Blockchain Technology for Secure Internet-of-Things

Alex Norta

Dymaxion OU, Tallinn, Estonia

alex.norta.phd@ieee.org

Abstract. We explore the intersection for securing the internet-of-things (IoT) with blockchain technology. IoT-systems are diffusing into society on many levels, generating large data sets that must be secured. The paper briefly points out the bottlenecks and security threats for IoT and consequently proposes ways of using blockchain technology as a possible remedy. Several application scenarios show where blockchains are already used in combination with IoT for tracking product provenance, managing office space, or energy management. A future evolving scenario of a machine-to-everything (M2X) Economy with smart autonomous devices such as self-driving vehicles, promises to render the need even more pressing for securing large created data sets in a distributed way. Finally, we also propose future research directions for creating blockchain solutions for IoT-system applications.

1. Introduction

The emergence of the Internet-of-Things (IoT) systems creates many novel business opportunities and it is expected that by 2025, ca 55 billion IoT devices will be in operation. The consequence of these IoT systems is the explosion in big-data generation that is challenging to secure [2]. Simultaneously, blockchain technology has found many usecases beyond the first application of Bitcoin [22]. The vision arises that novel blockchain technology is a means of securing [29]future distributed IoT systems. Thus, in this paper, the aim is to first introduce in Section 2 the three aspects of IoT [36], security and blockchain technology [17]. Next, in Section 2, we explore the relationship between these elements of investigation and how blockchains are useful for resolving security problems in IoT. Section 3 then points out what open research issues exist for blockchains in the context of securing IoT. Section 4 shows examples for existing application cases and finally, Section 5 concludes this paper.

2. Properties of IoT, Blockchain and Security

The networking capability of IoT enables data flow to and from objects and devices equipped with sensors and actuators using the Internet. As such IoT-systems build a bridge between the digital- and physical worlds without human intervention. The main IoT functionalities are sensor-laden devices, the autonomous exchange of data across the Internet and the creation of real-time linkages between devices for data exchange. The potential of IoT for improving lives stretches over many interesting application cases, e.g., to monitor the health of patients [33], or energy-use optimization [9], etc. Consequently, novel latency-related problems arise [30] due to billions of transactions occurring between the devices of low computing power and low data storage, while standards are still in development [11] for highly efficient-,effective- and secure network connectivity. With respect to the latter, anecdotal examples for privacy- and security problems are Amazon's Alexa[1] that is suspected to spy on users; or hacked heart pacemakers [27], security cameras [1], baby monitors [20]. Consequently, many consumers do not trust connected devices[2].

Currently, IoT-systems are constructed based on a centralized architecture [21] where connections occur only to identified-and verified devices through cloud services that have high data-storage capabilities. This yields high maintenance costs since extra infrastructure is required to manage the number of interconnected IoT-device. Furthermore, when a large number of IoT-devices are interconnected at a time, the amount of communication increases substantially [32] and if the related scalability-engineering issues reach beyond a limit, disruptions of cloud services occur that lead to security issues [26]. We infer in this paper that a decentralized network promises to be a solution for the listed IoT issues.

Note also that a small breach in the security of an IoT-system can allow hackers to access large sets of information. The core security properties of consideration [28] are confidentiality, i.e., data is secured to authorized parties; integrity, i.e., data is secured; availability, i.e., data is accessible when and where needed; non-repudiation, i.e., an IoT-system provides a trusted audit trail; authenticity, i.e., components can prove their identity; privacy, i.e., an IoT-system does not automatically see customer data.

Modern blockchain technology has arisen with the usecase of bitcoins [23] where transaction data is stored in chained blocks that are mined into existence in a distributed way. Such events are hashed and stored on a block after validation, e.g., with proof-of-work, or proof-of-stake [4], while by now many more consensus algorithms exist [4],also specifically for the IoT domain [19,34]. Blockchain systems are decentralized and distributed without requiring a third-party presence. Each new block stores a reference of the previous transaction by including a SHA-256 hash of the previous transaction, thereby creating a chain of blocks that are computationally difficult to create and tamper resistant. Another notable characteristic is that blockchains allow for immutably traceable of the stored transactions that are replicated between many nodes. Smart contracts are extensions in that programming languages are part of the protocol layer to define with code the terms of agreements [12] between buyers and sellers. Briefly, public smart-contract blockchains such as Ethereum [8] allow any node to access and view a ledger without a central authority and the parties have little-, or no knowledge of each other. Permissioned blockchains such as Hyperledger [10],

[1]https://www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio

[2]https://www.smartcitiesworld.net/news/news/two-thirds-of-consumers-think-connected-devices-are-creepy-4151

limit ledger access via a governance structure of authority [15] to known-, or trusted third parties. This governance structure of authority also enforces rules and responds to incidents that include cyber threats.

3. Research Direction for Blockchain to Secure IoT

Well known IoT-shortcomings pertain to device autonomy that is limited by the integration need into heterogeneous systems, rendering point-to-point communication as complex to coordinate and easy to attack to compromise data while the virtual identity of IoT-devices creates trust- and authentication issues. Further security threats for IoT [14],besides unauthorized physical device access, are software attacks, e.g., viruses and worms, DDoS-, man-in-the-middle attacks to obtain passwords. Solutions for such security issues focus on identity management and encryption to the point where the entire IoT-device lifecycle is protected.

Blockchain technology promises to mitigate these issues above providing a framework for automated security and attack prevention. Furthermore, blockchains are fully decentralized systems and by adoption into IoT systems, may overcome the centralization architecture of IoT as a single point of failure and security shortcoming. Thus, blockchain technology complements IoT towards creating an internet-of-trusted-things (IoTT) [37] where blockchain traces, authenticates and stores IoT-data. Every IoT-node is registered on a blockchain with an ID to uniquely identify a device in a universal namespace. Consequently, for a device to connect to another device, using the blockchain ID as URL maybe performed as follows. First, the IoT-device may use the local blockchain wallet to raise an ID request that is sent to the target device, which uses blockchain services to validate the signature using the public key of the sender without the need of any centralized arbitrator, or -service. Blockchain technology promises a standardization of IoT-system aspects for tracking millions of connected devices along respective IoT-device lifecycles [24,31] yielding a history of connected equipment and enhanced coordination between devices. Blockchains also establish decentralize IoT-systems with trust [35] where nodes reach a consensus [5] to approve transactions. Furthermore, blockchains may enable coordinating the transactional layer of an IoT-ecosystem to thereby solve the problems of IoT-security, -scalability,-privacy and confidence.

Problems exist for IoT-system use due to the amount of large data sets [13] processed by IoT-systems, resulting in latency due to blockchains. Thus, the ledger replication introduces latency and acquiring a block consumes extra time.Since this is not acceptable in a near-time and real-time service situation, a blockchain is not best suited for recording raw data at the source. The ledger-size may lead to centralization and pose a scalability bottleneck for blockchains.That means novel sharding mechanisms [6] are necessary for IoT devices that cannot maintain a blockchain of many gigabytes. Briefly, sharding is a technique for partitioning blockchains into smaller parts that low-capacity IoT-devices can manage. Each shard is distinctive and independent from other shards holding their own data sets. The purpose of splitting shards to IoT-devices is to enhance the scalability of blockchain use to process more transactions per second. Sharding can help reduce the latency or slowness of a network since it splits a blockchain network into separate shards. However, there are some security concerns surrounding sharding in which shards can be attacked. Additionally, the IoT processing power- and time hurdle, and storage issues are problematic for performing encryption algorithms for all the objects involved. The IoT-devices may have very different computing capabilities and run heterogeneous systems. The very low storage capacity of most IoT-devices is prohibitive to storing many blocks.

Blockchain technology is applicable for IoT-devices in that each create-, read-, update- and delete transaction is stored on-chain. With introducing blockchain-based identity for IoT-devices, it is possible to control access management and to monitor the information collected by respective sensors with greater transparency and potential convenience. Furthermore, storing data on chains of transactions prevents data modification during the verification by authentication systems and disallowing data duplication by erroneous data without the need of a third data-transfer party betweenIoT-devices. Thus, blockchains potentially enable a resilient IoT-ecosystem promising the adoption of a standardized, point-to-point communication model to reduce installation- and maintenance costs, and reduce storage in IoT-devices. Blockchains are replicated and restored preventing errors in nodes due to a collapse, or attacks. Blockchains can record transactions and digital interactions between IoT-devices securely since each block registers the operations with a timestamp attached, verifying the correct- and unmanipulated occurrence sequence while being safe, auditable, transparent, potentially efficient, and interruption-resistant.

4. Application Cases

The current use of blockchains in industry secure IoT-systems to typically determine product provenance as it is easy to forge products sold to unsuspecting consumers. For example, microchip-embedded labels and stored on blockchains track the integrity of a good, e.g., baby formula, wine. Consequently, blockchains track the product lifecycle starting from the moment of production, tracking the entire supply chain to the point of sale with the final consumer purchase. By storing such data on a blockchain, product details can not be forged and the integrity of the end-product is ensured. Thus, blockchains can prevent data leaks that occur in centralized IoT-systems. Concrete examples are the provenance tracking with blockchains for Australian sports clothing[3], the efficient and effective management of services related to office space[4], or using blockchain technology for trading energy [3].

In a more visionary setting, the application of blockchain to securing IoT systems is relevant for the emerging machine-to-everything (M2X) Economy [18] that results from the interactions, transactions, collaborations and business enactments among humans, autonomous- and cooperative smart devices/machines, software agents and physical systems. The corresponding ecosystem is formed by automated, globally-available, heterogeneous socio-technicale governance systems with loosely coupled, P2P-resembling network structures and is characterized by its dynamic-,continuously changing-, interoperable-, open- and distributed nature. Thereby, the M2X Economy employs concepts such as cyber-physical systems [7], IoT and wireless sensor networks. Thus, it is predictable that the evolving M2X applications and the corresponding ecosystem will diffuse the economy and society at large in many ways. Besides machine-to-machine (M2M) interactions, this framework also comprises machines interacting with humans (M2H), or infrastructure components (M2I) such as smart traffic lights, or smart toll gates.

The following example of an M2X Economy intends to give a better understanding and stems from the sub-set of the vehicle-to-everything (V2X) domain. More concretely, we assume in the future, vehicles may own themselves, or private corporations [18] and people can rent such vehicles for rides. For this example, we assume that Alice requests a self-driving car to transport her from Point A to B and several route options exist. A fast route option is expensive while being the most comfortable for which toll gates charge automatically a fee for the self-

[3]https://www.zdnet.com/article/ip-australia-and-nrl-trial-blockchain-to-combat-counterfeits/

[4]https://medium.com/coinmonks/blockchain-in-facilities-management-refocusing-on-the-office-experience-7e9efbe9ab29

driving vehicle. On the other hand, a more time consuming route is cheaper and includes traffic lights with traffic congestion. Depending on the price preference, Alice may select her preferred option on a mobile phone as she orders the vehicle and indicate her urgency for reaching the final destination. We furthermore assume the self-driving vehicles are able to communicate with other cars and the smart traffic lights that belong to the road infrastructure. A vehicle may negotiate an agreed smart contract for a green-light phase for a faster commute to Alice's final destination where the smart traffic lights receive a small crypto-currency fee in return. Note that although a self-owning and self-driving vehicle is an ongoing research topic, self-driving vehicles have become a normal part of Tallinn, Estonia´s public transport [25]. Also autonomous delivery robots are part of Tallinn to deliver orders from a business to customers [16]. In summary, it becomes evident that theM2X Economy generates large amounts of data sets in a distributed way that must be secured by novel generations of smart-contract blockchain systems.

5. Conclusion

The focus of this paper is to discuss that IoT-systems with centralized architecture are a single point of failure. The conceptual security properties must be assured in IoT-system, i.e., confidentiality, integrity, availability; additionally privacy, authentication, and non-repudiation. Blockchain technology promises to be a framework securing IoT-systems for large-data management in a distributed way. Still, the current performance and scalability of IoT are incompatible with blockchain functions. This situation becomes even more pressing once the IoT devices are complemented with smart autonomous devices such as self-driving vehicles. New types of blockchains with novel consensus- and validation algorithms are needed for billions of securely connected IoT-devices. Since IoT-systems and certainly smart autonomous devices are a massive source of unstructured data that must be combined and understood to extract intelligence with advanced analytics for actionable decision-making. With blockchain securing the immutably traceable provenance of such massive data sets, a high quality of such analytics efforts can be addressed.

References

[1] Peshraw Ahmed Abdalla and Cihan Varol. 2020. Testing IoT Security: The Case Study of an IP Camera. In2020 8th International Symposium onDigital Forensics and Security (ISDFS). IEEE, 1–5.

[2] Fadele Ayotunde Alaba, Mazliza Othman, Ibrahim Abaker Targio Hashem, and Faiz Alotaibi. 2017. Internet of Things security: A survey. Journal ofNetwork and Computer Applications88 (2017), 10–28.

[3] M. Andoni, Va. Robu, D. Flynn, S. Abram, D. Geach, D. Jenkins, P. McCallum, and A. Peacock. 2019. Blockchain technology in the energy sector: Asystematic review of challenges and opportunities. Renewable and Sustainable Energy Reviews100 (2019), 143–174.

[4] S.M.H. Bamakan, A. Motavali, and Alireza B. Bondarti. 2020. A survey of blockchain consensus algorithms performance evaluation criteria. ExpertSystems with Applications(2020), 113385.

[5] Sujit Biswas, Kashif Sharif, Fan Li, Sabita Maharjan, Saraju P Mohanty, and Yu Wang. 2019. PoBT: A lightweight consensus algorithm for scalableIoT business blockchain. IEEE Internet of Things Journal7, 3 (2019), 2343–2355.

[6] Xingjuan Cai, Shaojin Geng, Jingbo Zhang, Di Wu, Zhihua Cui, Wen Sheng Zhang, and Jinjun Chen. 2021. A Sharding Scheme based Many-objective Optimization Algorithm for Enhancing Security in Blockchain-enabled Industrial Internet of Things. IEEE Transactions on Industrial Informatics(2021).

[7] Hong Chen. 2017. Applications of cyber-physical system: a literature review. Journal of Industrial Integration and Management2, 03 (2017), 1750012.

[8] Chris Dannen. 2017.Introducing Ethereum and solidity. Vol. 318. Springer.

[9] Guillermo del Campo, Silvia Calatrava, Guillermo Cañada, Jorge Olloqui, Rocio Martinez, and Asuncion Santamaria. 2018. IoT Solution for EnergyOptimization in Industry 4.0: Issues of a Real-life Implementation. In2018 Global Internet of Things Summit (GIoTS). IEEE, 1–6.

[10] Vikram Dhillon, David Metcalf, and Max Hooper. 2017. The hyperledger project. InBlockchain enabled applications. Springer, 139–149.

[11] Keith Dickerson, Raúl García-Castro, Peter Kostelnik, and Marek Paralič. 2021. Standards for the IoT. InIoT Platforms, Use Cases, Privacy, andBusiness Models. Springer, 125–147.

[12] V.K. Dwivedi and A. Norta. 2018. A Legally Relevant Socio-Technical Language Development for Smart Contracts. In2018 IEEE 3rd InternationalWorkshops on Foundations and Applications of Self* Systems (FAS* W). IEEE, 11–13.

[13] Yosra Hajjaji, Wadii Boulila, Imed Riadh Farah, Imed Romdhani, and Amir Hussain. 2021. Big data and IoT-based applications in smart environments: A systematic review. Computer Science Review39 (2021), 100318.

[14] Vikas Hassija, Vinay Chamola, Vikas Saxena, Divyansh Jain, Pranav Goyal, and Biplab Sikdar. 2019. A survey on IoT security: application areas, security threats, and solution architectures. IEEE Access7 (2019), 82721–82743.

[15] C.V. Helliar, L Crawford, L. Rocca, C. Teodori, and M. Veneziani. 2020. Permissionless and permissioned blockchain diffusion. International Journal of Information Management54 (2020), 102136.

[16] Kirsten Korosec. 2020. Starship Technologies is sending its autonomous robots to more cities as demand for contactless delivery rises - TechCrunch.URL: https://techcrunch.com/2020/04/09/starship-technologies-is-sending-its-autonomous-robots-to-more-cities-as-demand-for-contactless-delivery-rises/. (Accessed June 12, 2021).

[17] Nallapaneni Manoj Kumar and Pradeep Kumar Mallick. 2018. Blockchain technology for security issues and challenges in IoT. Procedia ComputerScience132 (2018), 1815–1823.

[18] Benjamin Leiding. 2020. The M2X Economy—Concepts for Business Interactions.Transactions and Collaborations Among Autonomous Smart Devices.Ph. D. Thesis, University of Göttingen, Göttingen, Germany(2020).

[19] Chunlin Li, Jing Zhang, Xianmin Yang, and Luo Youlong. 2021. Lightweight blockchain consensus mechanism and storage optimization for resource-constrained IoT devices. Information Processing & Management58, 4 (2021), 102602.

[20] Manuel Maya. 2020. Internet of Things: A Deeper Dive in Your Privacy and Information. (2020).

[21] H. Muccini and M.T. Moghaddam. 2018. IoI architectural styles. InEuropean Conference on Software Architecture. Springer, 68–85.

[22] Satoshi Nakamoto. 2008. Bitcoin: A peer-to-peer electronic cash system. Decentralized Business Review(2008), 21260.

[23] S. Nakamoto. 2019.Bitcoin: A peer-to-peer electronic cash system. Technical Report. Manubot.

[24] Antonio L Maia Neto, Artur LF Souza, Italo Cunha, Michele Nogueira, Ivan Oliveira Nunes, Leonardo Cotta, Nicolas Gentille, Antonio AF Loureiro, Diego F Aranha, Harsh Kupwade Patil, et al.2016. AoT: Authentication and access control for the entire IoT device life-cycle. InProceedings of the14th ACM Conference on Embedded Network Sensor Systems CD-ROM. 1–15.

[25] Árpád Papp-Váry et al.2018. A Successful Example of Complex Country Branding: The 'E-Estonia'Positioning Concept and Its Relation to thePresidency of the Council of the EU. Acta Universitatis Sapientiae, European and Regional Studies14 (2018), 87–115.

[26] Jiye Park, Markus Jung, and Erwin P Rathgeb. 2019. Survey for Secure IoT group communication. In2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops). IEEE, 1026–1031.

[27] Haidhar Athir Mohd Puat and Nor Azlina Abd Rahman. 2020. IoMT: A Review of Pacemaker Vulnerabilities and Security Strategy. InJournal ofPhysics: Conference Series, Vol. 1712. IOP Publishing, 012009.

[28] J. Sengupta, S. Ruj, and S.D. Bit. 2020. A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. Journal of Network and Computer Applications 149 (2020), 102481.

[29] Saurabh Singh, ASM Sanwar Hosen, and Byungun Yoon. 2021. Blockchain security attacks, challenges, and solutions for the future distributed IoT network. IEEE Access9 (2021), 13938–13959.

[30] Ahmed Slalmi, Rachid Saadane, Abdellah Chehri, and Hatim Kharraz. 2021. How will 5G transform industrial IoT: latency and reliability analysis. InHuman Centred Intelligent Systems. Springer, 335–345.

[31] Gábor Soós, Dániel Kozma, Ferenc Nándor Janky, and Pál Varga. 2018. IoT device lifecycle–A generic model and a use case for cellular mobilenetworks. In 2018 IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud). IEEE, 176–183.

[32] Alireza Souri, Aseel Hussien, Mahdi Hoseyninezhad, and Monire Norouzi. 2019. A systematic review of IoT communication strategies for an efficient smart environment. Transactions on Emerging Telecommunications Technologies(2019), e3736.

[33] K Narendra Swaroop, Kavitha Chandu, Ramesh Gorrepotu, and Subimal Deb. 2019. A health monitoring system for vital signs using IoT.Internet ofThings5 (2019), 116–129.

[34] Yujuan Wen, Fengyuan Lu, Yufei Liu, Peijin Cong, and Xinli Huang. 2020. Blockchain Consensus Mechanisms and Their Applications in IoT: A Literature Survey. InInternational Conference on Algorithms and Architectures for Parallel Processing. Springer, 564–579.

[35] Xu Wu and Junbin Liang. 2021. A blockchain-based trust management method for Internet of Things. Pervasive and Mobile Computing72 (2021), 101330.

[36] L. Xing. 2020. Reliability in Internet of Things: Current status and future perspectives. IEEE Internet of Things Journal7, 8 (2020), 6704–6721.

[37] Bin Yu, Jarod Wright, Surya Nepal, Liming Zhu, Joseph Liu, and Rajiv Ranjan. 2018. Iotchain: Establishing trust in the internet of things ecosystem using blockchain. IEEE Cloud Computing5, 4 (2018), 12–23.