Challenges and Research Directions for Blockchains in the Internet of Things

Frank Golatowski, Björn Butzin,
Tim Brockmann, Thorsten Schulz, Martin Kasparick
Institute of Applied Microelectronics and Computer Engineering,
University of Rostock, Germany
{firstname.lastname}@uni-rostock.de

Yuhong Li, Rahim Rahmani
Institutionen för data- och systemvetenskap,
Stockholms Universitet
Kista, Sweden
yuhongli@dsv.su.se, rahim@dsv.su.se

Aviv Haber
Mavennet Systems Inc.
Toronto, Canada
aviv@mavennet.com

Mustafa Sakalsız
T2 Software
Ankara, Turkey
mustafa.sakalsiz@t2.com.tr

Özer Aydemir
IOTIQ
Leipzig, Germany
ozer@iotiq.de

***Abstract*—In this paper, we analyze the state of the art in distributed ledger technologies and blockchains and investigate potential applications in the Internet of Things (IoT) domain. Afterwards, we discuss interoperability of blockchains, and their use in smart contracts, and artificial intelligence.**

***Index Terms*—blockchain, Internet of Things, distributed ledger technology, industry 4.0, artificial intelligence**

I. Introduction

Internet of Things (IoT) connects vast number of various kinds of devices, collecting and processing data, making decisions by using the data. IoT provides a means of converting physical world into digital system and thus plays a more and more important role for people's daily life, industries, business and the whole society. In this context, security, privacy and trust are prerequisites and necessities for IoT systems and applications. For example, without guarantee of data integrity, decision makings based on data obtained from IoT devices, such as autonomous driving, will cause great trouble. Without trust on the devices providing data, services like supply chain will not be used by companies. Similarly, without privacy protection, services related with healthcare will not be welcomed by people.

However, due to the distributed, ubiquitous and large scale feature of IoT, IoT systems expose multiple surfaces of security, privacy and trust threats. The use of cloud server may introduce vulnerability of single point failure/attack, various vertical application domains face context specific risks. Many off-shelf IoT products are implemented with poor security/privacy mechanisms on account of the cost consideration. In order to provide secure IoT services, lots of work have been done to identify the security challenges and provide solutions, such as DDoS [1], data integrity [2] [3], trust [4] [3] and system availability [2]. Nevertheless, the existing work can only provide solutions for one application domain, none of the work solve the security problems at the system level and can benefit for all the IoT systems and applications fundamentally.

Blockchain is a distributed ledger technology (DLT) and has matured significantly. It provides distributed trust, anonymity and data integrity, ensuring availability. Blockchain can benefit IoT in two aspects fundamentally: One is, they are both distributed systems in nature. The other is, blockchain has intrinsic security mechanisms by design. Therefore, blockchain can be a promising technology for meeting the requirements of IoT. Work in [5] [6] [7] have also surveyed and investigated the integration of blockchain and IoT.

However, due to the characteristics of IoT, introducing blockchain to IoT raise many challenges. First, most IoT devices face resource and network connectivity constraints, but mechanisms and algorithms of blockchain are resource consuming and need high network bandwidth. Secondly, the number of devices in IoT is huge and is increasing. Current blockchain mechanisms scale poorly with the increase of nodes. Thirdly, due to the isolated, vertical deployment of IoT applications as well as the heterogeneity of devices, data, and services, using the same type of blockchain platforms or distributed ledgers is impossible. Interoperability among different DLT is necessary, but have not been well solved by DLT technologies. Also, domain-specific (e.g., industrial IoT) requirements and challenges should be analyzed. Fourthly, different technologies have been used in IoT, such as cloud computing and artificial intelligence. If, and how mechanisms related to these technologies need to be changed or can be used, is still unclear. Finally, different IoT applications have different quality of service (QoS) requirements, how to provide the QoS is also a challenge. For example, mining in blockchain is time consuming, how to support IoT applications with low latency requirements needs to be considered.

II. Distributed Ledger Technology

Distributed ledger technology (DLT) is a type of database that has the following notable features:

- Distributed participation
- Decentralization

- Distributed consensus
- Public-private key cryptography

In such distributed ledgers, every network participant possesses an exact replica of the network's transaction history. The information is updated to all nodes (network participants) in near-real time. All parties see and share the same information. Decentralization is important because the information stored on a blockchain is not controlled or harvested by any single party. Therefore, there is no single point of failure. If a node fails or is compromised, the network carries-on undisturbed by the remaining network participants. The information in a DLT is shared and can be simply verified by reconciling one version of the database to another hosted on a separate node. Consensus in DLT networks can take many forms including: Proof of Work, Proof of Stake, Proof of Authority, practical Byzantine Fault Tolerance, Single Authority, etc. Regardless of the type, each form of consensus ensures that transactional accuracy within the network is agreeable among network participants. This contrasts with traditional databases, whereby inputted information is assumed accurate until reviewed.

Public-private key cryptography allows participants to transact pseudonymously. Public keys are a user's address on a blockchain network (where a blockchain network is the set of nodes operating on the same blockchain). Transactions are sent to and from public keys. Each public key has an associated private key, which effectively acts as the password, allowing users to access their digital assets. This approach provides security for transactions on DLT networks.

These foundational features are cornerstones solving the problems of security, privacy, integrity, and trust in various systems. It allows DLT to be used in many different areas, such as cloud computing, Internet of Things (IoT), data storage, network management (e.g., software-defined networking, access control), and digital content distribution.

Blockchains are one particular form of DLT, and consists of blocks (e.g. blocks of transactions) that are securely linked with each other using cryptographic mechanisms. Bitcoin—the most famous example of a blockchain, is a decentralized, peer-validated, time-stamped bookkeeping system that stores all valid transactions. The accounting system is publicly auditable by all network peers, which may be either individuals or autonomous agents working without human intervention. Transactions are sent to the Bitcoin network and their validity is checked independently by the peers. Valid transactions are collected in cryptographically sealed blocks. A specific type of peer, called miners or (more generally) voters, are in competition to validate the new block and interlock it with the last block. This forms a chronological sequence - a chain of blocks. The competition is based on the relative processing power of each miner in relation to the total processing power of all the active miners and is thereby a form of *Proof of Work* consensus. Thus, [8] consider it as the first example of a common digital currency that provides a solution to the problem of lack of confidence in monetary transactions. The authors further conclude that the blockchain opens countless new opportunities for businesses that directly share values between subscribers. Despite being originally designed for payments, blockchains have evolved into a much more versatile technology. In the context of smart grid, [9] has proposed a sovereign blockchain-based solution that uses smart contracts to create a tamper-proof system for consumer data protection. By using DLT, users can monitor how the electricity is used and the risk of conflicts between what electricity companies and consumers report is eliminated. [10] introduced an attribute-based signature scheme for medical records with N authorities. By using blockchain technology, the system is fault-tolerant to N-1 corrupted authorities. This ensures patient privacy and immutable medical records.

Unfortunately, problems such as small throughput, high latency, wasted resources, ease of use, security, and interoperability between multiple chains have been identified in [11] as the main technical challenges for blockchain adoption. One specific vulnerability that some blockchains have is to eclipse attacks. The eclipse attack exploits the fact that many nodes are only connected to a small subset of the total nodes in the network. With this is mind, an attacker can monopolize all incoming and outgoing connections to a particular node, separating it from the rest of the network [12].

III. Overview of DLT

In his article, J. Seeger [13] describes basic concepts of DLT and gives an overview of well-known DLTs. Ethereum is a blockchain with its own crypto-currency (Ether) that uses a sandbox style Virtual Machine (VM) called the Ethereum Virtual Machine (EVM). This VM is able to execute programs (*DApps* - distributed apps) written in the Ethereum-specific programming language *Solidity*. This enables the implementation of smart contracts on the ledger, and Ethereum is the first to support this (see sec. V). Smart contracts create countless opportunities and use cases for DLTs. By providing a virtual machine which restricts the language and creates a secure environment, the smart contracts can be executed on the machines of peers. Ethereum is the most popular platform for companies using Initial Coin Offerings and related tokens.

IOTA [14] is a distributed ledger that allows micro transactions without fees as well as secure data transfer for the IoT. It represents a component of a novel machine-to-machine communication that is suitable for industrial applications. This is based on multidimensional Directed-Acyclic-Graph technology developed by the non-profit IOTA Foundation.

The AION network [15] is a multi-tier blockchain network designed to support a future where many blockchains exist to solve unique industry problems and to power the services of the modern world. AION is posed to become the common protocol used for these blockchains, enabling more efficient and decentralized systems to be built. The AION protocol enables the development of a federated blockchain network, making it possible to seamlessly integrate dissimilar blockchain systems in a multi-tier hub-and-spoke model, similar to the internet.

The Hyperledger-Project of the Linux Foundation aims at the collaborative development of blockchain implementations. In this project, five frameworks and tools were developed

that are mainly based on the Ethereum Virtual Machine. The frameworks are tailored for specific applications, like bonds (Sawtooth), financing (Iroha), and digital identities (Indy).

Big IT companies like Microsoft, Oracle, Amazon, and SAP have their own cloud-based blockchain solutions. Microsoft offers Hyperledger, Ethereum, and Corda for Azure, Amazon offers Blockchain as a Service, Oracle offers Distributed Ledger in his cloud, and SAP offers the Leonardo blockchain. [13] DLT technologies differ according to their ledger access and data validation.

TABLE I
CATEGORIZATION OF DISTRIBUTED LEDGERS

	Permissioned	**Permissionless**
Private	Only members can validate and read. Ex.: Hyperledger, R3 Corda	Only pre-defined members can read/write. Ex.: Ethereum or Bitcoin test network
Public	Only members can validate but data is open to everyone. Ex.: Ripple	Every user can join and validate transactions. Ex.: Ethereum, Bitcoin

Distributed ledgers that are established between institutions mostly prefer private, permissioned ledgers (see table I). Performance and scalability problems of DLTs can be address more easily, since the network is more trusted than public ledgers.

IV. BLOCKCHAIN, IOT, AND INDUSTRY 4.0

The Internet of Things (IoT) is a technological phenomenon whereby devices, machines, objects, or even people are connected to the internet. These connected devices can automatically communicate with each other, without the need for human interaction. In the context of enterprise, IoT has significant implications when it comes to transparently tracking and tracing large and complex interactions between automated processes. Blockchain could be the underlay that records all transactional data in an immutable, auditable distributed ledger. Data is accessible by any stake-holding party whose connected device is part of the value chain. A recent number of publications describe the challenges, potentials, and use case of blockchains in combination with IoT [16] [17] [18] [19].

Christidis et al. [16] show that blockchains are generally well-suited for IoT purposes due to their as distributed, trustless, and peer-to-peer nature. As an example, the authors introduce a blockchain network that is used for all devices of a manufacturer, which stores the hash of the latest device firmware on the network. Via a distributed peer-to-peer file system, the devices are allowed to request the latest firmware by its hash. The authors also give a summary about possible services between devices. For example, it is possible to use micro-payments (Bitcoin or Ethereum) to enable the devices to rent disk space or monetize API calls. Another possibility mentioned are smart electronic locks (“slocks”), which use smart contracts to unlock such things as shared cars, houses, and hotel rooms. Yet another opportunity are solar panels which record their output on the blockchain, and sell it to other parties via smart contracts. There are some challenges to these applications, including small throughput, high latency, as well as legal questions regarding the connection between real world assets and what is recorded on the blockchain. Another major concern is privacy, because although the records are immutable, they are visible to anyone.

Conoscenti et al. [20] introduce a list of 18 use cases of blockchains documented in different literature divided in the categories „Data storage management“, „Trade of goods and data“, “Identity management“, “Rating system“ and “Other“. By means of a systematic literature review, the authors try to spot the main factors that affect the levels of integrity, anonymity, and adaptability of blockchains. It was concluded that large blockchains systems like Bitcoin are the most secure. At the same time, Bitcoin scalability issues make it poorly suited for IoT. Additionally, the blockchain only guarantees pseudonymity, not anonymity. The authors plan to test further blockchains to find a solution suitable for IoT, in which the compromise between scalability and security is acceptable.

Dorri et al. [17] use the blockchain/bitcoin technology to secure a smart home environment. The architecture foresees a shared overlay for common access to multiple smart homes. Each smart home has a typical gateway component that acts as a miner and potentially also as a cluster head within an overlay compound. The smart home miner device handles its own private blockchain, governing all internal and external communications between local storage, cloud storage, and the smart devices. External users, such as the home owner and commercial service providers are granted monitoring and transaction access through the miner gateway device. Within the workshop paper, the authors focus on the introduction of the smart home components, the transactions in between, and how they are secured by the blockchain technology. Also discussed is how information security aspects are addressed as well as ensuring the overhead of the cryptography functions is manageable on medium powered devices. A comparison with established systems does not emerge from the paper.

Fremantle and Scott [21] conclude: “Blockchains are cryptographically secure ledgers that typically require a significant amount of memory, disk space, and processor power to work. These requirements go beyond typical IoT devices and even beyond more powerful systems in IoT networks such as hubs. One option to address this is to use remote attestation, but as yet there is little or no work in this space.”[21]

Huh et al. [18] use Ethereum to configure devices and manage public keys via a blockchain. They show a proof of concept using smart contracts for a small amount of IoT devices (air conditioners, temperature sensors, lighting devices, metering devices). However, the concrete advantage of the proposed methodology does not become clear.

Esposito et al. [22] deals with “the potential to use the blockchain technology to protect healthcare data hosted within the cloud.”[22] They propose a system where complete patient data is stored in the blockchain, therefore being distributed over all peers in the patient network. Some interesting problems are addressed in the paper: How can the storage within

a blockchain fit to the requirement of "right-to-erasure"? Blockchain was not designed to store huge amounts of data, like images. To solve it, the authors propose to store the data outside the blockchain in a database and to store only hashes of the data in the blockchain.

Fujitsu presented in the Hannover Fair 2018 a demonstration of its envisioned smart factory of the future. According to [23] they have implemented IOTA DLT into their product portfolio and its IoT-Suite IntelliEdge [24]. Further [23] outlines four other partnerships that uses IOTA in context with IoT, like the world's first IOTA charging station and an automated order controlled production process.

The tutorial from Chainskills [25] shows the possibility to set up a private Ethereum blockchain on a IoT environment that consists of a computer and one or more Raspberry Pi 3 devices. It is mentioned that the concept behind private Ethereum blockchain differs from other concepts like the private blockchain "championed by Hyperledger, Eris/Monax, and or the recently announced Enterprise Ethereum Alliance."[25]

V. Blockchain and Smart Contracts

The idea for smart contracts was presented in 1996 by Nick Szabo. A smart contract is a computer program formalizing a set of rules that parties signed the contract have agreed to interact with each other. When the rules described in the smart contracts are fulfilled, the program will executed automatically in the blockchain system. A smart contract formalizes (i.e., in machine-understandable programs) the relationships between the participants in the blockchain, which might be people, institutions, companies and the assets they own. Therefore, benefits include low contracting, enforcement, and compliance costs. From another point of view, since various algorithms and functions can be activated and executed upon the reception of the fulfilment of contract rules, smart contract provides also a simple form of decentralized automation. Afanasev et al. [26] described three advantages of smart contracts:

- accessibility of a common runtime environment for all smart contract objects and subjects,
- accurate mathematical description, and
- strict execution logic.

The first blockchain implementation - Bitcoin has only limited smart contract support (non-Turing-complete scripting). Ethereum, implemented in 2013 as an electronic payment system, is the first blockchain implementation supporting smart contracts. This implementation has the following features:

- self-tracking fulfillment of predefined requirements,
- decision making based on a predefined algorithm,
- signable by human and machine.

Due to these features, Ethereum has served as basis for the majority of today's smart contract implementations [26]. Currently, there are two approaches for a blockchain to support a smart contract. One is to use specialized sandbox-styled programming languages, examples are Solidity (similar to C and JavaScript), Serpent (similar to Python), LLL (Low-level Lisp-like Language), Mutan (Go-based), and Viper (strongly-typed Python-derived decidable language) [26].

The other is to use containers and integrate it with the internal API of the blockchain platform. Instead of developing a specialized programming language with a custom virtual machine, regular programming languages can be used with containerized platforms. In this approach, Docker containers create a safe environment for smart contracts, which can call the internal API of the blockchain platform, so they can make operations on the blockchain. Every supported language has a proxy server, which translates functions into internal blockchain platform API calls. This approach cannot be said to be safer than the sandbox or virtual machine approach, but it is very practical, especially for private ledgers. The most popular example of this approach is the Hyperledger Fabric, which is the most supported open-source private ledger platform.

In addition, Afanasev et al. [26] summarized three types of solutions for smart contracts: a private blockchain-based solution, a specialized blockchain-based solution, and a private Ethereum blockchain in conjunction with the "Proof of Stake" (PoS) consensus mechanism. Currently, smart contracts are being considered for a wide variety of uses, particularly for regulatory compliance, product traceability, service management, defeating counterfeit products, and fraud detection.

Magazzeni et al. [27] described the use of smart contracts in finance and government applications based on distributed ledger technology, and discussed the challenges for verification and validation. Since distributed ledgers ensure that all parties are on the same shared knowledge, the smart contracts eliminate the need for an additional trusted third party (law firm, bank, ...) and act as a witness for a multi-step transaction. In [27], the specific smart contract programs perform the transaction in real-time on dematerialized goods with its own medium (i.e., an integrated cryptocurrency). While the contract moves from natural language to formalized code, different questions for validation and verification become a challenge.

Gao et al. use the smart contract to identify malicious usage of electrical power [9]. Consumer data being manipulated maliciously on the smart grid network will trigger the smart contract to send an encrypted message to the smart meter. The warning is then shown to the consumer on the screen of the smart meter. Y. Zhang and J. Wen [19] described the transaction of smart property and paid data on the IoT by means of blockchain technology and smart contracts. The use of smart contracts is further elaborated in [28].

Smart contracts provide an increasing network of fault-tolerance and autonomy for the Cyber-Physical Systems (CPS) domain. However, smart contracts also present some drawbacks, when used with blockchains, such as:

- privacy/confidentiality issues due to the public contracts;
- insufficient size of production networks compared to global P2P networks;
- smart devices lack of computing power for proof of work;
- lack of storage capacity for complete transaction log;
- increasing minimum cost of equipment;
- high transaction-costs in blockchains.

VI. Interoperability between Blockchains

As the market stands today, there is an abundance of blockchain platforms. Each serves its own unique use-case – from digital currencies to provenance tracking in supply chains. Each of these solutions operates in their own siloed ecosystem. Different platforms cannot communicate.

Protocols like AION, Cosmos, Polkadot, ICON, or Wanchain are developing solutions at the cutting edge of blockchain interoperability. Interoperability is the catalyst enabling broad commercial adoption via increased scalability and transaction throughput. Some notable benefits are:

- enable ecosystem applications such as identity, payment, and storage to interact across multiple blockchains;
- enable enterprises to link public and private networks to optimize their cost, privacy, and security;
- high performance computing by spanning out workflows to fit-for-purpose blockchains;
- decentralized exchange of native coins and tokens across multiple blockchain platforms;
- assets outlive the network, in which they were created.

However, the following challenges complicate seamless communication between heterogeneous networks:

- Bridges introduce longer finality time.
- Different blockchains have different architectural designs (Bitcoin: 6 blocks, approx. 1 h confirmation time. AION: 90 blocks, approx. 15 min confirmation time).
- Transaction signing is complex: Different networks use different cryptographic curves.
- Bridges need to be more secure, but allow more transaction throughput than the networks which they connect.
- Pricing disparity between tokens trading on their native network and the same token on an external network.

VII. Blockchain and Artificial Intelligence

Today, academic and industrial researchers are treating both blockchain and artificial intelligence (AI) as the most promising emerging technologies. As they start to mature, efforts are made trying to combine the two.

Open access trusted information: One of the concepts that is gaining the most traction in the AI space, is the creation of an open repository of trusted data that AIs can use as training data. Opposed to rely on closed environments, blockchain can provide open access with the right amount of accountability, when it comes to provenance and trust. Examples of these applications are AI Crypto, Synapse Ai, or Dopamine.

Traceability applications: AI and blockchain are also being used in tandem to create end-products that require immutability and traceability provided by blockchain, but also require AI to identify patterns and anomalies, detect fraud, detect delays, or detect other external events. Namahe and Numerai are examples of such platforms.

Proof-of-Intelligence (PoI): One of the largest criticisms of some blockchain implementations has traditionally been the amount of resources that are being consumed. While this is not true for all types of blockchains, it is for the ones using Proof-of-Work (PoW) as part of their consensus algorithm. PoW focuses on providing nodes with a mathematical puzzle that they need to solve in order to create a new block. The puzzle in itself has no value beyond avoiding Denial of Service attacks and defining who is next in charge of creating a new block. The goal of PoI is to use the computing power that goes into solving the puzzle for a purpose, to solve real life problems in the area of artificial intelligence. PoI is still a concept without implementations known to the authors.

In [29] the authors consider how blockchain can improve AI as well as how AI can improve blockchain. They envision that blockchain and AI can "complement each other to revolutionize the next digital generation." [29]

TABLE II
Blockchain and AI

Blockchain for AI	**AI for Blockchain**
Secure data sharing marketplace for AI	Secure and scalable blockchains
Decentralized computing for AI	Privacy-preserving personalization
Explainable AI	Automated referee and governance
Coordinating untrusted devices	

Table II summarizes the sense in which both technologies can have value to each other. To underline these features some examples are given in the paper.

Sometimes the behavior of AI algorithms is difficult to understand. If future systems use decisions that come from AI, a clear understanding of the decision-making process is necessary. Blockchain can track the decision chain based on the used training data. This is important, such as in the case of incidents, to identify whether the machine or humans are responsible for a faulty behavior. Blockchain can give privacy of data back to the users. Instead of letting service providers of the shared economy analyze the user data for personalization, completely new approaches are possible. If a user analyzes their own data with AI, "relevant content will be pulled, rather than pushed, and displayed to users" [29].

Blockchain is secure and almost impossible to hack. However, the applications on top of blockchain platform are not secure. AI detects presences of attacks and mechanisms can be initiated to prevent or eliminate the damage. Further, AI can ease the configuration manifold parameters that are necessary to setup blockchains.

VIII. Conclusion

In the paper at hand, we analyzed the challenges and research directions for blockchain in IoT. We derive the following conclusions:

Section II: DLT as a technology can be applied in seemingly all environments where any kind of transactions are performed, such as supply chain, smart grid, smart government and smart communities. DLT has the potential to change the way how transactions are conducted in everyday life and benefit people in different aspects, such as security, privacy, and lower cost in management. Despite its potential, DLT

suffers from some technical limitations and challenges. When applied in different environments, the throughput, latency, and security issues of DLT must be considered carefully in the context of each environment.

Section III: The interoperability among hundreds of blockchain platforms puts forward another challenge for using DLT. In addition, with the increase of participants and ledgers in the network, scalability becomes another issue to be considered when applying DLT to solve various problems in transactions.

Section IV: Without DLT, the data from all IoT interactions would be recorded and siloed by the party hosting each connected device. In the world of highly integrated supply chains, where stakeholders are numerous, sharing of complete data is paramount. To increase the practicability of using DLTs for IoT, further research is needed to overcome its technical limitations. To quantify advantages it is necessary to present and evaluate further practical implementations and assess their performance.

Section V: Smart contracts depend on the computing system on which they execute. When smart contracts involve multiple systems, providing a secure and trustworthy environment remains an open challenge.

Section VI: Without interoperability, a robust Web 3.0 is impossible to achieve as value and information cannot seamlessly federate on-chain. Off-chain conversion re-introduces centrality, which contradicts decentralization. Being able to build a universal bridge remains a hard, unresolved challenge.

Section VII: Blockchain can provide traceability and accessibility to AI. Vice versa, AI has the prospect to serve as a beneficial proof of work instead of meaningless calculations.

Summarized, DLT and blockchains come as promising technologies for the IoT domain especially if the aforementioned issues are addressed.

References

[1] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "Ddos in the iot: Mirai and other botnets," *Computer*, vol. 50, no. 7, pp. 80–84, 2017.

[2] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645 – 1660, 2013.

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

[4] F. Hawlitschek, B. Notheisen, and T. Teubner, "The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy," *Electronic Commerce Research and Applications*, vol. 29, pp. 50 – 63, 2018.

[5] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, "Blockchain and iot integration: A systematic survey," *Sensors*, vol. 18, no. 8, 2018.

[6] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with iot. challenges and opportunities," *Future Generation Computer Systems*, vol. 88, pp. 173 – 190, 2018.

[7] E. F. Jesus, V. R. Chicarino, C. V. de Albuquerque, and A. A. d. A. Rocha, "A survey of how to use blockchain to secure internet of things and the stalker attack," *Security and Communication Networks*, vol. 2018, 2018.

[8] T. Aste, P. Tasca, and T. D. Matteo, "Blockchain technologies: The foreseeable impact on society and industry," *Computer*, vol. 50, no. 9, pp. 18–28, 2017.

[9] J. Gao, K. O. Asamoah, E. B. Sifah, A. Smahi, Q. Xia, H. Xia, X. Zhang, and G. Dong, "Gridmonitoring: Secured sovereign blockchain based monitoring on smart grid," *IEEE Access*, vol. 6, pp. 9917–9925, 2018.

[10] R. Guo, H. Shi, Q. Zhao, and D. Zheng, "Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems," *IEEE Access*, vol. 6, pp. 11 676–11 686, 2018.

[11] M. Swan, *Blockchain: Blueprint for a new economy*. O'Reilly, 2015.

[12] Y. Marcus, E. Heilman, and S. Goldberg, "Low-resource eclipse attacks on ethereum's peer-to-peer network." *IACR Cryptology ePrint Archive*, vol. 2018, p. 236, 2018.

[13] J. Seeger, "Sicher verkettet," *iX*, vol. 7, pp. 44–48, 2018.

[14] S. Popov, "The Tangle," *Whitepaper*, p. 23, 2018, Version 1.4.3.

[15] M. Spoke, "Aion: Enabling the decentralized internet," AION, White Paper, Jul 2017. [Online]. Available: https://aion.network/media/en-aion-network-technical-introduction.pdf

[16] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[17] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for iot security and privacy: The case study of a smart home," in *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, March 2017, pp. 618–623.

[18] S. Huh, S. Cho, and S. Kim, "Managing iot devices using blockchain platform," in *2017 19th International Conference on Advanced Communication Technology (ICACT)*, Feb 2017, pp. 464–467.

[19] Y. Zhang and J. Wen, "The iot electric business model: Using blockchain technology for the internet of things," *Peer-to-Peer Networking and Applications*, vol. 10, no. 4, pp. 983–994, Jul 2017.

[20] M. Conoscenti, A. Vetrò, and J. C. D. Martin, "Blockchain for the internet of things: A systematic literature review," in *2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)*, Nov 2016, pp. 1–6.

[21] P. Fremantle and P. Scott, "A survey of secure middleware for the internet of things," *PeerJ Computer Science*, vol. 3, p. e114, May 2017.

[22] C. Esposito, A. D. Santis, G. Tortora, H. Chang, and K. R. Choo, "Blockchain: A panacea for healthcare cloud-based data security and privacy?" *IEEE Cloud Computing*, vol. 5, no. 1, pp. 31–37, Jan 2018.

[23] C. Mueller, "How iota is enabling industry 4.0," May 2018. [Online]. Available: medium.com/@iotasuppoter/how-iota-is-enabling-industry-4-0-b867564f57a3

[24] FUJITSU, "Fujitsu iot solution intelliedge™," Jan 2019. [Online]. Available: www.fujitsu.com/emeia/products/computing/pc/edge-computing/

[25] Eloudsa, "Create a private ethereum blockchain with iot devices," Feb 2017. [Online]. Available: chainskills.com/2017/02/24/create-a-private-ethereum-blockchain-with-iot-devices-16/

[26] M. Y. Afanasev, Y. V. Fedosov, A. A. Krylova, and S. A. Shorokhov, "An application of blockchain and smart contracts for machine-to-machine communications in cyber-physical production systems," in *2018 IEEE Industrial Cyber-Physical Systems (ICPS)*, May 2018, pp. 13–19.

[27] D. Magazzeni, P. McBurney, and W. Nash, "Validation and verification of smart contracts: A research agenda," *Computer*, vol. 50, no. 9, pp. 50–57, 2017.

[28] R. Beck, "Beyond bitcoin: The rise of blockchain world," *Computer*, vol. 51, no. 2, pp. 54–58, February 2018.

[29] T. N. Dinh and M. T. Thai, "Ai and blockchain: A disruptive integration," *Computer*, vol. 51, no. 9, pp. 48–53, September 2018.