Blockchain for IoT Security and Privacy in Healthcare Sector

Umair Shafique, Hafiz Usman Zia, Fiaz Majeed, Samina Naz, Javeria Ahmed, Maleeha Zainab

***Abstract*—**The Internet of Things (IoT) has become a hot topic for the last couple of years. This innovative technology has shown promising progress in various areas and the world has witnessed exponential growth in multiple application domains. Researchers are working to investigate its aptitudes to get the best from it by harnessing its true potential. But at the same time, IoT networks open up a new aspect of vulnerability and physical threats to data integrity, privacy, and confidentiality. It is due to centralized control, data silos approach for handling information, and a lack of standardization in the IoT networks. As we know, blockchain is a new technology that involves creating secure distributed ledgers to store and communicate data. Some of the benefits include resiliency, integrity, anonymity, decentralization, and autonomous control. The potential for blockchain technology to provide the key to managing and controlling IoT has created a new wave of excitement around the idea of putting that data back into the hands of the end-users. In this manuscript, we have proposed a model that combines blockchain and IoT networks to address potential security and privacy issues in the healthcare domain and how various stakeholders will interact with the system.

***Keywords*—**Internet of Things, IoT, blockchain, data integrity, authentication, data privacy.

I. Introduction

THE IoT has become the topic of much discussion and speculation recently. IoT is a vision of a world in which every product, device, and thing contains electronics, software, sensors, and network connectivity to allow them to share information with the cloud. However, many of these products will need to store large amounts of data, and that data could be sensitive. A huge amount of technology companies is now focusing on IoT to help create the next great leaps in our society. It is about how we can take what we know, connect it to things we already use, and start building new products and solutions [1]. Devices can sense and interact with their environments and with other connected devices in real-time. This poses challenges for trust and security in the IoT realm [2], [3].

Blockchain is also a relatively new technology, with the introduction of Bitcoins by Satoshi Nakamoto [4]. The real power of blockchain is in its ability to track and record the ownership of information on a distributed ledger that is stored securely on thousands of computers instead of one. Along with cryptocurrency, over the last few years blockchain expanded rapidly in various domains e.g., governance, healthcare, education, identity management, IoT networks, and so on.

As the IoT continues to evolve, the number of connected devices is growing rapidly. This leads to massive amounts of data that must be stored, analyzed, and shared. Keeping this in mind, researchers, scholars, and industry experts disrupt various IoT application and try to address prevailing IoT networks issues.

The idea behind the blockchain is that a decentralized system can be built to ensure trustless transactions and security in the IoT space. This means that the blockchain is an attractive technology for storing, securing, and transferring data in a decentralized environment.

A variety of blockchain projects are being developed for the IoT. These include Helium [6], IOTA [7], ITC [8], OriginTrail [9], etc. While there is some overlap in their intended areas of use, each project is focused on specific industry verticals, such as manufacturing, finance, healthcare, retail, quality control, and regulation. With IoT, we are dealing with a wide variety of use cases ranging from those in the "Smart Cities" category to wearables, healthcare, supply chain management, and many more. In addition, these use cases have different requirements.

It is often challenging to identify the right blockchain technology to meet a certain IoT device’s requirements. To the best of our knowledge, there are few evaluations available that can help choose the right BC technology for a given IoT network.

The healthcare industry is huge and it has been growing at a tremendous pace over the last few years. This paper looks at the challenges of the current healthcare infrastructure and how blockchain-enabled IoT networks can revolutionize said infrastructure. The sector includes providers, payers, patients, vendors, manufacturers, researchers, and so on. Some of these different healthcare players perform very different roles within the system.

This work focuses on highlighting the characteristics of IoT-enabled Blockchain applications in healthcare and who will benefit from such a solution.

II. Background

IoT and BC are two disruptive technologies that enable a lot of things that were not possible before. However, to realize the potential of these two technologies working together, it is important to understand their background first. In this section, we briefly describe the characteristics of IoT, major security risks to IoT infrastructure, blockchain, its applications, and the convergence of IoT and BC.

Umair Shafique, Hafiz Usman Zia, Fiaz Majeed, Samina Naz, Javeria Ahmed, and Maleeha Zainab are with the University of Gujrat, Gujrat, 50700, Pakistan (e-mail: umairg92@gmail.com, usman.zia@uog.edu.pk, fiaz.majeed@uog.edu.pk, samina.naz@uog.edu.pk).

A. Internet of Things

The IoT is an interdisciplinary term that refers to the network of connected objects that can be discovered using standard communication protocols. Things in a network can be devices or objects, including computers, machines, vehicles, appliances, and other devices, which allow them to communicate over a network and interact with each other.

The IoT technology can be categorized into three main types: internet-oriented, which provides middleware for information exchanges between the physical devices; things-oriented, which provides sensing ability and semantic-oriented, which can link these devices to provide context about a situation. This makes it important to understand how each type works to apply them effectively for the intended purpose [10].

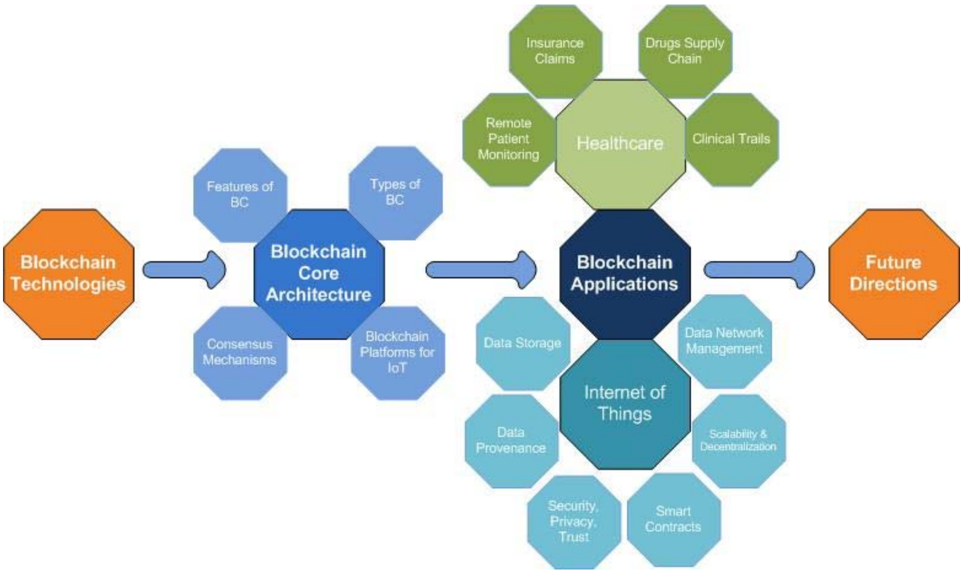

Fig. 1 Overall Blockchain and IoT Architecture with Applications in the Healthcare Sector

B. Major Security Risks in IoT Networks

With the increasing pace of development of the IoT, the security of IoT networks has become one of the most prominent areas. However, the security of IoT does not adapt well to the structured approach. Current security technologies and measures cannot meet the standards and their vulnerabilities are growing due to connectivity with the internet [11], [12].

1) Risks of Data Gathering

The entire IoT is a complex system comprised of many different devices that must work together. Because of this complexity, the entire system needs to be regularly updated to ensure proper functionality. In the current IoT sensing control system, the heterogeneity in the sensing devices and the heterogeneity in the sensing control schemes present a challenge to the effectiveness of the control.

The increasing ease with which malicious code can be spread around the Internet has led to increased security risks. Furthermore, many computers are vulnerable because they run outdated software. Attackers will often find themselves in an advantageous position in terms of access to information or resources they desire [12].

2) Risks of Data Transmission

As the number of sensors on devices grows, the complexity of device protection increases. However, this complexity is usually not put in place as an intentional deterrent. Instead, it is a result of the sheer number of these sensors that make up today's technology. It is possible to attack the data as it is being transmitted [12], [13].

3) Risks of Tag Being Embedded

After collecting the necessary data, IoT devices can send their information directly to the cloud for processing. However, in some situations, this may be a very open process. For example, they could be tracked or intercepted by someone else. It is important to be careful about what information you collect and how you use it [13].

4) Risks of Data Storing

IoT devices are a large part of the Internet, and they collect a lot of data, but it is not always secure. They also keep a lot of information about you personally – passwords, personal preferences, etc. The information is often stored in an insecure and centralized location.

When you store data on a computer, you can lose it in many ways. It can happen through human error, hardware failure, power loss, and many other things. It is possible to lose all of the data on a hard drive and it would be pretty impossible to recover it.

5) Risks of Authentication and Access Control

Message identification and authentication are the most common authentication methods in IoT, used to verify that the origin of a message is from a valid source.

The intruder may use either an exhaustive or a surveillance method to obtain the message authentication code. Once he has obtained the correct message authentication code, the intruder can pretend to be the legitimate sender, and carry out the rest of the transaction.

6) Risks of IoT Infrastructure

Currently, the IoT system architecture is a centralized and supervised system. It is based on the assumption that only a trusted third party can securely provide the system with information about all connected devices. However, this approach fails to protect against the potential risks associated with compromised devices or malicious attackers. The resulting huge volume of data and the increased usage of the Internet make it a challenge for IoT operators and third-party companies alike [11].

C. Blockchain Technology

A blockchain is a record of all the transactions that have occurred on an account. As more people make a transaction, the chain grows and becomes longer. Every transaction has to be validated by the blockchain, so it is pretty secure. Once you have created your block, you want to let others verify it. That means you need a way to do this securely. This is what you have to do: create your block, find some way to verify it, and store it on a publicly accessible web server.

A blockchain combines a public ledger and a decentralized timestamping service to provide a distributed, tamper-proof way of recording events and protecting information. It can be used to create any number of applications including financial systems, voting, legal contracts, and record-keeping for many areas.

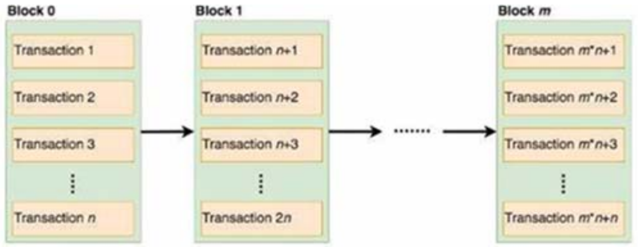

Fig. 2 Structure of Blockchain [5]

Blockchains are distributed databases that are used to store data across a network of computers. Decentralized applications (or DApps) are applications that run on these networks. Blockchain maintains information among the people who are involved in the network [11], [12].

D. Types of Blockchains

Blockchain can be used to verify the integrity of transactions, provide strong authentication, and provide trust without relying on a single trusted peer. Different blockchain implementations can represent different types of consensuses, but they all represent the idea of a distributed ledger [14].

TABLE I
COMPARISON BETWEEN TYPES OF BLOCKCHAINS AND IOT NETWORK

Properties	IoT	Public BCs	Private BCs	Hybrid BCs
Ownership (type of network)	Centralized	Decentralized (everyone in the network owns it)	Centralized	Combination of Public+Private
Resource Consumption	Resource restricted	Resource consuming Block mining is time-consuming	Less resource consuming	Less resource consuming
Access	Demands low latency	Open Read/Write	Permissioned read/write	Open+Permissioned
Membership (Who can Participate)	Authentic and Authorized access	Open/Transparent	Private	Open+Private
Consensus Mechanism	Private	Proof-of-Work, Proof-of-Stake, and other Consensus Mechanisms	Voting or multi-party	Voting or Multi-party
Speed of Consensus	---	Slow	Faster	Slightly Faster
Node Identity	---	Anonymous	Known identities	Identified
Immutability (ability to remain unchanged)	Known identities	Collusion attacks are possible by either a 51% attack or using quantum computing	Collusion attacks possible	Collusion attacks possible
Anonymity (privacy of one's data)	Attacks possible	Malicious as Anyone Can Participate in the Network	Trusted	Trusted

There are three types of blockchains currently classified in literature. The first is public, where transactions are made public. The second is private, where only authorized participants have access to the network. The third is hybrid, which combines public and private in one ledger [15].

1) Public Blockchain

The blockchain is a decentralized database of transactions (ledger). It is considered to be a distributed ledger as it is a shared ledger. Such a type of blockchain allows users to run their own rules on the data stored on the system. This could be used to limit access to certain data, for example. The fact that blockchain is a decentralized system means it is very difficult to tamper with data.

2) Private Blockchain

This is in contrast to a public blockchain, in which anyone can participate. Such types of blockchains are often mentioned as permissioned in which only certain participants or validators are allowed to participate.

3) Hybrid Blockchain

A hybrid blockchain is a combination of public and private blockchains. Private blockchains provide secure storage of sensitive data, and they offer a way to distribute such data securely to other parties. In return, a user of a hybrid blockchain can access their data without having to expose it to the general public. The security of hybrid blockchains makes them ideal for sensitive information and data sharing.

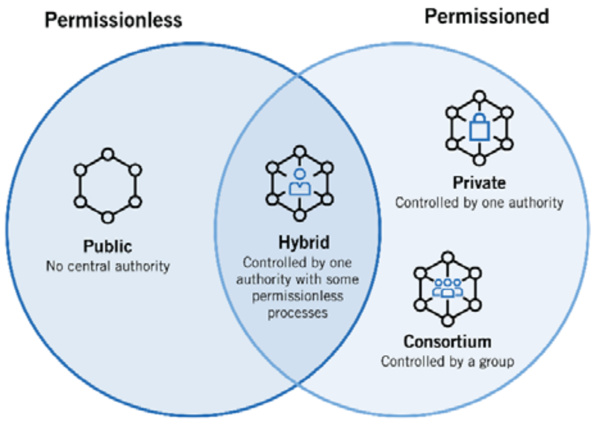

Fig. 3 Types of Blockchain

E. Blockchain Consensus Mechanism

The consensus process is a decentralized way of getting agreement on information or data among a group of networked devices. The process allows the network to make changes to its shared state in a consistent and ordered fashion. Blockchains employ various consensus protocols to ensure that transactions reach the same state after a particular period. These consensus algorithms include Proof of Work (PoW), Proof of Stake (PoS) [16], Proof of Elapsed Time (PoET), and Proof of Burn (PoB) [17].

III. Integration of Blockchain with IoT

The integration of blockchain into IoT is not new, but its broad application has opened up a relatively new field of research and development in the IoT domain. While the use of distributed ledgers can make data sharing more secure, more flexible, and more efficient, it can also be costly.

TABLE II
Review of Blockchain Based IoT Solution

Ref.	Domain	Contribution	Issues
[18]	Blockchain for IoT	Blockchain review Identify BIoT applications Design of an optimized BIoT	Resource scarcity of IoT devices Critical analysis of scalability, security & privacy issues of BIoT Critical analysis of legal and consensus Issues of BIoT
[19]	Blockchain and IoT Integration	Identify BIoT application areas Propose device manipulation and data management	Computational and power cost Identification of issues and Solutions in ensuring Security, privacy, scalability, and consensus in BIoT Futuristic demand for smart contracts in BIoT
[20]	BIoT Integration	Possible integration mechanism and platforms	Storage Regulatory issues in BIoT Analysis of IoT constraints in implementing smart contracts

IV. Blockchain-Enabled IoT in Healthcare Sector

IoT technology is evolving as a way to help connect more things, and BC technology is evolving as a way to help make sense of all of the information that is collected from the things connected to the network.

Fig. 4 depicts the overall structure of the general framework for IoT and Blockchain integration in the healthcare sector. It is three-layer architecture to organize the processes needed for integrating different applications. These layers provide a standard interface between the IoT devices and the blockchain services. This includes not only the interface between the device and the blockchain but also the interface between the users and the services. Users are given a set of roles based on which they get services.

A. Application Layer

This layer is what connects the world of the IoT and the blockchain. It is the communication protocol that is responsible for transmitting data from one network to another. The legitimate IoT devices and other users will be able to access the system services, including database storage and services, such as authentication. They will be given a set of roles based on which they get these services. The use of cryptocurrency and IoT in conjunction with DApps browsers such as Metamask [21] creates a potential new platform for security and protection of users' sensitive data.

B. Business Layer

It acts as an abstraction layer between IoT and blockchain. Functions that are specific to the IoT are coded here as per the application requirements and used when needed. This is the layer where services, including smart contracts, user validations, and access control reside. This layer is the core of the framework and contains all of the logic to run applications.

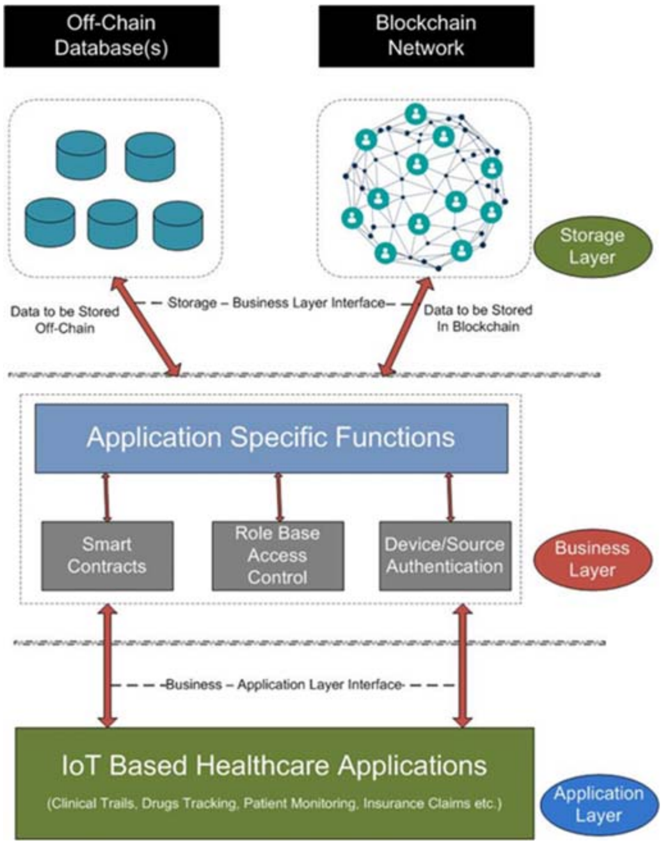
Off-Chain Database(s)
Blockchain Network
Storage Layer
Data to be Stored Off-Chain
Storage – Business Layer Interface
Data to be Stored In Blockchain
Application Specific Functions
Smart Contracts
Role Base Access Control
Device/Source Authentication
Business Layer
Business – Application Layer Interface
IoT Based Healthcare Applications
(Clinical Trails, Drugs Tracking, Patient Monitoring, Insurance Claims etc.)
Application Layer

Fig. 4 General Framework for IoT and Blockchain Integration in Healthcare Sector

C. Storage Layer

Data privacy is one of the big issues with storing data in a network. To address this issue, data stored in the blockchain are encrypted [21]. However, the data you encrypt can include information you need to validate the integrity of data with a timestamp. On-chain data storage is when you store data on the blockchain itself. Sensitive data are stored in a private database, this is called off-chain storage, and the blockchain keeps the information about the integrity of data along with a timestamp. So, blockchain data can be immutable as well as verifiable [22].

V. System Evaluation

In this section, we look at the potential of our proposed framework for healthcare. Permissioned blockchains are the ones where only known nodes are allowed into the network which are given developed using the features mentioned in the proposed framework. Permissioned blockchain networks use a set of trusted nodes to confirm transactions. These nodes will need to be approved before they can participate in the network.

Below are the details about a few nodes:

A. IoT Device

Sensors will take care of the first phase of data collection, and they can communicate directly with other devices on the same network. Data can then be framed for storage purposes, communicated, and saved onto the blockchain network. Immutable records in the blockchain are used to store every interaction so that they can never be deleted or altered.

When it comes to keeping our information secure, we tend to think about the security of our computers, and sometimes overlook some of the other devices that may hold sensitive data. For instance, an internet-connected camera or a smartphone could contain information that you want to keep private.

B. Off-Chain Database:

It is an unalterable database that is stored on a secure server, where its contents are controlled and stored for privacy and security reasons. That way, a database of patient data can be private to your network while still being secure against hacking attacks.

Optionally, we can hash our data before it is stored in the database.

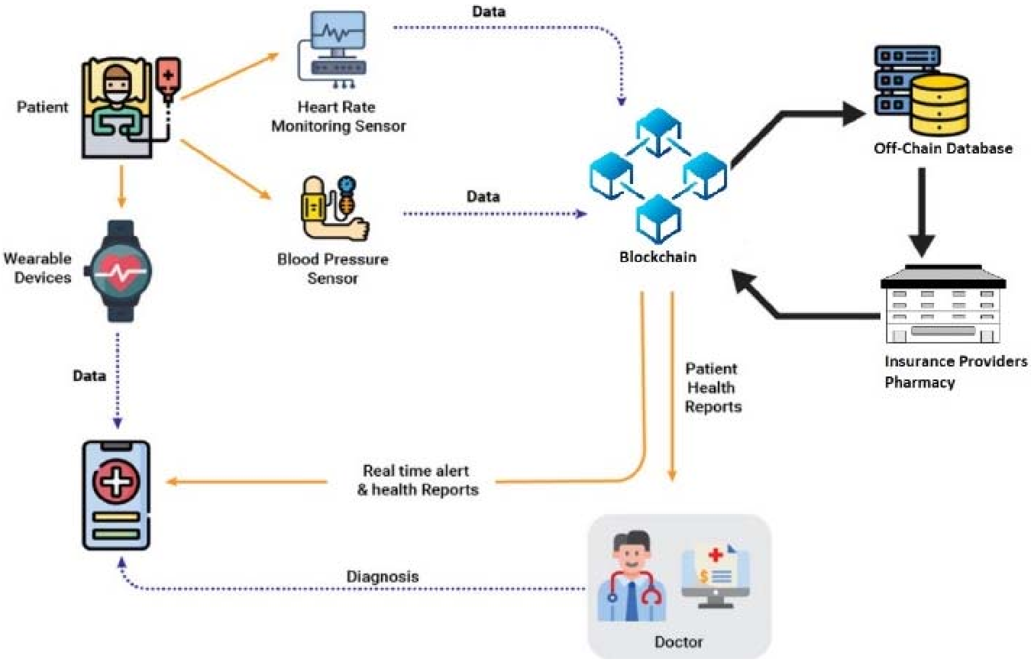

Fig. 5 System Evaluation

C. Doctor

Using a blockchain DApp, doctors can view patient health data remotely and check whether their prescriptions are effective. As long as they use the app and keep their data secure, only they and the patients know who is looking at their data.

D. Pharmacy

The pharmacist, using a blockchain-based platform, can access medical prescriptions for a specific patient. The pharmacist can also access the patient's location to ensure that the correct medications are delivered.

E. Patient

The patient is the most important entity in healthcare. Patients are indeed the biggest consumer of healthcare services. Although patients' record is permanently stored in the blockchain, they can access them at any type provided the credentials and but they do not have the right to alter their medical history.

F. Insurance Company

In the healthcare sector, insurers are often a critical part of a healthcare delivery system, including hospitals, doctors, and medical clinics. The insurance company is another important part of this system and can access the services using a DApp. After the claim is being made by the patient, the company can verify the patient's record on the blockchain as it has the authority to do so.

VI. Conclusion

This paper has provided a set of important lessons to take away from blockchain technology. We have also identified the important points that blockchain can add to IoT, but not every idea is suitable for every application. As a future direction, it would be interesting to see this framework tested in an experimental setting. This would provide better information on how effective the system is as a whole. The BIoT applications can solve scalability and security issues in the future. By integrating IoT with blockchain we leverage unique benefits such as immutable record keeping, traceability, trust, transparency, etc.

References

[1] Mendez Mena, D., Papapanagiotou, I., & Yang, B. “Internet of things: Survey on security”. Information Security Journal: A Global Perspective, 27(3), 162–182. 2018.

[2] Susanto et al, “The trend malware source of IoT network”. Indonesian Journal of Electrical Engineering and Computer Science, Vol. 22, No. 1, pp. 450~459, April 2021

[3] Mamoona H et al, “Internet of things and ransomware: Evolution, mitigation and prevention”, Egyptian Informatics Journal, pp. 105-117, 2021

[4] Satoshi, N., Bitcoin: A peer-to-peer electronic cash system. 2008. URL http://bitcoin.org/bitcoin.pdf (accessed 20 Feb 2022)

[5] H. F. Atlam, "Blockchain with the Internet of Things: Benefits, Challenges, and Future Directions," I.J. Intelligent Systems and Applications, published online, vol. 6, pp. 4048, 2018.

[6] Amir Haleem et al. White Paper, “Helium” 2018 http://whitepaper.helium.com/ (accessed 24 Feb 2022)

[7] Harbor, C. Iota Data Marketplace. 2018 https://data.iota.org/ (accessed 25 Feb 2022)

[8] IoT Chain White Paper, “IoT Chain, A High-Security Lite IoT OS”, https://iotchain.io/pdf/ITCWHITEPAPER.pdf (accessed 25 Feb 2022)

[9] OriginalTrail White Paper. https://origintrail.io/storage/documents/OriginTrail-White-Paper.pdf (accessed 25 Feb 2022)

[10] Rachit et al, “Security trends in Internet of Things: a survey” SN Applied Sciences, 3:121, 2021

[11] B. K. Mohanta, D. Jena, S. Ramasubbareddy, M. Daneshmand, and A. H. Gandomi, “Addressing security and privacy issues of IoT using blockchain technology,” IEEE Internet Things J., vol. 8, no. 2, pp. 881–888, Jan. 2021.

[12] B. K. Mohanta, D. Jena, U. Satapathy, and S. Patnaik, “Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology,” Internet Things, vol. 11, Art. no. 100227, Sep. 2020

[13] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, “A survey on IoT security: Application areas, security threats, and solution architectures,” IEEE Access, vol. 7, pp. 82721–82743, 2019.

[14] Lao L, Li Z, Hou S, Xiao B, Guo S, Yang Y. A survey of IoT applications in Blockchain systems: architecture, consensus and traffic modeling. Assoc Comput Mach. 2019;1(1):32.

[15] Zhang R, Xue R, Liu L. Security and privacy on the blockchain. ACM Comput Surv. 2019;52(3):1-34

[16] A. Kiayias, A. Russell, B. David, and R. Oliynykov, ‘‘Ouroboros: A provably secure proof-of-stake blockchain protocol,’’ in Proc. Annu. Int. Cryptol. Conf. Santa Barbara, CA, USA: Springer, 2017, pp. 357–388

[17] Dwivedi, Ashutosh Dhar, Gautam Srivastava, Shalini Dhar, and Rajani Singh. “A decentralized privacy-preserving healthcare blockchain for iot.” Sensors 19, no. 2 (2019): 326

[18] T. M. Fernández-Caramés and P. Fraga-Lamas, ‘‘A review on the use of blockchain for the Internet of Things,’’ IEEE Access, vol. 6, pp. 32979–33001, 2018

[19] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, ‘‘Blockchain and IoT integration: A systematic survey,’’ Sensors, vol. 18, no. 8, p. 2575, 2018

[20] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, ‘‘On blockchain and its integration with IoT. Challenges and opportunities,’’ Future Gener. Comput. Syst., vol. 8, pp. 173–190, Nov. 2018.

[21] Metamask - Brings Ethereum to your browser. Available online: https://metamask.io/ (accessed on 11 March 2022)

[22] Kosba, A.; Miller, A.; Shi, E.; Wen, Z.; Papamanthou, C. Hawk: the blockchain model of cryptography and privacy-preserving smart contracts. In Proceedings of the 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 22–26 May 2016; pp. 839–858.