Imperial College London

Understanding Blockchain Technologies through Visualization

Dan McGinn – d.mcginn@imperial.ac.uk
Data Science Institute

Presenting to Nordic Capital Markets Forum

Copenhagen – 28 April 2016

Imperial College London

Research Areas

- Pattern discovery of human and algorithmic behaviours in real-time streaming data
- Visualizing abstract big data sets

Imperial College London

Agenda

1. ‘Distributed Ledger Technology’ explained - Bitcoin as a case study
2. What is the innovation and what does it facilitate?
3. Good & Bad use cases for DLT
4. Computational limitations of trustless DLT
5. Regulation and Governance on a blockchain
6. Questions

Imperial College London

1. Bitcoin Explained

A whole system consisting of three main components

1. Protocol
2. Peer-to-Peer Network
3. Blockchain database

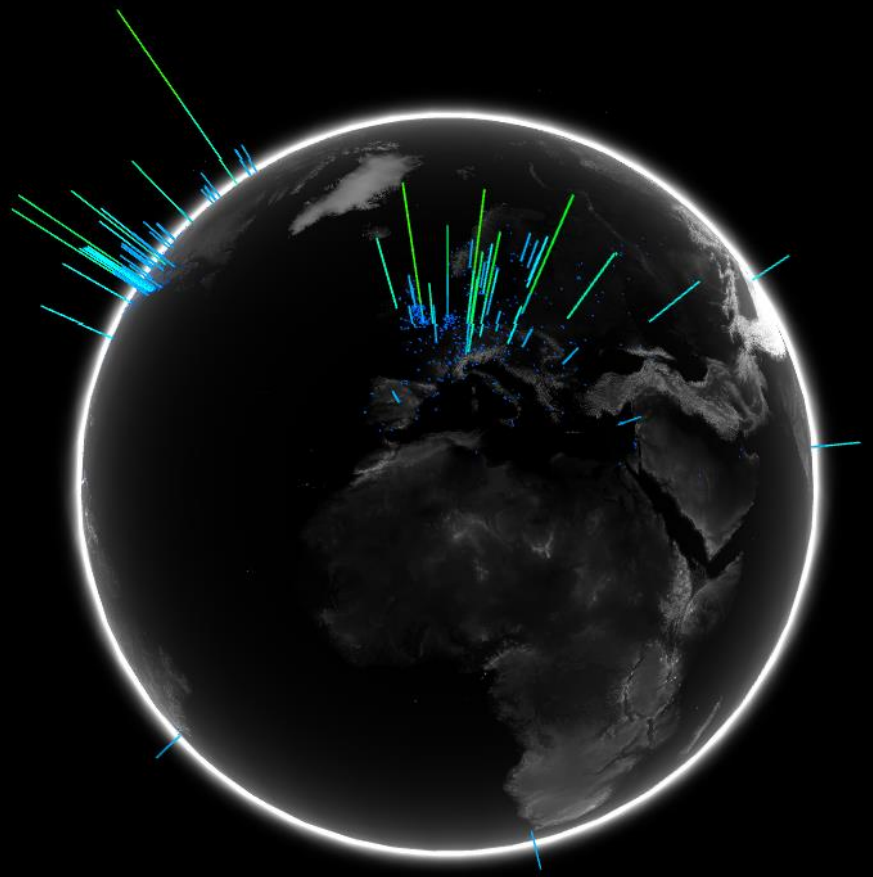
No singular novel innovation

Above all it’s a transaction database, secured by cryptography and economic incentives, that’s distributed amongst trustless participants

Imperial College London

1. Bitcoin Explained

2. Peer-to-Peer Network

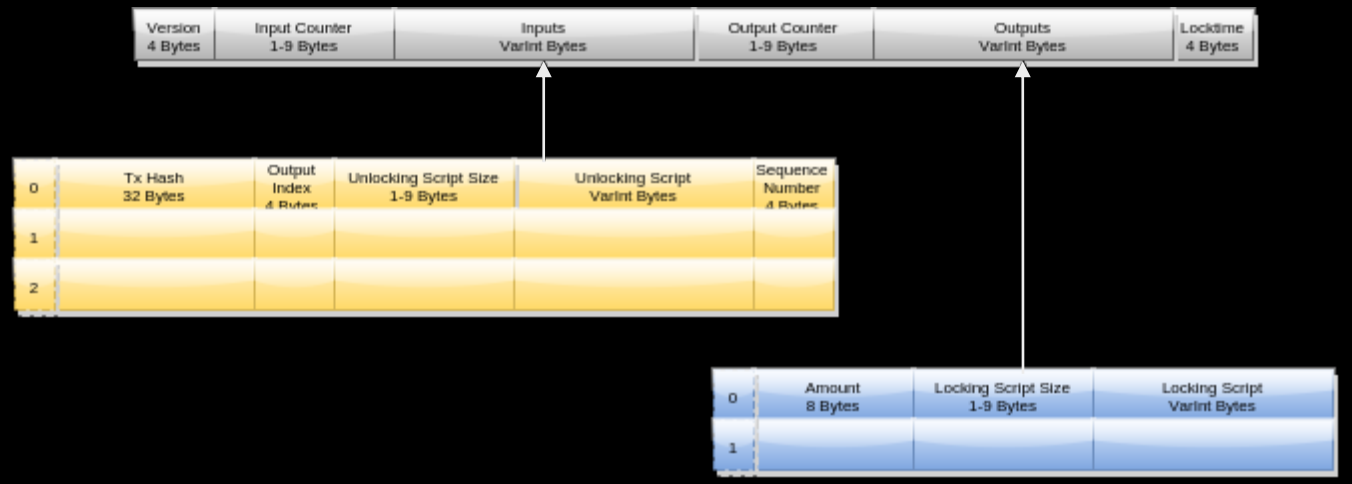


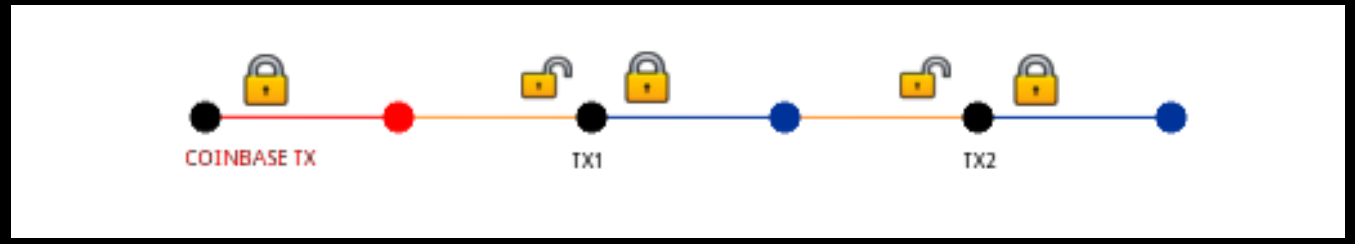
Imperial College London

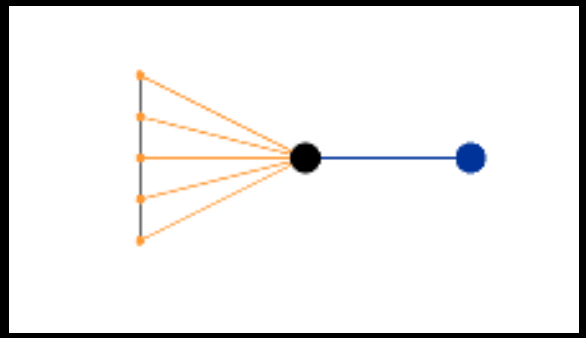
1. Bitcoin Explained

3. Blockchain Database

Transactions







Imperial College London

1. Bitcoin Explained

3. Blockchain Database

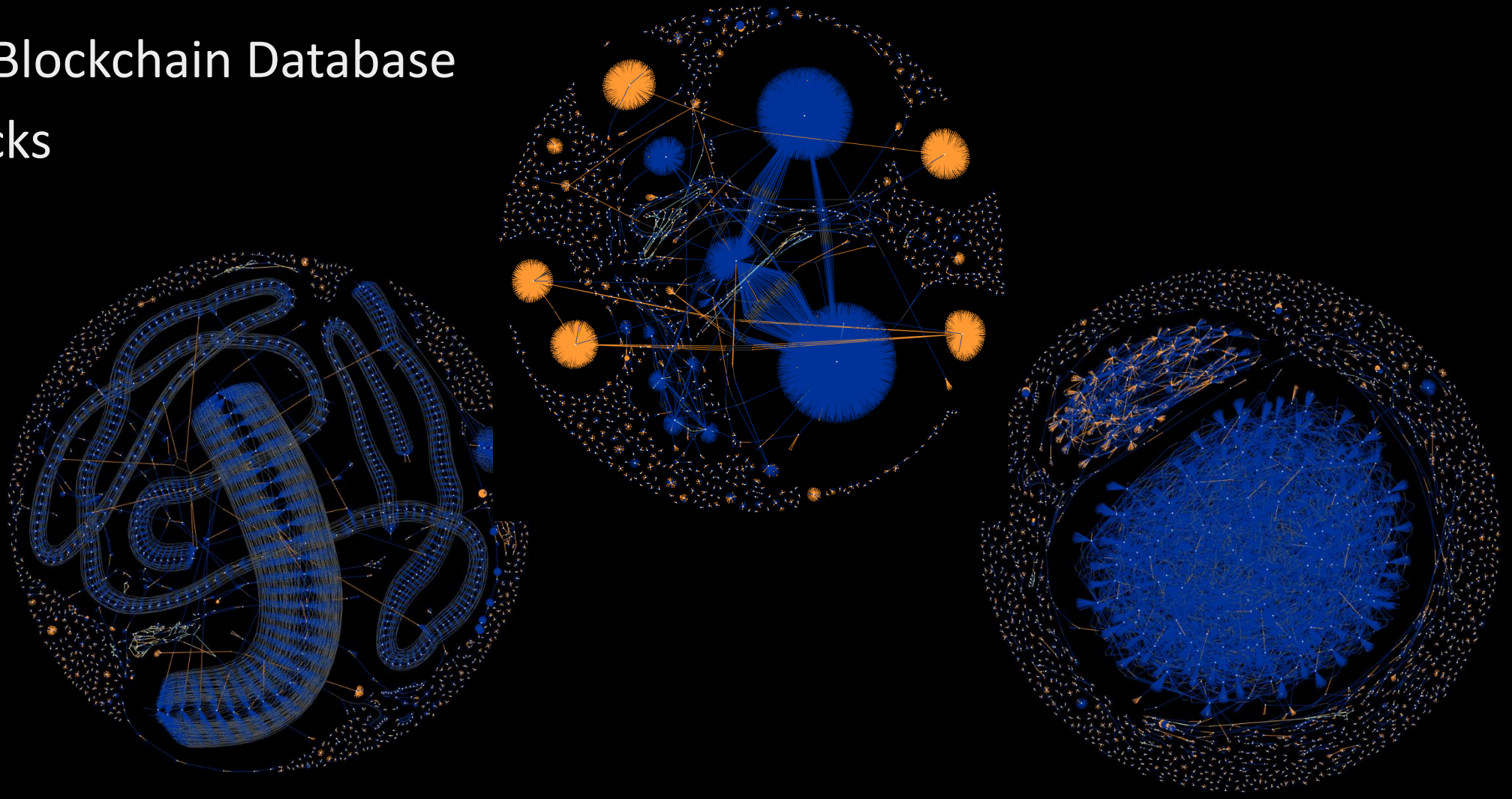
Mining

Imperial College London

1. Bitcoin Explained

3. Blockchain Database

Blocks



Imperial College London

1. Bitcoin Explained

3. Blockchain Database

Not New!

Allows anyone to compute and verify the current system state according to the consensus of participants

Imperial College London

2. What is the Innovation?

- Not blockchain
- Not proof-of-work
- Cryptography + Economic Incentives →

A: Decentralized Digital Trust

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

Imperial College London

2. What is the Innovation?

- Old Old Trust Model – Show me your armies
- Old Trust Model – Show me your reputation and relationships
- Current Trust Model – Show me your license
- New Trust Model – Show me your code

Imperial College London

2. What is the Innovation?

Internet = Disruptive platform for information dissemination

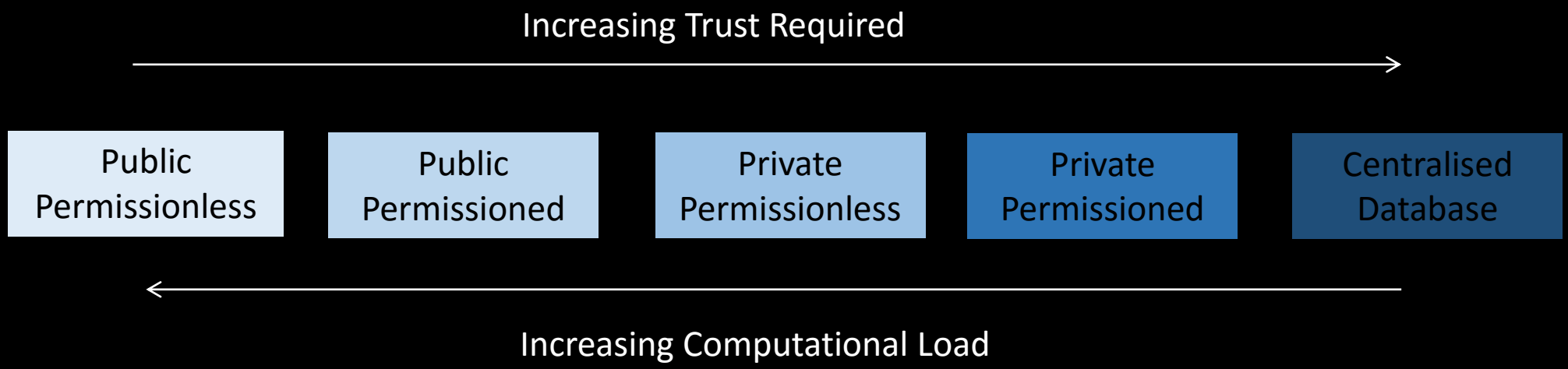
Blockchain = Disruptive platform for the exchange of value

- Cheaper?
- Faster?
- Increased security?
- Increased anonymity?
- Censorship resistant

Imperial College London

2. What is the Innovation?

Blockchain Spectrum of Trust



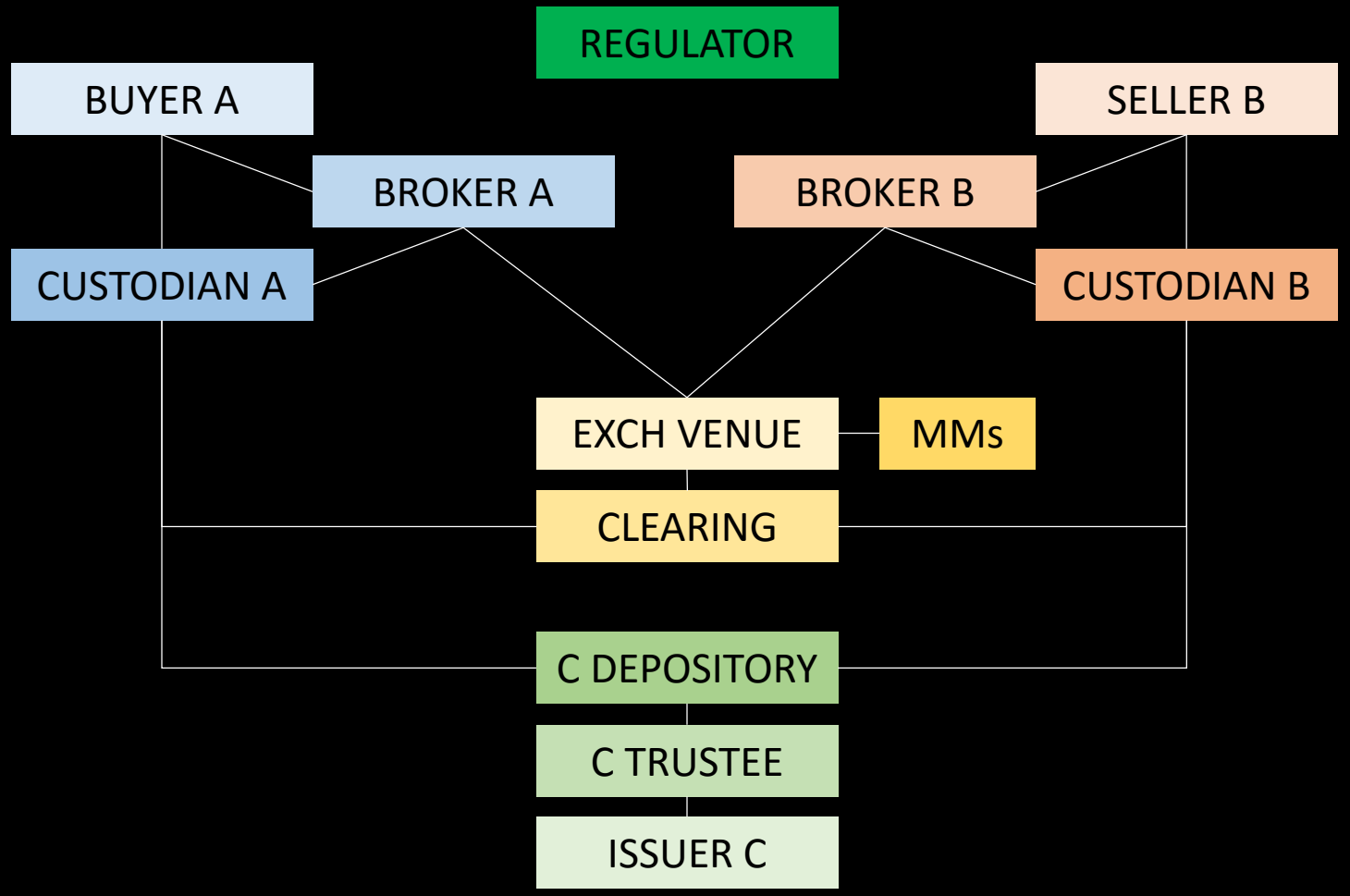
Imperial College London

3. DLT Use Cases

- Good for disintermediating central authorities
- Good where there exists mistrust amongst strangers
- Good for reducing reconciliation costs & counterparty risks
- Good where chronological transactions are highly interdependent
- Good for transparency & interoperability
- Bad where a central authority retains control
- Bad where known parties can be trusted through authentication
- Bad where data volumes are high

Imperial College London

3. Use Cases

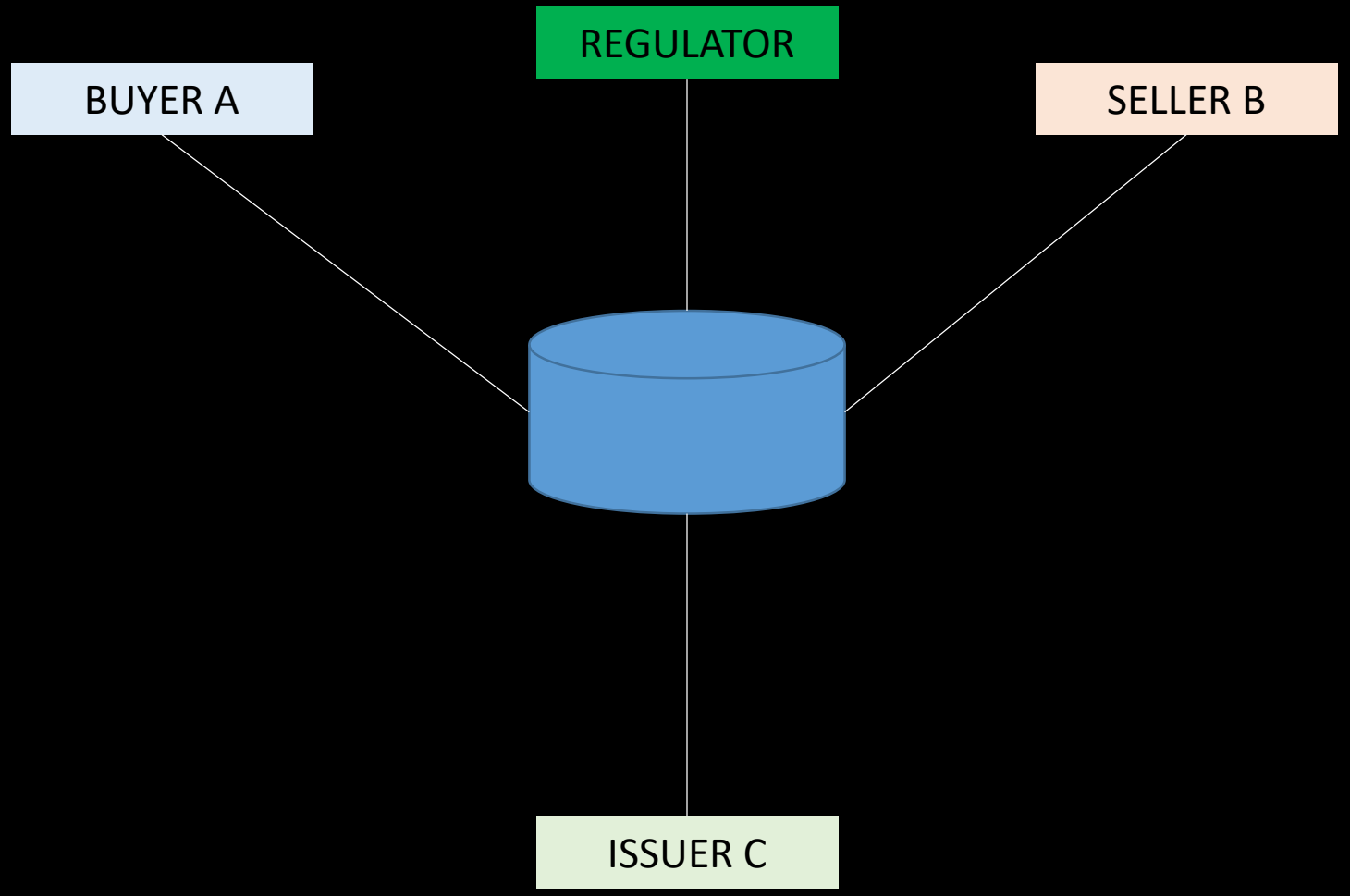


Imperial College London

3. Use Cases

- Good

eg DvP

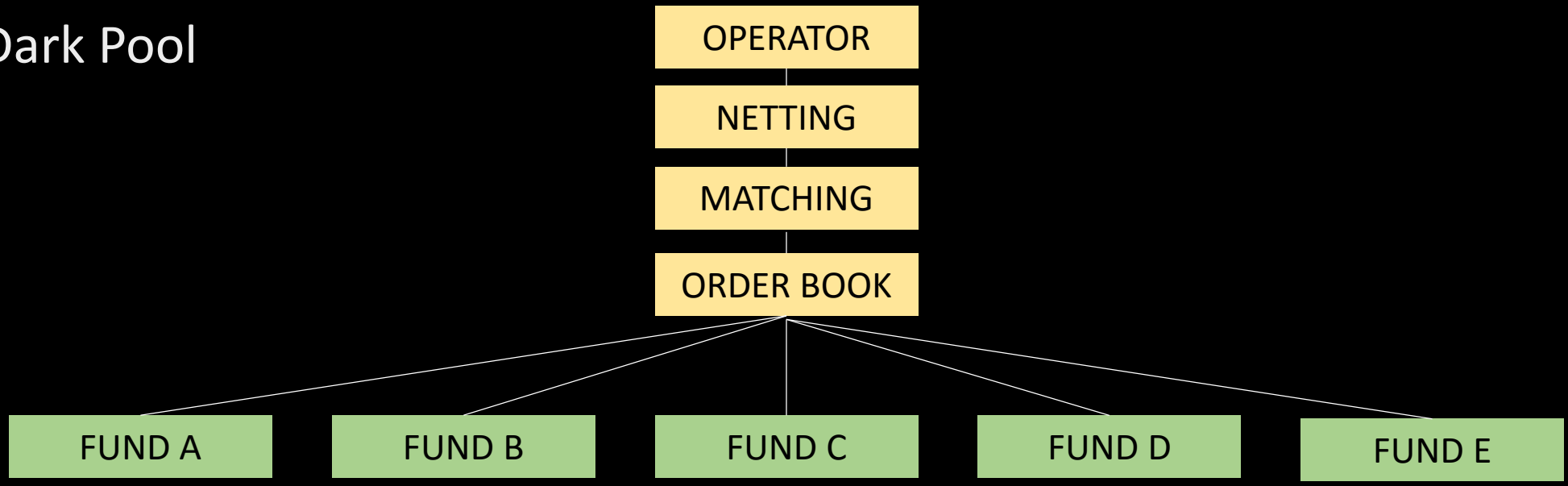


Imperial College London

3. Use Cases

- Bad

eg Dark Pool



- In MOST cases, a properly authenticated and replicated traditional database will be a more appropriate solution

Imperial College London

4. Computational Limitations

- Mass replication of data for truly trustless operation
- Every node must verify every transaction, no matter how small
- Latency between transaction broadcast and consensus acceptance
- Proof of work expensive and computationally useless
- Proof of stake untested
- Costs can be reduced by increasing trust amongst participants
- Compliance functions can be achieved through smart contracts

Imperial College London

5. Regulation & Governance

- Bitcoin IS regulated: by strict rules adopted by user consensus
- Tendency to centralisation: both validating miners and developers
- KYC & AML can be satisfied with new e-government tools
- Privacy can be augmented with zero-knowledge proofs
- Will capital relief be available for the risks DLTs can reduce?

Imperial College London

Summary

- DLT's facilitate the creation of an agreed shared database to establish an agreed truth state amongst trustless strangers
- Still very nascent technology and will take time to mature and gain adoption, probably in niche areas
- Interoperability levels will determine success
- Costs and benefits over existing technologies remain an open question
- DLT's are less useful for centralised applications where a traditional database will be more appropriate in most cases

Imperial College London

Thank You!

Questions?