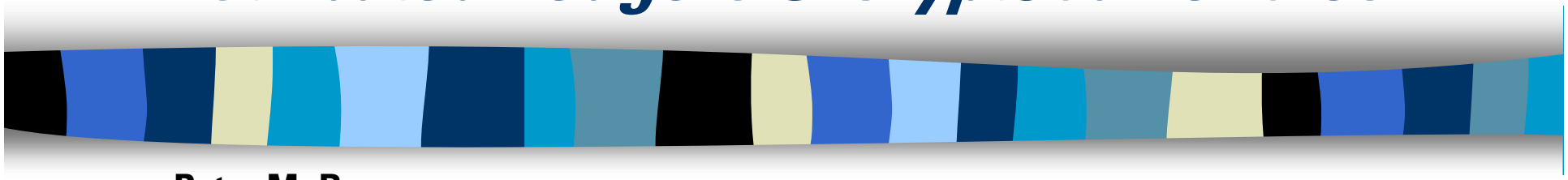
7CCSMDLC: Part A
Distributed Ledgers & Cryptocurrencies



Peter McBurney
Professor of Computer Science
Department of Informatics
King's College London

Email: peter.mcburney@kcl.ac.uk
Bush House Central Block North – Office 7.15

January 2021

Outline: Part A

- Course Information & Arrangements – this information is in Part B
- Bitcoin and Blockchain
- Distributed Ledger Technology
- Smart Contracts
- Current Landscape

The Team

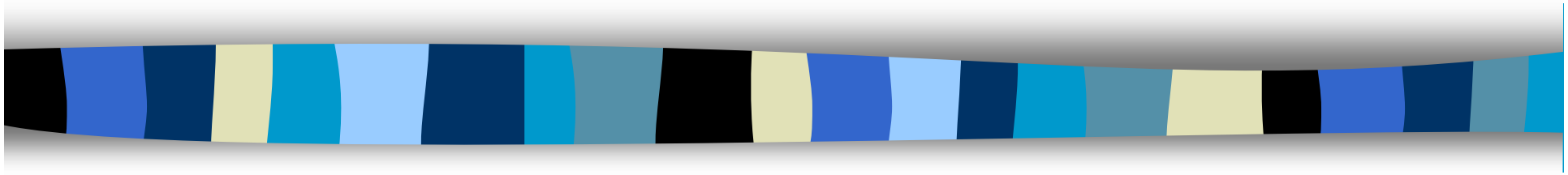
- Peter McBurney

  peter.mcburney@kcl.ac.uk

- Mr Wenbin Wu

  wenbin.wu@kcl.ac.uk

Department of Informatics
Bush House – Central Block
Level 7 North.



Bitcoin and Blockchain

Blockchains are the new black

"We may be witnessing one of those potential explosions of creative potential that catalyse exceptional levels of innovation."

Sir Mark Walport
Chief UK Government Scientific Advisor
January 2016.

"I wish I was 30 years younger because this is really interesting stuff!"

Jeremy Wilson, Vice-President Corporate Banking,
Barclays Bank. July 2015.

The Problem

We desire an electronic money system that ensures

- The e-money is authentic (not counterfeit)
- The same e-money cannot be spent more than once (*double-spend problem*).

How to do this?

- Need a trusted person or organization to issue the money and record all transfers.

How to do this without such a person?

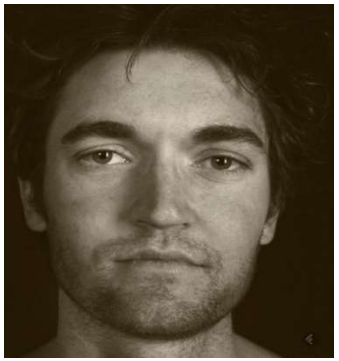
Precursers

- Bitcoin was first truly decentralized system for e-money

- Previous technologies
  - Asymmetric key cryptography
  - eg, Hashcash (1992) – a Proof-of-Work (PoW) system to hinder spam and DDoS attacks
  - b-money (1998) – application of Hashcash to e-money, with transactions broadcast to all participants
  - Protocols for distributed consensus

- Underlying philosophy
  - **Cypherpunk Movement** (from 1992 onwards): Advocates of cryptography and privacy technologies for social & political change
  - See e-money as a way to avoid Government control
  - Still a large section of the cryptocurrency community.

Satoshi Nakomoto



Andrew O'Hagan [2016]: The Satoshi Affair.
London Review of Books, 38 (13) 30 June 2016, pages 7-28.

The Bitcoin Blockchain

- Cryptographic currency: Bitcoin
  - White paper published in 2008

    Satoshi Nakamoto [2008]: *Bitcoin: A Peer-to-Peer Electronic Cash System.*
  - First code released 2009

- Design properties:
  - No central authority
  - Decentralized
  - No double-spending of currency
  - Open and public
  - Anonymous (actually Pseudonymous)

- Enabled by Blockchain technology.

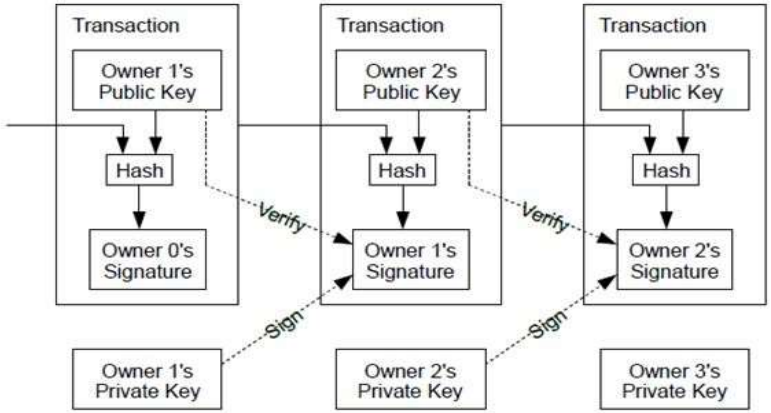
Bitcoin Blockchain

- Transactions
  - Transactions represent & are exchanges of Bitcoin
  - Transactions signed by digital signatures
  - Transactions aggregated into blocks & uploaded
  - Blocks chained together

- Aggregation and chaining done by Miners
  - Doing this takes processing power (some work)
  - Miners paid in bitcoin

- Blockheaders have dynamic-membership multi-party signatures based on computation power (not on knowledge or permission).

- Chaining done by hashing.


Transaction
Owner 1's Public Key
Hash
Owner 0's Signature
Transaction
Owner 2's Public Key
Hash
Owner 1's Signature
Transaction
Owner 3's Public Key
Hash
Owner 2's Signature
Verify
Verify
Sign
Sign
Owner 1's Private Key
Owner 2's Private Key
Owner 3's Private Key

//

A metaphor — coffee transactions

Credit: World Barista Championship

Blockchain for Bitcoin

- Focus: Crypto-currency transactions
- No central authority
  - No central bank
  - No need to trust anyone
- Witnessing done by entire community on the blockchain
- Chaining makes it very difficult to alter past records
  - Need to alter all the records since then
- Witnessing makes it hard to alter or create false past records
  - Have to get 50% + 1 participants to agree your new chain is the correct one
  - Forking
- Coins tagged
  - So cannot double spend.

Bitcoin process

- A bitcoin (or part) is represented by a chain of current and past owners
  - Represented by their wallets (effectively their public keys).

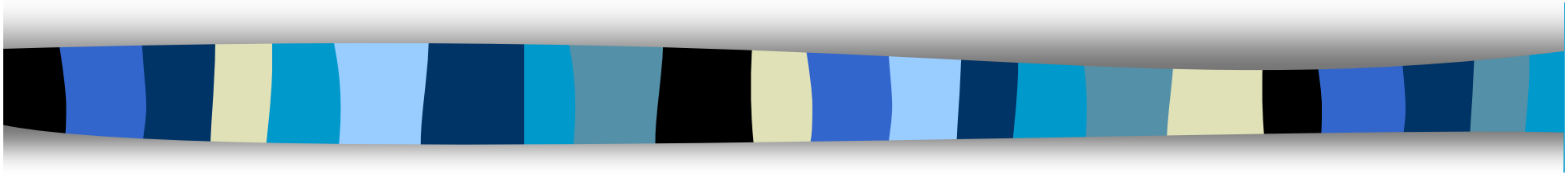
- The process
  1. Sender A creates new transaction
     - Sender A signs with his private key
     - Sender A signs with the public key of Receiver B
  2. New transactions sent to all nodes
  3. Each miner (mining node) bundles recent transactions into a block
  4. Each miner tries to solve a difficult mathematical problem (Proof-of-Work)
  5. When solved, the miner informs all nodes
  6. Nodes check for validity and accept (or not-accept) the block
  7. If accepted, miners start working on the next block (using the hash of the block just accepted)
  8. Accepted blocks are linked into the main chain. If competing chains exist, nodes accept the chain with the most PoW.
  9. Successful miner paid in new bitcoin (reward for PoW) and transaction fees.

Proof of Work

- PoW is part of the protocol for validation and consensus
- Why is it necessary?
  - Bitcoin is open, and we need to motivate the validation & uploading process.
  - So we reward the validators/uploaders (fees + new bitcoin)
  - But how to ensure honesty? How to distinguish between different nodes seeking payment?
- For a closed system, we may not need PoW.
- Other Protocols include:
  - Proof of Stake (PoS)
  - Proof of Authority (PoA)
  - Proof of Identity (PoI)
  - Proof of Elapsed Time (PoET)
  - etc

Who are the users of Bitcoin?

- Online gambling (original use-case?)
- Criminals and people laundering money
- Governments & people evading international sanctions
  - eg, DPRK, Iran, Russia
- People in countries with capital export controls, hyperinflation or with high levels of corruption
  - eg, Zimbabwe, Venezuela, Indonesia, North Korea
- Anyone having a need for money for any legal or illegal purpose.



Distributed Ledger Technology

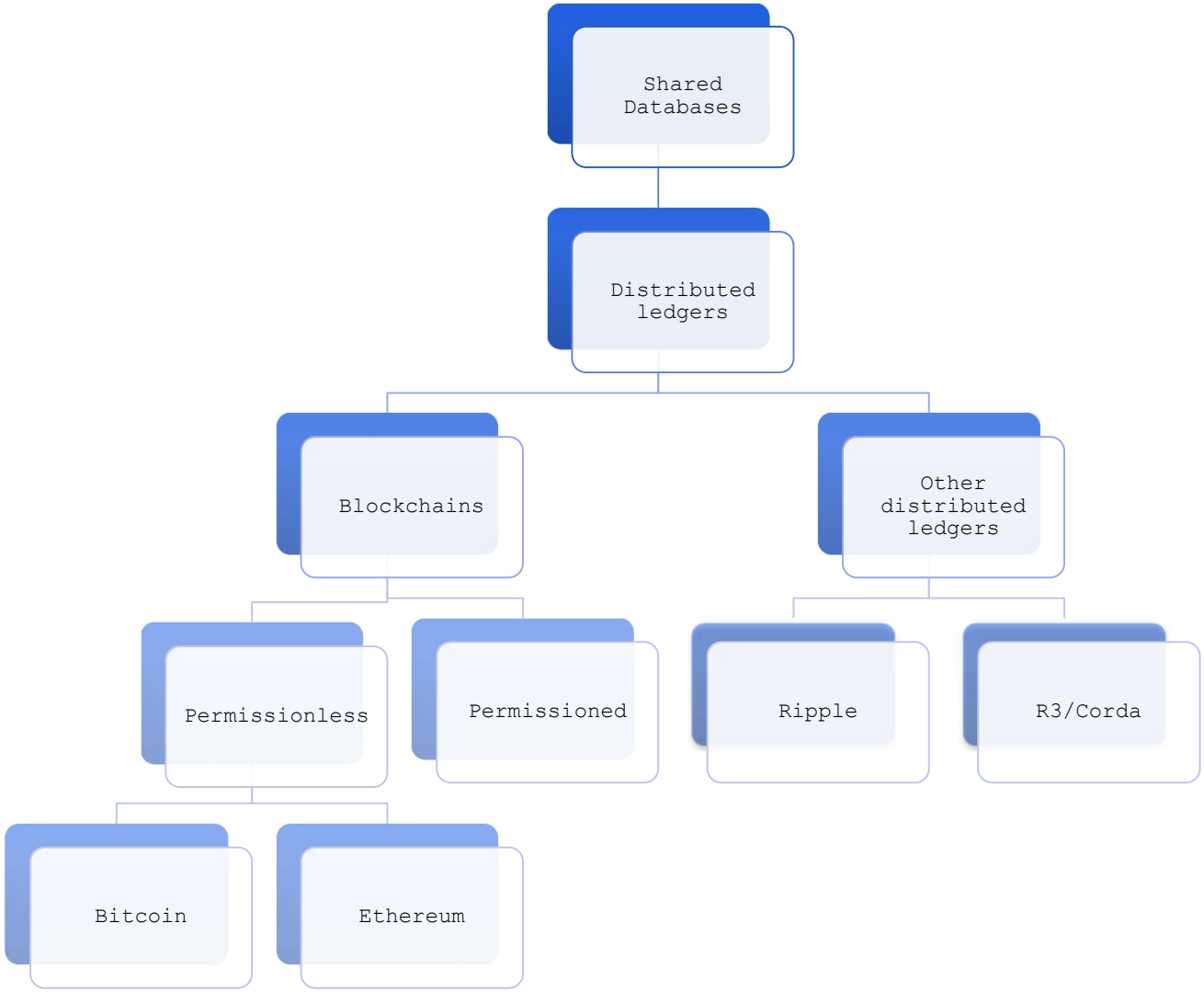
A Blackboard metaphor

Stateful shared state

In Computer Science parlance:

- All nodes on a distributed ledger agree on the values of the variable(s) on the ledger. They have a **shared state**.
- The ledger also preserves past states (the history), so the protocol is **stateful**.
  - In contrast, HTTP (Hyper-Text Transfer Protocol) is state-less.
- Distributed Ledgers have **stateful shared state**.
- This property can prevent “double-spending” of some currency or asset.

Shared databases



DLTs – Evolving thinking over last several years

Distributed Ledger Technologies appropriate for:

- Cryptocurrency transactions
- Currency transactions
- Transactions involving exchanges of ownership of assets
  - eg, chains of custody
- Records of information
  - eg, personal identity, chains of custody
- Promises and commitments
  - eg, futures contracts, trade flows, insurance, regulatory compliance.

Blockchains and Distributed Ledgers

Several computer technologies are combined:

- Duplicated databases
- Hashing
- Asymmetric key cryptography
- Agreement protocols

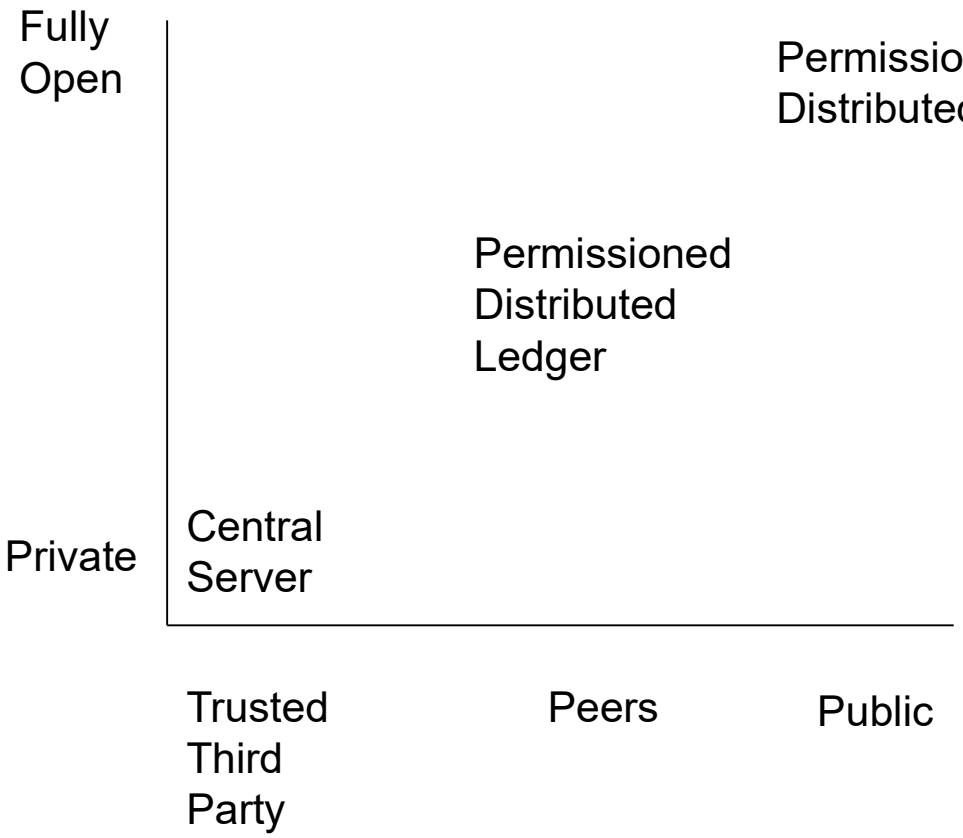
Features

Redundancy & robustness
No central authority
Transactions observable
Immutable records
Non-repudiable records
Encrypted records
Content agnostic
Programmable (potentially)

The Design Space for DLTs

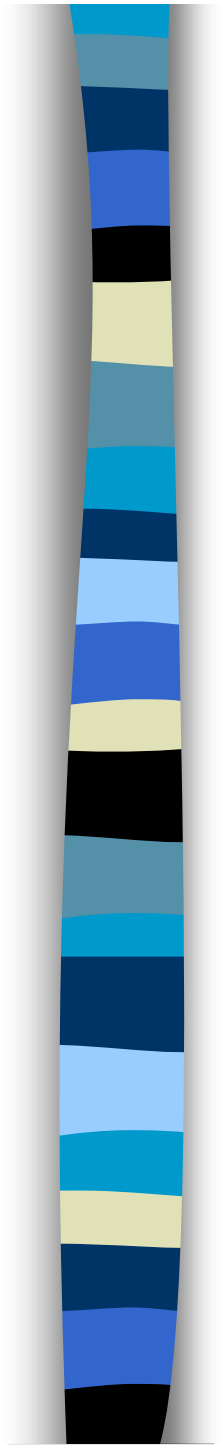
- Closed or open ?
  - Permissioned or Permission-less
  - Who is the witnessing/voting community?
- Payments for mining?
  - What currency? (Bitcoin, Ether, XRP, Citicoin, etc)
- Consensus & voting protocols?
- Blocking & chaining?
- Records
  - Who can see? Where stored? Who owns? Who may use?
- Smart contracts
  - vs. software architecture
- How is differential access ensured?
- How are privacy and security ensured?

Trade-off: Confidentiality vs. Trustlessness



Who is the community?

- One organization
- Multiple organizations
- Public
  - Permission-less



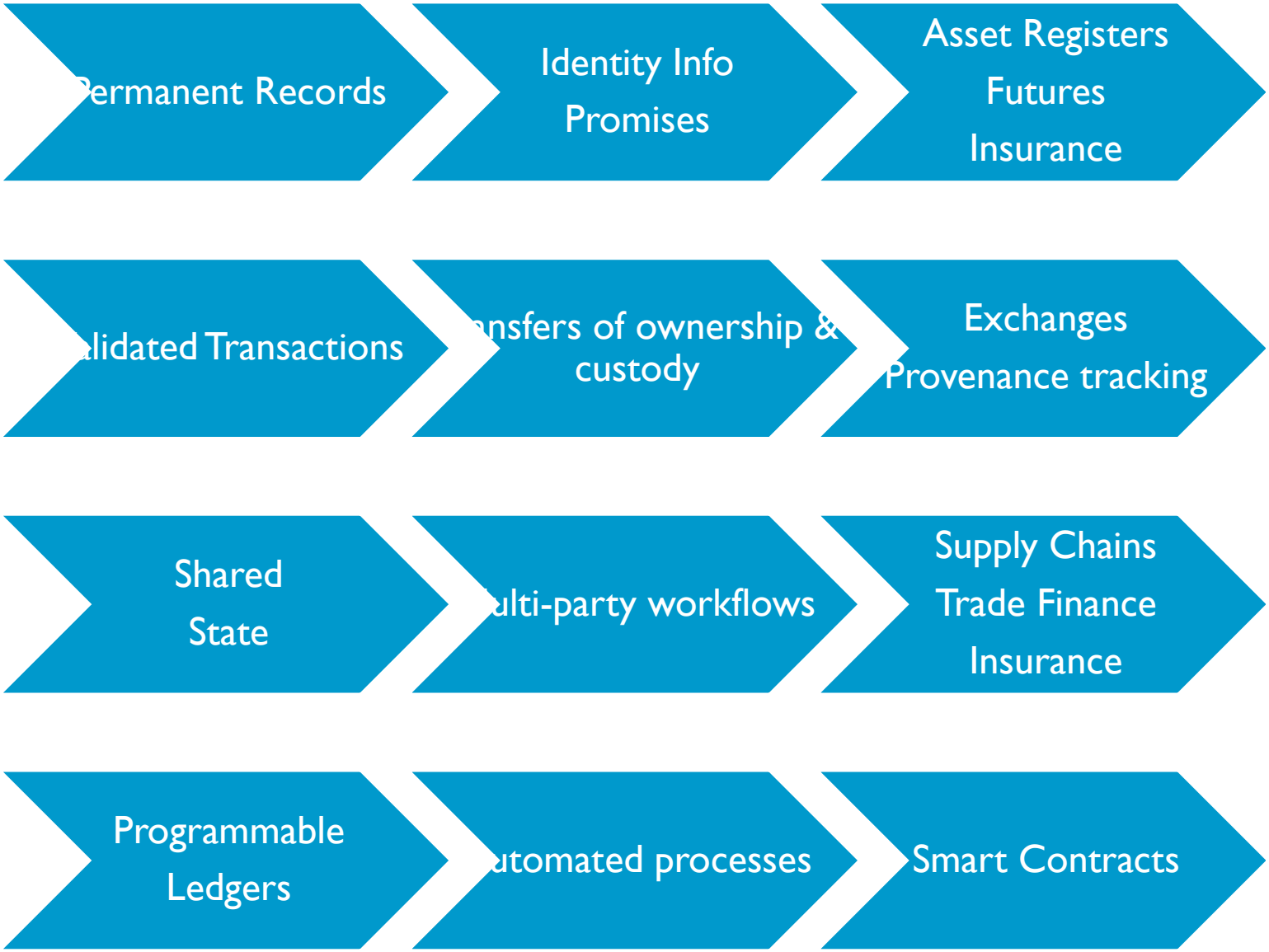
Trust moves to software

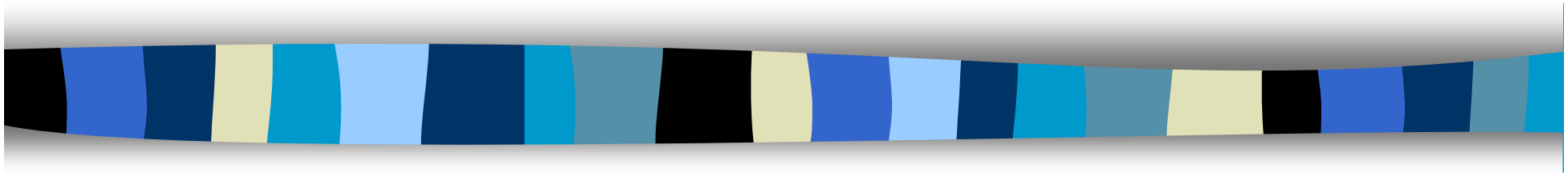
- Trustless transactions
  - The connected community acts to witness transactions
  - So no need of trusted third parties

- But trust is still required
  - Who specifies, designs and creates the software?
  - Who verifies the software properties?
  - Who identifies and fixes bugs?
  - Who maintains & updates the software?

- Example:
  - 2016 Exploitation of DAO (Decentralized Autonomous Organization).

DL features and enabled applications

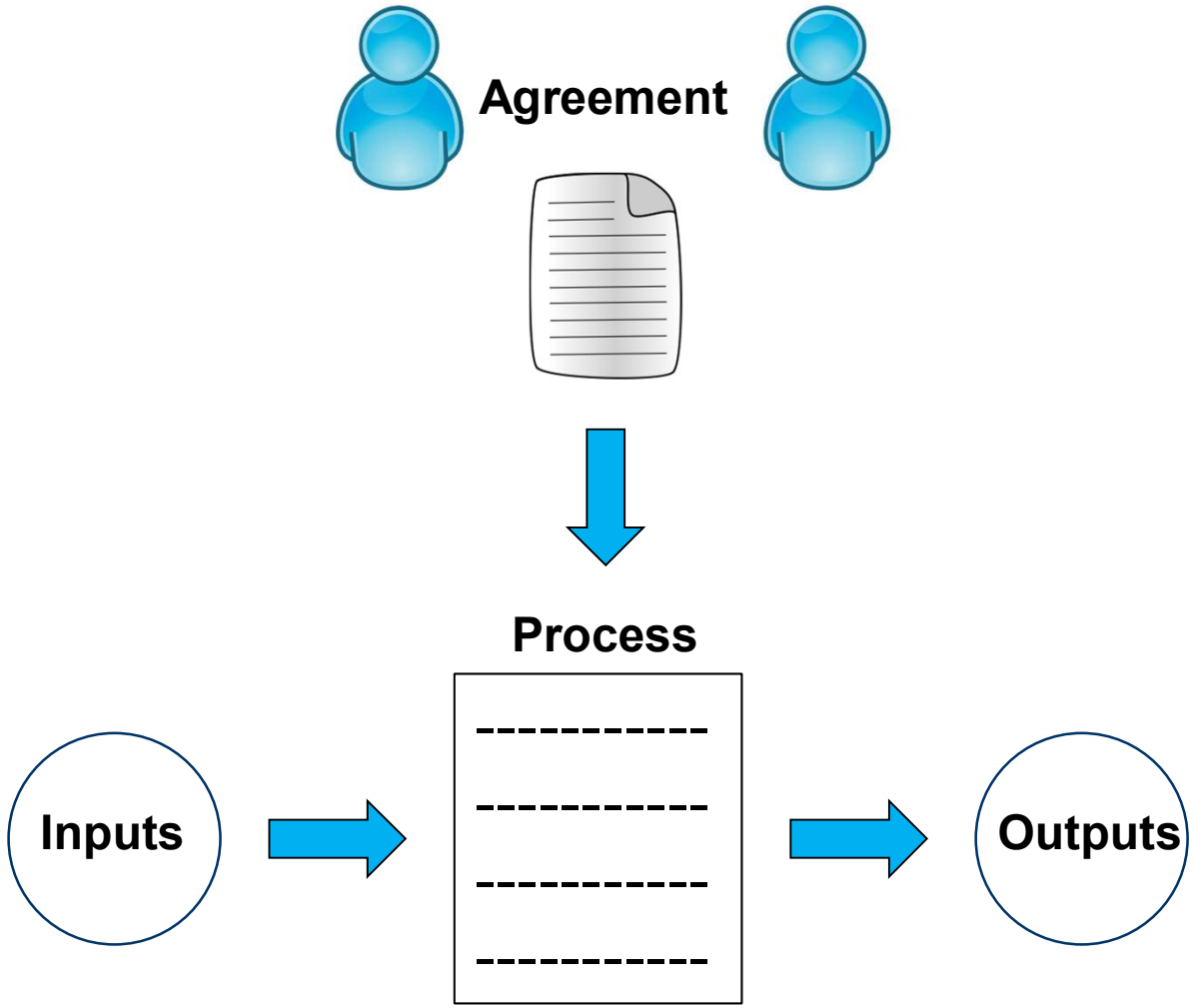




Smart Contracts

A smart contract . . .

. . . is an automated process, usually based on agreement between two or more parties, that autonomously executes at a trigger

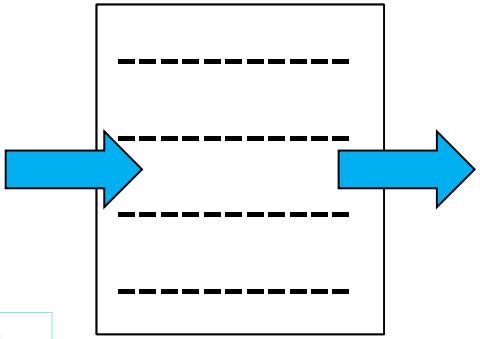


Smart Contracts are Automated Performance Scripts

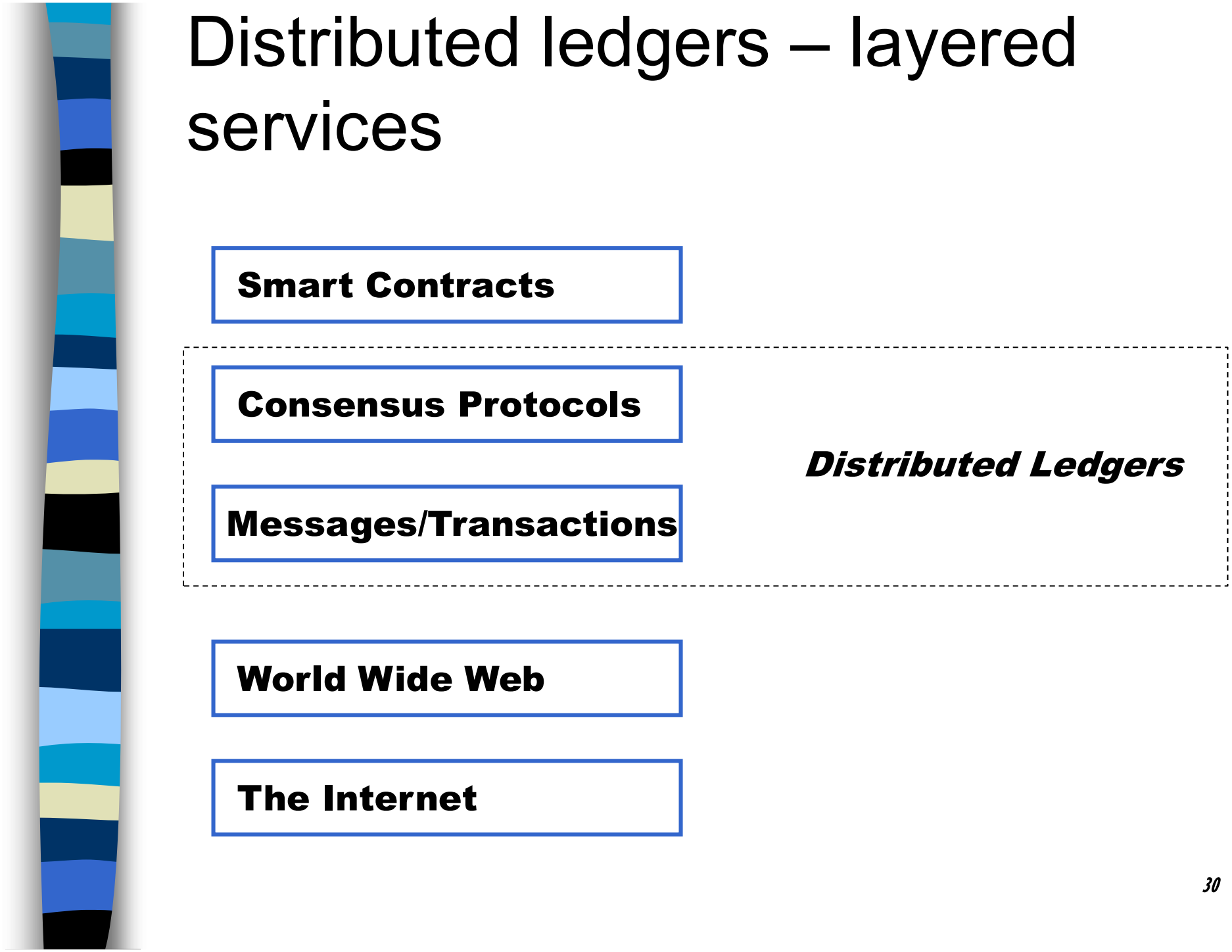
Example

Inputs: Satellite images of wheat fields
Weather forecasts
(To forecast harvest dates and crop quality)

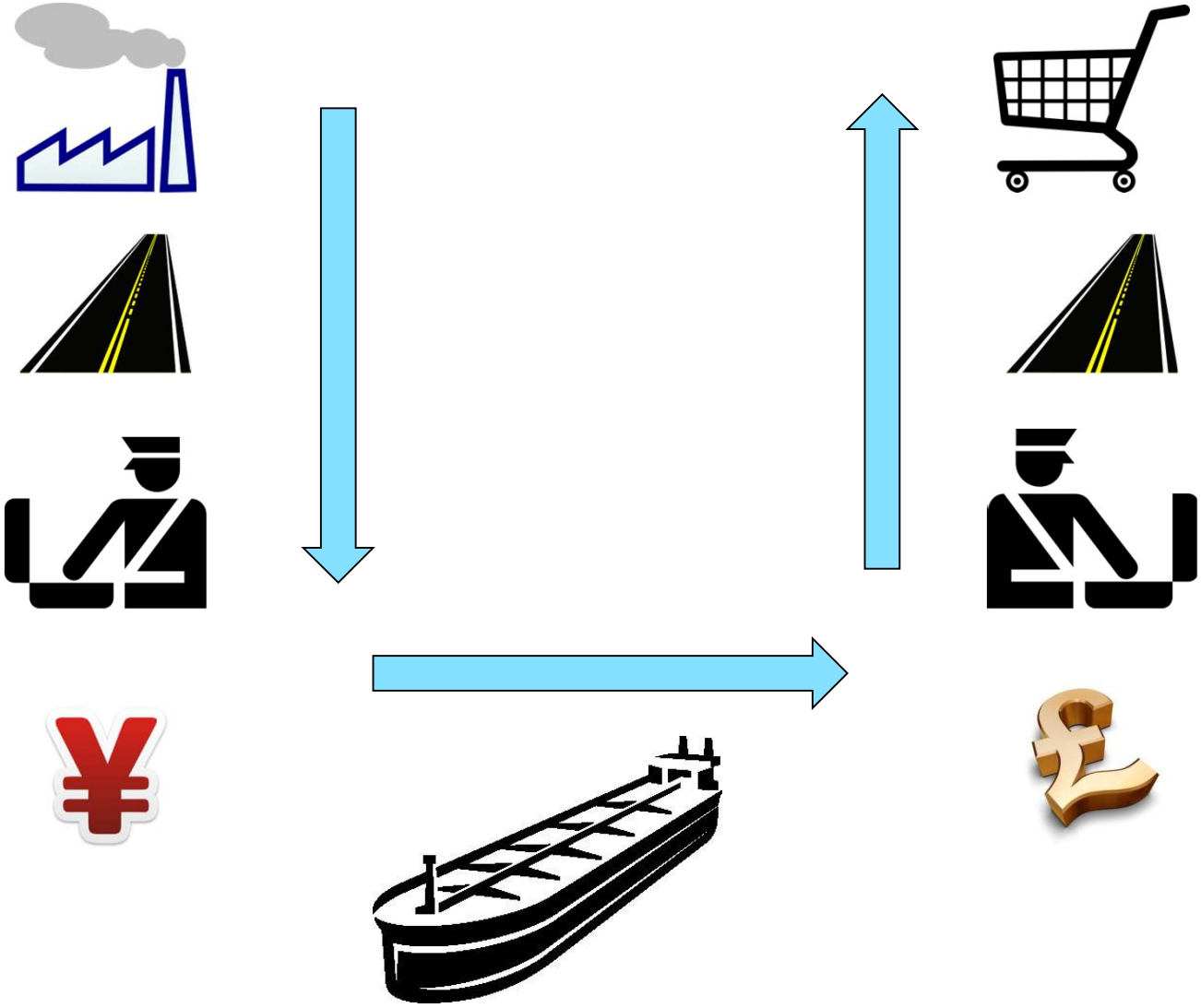
Outputs: Execution of wheat futures contracts.

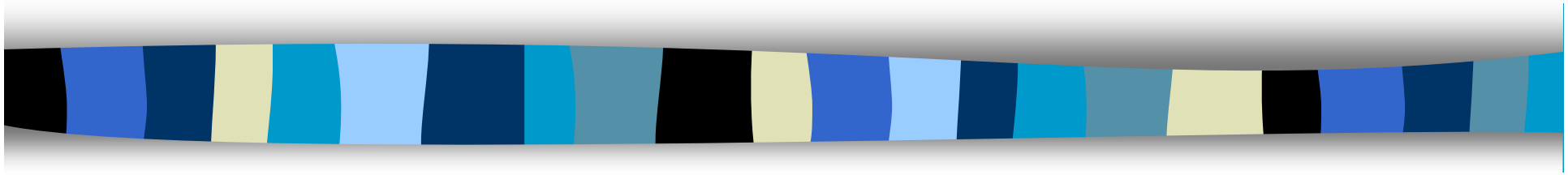


Distributed ledgers – layered services



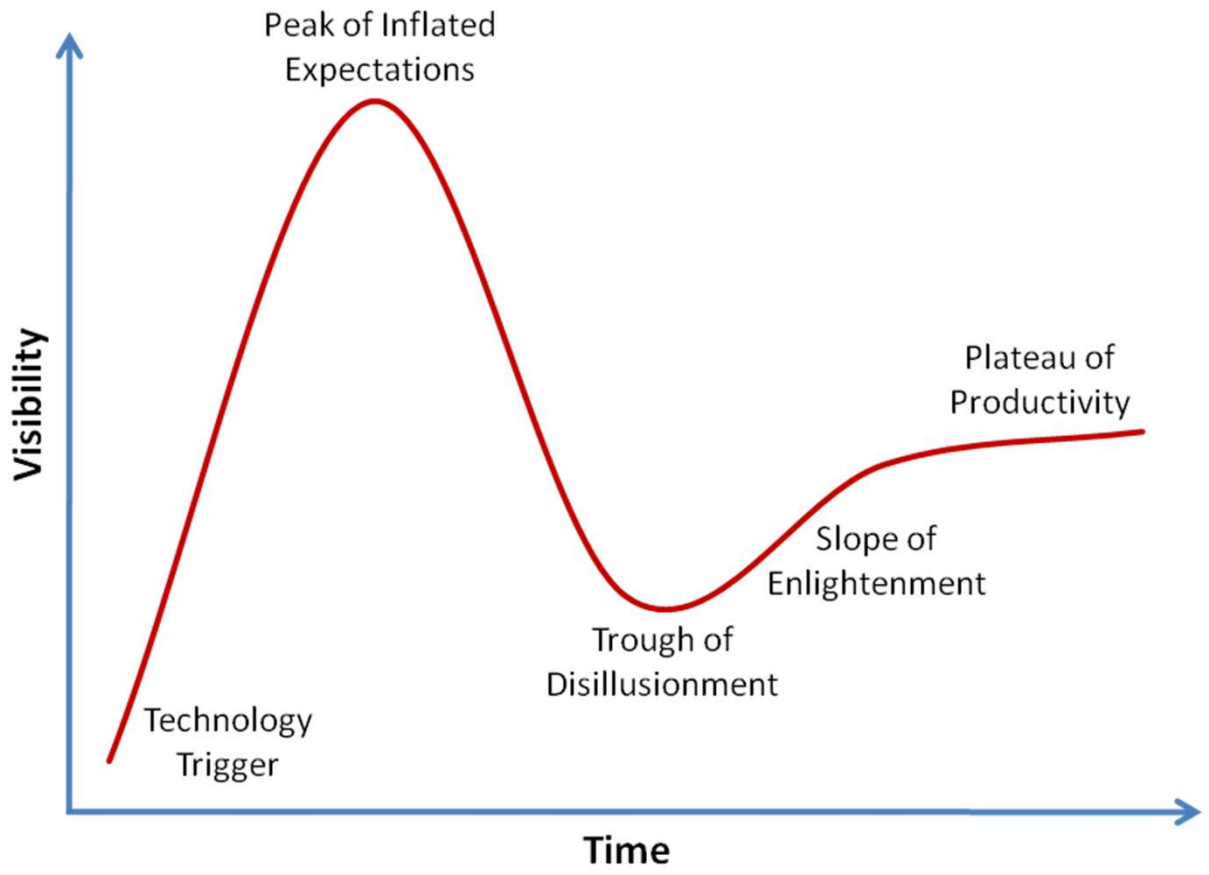
Application: Trade Finance





The Current Landscape

The Gartner Technology Hype Cycle

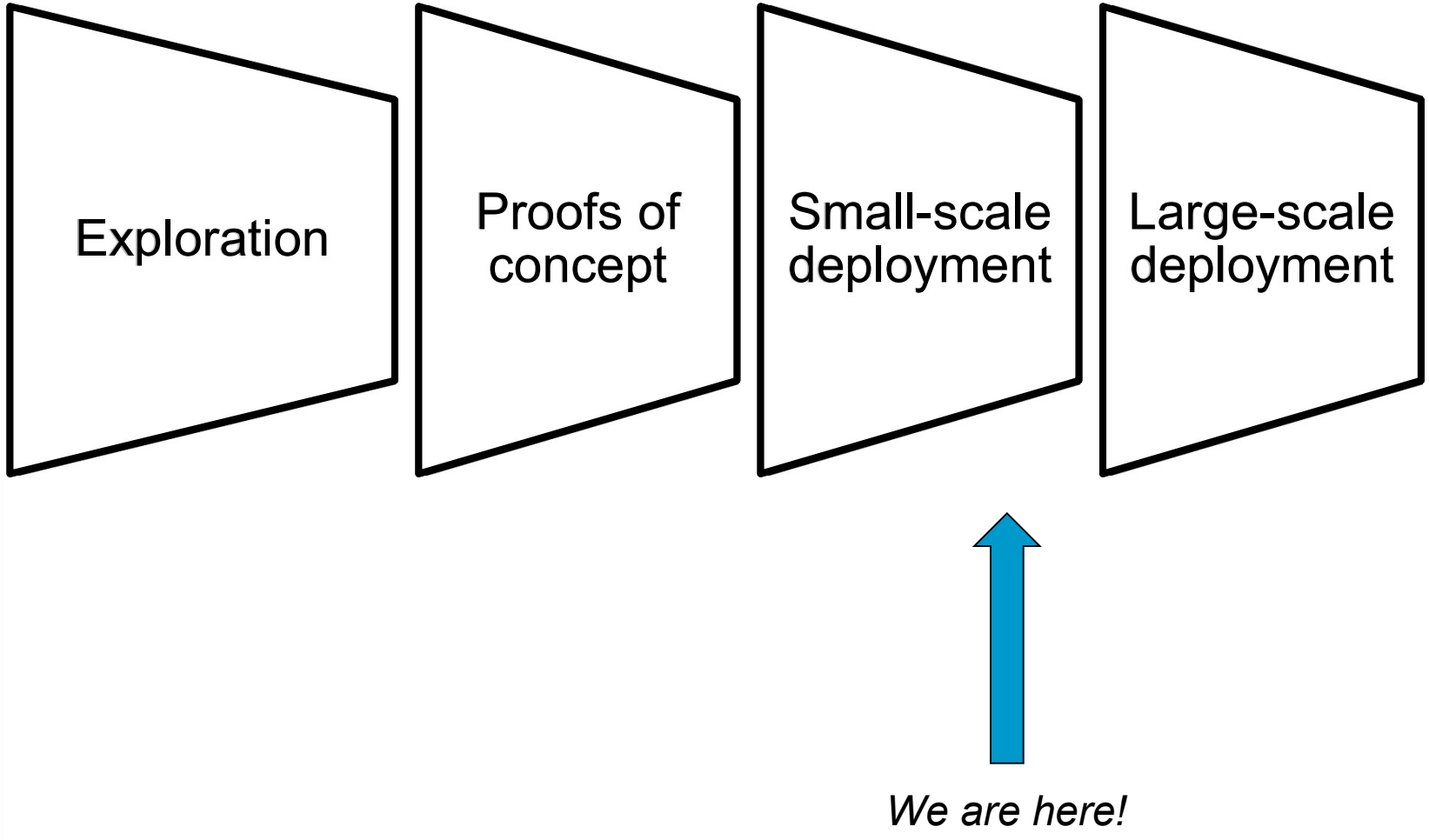


Source: The Gartner Group

Initial Coin Offerings (ICOs)

- Initial Coin Offerings (ICOs) or Token Generation Events (TKEs)
  - Pre-sales of future tokens
  - Raising funds on the basis of future system development (a white paper)
- *Funding your start-up airline by pre-selling the frequent-flyer miles!*
- As much as $4 billion raised (Block.one)
- Risks
  - Regulatory: are these securities?
  - Class-action law suits
  - Promises only
- A bubble!

DLT: Stages of development



Source:
Kwôri & NRF Report

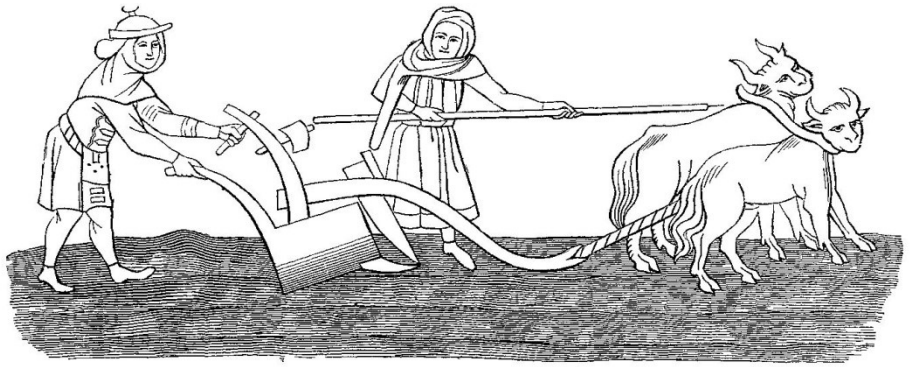
Applications of DLT

- Permanent identity information
  - eg, University degrees
  - Land registers
- Trading Platforms
  - High-value, low-frequency transactions
- Asset registers & tracking
  - eg, diamonds, works of art
- Automated data aggregation
  - eg, management accounting
- Workflows across multiple organizations
  - eg, Supply chains, BoLs, trade finance
  - Post-trade commodities management.

Research Challenges

- Conceptual framework
  - What is the space of possible designs?
  - What is the fit between designs and applications?
    - For instance: what level of privacy is appropriate for each application

- Technical
  - Platforms & dev tools still immature
  - Scale
  - Speed
  - Appropriate designs
  - Verification
  - Robustness against attack
  - Privacy on networks.



Implementation challenges - Technical

- Data Management
  - Privacy, confidentiality, storage, ownership, exploitation, IP
- Production readiness
  - eg, security, compliance & monitoring requirements, analytics capabilities
    - William Mougayar: 18-24 months to finalize after a PoC!
- Integration with legacy systems
- User-friendly interfaces and APIs
- Managing multiple DLs
  - Different underlying technologies
  - Different interfaces
  - Data reconciliation between DLs
  - Key management.

Implementation Challenges: Organizational & Legal

- Organizational challenges
  - Managing stakeholders
  - Managing revocation & cancellation
  - Business Process Engineering/Re-engineering
    - Especially for inter-organization workflows
  - Governance & Management
    - eg, of permissions
  - Data ownership, privacy & usage

- Legal and Regulatory aspects
  - Competition (Anti-Trust) Law
  - Ownership of IP
  - Data privacy & management
  - Legal status of smart contracts.

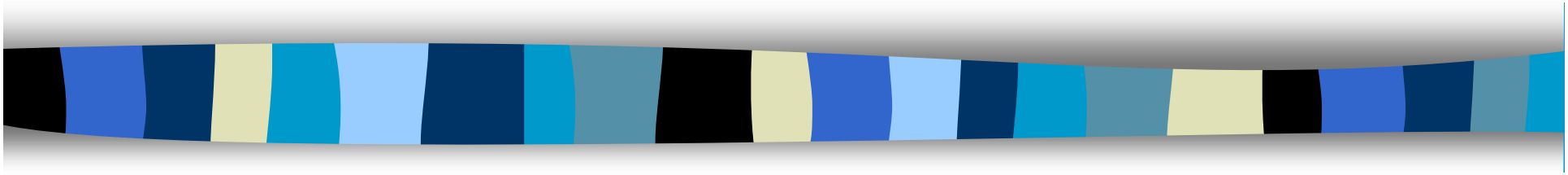
The Future

When	Innovation	Enables	Era	"Native" Applications	Organization Impact
1993-7	World-Wide-Web	Easy dissemination of Information	Information Society	Advertising e-Commerce Database access	BPE/BPR inside organizations
2015→	Blockchains & Distributed Ledgers	Agreement on shared information & actions Stateful Shared State	Joint-Action Society	Identity records Exchanges Chains of custody Complex workflows Insurance	BPE/BPR across organizations.

Exercises

1. List the sequence of events involved in acceptance of new blocks by nodes.
2. Describe the mathematical problems used in Bitcoin for PoW.
3. What is the total maximum number of Bitcoin to be issued? How many have been issued so far? What will miners be paid after the maximum is reached?
4. What is a wallet? What is the difference between wallets held on personal machines versus wallets held on an exchange?
5. List the major Bitcoin exchanges and their country of location. Is there a major exchange which has not been hacked at least once?

Thank you!



peter.mcburney@kcl.ac.uk