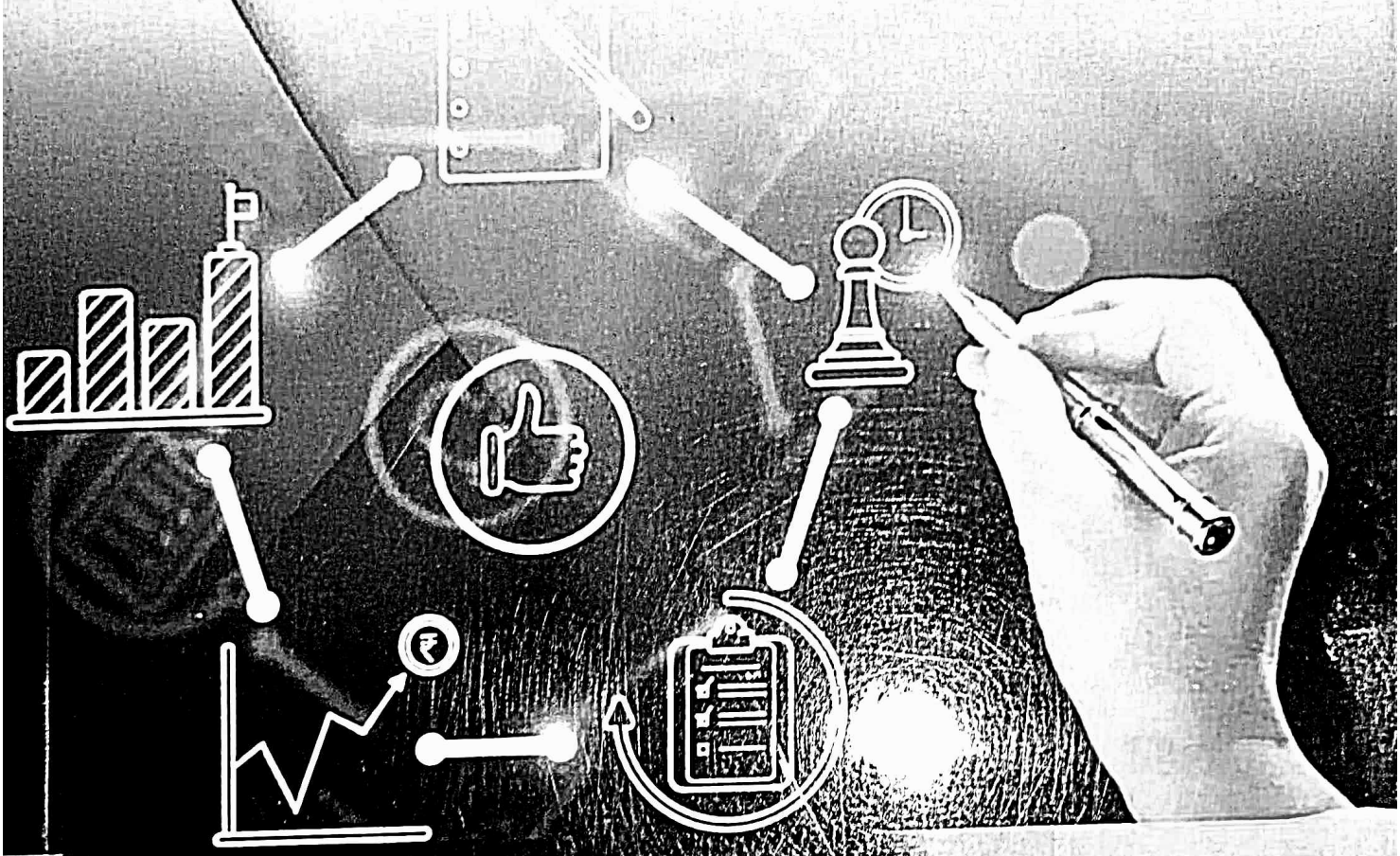
Business Finance
The Changing Scenario



Editors

Dr. Vijay Vrat Arya

Dr. Ajay Kumar Kansal

Business Finance

The Changing Scenario

Dr. Vijay Vrat Arya
M.Com., M.B.A., Ph.D., UGC-NET
Assistant Professor
Department of Commerce
Shaheed Bhagat Singh College,
University of Delhi, New Delhi
Email: vijay.arya@sbs.du.ac.in

Dr. Ajay Kumar Kansal
M.Com., Ph.D., UGC-NET
Assistant Professor
School of Management
Gautam Buddha University,
Greater Noida, U.P.
Email: ajaykansal05@gmail.com

Published by :

New Vision

Publisher, Distributer and Order Supplier
C-1/88, Sanjay Enclave, Rajapuri Road, Uttam Nagar, Delhi 110059
Email: newvision.publish@gmail.com
Website: http://newvision.org.in

BUSINESS FINANCE : The Changing Scenario

Published By : New Vision

Publisher : New Vision
Reg. Office: C-1/88, Sanjay Enclave, Rajapuri Road,
Uttam Nagar, Delhi - 110059
Email: newvision.publish@gmail.com
Website: http://newvision.org.in

Our Book Circulation, Distribution and Marketing Network
Agra, Ghaziabad, Meerut, Noida **(U.P.)**; Jaipur **(Rajasthan)** ; Mehsan
(Gujarat) ; Ferozepur **(Punjab)** ; Hazaribagh **(Jharkhand)** ; Patn
(Bihar) ; Kochi **(Kerala)**

ISBN : **978-81-949466-5-6**

Editors : **Dr. Vijay Vrat Arya**
Dr. Ajay Kumar Kansal

Printed by : **Modern Print Service**
Ram Nagar Market
Gandhi Nagar, Delhi-31

Edition : Ist

Year : 2021

Design & Layout by : ilyas khan

CONTENT

Chapter - 8

IMPACT OF BLOCKCHAIN IN IoT

Gourab Das
Assistant Professor
Department of Commerce
Vidyanagar College, Charashyamdas, South 24 Parganas, West Bengal
Email: 2009gourabdas@gmail.com

ABSTRACT

IoT allows communication to take place globally between human to human, human to things, things to things. As data are shared among different participants in a distributed network there are lots of security issues that are to be handled properly to secure the data. Blockchain technology which is an emerging technology can play a vital role to solve different security issues in IoT devices, the data they retrieve, produce, and process. Apart from security issues, the blockchain has different perspectives. Smart contracts can be created using blockchain technology to make data immutable in a distributed peer-to-peer networking environment apart from cryptocurrencies like "BitCoin". This chapter focuses on the analysis of the Internet of Things (IoT), different perspectives of blockchain technology, integration of IoT with Blockchain, different smart contract applications of it. This chapter also focused on the impact of blockchain on data management, cost-benefit, risk reduction and up-gradation of system.

Keywords: *Internet of Things (IoT), Blockchain, Security, Smart Contract.*

INTRODUCTION

Both of internet of things (IoT) and blockchain are emerging concepts and technology nowadays that can create new possibilities by transforming the existing concepts. Applications can be created by merging them. The decentralized nature of blockchain can serve as a benefit for the IoT. Apart from computers, other gadgets like laptops, TVs, fridges, stoves, electrical appliances, cars, and smartphones are examples of different equipment that can be connected to communication networks (Jesus, *et.al.* 2018.). Smart cities, smart healthcare, and smart home are several types of applications within the IoT domain. Due to the increasing number of IoT applications, the unseen, impenetrable, common collection, processing, and distribution of data in people's private lives are open to serious security and privacy threats. Here blockchain holds the security and

privacy in IoT. Standard mechanisms and protocols are needed to support the huge expansion of IoT to reduce the existing heterogeneity in the field. The adoption of the IoT has been reduced due to this heterogeneity problem. However, apart from heterogeneity and integration challenges trustworthiness is another important factor that needed to be addressed. Nowadays the information provided by the government and financial entities trusted by the public. But we cannot guarantee that the information provided by external entities such as the IoT companies (Reyna *et.al.* 2018). Information can be altered by the untrusted entities according to their interest, hence completely reliable information might not be provided by them. So it is a must to verify whether the information has been modified or not. All the participants must guarantee that the IoT data remains immutable through a distributed service trusted by all the participants. The trustworthiness can be achieved if all the participants can guarantee that the data does not tamper if there is a proper verification mechanism. Moreover, the information provided to citizens by the government should have a system that guarantees data reliability (Reyna et.al. 2018)

Blockchain is the technology that can be leveraged for a peer to peer distributed network to achieve the above purpose.

The chapter has contributed mainly on the study of blockchain, a different perspective of blockchain technology, analysis of IoT, security issues in IoT, and how security issues can be resolved through IoT, the study of Integration of IoT with Blockchain, its related applications, and case studies of IoT and Blockchain Integration. Another section describes the preliminaries of blockchain technology, a brief description of different terminologies of blockchain. It also explains the background of IoT and analytics of IoT and describes the different applications of IoT-Blockchain integration.

BLOCKCHAIN

A blockchain is nothing but an immutable ledger that replaces the concept of the traditional ledger by creating blocks and linking them cryptographically to form an almost unbreakable chain. For example, if a person wants to buy a new house and got the authority of that house then the purchase is a valid transaction and a block will be generated and linked with the previous blocks of other people who have purchased houses earlier. Blockchain is a solution to all the participating nodes in a distributed network to maintain a continuously growing list of data records. A public ledger records all the data, including information after the completion of every transaction. No third-party organization is needed in the middle of blockchain. All nodes in the blockchain maintain every transaction ever completed in Blockchain and share among themselves. All anonymous nodes in blockchain make it more secure for other nodes to confirm the transactions. The first application was 'Bitcoin' that introduced Blockchain technology. In a decentralized marketplace, the participants can make transactions to buy and sell products through Bitcoin.

Figure 1. Blockchain

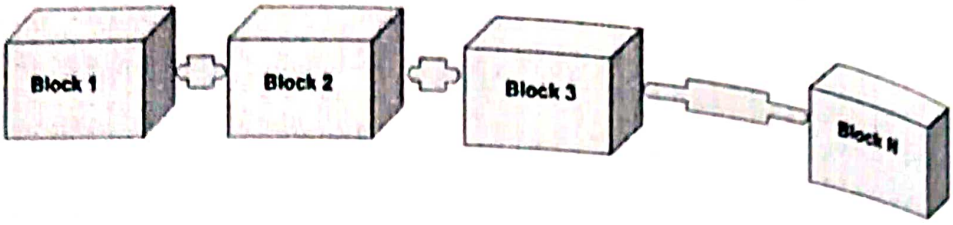


Figure 1 is a diagrammatic representation of blockchain, where N blocks are connected to form the chain.

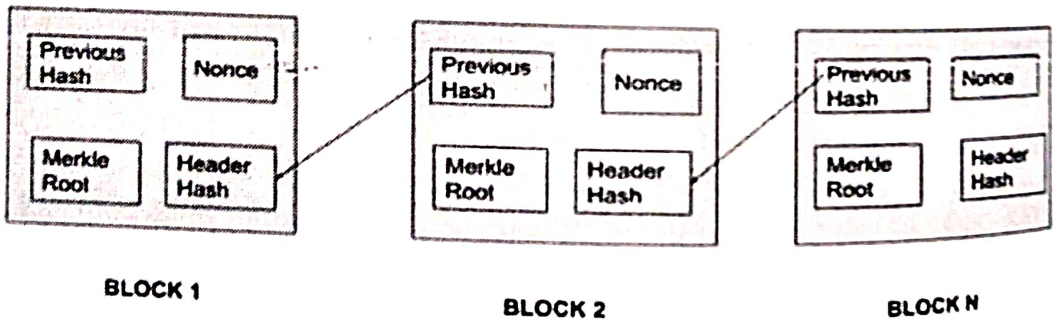
Lakhani in 2017 defined blockchain as *"A blockchain is an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way".*

The evolution of blockchain can be categorized into three generations. Bitcoin was the first application of blockchain and termed Blockchain 1.0. Blockchain 2.0 was used for financial services and contacts. Blockchain 3.0 was introduced to implement applications for the public sector, healthcare and is used for more general purposes.

Blockchain Structure

The blocks are tamperproof. The structure of the blockchain has two portions. They are blockchain headers and transactions. The blockchain header has a) hash value of the block, b)the hash value of the previous block, c) nonce, and d) Merkle root. Another is the transactions, *i.e.* the data stored in the block. *Figure 2.* Shows a diagram of the blockchain header. Each block starting from Block A to Block N all have the four fields in their header. These are as follows:

Figure 2. Blockchain Header



A Hash Balue of the Header: The principal block identifier is the hash value of the header. Each complete node computes after receiving the new block. To identify a block unambiguously the hash is used.

Previous Hash Value: This field holds the hash value of the previous block. It is used to create the chain by linking the blocks with each other.

Nonce: A nonce is a number that is used and validated before generating the header hash value of the current block.

Merkle Toot: This concept of the Merkle tree was introduced by Ralph Merkle. Also known as a hash tree.

- each leaf node of the Merkle tree is labeled with the hash of a data block.

- each non-leaf node of the Merkle tree is labeled with the cryptographic hash of the labels of its child. Merkle tree root is one of the fundamental data structures behind blockchain. Construct a Merkle tree with all sets of transactions and if someone wants to change any transaction then the Merkle root will be changed.

Consensus

The miners need to perform the proof of work (or mining) to generate the hash which will connect the block in the chain. This proof of work is termed a consensus algorithm. Some of the consensus algorithms are described below:

PoW (Proof of Work): Mining is also termed as Proof-of-Work performs critical calculations and generates blocks. In blockchain to mine, one new hash for a block takes 10 minutes. Power Consumption is very good. PoW consensus is open and entirely decentralized. The scalability is excellent in terms of no. of nodes and throughput is limited. The power consumption is very poor and has high latency. It is used in permissionless blockchain and vulnerable to Sybil attack.

PoS (Proof of Stake): PoS concept states that a person can mine or validate block transactions according to how many coins he or she holds.

BFT (Byzantine Fault Tolerance): In BFT tens of thousands per transaction can be possible but cannot accommodate more nodes. Power consumption is very poor. BFT is for permission blockchain. Beyond cryptocurrency, the blockchain is used by a smart contract. A smart contract is based on the state-machine replication protocol where a smart contract is a state machine and across multiple nodes, in a distributed environment its consistent execution is achieved using state machine replication. The state-machine replication protocol belongs to the family of Byzantine Fault Tolerant (BFT).

DBFT (Delegated Byzantine Fault Tolerance): A variant of standard BFT is termed as Delegated Byzantine Fault Tolerance (DBFT).NEO whitepaper describes within a peer-to-peer network there are two types of clients. They are bookkeepers and ordinary nodes. The bookkeepers take place in the consensus process and they are elected by the ordinary nodes.

PoB (Proof of Burn): This consensus algorithm combines both the PoW and PoS and partially overcomes their shortcomings and the miners must prove that they have burned some coins. PoB has no energy costs involved and the cryptocurrency for PoB is a slim coin.

PoET (Proof of Elapsed Time): Intel has developed this consensus protocol which is a lottery-based consensus protocol for Sawtooth Lake, a blockchain-based distributed application platform. Efficiency and fairness are the two approaches that have made this consensus more advantageous than consensus like Pow. This algorithm allows the miner who has the least waiting time to mine the next block.

PoA (Proof of Activity): It is a hybrid version of PoW and PoS. Shortcomings of both the algorithms are overcome with the higher computing power to mine a new block. PoW and PoS are vulnerable to 51% attack, double-spend attack. PoA prevents the chance of the above-mentioned attacks.

Raft-based Consensus: Raft is a consensus algorithm that is designed to be easy to understand. It's equivalent to Paxos in fault-tolerance and performance. The difference is that it's decomposed into relatively independent subproblems, and it cleanly addresses all major pieces needed for practical systems.

Smart Contracts

A contract between two parties without a third party involved in a decentralized networking environment or platform. It is faster, cheaper. A smart contract is one of the applications of the blockchain. It is termed Blockchain 2.0. Suppose supporters will fund a product team for a project. Supporters and the Product team will be agreed upon some protocols. Then those protocols will be written which will be put in a blockchain platform. Once the rules are fixed no one will be able to tamper with the contract. Suppose in the code it is written that after 1 month if the product team does not meet the criteria the supporters will get back their refund from the product team. And as the contract is already written no one can change the rule. The features of a smart contract can be as follows:

- It is distributed
- Code written within the contract will be executed
- Based on the blockchain, if the blockchain is stable and everyone can see the transactions.
- Here "Code is the law"
- Secure peer to peer communication
- Security caused attacks on Ethereum smart contract ("The DAO attack")
- Quorum is a permission version of Ethereum

Different platforms are there to run smart contracts like ethereum, hyper ledger fabric, quorum, *etc. Table-1* compares different blockchain platforms to run smart contracts. Ethereumis a platform that supports smart contracts. It is a blockchain framework where different applications for the IoT devices can be developed using this platform, where the applications are known as DApps.The built-in language to write codes is known as solidity. The EVM is the Ethereum Virtual Machine and the

cryptocurrency is known as ether. Coins are obsolete . The network type is public or private for ethereum. PoW and PoS are the consensuses supported by ethereum. The industry focus is cross-industry. Hyper LedgerFabric is a platform where various projects of blockchain-based on smart contracts are developed. Bitcoin as a cryptocurrency is used here.IBM's Bluemix platform, which is a hyper ledger fabric eases the integration of IoT by offering it as a service. The network type is private for hyper ledger fabric. Network accessibility is permissioned. BFT and PBFT are the different consensuses for it. Dapps are developed on this platform. Cross-industry is the industry focus. Quorum is a permission-based platform where smart contracts can be developed to support only financial industries. Raft based consensus, Istanbul BFT, Clique POA is the consensus for a quorum. Corda (Pustisek & Kos, 2018) is a permissioned blockchain and open-source distributed ledger platform mainly for financial industries where the data is not kept publicly in the blockchain rather it is kept by the financial organizations. Several consensus algorithms can run using notary nodes.

Table 1: Different Blockchain Platforms to Run Smart Contracts

Platform Name	Network Type	Network Access	Consensus	Suitable for IoT	Industry Focus
Ethereum	Public (or private)	Permissionless	PoW,PoS	Yes	Cross-industry
Hyper ledger	Private	Permissioned	BFT,PBFT	Yes	Cross-industry
Quorum	Special version of Ethereum	Permissioned	Raft-based Consensus, Istanbul BFT , Clique POA Consensus	Yes	Financial Service
Corda	open-source distributed platform	Permissioned	Several consensus algorithms can be run using notary nodes	Yes	Cross-industry

INTERNET OF THINGS (IoT) BACKGROUND

IoT visualizes the whole world as a distributed peer-to-peer network where all the nodes can store and share data globally. Examples of IoT applications are smart homes, smart cars, smart water, smart grid, wearable, industrial internet, smart retail, smart supply chain, smart farming, etc. IoT allows communication over the globe where the IoT nodes are not only any smart gadgets but also real-life objects and things.

The 2018 ranking of Top IoT Segmentsstates that according to the latest IoT analytics by 2018 it has been shown that most of the IoT projects identified are on Smart City (367 projects), followed by industrial settings (265) and Connected Building IoT

projects (193). The USA ranked top by making up maximum IoT projects (45%), followed by Europe (35%), and Asia (16%). When looking at individual IoT segments and regions there are large differences can be seen. Europe (45%) ranked top in the Smart City projects, while the USA is an expert in Connected Health (55%) and Connected Car (54%). Smart Agriculture projects (31%) are explored maximum in the Asia Pacific region.

DIFFERENT APPLICATIONS OF INTEGRATING BLOCKCHAIN WITH IoT

Different IoT based front end devices run different applications where blockchain will be there in the backend and serve as a distributed ledger to ensure the trustworthiness in a distributed peer to peer network.

Fast Payment Protocol is a fast payment protocol that is implemented through smart contracts on the ethereum platform to prevent the double-spending attack. Digital payment is done through IoT-based front-end devices and the blockchain in the back end ensures the validity of the payments across the system. However, the blockchain is vulnerable to double-spending attacks.

Traceability System for Agriculture Product (Pustisek & Kos, 2018)is a traceability system for agriculture products based on IoT and Blockchain technology analyzes food quality problems. IoT technology is more reliable than the traditional, manual recording of data and the blockchain is more credible than the existing traditional database.

Architectures for IoT based Application using Blockchain: it proposes 3 different architectures for IoT frontend blockchain applications. The applications are developed on the ethereum platform as bitcoin is obsolete for micropayments due to time constraints to mine a block.

Trust List (Kataoka, Gangwar, & Podili, 2018): is a Trust-List to a blockchain network. It represents the distribution of trust among IoT-related stakeholders like service providers, developers and network operators, and autonomous enforcement of IoT traffic provided by Software-Defined-Networking (SDN) and blockchains.

MioT Framework is a general framework and solutions have been proposed to find out the origin of ownership for Medical IoT devices. MioT plays an important role in the healthcare sector. It is essential to trace out whether the MioT device is original or counterfeited as one device can be used by several patient parties during its lifetime. The framework is implemented on the Ethereum platform where two smart codes are executed. One is a manufacturer smart contract and another is IoT smart contract. The codes will be executed without any third-party involvement or central authority control.

Implementation of Smart Contracts for Blockchain-based IoT Applications: An application for buying and selling data (measurements) of IoT sensors related to weather. The huge amount of data collected by IoT sensors can be shared to achieve economic scalability and to reduce costs. Here an IoT application is developed which is

based on sensing-as-a-service (s2aas) business model and implemented through blockchain. Two Dapps i.e. two smart contracts are deployed and interacted over ethereum blockchain. There is a front end or the interface between the users and the blockchain which displays the lists of sensor data, the time interval for which to buy the selected data, etc.

Safe Farming: IoT based prevention system is built to protect the crop from the animal's attack. IoT sensors report any disturbance to a Repelling and Notifying System (RNS) in the field, which produces ultrasonic waves for animals thus they can leave the field. Farmer Management System (FMS) maintains a blockchain that generates a new block wherever an attack happens and this blockchain shares all the data related to different attacks in the field.

Privacy in Blockchain-enabled IoT Devices: This is an artificial guideline for blockchain-enabled IoT devices that is being proposed. Applications are built on the ethereum platform. The applications are not only financial applications but also other decentralized applications. Here the authors have described their work by illustrating an example of CCTV, where the CCTV camera is controlled by the smart contract. The smart contract is created by the manufacturer and the contract will run when the owner rents the camera to the renter for a particular duration of time. When the renting duration will get over the contract will stop running and the owner will get some benefits.

AutoPay (Huckle *et.al.* 2016) is an auto-pay service system that provides security and trust by embodying an authorized human being. This personification is done through smart contracts and their blockchain interface. Autopay service is acting as an autonomous payment device. Autopay service can initiate several features in an embedded system; for example in a car's display. It can be integrated with an application called 'Journey Planner'. Whenever a person enters his/her destination data in the journey planner, it checks the vehicle's essential data and proposes the best route to the destination. If the car is low on fuel, it will search a route where the person can find a gas station on the way. The payment for fuel can also be done through the smart contract feature of the auto-pay service. It can also be integrated into a person's smartphone's AI application (like Apple's Siri) to get information about parking availability at the destination. It can also integrate a smart grocery management application where ordering, payment, and delivery can be coordinated through this auto-pay service block chain interface. Access to the system can be given to another person with limited privileges. For example, the authorized person can give his/her car's auto-pay service to his/her children but auto-pay service may not work in some specified cases. The authorized person can also quickly find out the unauthorized transactions, tried by his/her children in the immutable transaction history on auto pay's interface to the car's blockchain ledger.

Food Supply Chain Traceability System (Tian, 2017) is a system in a distributed network for real-time food tracing which is based on HACCP (Hazard Analysis and Critical Control Paths), blockchain, and IoT. This system provides a distributed platform

where all the supply chain members communicate with each other with openness, transparency, security, and reliability. As scalability is one of the main disadvantages of blockchain, a new concept BigChainDB is being proposed which combines the key characteristics of distributed databases like high throughput, low latency, and high capacity with the key characteristics of blockchain-like Decentralized control, Immutability, and Creation & movement of digital assets.

CONCLUSION

Internet of Things (IoT) devices have become smart and autonomous and they can communicate over a distributed decentralized network. IoT applications are generating a huge amount of data and securing those IoT data is a concern. Here blockchain technology plays an important role. As blockchain achieves trustworthiness among the participants in a decentralized distributed network by providing the means of verifying the immutability of the data, it can be integrated with IoT to secure the IoT data. This chapter tried to show the Blockchain-IoT integrations, different applications of it. It is identified different security attacks in IoT and also addressed how they can be resolved using blockchain technology. The application of blockchain technology allows enterprises to manage data on edge devices in an IoT system, reducing costs associated with IoT device maintenance and data transfer. It reduces the risks of managing data because there is no centralized data repository and the ledger is not vulnerable to cyber-attacks.

REFERENCES

1. Alblooshi, M., Salah, K., and Alhammadi, Y., (2018). *Blockchain-based Ownership Management for Medical IoT (MIoT) Devices.* In 2018 International Conference on Innovations in Information Technology (IIT) (pp. 151-156). IEEE.

2. Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y. and Muralidharan, S., (2018). *Hyperledger fabric: a distributed operating system for permissioned blockchains* (2018). arXiv preprint arXiv:1801.10228.

3. Brown, R.G., Carlyle, J., Grigg, I., and Hearn, M., (2016). *Corda: an introduction.* R3 CEV, August.

4. Dagher, G.G., Mohler, J., Milojkovic, M., and Marella, P.B., (2018). Ancile: *Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology.* Sustainable cities and society, 39, pp.283-297.

5. Hao, Z., Ji, R., and Li, Q., (2018), *FastPay: A Secure Fast Payment Method for Edge-IoT Platforms using Blockchain.* In 2018 IEEE/ACM Symposium on Edge Computing (SEC) (pp. 410-415). IEEE.

6. Hong, W., Cai, Y., Yu, Z., and Yu, X., (2018), *An Agri-product Traceability System Based on IoT and Blockchain Technology.* In 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN) (pp. 254-255). IEEE.

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

8. Iansiti, M., and Lakhani, K.R., (2017). *The truth about blockchain.* Harvard Business Review, 95(1), pp.118-127.

9. Iqbal, R., and Butt, T.A., (2020). *Safe farming as a service of blockchain-based supply chain management for improved transparency.* Cluster Computing, pp.1-12.

10. Jesus, E.F., Chicarino, V.R., de Albuquerque, C.V. and Rocha, A.A.D.A., (2018). *A survey of how to use blockchain to secure the internet of things and the stalker attack.* Security and Communication Networks, 2018.

11. Kataoka, K., Gangwar, S., and Podili, P., (2018), *Trust list: Internet-wide and distributed IoT traffic management using blockchain and SDN.* In 2018 IEEE 4th World Forum on the Internet of Things (WF-IoT) (pp. 296-301). IEEE.

12. Khan, M.A., and Salah, K., (2018). *IoT security: Review, blockchain solutions, and open challenges.* Future Generation Computer Systems, 82, pp.395-411.

13. Nakamoto, S., (2008). *Bitcoin: A peer-to-peer electronic cash system.*

14. Papadodimas, G., Palaiokrasas, G., Litke, A., and Varvarigou, T., (2018), *Implementation of smart contracts for blockchain-based IoT applications.* In 2018 9th International Conference on the Network of the Future (NOF) (pp. 60-67). IEEE.

15. Pouraghily, A., Islam, M.N., Kundu, S., and Wolf, T., (2018), *Privacy in Blockchain-Enabled IoT Devices.* In 2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI) (pp. 292-293). IEEE.

16. Pustišek, M., and Kos, A., (2018). *Approaches to front-end IoT application development for the ethereum blockchain.* Procedia Computer Science, 129, pp.410-419.

17. Reyna, A., Martín, C., Chen, J., Soler, E., and Díaz, M., (2018). *On blockchain and its integration with IoT. Challenges and opportunities.* Future Generation Computer Systems, 88, pp.173-190.

18. Tian, F., (2017), *A supply chain traceability system for food safety based on HACCP, Blockchain & Internet of things.* In 2017 International Conference on Service Systems and Service Management (pp. 1-6). IEEE.

19. Yli-Huumo, J., Ko, D., Choi, S., Park, S., and Smolander, K., (2016). *Where is current research on blockchain technology?-a systematic review.* PloS one, 11(10), p.e0163477.