Blockchain Applications

IN5420 Distributed Blockchain Technologies

Michael Eikeland

May 2018

Blockchains and Smart Contracts for the Internet of Things[1] examines whether blockchains and smart contracts are a good fit for the Internet of Things (IoT). While they find that the underlying composition of such a blockchain will depend on a lot of factors they claim that blockchain universally possess these benefits:

- A robust, truly distributed peer-to-peer system that is tolerant of node failures.
- A network that can identify conflicts and forks and resolve them automatically so as to converge to a single, globally accepted view of events.
- Transparency, verifiability, auditability on the network's activity. We get verifiable processes, whether these concern the exchange and tracking of a digital asset, or a data-driven interaction between parties. Every transaction presents a publicly auditable proof that it was authorized to interact with the system. Eliminates the possibility of disputes, makes reconciliation redundant.
- "A method for tagging different pieces of information as belonging to different participants, and enforcing this form of data ownership without a central authority".
- A system that allows non-trusting participants to interact with each other in a predictable, certain manner.

They argue that for the IoT-era blockchains could, through persistant data and filesystems, increase security in IoT-devices as information and data, along with important files, such as firmware updates, could be distributed between the devices. Thus these devices do not necessarily become as big of a security risk should the manufacturer stop supporting them.

While blockchains could make for fully autonomous processes between different party, such as in a supply chain, they also have some downsides. Compared to a more traditional, or centralized, solution, blockchains would due to the distributed nature of execution and validation, have lower performance. Another

problem might be that in a market context, competitors might gain an advantage through monitoring your activities on the blockchain.

While [1] addresses whether blockchain is a feasible solution to the challenges that come with IoT, **LSB: A Lightweight Scalable BlockChain for IoT Security and Privacy**[2], is more concerned with the feasability of deploying today's blockchain technology in an IoT environment. They find that *it is not*, and suggest a *Lightweight Scalable Blockchain (LSB)*, a blockchain custom-tailored to the IoT context. The authors point out resource consumption, centralization and lack of privacy as challenges that especially pertain to IoT. Furthermore, some capability issues between IoT and current blockchain technology is pointed out: complex consensus algorithms, scalability and overheads, latency, security overheads and throughput. LSB addresses these issues.

As the name **Providing Privacy, Safety, and Security in IoT-Based Transactive Energy Systems Using Distributed Ledgers**[3] implies, the paper looks at a more specific use case of blockchain in an IoT context, namely energy systems. This paper suggests using a distributed ledger within a permissioned network (i.e. a designated authority that can issue regulations) along with IoT devices (such as smart meters) to balance a microgrid with electricity. The authors put particular emphasis on the privacy aspect of such a system, in that energy usage of a household could be leaked and linked.

References

[1] K. Christidis and M. Devetsikiotis. "Blockchains and Smart Contracts for the Internet of Things". In: *IEEE Access* 4 (2016), pp. 2292–2303. DOI: 10.1109/ACCESS.2016.2566339.

[2] Ali Dorri, Salil S. Kanhere, Raja Jurdak, et al. "LSB: A Lightweight Scalable BlockChain for IoT Security and Privacy". In: (Dec. 8, 2017). arXiv: 1712.02969 [cs]. URL: http://arxiv.org/abs/1712.02969 (visited on 05/07/2018).

[3] Aron Laszka, Abhishek Dubey, Michael Walker, et al. "Providing Privacy, Safety, and Security in IoT-Based Transactive Energy Systems Using Distributed Ledgers". In: (Sept. 27, 2017). arXiv: 1709.09614 [cs]. URL: http://arxiv.org/abs/1709.09614 (visited on 05/07/2018).