The intersection of IoT ecosystem security and blockchain technology in the context of industry 4.0

Cite as: AIP Conference Proceedings **2333**, 030011 (2021); https://doi.org/10.1063/5.0043741
Published Online: 08 March 2021

Plamenka Borovska and Martin Gugutkov

The Intersection of IoT Ecosystem Security and Blockchain Technology in the Context of Industry 4.0

Plamenka Borovska[1,a)] and Martin Gugutkov[2,b)]

[1] *Technical University of Sofia, 8 boul. Kliment Ohridsky, 1000 Sofia, Bulgaria*
Faculty of Applied Mathematics and Informatics, Informatics Department, bl. 2, office 2209
[2] *Technical University of Sofia, 8 boul. Kliment Ohridsky, 1000 Sofia, Bulgaria*
Faculty of Industrial Technology, Dept. of Material Science

[a)]pborovska@tu-sofia.bg
[b)]martin.gugutkov@gmail.com

Abstract: In this paper we have revealed and analyzed the anatomy of the intersection of Internet of Things (IoT) ecosystem security and blockchain technology in the context of Industry 4.0. The design principles and related innovative technologies to Industry 4.0 such as Industrial Internet of Things (IIoT) and edge computing have been considered. IoT and edge computing security issues have been investigated. The potential and benefits of Blockchain technology for securing IIoT are revealed such as the deployment strategies of blockchain enabled gateway and blockchain-enabled smart end devices. It has been shown that integrating blockchain with an IIoT ecosystem increases the security of the entire system.

INTRODUCTION

Industry 4.0 refers to a new phase in the Industrial Revolution that focuses heavily on interconnectivity, automation, machine learning, and real-time data [1,2]. It is a digital revolution being witnessed in the present, aiming to digitize the entire manufacturing process with minimum human or manual intervention. The vision is to build and develop an empowered virtual world that would steer the physical world. Cloud computing, big data analytics, Industrial Internet of Things (IIoT) and cyber physical systems are the key technological foundations for this industrial revolution. Industry 4.0, also sometimes referred to as IIoT [3,4] or smart manufacturing, integrates physical production and operations with smart digital technology, machine learning, and big data to create a more holistic and elaborated ecosystem for companies engaged with manufacturing and supply chain management. While every company and organization operating today is different, they all face a common challenge—the need for connectivity and access to real-time insights across processes, partners, products, and people. One of the biggest challenges in front of any modern ecosystem is its security and data protection. Blockchain is the biggest innovation when speaking about protection of the integrity and securing multiple devices. The goal of this paper is to investigate and reveal the intersection of IoT ecosystem security and Blockchain in the context of Industry 4.0.

INDUSTRY 4.0 - DESIGN PRINCIPLES AND RELATED TECHNOLOGIES

There are 4 Design Principles in Industry 4.0 (Fig. 1) such as interconnection, information transparency, technical assistance, and decentralized decisions [1].

• *Interconnection:* The main and most important feature of Industry 4.0 is to interconnect and construct various machines, cyber physical systems, sensors, devices and people capable to interact and exchange data, which is later subjected to analysis to extract knowledge. This knowledge is key factor in decision making and improving automation on later phase.

Applications of Mathematics in Engineering and Economics (AMEE'20)
AIP Conf. Proc. 2333, 030011-1–030011-7; https://doi.org/10.1063/5.0043741
Published by AIP Publishing. 978-0-7354-4077-7/$30.00

• *Information Transparency:* Transparency means the operators to have the same set of data and so being able to make better decisions.

• *Technical Assistance*: Assistance systems aim to collect and visualize the information. They serve as an interface for the human interaction. The better the visualization, the more efficient and informed decisions are made. Furthermore, critical urgent issues also will be solved immediately.

• *Decentralized Decisions*: There are smart nodes in many different locations of the cyber physical system. In parallel of gathering the data they also analyze it and even, based on the results, they can make autonomous decision and perform actions. This may happen locally and at the same at the technical level, fully automated.

Industry 4.0 brings in technologies and physical elements that change the way of manufacturing and delivering the products. The manufacturing industry is on the top of the Industry 4.0. There are three areas where it will support:

- *Smart supply chains* – Better coordination and having access to the information from each supply chain simultaneously makes it possible to have a clear view of the whole product planning and manufacturing flow. This results in new models and processes referring to the ownership and interaction across supply chains;
- *Smart manufacturing* – New technologies are deployed in the Industry, such as autonomous robots, multi-purpose manufacturing lines, augmented reality, etc. All they aim to improve productivity and speed up manufacturing. Having new features in manufacturing leads to new business models, one example being the mass customization, which is more cost efficient for the client;
- *Smart products* – The product itself can be part of the smart processing by gathering feedback data from customer during operation. This reduces a lot the time to delivery of the product to market and makes the remote support more efficient.

The key technological features that mark the emergence of Industry 4.0 are:

- *Cyber Physical Systems (PSC)* - integrating physical hardware with computation and networking capabilities and intelligent software to monitor and control physical processes is probably the main feature of Industry 4.0;
- *Internet of Things (IoT)* – bringing the devices to a new era of interconnection and constant data exchange between end devices building up the backbone of the new technologies;
- *Cloud Computing* – According to Microsoft, "cloud computing is the delivery of computing services – servers, storage, databases, networking, software, analytics, intelligence and more – over the Internet (the cloud) to offer faster innovation, flexible resources and economies of scale";
- *Big Data* – when the volume of data largely exceeds the capacity of data storage devices can handle, the only solution is Big Data technologies;
- *Digital Manufacturing/Production* - robots replacing the old manufacturing lines;
- *Industry 4.0 Logistics* – One of the key discussion areas around Industry 4.0, besides its usage in manufacturing and production, has been around logistics and how traditional warehouse operations have to be revolutionized;
- *Artificial Intelligence (AI) and Autonomous Systems (robots)*
- *Augmented reality.*

The Industrial Internet of Things (IIoT) [3] refers to the implementation of the IoT in the industrial sectors, integrating various machines, systems, and devices using sensors and IoT gateways so that they can seamlessly collect, process, and exchange data.

Although IIoT is so powerful speaking about industrial improvement, significant challenges of security, privacy and interoperability should be taken into consideration. There is no security architecture built in IIoT networks which makes them vulnerable to cyberattacks. This lack of security can result in poor manufacturing standards and processing capabilities as well as small storage capacity. Concerning industry, there is confidential data like the design of new products, assembly procedures, financial, and personal data, and so, an attack proof security model is essential. Due to lack of security measurements deployed in IIoT, privacy concerns are likely occur. Encryption is important but often is missing. Usually there are many small devices with limited capabilities that need to communicate on vast distance. And all that bring challenges to IIoT privacy insurance. Safety and reliability are with no doubt main features for any industrial system to be useful and successful. Recently, all manufactures and plants have been handling only the local physical part of these main features. Bringing the digital and especially the networking part in IIoT, systems need to be improved on the technical side. In the 3th Industrial Revolution the data has been stored on local computer machines and have been only locally secured. Nowadays, malicious actions could come from all over the world. The need of remote management and updating the devices software create serious safety concern. This is mainly because

of the issues in integration and interpolation with existing infrastructures, which could differ in software and communication protocols and also could concern the legacy devices with all corresponding restrictions. There are also issues about the physical locations of the devices. Sometimes endpoints may go out of support due to inaccessible location. There are also issues with different types of network connection technologies. For example, wireless connections may face interferences or disruptions. All of the mentioned so far may lead to loss of critical information and may cause system vulnerabilities [3,19].

When we speak about the impact of cyberattacks against an IIoT system, in comparison with any other system, we could see that in many ways it is far more critical and complicated. There are many people working in the plant who can be harmed. A security vulnerability in a smart camera may lead to stealing of sensitive client data, but in a smart car and factory this may cost lives and businesses [4,5].

EDGE COMPUTING SECURITY ISSUES

Edge computing [1,12, 13,16] is a distributed computing paradigm that brings computation and data storage closer to the location where it is needed, to improve response times and save bandwidth. In general edge computing moves the computation and processing closer to the devices that produce the data, i.e. to the gathering point. As a result, there are less latency and performance issues. Also, companies can save money by processing locally. With the growth of the number of IIoT devices connected to the systems, more and more real time data is required to be processed and so the need of distributed computing is a necessity. Edge computing is changing the way data is being gathered, processed, and stored. Sustainable modern trend is that 75% of the data will be processed outside the traditional data center or cloud.

With the emergence of 5G wireless networks, the speed of the network data transfer is increased and support for applications like video processing and analytics, self-driving cars, artificial intelligence and robotics is possible. This is the latest application of edge computing. At the beginning the main purpose of it was to reduce the cost for data transportation, and now the main purpose is to fasten processing and computing. 5G wireless technologies promise the benefits of high bandwidth and low latency for applications, enabling companies to increase data bandwidth. Instead of just offering faster speeds and companies to continue processing data in the cloud, many carriers are applying edge-computing strategies into their 5G deployments in order to offer faster real-time processing, especially for mobile devices, connected cars and self-driving cars.

The hardware used for edge-computing also should meet specific requirements and provide local storage and processing power for all connected devices. Thus, an edge gateway may process the data as needed and send only the relevant informative data to cloud for storage. So the cloud storage space and network bandwidth will not be overused.

Usually the first purpose that forces a company to deploy the edge-computing architecture is the cost saving, but according to some articles when using cloud for their applications, the bandwidth used for data transfer costs money and should be considered as disadvantage. Companies such as NVIDIA have recognized the need for more processing at the edge, which is why we're seeing new system modules that include built in artificial intelligence functionality. AI algorithms require large amounts of processing power, which is why most of them run via cloud services. The growth of AI chipsets that can handle processing at the edge will allow for better real-time responses within applications that need instant computing.

Although the edge computing has many pros as technology and is largely used nowadays, before turning to it we should consider one big disadvantage – the security issue. As you may consider there are a lot of decentralized devices performing processing, handling and filtering data and each of them should be secured. Usually securing one server is not trivial in case many devices collaborate continuously. Usage of encrypted communication, access-control and even VPN tunneling are utilized for this purpose. Another powerful solution about securing edge computing is Blockchain [12,21,20]. It is used to record all transactions in the end to end communication. All the actions performed are transparent, immutable and secure within the whole ecosystem.

Many industries aim to personalize customer experiences, generate faster insights and actions, and maintain continuous operations usually by using edge computing. Within each industry, however, there are particular user cases that lead to specific implementation. As an example, a bank that uses this technique to analyze ATM video in real-time to improve customer safety. Mining and producing companies may analyze their productivity data in order to improve the work process. Sales can personalize customer experience and provide special offers.

BLOCKCHAIN TECHNOLOGY

Usually, the term "blockchain" [6] is considered to refer to Bitcoin, which is its original purpose. This is not strange because Blockchain was invented by a person (or group of people) using the name Satoshi Nakamoto in 2008 to serve as the public transaction ledger of the cryptocurrency bitcoin. The technology behind bitcoin lets people who do not know or trust each other build a dependable ledger. This has implications far beyond the crypto currency. Bitcoin is highly secured digital currency because of the blockchain linkage of the blocks and still protecting user identity. The technology whatsoever is not limited to digital currencies and even if finances are a big part of it, it has huge impact on security and manufacturing. The idea behind it is the old well known method used in general financial ledger to record everything and the record could not be changed. The innovative idea that makes this technology so important is the decentralization, making it fast and reliable and adding trust to the data. Being decentralized, there is no single server that processes all data. This improves response and processing times and results in removing single points of failure, increasing the reliability of the system, even when some nodes are not working and the rest of the nodes overtake their functions [18].

The blockchain technology involves a chain of blocks linked together, from the genesis block to the latest block. Every node connected to the network maintains a complete copy of the entire blockchain. This redundancy results in a very resilient system. The collection of blocks is totally open and public to everyone. Each block can be thought of as a page in a ledger, which is used to maintain records of transactions and operations. The individual blocks are composed of several components. Roughly these can be differentiated into the head of the block (block header) and its body (block body) [7]. The open ledger in the blockchain is distributed by nature. The important feature of blockchain is that once the data is recorded into the ledger, then that data can not be erased. In order to do any change to a block, in theory, entire set of blocks must be altered. Moreover, each block would be approved by the network, before being added to the chain. Every block in the chain contains its own hash and the hash of the previous block for verification of the place in the chain. Using blockchain technology, participants in the network can confirm transactions without the need for a trusted third-party intermediary [9]. In fig.2 the linkage of three blocks is shown in order to visualize the creation of a blockchain. As it is written on the labels, the "previous hash" value in the first block is "0000" and this block is named Genesis block. Each of the following blocks has its own hash as well as the hash of the precursor [10].

FIGURE 1. Design principles of Industry 4.0

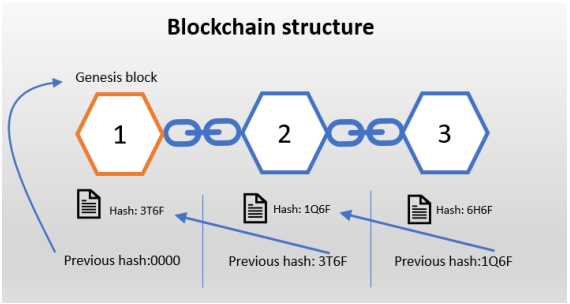

FIGURE 2. Blockchain structure

The data transferred via transactions are secured with cryptographic hash function. Hashing fundamentally standardize the data by taking various outputs and passing them through mathematical function, giving output in a fixed format. This procedure produces a unique hash value for each input. It is very difficult to guess the input value, and even in some hash algorithm techniques it is considered as impossible. Hashing is used to check for integrity of the data. It does not modify the data. Furthermore, hashing is entirely different even if there is a small alteration in the input. All of the above mentioned shows that blockchain technology as a suitable option for securing the IIoT devices.

The blockchain technology and distributed ledger technology (DLT) [24] are commonly used interchangeably, but lately there are attempts to separate them by their different underlying architectures. Blockchains can be thought of as a special subset of distributed ledgers that share the same architectural model, but have additional characteristics, that

set them apart. As a main difference can be mentioned the data structure. In blockchain technology there is a chain of cryptographically linked blocks, and/or global broadcast.

There are also some arguments about the blockchain structure. Some people think that it should be composed of transactions batched into blocks, which are cryptographically linked to each other. Other used broader definition which allows transactions that are not batched into blocks, but are directly chained together and instantly confirmed.

There are three primary types of blockchains [8]:

- *Public blockchain* – It is open source. All transactions are fully transparent for anyone. There are absolutely no access restrictions. Anyone can send transactions to it as well as become a validator. This type of blockchain is designed to be fully decentralized and everyone is open to join the network. No one can control the recording and processing of the transactions. The public blockchains are token associated, so the participants in the network receive a reward;
- *Private blockchain* – This type of blockchains are also known as permissioned blockchains. There are some notable differences from public blockchains. Participants need consent to join the networks. Transactions are private and are only available to ecosystem participants that have been given permission to join the network. Private blockchains are more centralized than public blockchains [8]. They are valuable for enterprises which aim to collaborate and share data, but don`t want their sensitive business data visible on a public blockchain;
- *Hybrid blockchain* – Depending on the architecture this blockchain lies somewhere between private and public blockchains. It makes it simple for business to operate with the transparency they are looking for, without having to sacrifice security and privacy.

Each type of blockchain has its pros and cons. Public blockchains while being transparent and resistant to tampering are slow and expensive whereas, private blockchains are somewhat centralized but can deliver much higher throughput and speeds. As a logical step, hybrid blockchains combine the benefits of both blockchains while trying to limit the disadvantages.

A *smart contract* [11] is a self-executing contract with the terms of the agreement between buyer and seller being directly written into lines of code. The code and the agreements contained therein exist across a distributed, decentralized blockchain network. The code controls the execution and transactions are trackable and irreversible. Smart contracts permit trusted transactions and agreements to be carried out among disparate anonymous parties without the need for a central authority, legal system, or external enforcement mechanism. While blockchain technology has come to be thought of primarily as the foundation for bitcoin, it has evolved far beyond underpinning the virtual currency. Smart contracts can be traced and audited but they are irreversible as making changes in the blockchain is very difficult.

THE INTERSECTION OF BLOCKCHAIN AND IIOT SECURITY

As the IIoT continues to expand, inefficient security practices, flawed protocols, and slow patch updates have made the cyber security of IIoT devices and networks an increasing concern [17]. Blockchain technology can provide benefits from tamper proof, decentralized, distributed and secure identity management. A major challenge when deploying blockchain in IIoT systems is finding the right way to implement the blockchain. Two main deployment strategies have been distinguished – blockchain enabled gateway and blockchain-enabled smart end devices. In this deployment a gateway is the demarcation point of the blockchain. The IIoT devices send all information to the gateway. In turn it has the ability to connect to a private blockchain network. All end points rely on the gateway to serve as a full node on the blockchain to which they can send their transactions and from which they can receive updates. The main advantages of this implementation are [4,5,15,22]:

- Fault-tolerance – unlike the current access control systems, where the servers are the centralized point, the presented solution stay stable even after numerous gateway failures;
- Secure and reliable log – every action reported to the gateway is logged onto the immutable blockchain. Such irreversible log of access control events may be used for forensic analysis;
- Secure device registration – all devices are registered in the blockchain enabling simple and secure authentication;
- Trusted business logic – implementing rules as smart contracts, ensure transparent and verified access control system.

Implementing this strategy, each IIoT device acts as a complete blockchain node. This implementation can be deployed without any added gateways or backend cloud services. However, they can be added to extend the network and increase security. This deployment also provides additional improvements [14]:

- *Advanced fault-tolerance* – the blockchain is replicated more often, thus it is getting more fault tolerant. Every IIoT device is functioning within the blockchain and there is no single point of failure;
- *Trusted IIoT device behavior* – the most important improvement is the ability of running a trusted code on IIoT devices. To achieve trust in such operations blockchain framework verifies the code that is executing whether it has been modified. This is available by checking an exact copy of the code stored on the blockchain.

Until 2017 there were a lot of projects implementing blockchain-enabled smart end devices. For example, the start-up Project Provenance Ltd. [22] was trying to secure the traceability of its products on a blockchain. The idea was to register the product at every step of the production process. In that way every product would get a "digital passport" that would prove its authenticity. In addition, some other important information about the product would be added. Afterwards, the buyer can scan the product via QR-code or NFC and access the information from the blockchain to check every step of the product process.

Identifying an IIoT device is process that can have a lot of vulnerabilities. The Factom Irisy company realized that the current form of authentication (based on certificates from authorities) is too expensive for IIoT devices and have started to implement a solution for this problem [22]. The future scalability of that method is also questionable due to the huge number of expected new devices. The idea involves every device to be registered in the blockchain, creating a digital identity of the device, which cannot be manipulated. It also offers the advantage that the information about the device can be dynamically updated and added in comparison to traditional certificates.

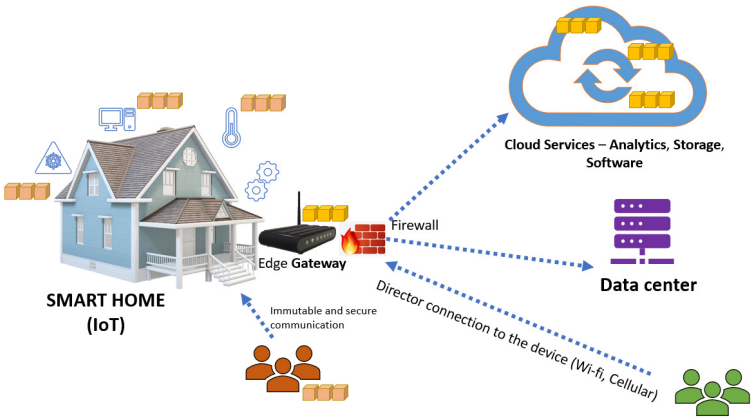

FIGURE 3. Intersection of IoT, Edge computing and blockchain

IBM has developed frameworks to enable small companies to get the benefits of IoT. They have introduced Watson IoT platform together with IBM Blockchain [23]. The platform ensures a private blockchain on which the company can share protected data securely with their partners. "IBM food trust" [23] insures with Blockchain the whole path from the producer to the market and home.

Integrating blockchain with an IIoT ecosystem increases the security of the entire system. Blockchain has excellent privacy and security characteristics that are essential in IIoT systems. Since blockchains consist of blocks of data that are interconnected and distributed, they are faster and more resilient to attacks as the data is not stored in a central hub. Besides, blockchains also use strong encryption algorithms and hashing techniques and are hence extremely secure. Transactions are also transparent and the identity of the users can be easily verified. This prevents malicious users and devices from penetrating and contaminating the blockchain network. If any device is corrupted, it can be safety removed from the network due to the distributed design of Blockchain. There is no dependency to any node in the network.

CONCLUSION

In this paper we have revealed and analyzed the anatomy of the intersection of Internet of Things (IoT) ecosystem security and blockchain technology in the context of Industry 4.0. The design principles and related innovative technologies to Industry 4.0 such as Industrial Internet of Things (IIoT) and edge computing have been considered. IoT and edge computing security issues have been investigated. The potential and benefits of Blockchain technology for securing IIoT are revealed such as the deployment strategies of blockchain enabled gateway and blockchain-

enabled smart end devices. It has been shown that integrating blockchain with an IIoT ecosystem increases the security of the entire system.

ACKNOWLEDGMENTS

This paper presents the outcomes of scientific research project “Conceptual and Simulation Modeling of Internet of Things Ecosystems (KoMEIN)”, contract № ДН02/1-2016, financed by the National Science Fund, Competition for Financial Support for Fundamental Research – 2016, Ministry of Education and Science, Bulgaria.

REFERENCES

1. Anand Nayyar, Akshi Kumar “A Roadmap to Industry 4.0 Smart Production, Sharp Business and Sustainable Development”, 2020
2. Laszlo Monostori, Vidosav D. Majstorovic, S. Jack Hu, Dragan Djurdjanovic - Proceedings of the 4th International Conference on the Industry 4.0 Model for Advanced
3. Evans PC, Marco A (2016) Industrial Internet: pushing the boundaries of minds and machines. Accessed Jul 2020
4. Skarmeta AF, Hernández-Ramos JL, Moreno MV (2014) A decentralized approach for security and privacy challenges in the Internet of Things. In: 2014 IEEE World Forum on Internet of Things (WF-IoT), Seoul, 2014, pp 67–72
5. Atamli AW, Martin A (2014) Threat-based security analysis for the internet of things. In: International workshop on Secure Internet of Things (SIoT). IEEE, pp 35–43]
6. Blockchains: The great chain of being sure about things". The Economist. 31 October 2015. Archived from the original on 3 July 2016. Retrieved 18 June 2016.
7. Marko Vidrih, What Is a Block in the Blockchain?, https://medium.com/datadriveninvestor/what-is-a-block-in-the-blockchain-c7a420270373
8. What Different Types of Blockchains are There?, https://dragonchain.com/blog/differences-between-public-private-blockchains/
9. Shermin Voshmgir, Blockchains & Distributed Ledger Technologies, https://blockchainhub.net/blockchains-and-distributed-ledger-technologies-in-general/
10. Explaining Blockchain Basics, https://dev.to/gmfcastro/my-best-shot-explaining-blockchain-4873
11. Smarts Contracts https://www.investopedia.com/terms/s/smart-contracts.asp
12. What is Edge Computing ?, https://www.ibm.com/cloud/what-is-edge-computing
13. Keith Shaw, What is edge computing and why it matters https://www.networkworld.com/article/3224893/what-is-edge-computing-and-how-it-s-changing-the-network.html
14. Mahdi H. Miraz , Maaruf Ali - Blockchain Enabled Enhanced IoT Ecosystem Security https://link.springer.com/chapter/10.1007/978-3-319-95450-9_3
15. Securing the IoT - Building trust in IoT devices and data, https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/iot-security
16. Rob van der Meulen, What Edge Computing Means for Infrastructure and Operations Leaders, Gartner Research, October 2018 by 2025
17. Internet of Things (IoT) security: 9 ways you can help protect yourself , https://us.norton.com/internetsecurity-iot-securing-the-internet-of-things.html
18. Blockchain mechanisms for IoT security https://www.sciencedirect.com/science/article/pii/S2542660518300167
19. Baraka William Nyamtiga, Jose Costa Sapalo Sicato, Shailendra Rathore, Yunsick Sung and Jong Hyuk Park - Blockchain-Based Secure Storage Management with Edge Computing for IoT, Published: 25 July 2019
20. Claus Pahl, Nabil El Ioini and Sven Helmer - A Decision Framework for Blockchain Platforms for IoT and Edge Computing
21. Joseph Denne - IoT will unlock the potential of cloud, the edge and blockchain
22. Vincent Dieterich, Marko Ivanovic, Thomas Meier, Sebastian Zäpfel, Application of Blockchain Technology in the Manufacturing Industry, FSBC Working Paper 2017
23. IBM Food Trust. A new era for the world’s food supply., https://www.ibm.com/blockchain/solutions/food-trust
24. Distributed ledger, https://en.wikipedia.org/wiki/Distributed_ledger