Imperial College
London

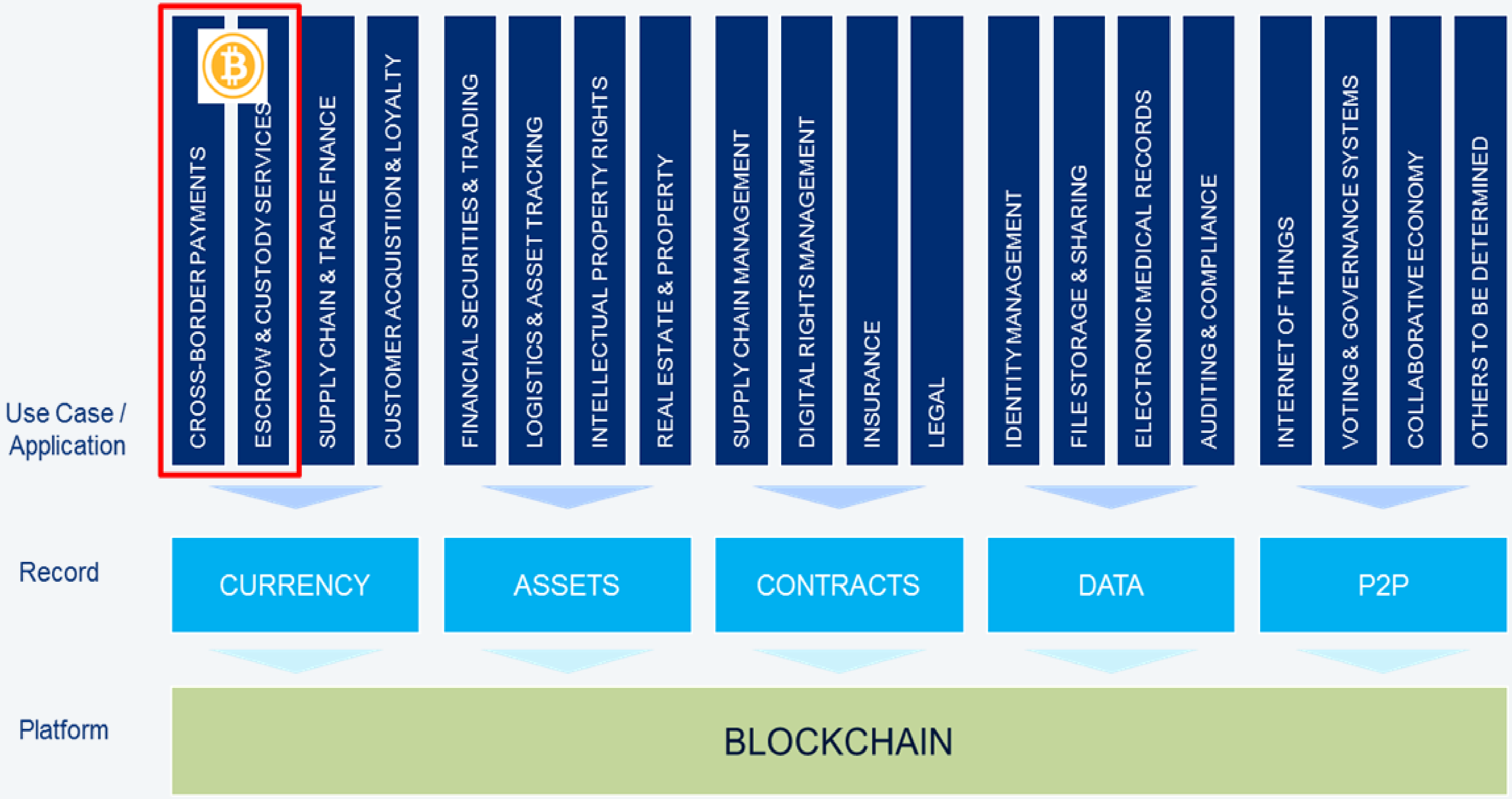
Blockchain – a brief overview

Dr Cathy Mulligan
Research Fellow
Co-Director, Centre for Cryptocurrency Research and Engineering
Expert and Fellow, World Economic Forum Blockchain Council
Vice Chairman, ETSI ISG on Context Information Management

@API_Economics

Blockchain is bigger than Bitcoin

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



Source: Citi Ventures and Imperial College

Distributed Ledger Technology

PERMISSIONLESS, PUBLIC, SHARED SYSTEMS	PERMISSIONED, PUBLIC, SHARED SYSTEMS	PERMISSIONED, PRIVATE, SHARED SYSTEMS	DATABASES
ETHEREUM/BITCOIN	*MICROSOFT COCO*	*HYPERLEDGER, KSI*	

Cross Stakeholder Decentralization

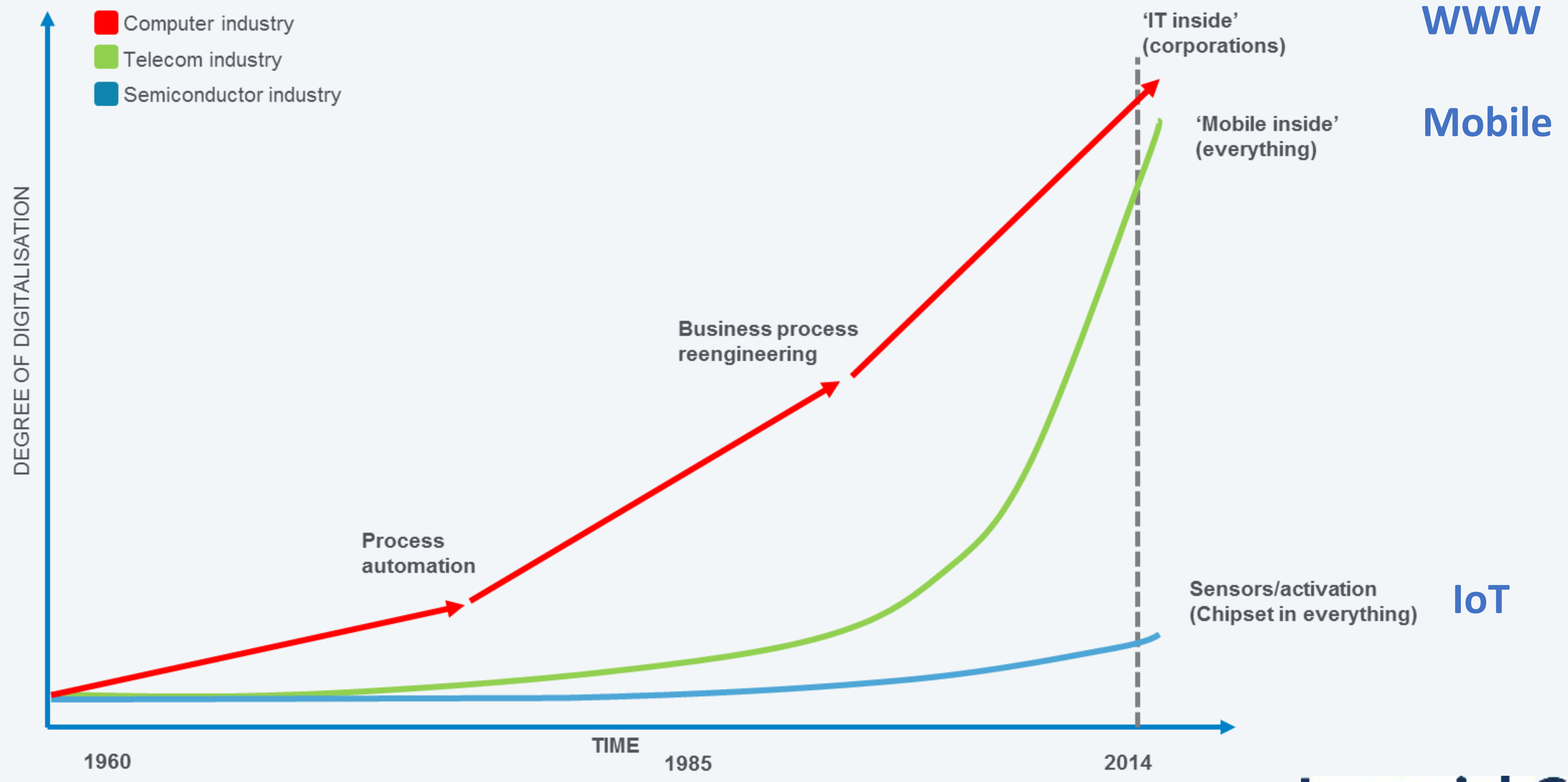
Imperial College London

Blockchain, Digital Disruption and Trust

Previous generations of digital technology have been about *data* and *information* and how to exchange it faster and more securely

Digital technology - transforming our world since 1960

DIGITALISATION + DATAFICATION = DISRUPTION OF ECONOMY SOCIETY, EVERYTHING



Source: Impact of Datafication on Strategic Landscapes

Source Mulligan/Ericsson 2014

Blockchain is about the exchange of *value*

Can we remove intermediaries and replace them securely with digitalised trust?


Download more graphics at www.psdgraphics.com
BANK


HOME
SOLD

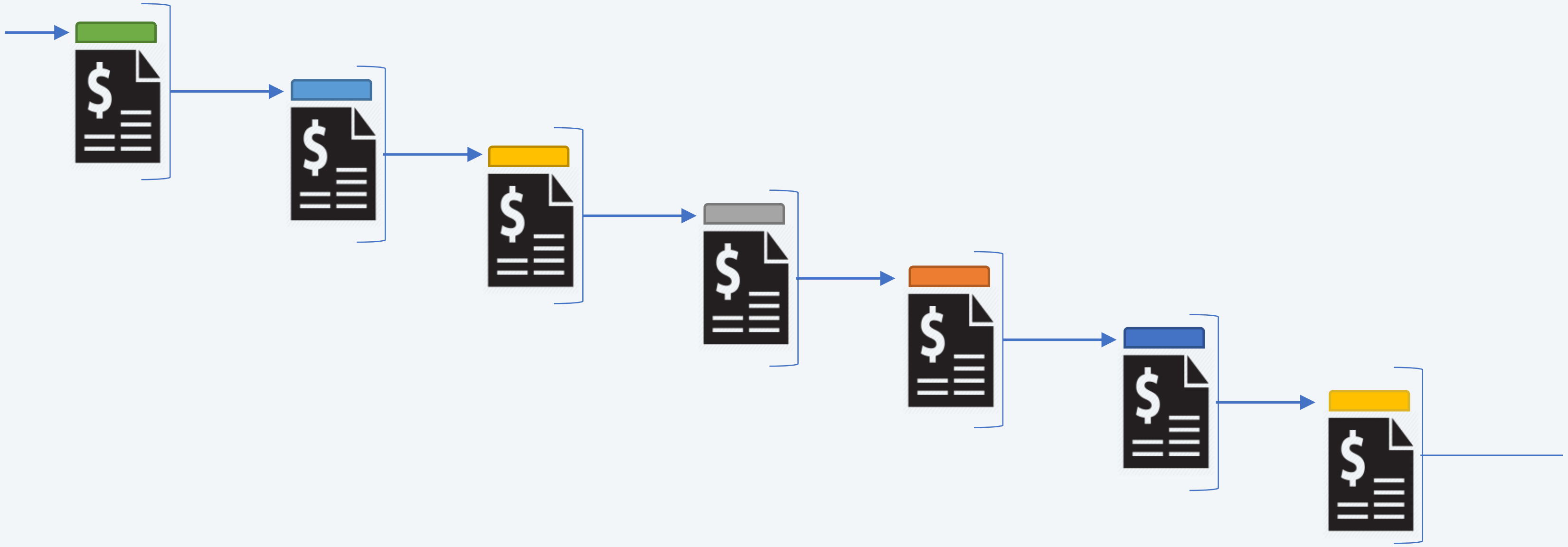
Brief overview of blockchain

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

How is it built?



- Periodically wraps up transactions as a **block** (similar to a page in a paper ledger)
- Each **block** depends on the previous block making a **chain** from the origin
- To edit a transaction in a **block** would require recalculation of all blocks after it
- Normally uses a **distributed ledger** with a **consensus** system and **public/private key cryptography**

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 or Incentives

- 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 crytpographically 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

Examples of Identity Management

Gradbase

Or why blockchain transactions don't always have to be financial in nature

Gradbase

- **Universities** upload degree data to blockchain
- **Students** are given link to their degree data (QR)
- **Employers** can confirm that degree is valid using Gradbase
- Degree information cannot be changed and can be shown to have come from relevant institution

Kacper Zylka

kacper.zylka12@imperia
+44 075495

Education

2012 – **Imperial College London –** Computing

SCAN TO VERIFY

2nd year group projects:

- created a social networking site for internal use by the seed investment prog Entrepreneur First, including user search by skills and interests, collaboration on pr discussion forums. Received the 3rd highest grade out of 40 teams working on d projects
- implemented core parts of an operating system (Pintos)
- wrote a compiler for a While language

2nd year optional modules: Professional Skills for Employability (including team w communication styles, negotiation etc. Distinction), Visualising Global Chal (performed research on infectious diseases, presented at a science festival)

3rd year optional module: Philosophy of Mind

2009 – 2012 **2nd Community High School (2SLO) in Warsaw**

Matura exam (advanced level): Mathematics – 94%, Physics – 88%, English – 95%

VERIFY DEGREE

SUCCESS

Qualification verified by Imperial College London

Transaction details

Confirmed by Bitcoin network.

Name:	Kacper Zylka
Date of birth:	08.10.1993
University:	Imperial College London
Qualification type:	Master of Engineering
Course name:	Computing
Year of graduation:	2016
Degree classification:	First-class Honours

Imperial College London

Thank you!

Comments
Q&A

Contact: c.mulligan@imperial.ac.uk

Imperial College London