Mesopotamian journal of Computer Science
Vol. **(2022)**, 2022, **pp**. 5–9
DOI: https://doi.org/10.58496/MJCSC/2022/006 ; ISSN: 2958-6631
https://mesopotamian.press/journals/index.php/cs

Research Article

Blockchain and Distributed Ledger Technologies for IoT Security: A Survey paper

Suleiman Abdulrahman [1,*], Maroning Useng [2]

[1] *Center for Atmospheric Research Nigeria, ICT University, Abuja, Nigeria*

[2] *Department of data science and analytics, Fatoni University, Pattani, Thailand*

ARTICLE INFO

Article History

Received 02 Jan 2022
Accepted 19 Mar 2022
Published 15 Apr 2022

Keywords

Blockchain

Ledger Technologies

IoT

Distributed Computing

ABSTRACT

As the Internet of Things (IoT) continues to grow, the security concerns associated with this technology become increasingly important. Blockchain and Distributed Ledger Technologies (DLTs) are emerging as potential solutions for IoT security due to their decentralized and immutable nature. In this survey paper, we provide a comprehensive overview of the state-of-the-art research in the use of blockchain and DLTs for IoT security. We begin by introducing the basic concepts of blockchain and DLTs, followed by a discussion of their potential applications in IoT security. We then review the existing literature on the topic, including both academic and industrial research. We categorize the literature into different application areas, such as authentication, access control, and data integrity. Finally, we discuss the open research challenges and potential future directions for the use of blockchain and DLTs in IoT security. This survey paper provides a valuable resource for researchers and practitioners interested in understanding the current state-of-the-art research in this important area of IoT security.

1. INTRODUCTION

The Internet of Things (IoT) has been rapidly gaining momentum in recent years, with an increasing number of devices being connected to the internet. However, the growth of the IoT has also led to an increase in security concerns, as many IoT devices are vulnerable to attacks due to their limited computational resources and lack of security measures. In this context, blockchain and Distributed Ledger Technologies (DLTs) have emerged as potential solutions for IoT security. Blockchain is a distributed database that stores data in a tamper-proof manner, making it an ideal technology for securing sensitive data. DLTs, on the other hand, are a broader class of technologies that allow multiple parties to maintain a shared ledger of transactions, without relying on a central authority. Both blockchain and DLTs offer the potential to provide increased security, privacy, and transparency in the context of the IoT[1].

In this survey paper, we provide a comprehensive overview of the state-of-the-art research in the use of blockchain and DLTs for IoT security. We begin by introducing the basic concepts of blockchain and DLTs, followed by a discussion of their potential applications in IoT security. We then review the existing literature on the topic, including both academic and industrial research. We categorize the literature into different application areas, such as authentication, access control, and data integrity. Finally, we discuss the open research challenges and potential future directions for the use of blockchain and DLTs in IoT security.

This survey paper aims to provide a valuable resource for researchers and practitioners interested in understanding the current state-of-the-art research in this important area of IoT security. By analyzing and summarizing the existing literature, we hope to identify key research gaps and provide guidance for future research in this area[2].

2. METHODS

2.1 Blockchain

Blockchain is a decentralized and distributed digital ledger technology that allows data to be recorded and stored in a secure and tamper-proof manner. In other words, it is a database that is maintained by a network of computers, rather than a single centralized authority.

*Corresponding author. Email: suleiman.a@carnasrda.com

The fundamental building blocks of a blockchain are blocks, which contain a set of data records, and a digital signature, called a hash, that links each block to the previous block in the chain. Each block in the chain contains a reference to the hash of the previous block, creating a chain of blocks that cannot be altered without invalidating the entire chain. This makes it extremely difficult for anyone to tamper with the data stored in a blockchain, as any changes made to one block would be immediately detected and invalidated by the rest of the chain.

One of the key features of blockchain technology is its decentralized nature, which means that there is no single point of failure or control. Instead, the network of computers that maintain the blockchain work together to validate transactions and ensure the integrity of the chain. This makes it more difficult for attackers to compromise the system, as they would need to compromise a majority of the computers in the network.

Blockchain technology has been primarily associated with cryptocurrencies, such as Bitcoin, which use blockchain to maintain a decentralized and secure ledger of transactions. However, blockchain has many potential applications beyond cryptocurrencies, such as in supply chain management, voting systems, and data storage.

In summary, blockchain is a digital ledger technology that allows data to be recorded and stored in a secure and tamper-proof manner, using a decentralized network of computers to maintain and validate the data. Its potential applications are vast, and it has the potential to revolutionize many industries by providing secure and transparent data storage and transaction management[3].

2.2 Distributed Ledger Technologies (DLTs)

The Internet of Things (IoT) is a network of physical devices, vehicles, home appliances, and other objects that are embedded with sensors, software, and network connectivity, allowing them to collect and exchange data. However, the growth of the IoT has also led to an increase in security concerns, as many IoT devices are vulnerable to attacks due to their limited computational resources and lack of security measures. In this context, Distributed Ledger Technologies (DLTs), such as blockchain, have emerged as potential solutions for IoT security.

DLTs are a broad class of technologies that allow multiple parties to maintain a shared ledger of transactions, without relying on a central authority. DLTs use a distributed network of computers to maintain the ledger, which makes it extremely difficult for any single party to alter or manipulate the data stored in the ledger. Blockchain is a type of DLT that uses cryptographic techniques to ensure the integrity and immutability of the data stored in the ledger.

One of the potential applications of DLTs in IoT is in the area of supply chain management. By using a blockchain-based system, it is possible to track the movement of goods through the supply chain, from the point of origin to the point of consumption, in a secure and transparent manner. This can help to prevent fraud and counterfeiting, and can also help to ensure that products are sourced from ethical and sustainable suppliers.

Another potential application of DLTs in IoT is in the area of identity and access management. By using a blockchain-based system, it is possible to create a secure and tamper-proof identity for each IoT device, which can then be used to control access to sensitive data and services. This can help to prevent unauthorized access and ensure the privacy and security of IoT data.

Finally, DLTs can also be used to create decentralized marketplaces for IoT data and services. By using a blockchain-based system, it is possible to create a marketplace where IoT devices can sell their data and services directly to other devices or to third-party applications. This can help to create a more efficient and decentralized IoT ecosystem, where data and services are exchanged in a secure and transparent manner.

In summary, DLTs, such as blockchain, offer the potential to provide increased security, privacy, and transparency in the context of the IoT. By using a distributed and tamper-proof ledger, it is possible to create a more secure and efficient IoT ecosystem, where devices and data can be trusted and verified. The potential applications of DLTs in IoT are vast, and it is likely that we will see many more use cases emerge in the coming years as the technology continues to mature[4].

3. APPLICATIONS OF BLOCKCHAIN IN IOT SECURITY

Blockchain has several potential applications in IoT security. Here are some of them:

1. Supply Chain Management: One of the primary applications of blockchain in IoT security is supply chain management. By using a blockchain-based system, it is possible to track the movement of goods through the supply chain, from the point of origin to the point of consumption, in a secure and transparent manner. This can help to prevent fraud and counterfeiting, and can also help to ensure that products are sourced from ethical and sustainable suppliers.

2. Identity and Access Management: Another potential application of blockchain in IoT security is in the area of identity and access management. By using a blockchain-based system, it is possible to create a secure and tamper-proof identity for each IoT device, which can then be used to control access to sensitive data and services. This can help to prevent unauthorized access and ensure the privacy and security of IoT data.
3. Decentralized Marketplaces: DLTs can also be used to create decentralized marketplaces for IoT data and services. By using a blockchain-based system, it is possible to create a marketplace where IoT devices can sell their data and services directly to other devices or to third-party applications. This can help to create a more efficient and decentralized IoT ecosystem, where data and services are exchanged in a secure and transparent manner.
4. Smart Contracts: Smart contracts are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code. They can be used to automate the execution of complex business processes between parties. Smart contracts can be utilized in the context of IoT to automatically execute transactions and enforce contracts between devices, thereby reducing the risk of fraud and increasing efficiency.
5. Data Integrity and Provenance: Blockchain can be used to ensure the integrity and provenance of IoT data. By storing data on a tamper-proof and distributed ledger, it is possible to verify that the data has not been altered or manipulated. This can help to improve the accuracy and reliability of IoT data, which is essential for applications such as remote monitoring and predictive maintenance.

Blockchain and DLTs offer a wide range of potential applications for improving the security and privacy of IoT devices and data. As the technology continues to mature, we can expect to see many more innovative use cases emerge in this area[5].

4. CHALLENGES AND LIMITATIONS

While blockchain and distributed ledger technologies (DLTs) have many potential benefits for IoT security, there are also several challenges and limitations to consider. Here are some of them:

1. Scalability: One of the main challenges of using blockchain in IoT is scalability. As the number of IoT devices increases, so does the amount of data that needs to be stored on the blockchain. This can lead to issues with block size, transaction processing speed, and network bandwidth. Some solutions to this challenge include using off-chain solutions, such as sidechains or state channels, to reduce the amount of data that needs to be stored on the blockchain.
2. Interoperability: Another challenge of using blockchain in IoT is interoperability. There are many different types of blockchains and DLTs, each with their own protocols, consensus mechanisms, and smart contract languages. This can make it difficult for IoT devices to communicate with each other, and for different blockchains to interoperate with each other. Some solutions to this challenge include developing standardized protocols and interoperability frameworks.
3. Regulatory Environment: The regulatory environment around blockchain and DLTs is still evolving, which can create uncertainty for IoT applications. There are also concerns around data privacy, data ownership, and liability, which need to be addressed in order to create a trusted and secure IoT ecosystem.
4. Security Risks: While blockchain and DLTs can help to improve IoT security, they also introduce new security risks. For example, smart contracts can be vulnerable to bugs and exploits, which can lead to security breaches. In addition, the decentralization of blockchain networks can make them more difficult to secure than centralized systems.
5. Energy Consumption: Finally, blockchain and DLTs can be energy-intensive, which can be a concern for IoT devices with limited battery life. Some solutions to this challenge include developing more energy-efficient consensus mechanisms, such as proof-of-stake, and using off-chain solutions to reduce the amount of data that needs to be stored on the blockchain.

While blockchain and DLTs offer many potential benefits for IoT security, it is important to carefully consider the challenges and limitations before implementing these technologies. By addressing these challenges, we can help to create a more secure and efficient IoT ecosystem[2, 3].

5. FUTURE DIRECTIONS

As blockchain and distributed ledger technologies (DLTs) continue to evolve, there are several future directions that could shape the future of IoT security. Here are some potential future directions:

1. Interoperability Standards: As the number of blockchains and DLTs grows, there is a need for interoperability standards that allow IoT devices to communicate with each other and with different blockchains. Developing standardized protocols and interoperability frameworks can help to create a more efficient and interconnected IoT ecosystem.
2. Integration with AI and Machine Learning: The integration of blockchain and DLTs with artificial intelligence (AI) and machine learning (ML) could lead to new applications in IoT security. For example, AI and ML algorithms could be used to detect anomalies and threats in real-time, while blockchain and DLTs could be used to secure and manage IoT data and transactions.
3. Privacy-Preserving Techniques: As data privacy concerns continue to grow, there is a need for privacy-preserving techniques that allow IoT devices to securely exchange data without revealing sensitive information. Techniques such as homomorphic encryption, zero-knowledge proofs, and differential privacy could be used to achieve this goal.
4. Energy Efficiency: One of the challenges of using blockchain and DLTs in IoT is energy consumption. Future research could focus on developing more energy-efficient consensus mechanisms and improving the scalability of blockchain networks, to reduce the energy requirements of IoT devices.
5. Integration with Edge Computing: The integration of blockchain and DLTs with edge computing could lead to new applications in IoT security. By processing and storing data at the edge of the network, it is possible to reduce latency, improve security, and increase the efficiency of IoT applications.

As the technology continues to mature, we can expect to see many more innovative applications of blockchain and DLTs in IoT security. By addressing the challenges and limitations, and focusing on these future directions, we can help to create a more secure, efficient, and interconnected IoT ecosystem[6].

6. CONCLUSION

Blockchain and distributed ledger technologies (DLTs) offer many potential benefits for IoT security. By providing a secure and decentralized platform for data storage, processing, and management, these technologies can help to improve the privacy, security, and efficiency of IoT applications. However, there are also several challenges and limitations to consider when using blockchain and DLTs in IoT, including scalability, interoperability, regulatory environment, security risks, and energy consumption. These challenges must be carefully addressed in order to create a trusted and secure IoT ecosystem. Looking to the future, there are many exciting opportunities for blockchain and DLTs in IoT security, including the development of interoperability standards, integration with AI and machine learning, privacy-preserving techniques, energy efficiency, and integration with edge computing. As the technology continues to evolve, it is important to stay abreast of these developments and to carefully evaluate the potential benefits and challenges of using blockchain and DLTs in IoT security.

Conflict of interest

None.

Acknowledgments

The author is grateful to the institution for their collaboration and provision of necessary facilities that contributed to the successful completion of this research.

Funding

The author's paper explicitly states that the research was self-funded and no support was received from any institution or sponsor.

References

[1] M. Crosby, P. Pattanayak, S. Verma, and V. J. A. I. Kalyanaraman, “Blockchain technology: Beyond bitcoin,” vol. 2, no. 6-10, pp. 71, 2016.

[2] A. Dorri, S. S. Kanhere, and R. J. a. p. a. Jurdak, “Blockchain in internet of things: challenges and solutions,” 2016.

[3] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, H. J. I. j. o. w. Wang, and g. services, “Blockchain challenges and opportunities: A survey,” vol. 14, no. 4, pp. 352-375, 2018.

[4] X. Lie, P. Jiang, T. Chen, L. Xiapu, and W. Qiaoyan, "A Survey on the Security of Blockchain Systems Future Generation Computer Systems," Elsevier, 2017.

[5] F. Tschorsch, B. J. I. C. S. Scheuermann, and Tutorials, “Bitcoin and beyond: A technical survey on decentralized digital currencies,” vol. 18, no. 3, pp. 2084-2123, 2016.

[6] M. Swan, *Blockchain: Blueprint for a new economy*: " O'Reilly Media, Inc.", 2015.