International Interdisciplinary Virtual Conference on
'Recent Advancements in Computer Science, Management and Information Technology'
International Journal of Scientific Research in Computer Science,
Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

# Blockchain With Internet of Things : Benefits, Challenges, And Applications

**Dr. Prafullkumar Ashokrao Ghuge, Dr. Haridas Janardhan Kharat**
Shankarlal Khandelwal Arts, Science & Commerce College, Akola, MS, India.

**ABSTRACT**
Real-world applications of blockchains, such as faster cross-border payment transactions, identity authentication, smart contracts, cryptos, and supply chain-blockchain technology, are here to stay and, like the Internet, have become the next innovation. The Internet of Things (IoT) is a network of network elements that can exchange information and be controlled and monitored through the use of unique identifiers. Mechanization, wireless sensor networks, embedded systems, and control mechanisms are just a few examples of well-known IoT technologies. Converging advances in real-time analytics, machine learning, resource sensors, and embedded devices demonstrate the IoT paradigm's rapid expansion. So, to begin, a brief overview of the fundamental concepts of IoT and Blockchain is provided.
**Keywords :** blockchain; smart contract; Internet of Things; security, networking, Sensors, Embedded Systems, Cryptocurrency.

## Introduction:

IoT refers to the concept of connecting everything to the Internet. Automobiles, household appliances, and other positioned beneath a vintage with computers, as well as software, detectors, effectors, and interconnection that allow these things to connect, collect, and exchange information, are all included. Kevin Ashton is widely regarded as the father of the Internet of Things [1], which extends Internet connectivity beyond standard devices such as desktops, laptops, smartphones, and tablets to a wide range of historically dumb or noninternet-enabled devices and everyday items. Sensors, the cloud, wireless devices, and security are the entirely new way used in the Internet of Things.

The basic life cycle of IoT includes four parts: (1) gathering data through devices using sensors; (2) storing the gathered data in the cloud for analysis; (3) sending the analysed data back to the device; and (4) acting accordingly [2]. IoT is relevant in many domains, making our lives easier. Smart Homes, Smart Cities, Agriculture, Smart Retail, Driverless Cars, and Healthcare are the primary applications of IoT. Security is still an important aspect of any technology and is critical to the smooth operation of IoT networks.Methodologies for supplying information security and verification, access control within the IoT network, privacy and trust among users and things, and the enforcement of security and privacy policies are some ongoing projects for

improving IoT security. The security issue in IoT arises from careless programme design, which leads to vulnerabilities, which is a major cause of network security issues.

Proper IoT initialization is done at the physiological level in IoT architecture so that any unauthorised receiver could indeed access the system. The Sensing device, Network layer, Middleware layer, Application layer, and Business layer are the five layers of IoT architecture [3]. Each layer has its own set of goals and issues. Consent, Truthfulness, and Accessibility are the three most important security goals in IoT. (CIA). There are four types of attacks in IoT based on security breaches: "Physical attack," "Software attack," "Network attack," and "Cryptographic attack."

Blockchain is a new technology that is being used in a variety of networks to ensure network security and reliability. Blockchain technology is also being prioritised in different demand management solutions, and it is gradually supplanting the present system.

The following are the issues associated with the present banking system:

i. Expensive transaction fees
ii. Increase spending by twofold
iii. Banks have become associated with cries for help.

Blockchain is the technical differences behind bitcoin and has solved the problem associated with centralised banks. Blockchain is a publicly distributed database that contains an encrypted ledger [4].In a centralised architecture, there is a centralized communication system to which every node is linked. This central coordination system will share, pass, and approve all data between the nodes. If the centralized communication platform fails, all of these independent dependent nodes will be disconnected. As a result, shifting from a centralised to a decentralised system is an urgent necessity. There will be more than one coordinator in the decentralised system. A decentralised system has no centralised authority because each node is treated as a coordinator. Each node is linked to the others, and the system is not dependent on just one coordinator.

Blockchain is made up of a chain of blocks, with each block containing a collection of all recently verified transactions. Figure 1 depicts the detailed and general structure of the Blockchain, which shows the sequence of blocks and how each block is cryptographically connected. All of these transaction information are stashed on each block, and a centralised hash code is calculated and stored into the block block by block. Once the transaction has been verified, this block is added to the Blockchain and the chain continues to grow.

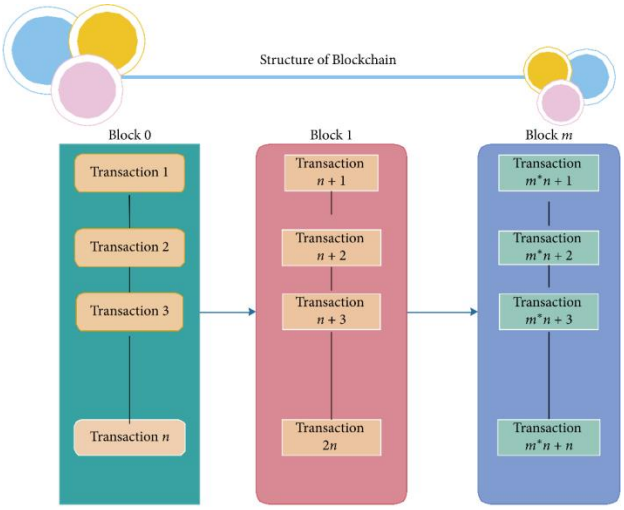


Figure 1: Blockchain structure

Blockchain is a dominant technology, second only to the well-known bitcoin. The operation of bitcoins on the Blockchain can aid in the comprehension of Blockchain technology. Santoshi Nakamoto introduced Bitcoin, the first decentralised digital currency, in 2009 [5].

IoT Architecture:

The Internet of Things (IoT) is the correlation and interaction of various devices via the Internet. These devices are made up of networking nodes, which can be servers or computers, that are linked together to share data. All devices have sensors that collect data that can be transferred, stored, analysed, and displayed in a useful manner [6].

There are numerous IoT architectures that are widely accepted. Various researchers and organisations proposed various architectures. The ITU defines the Internet of Things architecture as four layers, as shown in Fig. [7]

- Application layer
- Service support and application layer
- Network Layer
- Device layer

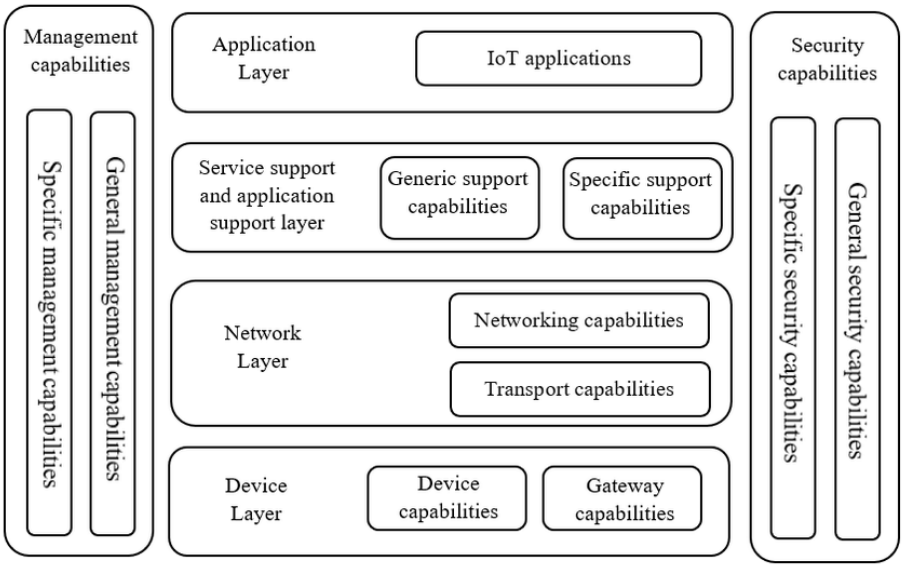


Figure 2: Internet of Things reference model and architecture [7].

IoT applications are included in the application layer. Many IoT applications are available, including healthcare, intelligent buildings, connected cars, smart energy, smart agriculture, and so on. The implied contract and implementation layer include common capabilities that can be used by various IoT applications [8].

The current Internet of Things architecture is based on a centralised model known as the server/client model. In this model, all gadgets are unable to interact with one another and must instead communicate with a centralised gateway. The centralised model has been used for many years to communicate a broad range of desktop computers and will keep supporting small-scale IoT networks; however, it will not be able to meet the needs to stretch the IoT network in the years to come [9].

## Characteristics Of Blockchain

The blockchain has several characteristics which render it appealing for the IoT to use to solve many of its problems. As illustrated in Fig. 3, blockchain features include:

1. Immutability: One of the primary benefits of blockchain is the ability to create unchanging ledgers. All centralised datasets can be manipulated, necessitating trust in a third party to maintain data integrity. Once an agreement has been agreed upon and recorded, it cannot be changed.

2. Decentralization: The lack of centralised control helps to ensure flexibility and resilience by utilising the resources of all network participants and eradicating numerous traffic flows, which reduces latency and eliminates the single point of failure that's present in the centralised model.

3. Anonymity: Anonymity allows users to conceal their personalities and keep their personality private.

4. Increased Security: Blockchain increases security because there is no one point of failure.

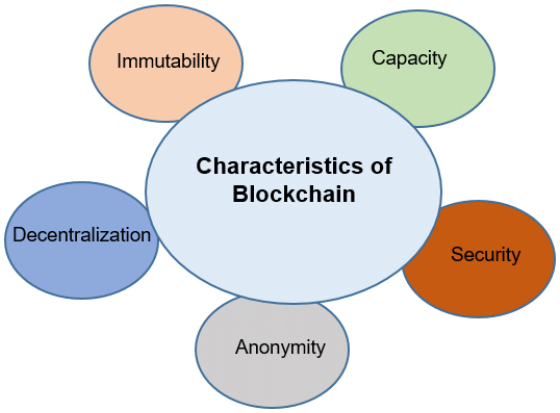


Figure 3: Characteristics of Blockchain

**Blockchain:**

Blockchain is the innovation that powers cryptocurrencies such as Bitcoin. It can help the Internet of Things by creating a decentralised ledger of all exchanges. This blockchain technology is stored in each network node.

To verify consumers and add new data to the blockchain, cryptography is used. The ledger cannot be changed or altered until all nodes have accepted the adding. Blockchain is less reliant on local storage options due to its decentralisation.

One application of blockchain in the Internet of Things is supply chain tracking. Engrained gadgets may perform payments according to supply chain tracking in some cases.

Blockchain might be employed to track the crispness of leafy greens, for example. This would help to prevent foodborne diseases outbreaks.

**The blockchain and IoT**

Gateway nodes can be used to create blockchain-based Iot solutions. These connections act as an intermediary between legacy applications and IoT devices. These gateways can exchange data with one another and also verify frames prior to actually adding them to the public blockchain.

Among the numerous advantages of combining blockchain and the Internet of Things, security and privacy are two of the most compelling reasons to integrate hybrid blockchain and IoT application forms. Adoption of blockchain in IoT can advantage us in all aspects of our lives. Blockchain, for example, can be used in the food business, and blockchain-based IoT systems can be used to track food safety.

This technology would also benefit smart farms and factory operations. IoT systems based on blockchain could also be used in public schools and universities. A smart app would allow parents to track their child's progress. Teachers could provide feedback and report inappropriate behaviour to parents, and vice versa.

**The Benefits of Blockchain and IoT**

The distributed ledger of a blockchain is tamper-proof, eliminating the need for the parties involved to trust one another, according to Andres Ricaurte, a senior vice president and global head of payments at an IT services company. As a result, no single party has control over the massive amount of data generated by IoT devices. Because of blockchain encryption, it is nearly impossible for anyone to overwrite existing data records. Furthermore, storing IoT data on blockchain adds another layer of security to block malicious attackers from gaining access to the network.

According to Vipul Parekh, senior director at management consulting firm Alvarez & Marsal, a primary challenge for IoT players is protecting information throughout the IoT ecosystem. IoT devices' security flaws make them an easy target for distributed-denial-of-service attacks, malicious attackers, and data breaches.

According to Parekh, the combination of Internet of Things and blockchain allows for novel possibilities that reduce inefficiencies, improve security, and increase transparency for all parties present while enabling secure machine-to-machine transfers. The combination of these technologies enables a physical asset to be tracked from the time natural resources are mined, for example, and throughout the supply chain until it reaches the end consumer. [10,11]

The following table compares blockchain and IoT. Both technologies have numerous advantages that can be combined to produce a better result. The Internet of Things has limitless benefits, and using a decentralised approach to IoT would solve many problems, particularly security. Adopting a standardised peer-to-peer communication model to process hundreds of billions of transactions between devices will significantly reduce the costs affiliated with installing and maintaining large centralised data centres, as well as distribute computation and storage needs across billions of devices that comprise IoT networks. This prevents a single node in a network from bringing the whole network to a halting halt. [12]

Table 2. Comparison between blockchain and IoT

| Blockchain | IoT |
|---|---|
| Decentralized | Centralized |
| Resource consuming | Resource restricted |
| Block mining is time-consuming | Demands low latency |
| Scale poorly with large network | IoT considered to contains large number of devices |
| High bandwidth consumption | IoT devices have limited bandwidth and resources |
| Has better security | Security is one of the big challenges of IoT |

The blockchain'sdecentralised, independent, and trustless capabilities make it an ideal component for becoming a foundational component of IoT solutions. It's no surprise that entrepreneurship IoT technologies were among the first to embrace blockchain technology. Establishing peer-to-peer communications, on the other hand, will present its own set of challenges, particularly in terms of security. IoT security is about much more than just safeguarding sensitive data. To prevent spoofing and theft, blockchain solutions will need to maintain privacy and security in IoT networks, as well as use verification and consent of people involved for transactions. [13]

## Challenges Of Blockchain With IOT

However, the complexity of blockchain, which include high computing costs and delays, poses a challenge in the combination of blockchain with IoT, which has limited power and storage capacities. The difficulties encountered when dealing with IoT data on the blockchain are illustrated in Figure 4 and summarised below.

1.Scalability: Scalability in the blockchain may lead to centralized power, raising concerns over the cryptocurrency's future. As the percentage of nodes that make up the network grows, the blockchain scales poorly. This is a serious problem because IoT networks are anticipated to have a large number of nodes [14].

2.Processing Power and Time: The amount of having to process power and time required to encrypt all of the objects in a blockchain system. IoT systems use a variety of devices with varying computing capabilities, and not all of them can run the same cryptographic techniques at the required speed [15].

3.Storage: While blockchain eradicates the need for a database controller to store transfers and device IDs, the ledger must be stored on the nodes themself [16]. The distributed database will grow in size as time passes and the number of nodes in the network grows. As previously stated, IoT devices have limited computation power and storage capacity.

4.Lack of expertise: Blockchain technology is still in its early stages. As a result, only a few people have extensive knowledge and skills in blockchain, particularly in banking. There is a widespread absence of comprehension of how the blockchain works in other applications [17]. Because IoT devices are everywhere, adopting blockchain with IoT will be extremely difficult without raising attention of the blockchain.

5.Legal and Compliance: Because blockchain is a new technology, it will be able to connect people from different countries without any legal or conformance code to follow, which is a serious problem for both businesses and individuals. This challenge will be a major impediment to the widespread adoption of blockchain in many business owners and implementations [18].

6.Naming and Discovery: Because blockchain technology was not designed for IoT, nodes in the network were not supposed to find each other. The Bitcoin application, for example, embeds the IP addresses of some "senders" within the Bitcoin client and is used by nodes to build the network topology. This approach will not work for IoT because IoT devices are constantly moving, causing the topology to change [19].

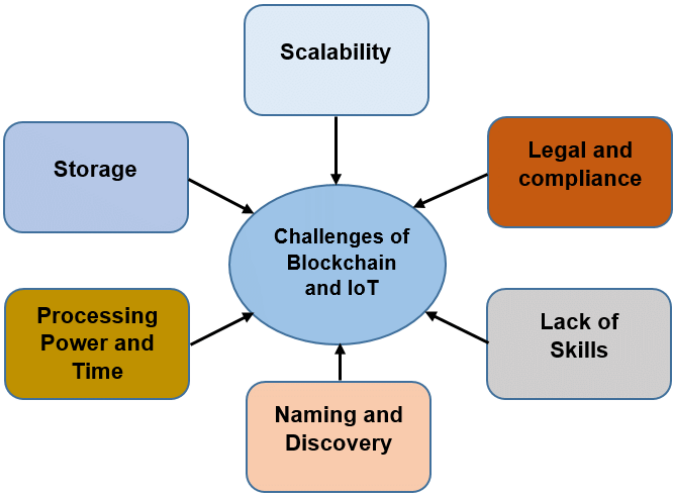


Figure 4: Challenges Of Blockchain With IOT

## Applications

The availability and protection of integrated resources are central concerns of the modern internet. These resources could be encrypted on a network-to-network chain referred to as a blockchain or ledger, where each user is aware of who they are transacting with. It may protect commercial interconnection and avoid fraud by simplifying the business, speeding up the process, eliminating failures, and saving it. People's lives will be transformed by distributed blockchain technology, which will allow them to execute trades as well as control money via phones, vote, rent a car, or even demonstrate their identity.

### 1. Smart Devices

A smart connects directly wirelessly and provides users with superior knowledge and control over previous generations. For example, if your washing machine breaks down, a code affiliated with your machine can connect to the internet and notify you. Such notifications keep the equipment in good working order, saving money on fuel efficiency and enabling you to monitor the devices while driving to work. Accessing such devices through the blockchain would protect the assets while enabling for information flow. [20-21]

### 2. Sensors for the Supply Chain

A sensor is a gadget that detects and reacts to input that comes from tangible facilities. Light, wind, movement, humidity, strain, and other environmental changes can all provide important information. Sensors in the supply chain help locate vehicle temperature changes, pressures, and other parameters. Such inputs are used when supply chain executives need to monitor product or vehicle circumstances and decide precisely where they are and where they are going. The ability of sensors in the supply chain and can provide real-time activity information determines their value.

### 3. The Smart Contract

A consensus mechanism evolved into a digital device designed to digital format inspire, test, or execute an agreement's arrangement and execution. Smart contracts enable the execution of reliable transactions without the need for third-party providers.

### 4. Keeping Track of Prescription Medications

According to the release, blockchains could enhance a patient's experience by enabling them to scan a barcode and instantly determine whether a prescribing is counterfeit. Its technology could also ascertain when pharmaceuticals were collected and transmitted throughout the manufacturing process at the necessary changes in temperature.

### 5. Voting through Electronic Means

The security of a vote is an issue related to national safety in any country. Cybersecurity is investigating the potential of using an online voting system to reduce the cost of hosting a national election while meeting and improving security standards. The voting mechanism has been based on paper and pen since the founding of democratic leaders. To reduce fraud and make voting verifiable and trackable, it is crucial to replace the present pen-and-paper methodology with contemporary election innovation. Blockchains enable a wide range of uses that benefit from the exchange.

### 6. Healthcare on the Blockchain

The blockchain has the potential to revolutionise healthcare data by putting the patient at the centre of health infrastructure and improve health security, privacy, openness, and interconnection. By trying to make electronic records more powerful, without an intermediary, and secure, such breakthroughs have the potential to create a new structure for health information sharing. This contemporary, ever-changing climate is ideal for advancement, research, and concept testing.

### 7. Blockchain Music

Blockchain technology may be beneficial in some cases in music. Through special edition digital releases, it could possible in order to maximize or create incentives and share profits with viewers. Employing it for a music service, on the other hand, is unjust, and trying to claim it is an alternative to any of the most important concerns musicians face is false.

### 8. Blockchain Identification

Identity management is now an essential part of our daily lives. Visiting another country, buying a new car, and enrolling in university all necessitate identification checks. Creating a new social media account requires mobile authorization as well. Bringing personal items is not always practical or even possible. This is where the blockchain's strong nondisclosure control comes into play.

### 9. Passports

Citizens can regulate electrical transport identifier using demonstrable data, such as biometric data, travel history, or any other connected data gleaned at control points by trustable government authorities or other contact points, according to the concept behind a blockchain-based passport. Rather than keeping the specifics to themself, each jurisdiction or agency makes the decision to rely on the data of the others.

### 10. Certificates of Birth, Marriage, and Death

Some things are more important than showing paperwork, such as birth certificates, marriage certificates, and expiry certificates that allow you to access various benefits (such as elections, employment, and residency), but ineptitude is becoming more common. More than one-third of children under the age of five do not have a birth certificate, according to UNICEF. By acquiring birth and death accreditations and letting people access to this vital information, the Blockchain can help to secure records.

### 11. Processing of Insurance Claims

Insurance claims could be handled using decentralized applications on the blockchain network. In this case, all policyholders may have access to the shared health coverage ledger to view actual policies. When a claim is filed, the claimant can submit evidence to the distributed ledger such as insurance documents, claim papers, and continuing to support claims proof. Policyholders must deal directly with distributors for statements. This activity is documented on a private blockchain, with contracts allowing for a workflow claim.

### 12. Data Exchange

The primary goal of blockchain is to improve the efficiency of data exchange across the supply chain, which includes manufacturers, shipment suppliers, distribution companies, governments, providers, order fulfillment, and consumers. Blockchains will enable the corporate entity to track the source of deterioration much faster, reducing the impact of contaminated products.

### 13. Copyright and Royalties Are Protected

Blockchains could be difference makers for copyright owners looking to digital format defend their rights. Without a doubt, it began to make itself known to copyright owners. It continues to remain to be seen whether the suggested compliance procedures for such channels will be executed. The outlook, however, remains positive. It's difficult to see blockchain being used to protect authorship in the following months. Before it can be widespread used to protect copyright, this method must first be widely adopted.

### 14. Property Registration, Real Estate, and Land Registration

Blockchains have the potential to significantly alter the marketplace for real estate, from capital investment to title management. It has the potential to change the relationship between taxpayers and tax authorities, as well as how tax returns are required to submit, taxes are paid, and data is handled. Blockchain technology has the

potential to disrupt and restructure finance, as well as to simplify transfer of funds, exchange, and real estate registration.

### 15. In a Catastrophic Situation (COVID-19)

The COVID-19 pandemic highlights the world's interconnectedness. This also highlights a complex reality: when we need quick, collective action or cooperation, vast amounts of critical information remain trapped in fortified information storage facilities and reputation mechanisms. The blockchain-IoT integrated solutions help us solve the most difficult problems we face between 2019 and 22.

## Conclusion:

In today's world, IoT technology is used in almost every industry, including agriculture, healthcare, and smart cities. In the field of healthcare, IoT is used for applications such as regular patient health monitoring, drug traceability, and so on. However, there are a number of security issues in IoT that can be addressed by integrating IoT with Blockchain.) eBlockchain is a decentralised technology that can be used to improve system security. Blockchain technology, in conjunction with healthcare, ensures that patients' sensitive health-related records are protected from tampering and leakage.

## References:

1. J. M. Kizza, “Internet of things (iot): growth, challenges, and security,” in Guide to Computer Network Security, pp. 517–531, Springer, Berlin, Germany, 2017.
2. P. Gokhale, O. Bhat, and S. Bhat, “Introduction to IOT,” International Advanced Research Journal in Science, Engineering and Technology, vol. 5, no. 1, pp. 41–44, 2018.
3. M. A. J. Jamali, IoT Architecture Towards the Internet of Things, Springer, Berlin, Germany, 2020.
4. N. M. Kumar and P. K. Mallick, “Blockchain technology for security issues and challenges in IoT,” Procedia Computer Science, vol. 132, pp. 1815–1823, 2018.
5. M. B. Hoy, “An introduction to the blockchain and its implications for libraries and medicine,” Medical Reference Services Quarterly, vol. 36, no. 3, pp. 273–279, 2017.
6. W. Stallings, “The Internet of Things: Network and Security Architecture,” Internet Protoc. J., vol. 18, no. 4, pp. 2–24, 2015.
7. ITU, “Overview of the Internet of things,” Ser. Y Glob. Inf. infrastructure, internet Protoc. Asp. next-generation networks - Fram. Funct. Archit. Model., p. 22, 2012.
8. A. Torkaman and M. A. Seyyedi, “Analyzing IoT Reference Architecture Models,” Int. J. Comput. Sci. Softw. Eng. ISSN, vol. 5, no. 8, pp. 2409–4285, 2016.
9. E. Karafiloski, “Blockchain Solutions for Big Data Challenges A Literature Review,” in IEEE EUROCON 2017 -17th International Conference on Smart Technologies, 2017, no. July, pp. 6–8.
10. H. F. Atlam, A. Alenezi, A. Alharthi, R. Walters, and G. Wills, “Integration of cloud computing with internet of things: challenges and open issues,” in 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2017, no. June, pp. 670–675.

11. H. F. Atlam, A. Alenezi, R. K. Hussein, and G. B. Wills, “Validation of an Adaptive Risk-based Access Control Model for the Internet of Things,” I.J. Comput. Netw. Inf. Secur., no. January, pp. 26–35, 2018.
12. M. Conoscenti, D. Torino, A. Vetr, D. Torino, and J. C. De Martin, “Peer to Peer for Privacy and Decentralization in the Internet of Things,” in 2017 IEEE/ACM 39th IEEE International Conference on Software Engineering Companion Peer, 2017, pp. 288–290.
13. S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” Www.Bitcoin.Org, p. 9, 2008.
14. M. Samaniego and R. Deters, “Blockchain as a Service for IoT,” 2016 IEEE Int. Conf. Internet Things IEEE Green Comput. Commun. IEEE Cyber, Phys. Soc. Comput. IEEE Smart Data, pp. 433–436, 2016.
15. H. F. Atlam, A. Alenezi, R. K. Hussein, and G. B. Wills, “Validation of an Adaptive Risk-based Access Control Model for the Internet of Things,” I.J. Comput. Netw. Inf. Secur., no. January, pp. 26–35, 2018.
16. A. Alenezi, N. H. N. Zulkipli, H. F. Atlam, R. J. Walters, and G. B. Wills, “The Impact of Cloud Forensic Readiness on Security,” in Proceedings of the 7th International Conference on Cloud Computing and Services Science (CLOSER 2017), 2017, pp. 511–517.
17. A. Banafa, “IoT and Blockchain Convergence: Benefits and Challenges,” IEEE IoT Newsletter, 2017. [Online]. Available: http://iot.ieee.org/newsletter/january-2017/iot-and-blockchain-convergence-benefits-and-challenges.html
18. Diana Asatryan, “4 Challenges to Blockchain Adoption From Fidelity CEO,” 2017.
19. H. F. Atlam, M. O. Alassafi, A. Alenezi, R. J. Walters, and G. B. Wills, “XACML for Building Access Control Policies in Internet of Things,” in in Proceedings of the 3rd International Conference on Internet of Things, Big Data and Security (IoTBDS 2018), 2018, pp. 1–6.
20. Ferrag, M.A.; Derdour, M.; Mukherjee, M.; Derhab, A.; Maglaras, L.; Janicke, H. Blockchain technologies for the Internet of things: Research issues and challenges. IEEE Internet Things J. 2018, 6, 2188–2204.
21. Cai,W.;Wang, Z.; Ernst, J.B.; Hong, Z.; Feng, C.; Leung, V.C. Decentralized applications: The blockchain-empowered software system. IEEE Access 2018, 6, 53019–53033