DECENTRALIZED DATA STORAGE AND PROCESSING FOR IOT DEVICES: UNLOCKING THE POTENTIAL

S.Narayanasamy,
Assistant Professor, Department of Computer Science and Engineering, J.J. College of Engineering and Technology, Trichy, Tamilnadu
Dr.P.Chellammal,
Professor, Department of Computer Science and Engineering, J.J. College of Engineering and Technology, Trichy, Tamilnadu
G.Keerthana,
Assistant Professor, Department of Computer Science and Engineering, J.J. College of Engineering and Technology, Trichy, Tamilnadu

M.A.Amarnath,
Assistant Professor, Department of Computer Science and Engineering, J.J. College of Engineering and Technology, Trichy, Tamilnadu

ABSTRACT:
Decentralized data storage and processing for IoT devices is an emerging paradigm that aims to address the challenges of managing and analyzing vast amounts of data generated by IoT devices. This approach involves distributing data storage and computational capabilities across a network of devices, enabling efficient and scalable data management. By leveraging edge computing, distributed storage systems, peer-to-peer networking, and advanced data processing techniques, decentralized architectures offer benefits such as improved data availability, reduced latency, fault tolerance, and enhanced privacy. However, decentralized systems also present challenges related to scalability, data security, data consistency, and network connectivity. This article highlights its advantages, key components, and challenges. The adoption of decentralized approaches holds significant potential to unlock the full capabilities of IoT devices, enabling real-time analytics, enhanced decision-making, and the development of innovative IoT applications.

Keywords: *IoT applications, decentralized systems, data storage*
DOI Number: 10.48047/nq.2020.18.8.nq20233 **NeuroQuantology 2020;18(8):243-251**

INTRODUCTION:

The rise of the Internet of Things (IoT) has transformed the way we interact with the world around us. With billions of interconnected devices, ranging from sensors and wearables to smart appliances and industrial machinery, the IoT has ushered in a new era of connectivity and data generation. However, this exponential growth in IoT devices has brought forth significant challenges, particularly concerning the storage and processing of the vast amounts of data they produce. Traditional centralized data storage and processing approaches struggle to cope with the sheer volume, velocity, and variety of IoT data.[1] These methods rely on sending all IoT-generated data to a central server or cloud infrastructure, which can result in issues like network congestion, latency, privacy concerns, and increased operational costs. To overcome these limitations, the concept of decentralized data

storage and processing has emerged as a powerful paradigm to harness the full potential of IoT devices.[2] Decentralized data storage and processing refers to a distributed architecture where data is stored and processed locally, at the edge of the network, closer to where it is generated.

This approach leverages the collective capabilities of IoT devices themselves, enabling more efficient, scalable, and resilient data management. One key advantage of decentralized storage and processing is the reduction of data transmission and associated latency. By performing data analysis and storage at the edge, near the source of data generation, the need for constant data transmission to a central server is minimized. This not only mitigates network congestion but also enables real-time decision-making capabilities, crucial in time-sensitive applications such as autonomous vehicles, industrial automation, and healthcare monitoring. Furthermore, decentralized storage and processing enhances data privacy and security.[3] With a centralized model, sensitive data is vulnerable to breaches and unauthorized access. In a decentralized system, data is distributed across multiple devices, making it less susceptible to targeted attacks. Additionally, by reducing reliance on a single point of failure, decentralized architectures offer higher resilience and fault tolerance, ensuring uninterrupted operation even in the face of network disruptions or hardware failures. Decentralized storage and processing also promote scalability and cost-efficiency.[4]

As the number of IoT devices continues to grow exponentially, central servers face increasing challenges in accommodating the sheer volume of data. Decentralization allows for horizontal scalability, where additional devices can be seamlessly integrated into the network, expanding the overall storage and processing capacity. Furthermore, decentralized architectures can optimize resource allocation by distributing computational tasks among participating devices, reducing the burden on individual nodes and minimizing infrastructure costs.[5]

Several technological advancements have fueled the adoption of decentralized storage and processing for IoT devices. Edge computing platforms, equipped with powerful processors and storage capabilities, enable local data processing and analysis. Distributed ledger technologies, such as blockchain, provide secure and transparent mechanisms for data sharing and decentralized governance. Additionally, peer-to-peer (P2P) networks, mesh networks, and fog computing architectures offer flexible and robust infrastructures to support decentralized IoT ecosystems.[6] In conclusion, decentralized data storage and processing present a compelling solution to the challenges posed by the ever-expanding IoT landscape. By bringing data management capabilities closer to the edge, this paradigm empowers IoT devices with improved performance, enhanced privacy, scalability, and cost-efficiency. As the IoT ecosystem continues to evolve, decentralized architectures are poised to play a pivotal role in realizing the full potential of interconnected devices, unlocking unprecedented opportunities for innovation and transformation in various industries.[7]

COMPONENTS OF DECENTRALIZED DATA STORAGE AND PROCESSING FOR IoT DEVICES:

The data storage and processing for IoT devices comprise of a complex apparatus. There are various components that have been listed below:

Edge Devices:

Edge devices are the IoT devices themselves, equipped with sensors, actuators, and computing capabilities. These devices form the foundation of decentralized data storage and processing. They collect data from their surroundings, perform local computations, and store or transmit relevant information to other devices or the network. Examples of edge devices include smart sensors, wearables, industrial machinery, and connected **vehicles.**[8]

Edge Computing Platforms:

Edge computing platforms provide the necessary infrastructure and software frameworks to enable data processing and

storage at the edge of the network. These platforms offer computational resources, such as edge servers or gateways, that have higher processing power and storage capacity compared to individual edge devices. Edge computing platforms facilitate local analytics, machine learning algorithms, and real-time decision-making, reducing the need for data transmission to a centralized server or cloud.

Distributed Ledger Technologies (DLT):

Distributed ledger technologies, including blockchain, enable secure and transparent data sharing and decentralized governance in IoT environments. Blockchain-based solutions provide a distributed and immutable ledger that ensures data integrity, authenticity, and consensus among participating devices. By leveraging smart contracts, DLT can automate trust and verification processes, enabling secure data transactions and enhancing privacy in decentralized storage and processing.[9]

Peer-to-Peer (P2P) Networks:

P2P networks play a crucial role in decentralized data storage and processing by enabling direct communication and data exchange between edge devices. P2P networks eliminate the need for centralized intermediaries, allowing devices to share data and computational resources in a decentralized manner. These networks ensure efficient data distribution, fault tolerance, and scalability by leveraging the collective computing power and storage capacities of connected devices.

Fog Computing:

Fog computing complements edge computing by extending the computational capabilities to the network edge, closer to the devices. It enables data processing and storage in the fog layer, which consists of interconnected fog nodes or fog servers. These nodes act as intermediaries between edge devices and centralized cloud servers, performing tasks such as data filtering, aggregation, and local analytics. Fog computing reduces latency, bandwidth requirements, and data transmission costs, making it ideal for decentralized IoT data management.[10]

Data Routing and Discovery:

Efficient data routing and discovery mechanisms are crucial for decentralized data storage and processing. These components enable devices to discover nearby peers, establish connections, and exchange data. Various protocols, such as Zigbee, MQTT, CoAP, and Bluetooth, facilitate data routing and discovery in IoT networks. These protocols ensure efficient and reliable communication among devices, enabling seamless data transmission and collaboration in decentralized environments.

Data Replication and Redundancy:

Data replication and redundancy mechanisms are essential for ensuring data availability and fault tolerance in decentralized storage. By storing multiple copies of data across different devices, the system can withstand device failures or network disruptions.[3] Replication strategies, such as data partitioning, erasure coding, or consensus algorithms, ensure that data remains accessible and consistent even in the presence of failures, enhancing the reliability and resilience of decentralized storage systems.[11]

Data Security and Privacy:

Security and privacy are critical considerations in decentralized data storage and processing. Encryption techniques, access control mechanisms, and authentication protocols protect data integrity and confidentiality. Privacy-preserving algorithms and techniques, such as differential privacy or secure multi-party computation, mitigate privacy risks associated with sharing sensitive data in a decentralized environment. These components safeguard IoT data and enable secure and private collaboration among devices.

In conclusion, it encompasses a range of technologies and protocols that facilitate local computation, data sharing, and collaborative decision-making.

DISTRIBUTED CONTENT DISTRIBUTION IN DECENTRALIZED DATA STORAGE AND PROCESSING FOR IoT DEVICES:

Distributed content distribution refers to the dissemination of content across multiple devices or nodes in a decentralized network. It involves distributing data, files, or digital content in a manner that ensures redundancy,

availability, and efficient access within the decentralized infrastructure. In a distributed content distribution system, content is replicated or distributed across multiple devices or storage nodes within the network. This redundancy ensures that the content is accessible even if some nodes become unavailable or fail. Distributed content distribution offers several benefits in the context of decentralized data storage and processing for IoT devices. By distributing content across multiple nodes, distributed content distribution increases data availability. Even if one or more nodes become offline or inaccessible, the content remains available on other nodes within the network. This ensures that IoT devices can access the required content, even in the presence of node failures or network disruptions.

With distributed content distribution, content can be stored closer to the IoT devices or edge computing devices. This reduces the latency involved in fetching content from a centralized server or remote location. By minimizing data transmission time, distributed content distribution enables faster access to content, supporting real-time processing and decision-making in IoT applications. Distributed content distribution allows for scalability in handling large volumes of data. As the number of IoT devices and data generated increases, distributing content across multiple nodes enables efficient storage and retrieval. Additional nodes can be added to the network, and content can be distributed among them, ensuring the system can handle the growing data load and accommodate the expanding IoT ecosystem.

By distributing content across multiple nodes, distributed content distribution helps balance the load among the network's devices or storage nodes. This prevents any single node from being overwhelmed with requests or data storage, ensuring even distribution of processing and storage resources. Load balancing enhances overall system performance and responsiveness.[4] Distributed content distribution improves fault tolerance within the decentralized infrastructure. If a node fails or becomes unavailable, the content replicated or distributed on other nodes remains accessible. This fault tolerance mechanism ensures that data is not lost, and the distribution system can continue operating without significant disruptions.

Distributed content distribution optimizes resource utilization within the decentralized infrastructure. By distributing content across multiple nodes, it allows for efficient use of storage capacity, bandwidth, and computational resources. This results in better resource management, improved system efficiency, and cost savings in terms of infrastructure requirements. Distributed content distribution plays a critical role in decentralized data storage and processing for IoT devices. It ensures data availability, reduces latency, supports scalability, provides fault tolerance, enables efficient resource utilization, and enhances the overall performance of the decentralized infrastructure.

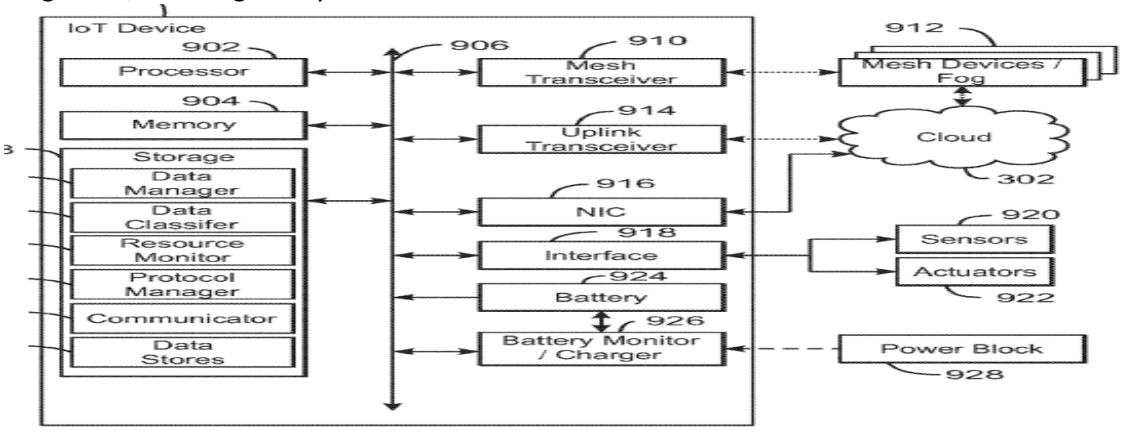

Fig.1 Components present in an IoT device for implementing a distributed content - distribution system

(Ref. US 11,296,937 B2, dt. Sep. 25, 2020)

ADVANTAGES OF DECENTRALIZED DATA STORAGE AND PROCESSING FOR IOT DEVICES:

One of the primary advantages of decentralized data storage and processing for IoT devices is reduced latency. By storing and processing data at the edge of the network, closer to the data source, the need for data transmission to a centralized server or cloud is minimized. This enables real-time processing and decision-making capabilities, crucial in time-sensitive applications such as autonomous vehicles, industrial automation, and healthcare monitoring. Reduced latency ensures faster response times, enhances overall system performance, and enables timely actions based on IoT data. Decentralized data storage and processing offer improved data privacy and security compared to centralized approaches. In a centralized model, sensitive data is vulnerable to breaches and unauthorized access. In contrast, decentralized architectures distribute data across multiple devices, making it less susceptible to targeted attacks. Additionally, decentralized systems reduce the reliance on a single point of failure, enhancing resilience and fault tolerance. Data encryption, access control mechanisms, and privacy-preserving techniques further protect the integrity and confidentiality of IoT data, ensuring that privacy concerns are addressed in a distributed environment.

Decentralized data storage and processing architectures offer scalability and flexibility to accommodate the growing number of IoT devices and the associated data volumes. Traditional centralized approaches face challenges in scaling their infrastructure to handle the increasing data influx. Decentralized architectures, on the other hand, can leverage the collective storage and processing capabilities of participating devices. Additional devices can be seamlessly integrated into the network, expanding the overall storage and processing capacity. This scalability ensures that the system can accommodate the exponential growth of IoT devices and adapt to changing requirements. Decentralized storage and processing can lead to cost efficiencies compared to centralized models. By reducing the need for constant data transmission to a central server or cloud, decentralized architectures minimize network bandwidth requirements and associated costs.[5] Local processing and storage at the edge of the network can also reduce data storage costs in the cloud. Moreover, decentralized architectures enable optimized resource allocation by distributing computational tasks among participating devices. This reduces the burden on individual nodes and minimizes infrastructure costs, making decentralized approaches cost-effective for IoT deployments.

Decentralized architectures offer higher reliability and resilience compared to centralized systems. In a centralized model, a failure in the central server can result in the loss of access to all data and services. In contrast, decentralized systems distribute data across multiple devices, ensuring redundancy and fault tolerance. Even if one device fails or is disconnected from the network, the system can continue to operate without significant disruptions. This resilience is particularly valuable in mission-critical IoT applications where continuous operation is essential. Decentralized data storage and processing enable localized data processing, which can be beneficial in scenarios where data sovereignty and compliance regulations are a concern. By keeping data within specific jurisdictions or geographic boundaries, decentralized architectures facilitate compliance with data protection regulations, such as the General Data Protection Regulation (GDPR). Localized processing also addresses data residency requirements, ensuring that data remains within specific regions or countries, thereby enhancing data governance and meeting regulatory obligations.

With the exponential growth of IoT devices, centralized data storage and processing can strain network bandwidth and lead to congestion. Decentralized architectures alleviate this burden by distributing data processing and storage closer to the edge, reducing the amount of data transmitted across the network. This reduces network

congestion and optimizes bandwidth utilization, improving overall network performance and efficiency.

DISADVANTAGES OF DECENTRALIZED DATA STORAGE AND PROCESSING FOR IOT DEVICES:

It brings numerous benefits, but they also present several challenges that need to be addressed. Supporting a large number of IoT devices generating massive volumes of data requires scalable decentralized storage and processing solutions. Ensuring that the system can handle the increasing data load, accommodate a growing number of devices, and maintain performance is a significant challenge.

Decentralized systems often involve data replication and distribution across multiple devices or nodes. Ensuring the security and privacy of data in such a distributed environment becomes crucial. Protecting data from unauthorized access, securing data transmission, and implementing robust authentication and encryption mechanisms are challenging in decentralized architectures. Maintaining data consistency across distributed nodes is challenging in decentralized systems. As data is replicated or distributed across multiple nodes, ensuring that all copies of the data remain consistent becomes complex. Dealing with conflicting updates, synchronization, and resolving data conflicts require careful design and synchronization protocols. Decentralized architectures aim to provide fault tolerance by distributing data across multiple nodes. However, managing node failures, network disruptions, and ensuring data availability in the presence of failures is a significant challenge. Implementing robust fault detection, recovery mechanisms, and replication strategies are essential for maintaining system reliability.

IoT devices may operate in remote or challenging environments with limited network connectivity. Maintaining consistent connectivity between devices and the decentralized infrastructure can be challenging. Addressing intermittent connectivity, managing low-bandwidth scenarios, and optimizing data transmission become crucial in decentralized systems. IoT devices often operate on limited power sources, such as batteries. Energy-efficient decentralized storage and processing mechanisms are necessary to minimize the energy consumption of IoT devices. Optimizing data transmission, processing, and resource utilization to reduce energy consumption becomes a key challenge. Decentralized data storage and processing raise challenges related to data governance, regulatory compliance, and data ownership. Ensuring compliance with data protection regulations, managing data access rights, and maintaining auditability in a decentralized environment require careful consideration and robust governance mechanisms.

Interoperability among different IoT devices, platforms, and protocols is crucial in decentralized systems. Ensuring seamless communication and data exchange between heterogeneous devices and systems becomes a challenge. Standardization efforts and interoperability frameworks are necessary to address this challenge. Managing and monitoring a decentralized infrastructure with a large number of IoT devices and distributed nodes can be complex. Efficient device management, monitoring data flows, diagnosing issues, and ensuring overall system health become challenging tasks in decentralized environments.[6] Addressing these challenges requires a combination of technological advancements, standardized protocols, robust security measures, and efficient management frameworks.

DECENTRALIZED DATA STORAGE AND PROCESSING FOR IOT DEVICES: ESTONIA'S SUCCESS STORY

Estonia has emerged as a global leader in digital governance and innovation, actively embracing decentralized technologies to empower its citizens and businesses. Estonia's e-Estonia initiative is a comprehensive digital transformation strategy that encompasses various aspects of governance, including decentralized data storage and processing for IoT devices. The country has built a robust digital infrastructure that leverages decentralized technologies to enhance efficiency, security, and accessibility of data.

One of the key elements of Estonia's approach is the X-Road platform. X-Road is a decentralized data exchange platform that enables secure and seamless data sharing between different government agencies, businesses, and IoT devices. It ensures interoperability and data integrity while maintaining privacy and security.

Estonia has implemented distributed ledger technology (DLT), commonly known as blockchain, to secure and decentralize critical data. The blockchain-based solutions ensure transparency, immutability, and tamper-proof records. For instance, Estonia's e-residency program, which offers digital identity for non-residents, utilizes blockchain technology to secure personal data and enable decentralized access. In terms of IoT devices, Estonia has implemented a decentralized approach to data storage and processing. Rather than relying solely on centralized servers, IoT devices in Estonia are designed to leverage edge computing capabilities. Edge devices perform local data processing, reducing the need for transmitting all data to a centralized location. This approach enables real-time decision-making, lower latency, and enhanced data privacy. Estonia's digital governance framework also emphasizes data ownership and control. Individuals have control over their personal data and can grant selective access to government agencies and service providers. This decentralized data governance approach ensures transparency, privacy, and empowers citizens to have greater control over their information.

Furthermore, Estonia has implemented robust cybersecurity measures to protect decentralized data storage and processing systems. It has established a strong legal framework and initiatives to combat cyber threats, ensuring the integrity and security of IoT devices and the data they generate. The country's digital governance strategy, leveraging platforms like X-Road and blockchain, along with its focus on edge computing, data ownership, and cybersecurity, showcases the potential of decentralized technologies in enhancing efficiency, privacy, and security in the IoT ecosystem.

CONCLUSION:

In conclusion, it offers significant advantages and transformative potential in the realm of data management and analytics. By distributing data and processing capabilities across a network of devices, it enables enhanced scalability, data availability, fault tolerance, and efficient resource utilization. The key components of decentralized data storage and processing systems include edge computing, distributed storage, peer-to-peer networking, data processing and analytics, blockchain or distributed ledger systems, security and privacy mechanisms, and data governance and management systems. These components work together to create a robust and efficient infrastructure for handling IoT data in a decentralized manner.

Decentralized data storage and processing systems address several challenges faced in centralized architectures. They provide scalability to accommodate the growing number of IoT devices and the massive volume of data generated. Furthermore, they ensure data availability by distributing content across multiple nodes, reducing latency by performing processing at the edge, and improving fault tolerance by replicating data. Additionally, decentralized systems optimize resource utilization and enable efficient data processing and analytics by leveraging distributed computing capabilities. However, decentralized data storage and processing also come with their own set of challenges. Scalability, data security, data consistency, fault tolerance, network connectivity, energy efficiency, data governance and compliance, interoperability, and management and monitoring are key areas that require careful consideration and innovative solutions. To fully realize its potential, collaboration among stakeholders is crucial. Collaboration between industry players, policymakers, standardization bodies, and research institutions can foster the development of interoperable and secure decentralized systems. This collaboration will ensure the adoption of best practices, the establishment of robust security measures, and the formulation of data governance frameworks that prioritize privacy, ownership, and

compliance.Furthermore, continued research and development efforts are necessary to address the existing challenges and improve the efficiency, scalability, and security of decentralized systems. Innovations in areas such as distributed consensus algorithms, edge computing technologies, data encryption, and decentralized analytics frameworks will further enhance the capabilities of decentralized data storage and processing for IoT devices. It has the potential to revolutionize how data is managed and processed in the digital era. By harnessing the power of distributed computing, secure data exchange, and efficient resource utilization, decentralized systems pave the way for more resilient, scalable, and privacy-preserving IoT applications. Embracing decentralized approaches will lead to a more robust and inclusive digital infrastructure that can support the exponential growth of IoT devices and the demands for real-time data-driven insights across various industries.

REFERENCES:

1. Xinxin Fan, Qi Chai, Lei Xu, and Dong Guo. 2020. DIAM-IoT: A Decentralized Identity and Access Management Framework for Internet of Things. In Proceedings of the 2nd ACM International Symposium on Blockchain and Secure Critical Infrastructure (BSCI '20). Association for Computing Machinery, New York, NY, USA, 186–191. https://doi.org/10.1145/3384943.3409436
2. S. Bajoudah, C. Dong and P. Missier, "Toward a Decentralized, Trust-Less Marketplace for Brokered IoT Data Trading Using Blockchain," 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 2019, pp. 339-346, doi: 10.1109/Blockchain.2019.00053.
3. Hickman, C. F. L., Alshubbar, H., Chambost, J., Jacques, C., Pena, C., Drakeley, A., &Freour, T. (2020). Data sharing: Using blockchain and decentralized data technologies to unlock the potential of artificial intelligence: What can assisted reproduction learn from other areas of medicine? Fertility and Sterility, 114(5), 927-933. https://doi.org/10.1016/j.fertnstert.2020.09.160
4. Yaqoob, I., Salah, K., Jayaraman, R. et al. Blockchain for healthcare data management: opportunities, challenges, and future recommendations. Neural Comput&Applic 34, 11475–11490 (2022). https://doi.org/10.1007/s00521-020-05519-w
5. Bhushan, B., Sahoo, C., Sinha, P. et al. Unification of Blockchain and Internet of Things (BIoT): requirements, working model, challenges and future directions. Wireless Netw 27, 55–90 (2021). https://doi.org/10.1007/s11276-020-02445-6
6. Aoun, A., Ilinca, A., Ghandour, M., & Ibrahim, H. (2021). A review of Industry 4.0 characteristics and challenges, with potential improvements using blockchain technology. Computers & Industrial Engineering, 162, 107746. https://doi.org/10.1016/j.cie.2021.107746
7. Nyamtiga, B. W., Sicato, J. C., Rathore, S., Sung, Y., & Park, J. H. (2019). Blockchain-Based Secure Storage Management with Edge Computing for IoT. Electronics, 8(8), 828. https://doi.org/10.3390/electronics8080828
8. Puri, V., Kumar, R., Le, C. V., Sharma, R., & Priyadarshini, I. (2019). A Vital Role of Blockchain Technology Toward Internet of Vehicles. Handbook of Research on Blockchain Technology, 407-416. https://doi.org/10.1016/B978-0-12-819816-2.00016-2
9. Ge, C., Liu, Z., & Fang, L. (2020). A blockchain based decentralized data security mechanism for the Internet of Things. Journal of Parallel and Distributed Computing, 141, 1-9. https://doi.org/10.1016/j.jpdc.2020.03.005
10. I. Yaqoob, K. Salah, M. Uddin, R. Jayaraman, M. Omar and M. Imran, "Blockchain for Digital Twins: Recent

Advances and Future Research Challenges," in IEEE Network, vol. 34, no. 5, pp. 290-298, September/October 2020, doi: 10.1109/MNET.001.1900661.

11. G. Wang, Z. Shi, M. Nixon and S. Han, "ChainSplitter: Towards Blockchain-Based Industrial IoT Architecture for Supporting Hierarchical Storage," 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 2019, pp. 166-175, doi: 10.1109/Blockchain.2019.00030.