ROUND TABLE

Notes from a roundtable discussion about Bitcoin, Cryptocurrency and the Blockchain

BitCoin, Cryptocurrencies and the Blockchain

21st May, Sopra Steria, London

Delivering Transformation. Together.

sopra steria

1. Introduction

1.1. Introduction

Sopra Steria convened and hosted a roundtable to discuss the emerging technology use cases of the Blockchain, future aspects of cryptocurrencies global acceptance, including Governance, Trust and Regulation, and considered how Blockchain technology (or its inherent capabilities outside of Bitcoin network) may influence future commercial trading patterns.

22 organisations attended the session (full details are at Appendix 1).

2. What are the use cases for and benefits of the Blockchain?

2.1. Introduction

At present financial services organisations operate complex systems for the management of transactions. The reconciliation of assets, contracts and the vast majority of transactions are controlled by paper, using printed forms, signed contracts etc. Most operations are still not digital, nor exist on a propriety trustable technology.

A blockchain is a shared ledger which enables all transactions to be visible to those participating in the blockchain. A blockchain is a single version of the truth that does not require trust between 3rd parties to enable transactions to be validated. Trust needs only to exist between the individual and the blockchain.

Any new organisation considering a venture into the blockchain space has the option to consider either:

1) Building their services on a widely used public blockchain (e.g. Bitcoin)
2) Creating a new private blockchain
3) Piggybacking on a public blockchain, with the use of a sidechain

A public blockchain is a 'Permissionless; blockchain, which means that any entity is able to post transactions, and insert messages using the 40 bytes of space that is allocated to all transactions. A private blockchain is a 'Permissioned' blockchain, which enables the tailoring of a newly created blockchain to the needs of the organisation or group of entities that require it.

2.2. Use cases

2.2.1. Asset registration

A service which is posting details of entries onto the Land Registry into a blockchain is likely to use a permissionless blockchain as this is freely visible for any entity to check against it. Honduras is partnering with Factom to use the public bitcoin blockchain for their Land registry.

Coloured coins can be used to control the transfer of assets, including any type of product where ownership can be declared. Smart properties, and smart contracts are new innovations that benefit from the public bitcoin blockchain. A standardised approach to the idea of coloured coins is available in the form of Open Assets. The Nasdaq is experimenting with this protocol in the recording of trades to the blockchain on their Pre-IPO trading arm, Nasdaq private markets.

2.2.2. Banking transactions

A bank or group of like-minded banks may opt to use a private permissioned blockchain which would be supported by only authorised computers, and where transactions are only visible to those with the permission granted to them. The 40 bytes allocated to the message space could be amended to any arbitrary value, and the type of proof needed to write transactions to the blockchain could be something practical for the purposes of the blockchain being designed. Governance would be central to the way the blockchain is supported and maintained and operated on, and would enable the innovation of the blockchain to be harnessed without the aspect of every transaction being in the public domain.

However, permissionless systems are the vast majority of applications and innovations being developed. Venture capital in permissionless centric blockchain start-ups is currently outpacing the investments made into the net in '95.

Her Majesty's Treasury recently issued a call for information which led to a response that some form of regulation will be applied.

2.3. Related reading:

Tim Swanson – Permissioned Ledgers

EBA – Blockchain tech could improve banking

2.3.1. Identity

One of the most important aspects of innovation on the blockchain is the idea of an identity. From a device in your kitchen, to the 'ultimate beneficial owner' of an asset, understanding the concept of an identity, and the interactions between identities are central to understanding how the blockchain environment can be harnessed.

IBM and Samsung are making steps in this direction with Adept: an initiative attempting to harness the blockchain to manage identity in 'the internet of things'. A decentralised 'internet of things' is analogous to an 'internet of identities', a principle that offers a variety of benefits to those hoping to capitalise on a decentralisation.

Relating identity to ownership allows for issues relating the difficulty of establishing an owner to be tackled.

Complicated relationships can be represented in a hierarchy of private keys – which can enable organisations, or entities within an organisation to be attached to the ownership of similarly complicated entities. Transactions between complicated relationships can be maintained, and trusted and used to enable ownership to be traced to the right entity.

An example is coal where ownership of the asset (and its value) changes over time. Ultimate value extraction is at the point of converting the coal into power. However, the use of blockchain identification enables a more distributed ownership of that value. As coal moves through the supply chain, the change in ownership of the asset can be related to complicated arrays of entities based on complicated rules of transition, meaning that downstream benefit can be correctly attributed according to predetermined agreements and triggers.

2.3.2. Security and Law Enforcement

The Suspicious Activity Report (SAR) system run by the Financial Crime Unit has received 350,000 submissions relating to blockchain transactions and there has been 1 successful conviction. The decentralised and public aspect to the blockchain allows for forensic analysis of transaction history and behaviour. The open and voluminous nature of data held within the blockchain means that a variety of valuable insights can be gained by law enforcement agencies to support efforts against money laundering and other serious crime.

3. Why is trust so important?

3.1. Context

Five acts of Congress have been passed in the US in response to the existence of the blockchain technology. The acts seek to apply standardisation to transactions and transfers regarding the way 'actors' and 'assets' are used. Currently EU Cyber Security Strategy makes no direct reference to blockchain technology. At present, very little regulation exists and governance is sought to reassure new companies that are innovating in this space that are operating within the law and are unlikely to be closed down or have action taken against them. Regulation can stifle innovation and in some cases, in particular in New York, the need to acquire and maintain a BitLicense can be prohibitive due to the associated costs.

There is a general view that with the internet, regulatory bodies are in a constant state of catch up, and only applying governance once the technology has matured, and its full implications are known.

It is worth noting however that a large part of the way cryptocurrencies are used is similar to pre-paid payment cards and the work that has been done so far in relation to governance in this space is applicable.

3.2. Governance concepts:

The following paragraphs represent a short list of directions currently being considered by regulatory bodies that may be applicable to the governance or regulation of blockchain technologies

- PKI Bridge
  - A trust model for the way that organisations across borders can interoperate. Nation to nation, or within a single nation via the administration of digital certificates
- Varying levels of disclosure
  - Veronimity – Fully verified Identity (link/source required might be misspelled)
  - Partial Anonymity – Described in detail by ISO29191
  - Anonymity – fully anonymous transactions
  - Pseudonymity – sender and receiver can by referenced, but do not connect to a known identity
- Trust framework
  - Similar to UK's Age Verification framework
- There is a Whitechapel thinktank that is leading some of the development of consensus around application of blockchain technology.

It's clear that significant progress has been made in some areas whilst more work is planned in relation to governance concepts and how these might develop. The following is a summary of the current position:

- Regulatory bodies are naturally behind the curve on this technology and are unsure what to do
- The concept of 'Identity' will need to be redefined, and is likely to form the basis of how regulations are formed
- The UK needs to be – and has an opportunity to be – a leading working environment for blockchain technology firms. Largely due to there not being prohibitive costs to operate a blockchain company that exists in New York and California.
- The government has a duty to protect users.

4. Misuse : what is the nature of the challenge to trust?

The trust in a market or technology is critically dependent on the trust that can be associated with transactions in that market. The markets of wine, art and diamonds are comparable to cryptocurrencies and blockchain services and markets due to the open and unregulated nature of their day to day use. These markets rely heavily on trust and – as was seen in a recent event within the wine market which saw a 42% drop in capitalisation – the loss of trust can have a huge impact.

Within these markets the police often struggle to overcome the fundamental challenge of how to evidence a crime and how to seize an asset.

Advanced fee fraud has been recorded as a crime that is being tackled by the police and other law enforcement agencies in relation to by users of cryptocurrencies.

An illuminating example relates to Titanium Stresser, a DDOS (distributed 'Denial of Service') that had been available for hire and associated with fraudulent activities. Part of the investigation into Titanium Stresser looked into the acquisition of 802 bitcoins and highlighted challenges and strategies in the way the investigation can yield results in the form of evidence and seized assets.

The main tool used to assist the investigation has been the transcripts gathered of online chats via Skype. However new technologies (Chainalysis) that trace bitcoin payments are likely to be of use in investigations of this nature due to the blockchain holding information on the journey of individual transactions. Challenges exist in relation to the way bitcoins pass through exchanges, and also bitcoin mixers which are tools created specifically for the purpose of hiding a transactions history.

It has been a point of contention as to how perfect a level of provenance can be discovered in relation to individual transactions, and there are blockchains and cryptocurrencies that are built specifically to provide anonymity for those creating transactions. Bitcoin however is a pseudonymous coin so transactions are associated with individual addresses which can be traced easily. For transactions which are sent from a multitude of senders to a multitude of recipients it is difficult to trace the route of the individual payments. So it is clear that, whilst bitcoin can trace provenance through bilateral transactions, complex exchanges that involve multiple sources and multiple recipients are often more opaque. A convention of how the multiple transactions could be adopted to instruct on how the payments are allocated. However, this would need to be applied at an application level and not within the core blockchain system as it exists in its current form.

5. What opportunities exist to establish an effective governance model?

5.1. Economic Internet of Everything

There are a variety of opportunities to be pursued in relation to blockchain technology and open organisations like Focafet are attempting to help with the way standardisation can be applied to concept of identity.

The UETP protocol is an attempt to provide a framework on how a transaction can be described when made between devices from a variety of networks. The attempt is to assist with the 'internet of things' and the identity of the 'things' on this network having a standard operating model on which to communicate and transact with other 'things'. For example, defining how information that defines the 'Who', 'What', 'When', 'Where' and 'How Much' of devices can be communicated.

However, there are challenges inherent in any attempt to govern the entities that perform transactions, for example an Organisational Legal Entity that is a standard term used, does not necessarily have a central authority and an entity described as having a formal Organisational Legal Entity name may not be a properly registered organisation. Where an organisation is defined as formally having registered as legal entity may a short time later become non-legitimate, and so there is a need for a self-governing real time authentication of entities that describe themselves in specific formal ways.

5.2. Regulation

The UK DCA is non-profit organisation that has worked with the Home Office in enabling communications made to be relevant and specific to cryptocurrencies and the blockchain. Basic restrictions on the ability for a bitcoin/blockchain company to be allowed to open a bank account are restricting enterprise and causing delay to the way innovations can be pursued and marketed in the UK. However, the UK DCA has broken ground and after a significant period of pursuit, has been granted a bank account.

A consensus has been achieved that, whilst regulation has its benefits and can promote growth and innovation in some places, a sensible approach is likely to be a system of Principles of Regulation - or self-regulation. This may allow for an aligned approach and will enable new firms to understand the approach being taken by their peers to help guide their activities. However, there remains in some quarters a desire to roll back even the first steps of regulation in relation to basic Know Your Customer (KYC) and Anti Money Laundering (AML) processes to enable an even more open approach to innovation.

The UK, if it is to become a leader in this industry, will need to find the right balance between regulation, innovation and support to enable new and existing companies to form a cohesive and resilient operation that adds value.

5.3. Other opportunities for exploitation and collaboration

The UK has enormous opportunity particularly due to its Common Law approach. The industry desires to get UK on the front foot. Whitechapel (forum) has links to government that this group should leverage. The main problem is the rate of change and increasing complexity. Dialogue will provide oxygen.

The UKDCA advised that the Regulatory regime paper issued on Budget day. UKDCA intends to lead the standardisation effort, aiming to assemble a community to develop a Publicly Accessible Specification (PAS - small British Standard) in a year.

Consumers can be properly protected. BoE needs to understand how.

AML is an issue and the problem is that the rush to regulate could stifle innovation.

The European Securities and Markets Authority (ESMA) has put out a call for information on cryptocurrencies and the technology that supports it. They should be encouraged to our next meeting.

There is a linkage to standards in many areas. The situation was likened to different cryptocurrencies and block chains being dissimilar bricks. Everyone wants a wall (lots of interoperability and re-use) but what we have are piles of dissimilar bricks. We need to start building if we want to understand what works and what doesn't. There is more work to do with International Standards Organisations.

6. Next steps

The following next steps were suggested:

1) To convene socially within the Blockchain interest group set up by Andy Coakley (Sopra Steria) on LinkedIn
2) To assist Patrick Curry (British Business Federation Authority) in contributing to the definition of the forthcoming convention on governance
3) To participate in a series of educational sessions that would enable the group to consider specific aspects of the topic and engage with a broader community.
4) A further session is to be convened in Q4 2015. Invites to attendees to be issued and expressions of further interest from wider industry welcomed.

Appendix 1 Attendees

The following attended the event :

Sopra Steria FS Solutions & Consulting Managing Partner
Sopra Steria Dir of Innovation
Sopra Steria Payments Lead
Bank of England Digital Currencies
British Business Federation Authority
Barclays Bank
ACPO National Cyber Crime "Protect"
City of London National Fraud Investigation Bureau
Safello - BitCoin Exchange
Elliptic and ex Bitcoin Foundation
Focafet & AMB Ambro (NL)
Blockchain
University of Groeningen, NL - EU Funded Internet Governance
Co Founder & General Council - Epiphyte (Crypto Finance)
Microexpert
Context in Trust
FinTech Stars
Roolo
EX CEO and Founder CHI-X exchannge.
Vocalink
Chainalysis
Sopra Steria Banking AP CONSEI
BNP Paribas
Alvarez and Marshall
Sopra Steria
UK Digital Currency Association

About Sopra Steria

Sopra Steria, European leader in digital transformation, provides one of the most comprehensive portfolios of end to end service offerings in the market: Consulting, Systems Integration, Software Development and Business Process Services. Sopra Steria is trusted by leading private and public organisations to deliver successful transformation programmes that address their most complex and critical business challenges. Combining high quality and performance services, added-value and innovation, Sopra Steria enables its clients to make the best use of information technology.

SOPRA STERIA
Three Cherry Trees Lane, Hemel Hempstead, HP2 7AH
+44 (0)370 600 4466 - info.uk@soprasteria.com

PB008V01

www.soprasteria.co.uk

sopra steria