Official Minutes of the 4th BARAC Meeting, 16th July 2018

Topic: Identity Anonymity and Regulation in Blockchain Systems

The BARAC project investigates technical, legal and managerial aspects related to use of DLT in the services industry including the significance of new business models and their effects on industry structure.

The focus of this meeting is on identity, anonymity and regulation in Blockchain systems. The presentations delivered during the meeting address KYC, identity, and how a DLT can mitigate the distribution of personal and private data. The conference closed with a lively discussion about data security in Blockchain technologies.

The discussion topics included a call to collaborate on further research on the topics presented by Geoff Goodell. Many of questions focused on General Data Protection Regulation (GDPR) by the EU and how DLT systems can be adapted to comply with its requirements. It was identified that the lack of regulation, and clarity about future regulation, of DLT systems may impede the development of new solutions by businesses. It was also identified that it is important to acknowledge differences in attitudes about self-sovereign identity between current and future generations.

"Blockpass: Passport to a Connected World." Presented by Guy Davies of Blockpass and Liam Bell of Edinburgh Napier University.

Blockpass is a new (one year old) company that aims to enable individuals, companies, devices, and objects to use self-sovereign identity.

Blockpass comprises two companies: Chain of Things, based in Hong Kong, and Infinity Blockchain Labs, based in Vietnam. The idea is that Blockpass will act as a curator of verifications, providing certificates and the required ecosystem for its users. Blockpass itself doesn't store or verify any data. It cooperates with certification authorities to accomplish this task.

In many currently popular applications, users have little or no control over their data. Blockpass implements self-sovereign identity by storing data in a decentralised manner using blockchain technology. Users first share their data with Blockpass, and they are able to use the Blockpass service to verify themselves to Blockpass-enabled applications. Following verification, the identifying data used for the session will be destroyed.

A key goal of Blockpass is to offer zero-knowledge proof of identity. Zero-knowledge proofs allow users to prove their knowledge of certain information without giving it away.

Blockpass shall collaborate with the Edinburgh Napier University to conduct further research in identity management.

14:30 "ObjectTech." Presented by Paul Ferris of ObjectTech

Paul Ferris gave a presentation about ObjectTech and its current projects. As data can be regarded as the raw material of the 21st century, it has become less clear who owns the data. ObjectTech is addressing this issue by developing solutions that allow the information to manage itself.

Although this approach depends upon secure technology, it also depends on the development of legal structures and regulations that will ultimately determine the degree to which it can be achieved. To this end, ObjectTech also engages in the regulatory environment, has established legal frameworks to enable this approach and participates in various working groups to ensure international adoption.

ObjectTech is currently working with Dubai and other air transport hubs to enable gate-free entry into the country by combining biometric verification with blockchain technology. A multi-biometric approach, employing facial recognition, LiDAR scanning and other biometric indicators will develop a profile of each passenger and verify it against multi-factor data held within a digital passport. The gate-free entry is just one application of self-sovereign identity. Further applications outside of air travel, such as payments and health make use of the same multi-factor approach, enabling a new economy of services that are highly personal, private and secure. It is estimated that by 2030 around 70% of adults will use self-sovereign identity technology.

"Digital Identity and KYC." Presented by Abbas Ali of R3.

The R3 network is an alliance of the world's largest financial institutions, insurers, regulators, exchanges, law firms, partners and financial technology providers committed to delivering the next generation of financial infrastructure based on blockchain. Corda is R3's opensource blockchain for business. The first generation of blockchain platforms were not designed for business. They lack key characteristics demanded by business including privacy and finality. Corda was designed from the start for business. Corda's smart contracts enable privacy and finality across any agreement or asset type.

Using self-sovereign identity can have many positive impacts in different use cases. Nowadays each bank has its own database of clients that it does not share with other companies. Concepts of sharing information can be seen in many cases, e.g. Google accounts that can be used to log in on multiple websites. The downside of this approach is that Google is the owner of all information and users do not have an influence on how the data are used. This could be addressed with self-sovereign identity allowing individuals to access and control their information.

Other projects in which R3 participates include LEIA 2, a collaboration with 12 banks to develop a KYC system. Most recently, 39 financial firms partnered with R3 to complete more than 300 transactions using R3's know your customer (KYC) application. In addition to that, it is working with the Decentralized Identity Foundation which aims to build protocols for interoperability between DLT platforms. It also partners with organizations including Gemalto, Evernym and other identity ISV's to develop identity networks on Corda.

"Decentralised Identity and Private Payments." Presented by Geoff Goodell of University College London

Geoff Goodell described two of his project he is currently working on.

The first project is based on decentralised digital identity architecture. The problem of digital identity is that powerful 3rd parties acting as authentication providers occupy a position of control, capture monopoly rents, and invite corruption. A solution to limit the power of third parties is to use DLT. Some human rights concerns related to digital identity include control points used to co-opt

the system, architecture that leads to surveillance, and non-consensual trust relationships. DLT can be used to empower businesses to establish their own practices and relationships, empower service providers to establish their own ID platforms, and empower users to manage linkages among their activities. To counteract the power of authentication providers a user-centred approach to identity would allow users to generate their own ID depending on the purpose of use. Goodell is working on a solution involving blind signatures in which the distributed ledger sends back a set of one-time credentials. For this system to work authentication and certification providers would need to be separate institutions.

The second project focuses on a different aspect of DLT in regulation. Users of cryptocurrency require privacy. Often people who conduct transactions on the DLT do not want to be tracked, an interest that in some cases may conflict with the KYC requirements imposed on bank accounts. People, technology and regulations form a system. To achieve agreement about a particular technology and the required regulation to protect essential privacy rights, policy and the mechanisms used by individuals to transact should be separated from each other. The idea is to develop a system that is in some ways similar to cash, which does not require a specific identification every time a transaction is conducted, and in which users only disclose the specific information required in each case. For this project, Goodell is inviting BARAC participants and members of CBT to collaborate.