Position Statement

Blockchain for IoT

May 31st 2016

Contents

Page

1 Personal Background 3

2 Directions in Blockchain for IoT 3

1 Personal Background

Prof. Theo Dimitrakos: Chief Researcher (permanent position) in the Security Futures Practice of BT Technology, Service & Operations (BT TSO) and a Professorial Fellow (part-time) at the School of Computing at the University of Kent. He has twenty years of research and innovation experience in a range of topics relating to Information Security, Identity and Access Management, Cloud Computing, Trust Management, Service Oriented Architecture (SOA), Web Services and Grid Computing. He is involved in the Cloud Innovation Strategy definition at BT, leading the Cloud Security stream, and has led the production of new innovative capabilities on Cloud Computing and Cyber Security. Theo also plays a leading role in some of the largest and most successful collaborative European research initiatives. Theo has also served in the programme committee of various academic and industry conferences and the editorial board of international journals. Theo has been an author of 8 books, over 100 technical papers in international conferences and journals and an inventor of over 20 patents. He has been an invited speaker in various security and cloud industry events. He has a PhD in Computing from Imperial College London in the UK and a BSc in Mathematics from the University of Crete in Greece.

Our BT Research and Innovation team has patented in excess of 10 patents related to Blockchain including Identity Management, Blockchain attack detection, or Blockchain driven service optimisation.

2 Directions in Blockchain for IoT

Blockchain infrastructures have general aptitudes which are interesting to the safe distribution of IoT both in home usage, public operations and industrial scenarios. With the Blockchain protocols ability to carry transactions even on un-trusted networks, deployments of nodes across diverse geographical areas can provide IoT vendors with globally available end points. Replication of status (i.e. public ledger) can be used to minimise latency, and support mobile IoT devices. Interoperability between IoT and Blockchain deployments can provide valuable complementarity.

However, simply interfacing IoT devices to Blockchain deployment does not solve security issues often associated with IoT. The main issue with IoT capabilities is that devices need a great degree of autonomy in order to function properly. Minimum human intervention also means that they require to self-manage security aspects. Security vulnerabilities in IoT devices have attracted attention from the IT community and the following aspects have been highlighted:

- Choice of trust and consensus models that allow for self-regulated memberships
- Secure network connectivity for outbound as well in inbound traffic
- Robust encryption of data transfer
- Device and possibly owner identification

In most cases, IoT devices have their software and hardware specifications in the public domain and can therefore be easily reverse engineered. Blockchain protocols do provide secure transfer and non-repudiability, however they do not provide protection against impersonation. Access keys can be stolen, or devices may be cloned.

The aim of this discussion is to provide commoditised and transparent security to end users, and how Blockchain protocol can be used to support this objective. The objectives include reduce the risk of impersonation of the device, or the associated end users. End users need to be able to associate an identity to their IoT devices without increasing the risk of identity theft. Different security aspects need to be customised and configured for IoT devices such as data encryption. Other security features should also be managed where applicable such as updates, intrusion detection, or malware removal.

Offices worldwide

Registered office: 81 Newgate Street, London EC1A 7AJ
Registered in England No: 1800000