Blockchain Enabled Industrial Internet of Things Technology

Shanshan Zhao, Shancang Li, *Member, IEEE,* and Yufeng Yao

***Abstract*—The emerging blockchain technology shows promising potential to enhance industrial systems and the Internet of things (IoT) by providing applications with redundancy, immutable storage, and encryption. In the past a few years, many more applications in industrial IoT (IIoT) have emerged and the blockchain technologies have attracted huge amounts of attention from both industrial and academic researchers. In this paper we address the integration of blockchain and IIoT from the industrial prospective. A blockchain enabled IIoT framework is introduced and involved fundamental techniques are presented. Moreover, main applications and key challenges are addressed. A comprehensive analysis for the most recent research trends and open issues is provided associated with the blockchain enabled IIoT.**

***Index Terms*—Blockchain, Industrial Internet of Things (IIoT), Security and Privacy, Social Systems.**

I. Introduction

As an emerging technology, the Internet of Things (IoT) is becoming a significantly increased research theme and opening up new revenue streams for industrial applications [1] and social IoT environments [2]. In the past few years, the utilization of IoT solutions in industrial enterprises have grown in many sectors [3], including financial services, insurance, manufacturing, transportation, healthcare, energy, government, and real estate *etc.* The IIoT focuses on the use of IoT in above sectors, which integrates emerging technologies, such as smart sensors, robots, machine-to-machine (M2M), big data analytics, artificial intelligence, and much more into traditional industrial procedures [4], [5]. The increasing IIoT is expected to produce extraordinary economic growth opportunities and competitive advantages in industry by conducting digital transformation to create new smart industrial enterprises and build the next generation smart systems [6].

As a subset of the broader IoT, the IIoT is dramatically changing the way industries work by interconnecting facilities, systems and creating new business models [7], [8]. The IIoT platforms are able to provide industry sectors with *connectivity, intelligent big data analytic, edge and cloud computing, and application development.* Using emerging and cutting-edge technologies, the IIoT promises to change the existing industrial production procedure by optimising manufacturing procedure, enhancing customer experiences, reducing costs and increasing efficiency in smart enterprises, where smart industrial facilities and human are seamlessly interconnected. It can be seen that the IIoT will make significant impact on existing business models in many areas, including manufacturing, energy, transportation, agriculture, retail, and many more.

Despite of the aforementioned potentials, the IIoT is also facing a number of challenges [9], [10], [11], [12], including interoperability, devices security and privacy, silo mentality, standardization, *etc*. The complicated IIoT system exposes industrial control system (ICS), process control systems, and other operational technologies to potential cyber attacks, hacktivism, employment sabotage and other security risks. The main challenges that the IIoT are facing as followings [13], [14], [15], [16] can be summarized as follows:

1) **Interoperability**, it is the biggest challenge in the interconnected IIoT systems. The drive to seamlessly bridge the operation technologies (OT) and information technologies could be obstructed by both technologies challenges and the lack of common software interfaces, standard data formats;
2) **Device reliability and durability**, for devices in a harsh industrial environment (such as manufacturing, energy and utilities, transportation and retail, *etc.*), facilities reliability and durability are very important. This includes the remote access control, reliability, connectivity, and reliable services provision;
3) **Security and privacy issues**, including authentication and access control in ICS security, data protection and privacy preservation under data protection regulations, as well as the protection and security of human, industrial assets, and critical infrastructures;
4) **Emerging technologies and skills of staff**, while new technologies allow higher levels of scalability, manufacturability, and autonomously collaborate with other systems, meanwhile the lack of the skills and understanding to exploit IoT and big data will bring with challenges;
5) **Silo mentality**, break silos between different disciplines and departments in industry form another important challenge;
6) **Scalability and latency** (i.e. verification speed), are two main challenges in blockchain technologies (e.g., in Blockchain a block with size of 1MB takes 10 minutes).
7) **Standardization**, lack of standards is also a main challenge in blockchain, in addition to unclear legal and regulatory framework, lacking confidence and techniques, and many more.

The emerging blockchain technologies have been gaining

Dr. Zhao and Prof. Yao are with Department of Engineering Design and Mathematics, University of the West of England, Bristol BS16 1QY, UK e-mail: {shanshan.zhao, yufeng.yao}@uwe.ac.uk).

Dr. Li is with the Department of Computer Science and Creative Technologies, University of the West of England, Bristol BS16 1QY, UK e-mail: Shancang.Li@uwe.ac.uk.

Manuscript received January 18, 2019.

enormous attentions from both industrial and academic staff, which promises to change all aspects of digital business in industry and solve the aforementioned challenges. The blockchain is a decentralised ledger technology which makes use of cryptography to securely host applications, store data, and exchange information [17]. The blockchain is expected to make a profound effect and influence over the existing IIoT platform.

In the past a few years, the sharing economy (or digital economy in the West) has increased significantly (e.g. in China, the sharing economy is expected to comprise 10% of the whole GDP by 2020 [18]). The introduction of blockchain will significantly increase IIoT data sharing economy. The blockchain-enabled IIoT will bring the world a huge business opportunities in secure and reliable data sharing economy. According to [18], [17], the market for IIoT will reach $£93.63bn$ by 2021 and it will impact upon global GDP as $£10.82tn$ by 2030. The IIoT will create up to 60% of these values in the transformational opportunities, including new business models and revenue streams. The core focus of IIoT is on operational efficiency, along with cost optimisation and linking data islands of automatic. However, many problems such as data interoperability, data integration, privacy issues, *etc.*, are the barrier to IIoT. The blockchain is expected to enable reliable and secure data streams marketplaces in industry [5].

Together with blockchain, the big data, smart robots, IoT, and artificial intelligent (AI) are five key technologies that drive the next industrial revolution. The blockchain-enabled IIoT will play a big role in many areas, including manufacturing, transportation, logistics, retail, and utilities. Meanwhile, other sectors, such as healthcare, energy and government, will also benefit from blockchain.

The blockchain is a decentralised ledger technology (DLT) which makes the use of cryptography to securely store data decentralised and immutable, without a central authority. In fact, a number of blockchain enabled IIoT systems are in developing in many industrial areas, including security, finance, logistics, *etc.* We will explore in details how blockchain will affect and influence over the IIoT in the next following Sections. The main contributions of this work are in threefold:

- We introduce the integration of blockchain and the IIoT to solve the challenges highlighted above.
- Aims to solve the tasks of providing trust between the components of industrial IoT and business models. For this purpose, a blockchain enabled IIoT architecture is proposed which combines the IoT platforms and the blockchain.
- This paper also presents smart contract for processing and storing data related to the interaction between components in the IIoT environment.

In next Section the background and current researches are presented.

II. Background and Current Research

In the past decade, the IIoT has attracted enormous research attentions from both academia and industries and is becoming one of key technologies to enhance manufacturing and industrial processes [19]. The IIoT presents great promises in accurate and consistent real-time data processing, sustainable and green practices, predictive maintenance (PdM), *etc.* According to [4], [20], the IIoT will add $£10.69bn$ to the global economy by 2030 [4]. It is undoubted that the IIoT will benefit all industrial sectors, including agriculture, manufacturing, energy and utilities, municipal services, *etc.* by increasing efficiency, developing new business models, creating of new revenue streams, and improving safety and risk management. Figure 1 shows the basic demands in IIoT systems, from which it is noted that the trustiness over the supply chain can significantly affect the running of each participants. The blockchain can provide industrial sectors with intrinsic features of transparency, traceability, respect of human rights, and compliance of regulations in an efficient and economical way [21].

A. Blockchain Platforms for IIoT

In IIoT systems, the IIoT platform plays a key role that can deliver smart connected operations, connect assets, and enable IIoT with following capabilities: *connectivity, big data analytic, and application development*. To solve the above challenges, the IIoT platform should consider following requirements: (1) Visibility of Asset; (2) Integration of technologies; (3) Ageing workforce; (4) Data islands; and (5) Cyber security. Meanwhile, the IIoT can also significantly affect customers or users behaviours. Most existing industrial facilities, such as micro-grids, smart-grid IoT, vehicular ad-hoc networks (VANETs), *etc.*, designed are unable to connect to IIoT with built-in intelligence, which need interfaces to communicate with IIoT. On the other hand, the operators in IIoT are assisted with new technologies such as augmented reality (AR), which can provide better interacting and forecasting process behaviours therefore become simplified and operate at improved efficiency [22], [23], [24], [21].

The Bitcoin was the first blockchain platform that provides a traceable, cheap and reliable cryptocurrrency exchange way. In IIoT domain, smart IoT devices can employ Bitcoin-based techniques to record and exchange transactional activities. The Ethereum platform etherum virtual machine (EVM) is widely used in IoT with built-in smart contract features and flexible consensus strategy, in which the smart contract offers IIoT applications with down compatible. The hyperledger [25] is a popular open-source blockchain platform developed by IBM, which offers distributed industrial components with consensus and membership strategies and can well support IBM Watson IoT Platforms. The hyperledger can significantly speed up IIoT applications [26].

More blockchain platforms for IIoT, including the multichain [27], [28], Litecoin [29], Lisk [30], Quorum [31], HDAC [32], *etc.* provide IIoT applications with traceability, trustworthiness, *etc.* These blockchain platforms can be measured using energy consumptions, cup utilization, memory utilization, the size of block, *etc.*

Figure 1 shows a proposed architecture of an IIoT [4], in which the sensing layer refers the implementation facilities; the network layer provides IIoT components with connectivity; the service layer offer cloud and big data analytics services;

and the application interface layer provides application development, respectively.

B. Blockchain vs IIoT

The emerging blockchain technology shows great potentials for the fourth industrial revolution, which could make dramatic impact on all sectors of the economy and will further transform it through the top notch efficiency [4]. The blockchain shows great potential to overcome the interoperability in IIoT. According to the IDC, up to 20% of IoT deployments will offer blockchain-enabled services and more than 10% of global GDP will be re-alted to the blockchain-enabled systems by *2027* [33]. The reasons that IIoT technologies can be well complemented by blockchain are:

1) In IIoT, the decentralised nature of blockchain technology will play a key role in the communication between two untrusted devices to keep devices information about their interactions, state, and digest of exchanged data.
2) The blockchain can significantly reduce the risks that customers are facing and save the cost in business processes.
3) The blockchain for IIoT should be designed as a basis for application that involve transaction and interaction, including smart contracts, *etc*.

As discussed above, the IIoT features to build the intelligent smart ecosystems of IIoT solutions, while the blockchain can address the IIoT interoperability, reliability, and security challenges. Introducing blockchain into IIoT will enable industrial enterprises and manufactures to register and verify both their physical entities (facilities, products, etc.) and services features (i.e. smart contract) in an irrefutable and decentralised network (i.e. public blockchain). Table I summarises the main applications of blockchain technology in industry.

C. Blockchain will Revolutionise IoT

In industry, the inexpensive data-keeping and accounting blockchain idea can initiate innovative technologies that will allow enterprises and individuals to create crypto currencies and accounting programs that will revolutionise their respective industries. In general, the blockchain will offer enterprises and individuals a safer and more reliable alternative to shipping and receiving goods. In logistics, the blockchain will allow companies to keep the shipping records across multiple devices and out of criminal hands. By allowing supply change to operate more efficiently and with better trust, the blockchain can improve the interoperability in logistics. For individuals, the blockchain will keep track of what and where they have spent, which will keep an individual's credentials safe and grant them a peace of mind that is not afforded by analogy systems [36]

In IIoT, the security of ICS is a big challenge [18]. The security nature of blockchain can offer ICS in IIoT a safer environment to tampering, where blockchain can create a wide range of cyber security opportunities that would affect entire ecosystems. For example, the blockchain can ensure the entire ecosystems secure and irreversible. Since IIoT is such a huge network that connects a huge number of devices, a large number of vulnerabilities are facing by the IIoT, when new devices are connected to IIoT, the vulnerabilities will increase exponentially. Meanwhile, the cryptographic algorithms have a limited lifetime before they have broken, which means the current secure algorithms can get hacked and if hackers adapt and learn more sophisticated hack technologies. Another reason is that there are many devices are resource-constrained in the IIoT (*e.g.*, smart sensors, micro-controllers, *etc.*)

III. Blockchain-enabled IIoT Architecture

In general, the blockchain nodes can be categorised into: *full node* (FN) and *lightweight node* (LN):

- **Full node**, it can download and check all blocks and transactions. FN can act as mining node and create blocks for the blockchain.
- **Lightweight node**, due to the restrict resources, a LN does can only store and process part of data on the blockchain. In IIoT, lightweight smart devices (sensors) can serve as a LN and can propose new transactions that will be propagated between nodes and eventually will be added to a block in the blockchain.

A. System Architecture

The blockchain can enable IIoT systems connect untrusted devices in a distributed and verifiable manner. Figure 2 shows an example of architecture of a blockchain enabled IIoT system, which contains following six main components:

1) **IIoT resource networks**, including the resources that IIoT can provided
2) **Blockchain network**, which records all information in the systems onto a decentralized private network
3) **Management hub**, mainly focus on the manage and maintenance of the whole system.
4) **Key servers**, generate the necessary cryptographic keys for nodes authentications and data encryption.
5) **Clients**, are the users that request access to the IIoT resources.
6) **Smart contract**, provides system interfaces between components in IIoT and blockchain.

An IIoT system mainly contains both light nodes (LN) (i.e., smart sensors, RFID readers, smart meter, *etc.*) and powerful full nodes FN (such as industrial computer, data analysis server, edge-computing servers, *etc*). In IIoT, the LN can connect peers running a FN in order to send and receive transactions, the LN can only store minimal data about blockchain but can send output requests encoded in CoAP messages to one or more FN using JSON-RPC over `http` that is understandable by the blockchain network. Then, the FN sends back a response that can be verified by LN by only checking its own token (data, states, etc.), if passed, the LN proceeds to construct the transactions. If failed, the LN will return an invalid response with modified output, as shown in Figure 3. It can be seen that a LN can connect to peers running a full node in order to send and receive transactions. The LN can inquire remote FN for outputs and

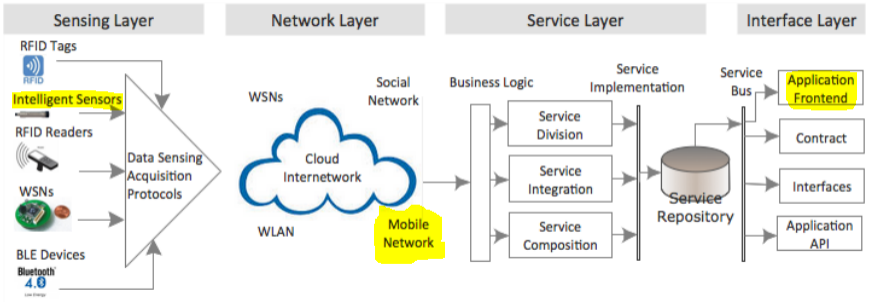

Fig. 1. An architecture of an IIoT platform [4]

TABLE I
APPLICATIONS OF BLOCKCHAIN TECHNOLOGY IN INDUSTRY

Use Case	Examples	Description
Supply chain management [34]	IBM/Maersk Provenance Everledger	Containers tracking in shipping Product information recording Certificates and transaction history
IT Services	ConsenSys	Build on request
Blockchain First	Etherum, Bitcoin	Develop using the tools provided by the blockchain
Energy platform	Siemens StromDAO	Have already been realised The Merkle tree
IoT	IoTA	is a cryptocurrency designed for the distributed fee-less micro-transactions for IoT
Vertical solutions	Axoni, Chain, R3, itBit, Clearmatics	Industry specific
IoT and Industry 4.0	Factom Iris Super computing systems IBM Watson IoT	IoT device identification over blockchain Sensos that timestamp data on the blockchain to save them from manipulation Platform to save selected IoT data on a private blockchain and share it with all involved business partners
3D Print	Genesis of Things Moog Aircraft group	Platfrom to enable 3D printing via smart contract Ensuring safe 3D-print of aircraft parts via blockchain [35]

then transmit its transactions. In IIoT environment, a LN can establish connections with multiple untrusted FN to support output retrieval, proof generation, updates to the structure, and conflict resolution. However, to improve the security between the protocols, more sophisticated mechanism needs to be developed.

In blockchain building , the top node (root FN) contains the greatest index of all outputs, and is stored at the client. Sibling nodes are concatenated and hashed to form the parent node. The maximum index between the siblings is passed onto the parent nodes. When new nodes are added into an IIoT, the clients needs to quickly work out which server is lying. The earliest point of disagreement can be found in $O(logN)$. Once the source of conflict is found, it is easy to find the lying server by checking the hash. Each FN stores limited information such as `PoW headers, Root Hash,` Own_{tran}.

B. System Interfaces

This section will discuss the interfaces in the blockchain-enabled IIoT system. It can be seen in Figure 2 that the interactions between components are defined in smart contract, as following:

1) $ResReg(d)$; $R' \leftarrow R \cup R(d)$, resources registration in blockchain, $R(d)$ is the resources that device d can provide;
2) $CReg(c)$; $U' \leftarrow U \cup R(c)$, U' is the registered clients for resource R;
3) $TokenGen(c) : T' \leftarrow T \cup TokenGen(r, c)$, is the token generated for user c related to resource r;
4) $SevReq(c) : S'_{req} \leftarrow S_{req} \cup SevReq(c, r)$;
5) $Resp(c, r) : R'_{res} \leftarrow R_{res} \cup Resp(c, r)$;
6) $AddAccess(c, R', T', R'_{req})$ define the access control added to c
7) $DeregisterClient(key, U) : U' \leftarrow U \cap U(key)$
8) $DeResReg(R, r) : R' \leftarrow (R - r) \cap R_{key}$.

From the above descriptions it can be seen that the clients and resources will be identified by their public keys and the access to resources requested by c can be added depends the response of the blockchain.

For a more complicated IIoT system, the distributed ledger technology blockchain allows digital information to be distributed and immutable, therefore, blockchain has the potential to be a good anti-corruption and fraud tool. To keep privacy, many IIoT systems require to (1) keep the sender and receiver identities confidential from peers, (2) carry out the transactions between two participants to be masked with the actual spent coin, and (3) hide the denominations in transactions.

For a large scale IIoT, it is very important to guarantee the scalability of the system. Figure 4 shows an example of a multiple chain blockchain based IIoT system, which provides secure authentication, smart contract, and transactional chained in a single IIoT platform.

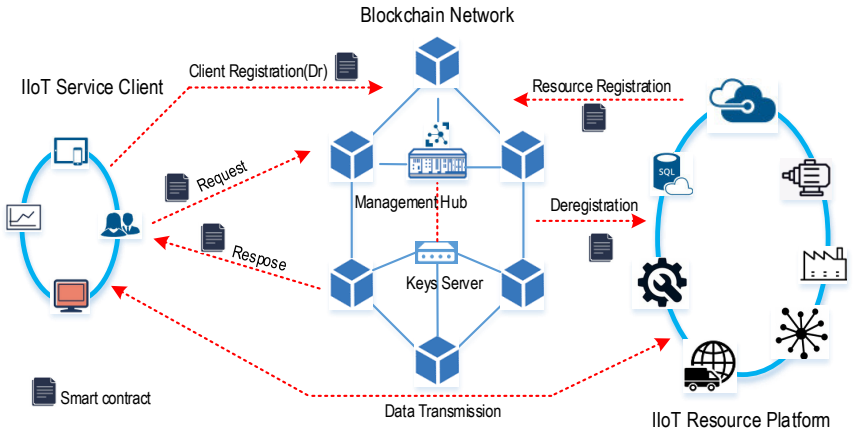

Fig. 2. Blockchain enabled IIoT Architecture

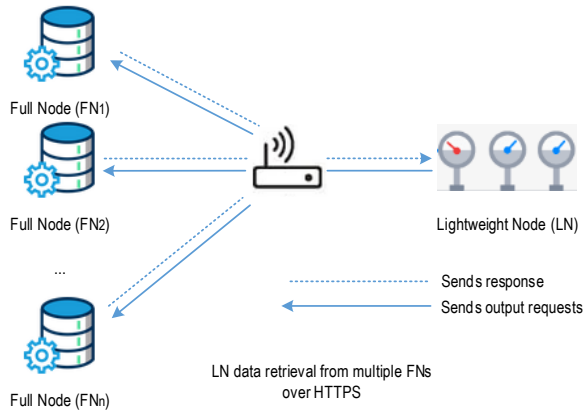

Fig. 3. LN data retrieval from multiple FNs

C. Integrating Blockchain into Existing IIoT

The blockchain is able to securely exchange and store data from components in IIoT systems without the need for an intermediary. The secure nature of blockchain will enable IIoT systems more dependable and safe, which can change the way the data is being deal with in IIoT. The features of blockchain makes it promises in creating new business models, such as data streaming sharing, financial, manufacturing, smart healthcare, *etc.* The decentralized collaborative IIoT systems can sense, share, and update data in a reliable manner that can be verified easily. Meanwhile, the blockchain can well manage and secure digital relationships of participants in IIoT and with the decentralized authenticity, trustiness issues in IIoT between multiple parties can be fixed. In the past few years, a number of blockchain enabled IIoT use cases have been reported, including manufacturing, financial, energy industries, insurances, *etc.*

1) Solutions: It is obvious that the ecosystems in IIoT are not turely secure. A commonly approach is to use microchips to streamline IoT security. Secure microchips are required for industrial devices, for example, for some ICS systems, the micro-controllers should be able to protect its chip memory using a memory-protect unit (MPU), and only approved cryptographic algorithms can be used in these systems. However, a challenge is that the chips manufacturers do not like to share their details of the solution to others. In this case, the blockchain based IIoT platforms are expected to secure the IIoT ecosystems in a matter of difficult to hack but easy to verify.

2) Public Device Blockchain: A number of device blockchain have been developed for IIoT, in which an irrefutable and decentralised public blockchain are used to secure register and record the devices to develop a secure and tamper proof way. The blockchain-enabled infrastructure in IIoT will enable an automation of cyber-defense. When attacks are detected, the IIoT platforms are able to automatically thwart them. Most existing IIoT security systems operate as a set of individual tools and are neither automated nor integrated.

D. Main Features in Blockchain-enabled IIoT

1) Interoperability: As discussed above, the interoperability is a big challenge in IIoT. In many existing IoT systems, the interoperability is managed at the application level, where the operators are required to be proficient in different smart operations. However, a huge volume of data will be created from interconnected facilities in IIoT, which requires a higher level of interoperability. Lack of interoperability among existing field systems is a major challenge of IIoT. Existing OT system largely work in silos that can increase the running costs and complexity of IIoT deployments. To bridge the gaps of shared data between smart facilities from different manufactures (or even in an organization) is always very challenging. The blockchain promises to establish seamless links between IIoT assets operating in different data protocols. However, it requires the developers to be proficient in different smart contract language, API, or third part of tools. Figure 5 shows an example of IIoT architecture to convert real-time data into business insights.

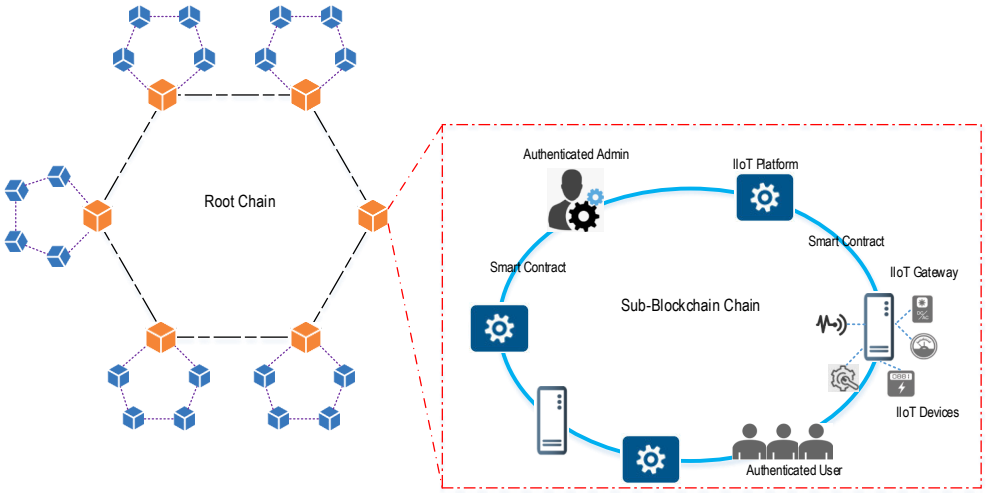

Fig. 4. Multi-chained IIoT Platform

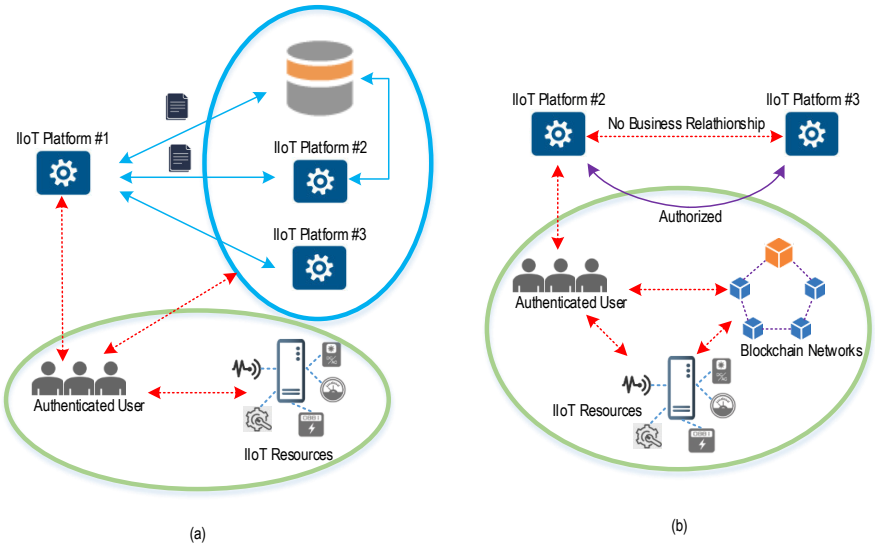

Fig. 5. IIoT architecture to convert real-time data into business insights (Interoperability)

Interoperability in IIoT is often focused around the data exchanges between business entities, for example, multiple companies follow the same standards. The interoperability denotes the ability of different IIoT systems and applications to communicate, exchange data, and use the information that has been exchanges [19]. The interoperability can reduce duplicate information and improve the efficiency, which is necessary in reducing cost, comprehensive. As shown in the example in Fig 5, the interoperability is generally centred around business entities.

In the blockchain-enabled IIoT, as shown in Fig 5, the authenticated users can directly retrieve data from platform #2. It can be seen that with built-in smart contracts, a user can authorize sharing of his data between two platforms without a formal business relationship: #2 and #3. The blockchain-enabled IIoT system stores authorization rules, user-associated public keys, and data access audit logs. Each organization will maintain the public key with their own user index system using smart contract-driven authorization rules.

In Figure 5 (a), data interfaces are entity-to-entity, in Figure 5 (b), data exchange using user-to-entity, the entity can directly access the data related products. In the blockchain-enabled solution, the product can retrieve data directly from supplier #1, however, through blockchain-enabled smart contracts, the product can authorize sharing of product data between $supplier\#1$ and $supplier\#2$, which does not have a formal business relationship. The blockchain layer stores authorization rules, along with other data like public key, as well as data access audit logs.

It can be seen that the blockchain can significantly improve

the **interoperability**, given these challenges, it remains to be seen whether blockchain can facilitate the transition from user-centric to data-centric data sharing.

2) Greater transparency: The blockchain technologies can make the data exchange, transactional data exchange more transparent. As a decentralized ledger, all network participants share the same documentations as opposed to individual copies, which can only be updated through consensus and each participant must agree on. Any change at a single transaction record would require the alternation of all subsequent records and the collusion of the entire network. As a result, data on a blockchain is accessible for all participants and is more accurate, consistent and transparent than when it is pushed through paper-heavy processes.

3) Improved traceability: The blockchain technology offers an opportunities to solve important glitches in traceability and provenance challenges in the IIoT. Due to the complexity of interactions between the stakeholders in traditional supply chain, it is very challenge to accurately track and link information to material without any bias between different stakeholders. The traceability are very important, in global supply chain, drugs, clinical trials, food, *etc.*

In blockchain enabled IIoT, the digital assets can be attributed with a traceable resource unit (TRU), which is a collection of one or more objects (goods) that cannot be individually traced further. The availability of details of transactions in IIoT, including price, data, location, quality, certification, or other relevant information within a smart contract can increase traceability of material through along the blockchain chain. The blockchain can offer precisely traceability for items in a complex supply chain. The blockchain can offer a global, inclusive solution for traceability.

4) Accountability vs Security Privacy: In IIoT, the accountability is fundamentally to developing trust in IoT devices and IoT services [37], in which all transactional events, data, should be ultimately attributable to some user or agent. Accountability offers greater responsibility to both service providers and users or the third part authorities holding services responsible for their functionality and behavior. In blockchain, a digital pseudonyms (a hash of an address) is used to provide some level of anonymity and each participant in the network can trace the activities of an entity with a given unique ID, this property further contributes to make the blockchain an interesting tool to build a tamper-proof log to be used in accountable IIoT.

The distributed ledger blockchain allows a secure platform, distributed, tamper-free, requires a sufficiently large network of untrusted peer. The privacy in blockchain-enabled IIoT involves data ownership, data transparency and auditability, and fine-grained access control, including permissions of data and IoT devices in IIoT.

IV. Key Enabling Technologies

In the past a few years, both the blockchain and the IIoT technology have been gaining enormous attention in industry applications, including security, finance, logistics, manufacturing, smart grids, etc. This section summarises the key technologies in blockchain enabled IIoT.

A. Identification and Tracking Technologies

The IIoT platform is a key component in IIoT, which involves following key technologies: (1) *Device identification and tracking technologies* in IIoT environment, which include pseudo-identity generation for IIoT devices, users, and services using public-key based pseudo-identities generation. (2)*Communication Technologies in IIoT*, in which the M2M communication technologies are the main stream. RolaWAN, Sigfox, et al are also useful. (3) *Networks Technologies in IIoT*, include the 5G, mobile network, industrial sensor networks, *etc.*; and (4) *Service management in IIoT*, OSGi platform, *et al.*

$$ID_{u,s}^{public} = G(pk_{sig}^{u,s}, pk_{sig}^{u,s}) \tag{1}$$

in which u and s are secure channel.

B. Blockchain across IIoT Nodes

As discussed in Section II, a blockchain system consists following main components: `hash function`, `transactions`, `cryptography key system`, `address`, `ledgers`, and `blocks`, *etc.*

1) Hash: is frequently used one way functions in blockchain, e.g., SHA256, which consists of $2^{256} = 10^{77}$ possible digest values.

2) Transaction: a transaction is a recording of exchange of assets (in IIoT, it could be data, digital values, units of inventory, *etc.*) between two participants. Each block can contain a number of verified and traceable transactions. A transaction record at list contains following information fields: `amount`, `inputs`, `outputs`, `timestamp`, `transaction ID` & `hash`, and more.

3) Public Key Infrastructure (PKI): PKI includes a pair of mathematically related keys (public key and private key). The public key can be public for all participates, but the private key remains secret for each participant in the blockchain system. The private key is generally used to sign transactions in blockchain systems and public key is usually to generate address by working with hush functions. In blockchain, the PKI are designed in a manner of hard to hack but easy to verify. PKI enables participants to efficiently verify transactions.

4) Address: An address of a participant can be generated from its' public key using hash functions and some additional information. For example, in Bitcoin system, the Bitcoin address for each user is derived from its 256 bits private key created using ECDSA standard)

$$Address = Base58(Privatekey) \tag{2}$$

5) Ledgers: a distributed ledger is a collection of verified and traceable transactions that is spread across all participants in a blockchain system (can be nodes, or computing devices or servers). Each node replicates and stores an identical copy of the ledger. The ledgers can be programmed to record everything of value (for example, in financial, it would be financial transactions, but in IIoT, it could be token, data, or even events). The ledger is maintaining through the use of distributed consensus mechanism.

Figure 6 describes an example of blockchain-enabled retail system, which records all transactional activities generated

in the procedures. Figure 7 shows a simple example with 4 nodes IIoT, where each node keeps a ledger. For example, in Figure 7, it can be seen that in step (1) a new transactional event (TE) $TE\#(n+1)$ is submitted to $node_B$, (2) B will then alert the rest nodes in the network (A, C, and D) that a new transaction $TE\#(n+1)$ has arrived; (3) at this point, $TE\#(n+1)$ is a pending transaction, and not included in a block within ledger; (4) A node will include $TE\#(n+1)$ within a block and complete the systems' required consensus method; (5) The new block that includes $TE\#(n+1)$ will be distributed across the blockchain and all other ledgers will be updated with the new block that includes $TE\#(n+1)$.

6) Chaining Blocks: Participants in blockchain may verify the most recent transactions that have not yet embedded into any prior blocks. A block can be seen as a page of the ledger that integrates all submitted transactions and then propagates in the whole system, which will be mined by a mining node and further added to the blockchain. Each block includes a block header, which contains the hash of block header of the previous block. It can be seen that this is a nice way to accurately chain all blocks in a blockchain system. Figure 8 shows an example of a simple blockchain header. A block typically consists of following data fields as shown in Table II

In Table IV-C3, the Merkle tree is used to store the hash of every transactions. Figure 9 shows an example of a Merkle tree in blockchain system, in which the `data0, data1` represent the transaction data, and $hash$ denotes the hash function used in the blockchain. It can be seen that the `root` combines the hashed hash value of all transaction data, which is the hash of all previous hash-combination.

C. Consensus Models in Blockchain

Many FNs serve as mining nodes which are competing to gain the right of publishing the new generated block. However, in the peer-to-peer blockchain system, when multiple FNs generated new blocks at approximately the same time, a consensus mechanism will be applied to make a consensus decision to select the `next block` of the blockchain. In general, consensus models in blockchain systems may have following features: (1) The initial state of the blockchain is agreed upon by all participants; (2) All participants agree to the consensus method for adding new blocks to the blockchain; (3) New block is chained to the previous block using the hash of block header; (4) All participants can easily verify every block.

In this section, we summarised the commonly used consensus models.

1) Proof of Work (PoW): In the PoW model, a participant can get the right to publish new block by solving a computationally expensive problem (for example, a puzzle in Bitcoin). The problem is very difficult to solve, but easy to verify, which enables other participants to easily validate the proposed next block. For example, in Bitcoin, each mining node computes the hash (SHA256) for the entire block header that match "leading zero criteria"

$$0x00000 = SHA256(H_{block} + Nonce) >> 59 \qquad (3)$$

in which increasing the number of 'leading zero' will cause the significant additional difficulty to solve the puzzle. It can be seen that the PoW model combines the trustless consensus and cryptographic. In blockchain, the puzzle difficulty adjustable, i.e., in Bitcoin it is adjusted every two weeks. The PoW has been widely used in a number of Blockchain applications, including `Bitcoin, Ethereum, Nonero, Dash, Litecoin, Dogecoin, etc.` [38]

2) Proof of Stake (PoS): The PoS takes the proportional ownership of the stake to participant in the validation of transactions. Depending on the relative amount of tokens a participant stakes, the probability they will be chosen as the next block raise.

The blocks created by participants with more stake are more likely to be selected as next blocks. The PoS consensus model does not need perform intensive computations and can save energy consumptions, time, and resources. In PoS, no block reward for the creator. A number of digital currencies use PoS, including Peercoin, ShadowCast, Nxt, BlackCoin, NavCoin, *et al.* It is worthy noting that the Ethereum is planning to implement its PoS protocol Casper in 2018/19 [39]. The disadvantage of PoS is that it is quite complex to implement PoS in a blockchain system.

3) Round Rubin (RR): In many complicated blockchain systems, there might have different level of trust between participants (for example, in IIoT, different devices might be in different security level). The PoW or PoS consensus model would be too complicated to determine, while a simple round robin consensus model will be more effective, in which nodes take turns in creating blocks. In case a participant is unavailable in its turn, the RR model uses nounce to handle turn to available participants to publish blocks. A problem of RR model is that it does not work well in the permisionless network due to malicious participants can cause odds of subverting the network.

4) PBFT: Practical Byzantine Fault Tolerance (PBFT) algorithm have been well discussed in [18], [40], [41], [42], which works on the assumption that the number of fault participants less than one third of all participants.

5) Other Consensus Models: There are a number of consensus models have been proposed for blockchain systems, including Ripple, multichain, sieve, raft, proof of elapsed time, quorum, and Federated consensus. In practical, it is important to properly design consensus mechanisms depends the requirements of applications.

D. Smart Contract

As discussed above, a smart contract is an automatically executable script and enforceable by FNs and LNs that participate in the blockchain management [37]. In blockchain-enabled IIoT, the interaction is mediated through smart contracts, where smart contracts can well encode and drive business logic process. For IIoT, the smart contract can be implemented in an efficient and more reliable decentralized way.

In IIoT, smart contracts define the rules and penalties around an agreement in the same way that traditional

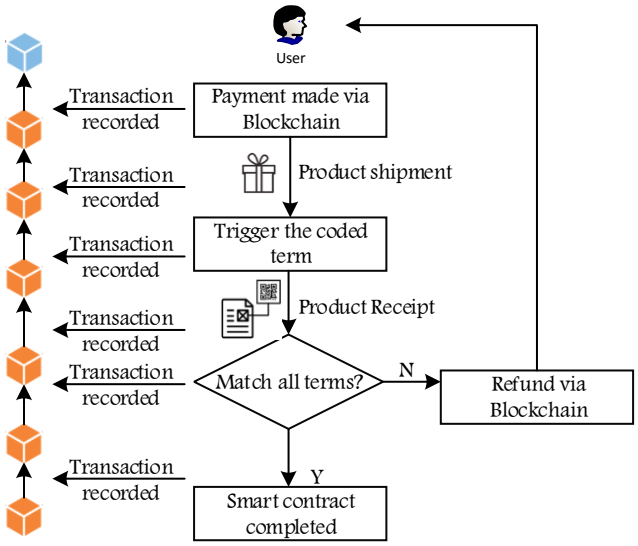

Fig. 6. Example of a ledger across IIoT nodess

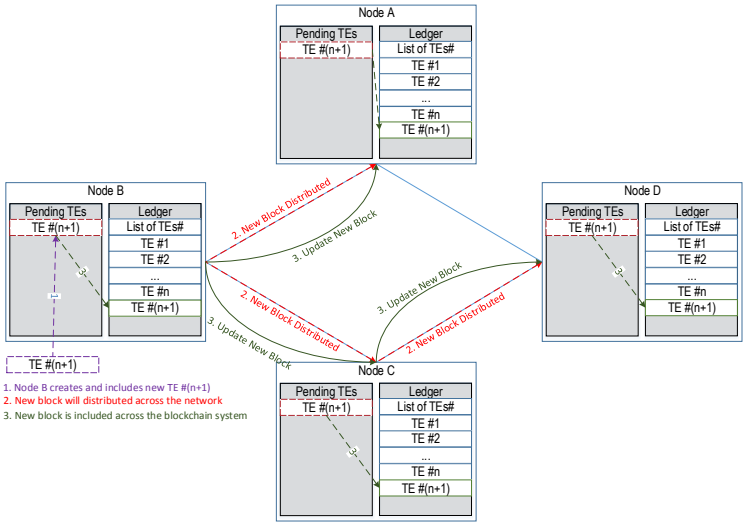

Fig. 7. Example of update of new TE across Blockchain systems

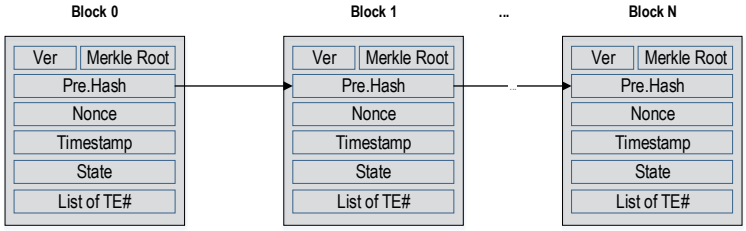

Fig. 8. Chaining of Blocks with TEs

Data Field	Description
Block number	block height
Current hash	hash value of current block
Previous hash	the hash value of previous block
Merkle	Merkle tree
Timestamp	the time stamp of xx
Block size	The size of the block
Nounce	Nounce value, manipulated by the mining node to solve the hash puzzle that gives them the right to publish the block
Transactions list	List of Ts included within the block

TABLE II
DATA FIELDS IN A BLOCK

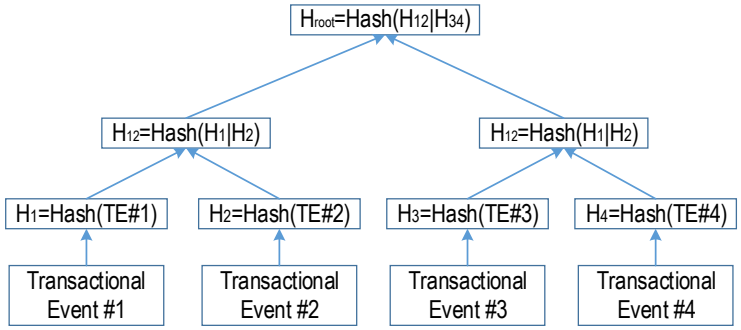

Fig. 9. Example of a Merkle Tree

	PoW	PoS	RR
Energy consumption	high	low	low
Equipment	Mining (ASIC, GPU)	No equipment	no
Security	High	Untested	low
Block Size	1MB	-	
Decentralised	Tends to centralise	Users can remain in control of their tokens	
Example	Bitcoin, Ethereum, Zcash	Ethereum after Casper	Permissioned Private

TABLE III
CONSENSUS MODEL IN BLOCKCHAIN

contract does without introducing a middleman. Smart contracts can help participants in a blockchain system exchange data, assets, shares, or conflict-free way while avoiding the services of a middleman [43]. Basically, a smart contract consist of following main components: `parties`, `triggering events`, `regulators`. Smart contract has been widely used in many industrial areas, such as financial derivations to insurance premiums, data extraction, product design, healthcare, insurance, *etc.* The smart contract can provide IIoT many benefits, including `autonomy`, `trust`, `traceability`, `safety`, `efficiency`, `auditability`, `accuracy`. However, there are still a few challenges in the deployment of smart contract must be addressed: (1) bug-free code; (2) governments regulations and taxation, *etc.*

V. KEY APPLICATIONS IN IIOT

The blockchain technology has been widely used in industries, including finance, e-government, manufacturing, e-healthcare, energy, real estates, education, *etc.* In finance, blockchain shows huge promises and has been used to build new market, cryptocurrency (up to 2068, according to coinmarketcap), payment and investment systems, such as `Ripple`, `Litecoin`, `Nxt`, `Peercoin`, `Dogecoin`, `Monero`, `etc.`

In e-government systems, the blockchain can offer effective identification verification over distributed ledger to store identities, such as e-passport in Dubai, e-identity in Estonia, blockchain based land registration, *etc.*

Modern supply chains have become increasingly sophisticated, and their impact on the competitiveness of many companies is an important factor to take into account, for example, the shared economy, the traditional taxi is competing with shared ‘didi, and the shared ‘haohaoyun has make great eco-and social logistics industry in China.

In blockchain-enabled IIoT applications, Ethereum is one of the most popular platforms, which can provide more features. The emerging M2M and 5G technology can significantly enhance the deployment of blockchain in IIoT. Figure 10 illustrates an example of IIoT in supply chain applications.

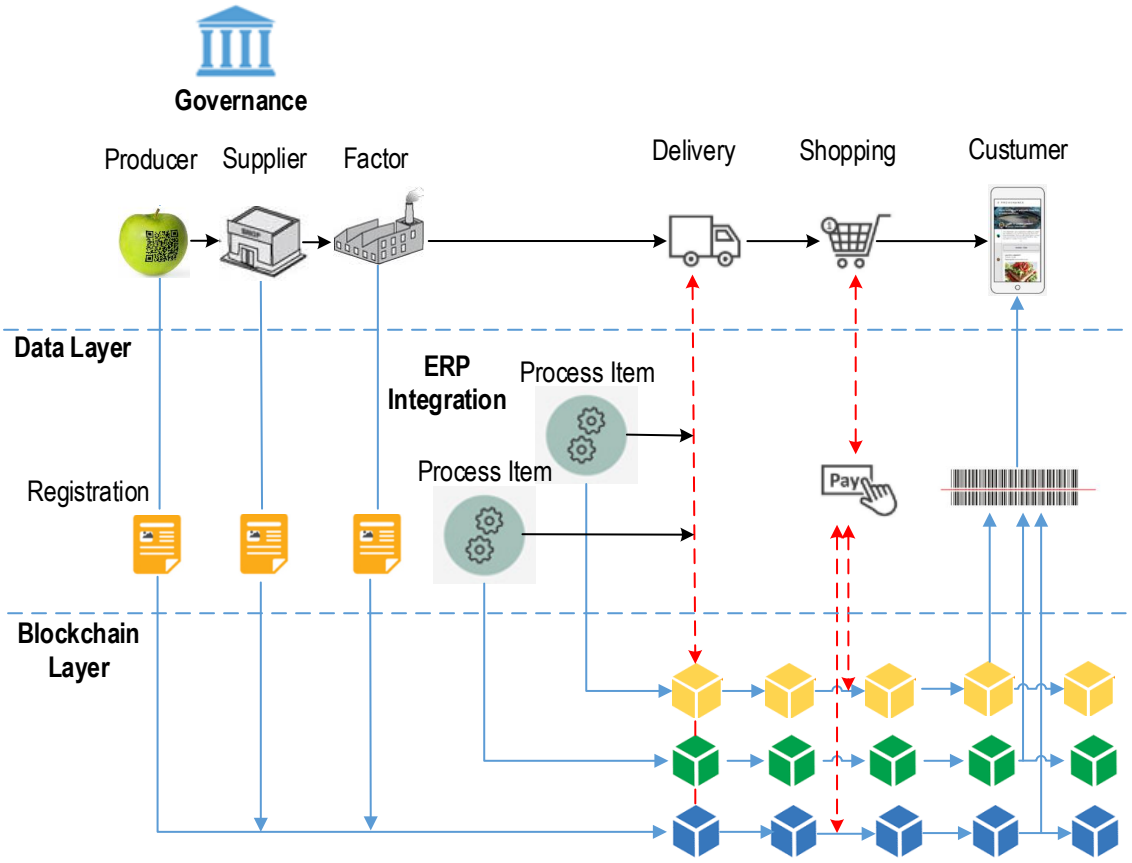

Fig. 10. Applications of Blockchain in IIoT

VI. Research Challenges and Future Trends

The blockchain enabled IIoT aims at developing a redundant, traceable, and secure complex interconnected IIoT environment. The blockchain enabled IIoT is still facing many challenges that must be addressed before it can be widely accepted and deployed in industries.

A. Technical Challenges

Although many research efforts have been conducted in the past few years both in blockchain and IIoT, there are still many challenges need to be addressed:

1) Security and privacy, in decentralized IIoT systems, the privacy and confidentiality, including entity identity, confidential and zero-knowledge transactions, crypto blinding, *etc.* are still very challenging.
2) Margin erosion and arbitrary changes, rapidly changing demands business process require the IIoT system can quickly react on an increasing frequency. To further improve the efficiency, reduce risk management, and provide trustiness between participants are still very challenging.
3) Modelisation of information is a major challenge. An IIoT ecosystem consists of large number of entities, to present each entity in blockchain (as `token`) in a traceable and transparent way. It is a major challenge to model raw information in a reasonable granularity level.
4) Supporting infrastructures in blockchain enabled IIoT. Integrating blockchain into IIoT involves implementation of the blockchain capability over the supporting infrastructures.
5) Overall agreement in the IIoT ecosystem requires all stakeholders to commit to investing in and using these new features. The sustainability and traceability of all entities and transactional events should be addressed in blockchain enabled IIoT.

B. Standardization Blockchain IIoT

The ISO approved the international standards on blockchain proposed by Australia in 2016 and the new standard for blockchain and distributed ledger technology (ISO/TC 307) is to be published in 2019 [44], [45]. Actually, there a number standards development activities relating to blockchain are in developing that covers main topics in blockchain, such as terminology, privacy, governance (AS ISO/IEC 37500), interoperability, security, and risks.

In industry, the UK and Europe have developed a number of standards to support financial transactions and the role of standards in building market confidence by addressing blockchain issues relating to the governance, authentications,

interoperability, and privacy. The standardization of blockchain technology should align to relevant existing international industry standards.

From the viewpoint of IIoT developers, the blockchain standardisation will play a key role in shaping the future of the technology. The blockchain standardization should be able to provide guidance to developers and users of blockchain technology.

C. Security and Privacy in Blockchain enabled IIoT

In the evolving IIoT ecosystem, security incidents and vulnerabilities are on the increase [46]. The sheer scale and inextricable interconnectedness of IIoT significantly expanded the security attack surfaces and there is much to be done from device authentication to the formal verification of new generation of smart contracts. Specifically, the security and privacy research of smart contract is an emerging area. It is important to consider following IIoT features in implement security solutions: (1) The identity and access management of digital primer; (2) Dynamic and continuously evolve of the entities in IIoT; (3) The heterogeneous with respect to communication, platform, devices, etc.; (4) Insecure design for IIoT infrastructure, devices, and users and privacy issues. Meanwhile, the privacy issues are very challenges in blockchain enabled IIoT, including:

- Threats arise for enterprise perimeters
- Privacy-sensitive information can be easily disclosed to third part
- Major privacy concerns arise for health-related data from the use of medical devices and fitness applications
- Wearable device collect huge amounts of personal data as well as data about the user environment

Meanwhile, the legal changes should also be considered in the blockchain-enabled IIoT. Both the Network and Information Security (NIS) Directive and the wide legal framework for personal data privacy General Data Protection Regulation (GDPR) became effective on may 2018. The GDPR is a regulation on data protection and privacy proposed by EU, which aims to give individuals the right to protection of their own data. The GDPR aims at creating a uniform data regulation framework within EU and to strengthen individuals control and use their personal data. For the new NIS Directive and GDPR, the data protection in blockchain environments is still an open problem. In the blockchain enabled IIoT, we need consider the new notification rules around personal data breaches, where blockchain IIoT applications need to permit actions like: search for all instances of personal data related; extract that data and provide it to the individual in a portable format; edit or remove the data on request. However, due to the immutability of blockchain, to remove data from blockchain is difficult. The IIoT platform should be able to delete a certain personal data from a previous block, although which would break the hash pointers between the blocks, but the platform can simple update the links by re-hashing the block and new technologies to be developed.

D. Research Trends

The shift towards blockchain enabled IIoT brings with numerous challenges as addressed above, a number of practical limitations and challenges around blockchain that will need to be addressed as these areas are explored. Future research directions include:

1) Mobility-aware fine-gained analysis, using 2-hop knowledge to construct geometric constraints w.r.t. fixed system of coordinates; attestation techniques for IoT, extending Kalis to perform attestation;
2) Bring-your-own-IoT (BYOT), enabling containerization and policies onto IoT, cloud-enabled devices, and IoT identity, identifying IoT devices by traffic patterns, leveraging identity for cloud repository of policies;
3) Incentivizing interoperability in blockchain enabled IIoT will continue to be an key research issue;
4) Security and privacy considerations, implementation of anonymous operations, as well as device identification, key managements, user engagement, will also need consideration. The privacy regulations (such as GDPR) need to clearly address data authorization and storage rules;
5) Since the lack of standards for blockchain technologies and DLT, the integrity of blockchain and existing industrial standards, protocols, and the data storage over cloud systems will be a key research issue;
6) The coming fifth generation of communication technology (5G) is a key research trend in blockchain enabled IIoT, which characterises ultra high speed, ultra low latency, and massive access and can offer new capabilities to the IIoT. Future work will need to consider the aggregate effect of 5G, blockchain in IIoT.

VII. Conclusion

In a complex IIoT ecosystem, various entities are integrated together to create, collect, process, transmit, and store data. The industries have strong interest in blockchaining both IIoT entities and the business processes. Due to the rapid advances in technology and innovations on business models, IIoT is expected to be widely applied to industries. In this paper we have addressed the integration of blockchain and IIoT from the industrial prospective. A blockchain-enabled IIoT framework is introduced and involved fundamental techniques are discussed. Key applications and challenges are addressed. We also analysed the research challenges and future trends associated in blockchain enabled IIoT.

References

[1] M. Yli-Ojanper, S. Sierla, N. Papakonstantinou, and V. Vyatkin, "Adapting an agile manufacturing concept to the reference architecture model industry 4.0: A survey and case study," *Journal of Industrial Information Integration*, 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2452414X18301377

[2] B. Zhou, C. Maines, S. Tang, Q. Shi, P. Yang, Q. Yang, and J. Qi, "A 3-d security modeling platform for social iot environments," *IEEE Transactions on Computational Social Systems*, vol. 5, no. 4, pp. 1174–1188, Dec 2018.

[3] P. K. Sharma and J. H. Park, "Blockchain based hybrid network architecture for the smart city," *Future Generation Computer Systems*, vol. 86, pp. 650 – 655, 2018.

[4] L. D. Xu, W. He, and S. Li, "Internet of things in industries: A survey," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 4, pp. 2233–2243, Nov 2014.

[5] S. Li and S. Zhao and P. Yang and P. Andriotis and L. Xu and Q. Sun, "Distributed Consensus Algorithm for Events Detection in Cyber Physical Systems," *IEEE Internet of Things Journal*, pp. 1–1, 2019.

[6] J. M. Müller, D. Kiel, and K.-I. Voigt, "What drives the implementation of industry 4.0? the role of opportunities and challenges in the context of sustainability," *Sustainability*, vol. 10, no. 1, p. 247, 2018.

[7] D. Kiel, C. Arnold, and K.-I. Voigt, "The influence of the industrial internet of things on business models of established manufacturing companies–a business level perspective," *Technovation*, vol. 68, pp. 4–19, 2017.

[8] C. Perera and D. S. Talagala and C. H. Liu and J. C. Estrella, "Energy-Efficient Location and Activity-Aware On-Demand Mobile Distributed Sensing Platform for Sensing as a Service in IoT Clouds," *IEEE Transactions on Computational Social Systems*, vol. 2, no. 4, pp. 171–181, Dec 2015.

[9] J. Huang, L. Kong, G. Chen, M. Wu, X. Liu, and P. Zeng, "Towards secure industrial iot: Blockchain system with credit-based consensus mechanism," *IEEE Transactions on Industrial Informatics*, pp. 1–1, 2019.

[10] Y. Sun, L. Zhang, G. Feng, B. Yang, B. Cao, and M. A. Imran, "Blockchain-enabled wireless internet of things: Performance analysis and optimal communication node deployment," *IEEE Internet of Things Journal*, pp. 1–1, 2019.

[11] A. Meloni, S. Madanapalli, S. K. Divakaran, S. F. Browdy, A. Paranthaman, A. Jasti, N. Krishna, and D. Kumar, "Exploiting the iot potential of blockchain in the ieee p1931.1 roof standard," *IEEE Communications Standards Magazine*, vol. 2, no. 3, pp. 38–44, SEPTEMBER 2018.

[12] D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, "Internet of things security: A top-down survey," *Computer Networks*, vol. 141, pp. 199 – 221, 2018.

[13] S. Li, L. D. Xu, and X. Wang, "Compressed sensing signal and data acquisition in wireless sensor networks and internet of things," *IEEE Transactions on Industrial Informatics*, vol. 9, no. 4, pp. 2177–2186, Nov 2013.

[14] P. Nash. (2017) Challenges of the industrial internet of things. [Online]. Available: https://www.invma.co.uk/blog/iiot-challenges

[15] S. Li and K. R. Choo and Q. Sun and W. J. Buchanan and J. Cao, "IoT Forensics: Amazon Echo as a Use Case," *IEEE Internet of Things Journal*, pp. 1–1, 2019.

[16] M. Isaja and J. K. Soldatos, "Distributed ledger architecture for automation, analytics and simulation in industrial environments," *IFAC-PapersOnLine*, vol. 51, no. 11, pp. 370 – 375, 2018, 16th IFAC Symposium on Information Control Problems in Manufacturing INCOM 2018.

[17] M. A. Khan and K. Salah, "Iot security: Review, blockchain solutions, and open challenges," *Future Generation Computer Systems*, vol. 82, pp. 395 – 411, 2018.

[18] A. Gottheil. (2018) Can blockchain address the industrial iot security? [Online]. Available: http://iiot-world.com/cybersecurity/can-blockchain-address-the-industrial-iot-security/

[19] W. J. Gordon and C. Catalini, "Blockchain technology for healthcare: Facilitating the transition to patient-driven interoperability," *Computational and Structural Biotechnology Journal*, vol. 16, pp. 224 – 230, 2018.

[20] Y. Yuan and F. Wang and D. Zeng, "Competitive Analysis of Bidding Behavior on Sponsored Search Advertising Markets," *IEEE Transactions on Computational Social Systems*, vol. 4, no. 3, pp. 179–190, Sep. 2017.

[21] F. Wang and Y. Yuan and J. Zhang and R. Qin and M. H. Smith, "Blockchainized Internet of Minds: A New Opportunity for Cyber-PhysicalSocial Systems," *IEEE Transactions on Computational Social Systems*, vol. 5, no. 4, pp. 897–906, Dec 2018.

[22] M. U. Hassan, M. H. Rehmani, and J. Chen, "Privacy preservation in blockchain based iot systems: Integration issues, prospects, challenges, and future research directions," *Future Generation Computer Systems*, vol. 97, pp. 512 – 529, 2019.

[23] R. Sahay, W. Meng, and C. D. Jensen, "The application of software defined networking on securing computer networks: A survey," *Journal of Network and Computer Applications*, vol. 131, pp. 89 – 108, 2019.

[24] P. Radanliev, D. C. D. Roure, R. Nicolescu, M. Huth, R. M. Montalvo, S. Cannady, and P. Burnap, "Future developments in cyber risk assessment for the internet of things," *Computers in Industry*, vol. 102, pp. 14 – 22, 2018.

[25] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich *et al.*, "Hyperledger fabric: a distributed operating system for permissioned blockchains," in *Proceedings of the Thirteenth EuroSys Conference*. ACM, 2018, p. 30.

[26] R. Naidu and A. Irrera. (2018) Multichain private blockchain white paper. [Online]. Available: https://www.multichain.com/download/MultiChain-White-Paper.pdf

[27] G. Greenspan. (2017) Nestle, unilever, tyson and others team with ibm on blockchain. [Online]. Available: https://www.reuters.com/article/us-ibm-retailers-blockchain/nestle-unilever-tyson-and-others-team-with-ibm-on-blockchain

[28] M. Samaniego and R. Deters, "Internet of smart things - iost: Using blockchain and clips to make things autonomous," in *2017 IEEE International Conference on Cognitive Computing (ICCC)*, June 2017, pp. 9–16.

[29] Litecoin. (2019) The cryptocurrency for payments. [Online]. Available: https://litecoin.org/

[30] Lisk. (2017) Lisk protocol documentation. [Online]. Available: https://lisk.io/documentation

[31] Quorum. (2019) Quorum whitepaper v0.2.pdf. [Online]. Available: https://github.com/jpmorganchase/quorum-docs/

[32] HDAC. (2018) Hdac white paper udpate (version 1.2.0). [Online]. Available: https://www.hdactech.com/en/News/news.do?mode=view&articleNo=16006

[33] M. I. Vincent Dieterich *et al.* (2017) Application of blockchain technology in the manufacturing industry. [Online]. Available: https://medium.com/@philippsandner/application-of-blockchain-technology-in-the-manufacturing-industry

[34] F. School. (2019) Blockchain center. [Online]. Available: https://www.frankfurt-school.de/home/research/centres/blockchain

[35] S. Li and D. Zhang, "A novel manifold learning algorithm for localization estimation in wireless sensor networks," *IEICE Transactions on Communications*, vol. 90, no. 12, pp. 3496–3500, 2007.

[36] D. Howard. (2018) How blockchain will revolutionize iot. [Online]. Available: http://www.iotevolutionworld.com/iiot/articles/436753-how-blockcha-will-revolutionize-iot.htm

[37] G. D'Angelo, S. Ferretti, and M. Marzolla, "A blockchain-based flight data recorder for cloud accountability," *arXiv preprint arXiv:1806.04544*, 2018.

[38] B. Hub. (2018) Blockchains and distributed ledger technologies. [Online]. Available: https://blockchainhub.net/blockchains-and-distributed-ledger-technologies-in-general/

[39] P. of Stake. (2018) An introduction to consensus algorithms: Proof of stake and proof of work. [Online]. Available: https://cryptocurrencyhub.io/an-introduction-to-consensus-algorithms-proof-of-stake

[40] E. Pasquali. (2018) Industrial iot and the (data) sharing economy. [Online]. Available: http://iiot-world.com/connected-industry/industrial-iot-and-the-data-sharing-economy/

[41] K. Yeow, A. Gani, R. W. Ahmad, J. J. P. C. Rodrigues, and K. Ko, "Decentralized consensus for edge-centric internet of things: A review, taxonomy, and research issues," *IEEE Access*, vol. 6, pp. 1513–1524, 2018.

[42] M. Singh. (2016) Types of consensus mechanism used in blockchain. [Online]. Available: https://www.linkedin.com/pulse/types-consensus-mechanism-used-blockchain-munish-singh/

[43] J. Cuomo. (2016) Smart contracts: The blockchain technology that will replace lawyers. [Online]. Available: https://blockgeeks.com/guides/smart-contracts/

[44] ISO. (2018) Iso/tc 307 blockchain and distributed ledger technologies. [Online]. Available: https://www.iso.org/committee/6266604.html

[45] S. Mumtaz and A. Al-Dulaimi and V. Frascolla and S. A. Hassan and O. A. Dobre, "Guest Editorial Special Issue on 5G and BeyondMobile Technologies and Applications for IoT," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 203–206, Feb 2019.

[46] L. Urquhart and D. McAuley, "Avoiding the internet of insecure industrial things," *Computer Law & Security Review*, vol. 34, no. 3, pp. 450 – 466, 2018.