International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 03 | March - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

Cyber Communication by Using Block Chain Technology Systems

Ch. Kodanda Ramu[1], Velamala Roja[2], Vedulla Raju[3], Rompilli Ganesh[4], N Appalnaidu[5]

[1]Associate Professor, Department of Computer Science & Engineering, Miracle Educational Society Group of Institutions, Bhogapuram, Vizianagaram, Andhra Pradesh, India - 535216

[2,3,4,5]B.Tech Student , Department of Computer Science & Engineering, Miracle Educational Society Group of Institutions, Bhogapuram, Vizianagaram, Andhra Pradesh, India - 535216

Email: kvr.chintu1978@gmail.com

Abstract - In the fast-growing digital age, systems for communicating through cyber means allow people, organisations and governments to share information in real-time. Unfortunately, the majority of the current communications networks use a centralised architecture, which are susceptible to cyber threats like data breaches, identity theft, man in the middle attack, and distributed denial of service attacks. These vulnerabilities degrade the confidentiality, integrity, availability and trust in the digital communication systems. This research proposes a secure cyber communication framework using blockchain technology to bypass the limitations of the current systems. The framework uses decentralised distributed ledger technology, public/private key cryptography, digital signatures, cryptographic hash functions and smart contracts to facilitate the secure transmission of messages, authenticate user identity and maintain a tamper-proof record of messages. All messages will be encrypted, digitally signed for authenticity and validated using consensus before being permanently recorded onto the blockchain. This architecture will reduce reliance on third-party intermediaries while providing greater resilience and transparency against cyber-attacks, as well as eliminating single points of failure. Performance, scalability and energy consumption will also be discussed in this study. According to the results, use of blockchain for cyber-communication is associated with high levels of security; therefore, the use of blockchain in future decentralised communication networks should result in more secure, trustworthy, and reliable systems within all key industries.

Key Words: Blockchain Technology, Cyber Communication, Secure Messaging, Distributed Ledger, Cryptography, Digital Signatures, Smart Contracts, Decentralization, Data Integrity, Network Security

1.INTRODUCTION

Cyber Communication Forms a Critical Element of Today's Global Connectedness, with Fast Sharing of Information Globally Between Individuals, Businesses, and Governments. Existing Methods of Communicating Based on Technologies Such as, Email, Chat, Social Networking, Cloud Computing, and IOT Are Fundamental to Many of Society's, Business' and Government's Most Essential Social, Economic and Administrative Activities Today. Presently, Most Forms of Technology Related Communication Are Based on Centralized Models of Electronic Communication that Provide Central Data Storage and are Managed Ability to Provide Central Control of Data only by a Central Existing Authority and/or Service Providers Which creates multiple security vulnerabilities: Data Breach, Identity Theft, Unauthorized Access, and Large-Scale Attacks. Blockchain technology is a Alternative Model that Eliminates Centralized Oversight of Communication & Allows Individuals to Rely on Each Other as Their Main Source of Trust Through a Decentralized Distributed Ledger System with Cryptographically Secure Features. By Incorporating Various Cryptographic Mechanisms Including, Public/Private Key Cryptography, Digital Signatures, Consensus Protocols, and Immutable Data Storage, cybersecurity in the form of Blockchain-Based Communication Systems Would Offer the Opportunity to Increase Confidentiality, Integrity, And Availability of Cybersecurity in Our Digital World. The Usage of Blockchain Based Technologies in Communications Will Potentially Change the Way We Communicate by Allowing for More Secure, Auditable, and Tamper-Proof Communications Using Traditional Communication Models.

Figure. 1 Secure cyber communication with blockchain

1.1 Background

The evolution of cyber communications over the years has changed significantly through the advances from early, analog forms of communication like telegraphs and telephony to the newest, advanced internet-based systems offering real-time transmitting of digital multimedia communications between individuals or organizations. With the emergence of computing, the internet, and social media-type technologies, cloud computing and mobile devices, have dramatically increased the speed of this transition and made digital forms of communications necessary for the business sector to function in a world built on digital systems. Digital communications systems based on traditional technologies are usually founded on the concept of a client-server interaction in which a central server controls the authentication of users, stores data, and routes messages. Although these systems facilitate scalability and have advantages from a management perspective, they are susceptible to single points of failure and require end-users to depend on third-party providers to handle their sensitive data and private information. As a result of increased threats to cybersecurity, researchers have worked on identifying alternative forms of communication systems that do not require a centralized authentication system, and have focused on the exploration of the use of decentralized technologies; specifically blue-chip technologies (blockchain). By providing data distributed over the entire network, but digitally stored as well as easily verifiable, and being able to maintain records of transactions without the necessity of a central authority, blockchain provides various opportunities for the implementation of secure identity management, encrypted data transfer, and unalterable audit-trails for individuals through the implementation of new and improved systems of digital communications that will address many of the concerns raised by traditional systems of communications.

1.2 Problem Statement

While advances have been achieved in both encryption and network security, centralized cyber communication systems remain susceptible to numerous complex cyber attacks. Attackers are most likely to attack centralized servers that store user credentials, communication logs, or any other sensitive information, hence, being prime targets for mass data breaches, unavailability for users, and privacy loss. Furthermore, centralizing control over the information stored on these servers creates a lack of transparency and autonomy for users, as well as a lack of verification for the integrity of the information stored on these servers or for detecting unauthorized changes to it. Trust in digital communication platforms is eroded by man-in-the-middle attacks, identity theft, data manipulation, and distributed denial of service attacks. There are also increased operational risks to users due to reliance on intermediaries (e.g., Internet service providers) to deliver services to users which reduces the system's resilience. As a result, there is an increased need for secure and decentralized methods of communication that will eliminate single points of failure, provide complete end-to-end data protection, and provide verifiable trust without relying on any centralized authority to do so. Electronic communication systems using blockchain technology will try to provide a solution to this problem through immutable records of transactions; by distributing the validation process among multiple entities and by providing cryptographic means for authenticating users, thereby yielding secure and trustworthy ways of transmitting information.

2. LITERATURE REVIEW

Blockchain is a new type of technology that allows for increased security, transparency, and trust. Initially described by Nakamoto as a decentralized, peer-to-peer network to conduct safe transactions without intermediaries, he paved the way for distributed trust as a real possibility. Following Nakamoto's work, other studies showed that blockchain wasn't just a cryptocurrency-based technology but could also be used for various things such as businesses, governance, and means of communication. Researchers have concluded that due to the decentralized nature, immutability, and consensus mechanisms of blockchain, it is a viable option for applications that rely on tamper-resistant data access and require high levels of reliability. Many of the articles reviewed discuss the technical building blocks of blockchain, such as cryptographic security and networking protocols. Stallings provided a description of the various core principles used in cryptography such as encryption, hashing, and digital signatures which are all the foundation of secure communication systems. Narayanan and colleagues provided a detailed overview of bitcoin and cryptocurrency technologies and described how blockchain achieves integrity and authentication through the use of public key cryptography and distributed validation. Drescher offered a basic description of the key aspects of blockchain, outlining its multi-layered architecture and operational functioning. There has been research available regarding blockchain technology being utilized within the communication networks and new forms of technology. Christidis and Devetsikiotis demonstrated how blockchain technology along with smart contracts can secure IoT communication through the use of decentralized authentication of devices and verification of the integrity of data sent or received [15].

Pilkington and Swan explained the potential of blockchain technology to create an environment where decentralized (or trustless) digital ecosystems exist, thus, removing the need for centralized authorities [2], [8]. Yli-Huumo et al., through a systematic review identified three primary challenges to implementing blockchain technology: scalability; privacy; and energy consumption [9]. A significant amount of attention has been given to researching the security concerns of blockchain systems. Li et al. performed a survey examining the vulnerabilities and security measures taken to

protect against unauthorized access and tampering with data [12]. Atzei et al. studied the vulnerabilities of Ethereum smart-contracts by analyzing attacks resulting from both programming errors as well as design flaws [20]. Wang et al. examined the use of smart contracts to enforce security policies and to control access in dispersed environments through blockchain technology [18]. Extensive studies have explored both performance and architecture. A taxonomy for designing blockchain-based systems was created to help facilitate the building of scalable systems and provide insights into how blockchain technology works, with lots of emphasis on improving performance (Xu et al). Dinh et al examined how blockchains can process data effectively, and they found limitations related to throughput and latency (Dinh et al). The comparative studies of different blockchain platforms (Ethereum vs. Hyperledger Fabric) highlighted the trade-offs associated with public vs. permissioned blockchains from a performance and scalability perspective.
In conclusion, based on the literature, blockchain technology has many advantages as a means of secure and private cyber communication due to decentralization, enhanced authentication and loyalty schemes, and the ability to provide an immutable record. There are currently challenges such as scalability, energy consumption (e.g. proof of work), vulnerability of smart contracts, and the ultimate complexity of integration and soft architecture. The overall findings suggest that there is still much research to be done to develop new and innovative blockchain-based communication frameworks that deliver a high degree of security and efficient performance.

2.1. Research Gaps

- Scalability for Real-Time Communication.
- Efficient Integration with Existing Infrastructure.
- Lightweight Security Mechanisms for Resource-Constrained Environments.
- Robust Key Management and Usability Challenges.

2.2. Objectives

- To Study Existing Cyber Communication Systems.
- To Understand Blockchain Technology and Its Core Components.
- To Design a Blockchain-Based Cyber Communication Model.
- To Implement Secure Identity Management.
- To Enhance Message Security.

3. METHODOLOGY

This report presents the systematic methodology that has been created to design, develop, and evaluate a secure cyber communication system based on blockchain technology. The methodology combines the use of cryptographic techniques, distributed ledger technology, smart contracts, and decentralised networking to provide confidentiality, integrity, authentication, and non-repudiation for communication data. In addition to providing confidentiality and integrity, the proposed framework uses a peer-to-peer architecture and consensus mechanisms to replace traditional centralised communication systems by validating transactions by consensus and maintaining records of transactions. The methodology has been divided into four phases: (1) design of system architecture; (2) development of a communication workflow; (3) implementation of security measures; and (4) deployment of system in practice.

Figure. 2 Blockchain communication methodology

3.1 System Architecture Design

The proposed system design includes five layers of architecture to provide increased modularity, scalability, and security: (1) user layer; (2) application layer; (3) blockchain network layer; (4) smart contract layer; and (5) storage layer. The user layer will provide a user interface for communicating, as well as to generate keys; the application layer will provide encryption and decryption services, as well as provide transaction processing services; and the blockchain layer will be responsible for validating and maintaining records of communication between users on distributed nodes based on consensus validation methods. Smart contracts facilitate the automation of access control, identification of users, and enforcement of communication rules to prevent unauthenticated users from accessing the

communication system. Large data files will be stored off-chain with the corresponding cryptographic hash of each file maintained on the blockchain to provide integrity and reduce storage costs associated with maintaining large data files.

3.2 User Registration and Key Generation

Each user joining the system undergoes a registration process that generates a unique public–private key pair. The public key serves as the user's digital identity, while the private key is securely stored on the user's device and used for signing and decrypting messages. This approach eliminates traditional password-based authentication and reduces risks associated with centralized credential storage. Decentralized identity management ensures that users maintain full control over their credentials without relying on third-party authorities.

3.3 Message Encryption and Digital Signature

When a user initiates communication, the message is first converted into plaintext and then encrypted using the receiver's public key to achieve end-to-end confidentiality. After encryption, the sender generates a digital signature using their private key. This signature verifies the sender's authenticity and ensures message integrity during transmission. Any alteration in the message content results in signature mismatch, enabling detection of tampering attempts.

3.4 Transaction Creation/Transmission

A blockchain transaction consists of an encrypted message, a digital signature, the sender's identity, the receiver's identity, and a timestamp. This transaction is sent on a peer-to-peer network to all participating nodes, who will receive it and assess whether or not it is valid. Broadcasting enables the system to be transparent and eliminates the need for centralized routing to send transactions to their intended destinations.

3.5 Consensus Verification/Block Creating

Once verified by consensus mechanisms such as Proof of Work or Proof of Stake, network nodes validate transactions. Only those transactions that are verified are then added to new blocks on the blockchain. A new block contains a digital hash of the previous block, thus creating a secure chain where no transaction within that chain can be changed retroactively. Each time the blockchain is updated, all participating nodes receive a new copy of the updated record of the blockchain to ensure each node has an identical copy of the most recent blockchain, thus ensuring that the system continues to function in a manner that is consistent and is resilient against attack.

3.6 Secure Message Retrieval/Decryption

The intended recipient of an encrypted message retrieves the message from the blockchain network and decrypts it using their private key. If successful, the decrypted message demonstrates that it was meant for them and has not been tampered with. The distributed ledger also serves as a permanent and independent audit trail of communication transactions, which can be verified transparently without revealing the content of the communication.

3.7 Security Mechanisms Implementation

The system integrates several types of security methods, such as public-key cryptography for authentication, a digital signature for non-repudiation (proof of notdoing), the use of cryptographic hash functions to ensure integrity of the data; consensus algorithms are used to validate transactions, and replicating the distributed ledger across all nodes in the system will provide for high availability (fail-safes). In addition, smart contracts are utilized to automatically enforce access control policies and communication rights, resulting in less manual intervention and fewer security risks.

3.8 Implementation and Deployment

The design and construction of the system will consist of developers building both the user-interface and backend-service components but in addition; the selected blockchain platform (e.g., Ethereum or a permissioned framework) will be used to implement and deploy smart contracts to manage the processes associated with identity registration, access control, and transaction validation. As a result, off-chain storage solutions will also be developed for storing large amounts of data; however, the blockchain retention policy of maintaining a verification hash of any data downloaded to off-chain storage will still apply. The developer will establish optimal hardware and software configurations for all nodes in the system to support efficient node performance, synchronize records in both the on-chain and off-chain environment, and provide secure data communications.

3.9 Performance and Evaluation Approach

To evaluate the proposed solution's effectiveness; it will be compared against traditional centralized communication models based on the following criteria: security, reliability, transparency, and resiliency to cyber-attacks. The evaluation will further analyze the methods/technologies used in the proposed solution relative to centralization to measure the following performance metrics: transaction latency; scalability; computational overhead; and storage capacity. Therefore, the evaluation will provide insight into the effectiveness of the proposed blockchain communication solution, particularly insight into the potential for providing better levels of trust and data protection and identifying opportunities for future improvements.

4. RESULTS AND DISCUSSIONS

A system based on artificial intelligence (AI) to identify product defects using images collected from the production line was evaluated for its ability to detect defect presence and location within shampoo products produced under simulated manufacturing environments. The model used Convolutional Neural Network (CNN) techniques to classify and detect defects using a method based on the YOLO architecture. The results obtained show that the automated approach improves accuracy and consistency

significantly compared to manual inspection methods. The ability of the CNN-based model to detect several different defect types (packaging damage, leaking products, improper labels and foreign materials) was effective. Image preprocessing techniques used (e.g., normalization, augmentation, noise reduction) increased the visibility of features used for classification and enhanced the performance of the model.

The proposed system represents a highly reliable and efficient inspection process since it is able to differentiate between defective and non-defective product with a high degree of reliability and very low probability of false inspection outcomes. The proposed AI-based video inspection (CCTV) model provides fast and accurate identification of product defects in shampoo products manufactured at high rates, making it useful for deployment in production lines. The real-time processing capabilities of the proposed system due to the use of YOLO architecture allow for immediate detection of defective products so they can be removed from the production stream, thus minimizing waste and preventing defective products from being sold to end consumers. Automated inspection of postal vehicles will benefit from the elimination of human fatigue and emotion, thus allowing for the application of consistent, predefined quality standards for the inspection process.

The automated system will also visually depict the defective areas on the vehicle using bounding boxes to assist the quality assurance experts in validation of the inspection results provided by the automated inspection process. The proposed automated postal vehicle inspection system will also provide a higher level of transparency and confidence in the use of an automated inspection process. The trained model can also be scaled to inspect other categories of fast-moving consumer goods (FMCG), such as bottles, with very few changes to the system. One limitation of the proposed approach to automated inspection is that the performance of the trained model is dependent on the quality and variety of the training set. If a defect occurs infrequently (rarely occurs in the training set), it may be difficult for the automated system to accurately identify the target defect through bounding boxes. Furthermore, poor lighting or visual obstructions may also affect the performance of the model to correctly identify a defective condition. Future enhancements to the model should include enhancing the training set with a broader range of defect categories, utilizing the latest training set augmentation techniques and adding more sensors as a part of the automated inspection process.

The experiments conducted show that the proposed AI-based system for detecting defects has been proven successful in delivering a dependable and efficient source of automated quality inspections in manufacturing environments; therefore meeting an important goal of the Fourth Industrial Revolution that is related to intelligent manufacturing and production systems having their own smart capabilities.

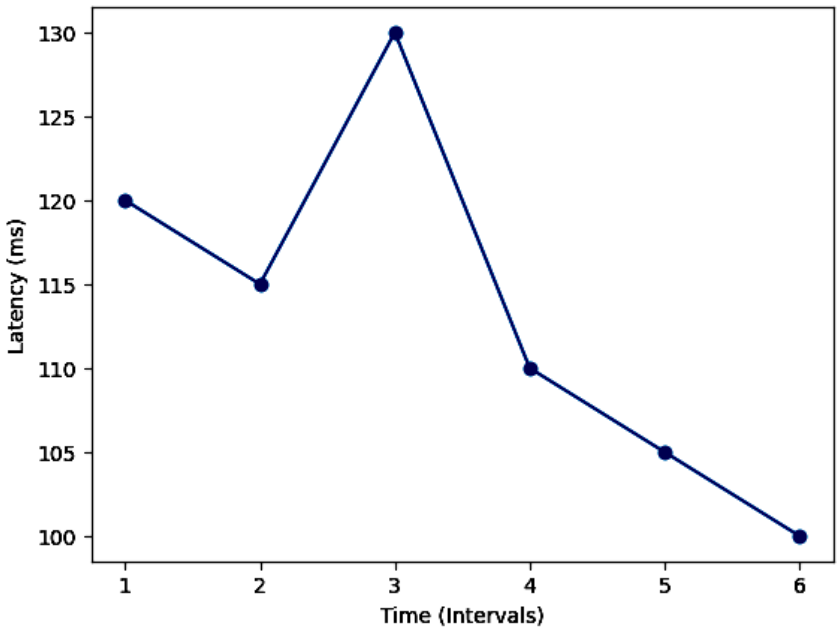

Figure. 3 Transaction Latency Over Time

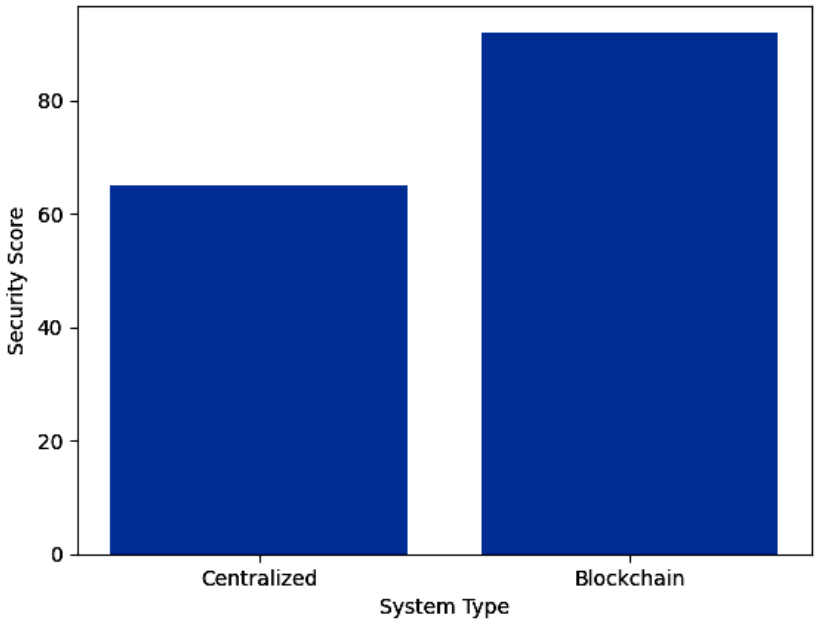

Figure. 4 Security Level Comparison

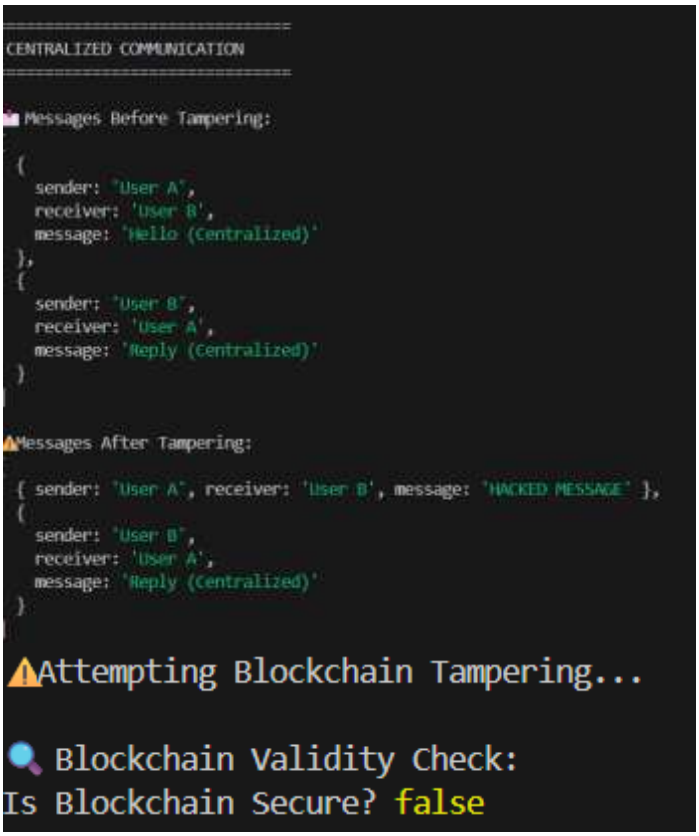

Figure. 5 Application User Interface

5.CONCLUSIONS

The expressed goal of this research is to prove the ability of Blockchain Technology to enhance the security, transparency and reliability of cyber communication systems. By using a decentralized distributed ledger, as opposed to a centralized architecture, this project will eliminate single points of failure and lower the dependence on Third Party Authority. In addition to providing decentralization, the implementation of the public/private key cryptography, Digital Signatures and Hashing Techniques, provides the properties required for protecting the confidentiality of communications, providing integrity of data, ensuring authentication and providing non-refutability of communications (the ability of recipients to verify the sender's identity). Consensus mechanisms, which provide the means to agree on the validity of a transaction among a group of networks (nodes), provide additional trust among participants by providing a method for validating transactions that are being completed on multiple nodes within the blockchain. The design of the proposed system

will protect against tampering and will be resilient to cyber-attacks.

Based on the analysis of the result from the research, the researchers concluded that the proposed blockchain-based communication systems provide an effective and resilient method for securely exchanging information in critical areas such as Finance, Healthcare, Government, and Defense. The challenges of using a blockchain-based communication system are primarily related to increased latency, limited scalability, and higher processing power requirements than traditional centralized communication systems. However, for applications requiring a significant amount of trust, these tradeoffs are acceptable. The researchers suggest that the use of Off-Chain Storage and advanced consensus algorithms could offer more efficient operation. Overall, the research findings demonstrate that Blockchain Technology represents an innovative and effective way to build next generation secure Cyber Communication Systems, which have the potential to revolutionize the future of Decentralized Digital Communications Networks.

REFERENCES

[1] W. Mougayar, *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*. Hoboken, NJ, USA: Wiley, 2016.

[2] M. Swan, *Blockchain: Blueprint for a New Economy*. Sebastopol, CA, USA: O'Reilly Media, 2015.

[3] D. Tapscott and A. Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. New York, NY, USA: Penguin, 2016.

[4] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 8th ed. Boston, MA, USA: Pearson, 2020.

[5] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, *Bitcoin and Cryptocurrency Technologies*. Princeton, NJ, USA: Princeton Univ. Press, 2016.

[6] D. Drescher, *Blockchain Basics: A Non-Technical Introduction in 25 Steps*. Berkeley, CA, USA: Apress, 2017.

[7] K. Christidis and M. Devetsikiotis, "Blockchain applications in IoT," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[8] M. Pilkington, "Blockchain technology: Principles and applications," in *Research Handbook on Digital Transformations*, E. G. Carayannis, Ed. Cheltenham, U.K.: Edward Elgar, 2016.

[9] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where is current research on blockchain technology? —A systematic review," *PLOS ONE*, vol. 11, no. 10, 2016.

[10] M. Risius and K. Spohrer, "A blockchain research framework," *Bus. Inf. Syst. Eng.*, vol. 59, no. 6, pp. 385–409, 2017.

[11] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: Beyond Bitcoin," *Appl. Innov. Rev.*, no. 2, pp. 6–19, 2016.

[12] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Gener. Comput. Syst.*, vol. 107, pp. 841–853, 2020.

[13] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," *Proc. IEEE*, vol. 107, no. 10, pp. 1754–1779, 2019.

[14] X. Xu et al., "A taxonomy of blockchain-based systems for architecture design," in *Proc. IEEE ICSE Companion*, 2017, pp. 243–252.

[15] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[16] T. T. A. Dinh et al., "Untangling blockchain: A data processing view of blockchain systems," *IEEE Trans. Knowl. Data Eng.*, vol. 30, no. 7, pp. 1366–1385, 2018.

[17] D. Yermack, "Corporate governance and blockchains," *Rev. Finance*, vol. 21, no. 1, pp. 7–31, 2017.

[18] S. Wang et al., "Blockchain-enabled smart contracts: Architecture, applications, and future trends," *IEEE Trans. Syst., Man, Cybern.: Syst.*, vol. 49, no. 11, pp. 2266–2277, 2019.

[19] Z. Li et al., "Performance evaluation of blockchain platforms: Ethereum and Hyperledger Fabric," *Future Internet*, vol. 12, no. 5, 2020.

[20] N. Atzei, M. Bartoletti, and T. Cimoli, "A survey of attacks on Ethereum smart contracts," *Int. J. Security Netw.*, vol. 12, no. 2, pp. 103–114, 2017.

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

[22] Z. Zheng, S. Xie, H. Dai, and H. Wang, "An overview of blockchain technology," in *Proc. IEEE Int. Conf. Big Data*, 2017, pp. 557–564.

[23] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," in *Proc. IEEE Int. Conf. Computer Information Technology*, 2016, pp. 2292–2303.

[24] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in *Proc. IEEE Symp. Security Privacy*, 2016, pp. 839–858.

[25] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," Ethereum Yellow Paper, 2014.

[26] V. Buterin, "A next-generation smart contract and decentralized application platform," Ethereum White Paper, 2013.