ITU

ITU Workshop on “Security Aspects of Blockchain” (Geneva, Switzerland, 21 March 2017)

Blockchains – risk or mitigation?

Patrick Curry OBE CEng

Director, BBFA: patrick.curry@bbfa.info

Director, Kyckr; patrick.curry@kyckr.com

Geneva, Switzerland, 21 March 2017

Internet Governance Forum 2015
Brazil

“Block chain technology is probably the biggest game changer for the Internet”

Questions

Is this for good or bad? Will it help to make the Internet safer and more secure – and more beneficial?

We need block chains to help make the Internet more trusted.

We need block chains to be trusted, which requires other components around/with block chains

Impact of Various Regulations in the Pipeline

Source Dr Anthony Kirby 2016

	Timing	Buy-side impact	Sell-side impact	Custodian impact	FMI impact	Gov / LE Impact	Risk Impact	Business impact	Systems impact	Data impact
AIFMD Reporting	Jul 2014	LOW-HIGH	LOW-MED	MEDIUM	LOW	LOW	LOW-HIGH	LOW-HIGH	LOW-HIGH	LOW-HIGH
TD 2	Jul 2015	LOW	LOW	LOW	LOW	MEDIUM	LOW	LOW	LOW	LOW
UCITS V	Mar 2016	LOW	LOW	LOW	LOW	LOW	LOW	LOW	MEDIUM	MEDIUM
EMIR	June 2016	LOW-HIGH	HIGH	MEDIUM	MED-HIGH	MEDIUM	MED-HIGH	LOW-HIGH	LOW-HIGH	HIGH
MAR	Jul 2016	MEDIUM	HIGH	MED-HIGH	HIGH	MEDIUM	MEDIUM	MEDIUM	MED-HIGH	HIGH
SFTR	>Jan 2017	MED-HIGH	HIGH	LOW	MEDIUM	MEDIUM	MEDIUM	MED-HIGH	MED-HIGH	HIGH
PRIIPs	>Mar 2017	HIGH	LOW	MED-HIGH	LOW	MEDIUM	MEDIUM	HIGH	HIGH	HIGH
MLD 4	Jun 2017	HIGH	HIGH	HIGH	LOW	MEDIUM	HIGH	MEDIUM	HIGH	HIGH
CRS	Sep 2017	MED-HIGH	HIGH	HIGH	LOW	MEDIUM	MEDIUM	MEDIUM	MEDIUM	HIGH
Benchmarks	Dec 2017	LOW-HIGH	HIGH	MEDIUM	HIGH	MEDIUM	HIGH	HIGH	MEDIUM	HIGH
ELTIF/MMR	Dec 2017?	LOW-HIGH	LOW	MEDIUM	LOW	LOW	LOW	MEDIUM	MEDIUM	MEDIUM
MIFID 2	Jan 2018	HIGH	HIGH	MEDIUM	HIGH	LOW	MEDIUM	HIGH	HIGH	HIGH
IDD	Jan 2018	LOW-HIGH	LOW	MEDIUM	LOW	LOW	MEDIUM	MEDIUM	MEDIUM	HIGH
PSD 2	Jan 2018	LOW	LOW	MEDIUM	LOW	HIGH	LOW	LOW	LOW	MEDIUM
GDPR	May 2018	HIGH	HIGH	HIGH	HIGH	HIGH	HIGH	HIGH	HIGH	HIGH
FRTB	Q1 2019?	LOW	HIGH	MEDIUM	LOW	MEDIUM	HIGH	MED-HIGH	HIGH	HIGH
CSDR settlement	Q1 2019?	MEDIUM	HIGH	HIGH	MED-HIGH	LOW	MEDIUM	MED-HIGH	MED-HIGH	HIGH

Game Changers

- Bank’s top issue – EU General Data Protection Regulation (GDPR) – fine up to 4% of global turnover with reputational damage
- Highest impact - data (quality)

- How much and for whom?
  - Anti Money Laundering Directive 4
    - Requires identification, strong authentication, beneficiary traceability & persons of significant control (PSC)
    - Requires any company to do Know Your Customer (KYC) checks for payments of €10,000 or more.
    - This affects everyone in Europe and every payments block chain
    - Includes virtual currencies
    - AL5 includes recognition for eIDAS
  - Payment Services Directive
    PSD2 requires requirement for Secure Customer Authentication, except for contactless card payments under €50, card not present transaction under €10, and payments to a payee that the payer has explicitly whitelisted

Other requirements

- Traceability
- Anti-counterfeits
- Compliance
- Authoritative sources
- ….(many more)

Employee - Gov

Employee - Industry

4 Contexts of Identity

Citizen

Consumer

www.sjolanders.homestead.com
SVERIGE
SUÈDE SWEDEN SCHWEDEN
PASS
PASSPORT
An tAontas Eorpach
European Union
ÉIRE
IRELAND
BELGIQUE BELGIË BELGIEN BELGIUM
CARTE D'IDENTITE IDENTITEITSKAART PERSONALAUSWEIS IDENTITY CARD
SPECIMEN
PERSONALAUSWEIS REPUBLIK ÖSTERREICH
MUSTERFRAU
ISOLDE

Assuring the blockchain internally

- Quality of written data
- Liability and shared risk. Reputation management
- Assured signatures and organisation ID *at that time*
- Smart contract automation could be a risk
- When do we need proof of work? Replace proof of work with PKI federation to reduce risks & costs, and improve performance
- When do we need proof of state? What alternatives?
- When do we need mining? What alternatives?

Assuring the blockchain externally

- Access control (AAA)
  - PKI federation to enable collaborative key management. ISO 29115/X.1254; ISO 29003; X.509
- Trusted attribute providers
  - Requirement for ROLOs (Register of Legal Organisations). Use other authoritative sources now
  - Other TAPs for an increasing range of attributes
- Collaborative governance
  - Common Policy and shared risk mitigation
  - Federated trust
  - Assured supply chains etc. Certification
  - Privacy and consent management

New technologies

- 15 identified by the banks
- Disruption
  - Blockchains
  - Trusted smartphones
  - Zero knowledge proof (ZKP)

Existing Standards

- ISO TC307
- ISO JTC1 SC27
- ISO TC68
- ITU-T Block Chain WG
- OASIS
- W3C

National

- NIST
- NASPO
- DIN
- AFNOR
- …. UK BSI

- Identity management
  - Authentication (ISO 29115)
  - Identity proofing (ISO 29003)
- Access control
- Privacy & de-identification
- Risk management
- Cyber assurance & ISMS
- Cryptography
- Incident management

What is specifically needed?

- Reference Architecture
  - Types & categories of block chain -
  - Technology options, terminology, architectures
  - Proof of Work, Proof of State
  - Components
- What’s in the BC
  - Data in the BC.
  - Rules, processes, actors, lifecycles
  - Security, provenance, assurance
  - Compliance
  - Governance – policies, procedures, mechanisms
- What’s around the BC
  - Best practices, terminology and reference architectures
  - Access control – Identity management, authentication
  - Interoperability, interfaces
  - Trusted attribute providers
  - Rules, processes, actors
  - Security, provenance, assurance
  - Governance

Key conclusion

- Many, many uses for block chains but the foundational requirement is block chains for the Internet itself.
- ID fraud is the top enabler of crime. Must involve law enforcement.
- Takedown Avalanche network in Dec 2016 – 400k domains
- Validate companies for each domain
  - Identify fraudulent companies
  - Identify shortcomings in the registration process
- Validate remaining 280m domains
- Future registration for any domain name should have a trust rating (e.g. LoA1-4), based on the LoA of the company
- [same could apply to gov organisations, persons & devices]
- All transaction results could be on a block chain for each TLD & ROLO

- Conversely, consider countries with national eID and national federated/hierarchical PKI systems.