Position Statement

Blockchain based Identity Management

May 31st 2016

Contents

1 Personal Background

Géry Ducatel: Principal Researcher in BT, Research & Innovation, Security Futures Practice. I have been involved in designing of a vision for the Blockchain for the last two years. The team has set out a programme around Blockchain and I lead on the Identity Management implications. In parallel to Blockchain I am involved in designing Identity as a Service for cloud deployment application services. Prior to that I have been involved in deploying Federated Identity management systems with BT Cloud Compute integrated into a solution retailed by BT Global Services.
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 Based Identity Management Solutions

Research and Technology is looking to implement complete Identity Management solutions relying on Blockchain identity. BT Research and Innovation has laid out a vision for Blockchain based service exploitation where users are empowered entities able to control and manage service consumption whilst enforcing privacy controls. Blockchain and Identity is gaining popularity, early examples have been described in Bitauth[3] is a solution for a decentralised authentication system which is based on SIN [4], a System Identification Number is a form of identity based on a cryptographic key pair. Blockstack, is another example of Blockchain based identity database. Blockchain base identification [5] has interesting privacy control management capabilities, however, its rigid implementation does not make it attractive to organisational scenarios.
Using blockchain for application provisioning provide many benefits from a point of view of process simplification. The Blockchain provides one operational component that advantageously replaces complex functions including: User Management, Billing, auditability. Whilst organisations need to extend and diversify their network and compute capabilities outside of their intranets, they also need to centralise functionalities such as access management in order to protect business continuity. This implies that the identity of the organisation overrides that of the employee using the system. Legacy user management has challenges such as user permission creep. Users are granted too much access in order to simplify the task of system administrators. This over-exposure has security and management cost implications [1]. In relation to billing and also budget control, some existing solutions have demonstrated the ability to ring fence blockchain transaction [2]. Historically, Blockchain authentication has been based on Public Key Infrastructure which is an effective way of identifying a user without having to maintain an Identity and Access Management solution. However, this does not allow organisation to easily control what users are allowed to do on a blockchain based service management.

3 Topics to Cover in Order to be Effective

The research is currently looking at bringing benefits from Blockchain based Identity Management solutions and integrate them with organisational processes.
Challenge/Opportunities with Identity solutions include:

- How to use smart contract to help organisations manage access to Blockchain solutions.
- How to apply Blockchain transaction policies and how to enforce them

- How to revoke Blockchain access once authorised

The research into Identity Management is looking at interoperability between Blockchain and other Identity and Access Management solutions in order to satisfy organisational access to Blockchain services.
Important milestones in this approach include the ability to apply and enforce blockchain usage policies. This will allow organisations to provision, de-provision, and delegate services. Having organisation wide policies will facilitate and will demonstrate an alternative to complex billing platforms. At an individual level, Blockchain based protocol can also be expanded to complement the management of Personally Identifiable Information in collaboration with existing Identity Management solutions.

4 References

[1] Adallom (2014) *Cloud Usage Risk Report*,

[2] Assia, Y., Buterin, V., m liorhakiLior, Rosenfeld M., *Colored Coins whitepaper*, https://docs.google.com/document/d/1AnkP_cVZTCMLIzw4DvsW6M8Q2JC0IIzrTLuoWu2z1BE/edit#heading=h.wxrvzqj8997r (retrieved 24/04/15)

[3] Martindale, E. (2014) BitAuth, for Decentralized Authentication https://github.com/bitpay/bitauth (retrieved 22/05/15)

[4] Garzik, J (2014) SIN: Fully decentralized, anonymous, secure identity https://en.bitcoin.it/wiki/Identity_protocol_v1 (retrieved 22/05/15)

[5] Blockstack docs (2016) https://blockstack.org/docs (retrieved 31/05/16)

Offices worldwide

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