On the Role of Blockchain Technology in Internet of Things

Robin Singh Bhadoria[1], Atharva Nimbalkar[2], Neetesh Saxena[3]
[1]Dept. of Computer Science & Engineering, Indian Institute of Information Technology (IIIT) Bhopal, Madhya Pradesh, India
[2]Dept. of Computer Science & Engineering, Indian Institute of Information Technology (IIIT) Nagpur, Maharashtra, India
[3]Department of Computing & Informatics, Bournemouth University, Poole, United Kingdom
robin19@ieee.org[1] atharvakn@gmail.com[2] nsaxena@ieee.org

Abstract
Blockchain is a database of records, which tracks the history of all transactions and communications between different nodes of a network. It provides a decentralized platform to execute transactions with mutual trust among the participants, while at the same time, eliminating the presence of a central mediating authority. Record of every transaction is stored in the Blockchain and is entirely tamper-proof. Blockchain creates a peer-to-peer network where all nodes get to verify transactions occurring in the network, through a consensus based governance system. It has been used to implement the world's most popular cryptocurrency *Bitcoin.* This is a highly promised technology, which is being adopted and implemented in several domains, such as Internet-of-Things-based systems, healthcare, energy systems, education systems, banking, and many more.

Keywords: Blockchain, Internet of Things, Decentralized, Proof-of-Work, Attacks, Characteristics.

Introduction

The Blockchain (BC) is an encrypted and distributed digital filing system designed to support unalterable and real time transactions. It's a public account of every transaction executed and exchanged between all the concerned parties. The record of each transaction is verified by the consent of a majority of the participants in the system. All participants mutually agree and are aware about the transaction processed along with the identities of all individuals involved in the transaction. The nature of all records in the Blockchain is unalterable. Once a transaction record is put into the Blockchain, it cannot ever be removed. This makes it impossible to make up a transaction that never occurred, which results in a private, secure and decentralized system. The Blockchain technology is a distributed model that has found its applications in many financial and non-financial sectors.

Blockchain is the technology that underpins the world's first and most widely used decentralized cryptocurrency, *Bitcoin.* The participants of Bitcoin, who use this digital currency by sending and receiving Bitcoins in exchange for commodities and services, generate transactions for the Blockchain. These transactions are pushed into a block and once a block is filled, it gets appended to the chain. This happens through a process called *mining.* The users, known as *miners*, solve a mathematical and resource consuming problem, called *Proof-of-Work* (PoW). The node that solves the problem first gets to mine the block to the Blockchain. Through this process, the chain continues as each new transaction record is added to it. One of the significant characteristics of the Blockchain is that the transaction history is available to all involved parties, hence it is impossible to make up any fake transactions. This is an example and a highlight of the Blockchain's secure, decentralized and private nature, which has a great potential to face the challenges posed by the Internet of Things (IoT).

The IoT is a massive network of various computing devices, embedded in everyday objects which are interconnected with each other. The IoT network enables them to transfer and handle the data. These objects can be mechanical devices, digital devices, and even RFID tagged animals [1]. The '*Things'* in IoT are provided with unique identifiers (UIDs) and are embedded with sensors, processors and other communication hardware. According to Gartner, there was an estimated 8.4 billion IoT devices in the world in 2017 and this number is expected to grow as by 2020 more than 65% of enterprises will adopt IoT products. The essence of the IoT is to empower the connected devices to interchange and compute data in order to interact with their environment and make decisions without the involvement of any human-to-computer interactions.

Sensors are a vital part of such devices. With the medium of embedded sensors, these devices gather data from their environment and make decisions, such as air conditioners adjusting their temperature settings, smart watches tracking the daily activities of their users, etc. These sensors continually emit data about the working state of the devices and this data is dumped onto the IoT network. Data is received from a wide range of devices, some of which may differ from others in the nature of their functionalities to a huge extent. IoT collects and integrates this data to perform required analytics and extract valuable information as required. This information is then shared with all the devices connected to the network to enhance their functionalities.

The term "*Internet of Things*" was first used by Kevin Ashton in 1999, while proposing an idea to integrate RFID sensors into supply chain management at Proctor & Gamble [2]. It was used in the context of the idea that a large amount of data present on the internet was made by direct interactions of humans with computers, such as typing, taking a picture or scanning a barcode [2]. This was an emphasis that our physical environment is composed of 'things', which are just as important a part of the internet like ideas and data.

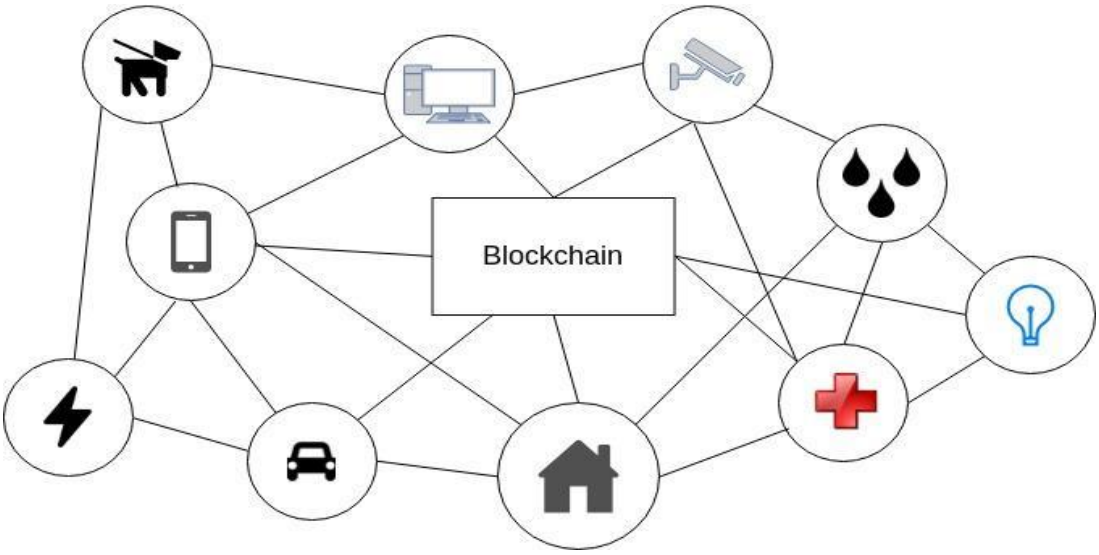

Figure 1: Representing the integration of Blockchain into IoT networks.

As shown in Figure 1, Blockchain can be integrated into an IoT network, where each device acts as a unique participant in the chain. Blockchain acts as a secure and tamper-proof record of all communications and transactions in the network.

Characteristics of Blockchain Technology

Cryptocurrency is not the only sector where Blockchain finds its applications. Any industry that demands resource management and transaction handling can use Blockchain. This technology is

useful in numerous sectors ranging from financial to medical industries. Blockchain has also been implemented in projects, such as a peer-to-peer based solar electricity grid in New York [3] and smart homes that are secured by Blockchain [4]. The core characteristics of Blockchain, such as security, privacy, and immutability offer solutions to many implementation challenges. These characteristics are discussed in detail in this section.

Decentralization: The decentralized nature of Blockchain eliminates many risks that are observed in a centralized database. The distributed scheme does not provide a centralized target for attackers to exploit. Likewise, it does not have any central point of failure that can halt the system if compromised. In Blockchain technology, identical copies of the database file are owned by all nodes present in the network. Whenever a new block is to be added to the chain, mutual consent of all participants is required. This is done by a consensus algorithm, which also ensures the integrity of all copies distributed across the network. A new block of transactions being added is verified by all parties on the basis of the consensus protocol and all nodes update their respective copies of the Blockchain. The consensus algorithm also defends against attacks trying to fork the chain. Thus, the consensus algorithm is responsible for maintaining the legitimacy of all blocks being added to the Blockchain.

In this ground-breaking paper on Bitcoin in 2008, *Nakamoto* proposed a consensus model called Proof-of-Work (POW). This requires nodes that are participating in the consensus process to solve a computationally difficult mathematical puzzle. This is done by brute-forcing random solutions until the problem is solved. This is a low probability process and requires a lot of trial and error to generate the final solution. When a valid proof of work is generated by a node, it gets to push the block to the chain. This process is called as *mining* in the context of Bitcoin and the node is called as a *miner*. The Proof-of-Work algorithm has significant drawbacks, such as the requirement for high computational resources and latency in confirming the transactions. According to Power Compare [5], the amount of electricity consumed by Bitcoin mining has crossed the electricity consumption levels of 159 countries and most countries in Africa. In spite of these disadvantages, the Proof-of-Work algorithm renders the Bitcoin system invulnerable to attacks like the Sybil Attack, Denial of Service, and also solves the double spending problem. Apart from Proof-of-Work, a few other consensus models, such as Proof of Stake, Delegated Proof of Stake, Proof of Burn, Proof of Elapsed Time and Proof of Capacity can also be used in a Blockchain [21].

Immutability: Blockchain maintains a history of all transactions performed by the participants in the network, ever since it was created. As the name suggests, the Blockchain can be visualized as a chain of blocks that are *linked* to each other in a linear fashion. Each block contains information, such as transaction details, timestamps, metadata, block specific details and more. When a block is filled with information, it is added to the Blockchain. The Blockchain running Ethereum cryptocurrency has a block size under 2 KB. The Bitcoin Blockchain has a size of 1 MB per block.
When a hash function meets a set of fixed properties, such as deterministic outputs, pre-image resistance, collision resistance and quick computation, it can be called as a cryptographic hash function. A cryptographic hash function is an essential concept for linking two adjacent blocks in a Blockchain. It generates a fixed output string known as a hash for an input of any length. The NSA developed SHA-256 algorithm generates an output hash of 256 bits. When represented in the hexadecimal system, this becomes 64 digits long. The size of the output hash would be the same if the input was a single character string or even a full sized novel. Every block in the Blockchain has its own unique signature, represented by a hash generated by taking the data inside that block, and the hash of the previous block. Every block in the Blockchain includes the hash of the previous block in its own hash. This is true for all blocks in the chain, the only exception being the very first block, which does not have any parent block included in its hash. It is also known as the Genesis block. Genesis blocks are hard coded into Blockchain clients.

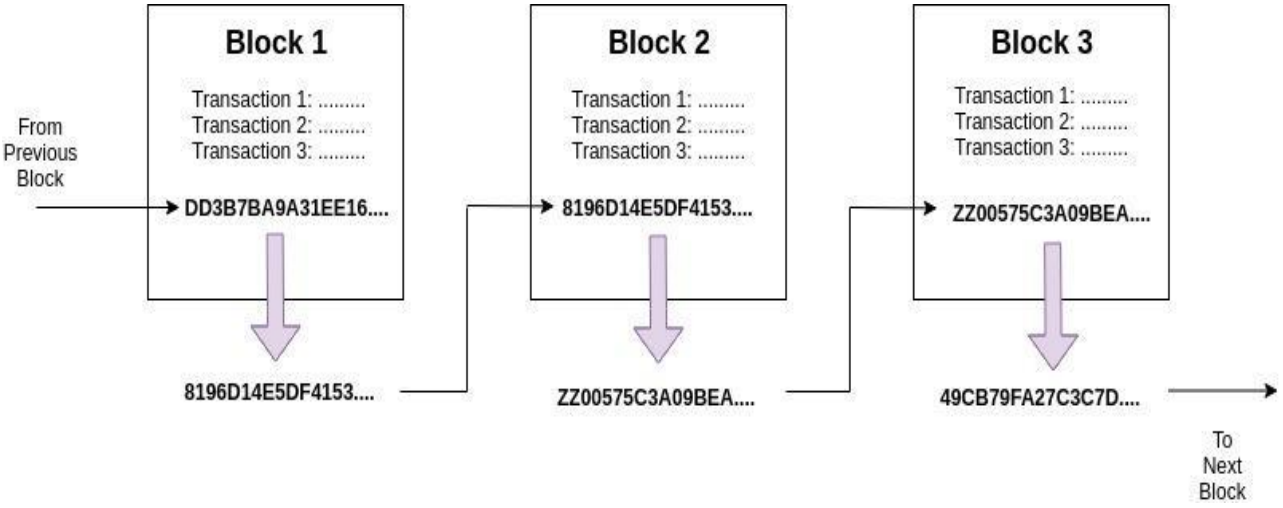

Figure 2: The interlinking of hashes in a Blockchain.

As shown in Figure 2, the hash of block 1 includes transaction details of that block, other information such as metadata or timestamps and importantly, the hash of the previous block. This hash is then included in the hash of block 2. This interlinking of hashes occurs across all the blocks in the entire chain.

The interlinking of hashes across the entire length of the Blockchain makes it infeasible for the data inside the blocks to be tampered with. One of the properties of an ideal cryptographic hash function is that even the smallest of changes in the input, such as changing one letter or the addition or removal of a space result in completely different hashes. Hence, if a malicious entity attempted to change the data in a particular block, it would result in a new signature for that block. As this signature is included in the next block's hash, it has to be recomputed also. Due to all blocks being interlinked, the hash of every single block following the modified block has to be recomputed. Meanwhile, the chain is constantly growing with new blocks being added to it continuously. So, along with computing hashes for the altered blocks, the malicious entity also needs to calculate signatures for all new blocks being added. Doing this would require more computing power than the rest of the network combined. Computing a hash for a block is a resource consuming task is because only a certain type of hash is accepted as valid. For instance, as of date, the Bitcoin Blockchain only accepts a block if its hash starts with 18 consecutive zeros.

In the Proof-of-Work consensus algorithm, for computing a valid hash, the information contained in a block constantly changes until the required pattern is generated in the output hash. As the block contains information, such as transaction details or timestamps, which cannot be changed, a certain segment of data is introduced in the block whose sole significance is to alter the generated hash. This part of the data is called nonce of the block, and can be a collection of any random alphanumeric characters. This process of changing the nonce is repeated on a trial and error basis, until a valid hash is generated. Thereafter, this block is broadcasted by the miner onto the network where all the remaining miners verify the validity of its signature. Once they reach a mutual agreement, the block is added on to the Blockchain. All copies of the Blockchain across the network update themselves. *Hashing* is a resource consuming process and the interlinked hashes make it infeasible to alter any part of the Blockchain. Thus, once a block is added on to the chain, it remains there forever in the exact form that it was added and is immutable.

Consensus based: A transaction can be defined as an exchange of assets between the involved parties. Every transaction must verify its authenticity and validity. Today's traditional transaction systems employ a trusted agent in the system to perform these validations. For example, a money transfer between two individuals can be done through a bank. The bank is responsible for verifying

the identities of both parties through a protocol, such as 3D secure, and ensuring that the money is received by the recipient. The bank acts as a trusted medium in this system. Blockchain eliminates this need for a third party to act as a trusted intermediary for mediating transactions. Instead, the block-chain's working is governed by its underlying implementation and its consensus based system. The consensus protocol defined in the Blockchain allows users to carry out transactions without having a central agency. The responsibility of verifying the validity and authenticity of the assets transferred in a decentralized system, such as the Blockchain is of the consensus algorithm. It defines the rules that make a transaction valid and prevents the same money from being spent twice. The Blockchain follows a governance model similar to the democracy where the truth is decided as whatever being said by a majority of the people. Bitcoin requires miners to submit a valid proof-of-work as required by the consensus algorithm to add their block to the chain accepted by the network.

Once a miner has generated a valid proof-of-work, by spending resources in the form of electricity, other miners have to verify the hash before it is mutually agreed that the block is placed on the Blockchain. Hence, addition of a new block cannot be instantaneous and introduces latency. Due to this, a situation can arise when two miners propagate their computed blocks across the network at the same time. Some miners validate the first block and some miners validate the other one. This results Blockchain to split into two blocks. Out of these two blocks, the valid block is decided based upon which block has a higher proof of work, i.e., which block had utilized more resources to generate its signature. The two chains might also grow individually when the miners keep on adding blocks to either of the chains. The longer chain prevails as it contains more proof of work and is considered as the main chain and the Blockchain again grows independently as one. The longer chain represents a majority of votes as more resources have been spent by miners in creating and adding blocks to this chain, making it longer than the second chain. The other chain is termed as ‘orphan’ and the transactions are ignored. This is how the blockchain removes central entities and uses a democracy based governance system for deciding what is accepted.

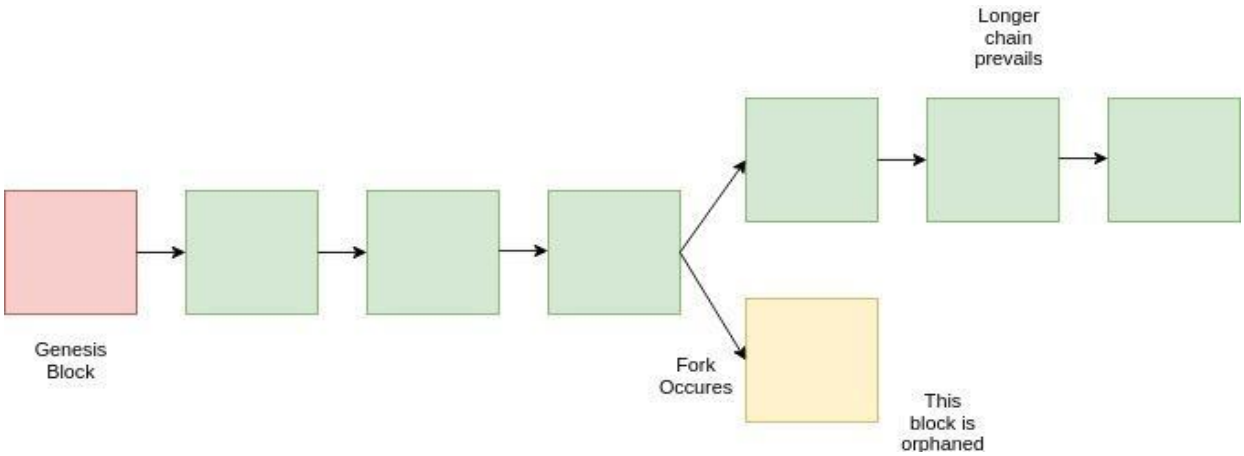

Figure 3: Proof-of-Work in longer chains and orphaned nodes.

As shown in Figure 3, when a split occurs in a Blockchain, the longer chain prevails because it contains more Proof-of-Work and is accepted as the main chain. The blocks in the other chain become ‘orphaned’ and their transactions are ignored.

Accessibility: Based on the accessibility of the Blockchain, it can be classified into two different categories: Permissionless (public) and Permissioned (private). A public Blockchain is open to all and anyone can join as either a participant or a consensus performing authority (miner). Private Blockchain has certain restrictions installed on who can participate in the network. Permission from the enterprise owning the Blockchain has to be obtained prior to joining the network. The Hyperledger Fabric is an example of a permissioned Blockchain.

Block Time and Block Difficulty

Block Difficulty: It is a measure of how difficult it is to find an eligible signature for a new block in terms of time or computational resources. Taking the example of bitcoin, more the number of consecutive zeros required in a hash to become a valid signature, more is the block difficulty. The block difficulty adjusts itself according to the total computational resources available on the network. In bitcoin, if more miners join the network, the total mining capability of the network increases. This new network with more nodes and more mining power will find it easier to generate a valid hash that has to start with five zeros than generating a hash that has to start with ten zeros.
To increase mining difficulty, the threshold value that forms the upper limit of the valid hashes is reduced. That is, this new condition for a hash to be valid will need to have more number of consecutive zeros than before. The Bitcoin Blockchain adjusts its mining difficulty in every two weeks.

Block time: It is defined as the amount of time it takes to mine one block. Bitcoin and Ethereum Blockchain has both expected block times and average block times. Bitcoin's expected block time is 1 block per 10 minutes. The average block time is calculated after **N** blocks have been mined. If the average block time is greater than the expected block time, the block difficulty is reduced. If the average block time is less than the expected block time, the block difficulty is increased.
Bitcoin has a block time of only 1 block per 10 minutes because the Blockchain needs to propagate the newest block across all nodes in the network so that they can update their local copies. This is to ensure proper alignment and synchronization of the Blockchain in the network.

Various Attacks and its Preventions in Blockchain

The IoT devices are vulnerable targets to many cyber-attacks, this is due to the extensive amount of security critical and private data that is used in the network. Most of the IoT devices are lightweight and must employ a major part of whatever computational power they can fathom into their core functionality. This presents a significant challenge in implementing the traditional security algorithms in IoT networks. It is said that the Blockchain has potential to overcome this challenge due to its distributed nature [12]. Due to low bandwidth and low resource availability, integrating Blockchain with IoT is a task with a few challenges.

The IoT relies heavily on a centralized entity for the storage of the gathered data. From a security standpoint, this can lead to threats of distributed denial of service attacks (DDoS), man-in-the-middle attacks, and more. As such attacks exploit the centralized nature of a network, the integration of Blockchain into IoT can provide a new perspective for security measures and possibly solve the vulnerabilities found in a centralized system. Traditional IoT networks are dependent on the server/client communication schemes, which is a centralized model. As stated in other work [6], even for the devices that are only a few feet apart, the connections have to go through the Internet.
In a Blockchain secured IoT network, a decentralized communication network between IoT devices can be implemented, where the Blockchain holds a unique identity of every device. Blockchain can implement a peer-to-peer communication model for large scale IoT networks. It will provide validation and consensus for all transactions. Transaction records between the devices can be stored onto blocks that can be pushed into the Blockchain. The use of permissioned Blockchain is recommended for an IoT network. Integration of the Blockchain into an IoT network from the perspective of security takes the following vulnerabilities into consideration:

Against Sybil Attacks: A Sybil attack is defined as an attempt to control a decentralized network by creating a large number of fake identities. A single user generates and controls these identities that look like genuine users to outsiders. Sybil attacks are difficult to detect as it is not always evident that a large number of accounts are being controlled by a single entity in a network. Having a large number of accounts at disposal grants an undue advantage to the attacking entity. Against a Blockchain, the fake nodes can create unfair control over the network and even manipulate the flow of data or transactions.

To prevent a Sybil attack: Some consensus algorithms in Blockchain like the Proof-of-Work are effective in mitigating an attack because Proof-of-Work requires a node to actually spend energy that cannot be retrieved back. So, it is infeasible to generate a large amount of fake nodes as that would require the expenditure of an equally large amount of resources.

Against Man in the Middle attacks: In this attack, the attacker sits between the two parties involved in a transaction and intercepts all packets being sent in both directions of the network. All data is exposed to the attacker and information can be stolen or tampered with. In certain Blockchain, such attackers can manipulate the transfer of assets or information on the system by manipulating the destination addresses of transactions. It is impossible for the two parties to know the attacker's presence. MITM attacks are quite dangerous as they can allow the injection of malware into the data, as the attacker appears to be a legitimate participant of the network.

Preventing a MITM attack: The methods enabling secure mutual authentication can be used to prevent such attacks from the Blockchain, as the one provided by BSeIn [7]. Mutual authentication with the use of elliptic curve encryption can also be employed for attack prevention [8].

Against Double Spending Attacks: Entities try to use the same money twice. The Bitcoin Blockchain solves this problem by keeping a confirmation mechanism that keeps track of the monetary details of each user in the Blockchain. When a transaction is carried out in Bitcoin, it goes into a pool of unconfirmed transactions. Miners pick transactions from here and add them into the block they are solving. If two duplicate transactions are sitting in the pool and they are picked up by two miners for their respective blocks, whenever one of these blocks in mined into the Blockchain, the other block will discard the duplicate transaction as invalid and the block will go stale. In the case when both of these blocks get mined together, it would result in a chain split and only one of these chains will prevail as the main chain. The other chain containing the duplicate transaction will be orphaned and the transaction will be ignored.

Against DDoS attacks: During a DDoS attack, a network is flooded with an overwhelming number of queries or requests, which results in the network being slowed down or it might even crash due to the large amount of traffic that is directed its way in the form of packets, connection requests, and more.

To prevent a DDoS attack: Blockchain can protect the IoT network from DDoS attack due to its consensus based nature. Whenever miners spend their resources and compute the hash for a block, it gets added on to the Blockchain and validates all the previous transactions once again. The longer the Blockchain grows, the more resistant previous blocks become to any manipulations. To prevent DDoS attacks, CoinParty [9] proposed an idea based on decentralized mixing service.

Against Impersonation attacks: An attacking entity tries to unauthorized operations by disguising itself as a legitimate participant. The Blockchain hides the user's privacy information and prevents impersonation attacks from happening.

Against Routing Attacks: A routing attack aims to intercept a message travelling through the network before it reaches its destination. The messages once intercepted are manipulated before sending it to their destinations. A routing attack can be detected by the network if the message received by one node is not the same as the message received by another. This signifies that the message has been tampered with. The attacking entity can take measures to prevent this from happening by dividing the network into two or more parts and isolating the nodes.

Preventing Routing Attacks: Round Trip Times (RTT) can be used to detect these attacks by recognizing irregular patterns in it. If an attack is detected, the nodes can reset their connections by disconnecting from the older nodes and connecting to other random nodes in the network.
Blockchain when used as a security implementation for IoT networks clearly provides much better security aspects than centralized networks. IoT networks implemented in this fashion can clearly bring many potential solutions to today's problems.

Applications of Blockchain into IoT Networks

The Internet of Things is distributed into many domains, each concerned with a particular type of devices and their applications. This section discusses the potential applications of Blockchain into these subdomains of IoT.

Internet of Vehicles (IoV): The IoV is defined as a distributed network of vehicles and their peripherals that allow the intercommunication and exchange of information between vehicles and entities such as roads, traffic lights, humans, or other vehicles. Significant research has seen the application of Blockchain into IoV. (Huang et al.). In the work [8], the authors have proposed a Blockchain model named LNSC. This model uses elliptic curve cryptography (ECC) for calculation of hash functions. The work in [10] presents a Blockchain based decentralized structure that removes third parties. The verification and authentication of transfer processes are looked after by a security manager network. A Blockchain based reputation system has been devised in the work [11], which is capable of classifying the received messages as true or false based on the sender's reputation scores.
The work in [19] presents PETCON, a localized peer-to-peer electricity trading system. PETCON allows locals transactions of electricity between the electric vehicles connected in a smart grid. It eliminates trusted third parties for the trade of electricity between the vehicles.

Internet of Healthcare things: IoT has already seen a lot of applications in healthcare [12]. IoT in healthcare has provided means for the clinical data in the form of Electronic Health Records (EMRs) to be fed into the system in a portable form for use. The work [13] presents a system, which is defended against selective predicate attacks. The use of Blockchain and IoT in healthcare has provided means for the protection of integrity, maintaining the privacy of patient EMRs, and their immutability.
The work [20] provides a system based on a consortium Blockchain, which instantiates blocks when new healthcare data for a particular patient is created. This block is distributed to all nodes in the patient network and is inserted into the chain only after verification by a majority of the nodes. This achieves a global view of the patient's history in an efficient way. This system exploits the immutable nature of Blockchains and can easily detect changes in healthcare data.

The cloud as a potential platform: In the work [15], the authors discuss fog and cloud as potential platforms for hosting Blockchain. A set of experiments performed on IBM's Bluemix Blockchain show the network latency as a dominant factor in the performance analysis.

Implementations in a smart city network: The work [17] proposes a security framework based on Blockchain for a smart city's communication network. It is shown that a Blockchain based

implementation is resilient to many threats observed in traditional communication networks. Blockchain will provide a common platform open to all smart devices in the city's network, enabling them secure communication on a decentralized environment.

Applications of Blockchain in the industry: The authors of work [18] present a Blockchain Platform for Industrial Internet of Things (BPIIoT). Applications of this platform are described, such as on-demand manufacturing, which enables users to transact directly with machines. This is made possible by the platform by providing Blockchain accounts to every machine and allowing the users to avail manufacturing services on demand. The BPIIoT platform also provides applications, such as traceability, smart diagnostics, and supply chain tracking.

Conclusion

This chapter provides an extensive view for the characteristics of Blockchain with in-depth explanations of its workings and different applications. The significance of Blockchain with IoT is highlighted through examples of cryptocurrencies and other projects. The security issues in the field of IoT are also discussed with implications of Blockchain being a potential solution. It has been observed that integrating the functionalities of Blockchain with IoT networks provides an effective solution to security and data privacy issues. Blockchain also provides mutual trust between the parties and eliminates the possibilities of malicious data manipulations. This chapter also concludes with the fact that private Blockchains are more likely to become feasible solutions in terms of scalability in different devices called *Things* in IoT. There are many areas, such as trust management and data processing, which still needs more attention with respect to implementing the concept of Blockchain.

References

[1] Ejaz, W., & Anpalagan, A. (2019). Blockchain Technology for Security and Privacy in Internet of Things. In *Internet of Things for Smart Cities* (pp. 47-55). Springer, Cham.

[2] Ashton, K. (2009). Internet of Things. RFID journal, 22(7), 97-114.

[3] Siliconrepublic, New York neighbours power up blockchain-based Brooklyn Microgrid. [Access Date: 13 April, 2019]

[4] Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017, March). Blockchain for IoT security and privacy: The case study of a smart home. In *2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops)* (pp. 618-623). IEEE.

[5] Powercompare, Bitcoin Mining Now Consuming More Electricity Than 159 Countries Including Ireland & Most Countries In Africa [Access Date: 13 April, 2019]

[6] Banafa, A. (2017). IoT and blockchain convergence: Benefits and challenges. *IEEE Internet of Things*.

[7] Lin, C., He, D., Huang, X., Choo, K. K. R., & Vasilakos, A. V. (2018). BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0. *Journal of Network and Computer Applications*, *116*, 42-52.

[8] Huang, X., Xu, C., Wang, P., & Liu, H. (2018). LNSC: A security model for electric vehicle and charging pile management based on blockchain ecosystem. *IEEE Access*, *6*, 13565-13574.

[9] Ziegeldorf, J. H., Matzutt, R., Henze, M., Grossmann, F., & Wehrle, K. (2018). Secure and anonymous decentralized Bitcoin mixing. *Future Generation Computer Systems*, *80*, 448-466.

[10] Lei, A., Cruickshank, H., Cao, Y., Asuquo, P., Ogah, C. P. A., & Sun, Z. (2017). Blockchain-based dynamic key management for heterogeneous intelligent transportation systems. *IEEE Internet of Things Journal*, *4*(6), 1832-1843.

[11] Yang, Z., Zheng, K., Yang, K., & Leung, V. C. (2017, October). A blockchain-based reputation system for data credibility assessment in vehicular networks. In *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*(pp. 1-5). IEEE.

[12] Hassanalieragh, M., Page, A., Soyata, T., Sharma, G., Aktas, M., Mateos, G., & Andreescu, S. (2015, June). Health monitoring and management using Internet-of-Things (IoT) sensing with cloud-based processing: Opportunities and challenges. In *2015 IEEE International Conference on Services Computing* (pp. 285-292). IEEE.

[13] 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.

[14] Wang, S., Ooi, B. C., Tung, A. K., & Xu, L. (2007). Efficient skyline query processing on peer-to-peer networks. In *2007 IEEE 23rd International Conference on Data Engineering*(pp. 1126-1135). IEEE.
[15] Samaniego, M., & Deters, R. (2016, December). Blockchain as a Service for IoT. In *2016 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)* (pp. 433-436). IEEE.
[16] Lin, J., Shen, Z., & Miao, C. (2017). Using blockchain technology to build trust in sharing LoRaWAN IoT. In *Proceedings of the 2nd International Conference on Crowd Science and Engineering* (pp. 38-43). ACM.
[17] Biswas, K., & Muthukkumarasamy, V. (2016). 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.
[18] Bahga, A., & Madisetti, V. K. (2016). Blockchain platform for industrial internet of things. *Journal of Software Engineering and Applications*, *9*(10), 533.
[19] 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.
[20] Esposito, C., De Santis, A., 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.
[21] Baliga, A. (2017). Understanding blockchain consensus models. In *Persistent* (White Paper).