Blockchain Engineering for the Internet of Things: Systems Security Perspective

Davor Svetinovic
Electrical Engineering and Computer Science
Masdar Institute of Science and Technology
PO Box 54224, Abu Dhabi, UAE
dsvetinovic@masdar.ac.ae

ABSTRACT

The Internet of Things (IoT) technology has a potential to bring the benefits of intelligently interconnecting not just computers and humans, but most of everyday things. IoT has a promise of opening significant business process improvement opportunities leading to economic growth and cost reductions. However, there are many challenges facing IoT, including significant scalability and security challenges due to the integration of potentially huge number of things into the network. Many of scalability and security issues stem from a centralized, primarily client/server, architecture of IoT systems and frameworks.

Blockchain technology, as a relativelly new approach to decentralized computation and assets management and transfer, has a potential to help solve a number of scalability and security issues that IoT is facing, primarilly through the removal of centralized points of failure for such systems. As such, blockchain technology and IoT integration provides a promising direction and it has recently generated significant research interest, e.g., [4].

In this talk, we present our experiences based on our recent project in enhancing security and privacy in decentralized energy trading in smart grids using blockchain, multi-signatures and anonymous messaging streams [1], that has built upon our previous work on Bitcoin-based decentralized carbon emissions trading infrastructure model [2]. In particular, we present the blockchain systems security issues within the context of IoT security and privacy requirements [3]. This is done with the intention of producing an early integrated security model for blockchain-powered IoT systems [5]. The presentation is constrained to the discussion of the architecture-level requirements [6]. Finally, we will present the main opportunity loss if the integration ignores the full realization of the real-world asset transaction paradigm.

CCS Concepts

•Security and privacy → Software security engineering;

IoTPTS'17 April 02-02 2017, Abu Dhabi, United Arab Emirates

ACM ISBN 978-1-4503-4969-7/17/04.

DOI: http://dx.doi.org/10.1145/3055245.3055256

Keywords

Systems security; IoT; blockchain; bitcoin; trust; privacy

Biography

Davor Svetinovic is an Associate Professor at Masdar Institute of Science and Technology, UAE. His primary areas of expertise are software systems engineering and systems security. He received his PhD (2006) and MMath (2002) degrees in Computer Science from University of Waterloo, Canada. Previously he worked as a visiting professor and research affiliate at the Massachusetts Institute of Technology (MIT); and as a postdoctoral researcher at Lero – the Irish Software Engineering Center, Ireland, and Vienna University of Technology, Austria. He leads the Strategic Requirements and Systems Security Group (SRSSG), and he has extensive experience working on complex multi-disciplinary research projects. He has published over 50 papers in leading journals and conferences. His current research interests include software engineering, systems security and privacy, blockchain engineering, smart grids energy trading, and cryptocurrencies. He is a Senior Member of the IEEE.

1. REFERENCES

[1] N. Z. Aitzhan and D. Svetinovic. Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. *IEEE Transactions on Dependable and Secure Computing*, 2016.

[2] E. Al Kawasmi, E. Arnautovic, and D. Svetinovic. Bitcoin-based decentralized carbon emissions trading infrastructure model. *Systems Engineering*, 18(2):115–130, 2015.

[3] I. Alqassem and D. Svetinovic. A taxonomy of security and privacy requirements for the internet of things (iot). In *Industrial Engineering and Engineering Management (IEEM), 2014 IEEE International Conference on*, pages 1244–1248. IEEE, 2014.

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

[5] H. Suleiman, I. Alqassem, A. Diabat, E. Arnautovic, and D. Svetinovic. Integrated smart grid systems security threat model. *Information Systems*, 53:147 – 160, 2015.

[6] D. Svetinovic. Architecture-level requirements specification. In *STRAW*, pages 14–19, 2003.