



Imperial College
London

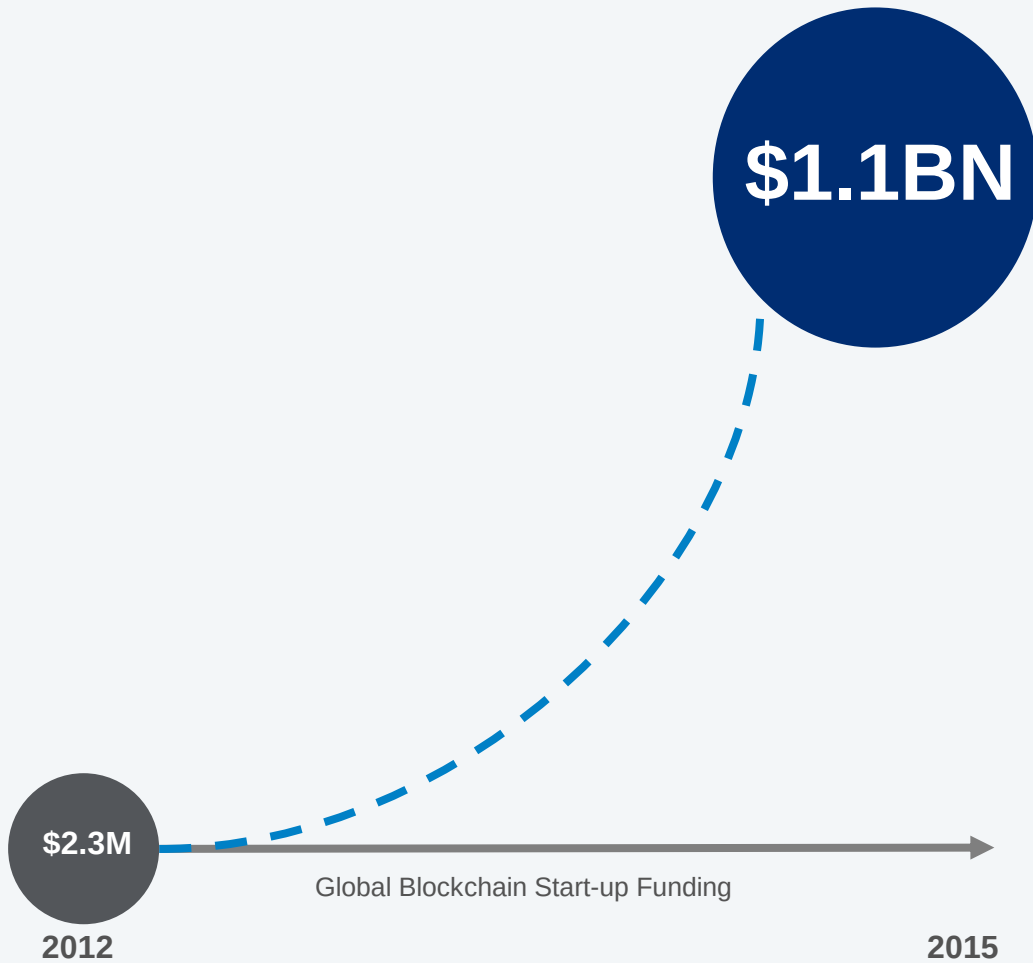
Blockchain & Digital Transformation

Dr Catherine Mulligan
Research Fellow
Co-Director, Centre for Cryptocurrency Research and Engineering
Director, Contextualised

@API_Economics

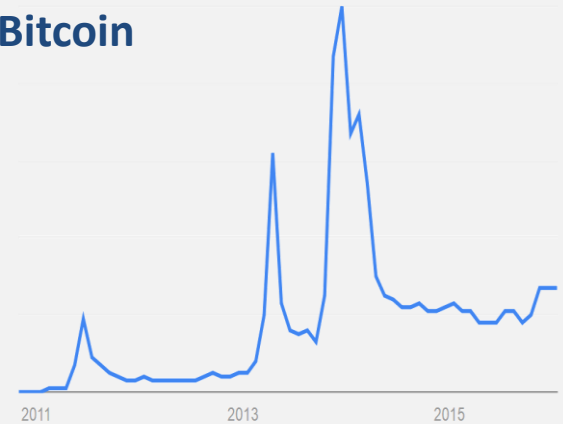
Growing interest in Blockchain

VENTURE CAPITAL ACTIVITY IN BLOCKCHAIN

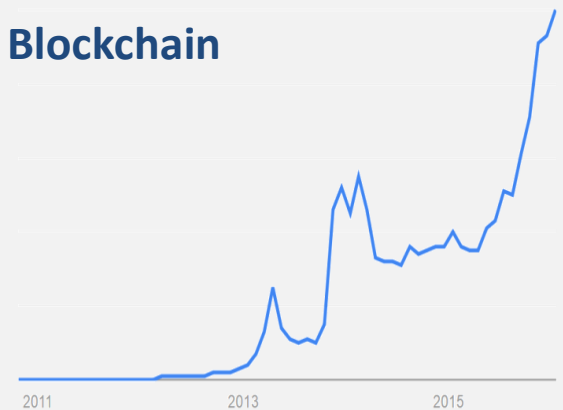


GOOGLE SEARCHES

Bitcoin



Blockchain



Digital Disruption and blockchain – the wave is cresting

Smart contracts

Decentralised asset
ownership and
management

Identity management

Decentralised Autonomous
Corporations

Peer-to-peer
commerce and
finance

New insurance paradigms

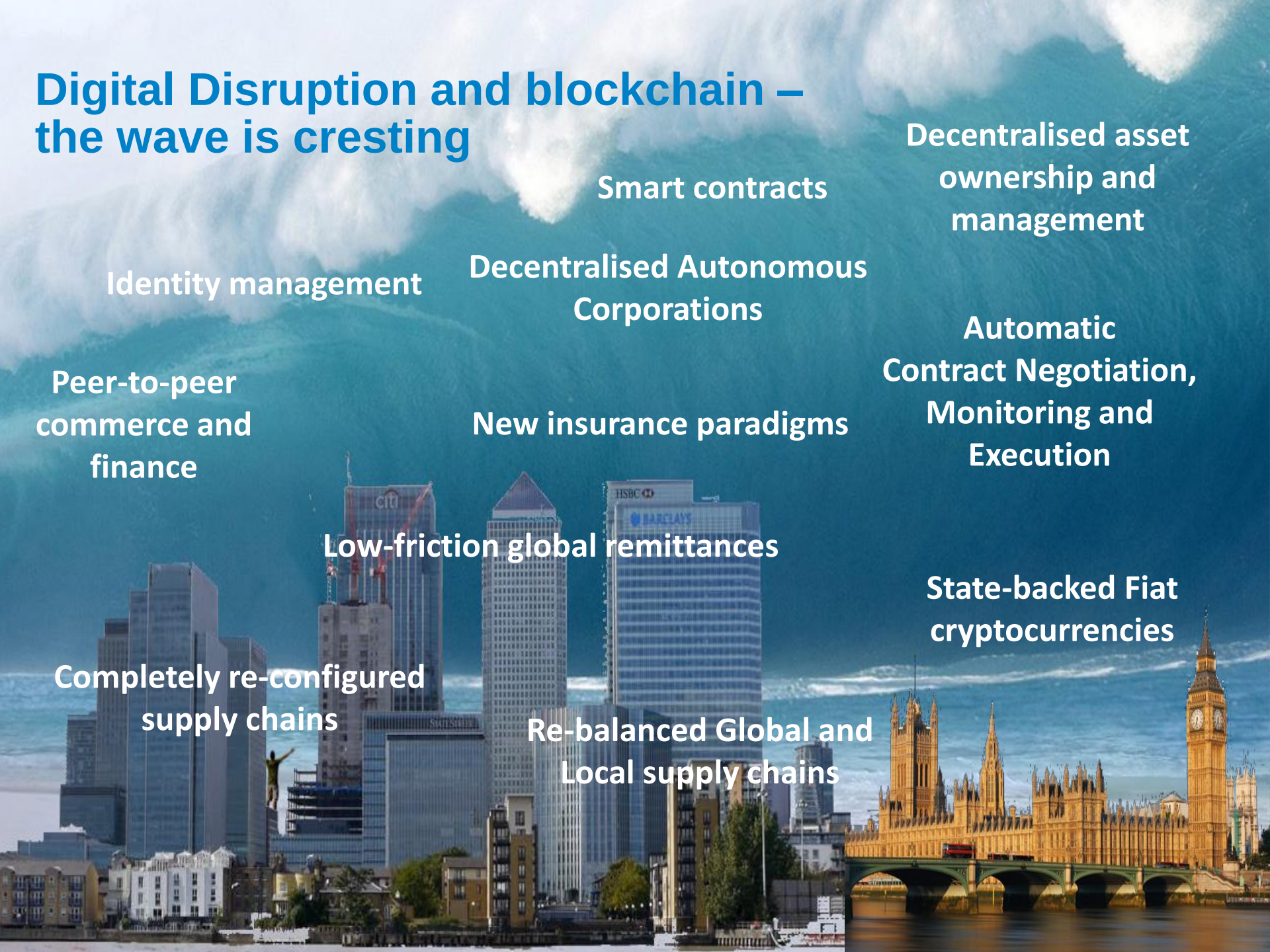
Automatic
Contract Negotiation,
Monitoring and
Execution

Low-friction global remittances

State-backed Fiat
cryptocurrencies

Completely re-configured
supply chains

Re-balanced Global and
Local supply chains



What is a Blockchain?

A Blockchain allows untrusting parties with common interests to co-create a **permanent, unchangeable and transparent record** of exchange and processing **without relying on a central authority.**

N.B: The terms “blockchain” and “distributed ledger” are often used interchangeably

1 - Consensus



Prevents “double spend” or validation of fraudulent transactions through:

- **Proof of work:** miners compete to validate blocks by solving highly processor / RAM intensive cryptographic problems for rewards
- **Distributed Consensus:** majority validation by trusted subnetworks of peer nodes within the network.
- **Proof of Stake:** achieves distributed consensus by network users proving their ownership of the currency

2 - The Ledger



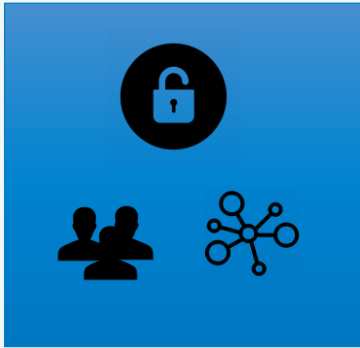
- Often referred to as the “Blockchain”, this is a **public record** of all transactions stored across a **distributed Peer-to-Peer (P2P) network** of servers.
- Verified transactions are added to “blocks” and the history provides proof of value or assets “owned”

3 - Reward

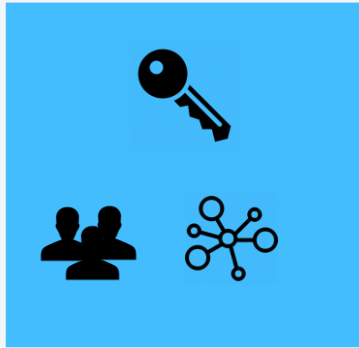


- A medium for transaction settlement within the network that rewards miners.
- Examples include “Bitcoin” – so miners are rewarded for processing transactions and providing a stable network
- Rewards are cryptographically generated and the protocol rules determine issuance and destruction of the rewards
- Rewards are required for public permissionless DLT such as Bitcoin to ensure network security. They are not a necessary part of all DLT

Wide range distributed ledger technologies



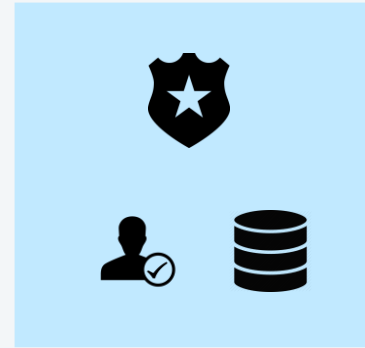
PERMISSIONLESS,
PUBLIC, SHARED
SYSTEMS



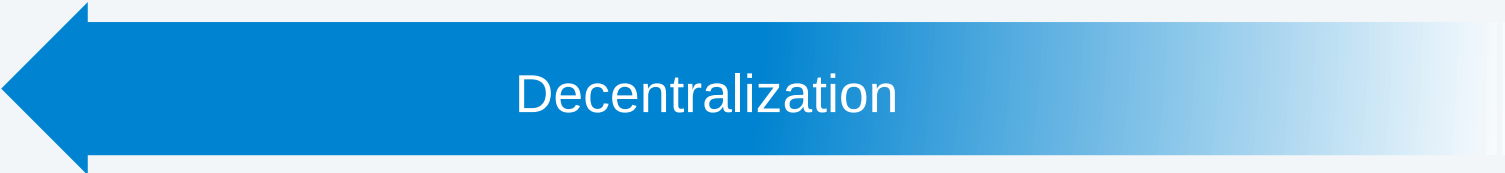
PERMISSIONED,
PUBLIC, SHARED
SYSTEMS



PERMISSIONED,
PRIVATE, SHARED
SYSTEMS



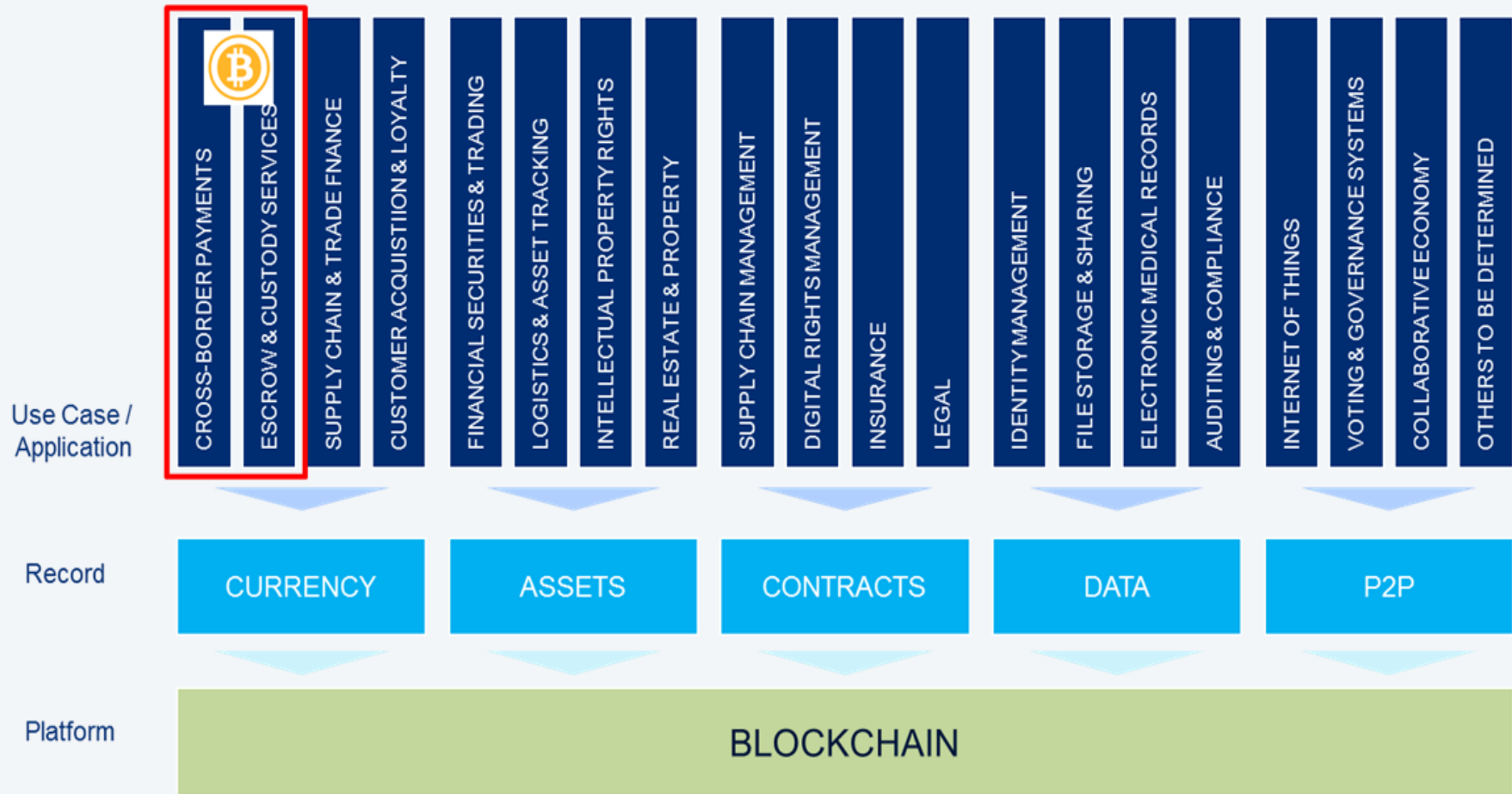
DATABASES



Decentralization

Blockchain is bigger than Bitcoin

DISTRIBUTED LEDGERS ARE PLATFORMS UPON WHICH VARIOUS APPLICATIONS CAN BE BUILT, WELL BEYOND FINANCIAL SERVICES



Source: Citi Ventures

Blockchain 1.0 through 3.0



1.0



2.0



3.0

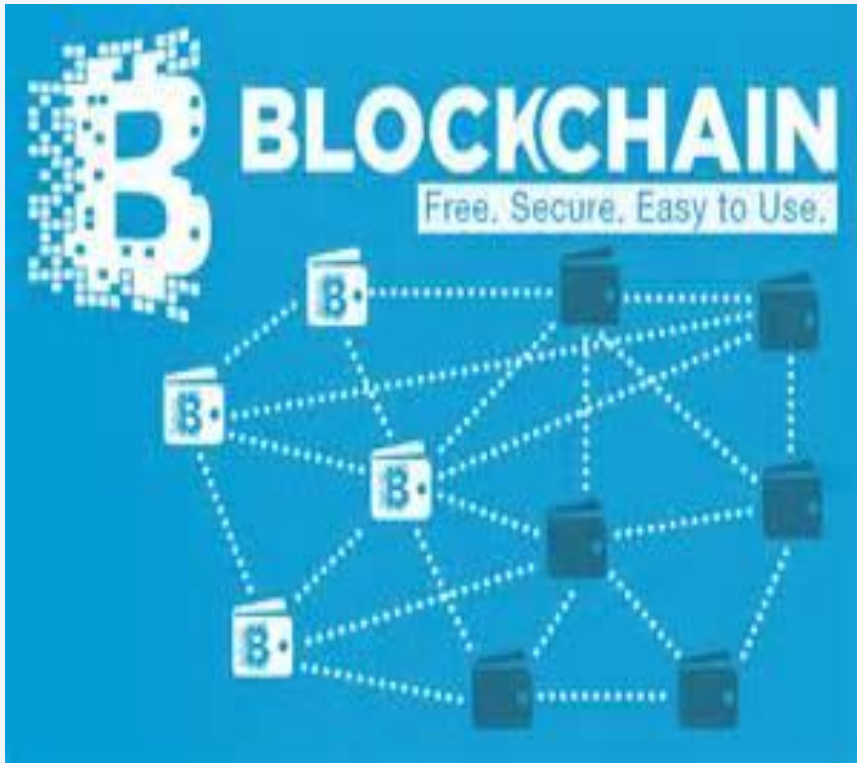
Increasing Decentralisation

Examples

A blue-tinted photograph of a modern glass-walled building. In the foreground, a person is sitting on a row of colorful, rounded outdoor furniture. The building's glass reflects the surrounding environment. The word "Examples" is overlaid in white text on the left side of the image.

Who will own identity?

Business models are **changing dramatically**



Protecting Critical Infrastructure



guardtime 

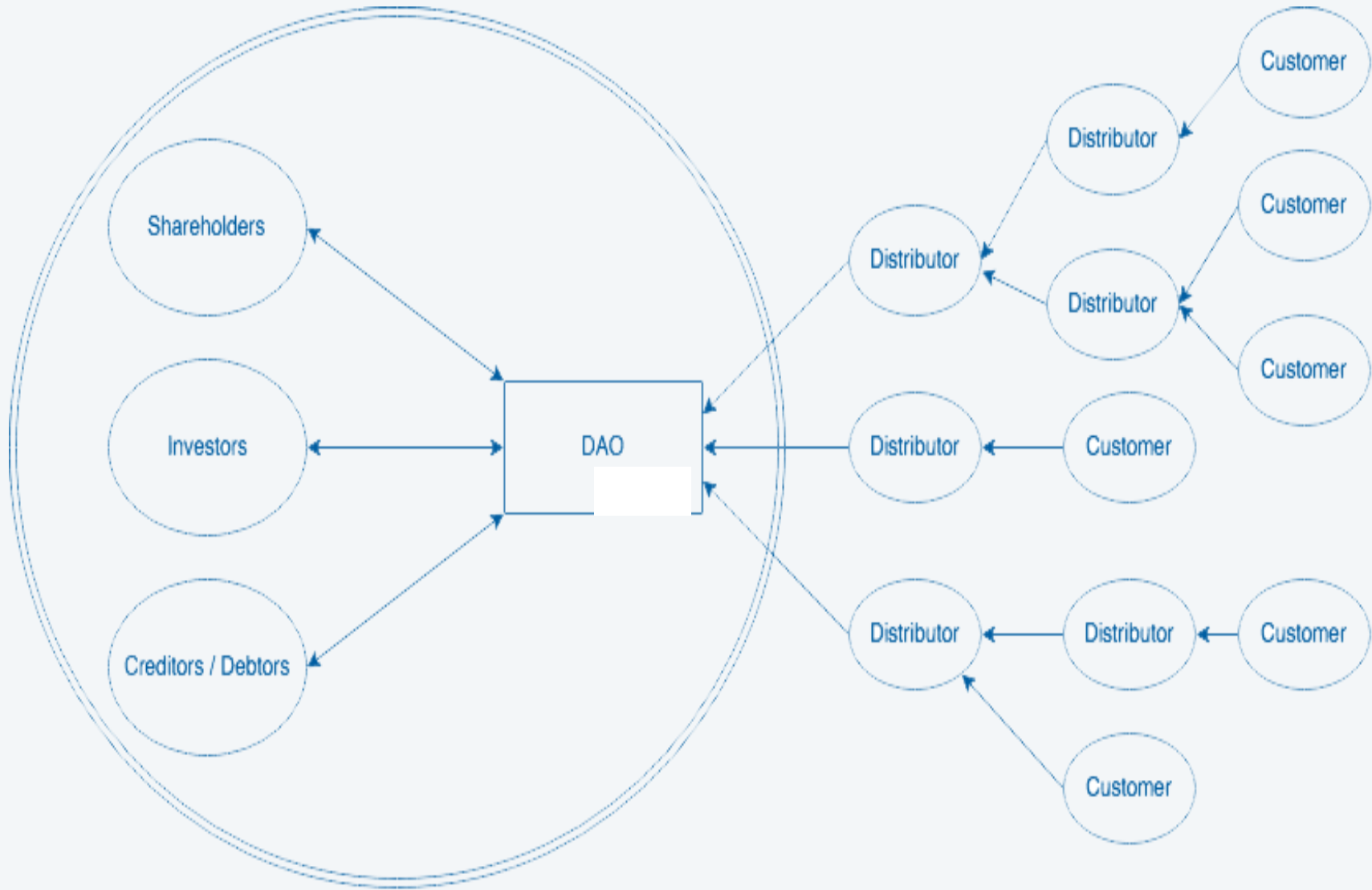
Imperial College
London

Protecting Critical Infrastructure – more than just integrity

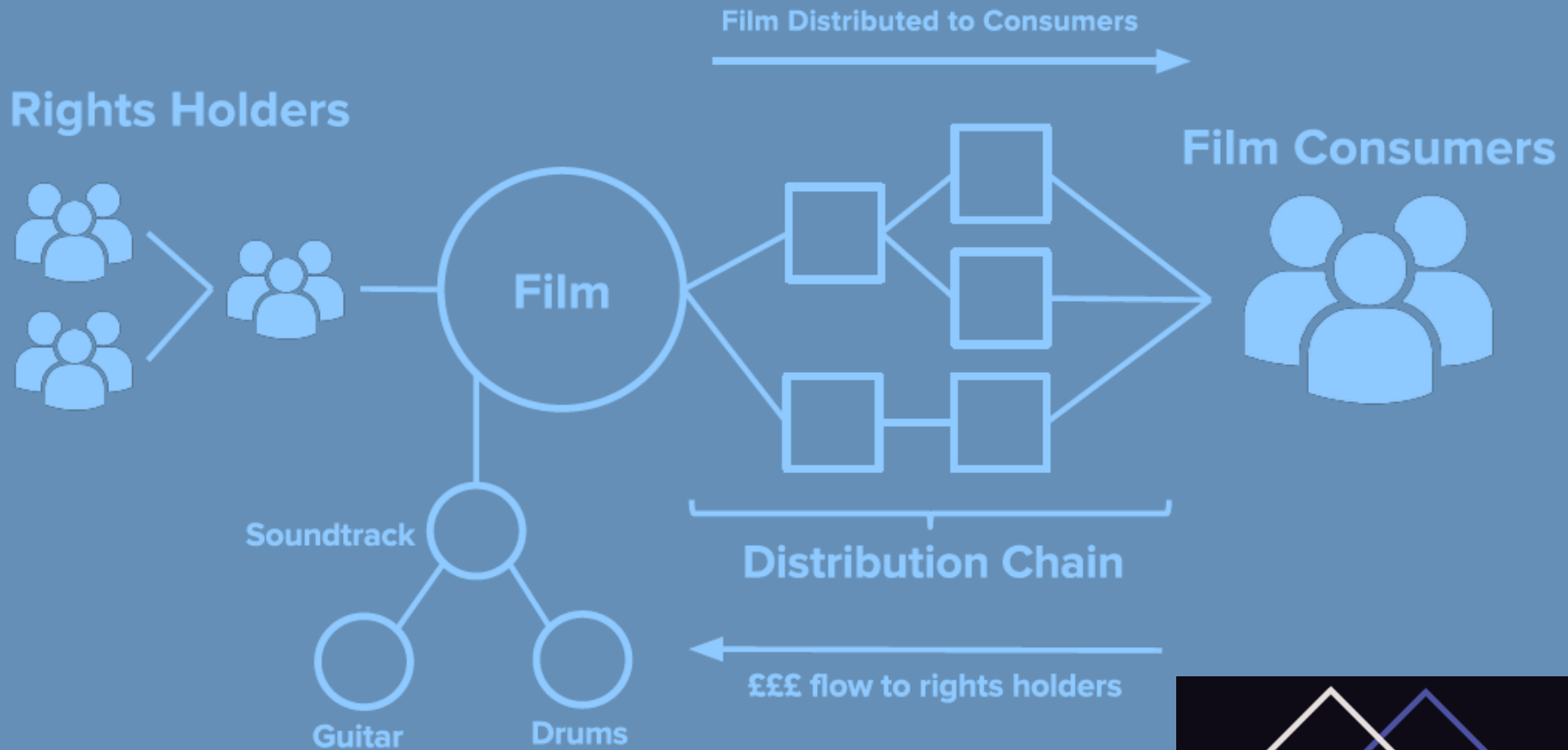
	Integrity Breach	Confidentiality Breach
Your Car	Your braking system stops working.	Your braking patterns are exposed.
Your Flight	Your plane's instruments report that you are 1,000 feet lower than you actually are	Your flight plan is posted on the Internet. (note: it already is)
Your Power Station	Critical systems compromised leading to shutdown or catastrophic failure	Your electricity bill is published online.
Your Pacemaker	Shutdown and death	Your heartbeat becomes public knowledge.
Your Home	Your security system is remotely disabled	The contents of your fridge are "leaked". You drink <i>how much</i> beer?

SOURCE: GUARDTIME

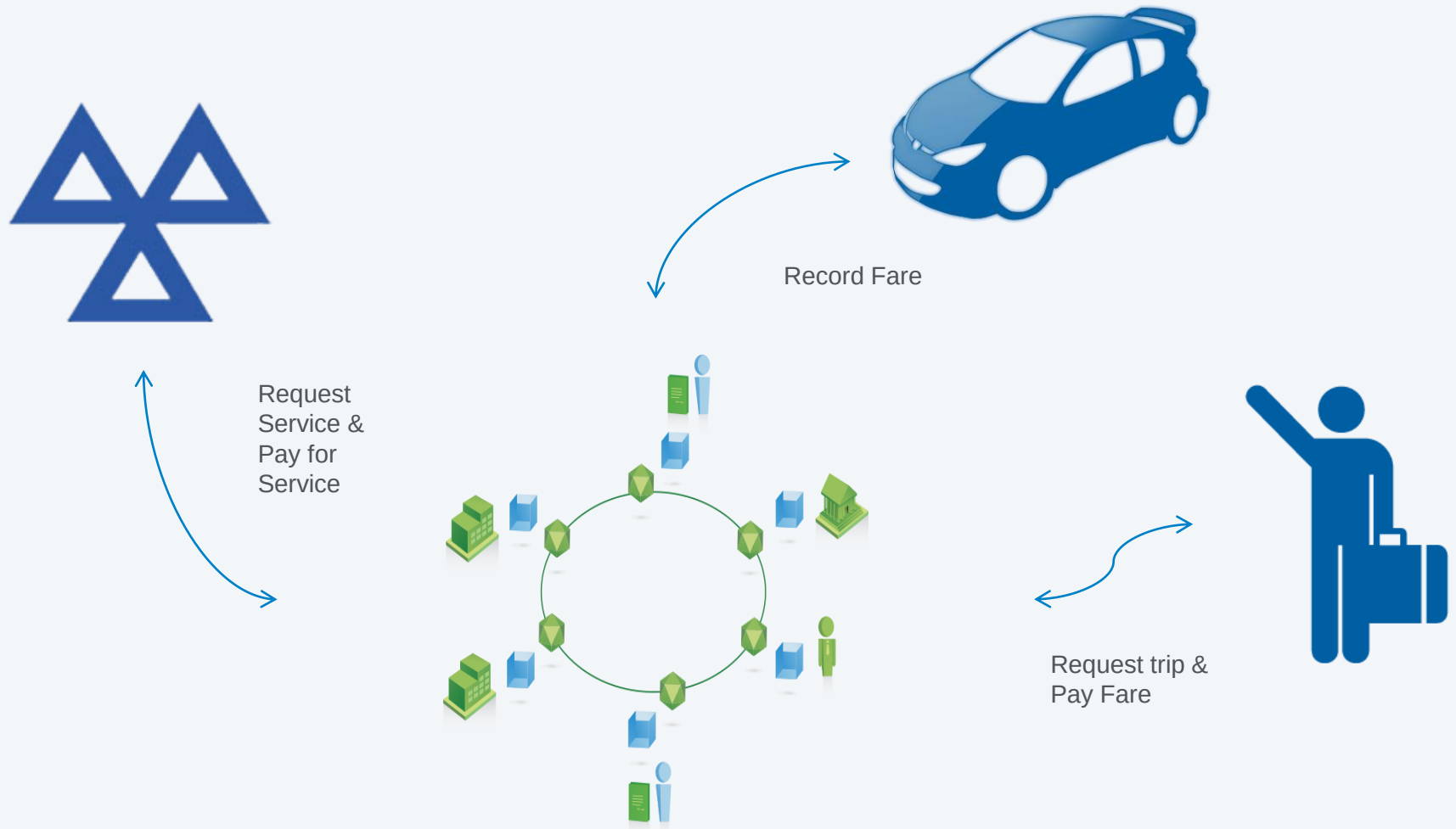
Distributed Autonomous Organisations



Digital Rights Management / Content Creation



Driverless Cryptocurrency Enabled Über



Thank you!

Comments

Q&A

Contact: c.mulligan@imperial.ac.uk