A Blockchain-Based Authentication Solution for 6G Communication Security in Tactile Networks

Khurram Shahzad, Ahmad O. Aseeri, and Munam Ali Shah

1 Department of Computer Science, COMSATS University, Islamabad 45550, Pakistan; khu777@gmail.com (K.S.); mshah@comsats.edu.pk (M.A.S.)
2 Department of Computer Science, College of Computer Engineering and Sciences, Prince Sattam Bin Abdul Aziz University, Al-Kharj 11942, Saudi Arabia
* Correspondence: a.aseeri@psau.edu.sa; Tel.: +966-(0)-11588368

Abstract: In this era, the ultimate vision is to transform current technologies into intelligent global environments to facilitate everyday transactions. The emerging Industry 4.0 has introduced promising potential technologies that have expedited the transition of Internet of Things (IoT) into the Internet of Everything (IoE), utilizing the advances in artificial intelligence. Such a transition implies that sensitive data can be effortlessly accessed via the open network used by various domains such as military, business, transportation, medical, and education, leading to potential security concerns. Although a blockchain, along with the above fields, already employs a fast network such as 5G, the explosive growth in the development and implementation of various Industry 4.0-related domains requires significantly faster networking speeds and a secure mechanism for data transfer. This exhibits the need for 6G to meet the requirements of real-time applications, as shown in the graphical representation of the abstract. The bulk of this work was performed on a blockchain, but some methodology was needed that fulfilled security at different levels, such as the process level, data level, and infrastructure level. Our contribution in this work was twofold: first, at the process level, a novel smart contract mechanism was described; and second, at the data level, a digital signature methodology was employed that allowed anonymization to authenticate and secure the blockchain without encryption.

Keywords: 6G; blockchain; authentication; tactile networks; smart contract; Industry 4.0

1. Introduction

The Internet of Everything (IoE) is a new distributed ecosystem technology that goes beyond the popular Internet of Things (IoT) by allowing the interconnection of multiple technologies and industrial sectors, which allows millions of items and sensors to create and share real-time data. Industry 4.0 relies on the IoE and the IoT’s promising potentials to achieve effective digital manufacturing and data and process transactions over a network, necessitating the use of a secure network, personal information, a data transfer system, and secure transactions [1,2]. Due to its decentralized, distributed ledger, free transaction charge, and tamper-proof and peer-to-peer technology, blockchain is well-suited for this purpose. Traditional centralized systems give greater communication and control, but a blockchain provides more secure and private assurances. In order to interact in efficient ways to fulfill the quickest manufacturing sector needs, which is the future of Industry 4.0, 5G and 6G are utilized. This could be possible with the enhancement of communication in three ways: (1) enhanced mobile broadband (eMBB); (2) massive machine-type communications (mMTC); and (3) ultra-reliable low latency communications (URLLC) [3], as shown in Figure 1.

In academia and business, the development of sixth-generation (6G) mobile communication network standards and related technologies has already become a major study topic.
To overcome the limits of existing fourth-generation (4G) and fifth-generation (5G) mobile communication networks, 6G networks are intended to be more dependable, scalable, intelligent, and power-efficient. The different factors [1] described in Figure 2 should be covered by the least futuristic implementation of 6G.

![Figure 1. Achievements in Industry 4.0 with 5G and 6G.](image1)

![Figure 2. Different aspects that are covered by 6G.](image2)

This paper discusses the necessity of obtaining faster network communication beyond 4G and 5G networks, as well as how 6G may provide forward-looking benefits, such as greater data transfer rates with less latency, quicker movement speeds, bigger system capacity, and better spectrum efficiency. Furthermore, 6G technology supports the real-time communication requirements in a variety of domains, including e-Health, artificial intelligence (AI), the line-of-controls (LOC) tracking system, and other real-time-based applications, necessitating the upgrade of existing systems to meet the level of 6G advancement to avoid data leakage caused by the mismatch [4].

Some improvements utilize blockchain technology [5,6] and consensus algorithms, i.e., tendermint [7], ripple [8], practical Byzantine fault tolerance (PBFT) [9], transaction speed [10], to fragment [11] the block and to speed up the entire mechanism [12]. However, the delegated proof-of-stake (DPoS) algorithm should play a role in enhancing the speed because DPoS speed is greater than proof of work and proof of stack [13]. Due to trade-off transactions, we could reduce cost and speed up the network [14] by managing legal and illegal activities, and we could categorize [15] and manage risk by following the ISO 31000 standard, i.e., the risk management standard [16], and by detailing an approach to the home network after observing how these communications are controlled and how to make the entire safe network. For handling the bulk of data in tactile networks, there is a need for some improvements [17] in network databases and security frameworks, such as transactions and smart contracts. The major concerns are shown in Figure 3.
Figure 3. Objectives that need improvement.

The process of sharing data can be made trustworthy by applying different monitoring schemes [18]; we can resolve the trustworthiness of IMS by using the DIaaS framework, which uses cryptographic techniques [19]. It is an open issue, when collecting data from sensors using IoT devices [20], to manage the trustworthiness of all the IoT devices; the question is how they can all be implemented using a single standard. BlockAudit and optical sensors using the write once read only technique are used to prevent logs from vulnerabilities [21]. A new version certified by smart contracts under ISO 27001 could help update the system. The purpose is to fulfill data management and transparency and prevent the data failing. In addition, tamper-proof, secure, and replicated logs need to be maintained by using the complex system i.e., a security information and event management (SIEM) [22,23].

The remainder of the paper is laid out as follows. Section 2 of this article is a literature review and a discussion of the security and privacy issues associated with 5G. Section 3 provides the details of the proposed solution. Section 4 presents the experiments and the results of the proposed solution. The paper is concluded in Section 5.

2. Literature Review

In this literature review we discuss many elements of security and privacy in Industry 4.0, as well as the difficulties and concerns that blockchains have addressed and that still need to be addressed. IoT devices are used in a wide range of industries, including business, smart logistics, banking, online commerce, society, health, military, and civilization, but network traffic management and security remain a major concern [6,24,25]. Some of these problems are identified and discussed in Figure 4.
2.1. Scalability

Due to its widespread adoption, blockchains are now being utilized in a variety of fields on a big scale. The consensus protocol has a direct impact on the scalability of blockchain technology. This method reduces information leakage during transactions [2,3].

2.1.1. Confidentiality Integrity and Availability (CIA)

Because blockchain technology is an emerging technology with access control to provide confidentiality, integrity, and availability, it meets the CIA’s standards. As blockchain data is decentralized, confidentiality is not guaranteed, but it ensures integrity and availability owing to its distributed ledger and tamper-proof nature.

2.1.2. Fault Tolerance

Fault tolerance in a blockchain may be defined as the ability of an artificial intelligence scheme to regulate errors and withstand any electronic or software faults and failures. In the IEEE specification, the term “fault and failure” is used. To process data in an advanced security system, a cryptographic method such as PBFT is combined with digital signatures and hash algorithms. Due to the proof-of-stake blockchain, PBFT is utilized to govern real-time systems and some aviation systems, like the SpaceX Dragon, rely on it [4].

2.1.3. Security

Due to the irreversible record-keeping method, a blockchain is more secure and difficult to tamper with. A one-way cryptographic hash method is used to accomplish this. Furthermore, thanks to private keys, a blockchain is considerably more secure [5], since these private keys provide signatures for transactions and prevent them from being modified. Every node should be able to update the signature.
2.2. Privacy

Data security, privacy, and dependability are all challenges that arise as a result of the IoT. The work in [6] provides secure transactions by encrypting ID information and hiding network operations from outsiders. Data is safe because it is more difficult for an anonymous individual to duplicate it. When data is anonymized using any method, it becomes harder for an adversary to search the data for a specific individual or acquire specific information from it.

2.2.1. Transparency

As everyone can observe the transaction history that is kept openly in a blockchain it provides transparency. A BC’s anonymity behavior provides full transparency and redundancy by leveraging a public network. As immutable data is transparent, it is more responsible. These functionalities can be enhanced by ensuring the application’s compatibility [7].

2.2.2. Transaction Control

Public key and private key generation make transactions more reliable and resistant to any leakage in the transaction. Users have the authority to create smart contracts and validate transactions [8] and can check the transaction history maintained by the blockchain. Due to the transaction history, a blockchain can analyze and control any supply chain.

2.3. Legal Issues

Before BC technology, a centralized system was employed. As a result, the biggest concerns were data protection and handling, particularly in the legal, healthcare, and military sectors. As we all know, laws differ from state to state, thus new laws and standards governing the security characteristics of IoT devices are urgently needed. It is necessary to enact regulations that deal with information and metadata, which is a major challenge in this field.

2.3.1. Information Privacy

Clients and owners have rights on a blockchain, which ensures security, privacy, authentication, and access control. The owner can allow third parties to read data using the data management system in [26]. By using the decentralized technique [27] we can give protection and provide privacy for data.

2.3.2. Information Handling

A blockchain protects the confidentiality of information by adopting encryption-based mechanisms, which depend on the system. Security, storage, and data management cannot be denied after BCT. A BC also limits the problem of transactional or data privacy and the expressiveness of programming languages.

2.4. Data Management

The undeniable property of a blockchain, which has the potential of workflow management in a cross-organizational framework, is data management. The literature review of BC policy describes its data-audit ability, i.e., its secure, efficient, and verifiable manners. Its privacy policy underestimates the types of disclosures as it requires less computational power and worth. Decentralized behavior is sustainable and can disseminate and manage the metadata flow in a safe environment. Major concerns of data management are provided in Figure 5.
2.4.1. Data Storage

As data storage is the most important aspect of data management, a BC also satisfies proof of capacity, often known as evidence of storage or proof of space. Shard data are encrypted using a private key to prevent other nodes in a network from accessing them. No one can tamper with the data since the blockchain stores it in a public ledger and keeps track of all prior data exchanges.

2.4.2. SPOF

The decentralized and shared behavior of a blockchain tackles the single point of failure as it has a public ledger and off-chain sources [5]. This character deals with the ‘bottlenecks’ of off-chain sources, called single points of failure. It makes the system more resilient than a centralized system. The products of a blockchain having the quality of SPOF reduce the likelihood of cyber-attacks.

2.4.3. Security Technique

Regarding performance, security techniques of IoT devices should be prioritized at different levels by observing the needs of organization policies and budgets. By filtering different literature [5], IoT data can be compressed to reduce the space need to store them.

2.5. Risk Management

The major point of discussion is risk management [5], which is applied to a scheme to assess, control, and identify risk.

2.5.1. Standard and Smart Contract Risk

Smart contracts handle the inconspicuousness in the IoT by using an extensible blockchain. Using smart contracts it is possible, through the immutability character [5] of a blockchain, to prevent fraudulent and operational errors. Smart contracts used by artificial intelligence [2] enable the use of strategies to maintain and update the system automatically. The application logic of the IoT and special entities, such as oracles, work with smart contracts to deal with real-world data with trust issues. Smart contracts can be compromised when a system is not up to date, not validated, or when contract data requests are overloaded. In advanced systems, this is now not possible due to multiple nodes being compromised because they need strong resources and large computational power, this effect is also enhanced due to the capability and processing power of cloud computers. Data mining techniques, which process big data and require a large amount of computing power, enable an application to address and filter the context and requirements of data. Hence, due to this behavior, applications become powerful. Smart contracts enable

---

**Figure 5.** Major concerns of data management.

- Data Storage
- SPOF
- Security Technique
- Data Management

---

**Figure 5.** Major concerns of data management.
fast action with the IoT and can secure [2,9] communication between devices. The IoT uses the current standard protocol to optimize the application of BC technology securely.

2.5.2. CIA and Policy Management

The IoT raises various difficulties in a security management system, including standards, authentication, secrecy, integration, and protocol. All of these qualities cannot be pursued in a single bundle; as a result, hybrid algorithm strategies must be used to handle these regulations.

2.6. Security

A BC may be used to accomplish security by utilizing proper tools, policies, and services for the detection and prevention of internal and peripheral malware threats. These components of security are shown in Figure 6 [8]. BC technology enhances security by improving the systems in [28,29], as shown in Figure 7.

Figure 6. Data security components.

Figure 7. Security can be enhanced by improving tools.

Security must be achieved through safeguarding sensitive data and eliminating design flaws. A system with security faults, as shown in Figure 8, cannot avoid threats, assaults, dangers, or vulnerabilities; data security, privacy, and reliability are the vulnerabilities. The components of security are depicted in Figure 9. Data encryption and data privacy are two security components based on the solution.
program consisting of code. Unfortunately, it is very difficult to ensure that the program is free of loopholes and flaws [11].

2.6.2. Loopholes

An adversary could find the weakest point in endpoint devices and penetrate it.

2.6.1. Vulnerabilities

Endpoint devices should be updated and fully secured because an adversary could find the weakest point in endpoint devices and penetrate it.

2.7. Consensus

A blockchain manages and checks vulnerabilities by managing authentication, modification, patching, and identification to secure the system from risk, threat, surface attacks, and vulnerability. Endpoint devices should be updated and fully secured because an adversary could find the weakest point in endpoint devices and penetrate it.

A blockchain manages and checks vulnerabilities by managing authentication, modification, patching, and identification to secure the system from risk, threat, surface attacks, and vulnerability. Endpoint devices should be updated and fully secured because an adversary could find the weakest point in endpoint devices and penetrate it.

2.6.2. Loopholes

When core developers work on the development of a blockchain they write a bug-free program consisting of code. Unfortunately, it is very difficult to ensure that the program is free of loopholes and flaws [11].

2.7. Consensus

A blockchain is made up of encrypted data blocks created by a series of hash codes. All devices connected to a network have a node assigned to them. By hash coding, each node has a copy of that record, and the blockchain’s immutability is ensured by the consensus.
method [12]. The consensus system, which is based on PoW, PoS, and PoI, validates each block’s transaction and provides a speedy response to a long chain of information in the blockchain.

2.7.1. The Need for High Processing Power

Computational power directly affects transaction time. So, the consensus protocol directly hits the scalability of a BC in IoT devices [2,7]. This process can be performed by using a full-scale quantum computing supremacy [13,14] 72-qubit device, Bristlecone, which is a quantum computer. Sycamore is a functional 53-qubit processor, but processors with over 53 qubits do not work properly and need to work for robust protocols in order to correct the quantum errors [14].

2.7.2. The Huge Amount of Energy

Due to the increase in IoT devices, a high amount of energy is required; using a blockchain in a hybrid system provides an efficient protocol. The redundancy error needs to be improved because a BC has multiple data in a single node, due to the public ledger. Minimizing redundancy requires less computational power to be use for the same amount of data in less space [8].

2.8. Addressing Space

A blockchain address is a numbered sequence of series that need less space for any database concerned with a centralized system.

Addressing Space and Data Needs

A BC has the flexibility to store all types of private or sensitive data related to a person or an entity. Moreover, a BC leads to data redundancy and so achieves transparency and verifiability due to the minimization of data. By using the hybrid methods, power of work and power of stack, developed by IBM, to mine blocks gives a reliable execution. When addressing space or storage, a hybrid system uses hard drive space instead of other computing resources [15].

Currently, 5G works at 50 Mbps and gives a latency of 10 ms, which needs to be improved at the highest rates. The speed factor also depends on the device type used for IoT devices. Radio spectrum regulators should work at all levels in all countries or around the world [16].

2.9. Related Work

With increasing commercial and creative possibilities for program developers to create new and innovative 5G-enabled network applications (NetApps) across a variety of business sectors, 5G infrastructures and architectures are being pushed to keep up with all of these NetApp requirements. This study focused on adapting 5G designs for future verticals and NetApps, and it started with a brief overview of the existing and future 5G environment, then moved on to the 5G-PPP initiatives that led to the early deployment of a 5G test platform in Romania. We also concentrated on the vertical contexts and NetApps, as illustrated by the two 5G-PPP initiatives, VITAL-5G and 5GASP, which developed a step-by-step 5G network to accommodate all of these difficult NetApps and vertical use cases.

The 5G-based network applications (NetApps) are crucial facilitators for the adoption of 5G solutions because they abstract the complexities underpinning the 5G infrastructure for T&L app developers, reducing the creation of services and deployment times, and optimizing 5G resource use. VITAL-5G is a European Innovation Action project to advance T&L services by demonstrating the benefits of 5G-based NetApps through real-world trials in state-of-the-art vertical (T&L) facilities (warehouses, hubs, ports) and sophisticated European 5G testbeds. VITAL-5G will provide an intricate experimental service portal and virtual repository to serve both internal and third-party experimentation, allowing for the
deployment, design, monitoring, and configuration, or reconfiguration, of NetApps in the vertical context. This work provided an overview of the existing issues and roadblocks that might hinder the adoption and penetration of 5G-based solutions in the T&L sector, as well as the methodology taken by the recently funded VITAL-5G project to solve them. VITAL-5G aimed to close the knowledge/expertise gap between telecommunications providers, vertical industries, and application developers by promoting and validating NetApps through its cutting-edge experimentation facilities, where cutting-edge technologies and NetApps were put to the test as part of T&L industry-driven use cases. The project goals, targeted innovations, and created NetApps presented in this article will help accelerate the adoption and penetration of more flexible, multi-modal, and reconfigurable 5G-based systems into the market [18].

The Personal Tactile Internet, enabled by 6G, must offer an infrastructure that allows everyone to use remote-controlled mobile robotic systems. The deployed cellular network must be able to handle peak traffic. The typical cellular-area pixels bear considerably less load than peak pixels when massive MIMO is used. As we approach the mm-wave spectrum above 80 GHz, massive new quantities of the spectrum might be exploited if the new spectrum could be used for communication and sensing simultaneously. As a result, the concept may be to go from a “gear” of spectrally wasteful spike modulation during low traffic and detecting demand to a gear of ZXM during low demand, to a gear of ZXM during high demand. As a result, the concept might be to go from a “gear” of spectrally inefficient spike modulation during extremely low traffic and sensing demand to a gear of ZXM during low demand, to continuous-phase modulation, QAM, and MIMO–OFDM, as demand develops. Spectral efficiency comes at the expense of more energy, and it is only necessary for MAC-pixels that experience a lot of traffic. Enabling the Tactile Internet alone for consumer applications and tackling the looming energy crisis under semiconductor technology and circuit constraints, presents us with an almost limitless number of difficulties [30]. Surprisingly, the majority of these problems cannot be handled just by mathematical understanding, but rather they the need consideration of network and hardware realities. To put it another way, genuine system understanding is a future issue for information theory’s role in 6G [19].

3. Proposed Solution

Digital watermarks can be added to a message by taking an image or video of all of these hashes and embedding the hash of the image or video in the message. The image is divided into small blocks of pixels, and all of these pixels can be shuffled with any matrix or algorithm to create the hash value of this image, and the receiver must know this matrix or algorithm in order to restore the image to its original state. Our first contribution was to provide a novel approach that ensured two important facts in the record.

1. The record should be unaltered;
2. The record should be tamper-free.

In a blockchain, the sender uses a digital signature to interact with another node through a message. A receiver obtains a public key from the ledger to validate the digital signature. Figure 10 depicts this signature in action for authentication.

(1) Sender calculates hash;
(2) Sender encrypts with its private key;
(3) A digital signature is transmitted with the SMS;
(4) The receiver uses the sender’s public key;
(5) The receiver decrypts the message;
(6) The hash value is obtained;
(7) The hash is matched.
In these IoT devices, we may improve this form of digital signature by using the hysteresis digital signature (HDS) scheme, which stores the digital signature of each message in a ledger. The following are some of Merkle’s signature restrictions when it comes to HDS:

**Merkle’s Signature**
- The one-way hash function is the base of Merkle’s signature, which is vulnerable now due to quantum computation.
- The compromise of a digital signature is a fail-stop signature scheme.
- It is the identity signature’s audit log.
- It makes it difficult for an attacker to modify a message.
- It uses a rule-based intrusion detection system.

Because blockchains in IoT devices are based on Merkel’s tree, this paper focused on communication authentication behavior. In place of Merkel’s tree, we suggested a new technique called the hysteresis digital signature. The simple process idea is depicted in Figure 11.
It was the first step in deploying AAA checks for BC authentication with signature logs. These logs were checked by managers following the ISO 27000 set of information security standards. We had a better approach communicating our sensitive data using BC technology by integrating the smart contract audit and ensuring AAA. The data controller was a software or hardware agent, or a third party, who inspected the data and processes that were stored or gathered.

Each block transaction was checked by a data processor, which then stored the information for auditing reasons. To finish the file processing, we transmitted them across two blockchains, as indicated in Figure 12. All activities were run on these two BCs. The following actions were taken to transfer data from one blockchain to another. In such a case, the system kept a record of past log history on both blockchain sides.

Figure 11. Model for the hysteresis digital signature.

Figure 12. All activities between the two blockchains.
4. Experiments and Results

Figure 13 depicts the percentage of improvements in transparency, accuracy, SPOF, docs temper, security, efficiency, and address space in the military, industry, transportation, healthcare, and education before and after our scheme, and Figure 14 depicts the percentage of improvements after our scheme.

![Figure 13](image1.jpg)

**Figure 13.** Results of various fields, calculated in an index, before 6G.

![Figure 14](image2.jpg)

**Figure 14.** Results of various fields, calculated in an index, after 6G.

These percentage values are also shown in Figure 15, which shows the security achievements that were achieved in IoT devices before blockchain technology, meaning security was achieved with a centralized system; these results are shown with the results achieved after applying blockchain technology.

For example, when a centralized system was used, transparency was 70 percent and accuracy was 85 percent; however, when blockchain technology was used, transparency was 92 percent and accuracy was 93 percent; SPOF was 60 percent when a centralized system was used but was reduced to 23 percent with blockchain technology; similarly, docs tempering was 50 percent but was reduced to 16 percent with blockchain technology; and 88 percent security was achieved. The same strategy was used in the fields of commerce, transportation, medicine, and education, as shown in the table. Figure 16 depicts the difference in improvements visually; that is the number of accomplishments that were achieved.
Figure 15. The difference of the results achieved before and after the launch of 6G.

| Analysis            | Military | Business | Transport | Medical | Education |
|---------------------|----------|----------|-----------|---------|-----------|
| Transparency        | Before 6G| After 6G | Before 6G | After 6G| Before 6G | After 6G | Before 6G | After 6G | Before 6G | After 6G |
| Transparency        | 70       | 92       | 38        | 51      | 55        | 66       | 50        | 68       | 76        | 80       |
| Accuracy            | 85       | 93       | 29        | 48      | 55        | 64       | 48        | 72       | 70        | 74       |
| SPOF                | 60       | 23       | 84        | 60      | 70        | 62       | 66        | 40       | 61        | 48       |
| Docs Tampering      | 50       | 16       | 53        | 32      | 53        | 25       | 43        | 28       | 68        | 49       |
| Security            | 88       | 91       | 22        | 38      | 66        | 70       | 60        | 74       | 62        | 68       |
| Efficiency          | 68       | 86       | 34        | 48      | 43        | 55       | 62        | 70       | 71        | 76       |
| Addressing space    | 66       | 86       | 45        | 70      | 58        | 65       | 38        | 49       | 66        | 72       |

Figure 16. Difference between Figures 13 and 14, shown graphically.
5. Conclusions

Because of the rapid progress and digitalization of Industry 4.0, it is impossible to guarantee 100 percent security even when we installed our privacy and security measures, but we might establish effective obstacles for the attacker. According to a review of the literature, blockchains are used in a wide range of industries. The features, shortcomings, problems, and concerns of blockchain technology in the IoT area were presented in this study. We could offer data safety and privacy by employing decentralized techniques and public ledgers. We compared and improved how blockchain technology affects and boosts transparency, accuracy, security, efficiency, and addressing space, as well as how to reduce single points of failure and document manipulation. Although a blockchain is slower than a centralized system, it addresses security issues. We strengthened the security of a blockchain by implementing AAA and conducting an audit of these smart contracts and data topics, because, according to our study, blockchain is the future medium of success.

Our next objective was to develop this blockchain by including a new authentication mechanism that would boost privacy and security. Depending on the structure of the organization, hybrid solutions could make the system speedier and more secure. To address these concerns, network speed, processing power, a secure network, risk management, a shared standard solution, and privacy rules were all requirements for upgrading. Only quantum neural network technology could address the fundamental demand for real-time applications in the digital age. There is a need to cover 6G, which will be a global demand beyond 2030, when everything will be connected to Industry 4.0 and everyone will be well-versed in AI and robotics.

Author Contributions: Conceptualization, M.A.S.; methodology, K.S.; resources, A.O.A. All authors have read and agreed to the published version of the manuscript.

Funding: The authors would like to acknowledge the funding support by the Department of Computer Science, College of Computer Engineering and Sciences, Prince Sattam Bin Abdul Aziz University, Kingdom of Saudi Arabia.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Chen, S.; Liang, Y.-C.; Sun, S.; Kang, S.; Cheng, W.; Peng, M. Vision, requirements, and technology trend of 6G: How to tackle the challenges of system coverage, capacity, user data-rate and movement speed. IEEE Wirel. Commun. 2020, 27, 218–228. [CrossRef]
2. Reyna, A.; Martin, C.; Chen, J.; Soler, E.; Diaz, M. On blockchain and its integration with IoT: Challenges and opportunities. Future Gener. Comput. Syst. 2018, 88, 173–190. [CrossRef]
3. Siow, E.; Tiropanis, T.; Hall, W. Analytics for the Internet of Things: A Survey. ACM Comput. Surv. 2018, 51, 74. [CrossRef]
4. Castro, M.; Liskov, B. Practical byzantine fault tolerance and proactive recovery. ACM Trans. Comput. Syst. 2002, 20, 398–461. [CrossRef]
5. Tasca, P.; Tessone, C.J. A Taxonomy of Blockchain Technologies: Principles of Identification and Classification. Legger 2019, 4, 5. [CrossRef]
6. Wang, Y.; Cai, Z.; Tong, X.; Gao, Y.; Yin, G. Truthful incentive mechanism with location privacy-preserving for mobile crowdsourcing systems. Comput. Netw. 2018, 135, 32–43. [CrossRef]
7. Casino, F.; Dasaklis, T.K.; Patsakis, C. A systematic literature review of blockchain-based applications: Current status, classification and open issues. Telemat. Inform. 2019, 36, 55–81. [CrossRef]
8. Joshi, A.P.; Han, M.; Wang, Y. A survey on security and privacy issues of blockchain technology. Math. Found. Comput. 2018, 1, 121–147. [CrossRef]
9. Khan, M.A.; Salah, K. IoT security: Review, blockchain solutions, and open challenges. Future Gener. Comput. Syst. 2018, 82, 395–411. [CrossRef]
10. Baghery, K.; Kohlweiss, M.; Siim, J.; Volkhov, M. Another Look at Extraction and Randomization of Groth’s zk-SNARK. In Proceedings of the International Conference on Financial Cryptography and Data Security, Virtual Event, 5 March 2021; Available online: https://link.springer.com/chapter/10.1007/978-3-662-64322-8_22 (accessed on 1 March 2022).
11. Marwala, T.; Xing, B. Blockchain and artificial intelligence. arXiv 2018, arXiv:1802.04451.
12. Yazdinejad, A.; Srivastava, G.; Parizi, R.M.; Dehghantanha, A.; Karimipour, H.; Karizno, S.R. SLPoW: Secure and Low Latency Proof of Work Protocol for Blockchain in Green IoT Networks. In Proceedings of the IEEE 91st Vehicular Technology Conference (VTC2020-Spring), Antwerp, Belgium, 25–28 May 2020, pp. 1–5.
13. Sultan, A.; Malik, M.S.A.; Mushtaq, A. Internet of Things Security Issues and their Solutions with Blockchain Technology Characteristics: A Systematic Literature Review. *Am. J. Comput. Sci. Inf. Technol.* 2018, 6, 27. [CrossRef]

14. Villalonga, B.; Lyakh, D.; Boixo, S.; Neven, H.; Humble, T.S.; Biswa, R.; Rieffel, E.G.; Ho, A.; Mandrà, S. Establishing the quantum supremacy frontier with a 281 piflop/s simulation. *arXiv* 2019, arXiv:1905.00444. [CrossRef]

15. Miller, A.; Juels, A.; Shi, E.; Parno, B.; Katz, J. Permacoin: Repurposing bitcoin work for data preservation. In Proceedings of the IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 18–21 May 2014; pp. 475–490.

16. O’Connell, E.; Moore, D.; Newe, T. Challenges Associated with Implementing 5G in Manufacturing. *Telecom 2020*, 1, 48–67. [CrossRef]

17. Patachia-Sultanoiu, C.; Bogdan, I.;Suciu, G.; Vulpe, A.; Badita, O.; Rusti, B. Advanced 5G Architectures for Future NetApps and Verticals. In Proceedings of the IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), Bucharest, Romania, 24–28 May 2021; pp. 1–6.

18. Trichias, K.; Landi, G.; Seder, E.; Marquez-Barja, J.; Frizzell, R.; Iordache, M.; Demestichas, P. VITAL-5G: Innovative Network Applications of NetApps Support over 5G Connectivity for the Transport & Logistics Vertical. In Proceedings of the Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit), Porto, Portugal, 8–11 June 2021; pp. 437–442.

19. Fettweis, G.P.; Boche, H. 6G: The Personal Tactile Internet-and Open Questions for Information Theory. *IEEE BITS Inf. Theory Mag.* 2021, 1, 71–82.

20. Fernandez-Caramés, T.M.; Froiz-Miguez, I.; Blanco-Novoa, O.; Fraga-Lamas, P. Enabling the internet of mobile crowdsourcing health things: A mobile fog computing, blockchain and IoT based continuous glucose monitoring system for diabetes mellitus research and care. *Sensors* 2019, 19, 3319. [CrossRef] [PubMed]

21. Ahmad, A.; Saad, M.; Bassiouni, M.; Mohaisen, A. Towards blockchain-driven, secure and transparent audit logs. In Proceedings of the 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, New York, NY, USA, 5–7 November 2018; pp. 443–448.

22. Thakker, J.; Chang, I.; Park, Y. Secure Data Management in Internet-of-Things Based on Blockchain. In Proceedings of the 2020 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 4–6 January 2020; pp. 1–5.

23. Tataria, H.; Shaﬁ, M.; Molisch, A.F.; Dohler, M.; Sjöland, H.; Tufvesson, F. 6G Wireless Systems: Vision, Requirements, Challenges, Insights, and Opportunities. *Proc. IEEE 2021*, 109, 1166–1199. [CrossRef]

24. Jesus, E.F.; Chicarino, V.R.; De Albuquerque, C.V.; Rocha, A.A.D.A. A survey of how to use blockchain to secure internet of things and the stalker attack. *Secur. Commun. Netw.* 2018, 2018, 9675050. [CrossRef]

25. Selvaraj, P.; Doraikannan, S.; Burugari, V.K. Security Vulnerabilities, Threats, and Attacks in IoT and Big Data: Challenges and Solutions; IGI Global: Dehradun, India, 2020; p. 27.

26. Tezel, A.; Papadonikolaki, E.; Yitmen, I.; Hilletofth, P. Preparing construction supply chains for blockchain technology: An investigation of its potential and future directions. *Front. Eng. Manag.* 2020, 7, 547–563. [CrossRef]

27. Shrier, D.; Wu, W.; Pentland, A. *Blockchain & Infrastructure (Identity, Data Security)*; Massachusetts Institute of Technology-Connection Science: Cambridge, MA, USA, 2016; Volume 1, pp. 1–19.

28. Li, X.; Jiang, P.; Chen, T.; Luo, X.; Wen, Q. A survey on the security of blockchain systems. *Future Gener. Comput. Syst.* 2020, 107, 841–853. [CrossRef]

29. Hasanova, H.; Baek, U.J.; Shin, M.G.; Cho, K.; Kim, M.S. A survey on blockchain cybersecurity vulnerabilities and possible countermeasures. *Int. J. Netw. Manag.* 2019, 29, e2060. [CrossRef]

30. Rahimi, A.; Maddah-Ali, M.A. Multi-Party Proof Generation in QAP-Based zk-SNARKs. *IEEE J. Sel. Areas Inf. Theory* 2021, 3, 931–941. [CrossRef]