ISSN No:-2456-2165

Study on Integration of Blockchain and IoT in Smart City Applications

Indu Joseph
Department of Computer Science
Datta Meghe College of Engineering
Airoli, Navi Mumbai, India

Dr. S. D. Sawarkar
Department of Computer Science
Datta Meghe College of Engineering
Airoli, Navi Mumbai, India

Abstract:- Blockchain is a distributed ledger and its data immutability property solves various data security issues. Every participant has a copy of data and validates it, hence removing a third party to verify the correctness of data. Smart contract is a programmatically written set of rules that reside on the blockchain which allows the execution of business logic when certain conditions are met and brings in automation with trust and safety for the data. This paper focuses on understanding blockchain, its features, challenges, types, and how its integration can be an advantage in IoT. The challenges faced in the integration of Blockchain and IoT is summarized and a study on the existing IoT-blockchain applications for smart city is done.

Keywords:- *IoT; Blockchain; Distributed Ledger; Smart Contract; Smart City.*

I. INTRODUCTION

IoT visualizes a connected world, where things can transfer data and interact with each other without any human interaction. Currently, most IoT systems rely on the centralized server-client paradigm, connecting to cloud servers through the Internet. In a centralized server/client model, the server connects and authenticates all devices and transactions in the network. The data involved cannot be trusted and there is complete dependency on the server. Blockchain technology offers a distributed peer-to-peer decentralized solution [1] and trustworthiness through data immutability. All participants in the network are involved in authenticating the data as each of them has a copy of the blockchain and any new data to be added needs to be approved based on a consensus algorithm and any smart contract added.

In this paper, the blockchain technology, smart contracts and its integration for IoT data is analysed. Main contributions of the paper are:
1. Study on Blockchain technology – features and challenges
2. Understanding types of Blockchain
3. Integration of Blockchain and IoT
4. Survey on existing blockchain-IoT applications in Smart City

II. BLOCKCHAIN OVERVIEW

Blockchain is a digital ledger where transactions are recorded with transparency and shared across all the nodes in a distributed network. Like a physical ledger, the existing records cannot be edited and needs to add a new entry for each transaction. Since this ledger is shared across all participants, the transactions cannot be added without reaching an agreement among them. In 2008, Satoshi Nakamoto with the concept of Bitcoin [2], described how blockchain technology could be used to maintain the order of transactions and avoid the double-spending problem.

Blockchain can be considered as a chain of blocks, containing transactions. Transactions are the actions performed by the participants in the network. A small set of transactions together form a block. On comparing to the physical ledger, a block can be compared with a page in the ledger book. Each block is having information on a transaction along with a signature made from its own and its previous block hash. The only exception is a Genesis block, which is the initial block of a blockchain. This does not have any previous block to cryptographically create a signature. The participants share these blocks and make sure they are in correct sequence and have not been tampered.

When a transaction needs to be added to the chain, all the members in the network validate it and a consensus algorithm [4] is used to come to an agreement. These consensus protocols make sure all the nodes on a network are in sync with each other. This guarantees the data can be trusted making it a self-auditing system, removing any third-party involvement to verify data. A unique signature created from the previous block hash along with the transaction data is appended to the chain of blocks in all nodes. In absence of this consensus mechanism, the blockchain is unable to track the order of transactions and the state in each node might be different leading to unstable data in the network. All these fundamental features of blockchain are illustrated in Fig1.

The Blockchain-IoT combination is a powerful use case to solve the security issues in IoT [3]. Blockchain being a distributed ledger gives an immutable source of truth when integrated in IoT. Like a physical ledger, the transactions can only be appended, not modified. It eliminates the central server concept of IoT and allows the data to flow through the blockchain distributed ledger for each transaction with appropriate authentication hence addressing security and privacy issues in IoT. Data correctness is verified by all participants in the network as each one of them has a copy of blockchain agreed upon a consensus algorithm. Blockchain characteristics that can be an advantage for IoT include immutability, decentralization, and better security [5].

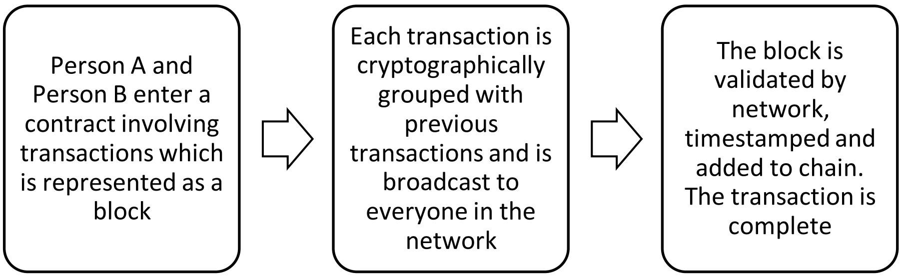

Fig1 Working of Blockchain

A. SMART CONTRACT

A smart contract is a set of rules under which the blockchain participants carry out some transactions. These can be considered as the simplest form of decentralized automation as it automatically performs tasks once the condition is met. The smart contract code is stored on the blockchain, and each contract is distinguished by a sole address, and for users to operate with it, they send a transaction to this address. The correct execution of the contract is enforced by the blockchain consensus protocol [6]. Smart contracts offer improvements such as cost reduction, speed, precision, efficiency, and transparency. Blockchain is fitting for storing smart contracts because of the technology's security and immutability [7]. They speed up blockchain, reducing the delay of mining.

A smart contract is deterministic which guarantees that the same input given to the contract will invariably give the same output. If these are built in a non-deterministic way, the smart contracts can give different states in different nodes and will fail the blockchain to come in agreement. Since the contract is placed on the blockchain, all participants on the network can inspect the rules and each one of them holds a cryptographically signed message of agreement execution. To edit any rules in contract, consensus needs to be achieved in the network.

B. CHALLENGES

Even though blockchain has many promising use cases, it is adopted only in a confined manner. The major challenges which pull back blockchain from being used extensively are discussed [8] and can be consolidated as below

- *Scalability*: When the number of transactions increases, there is a remarkable slowdown seen. For real time applications, blockchain is expected to speedup to become viable.
- *Interoperability*: Most of the blockchains work in silos and do not communicate with other networks. They are incapable of sending and receiving information between blockchain based systems, which leads to a major concern for large scale applications [9].
- *Complexity of Blockchain*: Blockchain application cannot be readily replicated and reused across use cases. Lack of technically proficient people for blockchain development is additionally a hurdle. Blockchain as Service decreases this complexity by enabling customers to use third-party service providers who manage infrastructure and requirements for the network. The client can customise the blockchain as per their demands and implement smart contracts.
- *The Majority Attack (51% Attacks)*: When a group of miners takes control of more than 50% of a network's mining power, it blocks the transactions produced by the rest of the network and can define a new transaction history. To face this situation Ethereum came up with a hard fork where a new blockchain is created by breaking the existing blockchain.
- *Integration Cost:* Time and money involved in incorporating this technology are higher. The cost of establishing a distributed network with blockchain integration and lack of expertise in this technology have added cost to this.
- *Lack of standardization:* There are a large number of blockchains created worldwide, which again can only be used as silos. The blockchain and smart contracts need to have some common standard which can bring in more integration among different systems.

III. TYPES OF BLOCKCHAIN

Blockchains are categorized [10] as public, private, and federated depending on the network type and actions permissions to a user. Table1 gives an overview of each Blockchain type, its strengths and challenges faced, and a framework implemented in this model.

IV. BLOCKCHAIN-IOT INTEGRATION

The current IoT system has centralized communication models. All devices are connected through cloud servers that need huge processing and storage capacities [11]. The IoT data that is transferred over the internet irrespective of its location brings in security and privacy concerns. Apart from these, there are other challenges like interoperability, lack of standards, legal and regulatory issues, and other developmental issues [12]. The single point expensive server that manages data, interacts with other client devices in the network. This data cannot be trusted due to security threats during data transfer. A decentralized approach to IoT network would solve trust issues and data vulnerabilities.

ISSN No:-2456-2165

Blockchain technology is a great solution to settle scalability, privacy, and reliability concerns in IoT. With the peer-to-peer approach of blockchain, more resilient environment is created eliminating single points of failure. The cryptographic algorithms used by blockchain would make consumer data more private [13] and immutable. Each block in the blockchain contains a hash formulated using the preceding block hash, hence prevent any tampering or removal of a block from the chain. Any data alteration to data is appended as a novel transaction delivering transparency and protection from attackers. Blockchain can store encryption keys to make the transfers more confidential. IoT device transmits encrypted information utilizing the public key of the destination device, which is then saved in the blockchain network. Then the sender encrypts the message accepting the public key of the receiver, in this way, only the receiver will be able to decrypt the conveyed message applying their private key. The Blockchain technology advancement in the IoT industry can ensure the proper management of data at various levels. Table2 summarizes how blockchain is a savior for the issues faced in IoT.

TABLE 1: TYPES OF BLOCKCHAIN

Model	Characteristics	Strengths	Challenges	Framework
Public Blockchain	Anyone can join the network and participate in consensus process. All transactions are fully transparent	Full decentralization High security Transparency	Slow Anonymity Low trust	Ethereum
Private Blockchain	Permissioned blockchains Needs the participants consent to join the networks. Transactions are private and are only available to participants that have been given permission to join the network	Confidentiality Authenticated Parties Privacy Faster Less Expensive	Centralized Single Point failure Lack of scalability Integration with legacy systems	Multichain
Consortium Blockchain	Hybrid of Public and Private Blockchain. Blockchain is being shared by different nodes like public, and participants who can access the Blockchain is restricted as in Private Blockchain.	Partial decentralization Confidentiality Authenticated Parties Privacy Faster Less Expensive	Fragmentation of applications Lack of scalability Integration with legacy systems	Hyperledger Fabric
Blockchain as a Service	Service provider hosts a cloud to deploy blockchain applications Service Provider manages the blockchain network while customer defines business logic	Flexibility Scalability Complexity Reduction	Environment cost Lack of regulation creates risky environment	AWS, Azure, Bluemix

TABLE 2 BLOCKCHAIN TO SOLVE ISSUES IN IoT

Blockchain feature	Issue in IoT	IoT with Blockchain
Decentralization	Central Server	No single point failure
	High costs for installing and maintaining servers	Cost savings and scalability
Cryptographic algorithms	Data cannot be trusted	Data is secure and confidential
	Cyber attacks	Immutable data
	Single thread of communication which can be intercepted	No man-in-the-middle attacks
Distributed Ledger	Centralized authority to manage data	Tamper-proof record of data managed in all nodes
Immutability	Data security and privacy Issues	Once data is recorded and stored it cannot be altered

A. Challenges of Blockchain in IoT

Blockchain was planned and designed for a network with powerful computers, and when we try to integrate this in IoT, this is far from the reality. Some of the challenges identified while incorporating blockchain are listed below.

- *Scalability*: The size of Blockchain ledger leads to centralization as it grows over time and required some record management. The number of transactions per block can be increased, resulting in fewer blocks within the chain and hence boost scalability in the blockchain. Sharding [19] is one of the proposed solutions for scalability issues in blockchain, which is to split the overheads of processing transactions among multiple, smaller groups of nodes. The blockchain network can be divided vertically into different shards or can bring a division in transaction validation and block construction. Transaction validation is much slower, so more nodes need to be assigned in this division. Hence the nodes can perform the validation and block construction without overloading the network. The blockchain can have a global state and shards need to update states, which can be done securely using consensus algorithm. The transactions will be addressed to the nodes based on the shards they affect. All the nodes work in parallel, thereby diminishing the overall time taken
- *Processing power and time*: Encryption algorithm needs to be implemented in each block involved in the Blockchain. With different computing capabilities, we cannot demand the same speed for this algorithm across all devices in the network. For solving this problem of high computational power requirement, a centralized-decentralized combined architecture is proposed [14] where intermediate servers can be used between IoT devices and the Blockchain. The block contains the principal contract with reference information to where the absolute data is saved, reducing the overall size of blockchain in the network. A state channel establishes a communication channel between participants so that state updates and transaction processing can be offloaded to them. A smart contract locks a part of the blockchain state enforcing the business logic among the participants. The participants perform transactions amongst each other (without the involvement of blockchain) and the final state is submitted directly to the blockchain. The smart contract ensures that the states of transactions are updated and open the locked portion of the blockchain state. This bypass the association of the miners, hence, saves the processing power and time. Subchains are proposed as a layered solution above the existing Bitcoin architecture [15] reducing the average first confirmation time of transactions. This architecture has a root chain and a set of child chains forming a hierarchical structure.
- *Storage*: Blockchain with the decentralized approach eliminates the need for a central server to store transactions and device IDs. The ledger must be stored on the nodes themselves, and the ledger keeps increasing as time passes by appending the transactions. IoT devices like sensors have low storage capacity, hence storing large blockchain becomes a major difficulty. To achieve better throughput, it becomes important to store a minimum data footprint. The signature that is stored in each block can be abbreviated using more efficient cryptographic algorithms. An architecture [19] to exclude IoT devices in the blockchain and alternatively, to request access control information from the blockchain on behalf of the IoT devices is proposed. It defines a new node called the management hub and involves a single smart contract that defines all the operations allowed in the access control system.

V. BLOCKCHAIN-IOT APPLICATION FOR SMART CITY

The various possible applications of IoT with blockchain technologies are highlighted [15][16]and feasibility analysis of blockchain use cases [17] is done which helps understand the necessity for the development of blockchain. Three use cases in Smart City are chosen to understand how blockchain can add value to it and are summarized below based on various sources [27-31]

A. Suuply Chain and Logistics

A supply chain network involves many stakeholders such as suppliers, producers, clients, brokers, and so on. An ideal supply chain requires end-to-end visibility, trust, and control. Due to the involvement of multiple stakeholders, information sharing becomes a major challenge. Due to the lack of transparency in the current supply chain and logistics, Blockchain-IoT combined can help enhance the reliability and traceability of the information [18]. An approach is to make the vehicles IoT-enabled to track the movement throughout the shipment process. IoT sensors like motion sensors, temperature sensors, pressure sensors for the connected devices provide real time updates on the goods and these are stored in the blockchain. Once the data is saved on the Blockchain, Smart Contracts gets fired allowing the listed stakeholders to access the information. Supply chain participants prepare for transshipment based on the requirement and run transactions. Table3 summarizes a few products available in the market [28][29] in the Supply chain use case.

TABLE 3 SUPPLY CHAIN - BLOCKCHAIN PRODUCTS

Area	Primary Purpose	How blockchain helps	Product in Market
Food Industry and Raw Materials	Scalability in food safety Complying food safety standards Gives the details of where raw materials for the product came from	Smart Contracts Immutable data in shared ledger Transparency and Trust	Walmart, Zeto, FoodGuardians, Dorae, Ripe.io
Diamond	Track the journey of diamonds from mine to cutter to polisher to jeweller	Data immutability Traceability	De Beers, Everledger
Drug	Fight counterfeit goods Production and shipment of drugs	Transparency and Traceability Smart Contracts for safety	BlockVerify, Modum
Product Tracking	Help consumers get transparent information of product throughout its journey	Transparent transactions and immutable data	Provenance, OriginTrail, ConsenSys, Kuovola Innovation, Riddle & Code, TradeLens
Logistics	Realtime tracking of cargo and inventory Reduce paper-based documentation	Traceability Ledger technology	CargoCoin, Tradeline, Cloud Logistics, Chronicled, ShipChain, Koopman

B. Smart Home

More and more data are collected and shared by instances of different IoT devices within a smart home, bringing more concern about privacy and security. Access control management and data sharing [20] in smart home data are analyzed. With a large amount of IoT data, potential challenges in creating a data marketplace are considered with the integration of blockchain [21][22]. An IoT architecture using three components private blockchain, public blockchain, and smart contract is proposed in consideration of these primary challenges. A smart home based on IoT-Blockchain architecture [23] brings advantages like data privacy, trust access control, and high extension ability. Blockchain brings transparency in IoT systems and data cannot be modified once added. Table4 consolidates a few products in the market available for the Smart Home use case.

TABLE 4 SMART HOME - BLOCKCHAIN PRODUCTS

Area	Primary Purpose	How blockchain helps	Product in Market
Home Security	Biometric data security Access Control	Data immutability	Telstra, Walmart
Sharing Economy	In home rentals, owners can remotely control and authorise access to guests Secure data	Smart contracts Access Management Data immutability	IoTeX and NKN Slok.it

C. Healthcare

The primary concern in smart healthcare is the data privacy and security due to the involvement of multiple stakeholders. Data generated through IoT devices in healthcare operations, help in effective decision making and better drugs and equipment management. Blockchain contribution to healthcare can be broadly divided into four areas: Firstly, it can improve the interoperability of different healthcare platforms and supply chains [24]. Secondly, patients can store and assign access control for their lifelong fitness records and medical history. Thirdly, it can give trusted datasets and reduce data archived under the control of one department, thus improve medical research and clinical trials. [25]. Another area where healthcare-blockchain can contribute is claim management and prevent insurance frauds. The charges for various healthcare services can be communicated transparently, thus preventing any type of deception.

Internet of Healthy devices is a subset of IoT that includes wearables, sensors and devices that provides information regarding activity, sleep and cardiac function. The IoT devices collect sensory data from devices and these need to be stored and accessed securely. Each of these areas is studied and the challenges in securing healthcare data [26] are analyzed. Table5 consolidates these use cases and gives an overall picture of how blockchain helps Healthcare IoT data.

TABLE 5 HEALTHCARE-BLOCKCHAIN PRODUCTS

Area	**Primary Purpose**	**How blockchain helps**	**Product in Market**
Medical Supply Chain Management	Know about the drug/product - Monitor and track raw materials to the production of drugs to different stages of storage and distribution Ensure drug/product is not tampered	Ledger keep recording the data every phase and is immutable Guarantees full transparency in shipping process. Tracks the people who handle them and validate the product	Chronicled, iSolve, Blockpharma, Tierion, MediLedgerProject,
Patient Data Management	Securely store patient data and prevent any unauthorized access to this data	Keep an immutable and transparent log of all patient data Conceal the identity of patient with secure codes that can protect the sensitivity of medical data. The decentralized nature allows to share data quickly and safely	Patientory, Medicalchain, BurstIQ, Factom, Guardtime, Robomed
Research and Clinical Trials	Allow anyone to validate a clinical trial and provide proof of existence for the data	Ensure data stored on ledger is not tampered and are secure Transparent and is accessible to everyone	Clinico, Curisium, SimplyVital health, Nebula Genomics, Encrypgen
Healthcare Claims Management	Eliminate the need of third-party handling claims Save time and cost for payers and providers	Standardisation with set of smart contracts Immutable data	PokitDok, Coral Health, HSBlox, Gem, Solve.care

VI. CONCLUSION

With the rapid growth in the number of connected IoT devices, many challenges arise on the security and trust of data. Blockchain technology can improve IoT systems by eliminating any intermediary parties to verify data, hence reducing the cost as well. Distributed ledger technology helps to overcome centralized architecture challenges and store data securely, hence build trust within the network. However, the characteristics of standard blockchain need to be modified due to the IoT requirements like storage and scalability. The various challenges faced in IoT-blockchain integration are discussed and potential solutions proposed are also reviewed. The various existing applications for the IoT-Blockchain convergence in Smart City use cases are surveyed and studied to understand the uniqueness covered in each implementation. Future research should focus on developing frameworks that can support diverse application requirements rather than introducing application specific frameworks.

REFERENCES

[1]. Samaniego, Mayra, and Ralph Deters. "Blockchain as a Service for IoT." 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). IEEE, 2016
[2]. Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008).
[3]. Christidis, Konstantinos, and Michael Devetsikiotis. "Blockchains and smart contracts for the internet of things." Ieee Access 4 (2016): 2292-2303.
[4]. Atlam, Hany F., et al. "Blockchain with internet of things: Benefits, challenges, and future directions." International Journal of Intelligent Systems and Applications 10.6 (2018): 40-48
[5]. Huang, Zhiqing, et al. "A decentralized solution for IoT data trusted exchange based-on blockchain." 2017 3rd IEEE International Conference on Computer and Communications (ICCC). IEEE, 2017.
[6]. Reyna, Ana, et al. "On blockchain and its integration with IoT. Challenges and opportunities." Future Generation Computer Systems 88 (2018): 173-190.
[7].] D. Houlding, Healthcare Blockchain: What Goes On Chain Stays on Chain, 2017. Available online: https://itpeernetwork.intel.com/healthcare-blockchain-goes-chain-stays-chain/.(Accessed 1 February 2018).
[8]. Lin, Iuon-Chang, and Tzu-Chun Liao. "A survey of blockchain security issues and challenges." IJ Network Security 19.5 (2017): 653-659.
[9]. Casino, Fran, Thomas K. Dasaklis, and Constantinos Patsakis. "A systematic literature review of blockchain-based applications: current status, classification and open issues." Telematics and Informatics 36 (2019): 55-81.
[10]. Niranjanamurthy, M., B. N. Nithya, and S. Jagannatha. "Analysis of blockchain technology: pros, cons and SWOT." Cluster Computing 22.6 (2019): 14743-14757.
[11]. Zheng, Weilin, et al. "NutBaaS: A Blockchain-as-a-Service Platform." IEEE Access 7 (2019): 134422-134433

[12]. Khan, Minhaj Ahmad, and Khaled Salah. "IoT security: Review, blockchain solutions, and open challenges." Future Generation Computer Systems 82 (2018): 395-411.

[13]. Singh, Madhusudan, Abhiraj Singh, and Shiho Kim. "Blockchain: A game changer for securing IoT data." 2018 IEEE 4th World Forum on Internet of Things (WF-IoT). IEEE, 2018.

[14]. Rifi, Nabil, et al. "Towards using blockchain technology for IoT data access protection." 2017 IEEE 17th International Conference on Ubiquitous Wireless Broadband (ICUWB). IEEE, 2017.

[15]. Rizun, Peter R. "Subchains: A technique to scale bitcoin and improve the user experience." *Ledger* 1 (2016): 38-52.

[16]. Novo, Oscar. "Blockchain meets IoT: An architecture for scalable access management in IoT." *IEEE Internet of Things Journal* 5.2 (2018): 1184-1195.

[17]. Kumar, Nallapaneni Manoj, and Pradeep Kumar Mallick. "Blockchain technology for security issues and challenges in IoT." Procedia Computer Science 132 (2018): 1815-1823.

[18]. Conoscenti, Marco, Antonio Vetro, and Juan Carlos De Martin. "Blockchain for the Internet of Things: A systematic literature review." *2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)*. IEEE, 2017.

[19]. Zamani, Mahdi, Mahnush Movahedi, and Mariana Raykova. "Rapidchain: Scaling blockchain via full sharding." Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2018.

[20]. Lee, Y., Rathore, S., Park, J.H. et al. A blockchain-based smart home gateway architecture for preventing data forgery. Hum. Cent. Comput. Inf. Sci. 10, 9 (2020). https://doi.org/10.1186/s13673-020-0214-5

[21]. Moniruzzaman, Md, et al. "Blockchain for smart homes: Review of current trends and research challenges." Computers & Electrical Engineering 83 (2020): 106585.

[22]. Zhou, Yiyun, et al. "Improving IoT Services in Smart-Home Using Blockchain Smart Contract." 2018 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). IEEE, 2018.

[23]. Dang, Thanh Long Nhat and Minh Son Nguyen. “An Approach to Data Privacy in Smart Home using Blockchain Technology.” 2018 International Conference on Advanced Computing and Applications (ACOMP) (2018): 58-64.

[24]. Mattke, Jens, et al. "How an Enterprise Blockchain Application in the US Pharmaceuticals Supply Chain is Saving Lives." MIS Quarterly Executive 18.4 (2019).

[25]. Rabah, Kefa. "Challenges & opportunities for blockchain powered healthcare systems: A review." Mara Research Journal of Medicine and Health Sciences 1.1 (2017): 45-52.

[26]. Katuwal, Gajendra J., et al. "Applications of blockchain in healthcare: current landscape & challenges." arXiv preprint arXiv:1812.02776 (2018).

[27]. Martin, Rick. “50+ Leading Blockchain Startups to Watch for 2019.” Ignite Ltd., 8 Feb. 2019, igniteoutsourcing.com/blockchain/top-blockchain-startups-to-watch.

[28]. Admin. “Supply Chain StartUps That Use Best Blockchain Technology.” Enuke Software, 8 Aug. 2019, www.enukesoftware.com/blog/supply-chain-startups-that-use-best-blockchain-technology.html.

[29]. “25 Top Blockchain Technology Companies 2020 | Updated List.” Software Development Company, 27 May 2020, www.leewayhertz.com/blockchain-technology-companies-2019.

[30]. StartUs Insights. “8 Blockchain Startups Disrupting The Healthcare Industry.” StartUs Insights, 20 Mar. 2020, www.startus-insights.com/innovators-guide/8-blockchain-startups-disrupting-the-healthcare-industry.

[31]. Bora, Pranjal. “Blockchain in Healthcare: An Executive’s Guide for 2020 | DAP.” Digital Authority Partners, 26 May 2020, www.digitalauthority.me/resources/blockchain-in-healthcare.