorov, E.O. Kiktenko, A.I. Lvovsky, Quantum computers put blockchain security at risk, Nat. Energy. 563 (2018) 465–467.
[38] B. Moustapha, The effect of propagation delay on the dynamic evolution of the bitcoin blockchain, Digit.Commun.Network. 6 (2) (2020) 157–166.
[39] X. Li, P. Jiang, T. Chen, X. Luo, Q. Wen, A survey on the security of blockchain systems, Future Generat. Comput. Syst. 107 (2020) 841–853.
[40] Z. Liu, N.C. Luong, W. Wang, D. Niyato, P. Wang, Y.-C. Liang, D.I. Kim, A survey on blockchain: a game theoretical perspective, IEEE Access 7 (2019) 47615–47643.
[41] J. Liu, Z. Liu, A survey on security verification of blockchain smart contracts, IEEE Access 7 (2019) 77894–77904.
[42] S. Rouhani, R. Deters, Security, performance, and applications of smart contracts: a systematic survey, IEEE Access 7 (2019) 50759–50779.
[43] M. Belotti, N. Božić, G. Pujolle, S. Secci, A vademecum on blockchain technologies: when, which, and how, IEEE.Commun. Surv. Tutorials. 21 (4) (2019) 3796–3838.
[44] F. Tschorsch, B. Scheuermann, Bitcoin and beyond: a technical survey on decentralized digital currencies, IEEE.Commun. Surv. Tutorials. 18 (3) (2016) 2084–2123.
[45] M. B. Mollah, J. Zhao, D. Niyato, K.-Y. Lam, X. Zhang, A. M. Ghias, L. H. Koh, L. Yang, Blockchain for future smart grid: a comprehensive survey, IEEE Internet.Things.J..
[46] J. Chen, Z. Lv, H. Song, Design of personnel big data management system based on blockchain, Future Generat. Comput. Syst. 101 (2019) 1122–1129.
[47] W. Feng, Y. Li, X. Yang, Z. Yan, L. Chen, Blockchain-based Data Transmission Control for Tactical Data Link, Digital Communications and Networks.
[48] H.-N. Dai, Z. Zheng, Y. Zhang, Blockchain for internet of things: a survey, IEEE Internet.Things.J. 6 (5) (2019) 8076–8094.
[49] S. Yang, J. Wang, S. Li, B. Deng, X. Wei, H. Yu, H. Li, Cost-efficient fpga implementation of basal ganglia and their parkinsonian analysis, Neural Network. 71 (2015) 62–75.
[50] S. Yang, J. Wang, Q. Lin, B. Deng, X. Wei, C. Liu, H. Li, Cost-efficient fpga implementation of a biologically plausible dopamine neural network and its application, Neurocomputing 314 (2018) 394–408.
[51] M. Wazid, A.K. Das, S. Shetty, M. Jo, A tutorial and future research for building a blockchain-based secure communication scheme for internet of intelligent things, IEEE Access 8 (2020) 88700–88716.
[52] X. Wang, X. Zha, W. Ni, R.P. Liu, Y.J. Guo, X. Niu, K. Zheng, Survey on blockchain for internet of things, Comput. Commun. 136 (2019) 10–29.
[53] J. Sengupta, S. Ruj, S.D. Bit, A comprehensive survey on attacks, security issues and blockchain solutions for iot and iiot, J. Netw. Comput. Appl. 149 (2020) 102481.
[54] L. Peng, W. Feng, Z. Yan, Y. Li, X. Zhou, S. Shimizu, Privacy Preservation in Permissionless Blockchain: A Survey, Digital Communications and Networks.
[55] M.A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, H. Janicke, Blockchain technologies for the internet of things: research issues and challenges, IEEE Internet.Things.J. 6 (2) (2018) 2188–2204.
[56] M.S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, M.H. Rehmani, Applications of blockchains in the internet of things: a comprehensive survey, IEEE.Commun. Surv. Tutorials. 21 (2) (2018) 1676–1717.
[57] R. Yang, F.R. Yu, P. Si, Z. Yang, Y. Zhang, Integrated blockchain and edge computing systems: a survey, some research issues and challenges, IEEE.Commun. Surv. Tutorials. 21 (2) (2019) 1508–1532.
[58] I. Makhdoom, M. Abolhasan, H. Abbas, W. Ni, Blockchain's adoption in iot: the challenges, and a way forward, J. Netw. Comput. Appl. 125 (2019) 251–279.
[59] M.U. Hassan, M.H. Rehmani, J. Chen, Privacy preservation in blockchain based iot systems: integration issues, prospects, challenges, and future research directions, Future Generat. Comput. Syst. 97 (2019) 512–529.
[60] Y. Xu, J. Ren, G. Wang, C. Zhang, J. Yang, Y. Zhang, A blockchain-based nonrepudiation network computing service scheme for industrial iot, IEEE Transactions on Industrial Informatics 15 (6) (2019) 3632–3641.
[61] P.K. Sharma, S. Singh, Y.-S. Jeong, J.H. Park, Distblocknet, A distributed blockchains-based secure sdn architecture for iot networks, IEEE Commun. Mag. 55 (9) (2017) 78–85.
[62] K. Gai, J. Guo, L. Zhu, S. Yu, Blockchain meets cloud computing: a survey, IEEE.Commun. Surv. Tutorials..
[63] R.B. Uriarte, R. De Nicola, Blockchain-based decentralized cloud/fog solutions: challenges, opportunities, and standards, IEEE.Commun.Stand.Mag. 2 (3) (2018) 22–28.
[64] M. Wu, K. Wang, X. Cai, S. Guo, M. Guo, C. Rong, A comprehensive survey of blockchain: from theory to iot applications and beyond, IEEE Internet.Things.J. 6 (5) (2019) 8114–8154.
[65] F. Tao, Q. Qi, Make more digital twins, Nature 573 (7775) (2019) 490–491.
[66] D.R. Wong, S. Bhattacharya, A.J. Butte, Prototype of running clinical trials in an untrustworthy environment using blockchain, Nat. Commun. 10 (1) (2019) 1–8.
[67] J. Al-Jaroodi, N. Mohamed, Blockchain in industries: a survey, IEEE Access 7 (2019) 36500–36515.
[68] C. Krittanawong, A.J. Rogers, M. Aydar, E. Choi, K.W. Johnson, Z. Wang, S.M. Narayan, Integrating blockchain technology with artificial intelligence for cardiovascular medicine, Nat. Rev. Cardiol. 17 (1) (2020) 1–3.
[69] Y. Liu, F.R. Yu, X. Li, H. Ji, V.C. Leung, Blockchain and machine learning for communications and networking systems, IEEE.Commun. Surv. Tutorials. 22 (2) (2020) 1392–1431.
[70] A. Bock, E. Axelsson, J. Costa, G. Payne, M. Acinapura, V. Trakinski, C. Emmart, C. Silva, C. Hansen, A. Ynnerman, Openspace: a system for astrographics, IEEE Trans. Visual. Comput. Graph. 26 (1) (2019) 633–642.

[71] Z. Lv, T. Yin, Y. Han, Y. Chen, G. Chen, Webvr-web virtual reality engine based on p2p network, J. Network. 6 (7) (2011) 990.
[72] E. Bellini, Y. Iraqi, E. Damiani, Blockchain-based distributed trust and reputation management systems: a survey, IEEE Access 8 (2020) 21127–21151.
[73] S. Yang, J. Wang, B. Deng, C. Liu, H. Li, C. Fietkiewicz, K.A. Loparo, Real-time neuromorphic system for large-scale conductance-based spiking neural networks, IEEE Trans.Cybern. 49 (7) (2018) 2490–2503.
[74] S. Yang, B. Deng, J. Wang, H. Li, M. Lu, Y. Che, X. Wei, K.A. Loparo, Scalable digital neuromorphic architecture for large-scale biophysically meaningful neural network with multi-compartment neurons, IEEE Trans. Neural Network.Learn Syst. 31 (1) (2019) 148–162.
[75] B. McMahan, E. Moore, D. Ramage, S. Hampson, B.A. y Arcas, Communication-efficient learning of deep networks from decentralized data, in: Artificial Intelligence and Statistics, PMLR, 2017, pp. 1273–1282.
[76] Y. Chen, W. Liu, Z. Niu, Z. Feng, Q. Hu, T. Jiang, Pervasive intelligent endogenous 6g wireless systems: prospects, theories and key technologies, Digit.Commun.Network. 6 (3) (2020) 312–320.
[77] M. Wang, T. Zhu, T. Zhang, J. Zhang, S. Yu, W. Zhou, Security and privacy in 6g networks: new areas and new challenges, Digit.Commun.Network. 6 (3) (2020) 281–291.
[78] M. Banerjee, J. Lee, K.-K.R. Choo, A blockchain future for internet of things security: a position paper, Digit.Commun.Network. 4 (3) (2018) 149–160.
[79] V. Chamola, V. Hassija, V. Gupta, M. Guizani, A comprehensive review of the covid-19 pandemic and the role of iot, drones, ai, blockchain, and 5g in managing its impact, IEEE Access 8 (2020) 90225–90265.