Securing Internet of Things (IoT) Devices Through Distributed Ledger Technologies (DLTs) and World Wide Web Consortium (W3C) Standards

Sthembile Mthethwa[1][0000-0001-7961-5240]

[1] Council for Scientific and Industrial Research (CSIR), Information and Cyber Security Centre (ICSC), Pretoria, South Africa
smthethwa@csir.co.za

Abstract. The tremendous growth of the Internet of Things (IoT) connected devices calls for a way for manufacturers to standardise the newly created devices for security purposes. As these devices are getting smaller and smaller so does the computational power in them. The resource constraints introduced by the devices eliminate some of the cryptographic features that can be performed by these devices. Thus, developers are looking for a secure method for automating processes and exchanging information in real-time. With that, new technologies like distributed ledger technologies (DLTs) introduce a promising solution for enabling large-scale IoT applications in a decentralized and autonomous manner. Therefore, this work aims to investigate the integration of DLTs and IoT to create a safe and secure environment for IoT devices whilst being aware of the constraints brought by these devices. In this paper, a proposed solution is presented that adopts emerging standards introduced by the World Wide Web Consortium (W3C), to ensure an internationally recognisable system and platform.

Keywords: Internet of Things (IoT), Distributed Ledger Technologies (DLTs), World Wide Web Consortium (W3C), IoT devices.

1 Introduction

The Internet of Things (IoT) is a network of devices consisting of sensors that can detect data from the physical environment and can communicate and interact with its surroundings [1, 2]. IoT turned conventional objects into smarter ones. There has been a tremendous increase in the adoption of IoT in various sectors. It is projected that there will be more than 75 billion IoT-connected devices in use by 2025 [3]. The continual use of IoT devices span to various sectors i.e., health (for medical equipment), governments or municipalities (smart devices to monitor energy use, and water and air quality), agricultural sector (monitor crop conditions—light levels, humidity, soil moisture, crop health, and more—and then automate irrigation and other processes accordingly) and engineering or operational technology (OT – which is part of IoT devices) (identify, monitor, and control physical devices, processes, and events).

Among these applications are many safety-critical tasks, where a malfunction or malicious tampering with devices can impact human health, may have a large financial impact, or tampers with privacy. Their increasing spread and importance also increase the interest attackers are developing for IoT-devices. [4, 5].

IoT devices collects data which is usually stored in a centralised cloud storage for analysis and processing by various applications. Consequently, the data becomes vulnerable to various forms of attacks and compromises its security [6].

With the advancements in IoT devices, whereby, the size of devices is significantly reduced, consumes less energy and reduced hardware cost which enables them to be integrated into everyday objects. Another issue is introduced due to the heterogeneity of IoT devices, whereby the architecture varies per device. These devices are manufactured by various companies with different specifications. It is worth noting that, with all the advancements in technology, IoT devices are still susceptible to challenges, such as:

- Constrained resources - IoT devices have constrained resources with respect to central processing unit (CPU) processing power, read-only memory (ROM), Random Access Memory (RAM), and battery life. However, these devices still have the capability of providing their intended functionalities such as collecting and transmitting data, across the Internet for storage and analysis [7].
- Privacy - these are issues relating to the collection, storage, use, and sharing of personal information. The vast amount of data generated by IoT devices raises privacy concerns, as personal information could be collected and used without consent.
- IoT device security – there are currently no proper measures to protect IoT devices from cyber-attacks, hacking, data theft, and unauthorized access. This can be due to various reason i.e., outdated software, weak passwords, unpatched vulnerabilities, lack of encryption, etc. Therefore, to ensure the security and privacy of sensitive information stored on these devices, it is essential to implement strong security measures.
- Interoperability – is the ability of different systems, devices, or components to work together seamlessly and exchange data effectively. Therefore, ensuring that different IoT devices can work together seamlessly, and exchange data effectively is essential.
- Identity management - which ensure that the right users have the right privileges in terms of accessing devices, data and applications, and monitoring their usage. Identity management in IoT is currently performed by exchanging identifying information between devices for first time connection. This process is susceptible to eavesdropping which can lead to man-in-the-middle attack [8]. Hence, there is a need for a unique identity management solution [9].
- Lack of standardization - the absence of agreed-upon specifications or protocols in a particular field or industry which can result in different systems,

products, or processes being incompatible with each other (thus, leading to inefficiency, and decreased interoperability). For example, in the context of IoT, this can cause difficulties in communication and data exchange between various IoT devices and systems. Establishing standards and protocols can help overcome this and ensure uniformity and compatibility. There is a lack of standardization in IoT devices, making it difficult to secure them consistently.

With the rapid increase of connected devices and services, it is vital for IoT device manufactures, and application developers to invest in a secure methods of automating processes and exchanging information in real-time [10]. Hence, to ensure secure IoT devices, new technologies like the distributed ledger technologies (DLTs) can be utilised which appears to be a promising solution for enabling large-scale IoT applications in a decentralized and autonomous manner. The first ever implementation of DLTs was experienced through the inception of Bitcoin, a peer-to-peer version of electronic cash that allows online payments to be sent directly from one party to another without going through a financial institution [11]. As an open, trust-less, transparent, immutable and distributed ledger, a DLT can record transactions among IoT devices in a verifiable and permanent way [10].

Over the years, the use of DLTs has shifted from the mere use of transacting cryptocurrencies but the main characteristics of DLTs have evolved and now includes various sectors like supply chain, manufacturing, etc., Below are some of the prominent features provided by DLTs that might be of interest in the field of information security and IoT:

- Decentralisation – no central entity controlling the network which can introduce a single point of failure. Instead, the network is made up of various nodes that work together to verify and validate transactions.
- Anonymity – the identity of participants is either anonymous or pseudonymous, thus improving privacy.
- Security – cryptography is used to sign data in order to prove that a transaction was approved by the owner thus, ensures that untrusted parties can communicate securely.
- Immutability – DLTs are permanent and unalterable network. Once a transaction is recorded, it cannot be modified or deleted. Thus, providing a high degree of security and trust. To guarantee data confidentiality and integrity, this quality is essential.
- Distributed - all network participants have a copy of the ledger for complete transparency. Information is not processed through a central server but is transmitted and verified by nodes in parts of the network. allowing for a peer-based network that can self-check.
- Traceability – enables any authorized entity to authenticate a transaction's history, if there is a need to prove the origin of a transaction.
- Transparency – all participants in the network can access information in the network according to the permission they have been granted. For example, in

a public network anyone can access and view all the transactions on the network.

- Consensus – a decision-making algorithm for the group of nodes active on the network to reach an agreement and for the smooth functioning of the system. In DLTs nodes do not trust each other but they can trust the algorithm that runs at the core of the network to make decisions.
- Auditability – since data in the network is reliable, accurate, verifiable, and cannot be altered; it allows the network to create an audit trail.

Considering these features, the use of DLTs can allow IoT devices to communicate among themselves and make decisions automatically. However, for a successful integration of DLTs with IoT, the following must be considered:

- Limitations of IoT devices - most DLT implementations rely on consensus algorithms (the process by which nodes in a network agree on a common state of the ledger) i.e., mining. This requires huge resource capacity which becomes computationally intensive for IoT devices. Majority of IoT devices are resource constrained (computational capacity, power, and storage), hence, the use of mining might not work as it utilizes a lot of resources (it is computationally intensive).

- Latency –ledgers maintain a history of all transactions which for example in a blockchain implementation, transactions are organised in batches known as blocks. However, not all DLTs employ blocks. Therefore, computational latency is important, which refers to the average time until blocks (or transactions) are added to the DLT so that the likelihood of tampering of previously added blocks or transactions is below a certain threshold. The approach of using blocks is time consuming which is not suitable for over-the-top IoT applications as they require low latency.

- Scalability – currently, DLTs do not scale very well as the number of nodes increases in the network, which will pose a challenge as IoT networks are increasing at a high speed and the number increases tremendously.

- Centralisation - current approaches in IoT implementations are largely centralised, which raises several security concerns i.e., single point of failure, trust, and privacy.

- Overhead traffic - which may be undesirable for certain bandwidth limited IoT devices.

In this paper a DLT-based architecture for IoT that delivers lightweight, standardised, decentralised, secure, and scalable platform is proposed. It aims to retain the benefits of DLTs while overcoming the aforementioned challenges of IoT devices. This architecture aims to be application–agnostic and well suited to diverse IoT use cases. The proposed solution aims to be in line with emerging standards aimed at standardising the process of identification.

The remainder of the paper is structured as follows: In Section 2, an overview of IoT and DLTs is provided as well as highlighting IoT challenges. In Section 3, current DLTs-based applications and services for IoT are provided. In Section 4, we present the proposed architecture and finally, conclusion and future work is provided in Section 5.

2 Overview of IoT and DLTs

2.1 Overview of IoT

The interconnectedness of IoT enables real-time collection and monitoring of various types of data about i.e., properties, individuals etc [12]. Sensors and actuators as well as heterogeneity and decentralisation are the key features of IoT [13].

The interconnectedness combine with lightweight nature of IoT devices, makes them susceptible to attacks. As IoT devices communicate with each other, a crucial aspect of IoT security is the ability to trust in data received from another device that is part of the network during the communication process [4] which is typical for wireless sensor networks (WSN). According to [12], WSNs "are ad hoc networks that are considered the major building blocks for IoT devices. They are used for gathering data from their surrounding and delivering them to users and for accessing connected IoT devices remotely". The communication between the Internet and the sensor nodes should satisfy secrecy, trustworthiness, verification, and non-revocation [12].

The main challenge is that IoT devices are constrained by energy, memory, and processing power. Another challenge is that they experience great data losses due to node impersonation. For example, an attacker gaining unauthorized access to an application and taking control of it. Therefore, it is infeasible for traditional security mechanisms, e.g., encryption of memory and data transmission, requiring strong computational power, to be applied on IoT devices as it contradicts its light-weight nature [4].

The number of devices in the IoT network are expected to increase tremendously in the future. Therefore, improving IoT device security is crucial.

2.2 Overview of DLTs

DLTs provides a universal data structure which combines a group of previously untrusted nodes in a distributed environment thus eliminating the need of a centralized third party to oversee everything that happens in the network whilst proving immutability [14]. The first ever successful implementation of DLT was Blockchain, which was introduced by Bitcoin the first decentralised digital currency [11]. It is noteworthy that, all blockchains are distributed ledgers, but not all distributed ledgers are blockchains [14]. Subsequently, other DLTs spanning from cryptocurrencies have been introduced over the years.

- Blockchain is a shared, decentralized, and immutable ledger of timestamped series of transactions [15]. Blockchain is based on a peer-to-peer topology as well as cryptography. To store a transaction in the ledger, most participating nodes in the blockchain network should agree and record their consent. Each new block includes a link to the prior block in the chain through cryptography. Each block encompasses a timestamp and hash function to the previous block. The participating nodes of the blockchain network place their trust in the integrity and security features of the consensus mechanism.
- Directed Acyclic Graph (DAG) is a directed graph data structure that uses a topological ordering [14]. In DAG, transactions are linked to one but possibly more transactions. However, links are specifically directed – pointing from prior transactions to newer ones in accordance with topological order. DAGs are acyclic; thus, it is a non-circular structure (whereby loops are not permitted) [15]. DAG does not add blocks sequentially (resulting to higher throughput), does not require proof of work from miners, zero transaction fee, provides higher level of scalability and is partition tolerant, which allows a portion of the network to split off the main network for a period and continue to run without the Internet connectivity [14]. There are several applications that use DAG such as IOTA (built specifically for IoT), Byteball, Hashgraph, etc.
- Hybrid DLTs are a combination of DAGs and blockchain technologies and one example is the Tempo ledger. It is an essential part of Radix, a DLT platform that works efficiently with IoT [14]. Tempo uses partitions of the ledger to accomplish the appropriate ordering of actions that occur in the whole network. The Tempo ledger comprises of three main elements; a networked cluster of nodes, a global ledger database that is distributed across the nodes, and an algorithm for generating a cryptographically secure record of temporally ordered events.

3 DLT-Based Applications and Services for IoT

The topic of integrating DLTs with IoT has gained a lot of traction over the years. This is fuelled by the improvements introduced by DLTs [16]. However, most research around this topic have mainly been focused on conducting surveys and theoretical work [17,18]. This has left a research gap for practical implementations of DLTs in the information security space; thus, presenting an opportunity for this study to make a plausible attempt to bridge the gap.

The first implementation occurred when IBM in partnership with Samsung designed a platform called ADEPT (Autonomous Decentralized Peer-To-Peer Telemetry) which utilises the design of bitcoin to construct a distributed network of devices [19]. In 2017, Slock.it was introduced which aims to provide the transparency and auditability features to the IoT objects by integrating blockchain with IoT [20]. It resolves the problem of connecting a device to the blockchain and improves the essential features for non-blockchain designers working on IoT systems by providing an interoperable and decentralised platform [15].

Chain of Things which provides an integrated blockchain and IoT hardware solution to solve IoT challenges regarding identity, security, and interoperability was introduced [21]. A survey of types of distributed consensus or trust protocols from an IoT perspective, has been conducted by [5] which provides trade-offs and recommendations. This would be vital for using DLTs for purposes of securing IoT devices.

To the best of our knowledge, SmartDID is the only distributed-identity management system for IoT that implements DIDs standards to preserve privacy [22]. Hence, the gap for ensuring IoT devices security using DLTs and standards.

4 Proposed Architecture

This section provides details about the proposed architecture for the integration of these two technologies and how we envision it working. The planned prototype would i.e., visualise and demonstrates the enrolment of devices, how IoT devices share data or communicate, assigning identities to the devices etc., whilst considering storage throughput in the order to cater for multiple of transactions per second between IoT devices.

The major contribution of this research is to propose a solution aimed at ensuring security is maintained even for resource constrained IoT devices. To achieve this, a DLT has been employed to benefit from some of its prominent features discussed in Section 1 and eminently solve some of the challenges outlined for IoT devices i.e., security, centralisation of data, privacy etc.

To solve the issue of standardisation in IoT devices, this paper aims to adopt standards introduced by the World Wide Web Consortium (W3C) which includes the use of Verifiable Credentials (VCs) and Distributed Identifiers (DIDs). The W3C VC data model ecosystem follows 4 basic roles that are followed as shown in Fig. 1 [23].

Firstly, an issuer is responsible for generating & issuing verifiable credentials about a subject. Secondly, a verifier computes the cryptographic proof to verify the legitimacy and authenticity of credentials about a particular subject. Thirdly, a holder receives and manage verifiable credentials from issuers, and create verifiable presentations which are presented to verifiers as proofs. A verifiable data registry maintains identifiers and schemas. The conceptual architecture is portrayed in Fig. 1.

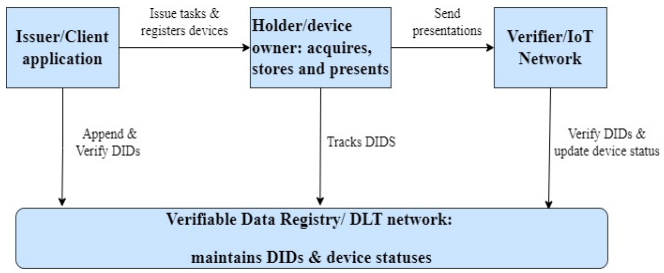

Fig. 1. Conceptual architecture.

This solution aims to ensure that device enrolment is secure, thus, prior to any IoT device being permitted to interact with other devices, it must be enrolled first following an enrolment process. During this process, each device is provided with a unique credential. To register, the device owner submits the registration request to the system. This request is handled by the client app which issues a secret for the enrolment process through the client app. For this process, public and private keys are used along with the unique DID. A DID Document is then generated and is binded with the public key. The timestamp and DID is then sent to the DLT for timestamping purposes. The DID is then sent to the device owner to be used for authentication purpose shown in Fig. 2. After the enrolment process, the device owner is allowed to access and consume services provided by the network. To use the network a device must first be authenticated. To achieve this, a DID authentication challenge in a form of JSON Web Token (JWT) that is authenticated by the user's JSON Web signature. The user signs the challenge using their associated private key and sends it back so that access can be verified. If verified, access is then granted, and this process is depicted in Fig. 2.

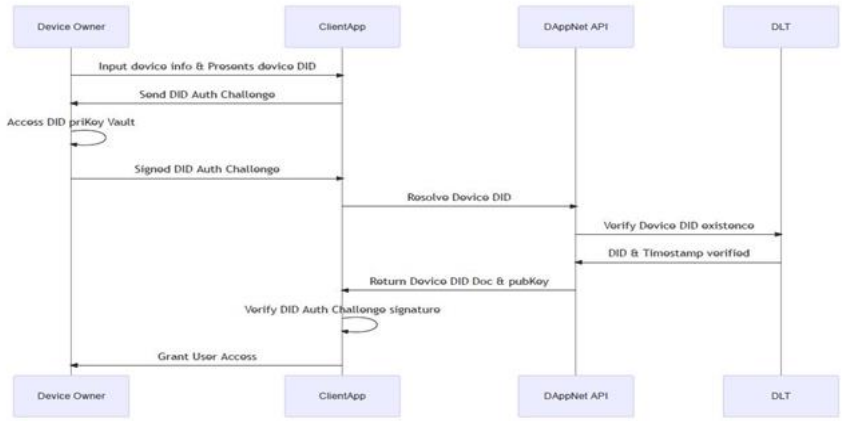

Fig. 2. Device authentication flow diagram.

With this solution, the device owner has control over all the devices and to whom they are to communicate with. Thus, improving security and ensuring privacy. With this approach, we can achieve some of the self-sovereign identity requirements namely, control, access, existence, transparency, etc. by Christopher Allen [24]. It is worth noting that, this is a proposed solution for ensuring that IoT devices are secure using DLTs and W3C standards. Therefore, performance metrics can only be shared at a later stage once the solution has been implemented and tested accordingly.

5 Conclusion and Future Work

In this paper, we have carried out an in-depth systematic review about the integration of DLT with of IoT to ensure secure IoT devices. It can be observed that the IoT scale is growing tremendously, and more researchers are investing efforts towards finding ways to integrate these two newly introduced technologies that are takin the world by storm (DLT and IoT). However, this growth can affect the performance of the DLT technology when integrated without performing an evaluation. For example, the POW consensus protocol involves many issues in the blockchain-IoT environment including throughput, delay, and high computing resource consumption, which affect the efficiency of IoT management [25, 26, 27]. Hence, it is essential to consider the proper consensus protocol and the resource constraints introduced by IoT devices when implementing the environment. In order to successfully implement a secure blockchain-IoT environment and communication protocols, energy and storage requirements or resource-constrained devices should be considered and managed. Hence, designing lightweight communication protocols or implementing energy manage-

ments techniques are challenging issues in a blockchain-based IoT environment. Thus, the importance of this research.

For this research, a background around IoT and DLTs have been shared as well as what has been done in terms of integrating these two platforms thus far. This paper presented a proposed solution for the integration of DLTs and IoT whilst being cognisant of the challenges presented by IoT devices. The solution employed 4 techniques: W3C standards, VC, DIDs and DLTs. The standards are still new and emerging but will be vital in order to have a standardise protocol to follow for the integration process are still a few changes and evolution being implemented for these standards, but they have promising implementations that require.

These standards are still being changed on a yearly basis, whereby new improvements are introduced to improve the performance and their adoption as well. For standardisation processes, it is vital to find and adopt standards that could ensure that the integration process is smooth and can be internationally recognised. The proposed solution goes further into portraying the flow of information during different stages of using the system i.e. When a user wants to enrol or register a device on the network, device-to-device communication, etc. As this is still a new field of research, more efforts are still required to ensure that it is properly integrated and can be standardised. Hence, further research efforts are still required in the near future to make the integration of DLTs a permanent and mature approach in the context of IoT device environment as well as ensuring security.

With the existing research, it becomes evident that more researchers are interested in this topic. Further research and experimentations are still required for the assessment of all possible DLTs to be used for this solution from the 3 types of DLTs discussed in this paper. From there, the proposed solution can then be tested. From the assessment, it can be important to develop or implement IoT specific DLT testbench using the cheapest and smallest possible embedded devices to demonstrate the effectiveness and practicality.

References

1. Bouras, M. A., Lu, Q., Dhelim, S., & Ning, H. (2021). A Lightweight Blockchain-Based IoT Identity Management Approach. https://doi.org/10.3390/fi13020024.
2. Pavithran, D., Shaalan, K., Al-Karaki, J. N., & Gawanmeh, A. (2020). Towards building a blockchain framework for IoT. Cluster Computing, 23(3), 2089–2103. https://doi.org/10.1007/s10586-020-03059-5.
3. Abed, S., Jaffal, R., Mohd, B. J., & Al-Shayeji, M. (2021). An analysis and evaluation of lightweight hash functions for blockchain-based IoT devices. Cluster Computing, 1. https://doi.org/10.1007/s10586-021-03324-1.
4. Tschirner, S., Zeuch, K., Kaven, S., Bornholdt, L., & Skwarek, V. (2023). Security in Distributed Systems by Verifiable Location-Based Identities. arXiv preprint arXiv:2302.14713.

5. Pretorius, M., & Mthethwa, S. N. (2019). A survey of distributed trust mechanisms suitable for IoT devices.
6. Javaid, M., & Khan, I. H. (2021). Internet of Things (IoT) enabled healthcare helps to take the challenges of COVID-19 Pandemic. Journal of Oral Biology and Craniofacial Research, 11(2), 209–214. https://doi.org/10.1016/j.jobcr.2021.01.015.
7. King, J., & Awad, A. I. (2016). A distributed security mechanism for resource-constrained IoT devices. Informatica, 40(1).
8. Mahmoud, R., Yousuf, T., Aloul, F., & Zualkernan, I. (2015, December). Internet of things (IoT) security: Current status, challenges and prospective measures. In 2015 10th international conference for internet technology and secured transactions (ICITST) (pp. 336-341). IEEE.
9. Sadique, K. M., Rahmani, R., & Johannesson, P. (2020). Identity management in internet of things: A software-defined networking approach. In Proceedings of the 2nd International Conference on Communication, Devices and Computing: ICCDC 2019 (pp. 495-504). Springer Singapore.
10. Fan, X., & Chai, Q. (2018). Roll-DPos: A randomized delegated proof of stake scheme for scalable blockchain-based Internet of Things systems. ACM International Conference Proceeding Series, 482–484. https://doi.org/10.1145/3286978.3287023.
11. Nakamoto, S. (2008). Bitcoin : A Peer-to-Peer Electronic Cash System. www.bitcoin.org/bitcoin.pdf.
12. Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. Journal of Network and Computer Applications, 88, 10-28.
13. Saxena, S., Bhushan, B., & Ahad, M. A. (2021). Blockchain based solutions to secure IoT: Background, integration trends and a way forward. Journal of Network and Computer Applications, 181(December 2020), 103050. https://doi.org/10.1016/j.jnca.2021.103050.
14. Atlam, H. F., & Wills, G. B. (2019). Intersections between IoT and distributed ledger. In Advances in Computers (1st ed., Vol. 115, Issue January). Elsevier Inc. https://doi.org/10.1016/bs.adcom.2018.12.001.
15. Farahani, B., Firouzi, F., & Luecking, M. (2021). The convergence of IoT and distributed ledger technologies (DLT): Opportunities, challenges, and solutions. Journal of Network and Computer Applications, 177(September 2020), 102936. https://doi.org/10.1016/j.jnca.2020.102936.
16. Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. Future Generation Computer Systems, 88(June), 173–190. https://doi.org/10.1016/j.future.2018.05.046.
17. Issa, W., Moustafa, N., Turnbull, B., Sohrabi, N., & Tari, Z. (2023). Blockchain-based federated learning for securing internet of things: A comprehensive survey. ACM Computing Surveys, 55(9), 1-43.
18. Ferrag, M. A., Derdour, M., Mukherjee, M., Derhab, A., Maglaras, L., & Janicke, H. (2018). Blockchain technologies for the internet of things: Research issues and challenges. IEEE Internet of Things Journal, 6(2), 2188-2204.
19. Panikkar, S., Nair, S., Brody, P., & Pureswaran, V. (2015). ADEPT : An IoT Practitioner Perspective. ibm.biz/devicedemocracy.
20. Majer, A. (2017). Slock.IT: Enabling IoT and the Universal Sharing Network. Blockchain Research Institute (BRI), December, 1–18.
21. Abderahman Rejeb, J. G. K. and H. T. (2019). Leveraging the Internet of Things and Blockchain in SC.pdf. 1–22.
22. Yin, J., Xiao, Y., Pei, Q., Ju, Y., Liu, L., Xiao, M., & Wu, C. (2022). SmartDID: a novel privacy-preserving identity based on blockchain for IoT. IEEE Internet of Things Journal.

23. Sporny, M., Longley, D., & Chadwick, D. (2019). Verifiable Credentials Data Model 1.0: Expressing verifiable information on the Web. W3C Recommendation 19 November 2019. https://www.w3.org/TR/vc-data-model/.
24. Allen, C. (2016). The Path to Self-Sovereign Identity. Life With Alacrity. http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereereign-identity.html.
25. Tewari, A., & Gupta, B. B. (2020). Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework. Future Generation Computer Systems, 108, 909–920. https://doi.org/10.1016/j.future.2018.04.027.
26. Lockl, J., Schlatt, V., Schweizer, A., Urbach, N., & Harth, N. (2020). Toward Trust in Internet of Things Ecosystems: Design Principles for Blockchain-Based IoT Applications. IEEE Transactions on Engineering Management, 67(4), 1256–1270. https://doi.org/10.1109/TEM.2020.2978014.
27. Mistry, I., Tanwar, S., Tyagi, S., & Kumar, N. (2020). Blockchain for 5G-enabled IoT for industrial automation: A systematic review, solutions, and challenges. Mechanical Systems and Signal Processing, 135, 106382. https://doi.org/10.1016/j.ymssp.2019.106382.