Blockchain Platforms for IoT Use-cases

Mohammad Chowdhury, Md. Sadek Ferdous, Kamanashis Biswas
mjchowdhury@swin.edu.au, s.ferdous@imperial.ac.uk, k.biswas@griffith.edu.au

IoT & Blockchain: The Internet of Things (IoT) is experiencing an exponential growth in a wide variety of use cases, such as wearable devices, agriculture, smart cities, smart homes, supply chain and so on. IoT technology is fundamentally different, mainly due to its decentralized topology and the resource-constraints devices. Thus, IoT systems often rely on centralized computing and storage system (e.g., cloud infrastructure) for processing distributed data. This computation model usually suffers from privacy and security vulnerabilities. In addition, such devices depend on a heterogeneous underlying network infrastructure which is easy to attack as evident in several recent cyber attacks. Recently, blockchain technology has gained popularity in different domains because of its multiple properties such as resiliency, support for integrity, anonymity, decentralisation and autonomous control. Thus, blockchain technology can be an effective mechanism to address the issues involving IoT. Hence, there has been enthusiasms to combine blockchain technology with IoT.

Existing IoT-focused blockchain platforms: Towards this aim, several blockchain solutions for IoT environments have been proposed: IOTA [1], Waltonchain [2] and OriginTrail [3]. IOTA uses a special consensus algorithm, called Tangle, which uses Direct Acyclic Graph (DAG) and is much lighter than conventional consensus algorithms such as Proof-of-Work and Proof-of-Stack. Waltonchain combines blockchain with IoT (specifically RFID) to create a management system for supply chains. It uses their own Proof of Stake & Trust (PoST) consensus along with a node reputation mechanism. Finally, OriginTrail is used in the supply chain domain where different IoT devices are expected to create a network to track the state of a product within the supply chain network. To enable this, OriginTrail utilizes a layer-based approach where a blockchain platform functions in the bottom layer with the option to attach any blockchain platform as required by the application.

Analysing & comparing IoT use case requirements: Different IoT use-cases need different requirements. For example, requirements in smart cities are different to that of the wearable fitness tracking or goods tracking system in supply chain management. Even so, we can identify several core requirements prevailing in all use-cases:

- Transaction speed & cost
- Scalability
- Data security & privacy
- Trust establishment
- Virtual network among partners

Among these, transaction speed and cost, and scalability will mainly determine if a particular blockchain platform can handle the amount of data generated by multitude of IoT devices as well as if it feasible in terms of the associated cost. Data security and privacy will need to consider the confidentiality, integrity, access control and ownership of data and IoT devices in the network. Trust establishment will consider how a platform can establish trust. Finally, the virtual network among partners will consider the scenarios when different partners need to share their data generated from their corresponding IoT devices just within themselves. Table 1 shows a brief analysis of the derived general requirements and the coverage of the existing blockchain solutions. It is evident from the table that the existing platforms do not address all our identified requirements.

Future work: In future, a detailed analysis of each of the requirement in the table will be done. The proposed concept level requirements and comparison of blockchain platforms will lay the foundation for understanding and developing blockchain platforms.

Table 1: Comparing IoT requirements and Blockchain platforms

Requirements	IOTA	Waltonchain	OriginTrail
Transaction speed and cost	500-800 transactions per second. 0 Fees.	4 transactions per second. Uses side chain to speed up.	Depends on IOTA, Ethereum, or NEO for consensus.
Data Security & Privacy	Support data security but not privacy of data	Support data security but not privacy of data	ZKP [4] to provide privacy of the transacted data.
Trust Establishment	IDoT [1] is used to build reputation systems	Use node reputation mechanism	Each stakeholder has to be approved by the previous node
Virtual network	Does not support. However, plan is in the pipeline.	Does not support private communication	Does not support private communication

Reference:

[1]. IOTA White Paper, https://iota.org/IOTA_Whitepaper.pdf
[2]. Waltonchain, White Paper, https://www.waltonchain.org/doc/Waltonchain-whitepaper_en_20180208.pdf
[3]. OriginalTrail White Paper, https://origintrail.io/storage/documents/OriginTrail-White-Paper.pdf
[4]. Feige, U., Fiat, A. and Shamir, A., 1988.Zero-knowledge proofs of identity.Journal of cryptology, 1(2), pp.77-94.