Blockchain and The Internet of Things: A Literature Review

Ashutosh Devulkar and Mohammed Awwad
Industrial and Manufacturing Engineering Department
California Polytechnic State University
San Luis Obispo, CA 93407, USA
adevulka@calpoly.edu, mawwad@calpoly.edu

Abstract
The Internet of Things (IoT) and Blockchain are some of the most popular and most significant trends in technology right now. To some extent, one can even say the technologies are a perfect pair as some of the issues like security and trust that come with IoT are taken care of by integrating Blockchain. The decentralized and encrypted nature of Blockchain makes it more robust and tamper-proof than the centralized systems used for IoT. This paper is a literature review that discusses the origins and workings of these technologies as well as discusses the application areas by integrating these two technologies and the challenges faced in integrating these technologies.

Keywords
Blockchain, Internet of Things (IoT), Distributed Ledger Technology (DLT)

1. Introduction
The internet of things (IoT) means a network of objects that are connected to the internet and can communicate with each other. At its core IoT is a network of devices that monitor the desired metrics through sensors and embedded chips, collect the metric data, and can send this data to other connected devices in the network for further processing or triggering a particular automated response. Various types of chips, sensors can be embedded in physical, real-world objects that can transmit data over the internet. The internet of things can find applications in various sectors and can add value to any scenario in which they are deployed. However, the internet of things does have security and privacy concerns. Blockchain, on the other hand, is a cryptographic distributed ledger that can allow secure data transfer in the network. Essentially, Blockchain can enable more secure communication of data by the devices in an IoT network. The paper is divided into the following sections: Section 2 discusses the internet of things technology, its history, working, architecture, applications, and challenges in implementing the applications. Section 3 discusses the blockchains technology, and finally, section 4 discusses the integration of Blockchain and the internet of things technologies.

2. Internet of Things

2.1. History
This section explores the origins of the Internet of Things (IoT). The Internet of Things can be referred to as an autonomous network of machines or objects that are connected to the internet, and that can communicate by exchanging data with other real-world physical devices or applications in the same network. Examples of such tools that can gather data from the real world, compute and transmit this data are smartphones, tablets, computers, etc. The concept of a network of smart devices was first put forward in 1982 when a Coca-Cola vending machine was modified to become the first appliance to be connected to the internet which could provide accurate data about the inventory of the drinks in the vending machine and the temperature of the drinks (Palermo 2014). Raji (1994) coined the concept of integrating and automating everything using the internet to send data in small packets. The term 'Internet of Things' was coined by Ashton K. (2009) for a presentation for Procter and Gamble while trying to link the use of RFID technology and the internet to its supply chain. Evans D. (2011) of Cisco Systems has defined the Internet of Things as "simply of point in time when more things or objects are connected to the internet than people." He also claims that as of 2020, there are more than 50 billion connected devices with 6.58 devices per person, according to a study performed by Cisco. Suresh et al. (2014) have given a brief history of the Internet of Things by providing a timeline. The following diagram can be a visual representation of the growth and development of the internet of things.

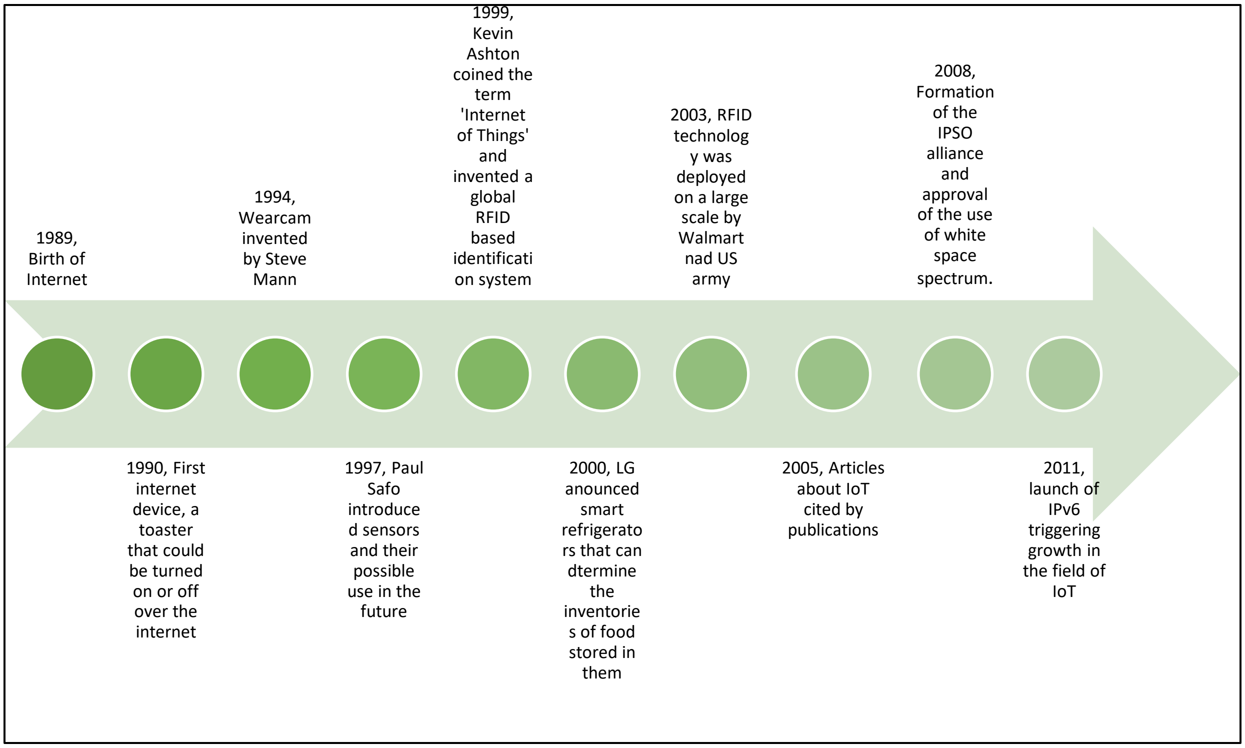

Figure 1: Timeline of Growth and Development of the Internet of Things

2.2. IoT Working

This section discusses the working of the Internet of Things. Siegel J.E et al. (2017) have stated that IoT is a complex network of intelligent sensor devices, a computing unit that is usually placed in the cloud, objects, or devices capable of transmitting, receiving data, and performing actions and a decision-making system. They have also stated that the sensors are used for monitoring a specific metric and can be uniquely identified through technologies like RFID, barcodes that can invoke the necessary action that corresponds to the decision made. Chopra K. et al. (2019) have divided the workflow of the internet of things into three phases. The first phases consist of sensing the metrics, the sensors being identified, and the communication of the metric-specific information. Different combinations of sensors can be used to design smart applications to sense a wide range of metrics like vibrations, humidity, temperature, chemical composition, pressure, etc. These sensors then get identified over the internet and then communicate this metric-specific information to the processing or the computing unit in the cloud. The second phase consists of triggering an action; the data received is processed and then forwarded to a decision-making system. The decision-making system determines what action to be invoked based on the processed information. The action is invoked, and the devices perform the invoked action. In the third phase, the results of the action, the feedback status of the system is communicated to the administrator.

2.3. IoT Architecture

Based on the characteristics of the internet of things, Zhong C. et al. (2015) have put forward a five-layer IoT architecture. The first layer is the perception layer, which is the interface between the physical world and the IoT network. This layer consists of various types of sensors that gather information from the physical world. The second layer is the network access layer, which consists of a base station node and the network access gateway. The base station receives data from the perception layer and connects to the network transmission layer through the network access gateway. The current access methods used are WIFI, Zigbee, Mesh, etc. The third layer is the network transmission layer, and its primary function is to facilitate the transmission and exchange of information. The fourth layer is the application support layer, and it facilitates intelligent analysis and storage of information as well as information processing. The fifth layer is the application presentation layer; the function of this layer is to build applications interfaces and presentation of the information.

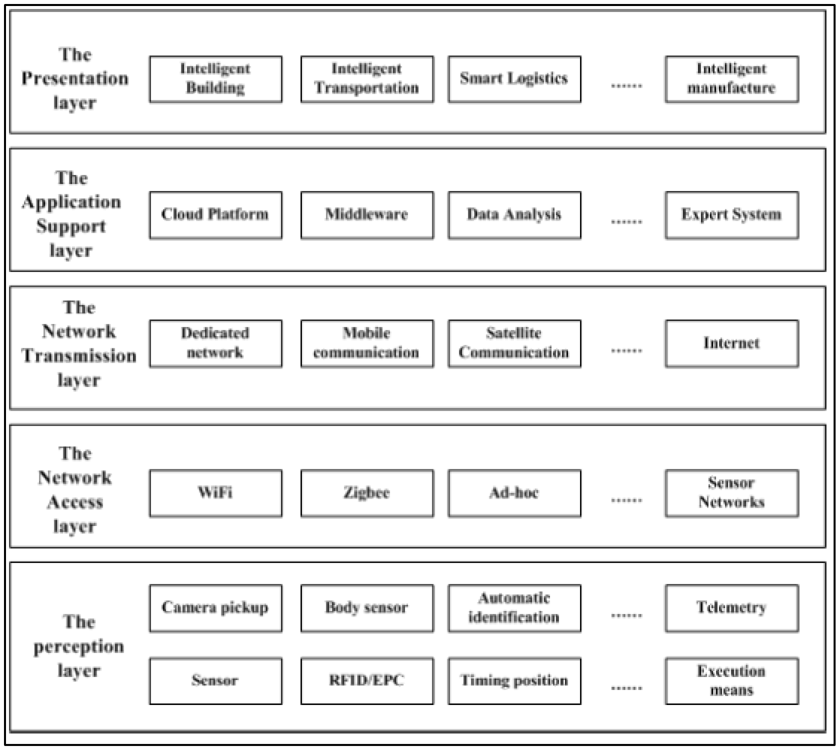

Figure 2: Five-layer IoT architecture

Weyrich & Ebert (2015) have highlighted the purpose of a reference architecture that can serve as an overall and generic guideline. The authors describe the various aspects and requirements of a reference architecture like connectivity, data collection, device management, scalability, and security. They also emphasize the importance of standard reference architectures with many industries and initiatives directed towards standardizing the architectures of IoT. The authors also describe different Internet of things architectures like the Reference Architecture Model Industrie 4.0 (RAMI 4.0), Industrial Internet Reference Architecture (IIRA), Internet of Things Architecture (IoT-A), Standard for Architectural Framework for the Internet of Things, and the Arrowhead Framework. Ray et al. (2018) have conducted a study of various architectures proposed by researchers based on their area of application.

3. Blockchain

3.1. History

This section discusses the origins and history of Blockchain technology. Blockchain is a decentralized digital database that can be co-owned and co-operated by various organizations. It is immutable, i.e. once a transaction is recorded in a Blockchain network, it is tough to change it. Iansiti et al. (2017) have defined Blockchain as "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable permanent way." Bitcoin was the first application that deployed Blockchain was invented by an individual or a group of individuals by the name of Satoshi Nakamoto in 2008, Iansiti & Lakhani (2017). Although the discovery or embodiment of the concept of distributed ledgers came in 2008, the concepts or the ideas behind the technology were proposed in 1970. Sherman et al. (2019) have informally identified the essential elements of blockchain technology and have traced the origins of these element technologies.

They have also suggested that David Chaum was the first cryptographer to propose a blockchain-like protocol in 1982. Ralph Merkel put forth the concept of hash trees and hash chains, now known as Merkel Trees, which are essentially data structures that allow using multiple hashes to be represented by a single hash in 1979, Merkel (1987). Haber and Stornetta (1990) tried to implement a system where documents could be time-stamped, and those time-stamps were tamper-resistant. Bayer et al. (1993) implemented Merkel Trees, which allowed them to collect multiple certificates into one block.

3.2 Blockchain Working

Blockchain contains information in the form of blocks. It is essentially a distributed ledger that can be open to anyone. Each block consists of data that is dependent on the type of Blockchain, a hash, and the hash of a previous block. A hash is a unique identifying characteristic of a block. When a block is created, its hash is calculated based on preprogrammed conditions; the hash is calculated in such a way that it is dependent on the data in the block, this means that changing the data in the block will change its hash. The other element of the Blockchain is the hash of the previous block; this makes Blockchain cryptographically very secure as each block points to the previous block. Any changes made in the data of block will change its hash value, and this will make all further blocks invalid. As most of the computers are capable of calculating hundreds and thousands of hashes in a matter of minutes, tampering of the blocks is still possible. Hence, blockchains use a consensus mechanism like 'Proof-of-Work' that slows down the creation of blocks. Further, to improve the security of a blockchain, the ledger is distributed and uses a peer to peer network. Whenever a new peer joins the network, he gets a copy of the entire ledger. When a new block is created, it is sent to peers in the network who verify the authenticity and validity of the block. After reaching a consensus the block, it is then appended to the existing Blockchain as a new block, Simply Explained (2017). Shah (n.d) explains the working of Blockchain as follows: It starts when someone in Blockchain initiates a transaction or a group of transactions; these transactions are sent to a network of peer to peer network of computers. Each computer in the blockchain network is called a node; every node has a copy of the existing ledger, which consists of the existing data and the logic. The transaction gets executed and validated based on pre-defined contracts called smart contracts. Once the transaction is completed successfully, it gets added to the ledger.

3.3 Distributed Ledger Technology

Rhodes (2020) defines distributed ledger technologies as a peer-to-peer network without a central administrator or central database, which is designed to work together to verify the accuracy of the data. Distributed Ledgers are a type of database in which the data is added to a continuous ledger when the participants in the network achieve consensus Hancock & Vaizey (2016). The ledger can be spread across countries and organizations. The terms Blockchain and Distributed Ledger Technology (DLT) are very often interchangeably used. While a blockchain is a type of database that takes several records and puts them in a block, and cryptographically links different blocks together to form a chain Hancock & Vaizey (2016), distributed ledgers are continuous ledgers, and records are stored one after the other instead of blocks Hancock & Vaizey (2016). Essentially Blockchain is a type of DLT. Further, unlike Blockchain, DLT does not require a proof of work (PoW) consensus mechanism Belin (n.d). Other types of distributed ledger technologies discussed by Rhodes (2020) are Directed Acyclic Graphs (DAG), Holochain DLT, Tempo (Radix).

3.4 Components of Blockchain

This section discusses the elements of blockchain technology. Sherman et al. (2019) have roughly outlined the aspects of Blockchain as:

a) Cryptographical linking of the blocks
b) Access policy – This determines who can read the data on the ledger
c) Control Policy – This determines who may participate in the network
d) Consensus policy – This determines the validity of any given state of the ledger

The author proposes that these are the main components of Blockchain and variations of these elemental technologies together form different types of blockchains and distributed ledger technologies. Rhodes (2020) has outlined peer-to-peer networks, nodes, and consensus mechanisms as the most common components of a distributed ledger technology. Shah (n.d) has identified three main components of Blockchain:

1. Transactions
2. Smart Contracts
3. Consensus Algorithm

Transactions - A Transaction in a blockchain network is essentially a transfer of something of value from the sender to the recipient. It can be a transfer of any form of a tangible or intangible asset. Transactions consist of three components -

- Recipient
- Signature of the sender
- Value

Any transaction that is executed in the blockchain network gets recorded permanently in the distributed ledger.

Smart Contracts - In blockchain technology, transactions are a set of predetermined contractual clauses that are executed by Smart Contracts. In short, Smart Contracts are the code that executes a transaction. Smart contracts are a type of computer protocol that facilitates, verify, and enforces the performance of predetermined agreements. Smart contracts can perform these transactions without the participation of any third parties. Once the transactions are executed, they get recorded and are traceable and irreversible. These smart contracts are written in a high-level programming language like JavaScript or Solidity for Ethereum.

Consensus Algorithm - Consensus algorithms are the mechanisms that are used to determine which transactions get added to a ledger. The primary objective of a consensus algorithm is to ensure there is an agreement between all participating peers as to what transactions are considered valid and what should be added to the shared ledger. A transaction is validated by verifying the identity of the initiator of the transaction; the transaction is not modified after initiation, verifying the ownership of assets being transferred. All the participants in the blockchain network (nodes) have to agree upon what transactions should be added to the distributed ledger and the exact ordering of the transaction.

3.5 Public and Private Blockchain

This section differentiates between public and private Blockchains. Jayachandran (2017) has drawn out the key similarities and differences between public and private blockchains. Practically, they are both decentralized ledgers using a peer to peer network to maintain and update the ledger, and both types of blockchains guarantee immutability of the ledger. Following is the summary of the differences pointed out by Jayachandran (2017) between the two types of blockchains.

Public blockchains are permissionless blockchains, which means that anyone can join the blockchain network, read and write data, and initiate transactions. The peers who want to process a transaction incentivize the processing of transactions through cryptocurrency. The consensus mechanism used is the Proof of Work (PoW) consensus mechanism. The transactions are pseudonymous, i.e., anyone can join as a trustless participant, and their addresses are publicly viewable. Processing of transactions costs digital currency. Public blockchains are censorship-resistant, i.e., a third party cannot add or remove the data entered by another party. E.g., Bitcoin, Ethereum.

Private blockchains can be shared permissioned (consortium blockchains) or permissioned. In shared permissioned or consortium blockchains, nodes are pre-approved participants. They have a higher transaction throughput and lower latency compared to other public blockchains. The limited number of nodes requires a different consensus mechanism like Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Practical Byzantine Fault Tolerance (DBFT). They are perceived as semi-decentralized ledger technology. E.g., Hyperledger, Corda. Whereas private blockchains are designed for instant deployment, and a legal smart contract bounds the validators. Very few nodes can make changes to the ledger.

4. Integration of Blockchain and IoT

As described by Pinto (2019), Blockchain and IoT are two emerging technologies that can complement each other to achieve greater potential. The author has also addressed a few key challenges that can be solved by the integration of these two technologies like security, data encryption, communication, cost reduction, and tracking. Pauw has emphasized the effectiveness of Blockchain in overcoming the bottlenecks of centralized networks used in IoT. He has also described how smart contracts can help reduce the need for a centralized application or middleware as well as the how the decentralized nature of Blockchain will eliminate the risk of a single point of failure that can disable the entire network. Windpassinger et al. (2017) have put forth their proposition that Blockchain can be the missing link to address the issues in IoT like scalability, single point of failure, record maintenance, privacy, time stamping, and reliability. IoT devices, through smart contracts, can autonomously interact with one another without the need for a central authority. The authors claim that this could be a solid foundation for a fully distributed, reliable digital infrastructure. As the IoT market is mostly unregulated, security hacking and data breach are a significant concern in IoT, IEEE Innovation at work (n.d). With Blockchain, it is possible to not only cryptographically secure these devices, but it is also possible to identify the device or point of the breach if a data breach were to happen. Further, in a decentralized ledger technology, there is no central authority; this will allow the IoT devices to communicate autonomously and will significantly improve their latency, making them more useful and fast for real-time applications.

4.1 Applications of Blockchain and IoT

4.1.1 Supply Chain and Logistics

Global supply chains are complex and involve multiple stakeholders. Traceability, transparency can be enhanced using Blockchain and IoT technologies. IoT sensors can monitor critical data like GPS location, temperature, vibrations, etc. in real-time, which will then be recorded on the Blockchain. Further, only the stakeholders listed in the smart contracts will be provided access to this data. Blockchain increases trust in the supply chain LeewayHertz (n.d). According to Banerjee (2019), IoT and Blockchain can help in improving traceability, transparency, and reduction of counterfeiting.

4.1.2 Automotive Industry

Autonomous cars and connected cars are the two trends that are transforming the automotive industry. Internet of Vehicles (IoV) is an emerging concept, and it allows vehicles to communicate with each other or with a network of other cars. Blockchain or distributed ledger technology enables users to exchange data quickly and more securely. Connected vehicles that can transmit data over the cloud have profound advantages. Connected cars have several advantages like better navigation, predictive maintenance, driver information, etc. The combination of IoT and blockchain technology can be used for automated fuel payments, autonomous cars capable of communicating with each other, smart parking, and intelligent traffic control.

4.1.3 Smart Homes

Smart devices at homes are becoming increasingly familiar with the introduction of smart home devices by Google, Amazon, Apple, and many more. Many of these devices capture sensitive information like biometrics, voice recognition, fingerprint data, etc. This data can be stored on a blockchain to make it resistant to unauthorized manipulation. Smart homes have the capability can take care of mundane everyday tasks, improve energy consumption efficiency.

4.1.4 Sharing Economy

Sharing economy is a concept in which users can share idle assets and services for a short term using a peer-to-peer transaction or smart contracts to facilitate collaboration, which is hosted on some online platform that connects buyers and sellers Chappelow (2020). This type of economic model is becoming increasingly popular. Similarly, idle IoT objects can be shared securely through smart contracts that ensure data integrity and allows for controlling the access of information. The sharing economy enables people to monetize their idle resources and things in a more secure manner through Blockchain.

4.1.5 Pharmacy Industry

Counterfeit medicines are an increasing problem in the pharmaceutical industry; hence tracking and tracing the shipments is crucial. IoT, combined with Blockchain, can be used to tackle this problem. The integrated technology can be used to monitor the shipment as well as other metrics like temperature, and geolocation can also be monitored. Thus, these technologies can be used to ensure the quality and authenticity of drugs in pharmaceutical supply chains.

4.1.6 Agriculture

IoT sensors can be deployed in farms to monitor various metrics like soil quality and crop-related data. This data can then be stored on a blockchain network, which can be made accessible to other stakeholders in the agriculture supply chains like retailers and distributors. The information allows transparency in the supply chain and allows the retailers to decide on the procurement of the crop. Further, the data captured by these IoT sensors can be utilized by farmers to make related decisions. Moreover, Blockchain or DLT can be used to trace and track the food products to the source in a faster and efficient manner. Data like fertilizers, pesticides used, environmental effects of the farming practices used, type of soil, crop yield can be stored on the Blockchain and made available to customers and concerned authorities.

4.1.7 Water Management

IoT sensors can monitor water contamination levels at the source, and the data collected can be stored on a blockchain and made available to decision making authorities. Blockchain also allows for tracking of water sources in the packaged drinking water supply chain. IoT devices can also be used to monitor the usage of water and detect leaks.

4.1.8 Healthcare

Healthcare is another sector where extensive research is being conducted for deploying these technologies. Wearable IoT devices are becoming increasingly popular. These devices can be used to remotely monitor various metrics like heart rate, blood pressure, etc. the collected data can then be stored on a blockchain network to protect the privacy of customers. They can be made available to healthcare professionals only at the discretion of the patients. Blockchain networks can be used in mobile healthcare applications for better auditing and data integrity.

4.1.9 Energy Sector

Blockchain technology can be deployed on the Internet of Energy (IoE) to enable the payment for energy consumption without any human intervention. IoT allows for better visibility of energy consumption; blockchain technology can be deployed for ensuring immutability and transparency in the monitoring of the smart grids. Smart grids allow for better control over the production and distribution of energy. Furthermore, blockchain technology can also be deployed for secure energy trading in the industrial sector.

4.1.10 Industry 4.0

IoT sensors can be deployed in a manufacturing environment to gather data and monitor various types of pre-defined metrics. The industrial internet of things allows for better control over manufacturing, preventive maintenance, and efficient manufacturing processes. The data collected is sensitive for industries, and the loss of this data to hackers can result in financial losses for these industries. To better protect this data, the data can be stored on Blockchain, and access can be granted to authorized personnel only. Further, Blockchain can be used for asset tracking in industries as well.

4.1.11 Smart cities

Recent smart city initiatives involve green energy, smart transport, smart water management, pollution management, smart homes, smart grids, universal identification, wireless internet systems, and much more, McFarlane (2019). These initiatives are highly reliant on IoT technology, and deploying IoT devices generates a lot of data. The security, integrity, transparency, and privacy can be ensured by storing the generated data on a blockchain.

Table 1: Applications of Blockchain and IoT

Sr. No	Application Field	Citation
1	Supply chain and logistics	LeewayHertz (n.d), Banerjee (2019), Mondal et al (2019), Fernández-Caramés & Fraga-Lamas (2018), Dasaklis & Casino (2019), Kshetri (2018)
2	Automotive Industry	LeewayHertz (n.d), Banerjee (2019), Fernández-Caramés & Fraga-Lamas (2018), Kang et al (2017)
3	Smart Homes	LeewayHertz (n.d), Banerjee (2019), Davis (2019)
4	Sharing economy	LeewayHertz (n.d), Huckle et al. (2016), Chapplelow (2020)
5	Pharmaceutical Industry	LeewayHertz (n.d), Bocek et al. (2107)
6	Agriculture	LeewayHertz (n.d), Banerjee (2019), Caro et al (2018)
7	Water Management	LeewayHertz (n.d), Parwekar (2011)
8	Healthcare	Fernández-Caramés & Fraga-Lamas (2018), Guo et al (2018), Esposito et al (2018), Liang et al (2017), Shae & Tsai (2017), Biswas & Muthukkumarswamy (2016)
9	Energy Metering	Fernández-Caramés & Fraga-Lamas (2018), Zhang & Wen (2015), Gao et al (2018), Li et al (2017), Lundqvist et al (2017)
10	Industry 4.0	Fernández-Caramés & Fraga-Lamas (2018), Hasan et al (2020), Banerjee (2019)
11	Smart Cities	Fernández-Caramés & Fraga-Lamas (2018), Biswas & Muthukkumarswamy (2016), IOTA (n.d), Li (2018), McFarlane (2019)

4.2 Challenges in Implementation of BIoT

This section discussed the challenges in leveraging Blockchain and IoT technologies

4.2.1 Technical Challenges

The most crucial type of challenges faced in implementing Blockchain and IoT technologies are technical, and these are discussed below:

<u>Throughput</u> – Memon et al. (2018) have pointed out that the average time to create a block in the blockchain network is about 10 minutes, and thus, a blockchain network can only handle seven transactions per second. Burlakov has also discussed this issue by drawing out the difference between the number of transactions handled by a distributed ledger technology like Ethereum and a centralized transaction processing firm like VISA. Ethereum can process 15 transactions/ sec while VISA processes 2000 transactions per second.

<u>Latency</u> – As suggested by Koteska et al. (2017), the latency of a distributed ledger technology depends on the consensus mechanism used by it. DLT that uses Proof-of-Work requires a lot of computation, and a single block takes about 10 minutes to be appended to the Blockchain. A single transaction is relayed twice across a network, first when

it needs to be validated and second when the transaction is appended to the Blockchain, Xie et al. (2019). The latency of other DLT like Hyperledger is comparatively lower, Hyperledger (n.d)

Storage – The blockchain technology requires each node in the network to maintain a copy of the ledger from the genesis block to the recent block appended to the Blockchain, Xie et al. (2019). Further application of other DLT in real-world scenarios will generate data. They have also pointed out the need to study the effective and secure storage of this data.

Size and Bandwidth – In 2015, the size of bitcoin was 25 G.B. and grew by 14 G.B. since 2014; if throughput gets increased to 2000 transactions/ sec, the Blockchain will increase 3.9 GB/ day Swan (2015). Running the nodes in a blockchain network requires resources and the size of the Blockchain promotes centralization.

Scalability –. The high latency and low throughput of Blockchain make it challenging to adopt for applications other than cryptocurrency. Xie et al. (2019) have presented a detailed study of the scalability issue by dividing it into throughput, storage, and latency aspects.

Energy Consumption – Burlakov (2019) has pointed out that the consensus mechanism, especially the Proof-of-Work consensus mechanism, requires a lot of computational power. In 2017, Bitcoin mining consumed the same amount of energy as the entire nation of Denmark. Deshpande et al. (2017) have highlighted that the distributed nature of Blockchain and DLT has increased the need for computational power, which can potentially result in high consumption of energy.

Security – Deshpande et al. (2017) have pointed out the need for safeguarding data integrity through robust encryption mechanisms as a critical challenge in the wide-scale implementation of DLT/Blockchain technologies. The authors have also highlighted the concern over data privacy as a significant challenge since data that might be sensitive to businesses will be entrusted to DLT/Blockchain technologies.

4.2.2 Financial Challenges

Apart from the technical challenges, the financial difficulties in implementing these technologies are:

High Cost – As pointed out earlier, deployment of blockchain technology requires a lot of resources like energy, storage, bandwidth, and hence could result in the rise of related costs. Swan (2015) has cited that the estimate of total energy consumption is about $15 million per day. Further, since Blockchain is a reasonably new technology, deployment, and maintenance of a blockchain network will require skilled labor and increases the initial cost of deployment.

Business Model – As pointed out by Swan (2015, traditional business models may not be suitable for the deployment of blockchain technology. Further, incorporating cryptocurrencies and smart contracts in the existing business models will require a lot of work. Peterson & Baur (2018) have pointed out that negotiating the terms of a smart contract requires a lot of time as well. Deshpande et al. (2017) have highlighted the potential disruption of existing operations due to the implementation of DLT/blockchain technologies poses a significant challenge.

Economic Impact – The lack of evidence on business gains and the general economic impact on businesses has been highlighted as one of the factors that might discourage companies from adopting DLT/blockchain technologies by Deshpande et al. (2017). The authors have cited that there is a lack of clarity about the improvements the technology offers over existing solutions. Hence, it isn't easy to gauge the medium- and long-term economic impact of the technology.

4.2.3 Functional Challenges

The functional challenges in leveraging Blockchain and IoT technologies are as described below

Governance and Regulation – Burlakov (2019) has cited that there are uncertainty and a lack of regulation of blockchain technology. Petersson & Baur (2018) have mentioned that in global supply chains, there are multiple regulatory bodies and authorities of different countries are involved. Hence, it would be difficult to adapt to various regulations and policies. Further, Blockchain gathers and stores data that may be sensitive for some businesses; therefore, there is a need for regulating the storage and transmission of this data. Deshpande et al. (2017) have stated that, given the decentralized nature of distributed ledger technologies, one of the key challenges will be to set out clear rules for the governance of the ledger, and it is essential to establish responsibilities and terms of use for participants in both permissioned and permissionless ledgers. The authors have also cited the importance of the development and adoption of specific regulations in the context of implementing DLT/Blockchain technologies. Another key concern highlighted by Deshpande et al. (2017) is the legal enforceability of smart contracts, particularly on how to enforce them using DLT/Blockchain. Cermeño (2016) has presented the position of various governments and authorities on virtual currencies, cryptocurrencies, and distributed ledger technologies.

Collaboration – Blockchain and distributed ledger technologies are relatively new but have the potential to be deployed in various fields. Petersson & Baur (2018) have pointed out the lack of collaborative efforts between the people in the areas of blockchain and supply chain.

Skilled Labor – Blockchain and Distributed ledger technologies are still in their incipient stages of development. Moreover, the technology is complex and convergence of many supporting technologies. Hence there is a lack of professionals and skilled workers with extensive knowledge in the field, Burlakov (2019). Deshpande et al. (2017) have highlighted the lack of clarity in terminology and immaturity of the technology as one of the limitations that inhibit its adoption.

Interoperability – With the growth in the number Distributed ledger Technologies, Deshpande et al. (2017) have highlighted the need for smooth interaction and transfer of data between different types of ledgers to realize the full benefits of DLT/Blockchain.

5. Conclusion

Blockchain, when combined with the Internet of Things (IoT), offers promising applications in various fields. A lot of research is being conducted to implement the combination of these technologies, especially in the areas of supply chain management, manufacturing, healthcare, and automotive industries. This paper discusses the general challenges that inhibit the implementation of these technologies, but there are challenges pertaining to the field as well. Both Blockchain and IoT are still in their incipient stages of development, and it may take years for these technologies to reach their potential fully but the future of these technologies looks promising, and the possibility of a connected world looks less of a dream.

References

"Internet of Things Done Wrong Stifles Innovation". *Information Week.* 7 July 2014. Retrieved 10 November 2014.

Raji, R. S. (1994). Smart networks for control. *IEEE spectrum*, *31*(6), 49-55.

Ashton, K. (2009). That 'internet of things' thing. *RFID journal*, *22*(7), 97-114.

Evans, D. (2011). The internet of things: How the next evolution of the internet is changing everything. *CISCO white paper*, *1*(2011), 1-11.

Suresh, P., Daniel, J. V., Parthasarathy, V., & Aswathy, R. H. (2014, November). A state of the art review on the Internet of Things (IoT) history, technology and fields of deployment. In *2014 International conference on science engineering and management research (ICSEMR)* (pp. 1-8). IEEE.

Siegel, J. E., Kumar, S., & Sarma, S. E. (2017). The future internet of things: Secure, efficient, and model-based. *IEEE Internet of things journal*, *5*(4), 2386-2398.

Chopra, K., Gupta, K., & Lambora, A. (2019, February). Future internet: The internet of things-a literature review. In *2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon)* (pp. 135-139). IEEE.

Zhong, C. L., Zhu, Z., & Huang, R. G. (2015, August). Study on the IOT architecture and gateway technology. In *2015 14th International Symposium on Distributed Computing and Applications for Business Engineering and Science (DCABES)* (pp. 196-199). IEEE.

Weyrich, M., & Ebert, C. (2015). Reference architectures for the internet of things. *IEEE Software*, *33*(1), 112-116.

Ray, S., Adhikary, P., Mitra, S., Halder, T., Paul, M., Mukherjee, A., ... & Sarkar, D. (2018, November). A Survey Paper on Architecture of Internet of Things. In *2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)* (pp. 908-913). IEEE.

Iansiti, Marco; Lakhani, Karim R. (January 2017). "The Truth About Blockchain". Harvard Business Review. Harvard University. Archived from the original on 18 January 2017. Retrieved 17 January 2017

Sherman, A. T., Javani, F., Zhang, H., & Golaszewski, E. (2019). On the origins and variations of blockchain technologies. *IEEE Security & Privacy*, *17*(1), 72-77.

Merkle, R. C. (1987, August). A digital signature based on a conventional encryption function. In *Conference on the theory and application of cryptographic techniques* (pp. 369-378). Springer, Berlin, Heidelberg.

Haber, S., & Stornetta, W. S. (1990, August). How to time-stamp a digital document. In *Conference on the Theory and Application of Cryptography* (pp. 437-455). Springer, Berlin, Heidelberg.

Bayer, D., Haber, S., & Stornetta, W. S. (1993). Improving the efficiency and reliability of digital time-stamping. In *Sequences Ii* (pp. 329-334). Springer, New York, NY.

Sherman, A. T., Javani, F., Zhang, H., & Golaszewski, E. (2019). On the origins and variations of blockchain technologies. *IEEE Security & Privacy*, *17*(1), 72-77.

Jayachandran, P. (2017). The difference between public and private Blockchain. IBM.

Rohan Pinto, Demystifying the Relationship between IoT and Blockchain, Forbes Technology council Post, 2019, Available Online – Post

Chrisjan Pauw, How significant is Blockchain in Internet of Things?, Cointelegraph, 2018, Available Online – Post

Windpassinger, N., & Tricoire, J. P. (2017). *Digitize Or Die: Transform Your Organization, Embrace the Digital Evolution, Rise Above the Competition*. IoT Hub.

Banerjee, A. (2019). Blockchain with IOT: Applications and use cases for a new paradigm of supply chain driving efficiency and cost. In *Advances in Computers* (Vol. 115, pp. 259-292). Elsevier.

Jim Chapplelow "Sharing Economy", Mar 2020 Available online - Post

Mondal, S., Wijewardena, K. P., Karuppuswami, S., Kriti, N., Kumar, D., & Chahal, P. (2019). Blockchain inspired RFID-based information architecture for food supply chain. *IEEE Internet of Things Journal*, *6*(3), 5803-5813.

Fernández-Caramés, T. M., & Fraga-Lamas, P. (2018). A Review on the Use of Blockchain for the Internet of Things. *Ieee Access*, *6*, 32979-33001.

Dasaklis, T., & Casino, F. (2019, May). Improving vendor-managed inventory strategy based on Internet of Things (IoT) applications and blockchain technology. In *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* (pp. 50-55). IEEE.

Kshetri, N. (2018). 1 Blockchain's roles in meeting key supply chain management objectives. *International Journal of Information Management*, *39*, 80-89.

Kang, J., Yu, R., Huang, X., Maharjan, S., Zhang, Y., & Hossain, E. (2017). Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains. *IEEE Transactions on Industrial Informatics*, *13*(6), 3154-3164.

Davis, N. (2018). Blockchain for the connected home: combining security and flexibility.

Huckle, S., Bhattacharya, R., White, M., & Beloff, N. (2016). Internet of things, Blockchain and shared economy applications. *Procedia computer science*, *98*, 461-466.

Bocek, T., Rodrigues, B. B., Strasser, T., & Stiller, B. (2017, May). Blockchains everywhere-a use-case of blockchains in the pharma supply-chain. In *2017 IFIP/IEEE Symposium on Integrated Network and Service Management (I.M.)* (pp. 772-777). IEEE.

Caro, M. P., Ali, M. S., Vecchio, M., & Giaffreda, R. (2018, May). Blockchain-based traceability in Agri-Food supply chain management: A practical implementation. In *2018 IoT Vertical and Topical Summit on Agriculture-Tuscany (IOT Tuscany)* (pp. 1-4). IEEE.

Parwekar, P. (2011, September). From internet of things towards cloud of things. In *2011 2nd International Conference on Computer and Communication Technology (ICCCT-2011)* (pp. 329-333). IEEE.

Guo, R., Shi, H., Zhao, Q., & Zheng, D. (2018). Secure attribute-based signature scheme with multiple authorities for Blockchain in electronic health records systems. *IEEE access*, *6*, 11676-11686.

Esposito, C., Santis, A. D., Tortora, G., Chang, H., & Choo, K. K. R. (2018). Blockchain: A panacea for healthcare cloud-based data security and privacy? IEEE Cloud Computing. 5 (1): 31–37, 2018.

Liang, X., Zhao, J., Shetty, S., Liu, J., & Li, D. (2017, October). Integrating Blockchain for data sharing and collaboration in mobile healthcare applications. In *2017 IEEE 28th annual international symposium on personal, indoor, and mobile radio communications (PIMRC)* (pp. 1-5). IEEE.

Z. Shae and J. J. P. Tsai, "On the Design of a Blockchain Platform for Clinical Trial and Precision Medicine," *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*, Atlanta, GA, 2017, pp. 1972-1980, doi: 10.1109/ICDCS.2017.61.

Biswas, K., & Muthukkumarasamy, V. (2016, December). Securing smart cities using blockchain technology. In *2016 IEEE 18th international conference on high performance computing and communications; IEEE 14th international conference on smart city; IEEE 2nd international conference on data science and systems (HPCC/SmartCity/DSS)* (pp. 1392-1393). IEEE.

Zhang, Y., & Wen, J. (2015, February). An IoT electric business model based on the protocol of bitcoin. In *2015 18th international conference on intelligence in next generation networks* (pp. 184-191). IEEE.

Gao, J., Asamoah, K. O., Sifah, E. B., Smahi, A., Xia, Q., Xia, H., ... & Dong, G. (2018). Gridmonitoring: Secured sovereign Blockchain based monitoring on smart grid. *IEEE Access*, *6*, 9917-9925.

Li, Z., Kang, J., Yu, R., Ye, D., Deng, Q., & Zhang, Y. (2017). Consortium blockchain for secure energy trading in industrial internet of things. *IEEE transactions on industrial informatics*, *14*(8), 3690-3700.

Lundqvist, T., de Blanche, A., & Andersson, H. R. H. (2017, June). Thing-to-thing electricity micro payments using blockchain technology. In *2017 Global Internet of Things Summit (GIoTS)* (pp. 1-6). IEEE.

Hasan, H. R., Salah, K., Jayaraman, R., Omar, M., Yaqoob, I., Pesic, S., ... & Boscovic, D. (2020). A Blockchain-Based Approach for the Creation of Digital Twins. *IEEE Access*, *8*, 34113-34126.

Li, S. (2018, August). Application of blockchain technology in smart city infrastructure. In *2018 IEEE International Conference on Smart Internet of Things (SmartIoT)* (pp. 276-2766). IEEE.

McFarlane, C. (2019). Are Smart Cities The Pathway To Blockchain And Cryptocurrency Adoption.

Memon, M., Hussain, S. S., Bajwa, U. A., & Ikhlas, A. (2018, August). Blockchain Beyond Bitcoin: Blockchain Technology Challenges and Real-World Applications. In *2018 International Conference on Computing, Electronics & Communications Engineering (iCCECE)* (pp. 29-34). IEEE.

George Burlakov (2019), *7 challenges to Adoption of Blockchain in 2019*, Blog

Koteska, B., Karafiloski, E., & Mishev, A. (2017). Blockchain implementation quality challenges: a literature. In *SQAMIA 2017: 6th Workshop of Software Quality, Analysis, Monitoring, Improvement, and Applications* (pp. 11-13).

Xie, J., Yu, F. R., Huang, T., Xie, R., Liu, J., & Liu, Y. (2019). A survey on the scalability of blockchain systems. *IEEE Network*, *33*(5), 166-173.

Swan, M. (2015). *Blockchain: Blueprint for a new economy*. “O'Reilly Media, Inc.".

Deshpande, A., Stewart, K., Lepetit, L., & Gunashekar, S. (2017). Distributed Ledger Technologies/Blockchain: Challenges, opportunities and the prospects for standards. *Overview report The British Standards Institution (BSI)*, *40*, 40.

Petersson, E., & Baur, K. (2018). Impacts of blockchain technology on supply chain collaboration: A study on the use of blockchain technology in supply chains and how it influences supply chain collaboration.

Cermeño, J. S. (2016). Blockchain in financial services: Regulatory landscape and future challenges for its commercial application. *BBVA Research Paper*, *16*, 20.

"Internet of Things Done Wrong Stifles Innovation". *InformationWeek*. *7 July 2014*. Retrieved 10 November 2014.

Iansiti, Marco; Lakhani, Karim R. (January 2017). *"The Truth About Blockchain"*. *Harvard Business Review*. Harvard University. Archived from the original on 18 January 2017. Retrieved 17 January 2017.

Simply Explained, "How does a Blockchain Work", YouTube : Video

Qasim Shah, "Deploy a Hyperledger Blockchain network in AWS", Udemy Course : https://www.udemy.com/course/deploy-a-hyperledger-blockchain-network-in-aws/

Delton Rhodes (March 2020). “Distributed Ledger Technology: An overview of DLT systems”. Komodo. https://komodoplatform.com/distributed-ledger-technology/

Hancock Mathew, Vaizey Ed (January2016). “Distributed Ledger Technology: beyond Blockchain”. Government Office for Science (U.K.).

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf

Oliver Belin (n.d), “The difference between Blockchain and Distributed Ledger Technology”. Tradeix. https://tradeix.com/distributed-ledger-technology/

IEEE Innovation at Work (n.d), “The potential of Blockcahin for IoT”. https://innovationatwork.ieee.org/the-potential-of-blockchain-for-iot/

LeewayHertz (n.d), “Blockchain IoT use cases – Real world applictions of Blockchain and IoT”. https://www.leewayhertz.com/blockchain-iot-use-cases-real-world-products/

Hyperledger (n.d). https://www.hyperledger.org/

IOTA (n.d). https://www.iota.org/solutions/smart-city

Ashutosh Devulkar is a graduate student pursuing a Master's degree in Industrial Engineering at California Polytechnic State University, San Luis Obispo, USA. He earned his bachelor's degree in Manufacturing Engineering from Savitribai Phule Pune University, India.

Mohamed Awwad is an Assistant Professor in the Department of Industrial and Manufacturing Engineering at California Polytechnic State University (Cal Poly), San Luis Obispo, CA. He received his Ph.D. and M.S. degrees in Industrial Engineering from the University of Central Florida, Orlando, FL, USA. Additionally, he holds M.S. and B.S. degrees in Mechanical Engineering from Cairo University, Egypt. Before joining Cal Poly, San Luis Obispo, Dr. Awwad held several teaching and research positions at the State University of New York at Buffalo (SUNY Buffalo), the University of Missouri, Florida Polytechnic University, and the University of Central Florida. His research and teaching interests include applied operations research, logistics & supply chain, blockchain technology, distribution center design, unconventional logistics systems design, and OR applications in healthcare and the military.