
ITU

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

A Security Perspective on Blockchain Use Cases @ Swisscom

David Watrin
Head of Security and Intelligence, Swisscom & David.Watrin@swisscom.com

Geneva, Switzerland, 21 March 2017

An adventure starting 2 years ago…

- Creation of a squad spanning across many organizations and functions
- Gathering hands-on experience with partners trying to address real life issues (e.g. eVoting)
- Moving away from the exploration phase to the operational/commercial one

Security is not the primary driver behind our activities

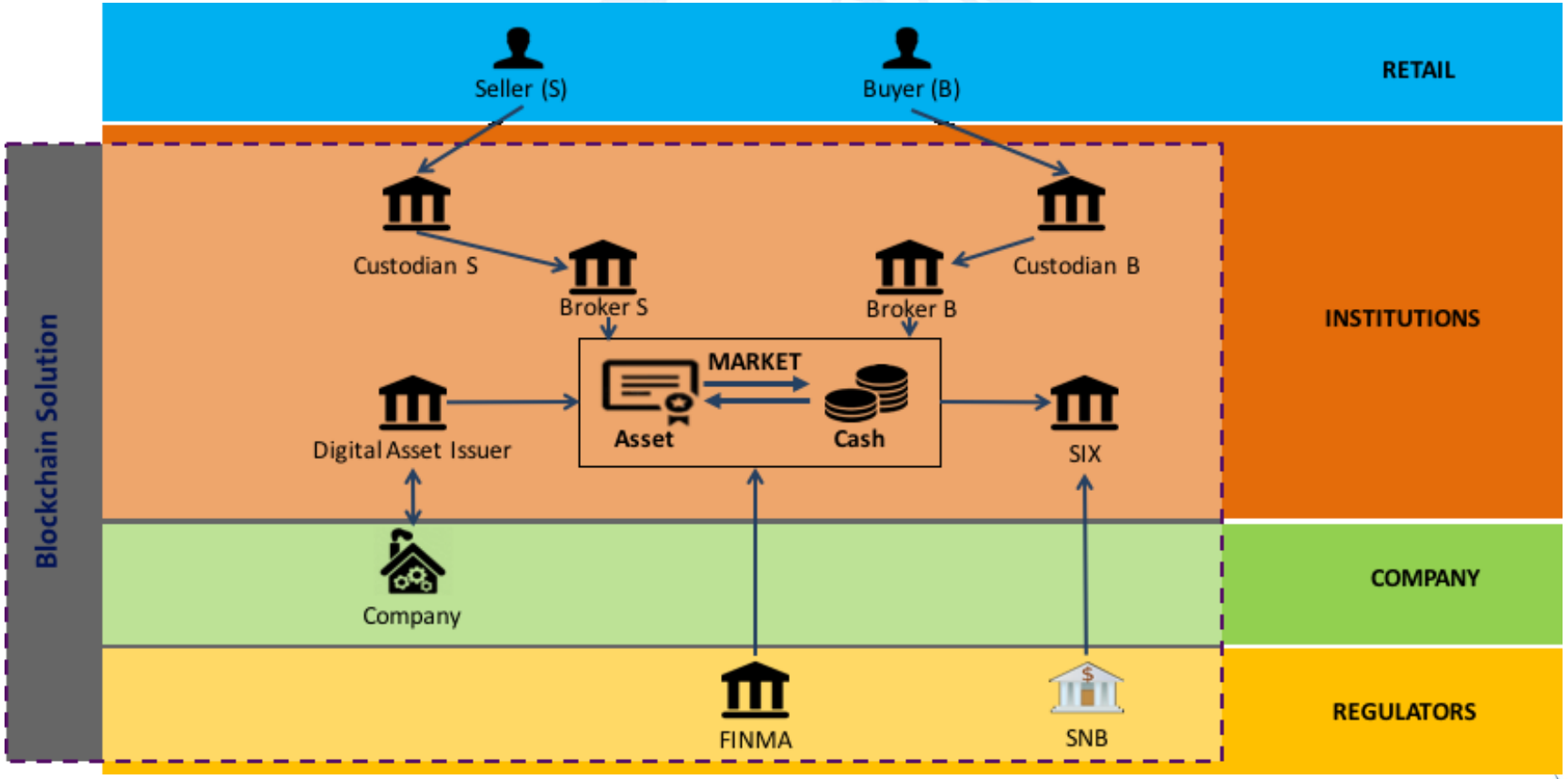
- The technology is complex but it allows simplifying the business ecosystem
- The main drivers are cost savings and new business proposals in key verticals (e.g. Finance)
- However Security engineers are in the driver seat

Use Case: Loyalty platform

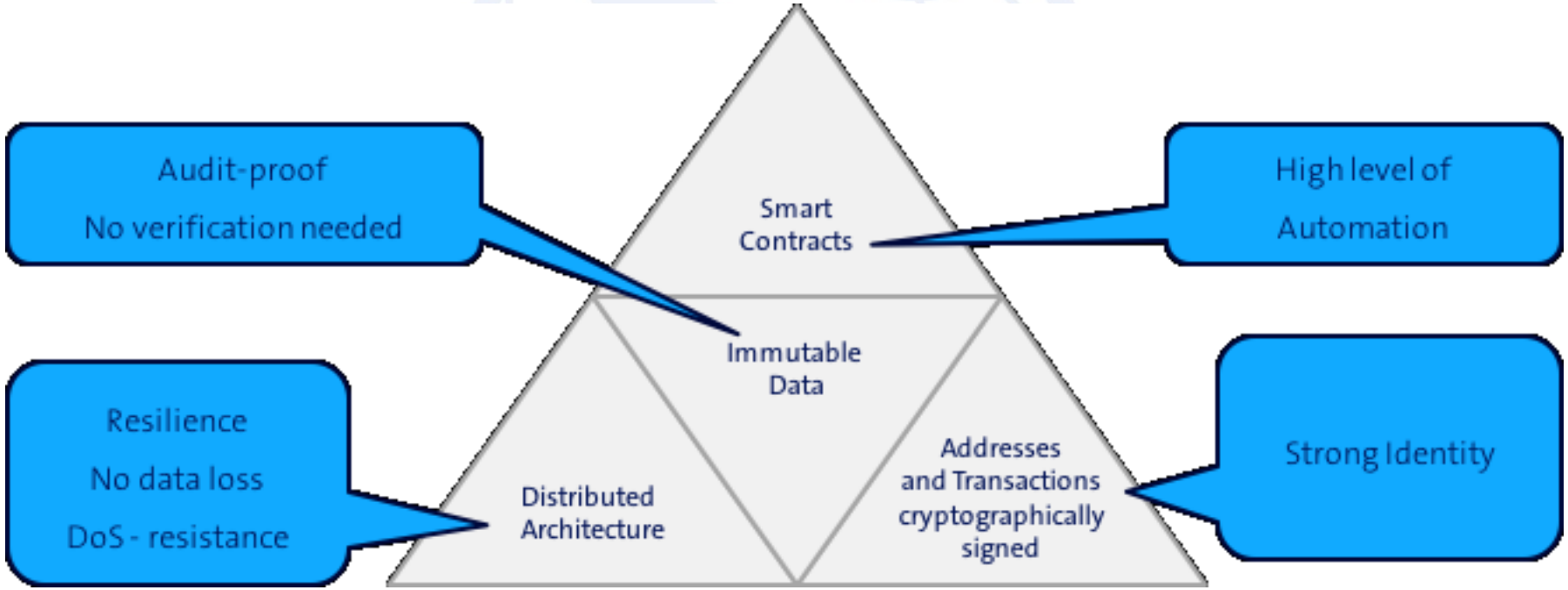
Identity & redemption process

- Low compliance requirements
- Test how to securely manage digital money
  - Age verification (zero knowledge proof)
  - Redemption (escrow contracts)

Use Case: Over the Counter transactions

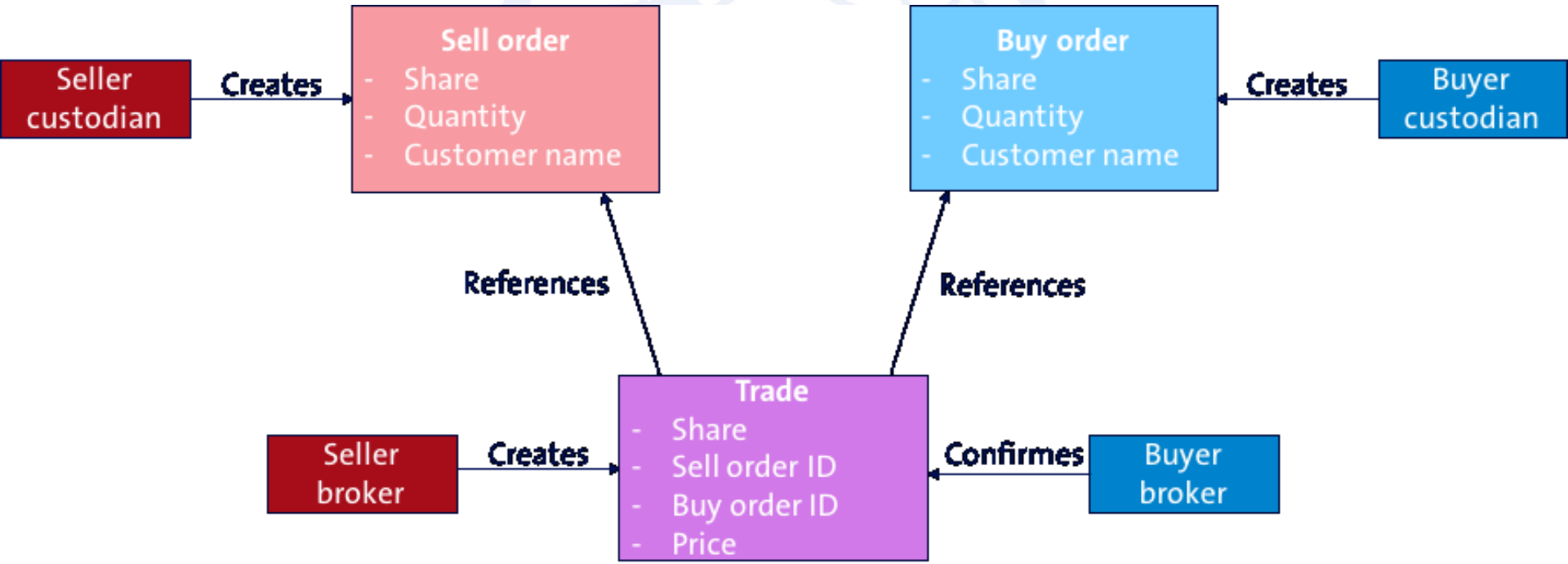


Over the Counter
Blockchain benefits



Over the counter

Data Model



Over the counter

Privacy models

	Sell order customer	Buy order customer	Sell order data	Buy order data	Trade data
Seller custodian	Visible	Hidden	Visible	Hidden	Visible
Buyer custodian	Hidden	Visible	Hidden	Visible	Visible
Other custodians	Hidden	Hidden	Hidden	Hidden	Hidden
Seller broker	Hidden	Hidden	Visible	Hidden	Visible
Buyer broker	Hidden	Hidden	Hidden	Visible	Visible
Other brokers	Hidden	Hidden	Hidden	Hidden	Hidden
Regulator	Visible	Visible	Visible	Visible	Visible
Share registrar	Visible	Visible	Visible	Visible	Visible
Payment services	Hidden	Hidden	Visible	Visible	Visible

Over the Counter

Trade-offs

- Smart contracts are good for **decentralized data processing**
- Data stored in blockchain are **public** to all participants
- Encrypting data **reduces** smart contract abilities to process the data

Over the counter

Our Solution

Privacy	Decentralization
* The data is encrypted and visible to participants according to the privacy model * Smart contracts **do not know the content** of the order or trade * Smart contracts **know the participants** of the order/trade (Custodians, brokers, share registrar and regulator)	* Smart contracts **control the lifecycle**: - Order states: pending, processing, filled - Trade states: open, confirmed, paid * Smart contracts **enforce** who can **change** the order/trade states

Over the counter

New Alternative with Hyperledger Fabric

- **Reduced complexity** of the solution
  - Key management and identity is **handled by the Fabric**
  - Fabric provides **CFSSL-based CA**
- Privacy is achieved through **the channel mechanism**
  - **No self-designed** cryptography solutions

HYPERLEDGER

Some Use Cases under assessments

- Bridging IoT silos
- Checking possible certificate revocation
- Supporting number portability process
- …

Conclusions and Recommendations

- Inherent blockchain properties such as transparency & immutability are strengthening business logics while simplifying business processes
- They enable new business models however these models need to have robust IPR agreements