r3.

FSG workshop

Introduction: R3

*Prepared by R3 for Asian Development Bank*

28 April 2017

About R3

The R3 consortium is the world's largest alliance committed to delivering the next generation of financial infrastructure based on distributed ledger technology (DLT)

R3's mission is to redefine the foundations of finance by harnessing the power of collaborative networks

About R3

- **London**
- **New York**
- **Singapore**
- Washington DC
- San Francisco
- Switzerland
- Seoul
- Sydney
- Taipei
- Tokyo
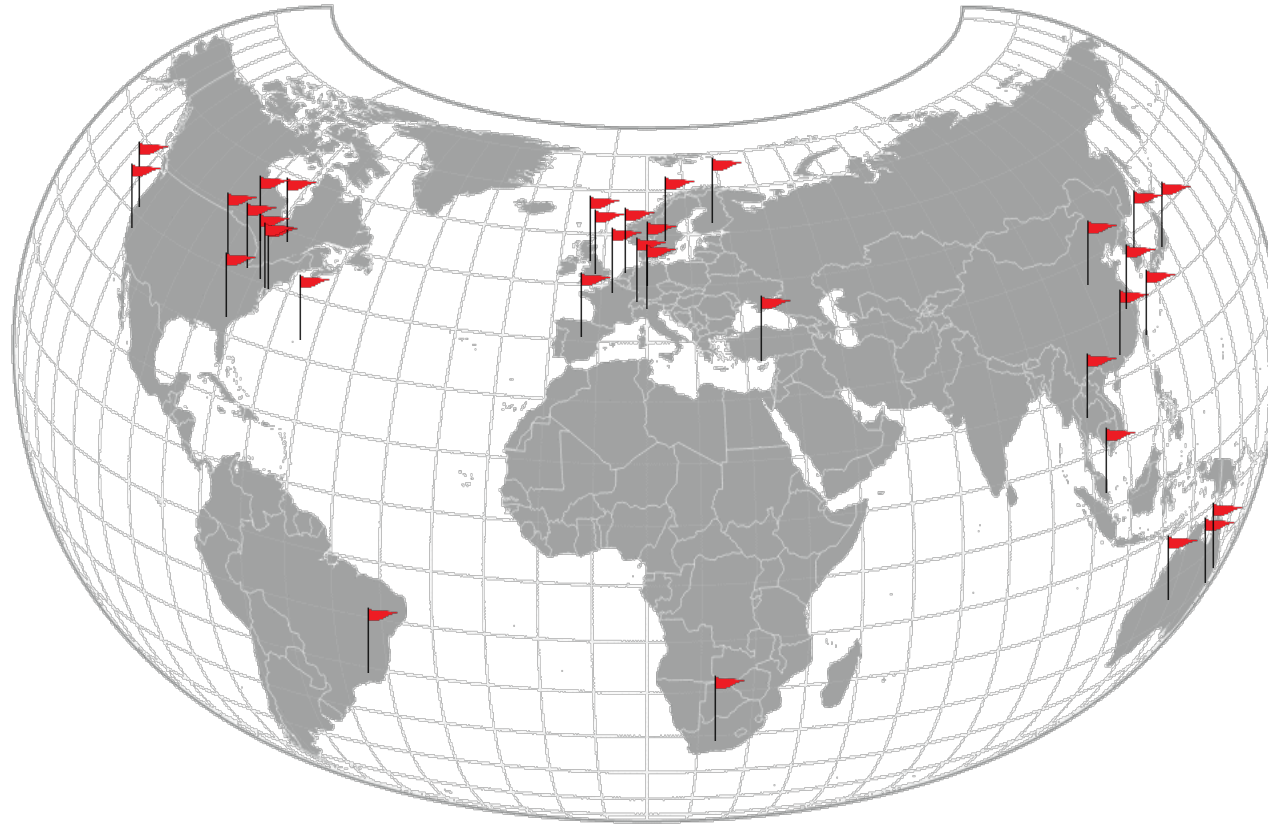
Members

1,100+ collaborators

from 75+ members

from 20+ countries

Supported by 110+ staff

Deploy DLT to redefine how technology supports financial services

The worlds largest DLT financial centre of excellence harnessing the power of collaborative networks

CORDA

Lab and Research

CorDapps

Partner

Top of stack technology

An eco-system of pre-selected certified partners, driving cost effective vendor engagements

Agenda

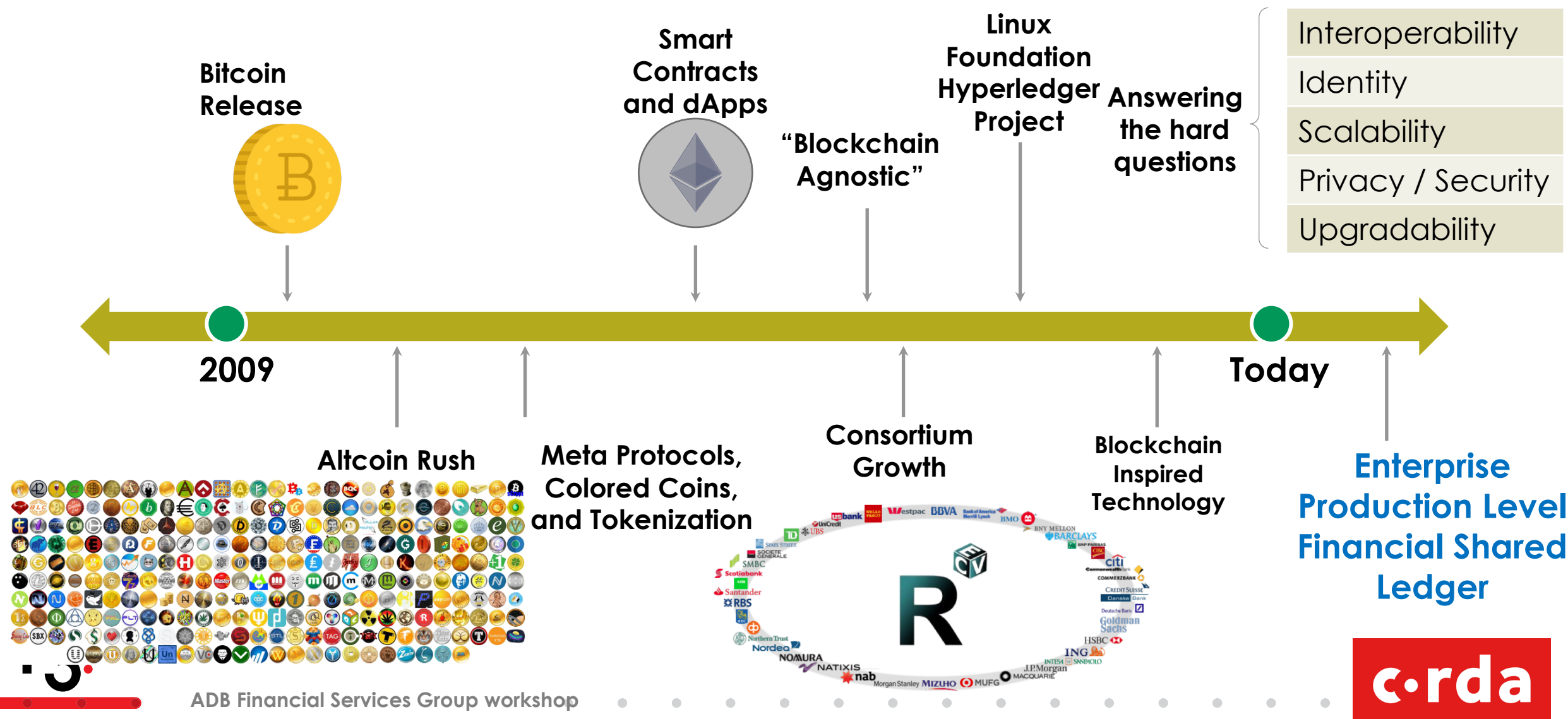- Gentle introduction to bitcoin

- Live demo: Bitcoin transactions

- Why blockchains are appropriate for cryptocurrencies... but not for industry

- What is meant by "distributed ledgers?"

Evolution from blockchains to industry distributed ledgers

Bitcoin Release

Smart Contracts and dApps

"Blockchain Agnostic"

Linux Foundation Hyperledger Project

Answering the hard questions

Interoperability
Identity
Scalability
Privacy / Security
Upgradability

2009

Today

Altcoin Rush

Meta Protocols, Colored Coins, and Tokenization

Consortium Growth

Blockchain Inspired Technology

Enterprise Production Level Financial Shared Ledger

In the beginning…

Cryptocurrency

Proof-of-work

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing

Blockchain

Mining

Why is Bitcoin's ledger called a blockchain?

Source: www.bitsonblocks.net

What problem are we trying to solve?

Problem statements			
	Bitcoin and Cryptocurrencies		**Industry Workflow Tools**
Purpose	A purely peer-to-peer version of electronic cash [which] would allow online payments to be sent directly from one party to another **without going through a financial institution**.	← →	Maintain and improve on successful competitive position by keeping customers happy, **increasing revenues, reducing costs, becoming more efficient**.
Problem statement	How do we use technology to create a financially inclusive system that anyone can participate in?	← →	How do we use technology to add shareholder value?
Solution	Open, decentralised payment networks	← →	Private data-sharing networks
Innovation	Disruptive	← →	Efficiency

Source: www.bitsonblocks.net
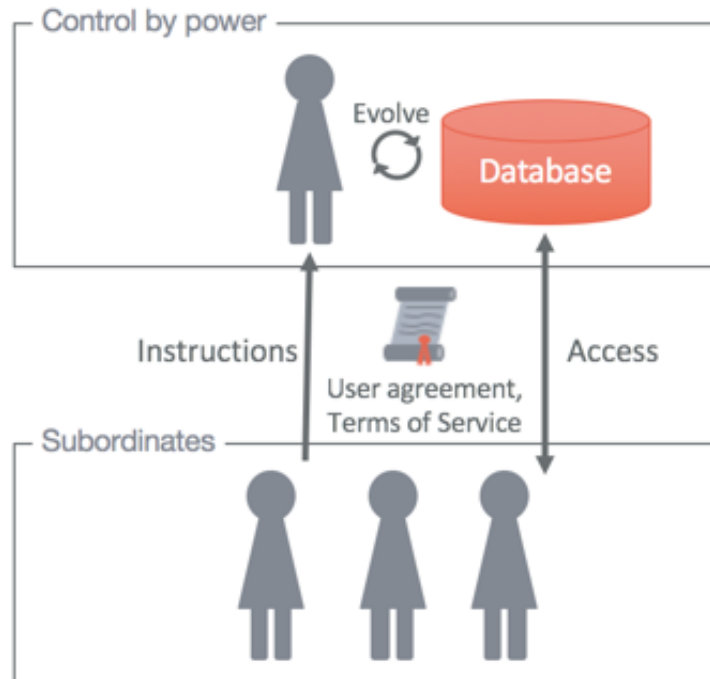
ADB Financial Services Group workshop

FSG workshop

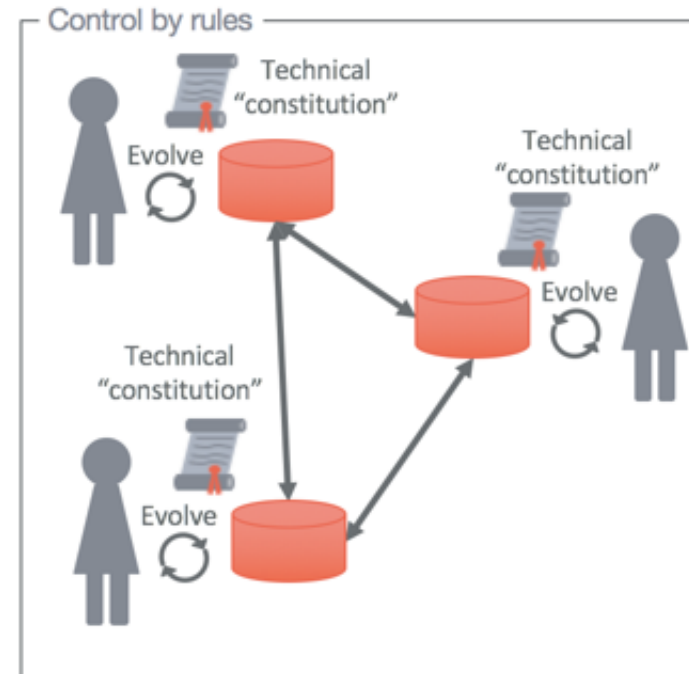## Part 2: Distributed Ledgers

Agenda

- What is the value of distributed ledgers?
- Video: Corda by R3's CTO Richard Brown
- Critical design decisions recap
- Hands-on: demo of R3 Corda

What's new? The <u>shared control </u>of validated data

With a traditional model, data evolves when the controlling authority evolves it, perhaps on instruction from subordinates. The authority has ultimate control over the data.
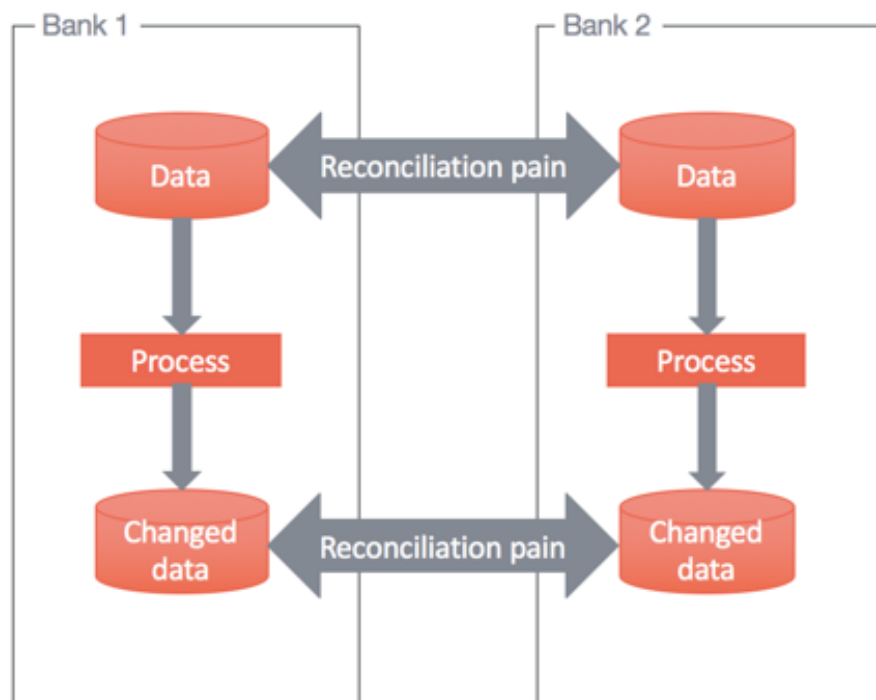
With a distributed ledger model, data evolves subject to predetermined rules, enforced by participants. Consensus between participants is important.
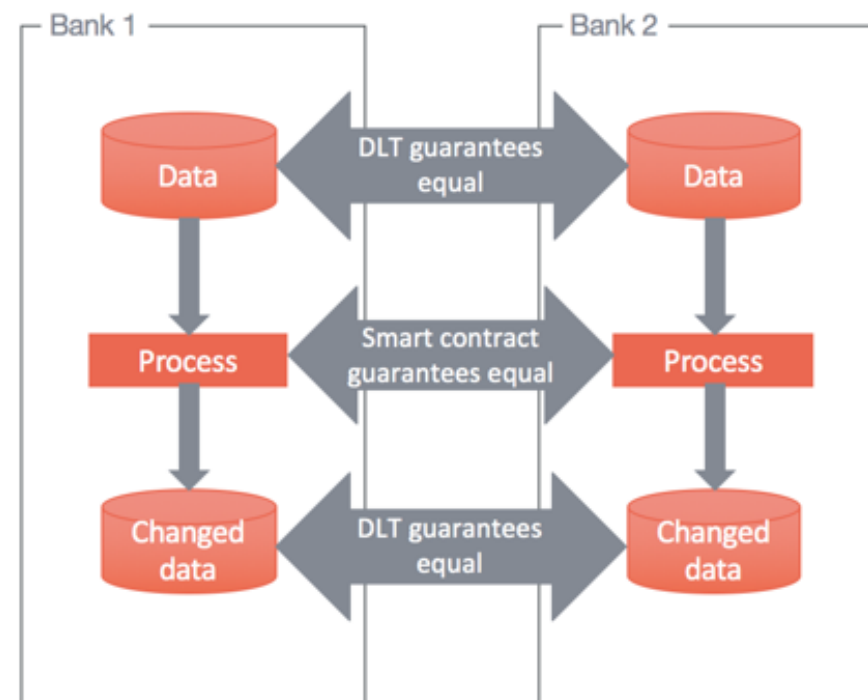
Source: www.bitsonblocks.net

The significant evolutionary step of DLT
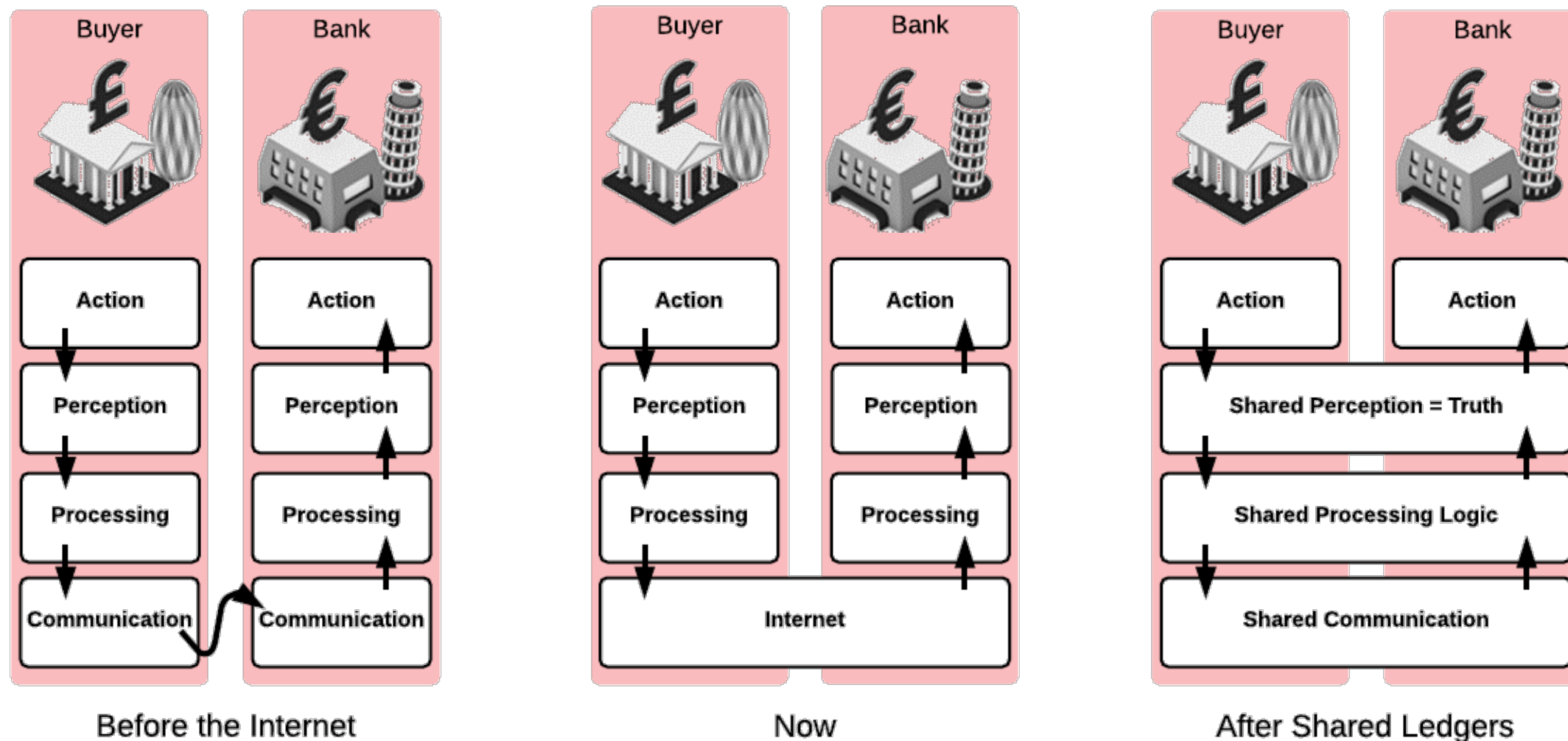
To put it another way

Independent ledgers...

With distributed ledgers and smart contracts...

"What I see is what you see, and we agree"

Distributed Ledgers at a Glance

Ledgers

Distributed Ledgers

Blockchains

Non-blockchains

Crypto-currencies

Industry ledgers
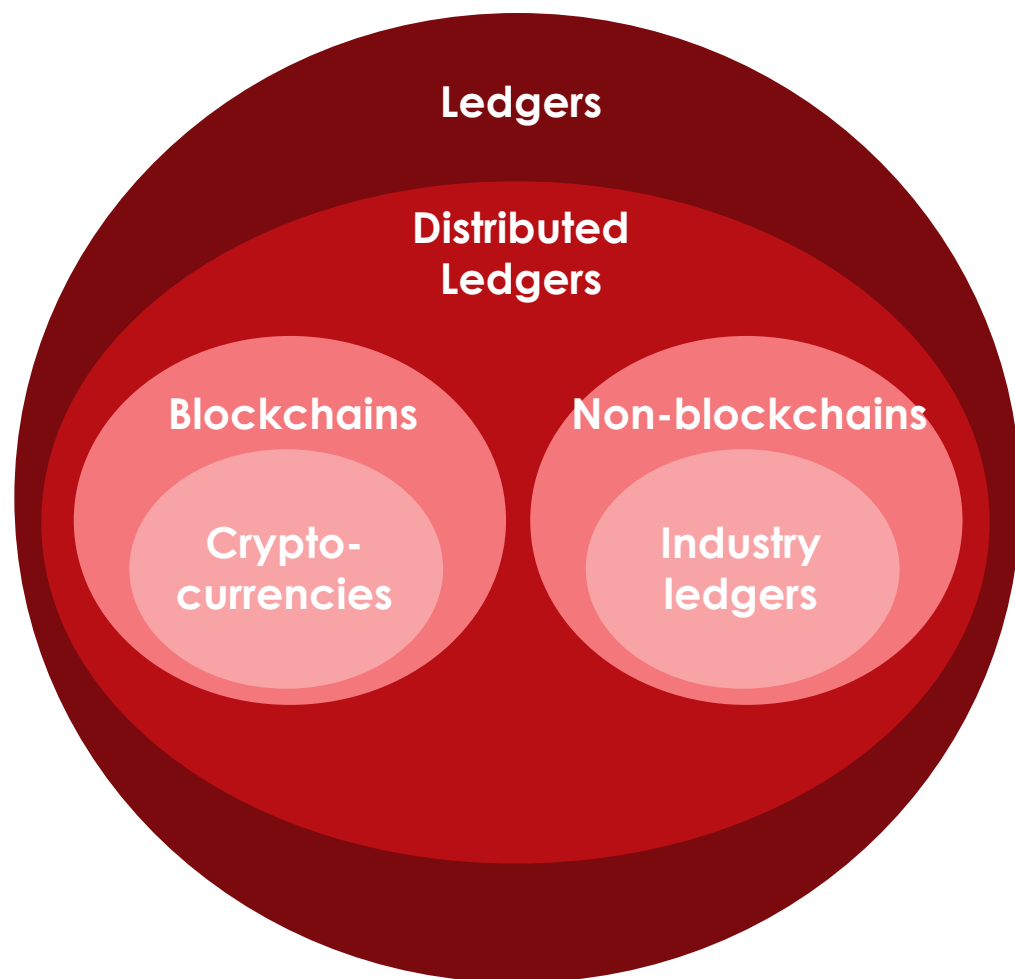
Non-repudiation & immutability with provable data integrity and audit trail

Automation of business logic when certain criteria are met ("smart contracts")

Cryptography to ensure identity authentication for each transaction

Distributed consensus to ensure the state of the ledger represents the agreed-upon truth of all stakeholders

Shared ledger so each participant sees the same view of the same data, updated in real time, subject to permissioning

r3.

corda

Don't share all data with all parties!

Broadcast Blockchain

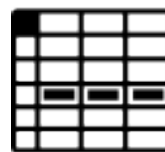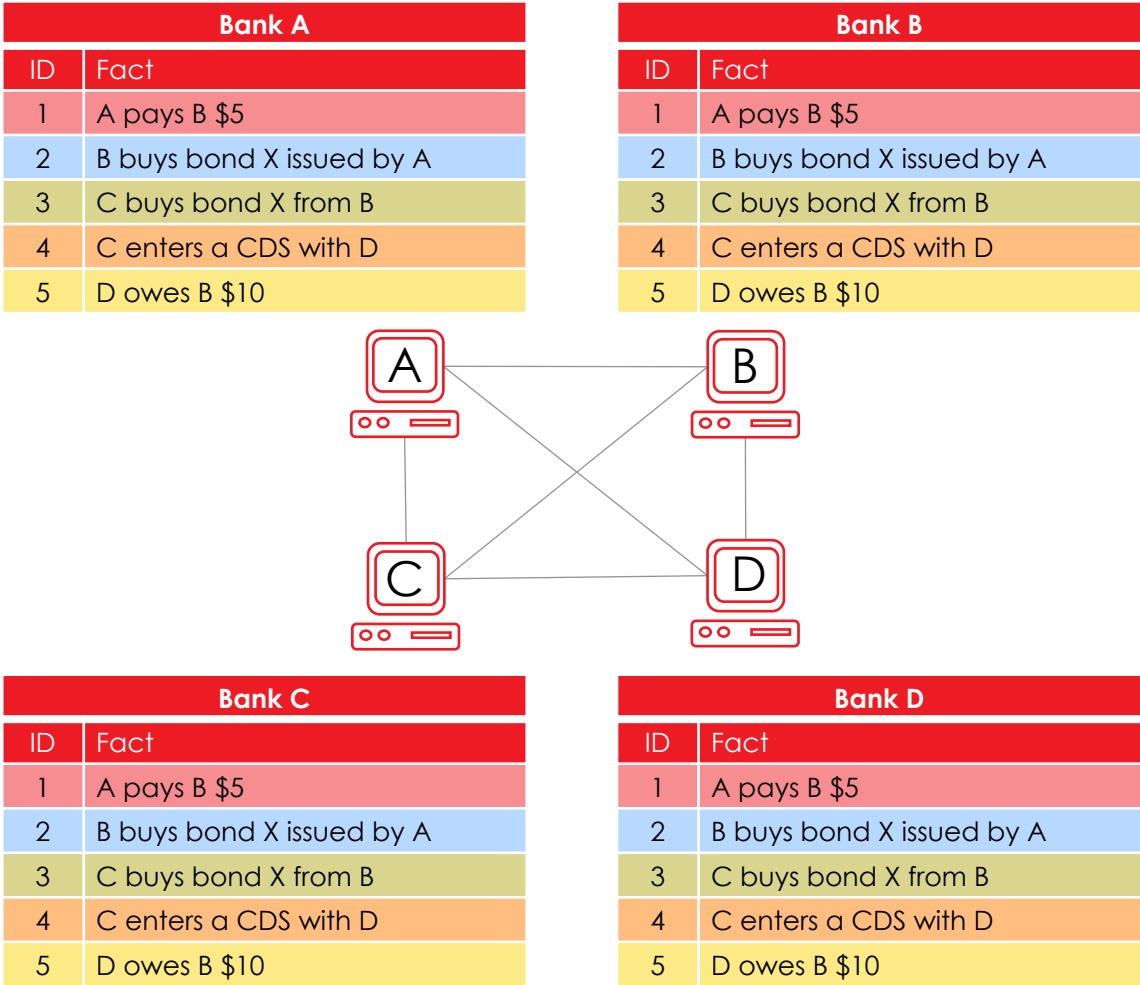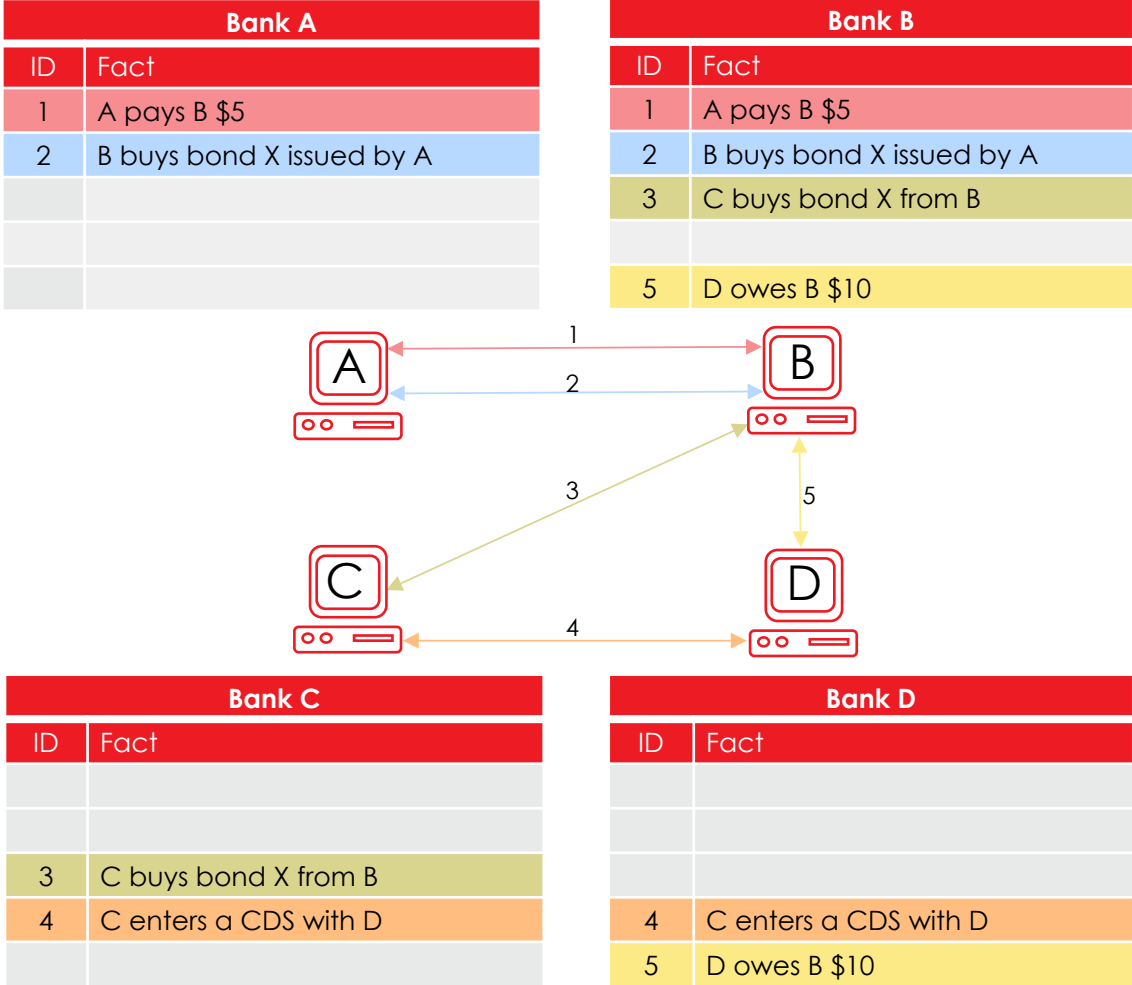| Bank A	
ID	Fact
1	A pays B $5
2	B buys bond X issued by A
3	C buys bond X from B
4	C enters a CDS with D
5	D owes B $10

Bank B	
ID	Fact
1	A pays B $5
2	B buys bond X issued by A
3	C buys bond X from B
4	C enters a CDS with D
5	D owes B $10

Bank C	
ID	Fact
1	A pays B $5
2	B buys bond X issued by A
3	C buys bond X from B
4	C enters a CDS with D
5	D owes B $10

Bank D	
ID	Fact
1	A pays B $5
2	B buys bond X issued by A
3	C buys bond X from B
4	C enters a CDS with D
5	D owes B $10

Corda DLT

Bank A	
ID	Fact
1	A pays B $5
2	B buys bond X issued by A

Bank B	
ID	Fact
1	A pays B $5
2	B buys bond X issued by A
3	C buys bond X from B
5	D owes B $10

Bank C	
ID	Fact
3	C buys bond X from B
4	C enters a CDS with D

Bank D	
ID	Fact
4	C enters a CDS with D
5	D owes B $10

Introducing Corda

Corda is a **distributed ledger platform** designed and built from the ground up to **record**, **manage** and **synchronise** agreements (legal contracts), designed for use by **regulated financial institutions**

What does Corda do which has never been done before?

- Confirm-as-you-go, not confirm-after-recording/calculating

- Mutual control over the evolution of that data

- Data changes conform to pre-agreed business logic

- Visibility into asset lineage and the inability to double spend

Corda by Richard Gendal Brown, CTO R3

- https://vimeo.com/193580475

Corda network – participants and roles
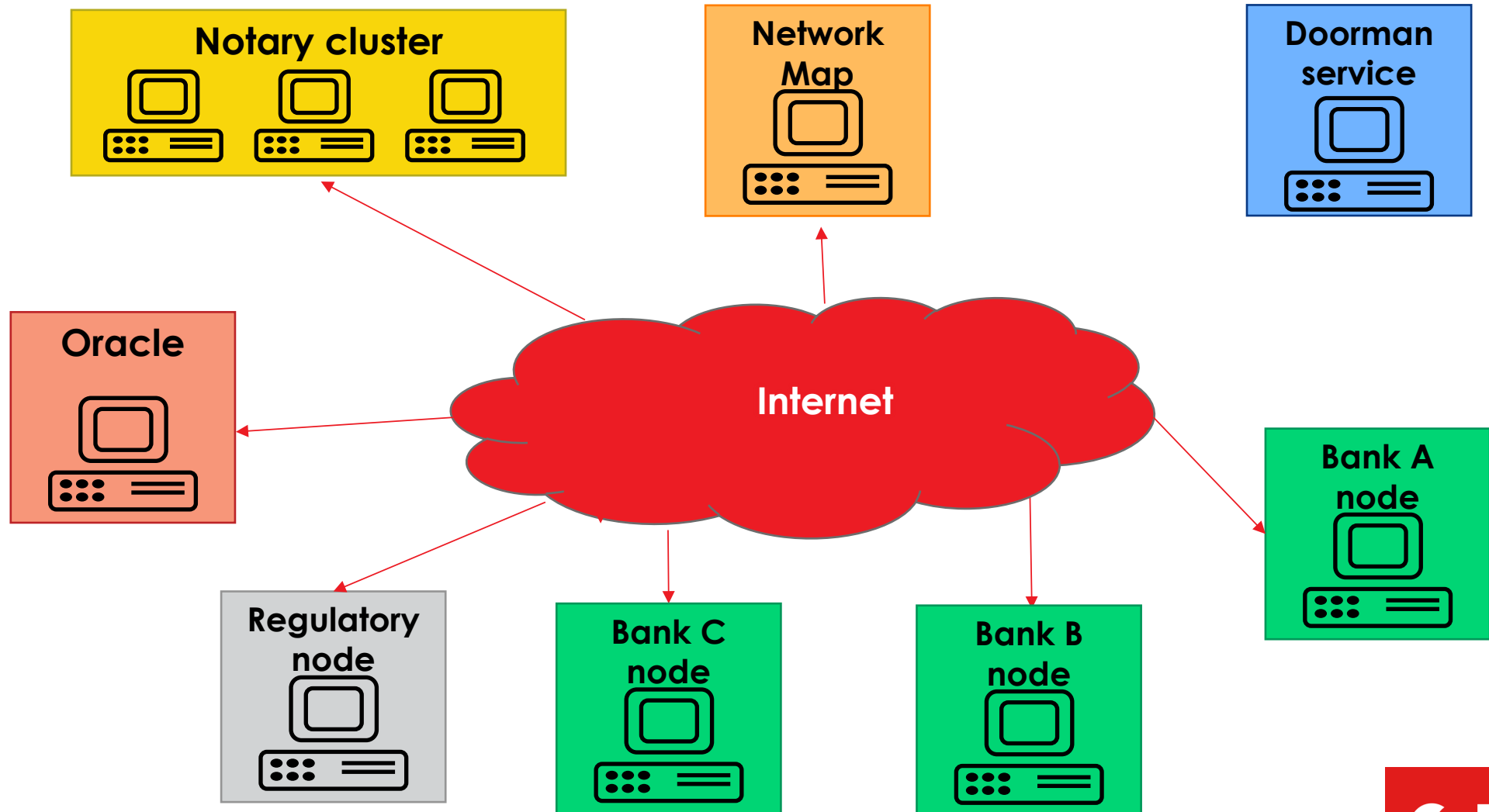
A unique shared ledger approach

Blockchain-inspired: takes best attributes from Bitcoin, Ethereum, and others.

Consensus: achieved at individual deal level, rather than system level. Supports a variety of consensus mechanisms.

Enterprise grade: built specifically for financial markets.

Regulator-focused: design directly enables regulatory/supervisor observer nodes.

Data privacy: transactions info propagated only to relevant nodes.

Smart contract: strong link between legal prose and smart contract code.

Easy integration: reuse existing developer skills and make integration with bank systems easy and safe. Query and join the ledger to existing DBs with SQL, and code contracts in modern, standard languages like Java.

FSG workshop

Part 3: Illustrative Financial Service Use Cases

When is DLT useful?

Control — the need to control data, IT assets or processes within organizational/national boundaries impedes your ability to adopt centralized 3rd party solutions

Risk — existing business/tech/operational controls are ineffective in preventing fraud and forgery

Complexity — trusted third parties add time, cost, complexity or risk

Data Visibility — timely data is often unavailable within and across organization boundaries

Cost — multiple parties running non-differentiating functions or processes that drive business/tech costs higher across the industry

Standard-ization — lack of technical standards prevent straight-through-processing and may lead to vendor lock-in
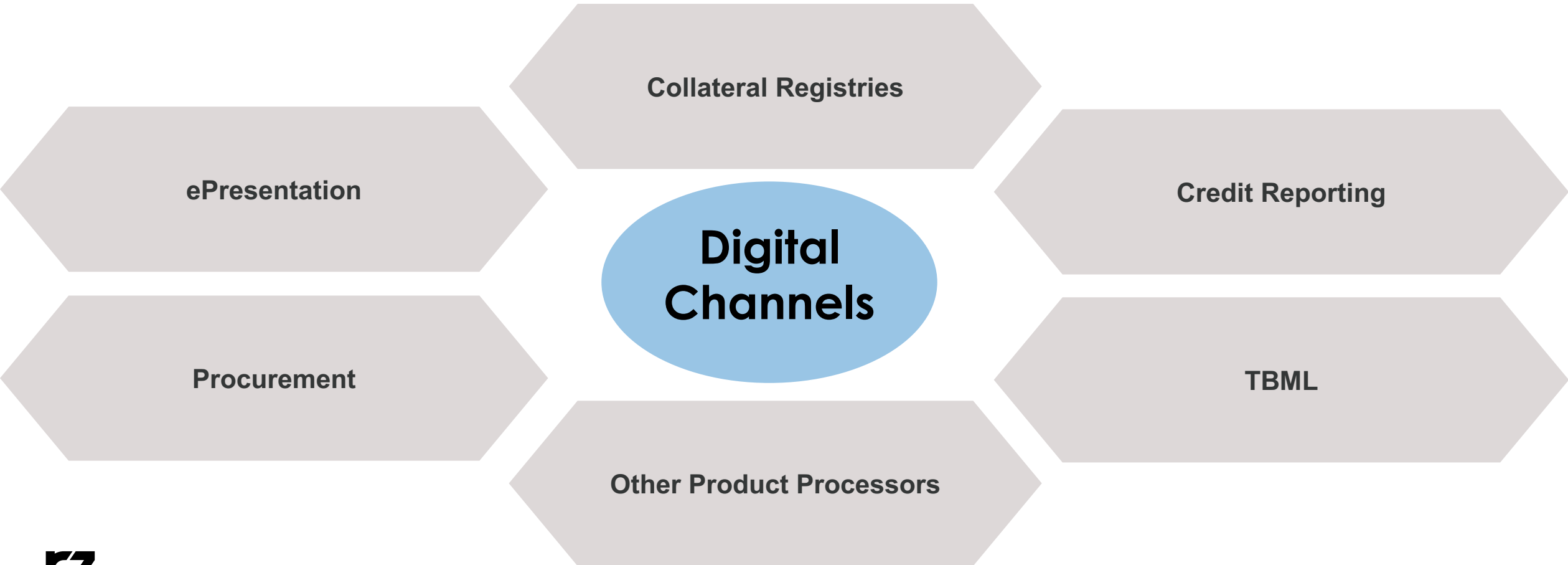
Legal — existing solutions and processes have created legal uncertainty pertaining to the title to assets or the finality of a transaction

FSG workshop

Part 3.1 : Trade Finance

Trade Finance – Areas of Focus

Collateral Registries

ePresentation

Credit Reporting

Digital Channels
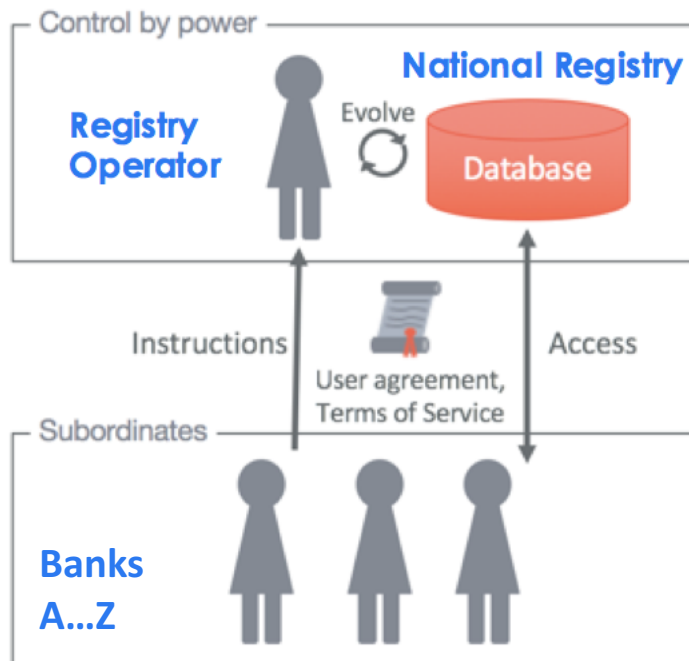
Procurement

TBML

Other Product Processors

FSG workshop

Part 3.2 : Collateral Registries

Land & Mortgage Note Registry - Challenges

- The national housing finance market is **error-prone, paper-based and costly.**

- **Lack of visibility** w.r.t. borrowers concerning the person who may collect, enforce or modify residential mortgage notes.

- **Legal uncertainty** for the transferability and enforceability of mortgage notes.

- **Inconsistent standards**, particularly w.r.t. recordkeeping practices that have resulted in to enforce a mortgage and mortgage notes.

- Potential for **fraud, forgery or alteration** of mortgage notes.

Centralized Registry (1/2)

Control by power

Registry Operator

National Registry

Evolve

Database

Instructions

Access

User agreement, Terms of Service

Subordinates

Banks A...Z

With a traditional model, data evolves when the controlling authority evolves it, perhaps on instruction from subordinates. The authority has ultimate control over the data.

Control

Risk

Complexity

Data Visibility
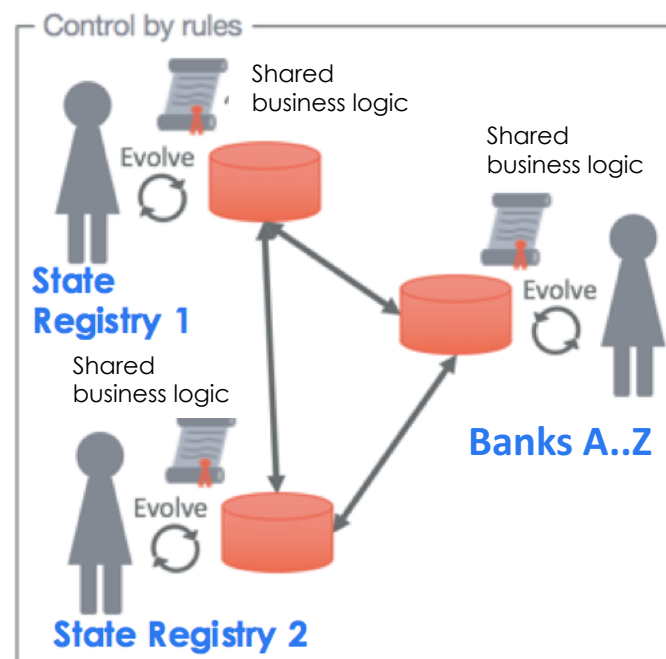
Registry – Distributed Ledger Based (2/2)

Shared control and validation of data.

Control

Risk

Data Visibility

Complexity

Control by rules

Shared business logic

Shared business logic

Evolve

State Registry 1

Shared business logic

Evolve

Banks A..Z

Evolve

State Registry 2

With a distributed ledger model, data evolves subject to predetermined rules, enforced by participants. Consensus between participants is important.

Note: not all countries will benefit from a distributed ledger! This varies on a case-by-case basis.

ADB Financial Services Group workshop

FSG workshop

Part 3.3 : Digital Identity & KYC Utilities

Importance of Digital Identity

Digital identity is a critical enabler of activity inside Financial Services broadly (e.g. LEI)

Operational decisions

Regulatory compliance

Customer experience & product delivery

The relevance of digital identity stretches beyond Financial Services
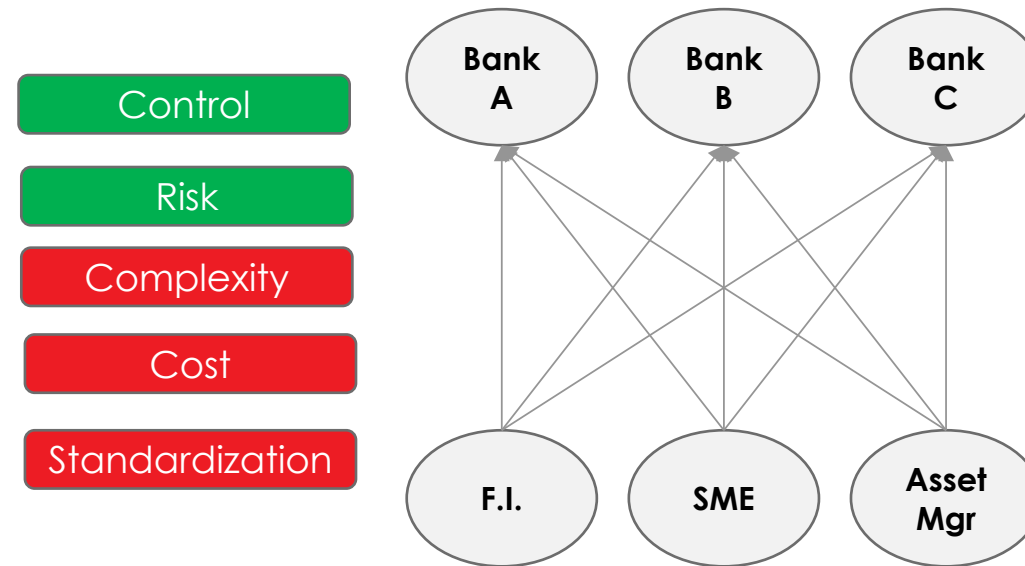
Public transactions

Private transactions

- Access to social assistance
- Access to education
- Access to healthcare
- Access to civic structures (e.g., voting)
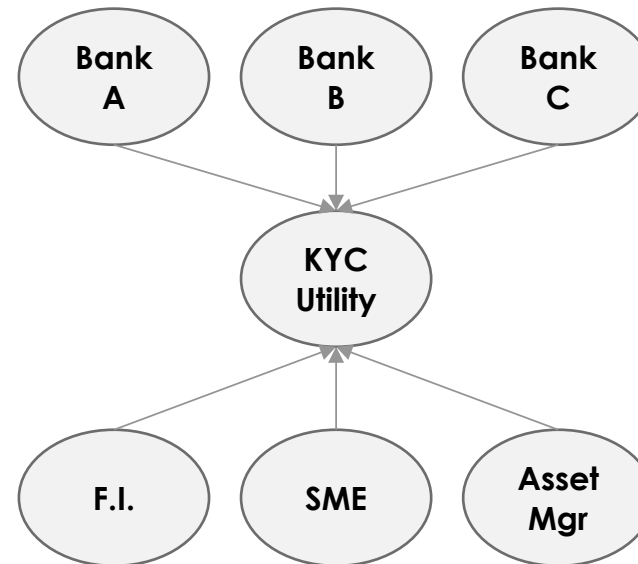
- Merchant transactions
- Large private provider transactions (e.g. renting an apartment, buying a car)

Source: WEF report

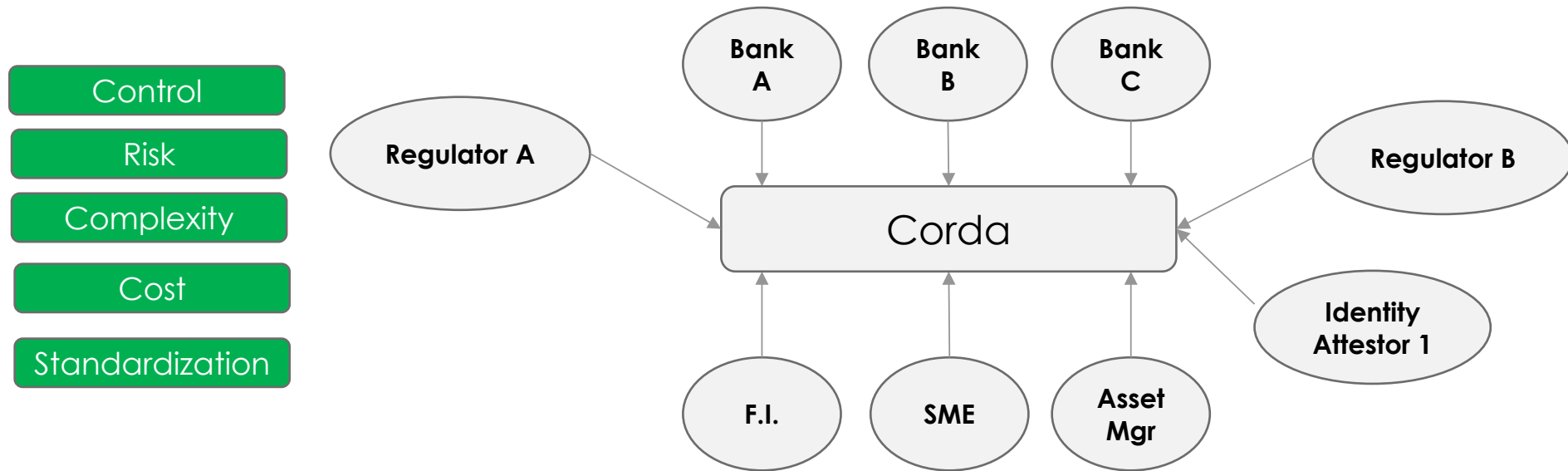ADB Financial Services Group workshop

r3.

c•rda

KYC – Model 1: Bank Centric Customer Onboarding

KYC – Model 2: KYC Utility (Centralized)

Control

Risk

Complexity

Cost

Standardization

Bank A

Bank B

Bank C

KYC Utility

F.I.

SME

Asset Mgr

KYC – Model 3 – Self-sovereign Identity (DLT-based)

Control

Risk

Complexity

Cost

Standardization

Regulator A

Bank A

Bank B

Bank C

Corda

Regulator B

Identity Attestor 1

F.I.

SME

Asset Mgr

Note: this assessment applies to Corda only. Blockchains will have a different assessment, in part, because they replicate data to all parties.

Summary

- Bitcoin, blockchain and distributed ledgers are different

- Corda was uniquely designed to cater to the need for the financial services industry

- Not everything needs a distributed ledger. Criteria must be applied to each use case being examined

- Payments

- Trade Finance

- KYC

FSG workshop

Prepared by R3 for Asian Development Bank

28 April 2017