**Secure and Efficient Blockchain-Based Data Sharing** **Framework for Internet of Things (IoT) Networks**

**Vikas Mahandule1, Harsha Patil2, Pranjal Tiwari3, Vivek Vishwakarma4**

*1HOD & Assistant Professor, Department of Computer Application, MIT Arts Commerce and Science College Alandi*

*1Assistant Professor Department of Computer Application, MIT Arts* *Commerce and Science College Alandi*

*3,4Students of Department of Computer Application, MIT Arts Commerce and Science College Alandi*

# Abstract

The Internet of Things (IoT) has become a pervasive technology with various applications ranging from smart homes and cities to industrial automation and healthcare. However, the increasing adoption of IoT devices has also raised significant concerns about cybersecurity and privacy. Blockchain, as a distributed and immutable ledger technology, has been proposed as a potential solution to enhance the security and privacy of IoT systems. Blockchain-based IoT systems offer several benefits, such as decentralization, transparency, and data integrity. However, they also pose unique cybersecurity challenges that need to be addressed for their secure and reliable deployment. In this paper, we review the existing literature and highlight the key challenges in cybersecurity for blockchain-based IoT systems. We categorize these challenges into three main areas: (i) IoT device security, (ii) blockchain security, and (iii) integration of IoT devices with blockchain (network security). Through an in-depth analysis, we present the current state of research and discuss potential solutions for each challenge. Additionally, we contribute by identifying future research directions to address these challenges and enhance the cybersecurity of blockchain-based IoT systems.

**Keywords:** Cyber security, [Internet of Things](https://www.mdpi.com/search?q=Internet+of+Things+(IoT)) (IoT), [Block chain](https://www.mdpi.com/search?q=blockchain),Security, [privacy’s](https://www.mdpi.com/search?q=privacy)

# Introduction

IoT devices usually have limited resources, including limited power consumption and storage capacity, and therefore have security implications such as inaccessibility, data leaks, tampering, and malware attacks [5,6]. In addition, the basic design of many IoT systems has a failure mechanism that makes them vulnerable to risk [7].

Blockchain technology was proposed by Satoshi Nakamoto in 2008. Based on Bitcoin technology, it has become a solution that increases the security and privacy of IoT systems [5]. Blockchain is a type of business system that makes data verifiable, transparent, and secure [3]. Blockchain techniques can be used to secure the devices integrity and security. It reduces the probability of data hacking. The term **Blockchain** means every piece of data (block) is connected with each other like a chain.

The blockchain offers enhanced security by using various methods where mostly the focus is to safe and secure the data from being hacked by various techniques like decentralization,transparency…. etc. These various methods enhances the speed and make the process faster as they remove third parties.

Blockchain techniques are useful not only in the cryptocurrencies but also in various other field’s like healthcare,Supply Chain management and Smart Contracts.

Let’s discuss those techniques in detail:

**Decentralization:**It is technique where system is not controlled by any single authority or server but every piece of data(*block)* it is connected with different nodes.The data is scattered into various nodes rather than keeping it at one place.This method helps to tackle from the theft and malware attacks .When hackers want to enter into any datasets and if we used decentralization technique it will me mostly complex for them to trace the data as it is scattered.

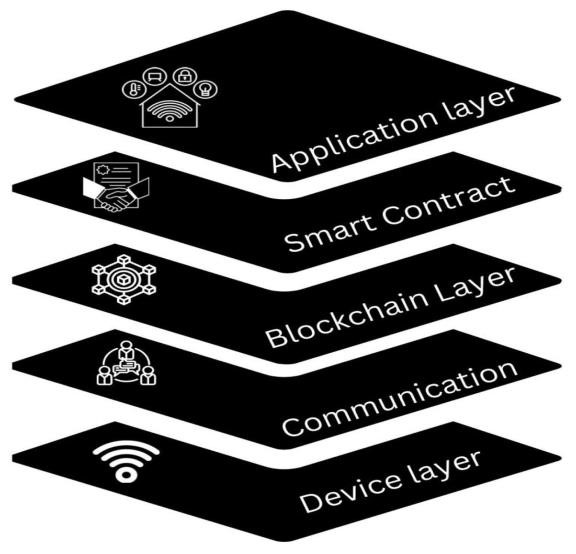
In context of IOT devices it is most important as multiple devices are connected and data is shared among them. This gives the feature for IOT devices to ensure and secure there data by scattering the data nodes. Decentralization method is transparent and fair because it is not controlled by single entity or person.

**Transparency:**The word transparency means every transaction is visible to everyone on the network which creates a sense of fairness. Each and every action is recorded and verified by each nodes and data is shared with very high security and care. This method is useful when someone tries to commit fraud or change data then the system notifies immediately.

For IOT,systems many devices constantly send and receive data and this verification features ensures the safety and security for all the various networks of IOT devices.

**Cryptographic techniques:**It is a method of securing data by converting it into a code i.e Encryption. By converting into code and only get decoded by authorized user gives more security and safety to IOT devices.

**Smart Contracts:**This is the feature where multiple IOT devices are controlled by single devices. We can control various devices from one central device also can monitor our each devices and there functionality.



**Fig 1- Layers of Blockchain**

Blockchain technologies and techniques ensures that data sharing should be safe secure and kept confidential. For achieving these all we need to understand some of the important features that each layers provide for this.

Fig 1 describes the image of different layers.We will look to the different layers and their role in protecting the transactions and the ways security is maintained:

**Device Layer:** The bundle of all the physical components that are used in IoT devices to collect data from their environment and sending that to blockchain networks. Some of the devices are Sensors, actuators and embedded system. They have different functions like Sensors are devices to collect data from environment and acuators are used to perform needed functions over that data. Whereas embedded systems are small computers that ensures that data is accurate , secure and accessible.

**Communication Layer:**This layer is vital for the establishment of connection between IoT devices and blockchain network. It consist of all the important technologies and protocols. It acts like a middleman who make the communication easy between the devices. If the communication is not established then it is crucial for data transfer. This layer also connects the network architecture which provides reliable and very smooth data transfer , processing.

**Blockchain Layer:**This layer is the core component that uses a distributed ledger technology. It is used for the verification and recording of transactions made by IoT devices. When a transaction occurs its checks the validity and authorization before completion. When a transaction request occur, such as sensor sending data to the blockchain, it is logged and confirmed through a process called **consensus**.

**Smart Contract Layers:** They are defined as the digital agreements that automatically execute actions when specific criteria are met. Smart Layers consist of some IoT devices that automatically works over Sensor. For example :Temperature Controlling devices adjust the temperature automatically with the climate.

**Literature Review:**

We present a thorough summary of the important research findings and ideas on blockchain security in Internet of Things systems in this part. blockchain technology in protecting IoT networks and devices. We also emphasise the main conclusions, such as how to design blockchain-based IoT systems with efficient and safe architectures, algorithms, and protocols, and how to assess performance indicators like trust, scalability, and privacy.

The advantages and disadvantages of integrating blockchain technology with the Internet of Things (IoT) were examined by Dorri et al. [1]. The writers began by outlining the idea of the Internet of Things and its possible uses in a number of sectors. The advantages of incorporating blockchain technology into the Internet of Things, including improved security, privacy, and transparency, were then covered. Still,I. The study addresses the vulnerability of blockchain systems to double-spending attacks as one of the main security problems. When a person spends the same cryptocurrency twice, it's known as a double spending assault and it erodes user confidence in the system. The authors covered a number of strategies, including the application of cryptographic and consensus processes, that can be utilised to reduce these risks. The possibility of 51 percent attacks is one of the paper's other major security challenges. When an attacker controls 51% of the processing power in a blockchain network, they can manipulate the system to their advantage. This is known as a 51% attack.

The report also covered the risks and obstacles of using smart contracts in blockchain systems. Smart contracts are self-executing contracts that are programmed to run when particular circumstances are met. These contracts, however, are open to a variety of attacks, including denial-of-service attacks and code exploits. The authors covered a number of strategies for reducing these risks, including auditing and vulnerability-testing smart contracts. The writers emphasised the necessity of additional study and advancement in this field to guarantee the broad acceptance and efficiency of blockchain technology.

The report also included a full evaluation of existing security measures and proposed solutions to these difficulties, making it an invaluable resource for blockchain security researchers and practitioners.

Yli-Huumo et al. [25] offered a thorough analysis of the state of blockchain technology research at the moment. The authors carried out a thorough analysis of scholarly works on blockchain technology that were released between 2008 and 2015. Based on a number of factors, including the kind of blockchain technology, the application area, and the research methodology, they examined the publications. The essay gave a thorough history of blockchain technology's development, from its beginnings as the foundational technology of Bitcoin to its present applications across numerous industries. The writers also covered the essential

A picture of these technologies and their attributes can be shown in Figure 3. Scalability, interoperability, and regulatory compliance are only a few of the main issues and restrictions related to blockchain technology that were mentioned in the article. The writers also talked about possible paths for blockchain technology research in the future, like using AI and creating fresh consensus techniques..

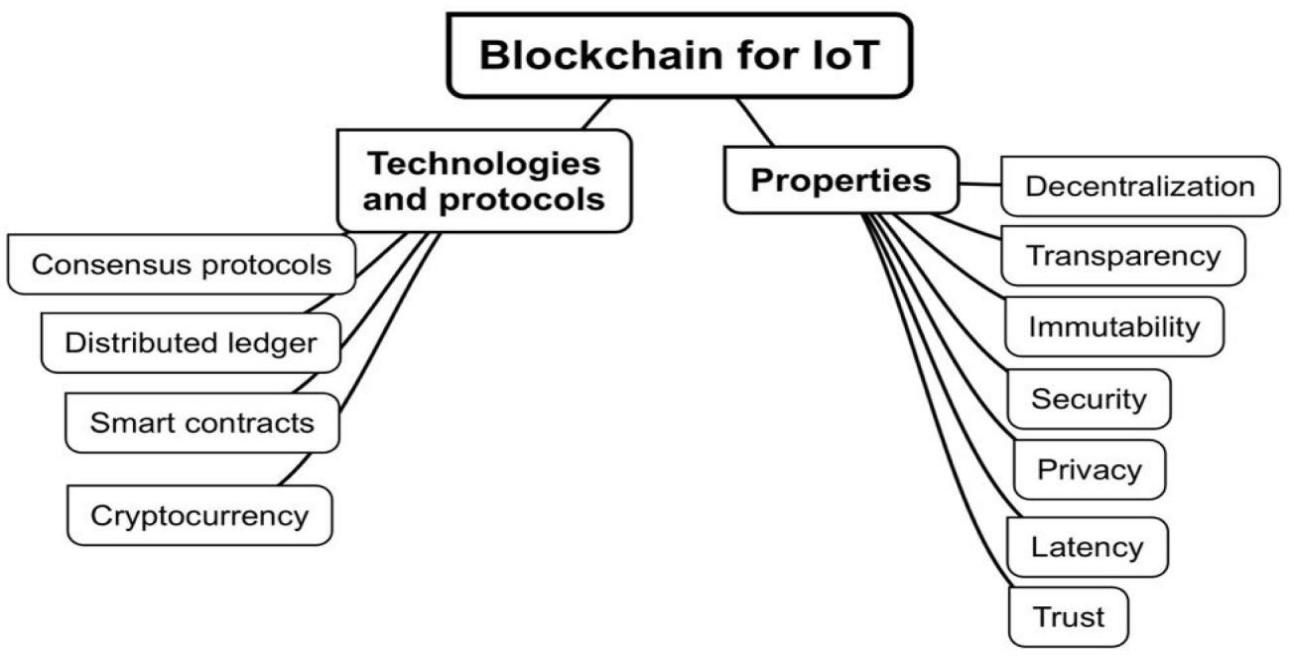


Figure 3 Technologies and Properties

# Research Methods

**Advanced Encryption Techniques**: The encryption means to convert text into code during data transfer to ensure data privacy and security. There are several techniques like **Ciphertext-Policy Attribute-Based Encryption(CP-ABE)**  and **Fully Homomorphic Encryption(FHE),** have been proposed to enhance security in IoT systems. These techniques are used to secure the data privacy and safety.

**Optimized Consensus Mechanisms**: IoT systems often face resource constraints so lightweight consensus algorithms like Delegated proof of Stake(DPOS) are suggested.This mechanism selects delegates to validate transactions,reducing computational costs and boosting transaction throughput.

**Hybrid Storage Solutions**:The combination of **Interplanetary File System(IPFS)**  and blockchain can provide a decentralized storage solution for IoT systems,improving data security and ensuring efficient data retrieval.

**Smart Contract Development**: Developing smart contracts for IoT networks can automate processes and improve system efficiency.Tools like **Ganache, Truffle,** and programming languages such as **Solidity** help in building applications and testing smart contracts.

**Blockchain and Edge Computing**: Combining blockchain with edge computing can reduce latency and bandwidth usage, creating a more scalable and efficient system for IoT devices.

**Privacy-Preserving Data Aggregation**: Techniques like **differential privacy**  and **Secure Multi-Party Computation(SMPC)** can aggregate data from various IoT devices while preserving individual data privacy.

**Performance Metrics and Evaluation**: Performance metrics such **transaction, latency,throughput** and **scalability** should be clearly defined to evaluate the effectiveness of blockchain-based IoT systems.Using real world IoT datasets for testing is essential.

**Challenges of Using Block chain for Securing IoT Networks**

The literature review uncovers significant findings regarding the cybersecurity of blockchain-integrated Internet of Things(IoT)systems.This section explores both the potential benefits and the challenges associated with applying blockchain technology for securing IoT networks.

## **4.1 IoT Device Security**

IoT devices are often resource-constrained and deployed in different environments , making them vulnerable to security threats. Key obstacles include:

**Authentication and Authorization:** Verifying IoT devices securely while using minimal resources is a challenge.

**Device Integrity and Firmware Updates:**Ensuring IoT devices integrityand secure firmware updates is crucial, but difficult due to their diverse and distributed nature.

**Secure Communication and Data Privacy:**IoT devices often lack encryption capabilities, leaving them vulnerable to data breaches.

4.1.1Device Authentication and Authorization

Ensuring that only authorized devices participate in a blockchain-powered IoT system is fundamental security requirement.However, due to the limited computing and storage capacities of IoT devices, conventional methods like usernames/passwords or cryptography keys may not be suitable for resource-constrained devices.

4.1.2 Device Integrity and Firmware Updates

Preserving the integrity of IoT devices and their firmware is critical in preventing unauthorized modifications that could compromise the security and privacy of the system.However, many IoT devices often lack the necessary tools to verify firmware integrity or detect and respond to tampering. Additionally, due to dispersed and diverse nature of IoT devices, updating their firmware can be a challenging task.

4.1.3 Secure Communication and Data Privacy

For IoT devices to effectively communicate and exchange data with the blockchain network and among themselves, secure communication channels and data privacy are essential. However ,many IoT devices may lack the necessary encryption software or transmit data in plain text, making then vulnerable to data breaches.

## **4.2. Blockchain Security**

Blockchain serves as the foundation technology that enables a decentralized and immutable ledger to record and verify transactions within blockchain based IoT systems.However, the use of blockchain introduce unique cybersecurity challenges that must be addressed to uphold system security and privacy.

***4.3. Network Security***

Effective operation of a blockchain-based IoT system relies heavily on the network connecting IoT devices to the Blockchain network.Primary concerns to related to network security in blockchain-based IoT systems .

**Conclusion**

We suggest the BBDSPP scheme as a solution to the problems with intricate communication procedures, limited adaptability, and inadequate security in conventional IIoT data sharing models. At first, we use the method to determine the values for the properties. This method makes it easier to implement an access control system for data sharing that permits any combination of permissions. Terminal members can freely choose the properties to decrypt. They can decrypt and access particular data as long as the attribute values match the predetermined access threshold. This guarantees strict control over data access in addition to the flexibility of data exchange. Furthermore, we pre-authenticate the identities of data accessors using non-interactive zero-knowledge proof procedures, which stops unauthorised members from pretending to be legitimate and stealing confidential information.

This prevents the additional computational load brought on by unauthorised access in addition to safeguarding the privacy of terminal users. By guaranteeing that data in the system can only be accessed by valid and authorised terminal members, it successfully stops unwanted access and the leakage of private data.

In addition, we store encrypted shared resources on the IPFS distributed storage system. Our solution to the storage efficiency problems in typical blockchain applications is to store a lot of data on IPFS and just save the corresponding storage addresses on the blockchain.

To conclude,

This preserves terminal user privacy while also preventing the extra computational burden caused by unauthorised access. It effectively prevents unauthorised access and the leakage of private data by ensuring that data in the system can only be accessible by legitimate and permitted terminal members.

Furthermore, we use the IPFS distributed storage system to store encrypted shared resources. We keep a great deal of data on IPFS and only save the corresponding storage addresses on the blockchain in order to address the storage efficiency issues that are common in blockchain applications.

# References

1. Dorri, A.; Kanhere, S.S.; Jurdak, R. Blockchain in Internet of Things: Challenges and solutions. *arXiv* 2016, arXiv:1608.05187. [[Google Scholar]](https://scholar.google.com/scholar_lookup?title=Blockchain+in+Internet+of+Things:+Challenges+and+solutions&author=Dorri,+A.&author=Kanhere,+S.S.&author=Jurdak,+R.&publication_year=2016&journal=arXiv)
2. 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. [[Google Scholar]](https://scholar.google.com/scholar_lookup?title=A+survey+on+the+security+of+blockchain+systems&author=Li,+X.&author=Jiang,+P.&author=Chen,+T.&author=Luo,+X.&author=Wen,+Q.&publication_year=2020&journal=Future+Gener.+Comput.+Syst.&volume=107&pages=841–853&doi=10.1016/j.future.2017.08.020) [[CrossRef]](https://doi.org/10.1016/j.future.2017.08.020) [[Green Version]](http://arxiv.org/pdf/1802.06993)
3. Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H. An overview of blockchain technology: Architecture, consensus, and future trends. In Proceedings of the IEEE international congress on big data (BigData Congress), Honolulu, HI, USA, 25–30 June 2017; pp. 557–564. [[Google Scholar]](https://scholar.google.com/scholar_lookup?title=An+overview+of+blockchain+technology:+Architecture,+consensus,+and+future+trends&conference=Proceedings+of+the+IEEE+international+congress+on+big+data+(BigData+Congress)&author=Zheng,+Z.&author=Xie,+S.&author=Dai,+H.&author=Chen,+X.&author=Wang,+H.&publication_year=2017&pages=557–564)
4. Panarello, A.; Tapas, N.; Merlino, G.; Longo, F.; Puliafito, A. Blockchain and IoT integration: A systematic survey. *Sensors* 2018, *18*, 2575. [[Google Scholar]](https://scholar.google.com/scholar_lookup?title=Blockchain+and+IoT+integration:+A+systematic+survey&author=Panarello,+A.&author=Tapas,+N.&author=Merlino,+G.&author=Longo,+F.&author=Puliafito,+A.&publication_year=2018&journal=Sensors&volume=18&pages=2575&doi=10.3390/s18082575) [[CrossRef]](https://doi.org/10.3390/s18082575) [[Green Version]](https://www.mdpi.com/1424-8220/18/8/2575/pdf)
5. Dorri, A.; Kanhere, S.S.; Jurdak, R.; Gauravaram, P. Blockchain for IoT security and privacy: The case study of a smart home. In Proceedings of the IEEE International Conference on Pervasive Computing and Communications

Workshops (PerCom Workshops), Kona, HI, USA, 13–17 March 2017; pp. 618– 623. [[Google Scholar]](https://scholar.google.com/scholar_lookup?title=Blockchain+for+IoT+security+and+privacy:+The+case+study+of+a+smart+home&conference=Proceedings+of+the+IEEE+International+Conference+on+Pervasive+Computing+and+Communications+Workshops+(PerCom+Workshops)&author=Dorri,+A.&author=Kanhere,+S.S.&author=Jurdak,+R.&author=Gauravaram,+P.&publication_year=2017&pages=618–623)

1. Islam, M.R.; Rahman, M.M.; Mahmud, M.; Rahman, M.A.; Mohamad, M.H.S. A review on blockchain security issues and challenges. In Proceedings of the

IEEE 12th Control and System Graduate Research Colloquium (ICSGRC), Shah Alam, Malaysia, 7 August 2021; pp. 227–232. [[Google Scholar]](https://scholar.google.com/scholar_lookup?title=A+review+on+blockchain+security+issues+and+challenges&conference=Proceedings+of+the+IEEE+12th+Control+and+System+Graduate+Research+Colloquium+(ICSGRC)&author=Islam,+M.R.&author=Rahman,+M.M.&author=Mahmud,+M.&author=Rahman,+M.A.&author=Mohamad,+M.H.S.&publication_year=2021&pages=227–232)

1. Raju, M.C.; Paul, K.S. A Comprehensive Review of Cyber Security in Blockchain-Based IoT. *Math. Stat. Eng. Appl.* 2022, *71*, 10646–10659. [[Google Scholar]](https://scholar.google.com/scholar_lookup?title=A+Comprehensive+Review+of+Cyber+Security+in+Blockchain-Based+IoT&author=Raju,+M.C.&author=Paul,+K.S.&publication_year=2022&journal=Math.+Stat.+Eng.+Appl.&volume=71&pages=10646–10659)
2. Mahmood, S.; Chadhar, M.; Firmin, S. Cybersecurity challenges in blockchain technology: A scoping review. *Hum. Behav. Emerg. Technol.* 2022, *2022*,

7384000. [[Google Scholar]](https://scholar.google.com/scholar_lookup?title=Cybersecurity+challenges+in+blockchain+technology:+A+scoping+review&author=Mahmood,+S.&author=Chadhar,+M.&author=Firmin,+S.&publication_year=2022&journal=Hum.+Behav.+Emerg.+Technol.&volume=2022&pages=7384000&doi=10.1155/2022/7384000) [[CrossRef]](https://doi.org/10.1155/2022/7384000)

1. Gubbi, J.; Buyya, R.; Marusic, S.; Palaniswami, M. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Gener. Comput. Syst.* 2013, *29*, 1645–1660. [[Google Scholar]](https://scholar.google.com/scholar_lookup?title=Internet+of+Things+(IoT):+A+vision,+architectural+elements,+and+future+directions&author=Gubbi,+J.&author=Buyya,+R.&author=Marusic,+S.&author=Palaniswami,+M.&publication_year=2013&journal=Future+Gener.+Comput.+Syst.&volume=29&pages=1645–1660&doi=10.1016/j.future.2013.01.010) [[CrossRef]](https://doi.org/10.1016/j.future.2013.01.010) [[Green Version]](http://arxiv.org/pdf/1207.0203)
2. Maple, C. Security and privacy in the internet of things. *J. Cyber Policy* 2017, *2*, 155–184. [[Google Scholar]](https://scholar.google.com/scholar_lookup?title=Security+and+privacy+in+the+internet+of+things&author=Maple,+C.&publication_year=2017&journal=J.+Cyber+Policy&volume=2&pages=155–184&doi=10.1080/23738871.2017.1366536) [[CrossRef]](https://doi.org/10.1080/23738871.2017.1366536) [[Green Version]](https://www.tandfonline.com/doi/pdf/10.1080/23738871.2017.1366536?needAccess=true)
3. Deep, S.; Zheng, X.; Jolfaei, A.; Yu, D.; Ostovari, P.; Kashif Bashir, A. A survey of security and privacy issues in the Internet of Things from the layered context. *Trans. Emerg. Telecommun. Technol.* 2022, *33*, e3935. [[Google Scholar]](https://scholar.google.com/scholar_lookup?title=A+survey+of+security+and+privacy+issues+in+the+Internet+of+Things+from+the+layered+context&author=Deep,+S.&author=Zheng,+X.&author=Jolfaei,+A.&author=Yu,+D.&author=Ostovari,+P.&author=Kashif+Bashir,+A.&publication_year=2022&journal=Trans.+Emerg.+Telecommun.+Technol.&volume=33&pages=e3935&doi=10.1002/ett.3935) [[CrossRef]](https://doi.org/10.1002/ett.3935) [[Green Version]](http://arxiv.org/pdf/1903.00846)
4. Qian, Y.; Jiang, Y.; Chen, J.; Zhang, Y.; Song, J.; Zhou, M.; Pustišek, M. Towards decentralized IoT security enhancement: A blockchain approach. *Comput. Electr. Eng.* 2018, *72*, 266–273. [[Google Scholar]](https://scholar.google.com/scholar_lookup?title=Towards+decentralized+IoT+security+enhancement:+A+blockchain+approach&author=Qian,+Y.&author=Jiang,+Y.&author=Chen,+J.&author=Zhang,+Y.&author=Song,+J.&author=Zhou,+M.&author=Pustišek,+M.&publication_year=2018&journal=Comput.+Electr.+Eng.&volume=72&pages=266–273&doi=10.1016/j.compeleceng.2018.08.021) [[CrossRef]](https://doi.org/10.1016/j.compeleceng.2018.08.021)
5. Moin, S.; Karim, A.; Safdar, Z.; Safdar, K.; Ahmed, E.; Imran, M. Securing IoTs in distributed blockchain: Analysis, requirements and open issues. *Future Gener. Comput. Syst.* 2019, *100*, 325–343. [[Google Scholar]](https://scholar.google.com/scholar_lookup?title=Securing+IoTs+in+distributed+blockchain:+Analysis,+requirements+and+open+issues&author=Moin,+S.&author=Karim,+A.&author=Safdar,+Z.&author=Safdar,+K.&author=Ahmed,+E.&author=Imran,+M.&publication_year=2019&journal=Future+Gener.+Comput.+Syst.&volume=100&pages=325–343&doi=10.1016/j.future.2019.05.023) [[CrossRef]](https://doi.org/10.1016/j.future.2019.05.023)
6. Khan, M.A.; Salah, K.; Imran, M. Blockchain-based secure and privacypreserving framework for smart healthcare systems. *IEEE Access* 2019, *7*, 116258–116273. [[Google Scholar]](https://scholar.google.com/scholar_lookup?title=Blockchain-based+secure+and+privacy-preserving+framework+for+smart+healthcare+systems&author=Khan,+M.A.&author=Salah,+K.&author=Imran,+M.&publication_year=2019&journal=IEEE+Access&volume=7&pages=116258–116273)
7. Joshi, A.P.; Han, M.; Wang, Y. A survey on security and privacy issues of blockchain technology. *Math. Found. Comput.* 2018, *1*, 121. [[Google Scholar]](https://scholar.google.com/scholar_lookup?title=A+survey+on+security+and+privacy+issues+of+blockchain+technology&author=Joshi,+A.P.&author=Han,+M.&author=Wang,+Y.&publication_year=2018&journal=Math.+Found.+Comput.&volume=1&pages=121&doi=10.3934/mfc.2018007) [[CrossRef]](https://doi.org/10.3934/mfc.2018007) [[Green Version]](https://www.aimsciences.org/article/exportPdf?id=d27803a2-7ce7-46e8-900d-30001fd4785a)
8. Deshmukh, A.; Sreenath, N.; Tyagi, A.K.; Abhichandan, U.V.E. Blockchain Enabled Cyber Security: A Comprehensive Survey. In Proceedings of the International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 25–27 January 2022; pp. 1–6. [[Google Scholar]](https://scholar.google.com/scholar_lookup?title=Blockchain+Enabled+Cyber+Security:+A+Comprehensive+Survey&conference=Proceedings+of+the+International+Conference+on+Computer+Communication+and+Informatics+(ICCCI)&author=Deshmukh,+A.&author=Sreenath,+N.&author=Tyagi,+A.K.&author=Abhichandan,+U.V.E.&publication_year=2022&pages=1–6)
9. Algarni, S.; Eassa, F.; Almarhabi, K.; Almalaise, A.; Albassam, E.; Alsubhi, K.; Yamin, M. Blockchain-based secured access control in an IoT system. *Appl.*

*Sci.* 2021, *11*, 1772. [[Google Scholar]](https://scholar.google.com/scholar_lookup?title=Blockchain-based+secured+access+control+in+an+IoT+system&author=Algarni,+S.&author=Eassa,+F.&author=Almarhabi,+K.&author=Almalaise,+A.&author=Albassam,+E.&author=Alsubhi,+K.&author=Yamin,+M.&publication_year=2021&journal=Appl.+Sci.&volume=11&pages=1772&doi=10.3390/app11041772) [[CrossRef]](https://doi.org/10.3390/app11041772)

1. Rajawat, A.S.; Rawat, R.; Barhanpurkar, K.; Shaw, R.N.; Ghosh, A. Blockchainbased model for expanding IoT device data security. In *Advances in Applications of Data-Driven Computing*; Springer: Singapore, 2021; pp. 61–71. [[Google Scholar]](https://scholar.google.com/scholar_lookup?title=Blockchain-based+model+for+expanding+IoT+device+data+security&author=Rajawat,+A.S.&author=Rawat,+R.&author=Barhanpurkar,+K.&author=Shaw,+R.N.&author=Ghosh,+A.&publication_year=2021&pages=61–71)
2. Haleem, A.; Javaid, M.; Singh, R.P.; Suman, R.; Rab, S. Blockchain technology applications in healthcare: An overview. *Int. J. Intell. Netw.* 2021, *2*, 130–139. [[Google Scholar]](https://scholar.google.com/scholar_lookup?title=Blockchain+technology+applications+in+healthcare:+An+overview&author=Haleem,+A.&author=Javaid,+M.&author=Singh,+R.P.&author=Suman,+R.&author=Rab,+S.&publication_year=2021&journal=Int.+J.+Intell.+Netw.&volume=2&pages=130–139&doi=10.1016/j.ijin.2021.09.005) [[CrossRef]](https://doi.org/10.1016/j.ijin.2021.09.005)
3. Page, M.J.; McKenzie, J.E.; Bossuyt, P.M.; Boutron, I.; Hoffmann, T.C.; Mulrow, C.D.; Shamseer, L.; Tetzlaff, J.M.; Akl, E.A.; Brennan, S.E.; et al. The PRISMA 2020 Statement: An Updated Guideline for Reporting Systematic Reviews. *Int. J. Surg.* 2021, *88*, 105906. [[Google Scholar]](https://scholar.google.com/scholar_lookup?title=The+PRISMA+2020+Statement:+An+Updated+Guideline+for+Reporting+Systematic+Reviews&author=Page,+M.J.&author=McKenzie,+J.E.&author=Bossuyt,+P.M.&author=Boutron,+I.&author=Hoffmann,+T.C.&author=Mulrow,+C.D.&author=Shamseer,+L.&author=Tetzlaff,+J.M.&author=Akl,+E.A.&author=Brennan,+S.E.&publication_year=2021&journal=Int.+J.+Surg.&volume=88&pages=105906&doi=10.1016/j.ijsu.2021.105906) [[CrossRef]](https://doi.org/10.1016/j.ijsu.2021.105906)
4. Le, T.V.; Hsu, C.L. A systematic literature review of blockchain technology: Security properties, applications and challenges. *J. Internet Technol.* 2021, *22*, 789–802. [[Google Scholar]](https://scholar.google.com/scholar_lookup?title=A+systematic+literature+review+of+blockchain+technology:+Security+properties,+applications+and+challenges&author=Le,+T.V.&author=Hsu,+C.L.&publication_year=2021&journal=J.+Internet+Technol.&volume=22&pages=789–802)
5. Al-Farsi, S.; Rathore, M.M.; Bakiras, S. Security of blockchain-based supply chain management systems: Challenges and opportunities. *Appl. Sci.* 2021, *11*, 5585. [[Google Scholar]](https://scholar.google.com/scholar_lookup?title=Security+of+blockchain-based+supply+chain+management+systems:+Challenges+and+opportunities&author=Al-Farsi,+S.&author=Rathore,+M.M.&author=Bakiras,+S.&publication_year=2021&journal=Appl.+Sci.&volume=11&pages=5585&doi=10.3390/app11125585) [[CrossRef]](https://doi.org/10.3390/app11125585)
6. Badri, S.; Ullah, J.S.; Alghazzawi, D.; Aldhaheri, S.; Pitropakis, N. BIoMT: A Blockchain-Enabled Healthcare Architecture for Information Security in the

Internet of Medical Things. *Comput. Syst. Sci. Eng.* 2023, *46*, 3667–3684. [[Google Scholar]](https://scholar.google.com/scholar_lookup?title=BIoMT:+A+Blockchain-Enabled+Healthcare+Architecture+for+Information+Security+in+the+Internet+of+Medical+Things&author=Badri,+S.&author=Ullah,+J.S.&author=Alghazzawi,+D.&author=Aldhaheri,+S.&author=Pitropakis,+N.&publication_year=2023&journal=Comput.+Syst.+Sci.+Eng.&volume=46&pages=3667–3684&doi=10.32604/csse.2023.037531) [[CrossRef]](https://doi.org/10.32604/csse.2023.037531)

1. Shafagh, H.; Burkhalter, L.; Hithnawi, A.; Duquennoy, S. Towards Blockchainbased Auditable Storage and Sharing of IoT Data. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, Dallas, TX, USA, 3 November 2017; pp. 45–50. [[Google Scholar]](https://scholar.google.com/scholar_lookup?title=Towards+Blockchain-based+Auditable+Storage+and+Sharing+of+IoT+Data&conference=Proceedings+of+the+2017+ACM+SIGSAC+Conference+on+Computer+and+Communications+Security&author=Shafagh,+H.&author=Burkhalter,+L.&author=Hithnawi,+A.&author=Duquennoy,+S.&publication_year=2017&pages=45–50)
2. Yli-Huumo, J.; Ko, D.; Choi, S.; Park, S.; Smolander, K. Where Is Current

Research on Blockchain Technology?—A Systematic Review. *PLoS ONE* 2016, *11*, e0163477. [[Google Scholar]](https://scholar.google.com/scholar_lookup?title=Where+Is+Current+Research+on+Blockchain+Technology?—A+Systematic+Review&author=Yli-Huumo,+J.&author=Ko,+D.&author=Choi,+S.&author=Park,+S.&author=Smolander,+K.&publication_year=2016&journal=PLoS+ONE&volume=11&pages=e0163477&doi=10.1371/journal.pone.0163477) [[CrossRef]](https://doi.org/10.1371/journal.pone.0163477) [[Green Version]](https://journals.plos.org/plosone/article/file?id=10.1371/journal.pone.0163477&type=printable)

1. Guo, H.; Yu, X. Survey on Blockchain Technology and Its Security. *J. Softw. Eng. Appl.* 2022, *3*, 100067. [[Google Scholar]](https://scholar.google.com/scholar_lookup?title=Survey+on+Blockchain+Technology+and+Its+Security&author=Guo,+H.&author=Yu,+X.&publication_year=2022&journal=J.+Softw.+Eng.+Appl.&volume=3&pages=100067&doi=10.1016/j.bcra.2022.100067) [[CrossRef]](https://doi.org/10.1016/j.bcra.2022.100067)
2. Lin, I.-C.; Liao, T.-C. A Survey of Blockchain Security Issues and Challenges. *Int. J. Netw. Secur. Its Appl.* 2018, *10*, 25–42. [[Google Scholar]](https://scholar.google.com/scholar_lookup?title=A+Survey+of+Blockchain+Security+Issues+and+Challenges&author=Lin,+I.-C.&author=Liao,+T.-C.&publication_year=2018&journal=Int.+J.+Netw.+Secur.+Its+Appl.&volume=10&pages=25–42)
3. Wylde, V.; Rawindaran, N.; Lawrence, J.; Balasubramanian, R.; Prakash, E.; Jayal, A.; Platts, J. Cybersecurity, Data Privacy and Blockchain: A Review. *Comput. Sci.* 2022, *3*, 127. [[Google Scholar]](https://scholar.google.com/scholar_lookup?title=Cybersecurity,+Data+Privacy+and+Blockchain:+A+Review&author=Wylde,+V.&author=Rawindaran,+N.&author=Lawrence,+J.&author=Balasubramanian,+R.&author=Prakash,+E.&author=Jayal,+A.&author=Platts,+J.&publication_year=2022&journal=Comput.+Sci.&volume=3&pages=127&doi=10.1007/s42979-022-01020-4&pmid=35036930) [[CrossRef]](https://doi.org/10.1007/s42979-022-01020-4) [[PubMed]](http://www.ncbi.nlm.nih.gov/pubmed/35036930)
4. Xu, X.; Weber, I.; Staples, M.; Zhu, L.; Bosch, J.; Bass, L.; Rimba, P. A Taxonomy of Blockchain-Based Systems for Architecture Design. In Proceedings of the 1st IEEE International Conference on Software Architecture (ICSA), Gothenburg, Sweden, 3–7 April 2017; pp. 243–252. [[Google Scholar]](https://scholar.google.com/scholar_lookup?title=A+Taxonomy+of+Blockchain-Based+Systems+for+Architecture+Design&conference=Proceedings+of+the+1st+IEEE+International+Conference+on+Software+Architecture+(ICSA)&author=Xu,+X.&author=Weber,+I.&author=Staples,+M.&author=Zhu,+L.&author=Bosch,+J.&author=Bass,+L.&author=Rimba,+P.&publication_year=2017&pages=243–252)
5. Zou, Y.; Meng, T.; Zhang, P.; Zhang, W.; Li, H. Focus on Blockchain: A

Comprehensive Survey on Academic and Application. *J. Syst. Sci. Inf.* 2018, *6*, 238–268. [[Google Scholar]](https://scholar.google.com/scholar_lookup?title=Focus+on+Blockchain:+A+Comprehensive+Survey+on+Academic+and+Application&author=Zou,+Y.&author=Meng,+T.&author=Zhang,+P.&author=Zhang,+W.&author=Li,+H.&publication_year=2018&journal=J.+Syst.+Sci.+Inf.&volume=6&pages=238–268&doi=10.1109/ACCESS.2020.3030491) [[CrossRef]](https://doi.org/10.1109/ACCESS.2020.3030491)

1. 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. [[Google Scholar]](https://scholar.google.com/scholar_lookup?title=A+systematic+literature+review+of+blockchain-based+applications:+Current+status,+classification+and+open+issues&author=Casino,+F.&author=Dasaklis,+T.K.&author=Patsakis,+C.&publication_year=2019&journal=Telemat.+Inform.&volume=36&pages=55–81&doi=10.1016/j.tele.2018.11.006) [[CrossRef]](https://doi.org/10.1016/j.tele.2018.11.006)
2. Conoscenti, M.; Vetro, A.; De Martin, J.C. Blockchain for the Internet of Things: A systematic literature review. In Proceedings of the IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), Agadir, Morocco, 29 November–2 December 2016; pp. 1–6. [[Google Scholar]](https://scholar.google.com/scholar_lookup?title=Blockchain+for+the+Internet+of+Things:+A+systematic+literature+review&conference=Proceedings+of+the+IEEE/ACS+13th+International+Conference+of+Computer+Systems+and+Applications+(AICCSA)&author=Conoscenti,+M.&author=Vetro,+A.&author=De+Martin,+J.C.&publication_year=2016&pages=1–6)
3. Kumar, N.M.; Mallick, P.K. Blockchain technology for security issues and challenges in IoT. *Procedia Comput. Sci.* 2018, *132*, 1815–1823. [[Google Scholar]](https://scholar.google.com/scholar_lookup?title=Blockchain+technology+for+security+issues+and+challenges+in+IoT&author=Kumar,+N.M.&author=Mallick,+P.K.&publication_year=2018&journal=Procedia+Comput.+Sci.&volume=132&pages=1815–1823&doi=10.1016/j.procs.2018.05.140) [[CrossRef]](https://doi.org/10.1016/j.procs.2018.05.140)
4. Alam, T. Blockchain-Based Internet of Things: Review, Current Trends, Applications, and Future Challenges. *Computers* 2022, *12*, 6. [[Google Scholar]](https://scholar.google.com/scholar_lookup?title=Blockchain-Based+Internet+of+Things:+Review,+Current+Trends,+Applications,+and+Future+Challenges&author=Alam,+T.&publication_year=2022&journal=Computers&volume=12&pages=6&doi=10.3390/computers12010006) [[CrossRef]](https://doi.org/10.3390/computers12010006)
5. Khan, M.A.; Salah, K. IoT security: Review, blockchain solutions, and open challenges. *Future Gener. Comput. Syst.* 2018, *82*, 395–411. [[Google Scholar]](https://scholar.google.com/scholar_lookup?title=IoT+security:+Review,+blockchain+solutions,+and+open+challenges&author=Khan,+M.A.&author=Salah,+K.&publication_year=2018&journal=Future+Gener.+Comput.+Syst.&volume=82&pages=395–411&doi=10.1016/j.future.2017.11.022) [[CrossRef]](https://doi.org/10.1016/j.future.2017.11.022)