Internet of Things 9 (2020) 100114

Contents lists available at ScienceDirect

Internet of Things

journal homepage: www.elsevier.com/locate/iot

Advancements in distributed ledger technology for Internet of Things ☆

Suayb S. Arslan [a,*], Raja Jurdak [b], Jens Jelitto [c], Bhaskar Krishnamachari [d]

[a] MEF University, Ayazaga cad. No.4, Maslak, Sarıyer, Istanbul, Turkey
[b] Queensland University of Technology, Brisbane City QLD, Australia
[c] IBM Research, Saumerstrasse 4, 8803 Rüschlikon, Sweden
[d] University of South California, 90007 Los Angeles, California, USA

ARTICLE INFO

Article history:
Available online 13 September 2019

Keywords:
Distributed ledger
Blockchain
Internet of Things
Smart cities
Smart grids
Identity management
Fog computing
Edge computing

ABSTRACT

Internet of Things (IoT) is paving the way for different kinds of devices to be connected and properly communicated at a mass scale. However, conventional mechanisms used to sustain security and privacy cannot be directly applied to IoT whose topology is increasingly becoming decentralized. Distributed Ledger Technologies (DLT) on the other hand comprise varying forms of decentralized data structures that provide immutability through cryptographically linking blocks of data. To be able to build reliable, autonomous and trusted IoT platforms, DLT has the potential to provide security, privacy and decentralized operation while adhering to the limitations of IoT devices. The marriage of IoT and DLT technology is not very recent. In fact many projects have been focusing on this interesting combination to address the challenges of smart cities, smart grids, internet of everything and other decentralized applications, most based on blockchain structures. In this special issue, the focus is on the new and broader technical problems associated with the DLT-based security and backend platform solutions for IoT devices and applications.

1. Scope of this special issue

Internet of Things (IoT) is a special umbrella term adopted by the industry to characterize the growing number of digital gadgets (all collectively called "Things") that may interact with each other over unreliable network links and are able to process information with their neighbours to reach common objectives [1]. Heat sensors, drones, actuators, highway control systems, manufacturing equipment and cell phones all fall under the umbrella term IoT. One of the objectives of this massive connectivity and interoperability is to allow systems to generate meaningful data so that systems can operate autonomously and efficiently without the need for active human intervention. Such data aggregation also led to new technologies such as Artificial Intelligence (AI) and Big data analytics to branch out and help IoT get smarter in order to address today's connectivity requirements. However, IoT currently faces few serious problems such as concerning device/data vulnerabilities and security threats due to vast deployment. Not all data generated by IoT would be insensitive and public. In fact, privacy is an insurmountable challenge and yet a must key to maintain when the connectivity is all over the place. Increasing centralization is yet another privacy loop hole that begins ending up in personal identity thefts nowadays. Above all, conventional

☆ Guest editorial version requested by the Journal Management.

* Corresponding author.
E-mail address: arslans@mef.edu.tr (S.S. Arslan).

https://doi.org/10.1016/j.iot.2019.100114
2542-6605/

communication models (such as server-client) are no longer able to serve the requirements of IoT and the described model of connectivity. It is quite likely that we shall see over 50 billion devices that produce data at massive scales and yet they have to coordinate with each other efficiently, reliably and securely.

Distributed Ledger Technologies (DLT) and in particular blockchains seems to be the missing technology between the management of billions of connected devices and privacy and reliability concerns of our next generation connectivity needs. Although these devices can operate with the help of a master or coordinator, IoT needs to make the shift towards decentralization using trustless peer-to-peer model for better sustainability [2]. In order to enable decentralization and trust-less security, DLT appears to be the silver bullet needed by the IoT world. DLT can be utilized to track billions of connected devices, enable transaction processing and verification, coordination and keep consumer data semi-anonymous. In addition, due to its decentralized architecture, DLT also avoids single points of failure and provides mass scale reliability for the stored and communicated content. DLT provides various tools that not only helps to resolve which devices interact but also the nature of interactions through the use of smart contracts that tremendously improve the connectivity and open up new ways of functionality. Although DLT answers many of the challenges of today's IoT technology, it does not come without any disadvantages. For instance, compared to a properly configured centralized database, DLT shall operate at a lower transaction processing rate leading to increased latency in the system. Secondly, security and parallel execution seems to share a trade-off. While providing security, replication of data of massive size shall bring down the scalability guarantees leaving IoT devices treated unequally. In fact, many attempts have been made in the past on the consensus protocols [3] to resolve the scalability issue of DLT and as of yet no definitive answer is found that meets all of the requirements of IoT. In this special issue, we aimed to bring the powerful combination of DLT and IoT to daylight while emphasizing the set of issues that still needs to be addressed.

Though they are not limited to, the scope of submissions were expected to fall in one of the following topics:

- Distributed ledger theory in IoT.
- Identity management in DLT for IoT.
- Novel IoT applications based on DLT including blockchains.
- Experimental studies based on DLT-based IoT schemes.
- Scalability, Security, Privacy, Storage optimizations in DLT for IoT.
- Auditability and privacy compliance of sensor data using DLT.
- Use of DLT in cloud, edge and fog computing.
- DLT applied to smart cities, smart grids and internet of everything.

2. Contributions to the special issue

This special issue consists of two accepted papers and we briefly summarize their highlights here.

Embedded microcontrollers (MCUs) become the key development strategy for IoT devices in all forms of different industries including medical, energy and automotive. Since the authentication is based on a pair of keys, any connected device is configured with a secret key. In order for the deployed device to receive service, this key is both used for authentication and for signing data that is communicated over the network. In MCUs, the secret must be preserved so that any illegitimate device cannot access to it. Conventional schemes require storage and hence only few IoT devices can handle them [4]. *Miguel Angel Prada-Delgado, Iliminada Baturone, Gero Dittmann, Jens Jelitto and Andreas Kind***,** in their paper entitled "PUF-derived IoT identities in a zero-knowledge protocol for blockchain" propose an alternative authentication approach based on public-key cryptography in which an MCU generates a secret key internally based on the fact that manufacturing technology shows lots of variations in their processes and hence this variability can be used as a physical unclonable function (PUF). Such a scheme eliminates the costly external key generation process. In addition, the utilization of DLT with PUF makes the device authentication completely independent of the manufacturer. Since the ledger contents are also distributed and can be processed by others, the manufacturer guarantees availability due to offloading the administration overhead.

In the context of IoT and embedded systems, reactive behaviour is quite desirable in case of changing conditions or user behaviours. For instance, smart contracts in DLT become active only if a predetermined set of conditions met by the changing conditions. These types of reactive systems can be specified with Event-Condition-Action (ECA) rules which provide for a high-level and flexible description. Unfortunately, programming ECA rules is a challenging one and more often than not it leads to various errors. **D.R. Cacciagrano** and **R. Culmone**, in their paper entitled as "IRON: Reliable domain specific language for programming IoT devices" propose error-resilient and easy programming language that relies on ECA rules. More specifically, they recommend complete format semantics to resolve potentially incorrect actions due to the execution of ECA rule-based systems. This domain-specific language (DSL) prevents several anomalies such as the presence of cycles that determine the non-terminations and the breaking of invariances. Their scheme is largely inspired by Integrated Rule on Data (IRON) language [5] which supports categorization of devices into sets, multicast and broadcast abstractions. The paper finally develops an interpreter based on a host language that captures and manages the anomalies.

Considered together, these contributions clearly demonstrate unique solutions to two out of many challenges when DLT meets IoT technology. We believe there shall be many more studies yet to appear to secure the marriage of DLT and IoT in order to allow scalable, secure and reliable connectivity which is promised in 5 G and beyond technologies.

References

[1] L. Atzori, A. Iera, G. Morabito, The internet of things: a survey, Comput. Netw. 54 (15) (2010) 2787–2805.
[2] P. Brody, V. Pureswaran, Device Democracy: Saving the Future of the Internet of Things, IBM Institute for Business Value, Tech. Rep., 2014.
[3] I. Bentov, et al., Proof of activity: extending Bitcoin's proof of work via proof of stake, IACR Cryptol. 2014 (2014) 452.
[4] C. Shepherd, G. Arfaoui, I. Gurulian, R.P. Lee, K. Markantonakis, R.N. Akram, D. Sauveron, E. Conchon, Secure and trusted execution: past, present, and future - a critical review in the context of the internet of things and cyber-physical systems, in: Proceedings of the 2016 IEEE Trustcom/BigDataSE/ISPA, 2016, pp. 168–177.
[5] F. Corradini, R. Culmone, L. Mostarda, L. Tesei, F. Raimondi, A constrained ECA language supporting formal verification of WSNS, in: Proceedings of the 2015 IEEE Twenty-ninth International Conference on Advanced Information Networking and Applications Workshops, WAINA, 2015, pp. 187–192.