Rethinking Blockchain Integration with the Industrial Internet of Things

Maha Alaslani, Osama Amin, Faisal Nawab, and Basem Shihada

Abstract

Blockchain is a decentralized technology that protects sensitive data from being controlled by a central authority and can play a vital security role in developing the Industrial Internet of Things (IIoT). Most of the IIoT-blockchain systems focus on optimizing consensus mechanisms, which cannot provide satisfactory scalability until addressing the inherited problems of the networking infrastructure. Excessive messaging overheads and low networking performance are two critical issues of the current blockchain configurations. Moreover, the well-known architectural models, cloud-centric, and fog-centric models cannot provide acceptable performance in IIoT due to data aggregation and synchronization timing overheads, privacy, and trust issues. As such, we propose two novel blockchain solutions that can fulfill the IIoT strict challenges and requirements. First, the context-aware data-driven solution decreases the irrelevant and useless data traffic. Second, the hybrid communications with second-layer chain solutions partition the data traffic through different communication media and provide better scalability and higher resistance against security issues. Finally, we present a future vision of the next blockchain generation that can fulfill the IIoT predictions.

I. Introduction

Internet of Things (IoT) is leading the way for the next industrial revolution by adding smart features and introducing the concept of IIoT [1]. It is aimed to improve the functionality of the next generation of the industrial age by connecting a large number of smart devices. A recent study states that a typical factory can include about 1000 devices per 100 square meters, with a growing need for several applications and services such as process monitoring and mobile control [2]. These applications generate and exchange vast amounts of critical and sensitive data that needs to be accurately monitored and controlled while preventing any security attacks and assuring data safety and integrity. Industrial systems are attractive environments for malicious attacks, where attackers can do enormous amounts of malicious activities that lead to sensitive data manipulation, industrial networks shut down, economic losses, threatens physical infrastructure, even jeopardizing national security. In 2017, the malicious software called Triton, was able to disable industrial safety systems and causing catastrophic damages [3]. Triton targeted the industrial infrastructures in the Middle East, and now it has expanded to North America and other countries. Such attacks can take place due to the lack of suitable protection mechanisms.

In respect to security issues, blockchain arises as one of the promising foremost solutions to fully integrate the IoT in the industrial field. Blockchain is a distributed, immutable ledger technology that is made up of valid and encrypted data to prevent malicious nodes from modifying the data. The information is transmitted/broadcasted throughout the network to be received by specialized machines that verify, accumulate, and add the data into the blockchain. The process that organizes the data into a consistent and authenticated chain of blocks is called a consensus process. Blockchain platforms use a prohibitively expensive approach to propagate data and blocks, which affects the network scalability and delay performance. The data are forwarded and duplicated to all peers as they are received. Furthermore, IIoT network communication gets highly stressed by sending a massive amount of redundant data and increasing the number of devices that aggravates the system complexity. These inefficiencies are not tolerable for consensus nodes, which need to make sure they have access to the most recent block. Nevertheless, blockchain performance bottleneck remains one of the most critical challenges, where the communication overhead, low throughput and long delay strictly limit the adoption of blockchain in IIoT.

Previous research focuses on optimizing the consensus mechanisms to improve the blockchain performance without compromising data integrity. Even though optimizing these mechanisms acts as a great solution, it can only enhance the scale of the main blockchain and cannot solve the inherited networking-level scalability issues. In this paper, we focus our study on the blockchain communication network-level opportunities and challenges in future IIoT platforms. We propose novel solutions for integrating the blockchain in IIoT while addressing the scalability problem and satisfying the IIoT stringent performance requirements. In the rest of this article, we introduce answers to the following questions

- What are the networking challenges that obstruct blockchain integration in IIot?
- Can data-centric networking control the massive growth of blockchain in IIoT?
- How can hybrid communications support hierarchical blockchain in IIoT and boost network performance?
- How can the blockchain support IIoT future predictions?

The remainder of the article is organized as follows: Section II discusses the IIoT characteristics and issues. Section III summarizes the two main bottlenecks that drive the IIoT scalability challenge and slow down Blockchain performance; consensus algorithms, and networking dissemination mechanisms. Then, Section IV summarizes the current Blockchain solutions. After that, Section V provides potential solutions to integrate Blockchain with the IIoT ecosystem. Finally, Section VI concludes the article.

II. BLOCKCHAIN in Industrial Internet of Things

IIoT, as a key enabler of the smart industry, connects different devices with various capabilities and complexity, varying from simple sensor nodes to intelligent control devices. The control devices can be used to bridge the gap between the simple IIoT sensors and the management applications. Several communication networks are used to build a smart industrial system that is able to exchange, process, and analyze the collected data. The interpreted data helps to enhance business efficiency and drive intelligent decisions.

IIoT is a dynamic network that has different configurations, traffic types and performance requirements that are distinct from traditional communication systems [1]. IIoT network operates commonly in wireless environments, where it suffers from electromagnetic interference, mechanical stress, critical temperature, and high humidity, which negatively impact the transmitted data quality. IIoT applications require reliable communication links with packet error rates between 10^{-9} to 10^{-2} [4]. Moreover, the network has to be flexible and reconfigurable to survive the explosive growth of IIoT applications, especially in the industrial sector, where the nodes exist across large areas.

IIoT devices generate networking traffic with different performance requirements and characteristics, such as cyclic and acyclic [1]. In a smart factory system, the cyclic traffic generated by sensors devices located in the field of interest. Unpredictable critical events, such as process alarms, are carried by the acyclic traffic that is mostly subjected to strict deadlines. Generally, mission-critical and time-sensitive industrial tasks have strict end-to-end latency requirements (between 0.5 to 100 milliseconds [2]). Delay is a significant factor that defines the system's Quality of Service (QoS) demands. Satisfying the end-to-end delay for the IIoT applications is a complicated task that is aggravated by unexpected system disturbances.

Conventional networking techniques cannot provide the desired guarantees in IIoT networks. Thus, it is essential to review the IIoT fundamental issues that are summarized as follows:

- **Interoperability and Auditability:** ensuring the auditing standards and strict regulations are required to implement a fully functional digital ecosystem. Interoperability between the system devices is another factor in reducing the deployment and integration costs.
- **System Availability:** system availability is a crucial requirement for any well-deployed industrial network compared to the general IoT network. IIoT has high availability requirements between 99.99% to 99.9999% [2]. If an IIoT task fails to initiate its functions and services at the right time, that will cost the industrial system millions of dollars and damage its economic value.
- **Security:** the main concern in any industrial system is providing a minimum security level. Yet, IIoT suffers from securing its sensitive and critical information. Thus, modern industrial networks have to ensure seamless and secure remote access to data and nodes located up at different location levels and networking segments.

In recent years, the blockchain revolution and its intersection with IIoT have gained considerable interest. Blockchain is a trusted data structure that builds on the Peer-to-Peer (P2P) distributed networks. Each peer in the network stores a copy of the blockchain ledgers that made of an immutable and encrypted chain of information. Therefore, the blockchain system is characterized by decentralization, trust, and immutability features. The decentralization is achieved through the P2P architecture, where the nodes of the network maintain a blockchain copy. Thus, there is no need for a third party authority, where the trust is obtained via the decentralized coordination mechanisms of blockchain. Moreover, the decentralization helps any blockchain system to be more resilient to attacks on its availability. In a blockchain, consensus mechanisms are the responsible feature that guarantees consistency and data authenticity. Once a data block is added to the blockchain, it is extremely hard to be revoked. The blocks cannot be modified and thus become immutable and auditable.

III. Blockchain Challenges in Industrial Internet of Things

Network scalability is one of the most critical issues in employing blockchain in IIoT. With the continual increase of data in the industrial field, integrating the blockchain in the IIoT system becomes difficult due to the corresponding network expansion associated with the target of reaping the full decentralization benefits. Mainly, two bottleneck issues that drive the scalability challenge and slow down blockchain operation and performance; consensus algorithms, and network dissemination mechanisms.

A. *Consensus, Agreement and Fault Tolerance*

Developing efficient and robust consensus mechanisms in an expanded IIoT network is a fundamental problem in distributed systems, where it is required to reach an agreement between several nodes to have a secure and trusted blockchain system. There are multiple well-known methods by which a blockchain network can agree over a new committed block. In an IoT environment, a state machine replication (SMR) is one of the building block for the most well-known consensus mechanisms [5]. Nevertheless, we will focus on the networking-level mechanisms, as shown in the following section.

B. *Network Dissemination Mechanisms*

The blockchain system utilizes the P2P networking infrastructure, where every node within the network dispenses a portion of network connection, computing power, and storage capacity. Hence, the operation performance of a specific network is controlled by the combined effort from its nodes.

In a blockchain environment, when the data is prepared to be published, the operator sends it towards P2P network, which helps all blockchain nodes to communicate. We can also say that the operator sends it to any devices that are available from the list called peers. After receiving the data, the peer instantly starts to disseminate it through the list of random peers of neighbors. After multiple transferals, many peers have a copy of the data. And, the consensus process is triggered where specialized machines start to include the data into the blocks and disseminate them across the network. As a result, the information is distributed through the network twice.

The first time is when the data moves from the publishing device to the consensus machine. Then again, back to the node which is waiting for updates on the blockchain. Every time this information is received in a different way through different peers. This process makes blockchain unique from large centralized systems where, in centralized mode, data paths are set rigidly to guarantee maximum speed. However, there is a possibility that the block may sometimes be located in nodes that are not available at the present time. Here the peer would wait until data appeared in the network. Similarly, it is likely the important data is prominent where it could reach a random node with better efficacy with no delay. P2P networks cannot usually ensure stable data transfers as delivery schemes in centralized systems. Whereas, P2P networks are much more resistant to complete network system cut off and malicious behaviors.

Alongside, if the node is in connection with just two peers, there will be approximately $O(2^n)$ messages for covering a network size of (n) nodes. For the IIoT network, total (n) could be exceptionally large. There are also mounts of devices with data that needs to be synchronized with the help of the network. In many cases, a device is required to learn close by nodes' status. The problem is even more aggravated under wireless connectivity that is slower and less reliable, compared to wired connections presumed in traditional blockchain protocols. Thus, applying blockchain into IIoT makes the process of data communication much harder. Hence, existing blockchain propagation mechanisms may not be suitable for the IIoT environment.

IV. Current Blockchain Status and Solutions

In the last few years, most of the blockchain-IIoT integration efforts were about overcoming the limitations mentioned above by filling the gap between several architectural solutions. In this section, we discuss the existing network-based solutions.

A. *Cloud-Centric Blockchain Model*

Cloud computing is a popular Internet paradigm that provides reliable services through powerful data centers. Cloud computing aims to simplify web-based data systems for end-users and acts as a receiver of data from ubiquitous IIoT sensors to be interpreted and analyzed. Therefore one way to provide the blockchain for IIoT is by merging the IoT and cloud computing [6]. Besides the hosting challenges, trust and privacy are two major drawbacks that prevent integrating the cloud model in the IIoT networks. Moreover, cloud computing usually provides a centralized architecture, which, in contrast to the blockchain, complicates the reliable data sharing with the participated devices. Therefore, a semi-centralized system or cloud paradigm will no longer be adequate for addressing the performance requirements and challenges of the emerging IIoT applications. However, a new structure based on a decentralized system will be needed.

B. *Fog-Centric Blockchain Model*

Fog computing is used as an option that takes the cloud computing paradigm to the network edges. The fog model provides storage, computing, and network services to the end devices using highly virtualized machines located at the edge of the network. These fog nodes have the capability to work as blockchain gateways and also enable interaction with core blockchain and IIoT devices. But the fog nodes usually work under multiple third party entities; hence, it makes it difficult to ensure absolute trust and security. The intelligent gateways are closer to the end-user, and they can perform end-to-end IIoT communications with the lowest possible latency. These gateways can perform analytics and data handling at the local level. Most of the IIoT applications have specific requirements for transmission, storage, and computation. Fog model provides a faster response for IIoT applications where the cloud servers have the capability to provide high computation power and large storage.

Therefore, the IIoT takes benefits from fog servers [6]. The fog servers have the ability to mitigate issues of centralized availability regarding the single point of failure and the possibility of malicious entities that may attack the information through the network. The fog layer's nodes have multiple segments of blockchain, which reduce the processing and memory requirements. However, they generate a large amount of traffic to maintain synchronization with the global blockchain. Nevertheless, aggregation and synchronization timing overheads are not compatible with a large number of delay-sensitive IIoT applications. Moreover, the fog model cannot guarantee secure and seamless data propagation between the IIoT devices and the fog nodes. To overcome these limitations, researchers need to reconsider designing new alternative blockchain solutions that can fulfill the IIoT strict challenges and requirements.

C. *Other Solutions*

Distinct research efforts focus on amplify the scale of the blockchain and boost the overall performance. Data management solutions that use deep reinforcement learning was proposed in [7] to maximize data collection amount, and geographic fairness and minimize the energy consumption. Another data-based solution is proposed in [8] where the blockchain platform uses lossless data compression method to store data in the main chain. However, the estimated blockchain size is not feasible for a large factory scenario. One way to address the challenge previously mentioned is by using local chain techniques to provide the needed scalability and practicability [9]. In this context, the data processing is done according to the complexity level, where the off-chain deals with the complex problems that the on-chain network cannot solve. The proposed solution did not store the exact data in the off-chain and only stores the data's hash-values. Therefore, it cannot assure information availability and reliability. On the other hand, the authors in [10] proposed a blockchain-based non-repudiation service provisioning scheme for IIoT network. The requested services are split into non-executable parts and then carried out via on-chain and off-chain channels in different phases for limiting the burden on the blockchain network. This method was targeted the non-repudiation services and needed to be extended to include other security factors, including trust and privacy. Nonetheless, the research efforts will not provide satisfactory results

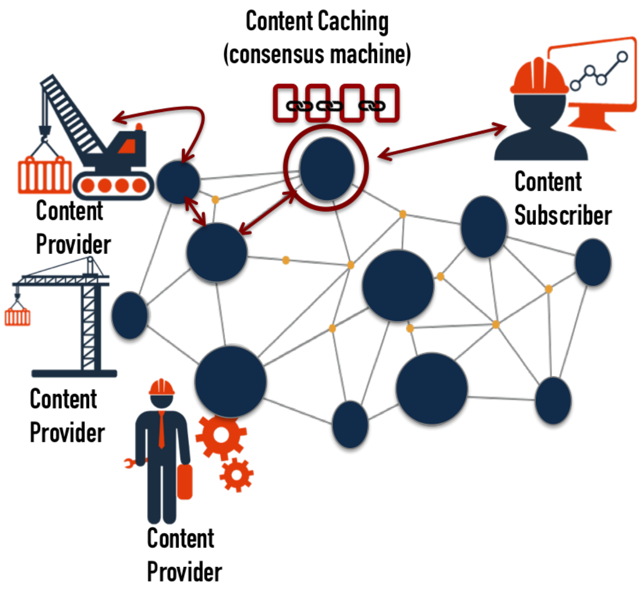

Fig. 1: Context-aware and data-driven communications: an IIoT device requests data from the network. When a content provider satisfies the request, it will respond with the required data, and the caching machines will act as a consensus node.

until the fundamental inherited problems from the underlying networking infrastructure removed and improved.

V. Rethinking of Industrial Internet of Things Blockchain Integration

Blockchain has the potential to be significantly beneficial for IoT to develop secure industrial networks. However, there is still a need for extensive research to identify the open issues and challenges experienced by using these two technologies together. Beyond the consensus optimization efforts, the blockchain networking layer remains another critical factor responsible for decreasing its performance, specifically in the IIoT case. Therefore, there is a demand for building and designing methods that can safely integrate blockchain with IIoT devices to immediately commit the data generated from heterogeneous IIoT devices. In the following, we propose two network-based solutions that can facilitate integrating the blockchain in the IIoT.

A. Context-Aware Data-Driven Solution

IP host-centric model for communication presently is the most effective model on the Internet. With everything else evolving, there has been a stretch limit in the host-based communication along with exploration for new models of communication. Information Centric Networking (ICN) is a noteworthy candidate for the future of Internet architecture. Here the content is the primary component irrespective of its location (host). This crucial component in ICN makes use of the data/content name rather than the address of the network. The name of the content must be unique, independent of location, and persistent. A consumer typically requests the content by name rather than the address of the provider.

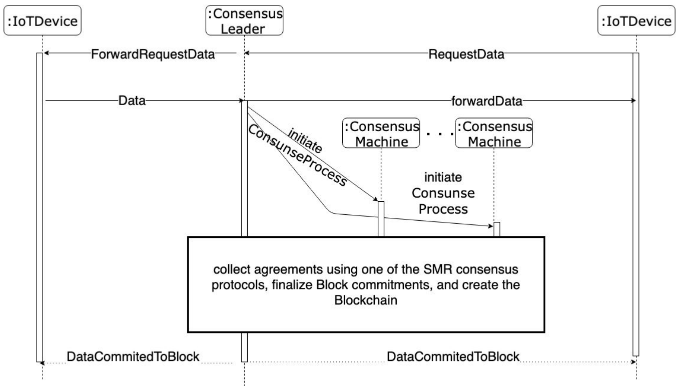

Fig. 2: UML sequence diagram illustrating Context-Aware and Data-Driven communications.

Therefore, in-network caching could be applicable at the time of communication, as it stores the data closer to the customer to improve data retrieval along with reducing network traffic. When the content is independent of location, ICN intrinsically handles nodes' mobility through reissuing the unsatisfactory requests.

ICN can also provide convenient data retrieval dependent upon the request/reply model, as illustrated in Fig. 1. In ICN, content security is based on attaching all information related to security with the content itself, which is essentially useful in IIoT networks. Most of IIoT communications and their applications fundamentally follow the content orientated paradigm [11]. For example, retrieving sensed values from IIoT sensor and updating the corresponding application with content which has recently been published (weather data, traffic information, patient status, etc.).

Data-based communication leads to a reduction in networking congestion and latency by the elimination of irrelevant data and useless traffic. One scenario in which the content-aware model can be implemented is the on-demand manufacturing, where the commodities are supplied as ordered. It allows consumers to get their desired requests, and producers can easily manage the merchandise production process without wasting goods or services. The smart monitoring system is another application that can continually pull the data from the on-site machines and sensors. It can predict the expected time and extent of the production process, maintain the machine uptime, and enhance the overall efficiency. Fig. 2 shows the Unified Modeling Language (UML) sequence diagram that illustrates the context-aware and data-driven communications where the group of the IoT devices that satisfied the arrived requests, start to push the data accordingly. Therefore, it can prevent the enormous communication redundancy and storage overheads. Then, the intermediate devices act as forwarding machines (content caching) that forward the request and the data messages. When a machine forwards a number of data messages between the IoT devices, it can initiate the consensus process with the predefined consensus machines and create the blockchain.

Some of the main features of ICN include in-network caching, content naming, and delivery schemes. If these

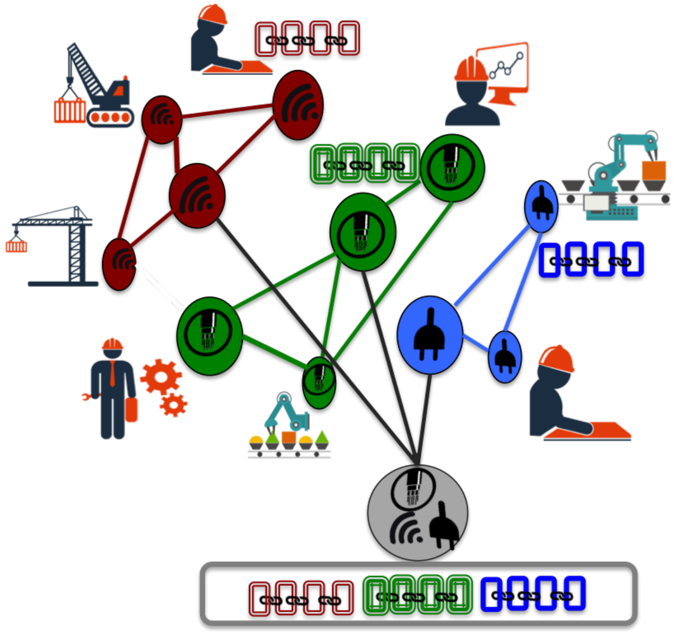

Fig. 3: Hybrid communication and second-level chain solutions: each group of IIoT devices communicates over different media and form its second-level chain. At the end, all the second-level chains will build up the main blockchain.

aspects are incorporated into the blockchain network, the content-based delivery model will minimize the communicated traffic and consequently boost the overall performance. Contents safety is another issue that needs to be ensured to guarantee an end-to-end protection for the IIoT network, where the content security is carried on the transferable data rather than connection channels.

B. Hybrid Communication and Second-Level Chain Solutions

In the blockchain context, hierarchical or second-layer chains are developed to solve the scalability problem with the conventional blockchain network. For blockchain's ultimate security and low deployment cost, developers will enable second-layer solutions such as sidechain and offchain [12], [6]. In offchain, data processing is done on the local chain and integrated with the main blockchain by sending the obtained results. Offchain does not publish every transaction on the blockchain immediately, but it entirely relies on the consensus algorithm of the main blockchain. Offchain helps to reduce network congestion and facilitates faster processing speeds. Contrary, sidechain offers an independent second-layer solution, full independence and sovereignty of sidechain is its most significant benefit. The data exchange system and operation of the sidechain are self-reliant. Thus, the security of the sidechain is also controlled by itself and does not affect the main chain. Multiple sidechains can be connected to the main blockchain using the two-way pegs. The two-way pegs allow exchanging the peered data between the sidechains and conventional blockchain.

Generally, both solutions can help to partition the communication domains in the industrial environments and, therefore, provide better scalability and higher resistance against security issues. Second-layer chains can be a good candidate to merge several communication technologies. The devices communicate in a specific protocol can create their second-level chain and then interchange the data with the parent blockchain. However, partitioning the IIoT network by using multiple second-level chains, one for each communication media, e.g., wireless, fiber optics, ethernet cables, or power line communication (PLC), will improve the blockchain scalability and reliability.

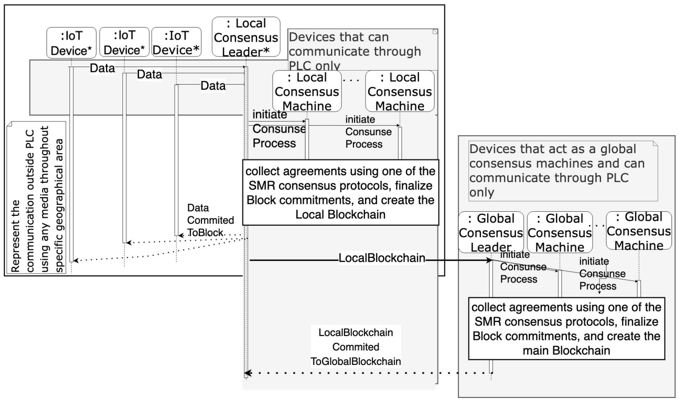
:IoT Device*
:IoT Device*
:IoT Device*
: Local Consensus Leader*
Devices that can communicate through PLC only
Data
Data
Data
: Local Consensus Machine
. . .
: Local Consensus Machine
initiate Consunse Process
initiate Consunse Process
Represent the communication outside PLC using any media throughout specific geographical area
collect agreements using one of the SMR consensus protocols, finalize Block commitments, and create the Local Blockchain
Data Commited ToBlock
LocalBlockchain
Devices that act as a global consensus machines and can communicate through PLC only
: Global Consensus Leader
: Global Consensus Machine
. . .
: Global Consensus Machine
initiate Consunse Process
initiate Consunse Process
collect agreements using one of the SMR consensus protocols, finalize Block commitments, and create the main Blockchain
LocalBlockchain Commited ToGlobalBlockchain

Fig. 4: UML sequence diagram illustrating geographical clustering by using PLC to communicate all the sensitive data with the consensus machines.

In the industrial domain, PLC is a great candidate for a secure information carry [13]. Using the build-in electrical cables to transport data has been investigated for a long time. However, it could be one of the candidates to communicate among the blockchain nodes while preserving security and privacy requirements. According to the IEEE Standard, IEEE 1901a-2019 is a PLC solution for broadband networks that can support a transmission rate of 860 Mbps, which is suitable for several IIoT applications. In our proposed method, shown in Fig.3, the devices that generate high priority data can communicate over PLC privately and without interfering with the other communication media and, therefore, build up their local blockchain. Then, an intermediate node that occupied with a single chip hybrid communication platform, such as the chip introduced by Semtech Corporation [14], can concatenate the local blockchains into a global one. The Semtech chip is integrated with radio frequency (RF), PLC, and Long Range low-power wide-area (LoRa) modems for smart IoT applications. Such a chip will provide the interoperability that needed to adopt the hierarchical or second-layer chain solutions.

However, we propose two scenarios, known as geographical and media clustering. The geographical clustering example can be implemented by allowing the consensus machines to utilize the PLC to exchange consensus messages. As shown in Fig. 4, all the sensitive industrial data is delivered to the consensus machines through the internal network. The IoT devices and the local consensus machines are grouped according to the geographical area (Please note that the gray area represents the communication through PLC only. The asterisk at the device name represents that the device can communicate

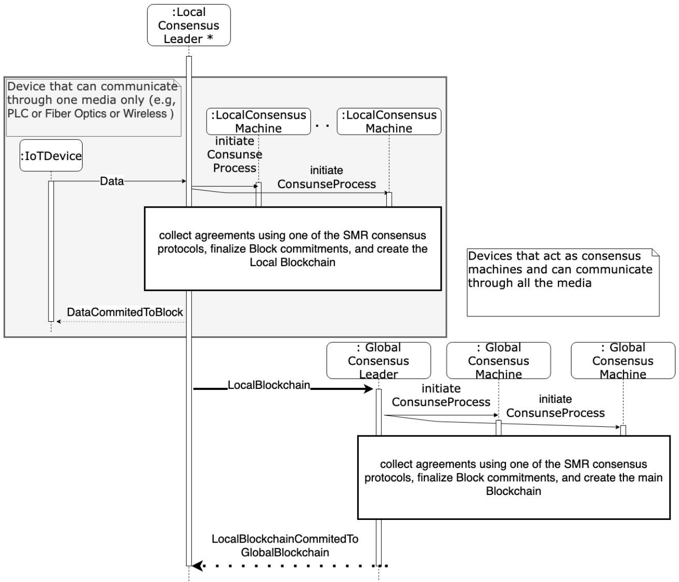
:Local Consensus Leader *
Device that can communicate through one media only (e.g, PLC or Fiber Optics or Wireless)
:LocalConsensus Machine
:LocalConsensus Machine
:IoTDevice
Data
initiate Consunse Process
initiate ConsunseProcess
collect agreements using one of the SMR consensus protocols, finalize Block commitments, and create the Local Blockchain
Devices that act as consensus machines and can communicate through all the media
DataCommitedToBlock
: Global Consensus Leader
: Global Consensus Machine
: Global Consensus Machine
LocalBlockchain
initiate ConsunseProcess
initiate ConsunseProcess
collect agreements using one of the SMR consensus protocols, finalize Block commitments, and create the main Blockchain
LocalBlockchainCommitedTo GlobalBlockchain

Fig. 5: UML sequence diagram illustrating media clustering where each group of devices both IoT devices and the local consensus machines are communicated through a specified media and create their local chains.

through multiple media). That means clustering the devices according to their distance from each other. The distance-based clustering help to improve the PLC data rate, especially when the participated devices are near to each other, and networking traffic is high. Upon, the local chain is confirmed, and the data is appended to the blocks, the reply messages are transmitted through other media such as WiFi and fiber optics to reduce the communication overheads. To concatenate the local chains to the main blockchain, the local consensus leaders have to communicate with the global consensus machines using the local networks, which further improve the system security.

The media clustering scenario, shown in Fig. 5, assumes that each group of devices both IoT devices and the local consensus machines communicate via a specified media, e.g., PLC, wireless, fiber optics and therefore create their local chains (Please note that the gray area represents the communication through a specified media only, an asterisk at the device name represents that the device can communicate through multiple media). This segregation decreases the number of participate devices that help to reduce the collision domain. Also, it helps to improve system resilience to security and privacy attacks. The local consensus leader has to be able to communicate through all the media to transmit the confirmed local chain to the global consensus machines. Therefore, the global consensus machines will initiate their consensus process and create the main blockchain.

The devices in the same network will not interface with each other through using different communication media; each has its own chain. To facilitate the communication between different parties, intermediate nodes that can provide interoperability and concatenate second-layer chains into a global one will be needed. The intermediates nodes may considerably increase the networking latency because another layer is added between the second-layer chain and the main blockchain. Therefore, the predefined delay threshold should be precisely managed to serve the delay-sensitive IIoT applications.

C. Industrial Internet of Things Future Predictions

Cryptographic functionality holds the utmost importance to allow the IIoT devices to participate with a blockchain network. The use of such computationally expensive functionality will make the IIoT sovereign and self-dependent. Many companies open new opportunities and struggle to implement the blockchain solution into the IIoT networks directly. Different devices were manufactured to enable full blockchain functionality on embedded devices and sensors, e.g., EthEmbedded [15].

In the near future, the smart industry will include remote involvement of humans and machines in real time to support the Industrial Tactile Internet (ITI). As ITI is expected to use ultra low latency communication and offers exceptionally high availability, reliability, and security, implementing blockchain in such a system becomes a big challenge. Proper integration of blockchain in ITI can introduce a new industrial revolution that enables efficient remote manufacturing of highly customized products, tracking essential data, and providing safe industrial environments to prevent accidents and hazards.

To fully support future industrial predictions, we need to see scenarios where IIoT devices will have better specifications like more data storage, processing power, and connection efficiency. Moreover, the price of hardware and the size of technology used in devices should be decreased according the well-known Moore's law. Moore's law states that transistors on microchips are increased by double in two years while reducing the hardware cost to half. However, designing new IIoT devices should incorporate the required security mechanisms in an early strategic planning phase to ensure a strong and secure smart industrial system. Rather than building a blockchain system that disinvests most of the sophisticated functionalities to satisfy the constrained IIoT devices. Finally, we give a summary for IIoT-blockchain system characteristics, uses cases, challenges, solutions and future predictions in Fig. 6.

VI. Conclusion

Blockchain is a promising solution for IIoT networks, where it can support several essential characteristics such as security, safety, reliability, and availability. However, current blockchain implementations hardly meet the IIoT strict needs and requirements due to its scalability bottleneck. Thus, prioritizing or limiting the number of redundant industrial data plays a vital role in integrating blockchain with IIoT. Context-aware solutions can help to reduce networking congestion and latency by the elimination of useless traffic. In the same context, second-layer proposals can provide independent solutions that help to scale the main blockchain with fewer overheads. Partitioning the industrial transmission domain by using build-in communication links such as PLC is another secure blockchain implementation that helps to reduce the networking traffic while maintaining the security and privacy aspects.

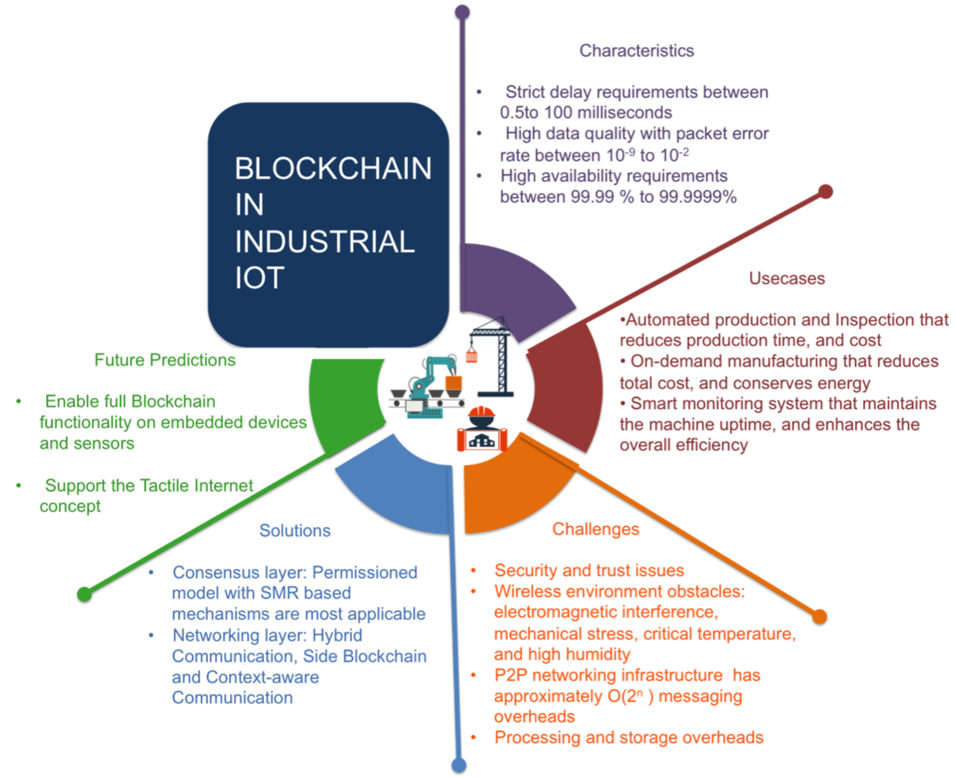
BLOCKCHAIN IN INDUSTRIAL IOT
Characteristics
• Strict delay requirements between 0.5to 100 milliseconds
• High data quality with packet error rate between 10^{-9} to 10^{-2}
• High availability requirements between 99.99 % to 99.9999%
Usecases
•Automated production and Inspection that reduces production time, and cost
• On-demand manufacturing that reduces total cost, and conserves energy
• Smart monitoring system that maintains the machine uptime, and enhances the overall efficiency
Challenges
• Security and trust issues
• Wireless environment obstacles: electromagnetic interference, mechanical stress, critical temperature, and high humidity
• P2P networking infrastructure has approximately $O(2^n)$ messaging overheads
• Processing and storage overheads
Solutions
• Consensus layer: Permissioned model with SMR based mechanisms are most applicable
• Networking layer: Hybrid Communication, Side Blockchain and Context-aware Communication
Future Predictions
• Enable full Blockchain functionality on embedded devices and sensors
• Support the Tactile Internet concept

Fig. 6: Blockchain in IIoT: characteristics, uses cases, challenges, solutions, and future predictions.

References

[1] S. Vitturi, C. Zunino, and T. Sauter, “Industrial Communication Systems and Their Future Challenges: Next-Generation Ethernet, IIoT, and 5G,” *Proc. IEEE Proc. IRE* (through 1962)*, vol. 107, no. 6, pp. 944–961, May, 2019.

[2] G. Alliance, “White paper-5G for Connected Industries and Automation,” Nov., 2018.

[3] J. Van Randwyk, “CES-21 2018 Annual Report,” Lawrence Livermore National Lab (LLNL), Livermore, CA (United States), Tech. Rep., Apr., 2019.

[4] S. Erik Josefsson, Head of Advanced Industries-Internet of Things-Stockholm, “White Paper-Manufacturing Intelligence Powered by 5G and IoT,” Oct., 2017.

[5] M. Alaslani, F. Nawab, and B. Shihada, “Blockchain in IoT Systems: End-to-End Delay Evaluation,” *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8332–8344, Oct., 2019.

[6] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, “Applications of Blockchains in the Internet of Things: A comprehensive survey,” *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1676–1717, 2018.

[7] C. H. Liu, Q. Lin, and S. Wen, “Blockchain-Enabled Data Collection and Sharing for Industrial IoT With Deep Reinforcement Learning,” *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3516–3526, June 2019.

[8] K. Toyoda, M. Shakeri, X. Chi, and A. N. Zhang, “Performance Evaluation of Ethereum-based On-chain Sensor Data Management Platform for Industrial IoT,” in *2019 IEEE Int. Conf. on Big Data (Big Data)*. IEEE, 2019, pp. 1–8.

[9] L. Bai, M. Hu, M. Liu, and J. Wang, “BPIIoT: A Light-Weighted Blockchain-Based Platform for Industrial IoT,” *IEEE Access*, vol. 7, pp. 58 381–58 393, May, 2019.

[10] Y. Xu, J. Ren, G. Wang, C. Zhang, J. Yang, and Y. Zhang, “A Blockchain-based Non-Repudiation Network Computing Service Scheme for Industrial IoT,” *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3632–3641, June 2019.

[11] B. Nour, K. Sharif, F. Li, S. Biswas, H. Moungla, M. Guizani, and Y. Wang, “A Survey of Internet of Things Communication using ICN: A Use Case Perspective,” *Comput. Commun.*, vol. 142-143, pp. 95–123, May, 2019.

[12] W. Tong, X. Dong, Y. Shen, and X. Jiang, “A Hierarchical Sharding Protocol for Multi-Domain IoT Blockchains,” in *ICC 2019-2019 IEEE Int. Conf. on Commun. (ICC)*. IEEE, 2019, pp. 1–6.

[13] L. Davoli, L. Veltri, G. Ferrari, and U. Amadei, *Internet of Things on Power Line Communications: An Experimental Performance Analysis*. Springer, Jan., 2019, pp. 465–498.

[14] “Semtech announces the Industry’s First Single Chip Hybrid PLC and LoRa Wireless Platform for Smart Grid, Smart Metering and IoT Applications,” Semtech Corporation, CA (United States), Tech. Rep., may, 2016.

[15] “Ethereum Computer Built on Embedded Devices,” Accessed Oct., 2019. [Online]. Available: http://ethembedded.com/