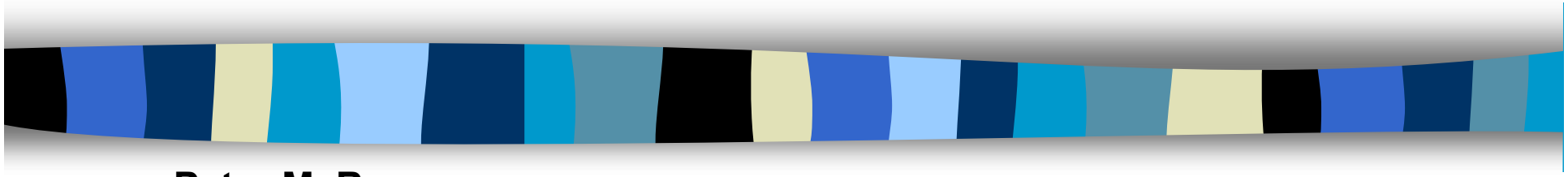
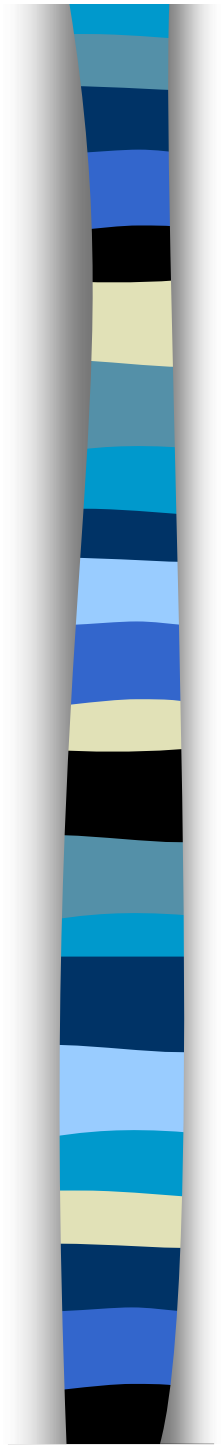
7CCSMDLC: Distributed Ledgers & Cryptocurrencies

Lecture 10: Some Case Studies



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

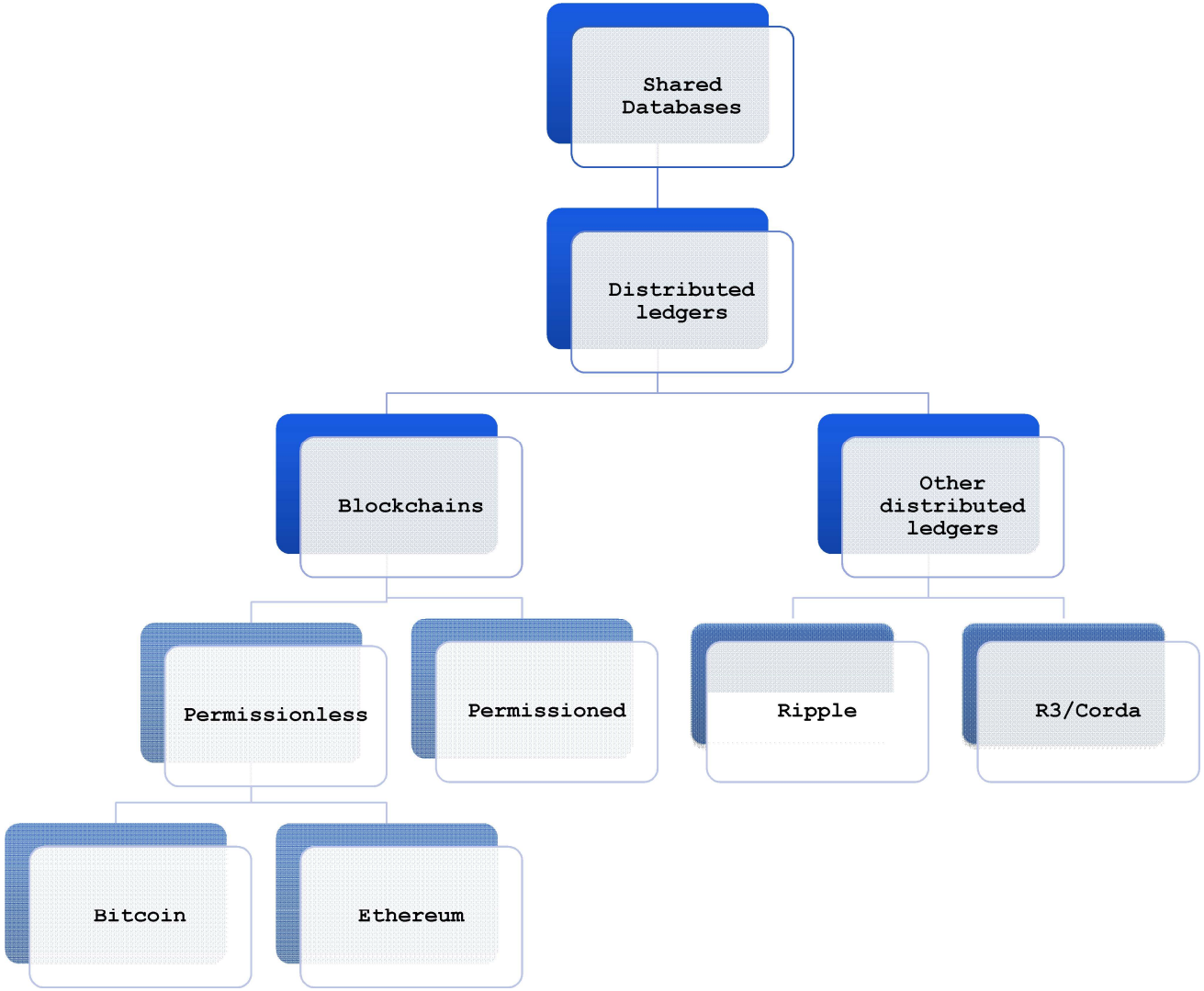
Email: peter.mcburney@kcl.ac.uk
Bush House Central Block North – Office 7.15



Outline

- Summary of features and benefits of DLT
- Applications of DLT technologies
  - Ignoring cryptocurrencies
- Challenges

Shared databases



Comparison of WWW and Blockchains

Launch period	Innovation	Enables	Era	"Native" Applications	Organization Impact
1993-7	World-Wide-Web	Easy dissemination of Information	Infor-mation Society	Advertising e-Commerce Database access	BPE/BPR inside organizations
2015-	Blockchain and Distributed Ledgers	Agreement on shared information & actions Stateful Shared State	Joint-Action Society	Identity records Chains of custody Insurance	BPE/BPR across organizations

DLTs – Evolving thinking over last several years

Distributed Ledger Technologies were considered appropriate for:

- First, 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.

What are main benefits of DLT

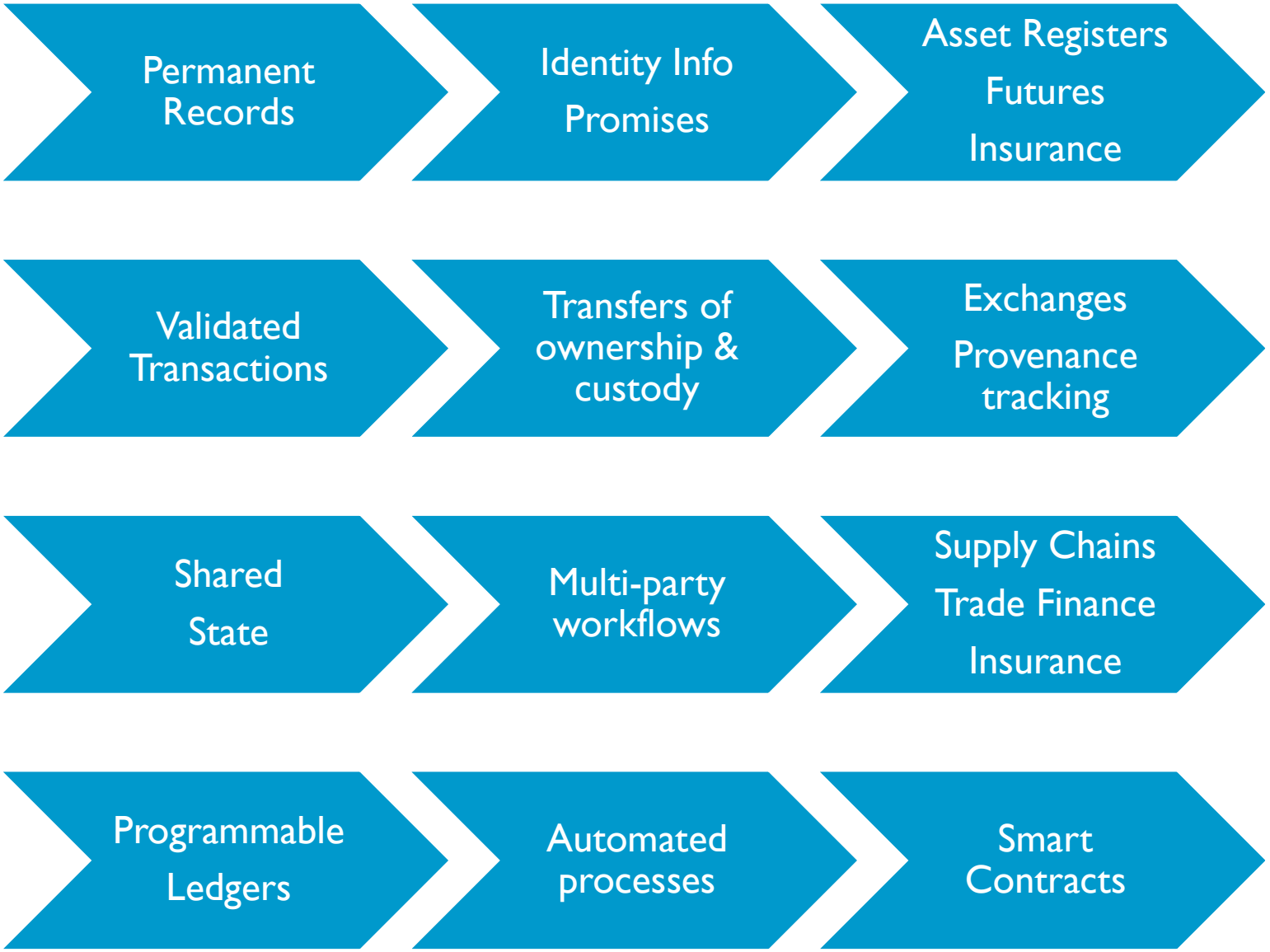
- Shared state
  - Different organizations needing the same data
- Stateful (history kept)
- Stored data is effectively immutable
  - It cannot be altered surreptitiously
  - It is *adamantine*
- Unique allocations & co-ordinated allocation
  - Solution to double-spend problem
- Witnessing of transactions
- In case of transfer of digital assets, settlement is immediate.

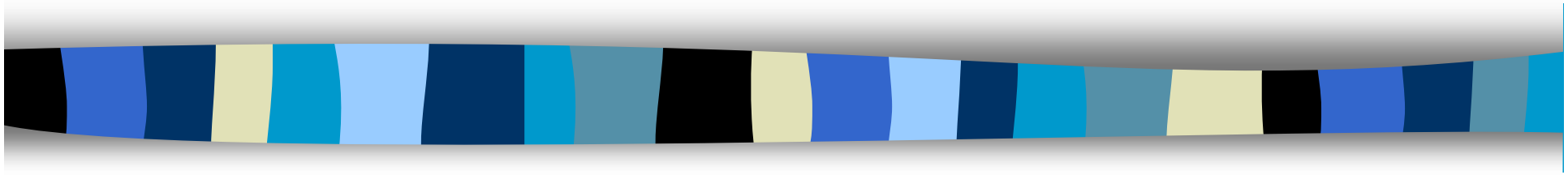
What are major use cases

These are based around the main benefits:

- Shared state
  - Cross-organizational workflows
- Stateful (history kept)
  - Provenance tracking
- Immutability of stored data
  - Permanent records/Provenance tracking
- Unique allocations /co-ordinated allocation
  - Solution to double-spend problem
- Witnessing
  - Multi-party aggregation
- Immediate settlement for digital assets
  - This has enabled new services, such as *Flash Loans.*

DL features and enabled applications





Applications

Education Degrees & Certificates

- Who
  - French Ministry of Education
  - Gradbase (was a spinout from Imperial College)
- Why
  - To enable employers to easily verify qualifications
  - To prevent fraudulent claims of qualifications
- How
  - Degree registered on blockchain
  - Code or RFID tag created which candidate can put on CV
  - Potential employers can verify existence & details
- Benefits
  - To make verification faster and easier
  - To prevent fraudulent claims of qualifications
- Challenges
  - Changing existing work processes
  - Getting universities etc to agree to register.
- Effectively, the service acts as a Stampery
  - Verifying that a certain degree existed at a certain date.

KYC/AML

- What
  - Put KYC/AML information on blockchain
  - Know Your Customer/Anti-Money Laundering Regulations
- Who
  - Many banks, financial institutions, private equity companies
  - Start-ups (eg, KYC Legal)
- Benefits
  - KYC/AML checks are more efficient & faster
  - Reduction in duplication of work
- Challenges
  - Different legal requirements in different sectors/ different applications.

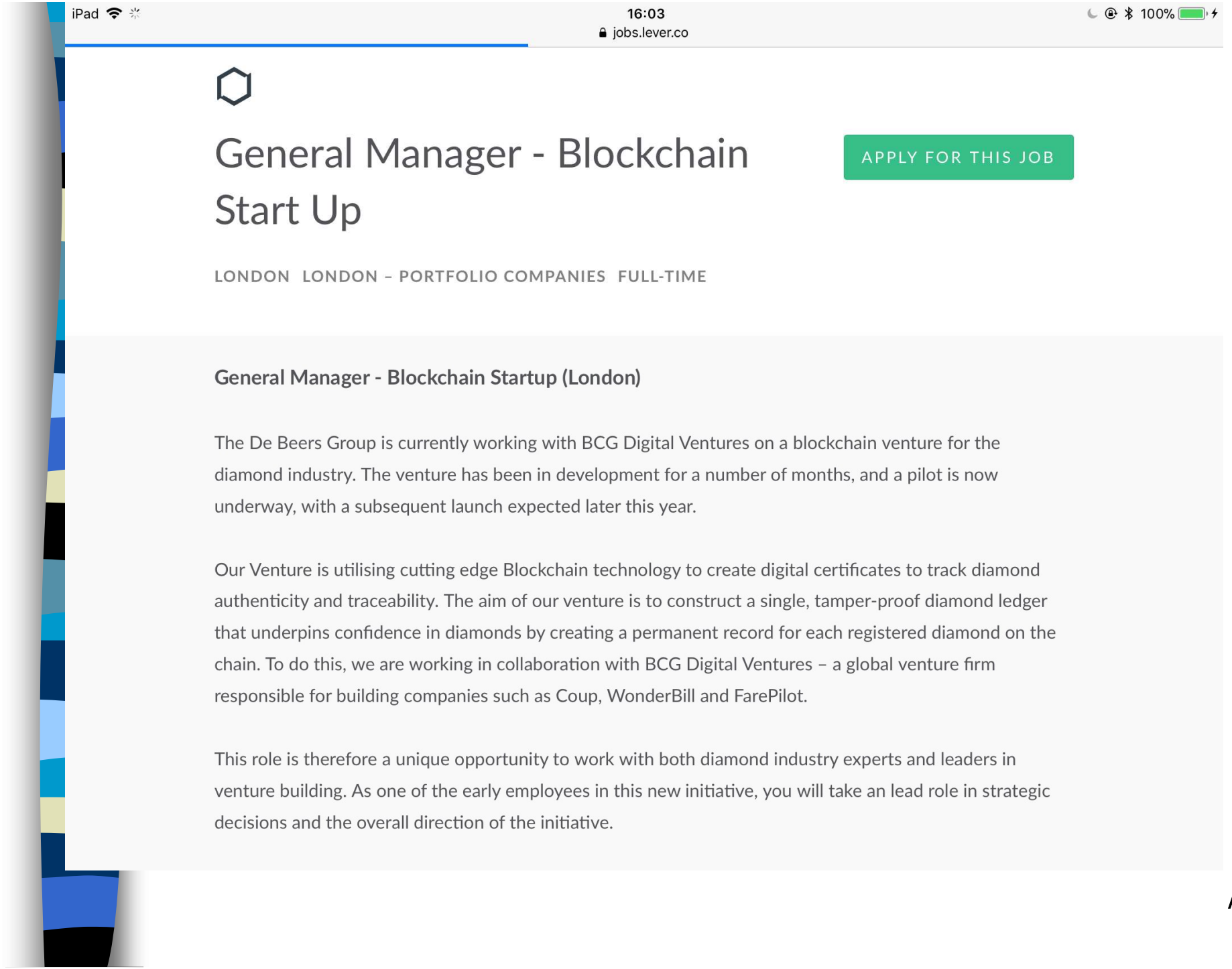
Land Registers

- Who
  - Government land registers in different countries
- Motivations
  - To enable fast, efficient access to land-ownership information
  - To create tokens associated with each piece of land
- Expected Benefits
  - Faster, cheaper, easier access to land registry data
- Challenges
  - Existing registers very large
  - Registers may record ownership (Freehold) and custody (Leasehold)
  - Existing register may only be a register of transfers (eg, UK)
  - Many users not technically sophisticated
    - Individual homeowners and small businesses.

Diamonds

everledger

- Who
  - Everledger
  - DeBeers diamond company
- Motivations
  - To verify sources of diamonds
  - To guard against blood diamonds & synthetic diamonds
- How
  - measurements, photos, videos of diamonds taken (both rough & refined)
  - Hash placed on blockchain
  - Certificates of source and authenticity
- Expected Benefits
  - Certification of ownership Verification of sources
  - Tracking of ownership & custody
  - Tracking of provenance
- Challenges
  - Linking stone to digital representation indelibly
  - Industry practices very traditional
  - Retail sector very fragmented
- Note: Everledger also doing fine art.


iPad
16:03
jobs.lever.co
100%
General Manager - Blockchain Start Up
APPLY FOR THIS JOB
LONDON LONDON – PORTFOLIO COMPANIES FULL-TIME
General Manager - Blockchain Startup (London)
The De Beers Group is currently working with BCG Digital Ventures on a blockchain venture for the diamond industry. The venture has been in development for a number of months, and a pilot is now underway, with a subsequent launch expected later this year.
Our Venture is utilising cutting edge Blockchain technology to create digital certificates to track diamond authenticity and traceability. The aim of our venture is to construct a single, tamper-proof diamond ledger that underpins confidence in diamonds by creating a permanent record for each registered diamond on the chain. To do this, we are working in collaboration with BCG Digital Ventures – a global venture firm responsible for building companies such as Coup, WonderBill and FarePilot.
This role is therefore a unique opportunity to work with both diamond industry experts and leaders in venture building. As one of the early employees in this new initiative, you will take an lead role in strategic decisions and the overall direction of the initiative.

Personalized access to health records – Dovetail

- Dovetail Lab (blockchain startup, now owned by Emis)
- What
  - Personal health records accessed via blockchain
- Why
  - To enable people to grant access rights to their health records on a case-by-case basis and without revealing the records
- Benefits
  - To ease and speed approved sharing of personal health records
- Challenges
  - Getting access to health record data
  - Working with NHS
  - Consumer adoption.

DOVETAIL

Real-time insurance: InsurWave

InsurWave is a blockchain consortium led by Maersk
- Maersk, EY, MS Amlin, Guardtime, *et al.*

- Goal
  - Real-time automated insurance adjustment
  - Using blockchain & smart contracts

- Why
  - New insurance products
  - Real-time calibration of risks & costs

  (eg, for ships in war zones)

- Challenges
  - Balance between sharing & privacy
  - No platform quite suitable.

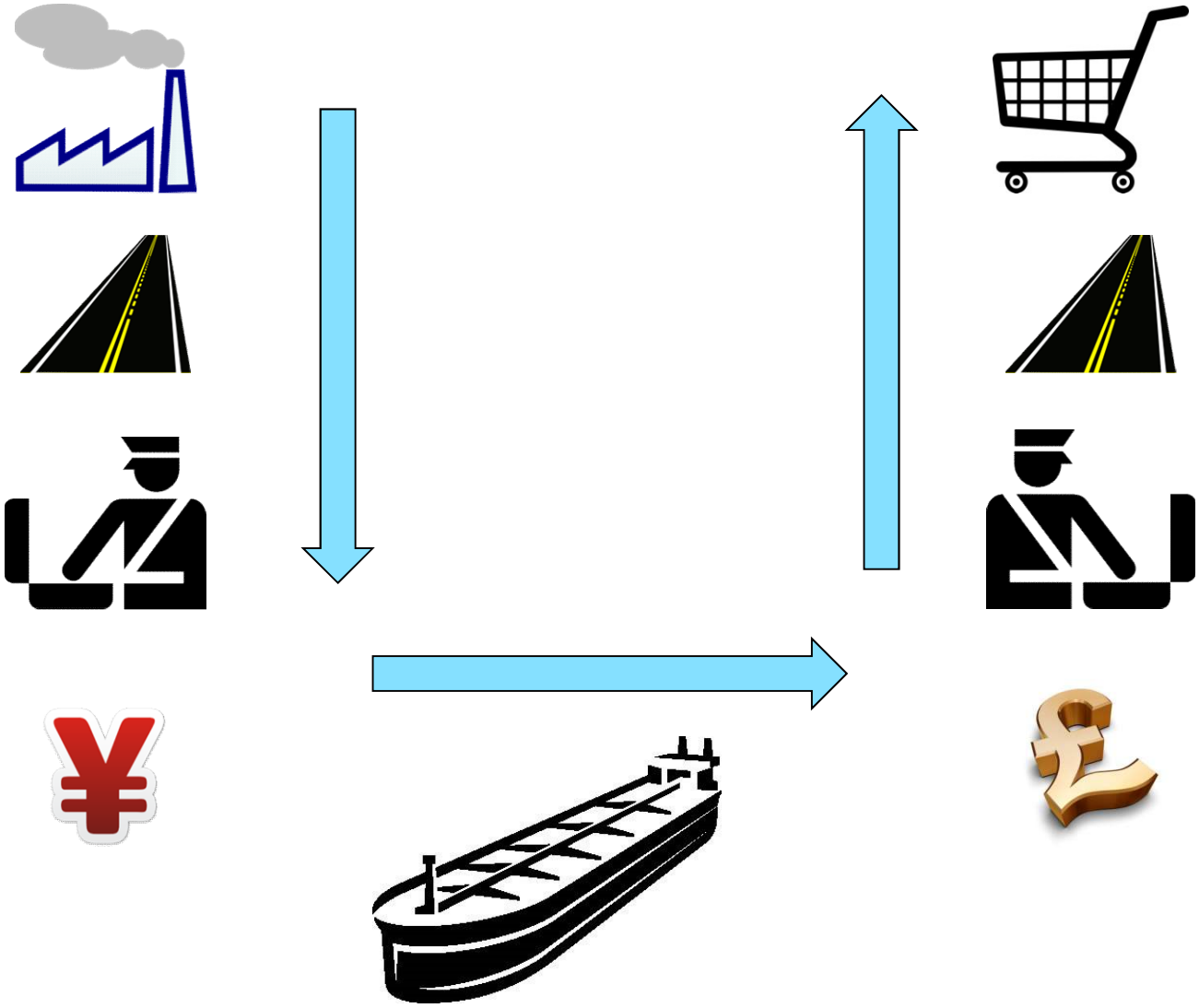
MAERSK

MS Amlin

INSURWAVE

Anti-Piracy Measures:
Djibouti Code of Conduct eligible countries

Application: Trade Finance



Post-trade workflows for energy commodity trades

- Vakt
  - www.vakt.com
  - Consortium of banks, energy companies & energy commodity traders

- Goal
  - To share data needed for management of post-trade logistics activities

- Why
  - To enter shared data just once
  - To eliminate reconciliation
  - To solve double-spend for resource
  - To monetize the data

- Challenges
  - Balance of data sharing with privacy
  - No platform was exactly right.

RegTech – Regulation Technology

- Who
  - Financial Conduct Authority UK
  - Proof of Concept with Santander
- Why
  - Reduce regulatory burden
  - 50K regulated entities
  - All sending raw data every quarter
  - FCA needs to analyze
- What
  - Put analysis programme on the blockchain
  - Regulated entities execute locally
  - Send results back to FCA

- Challenges
  - Ensuring consistent semantic understanding of data and entities
  - SMEs not all technically sophisticated.

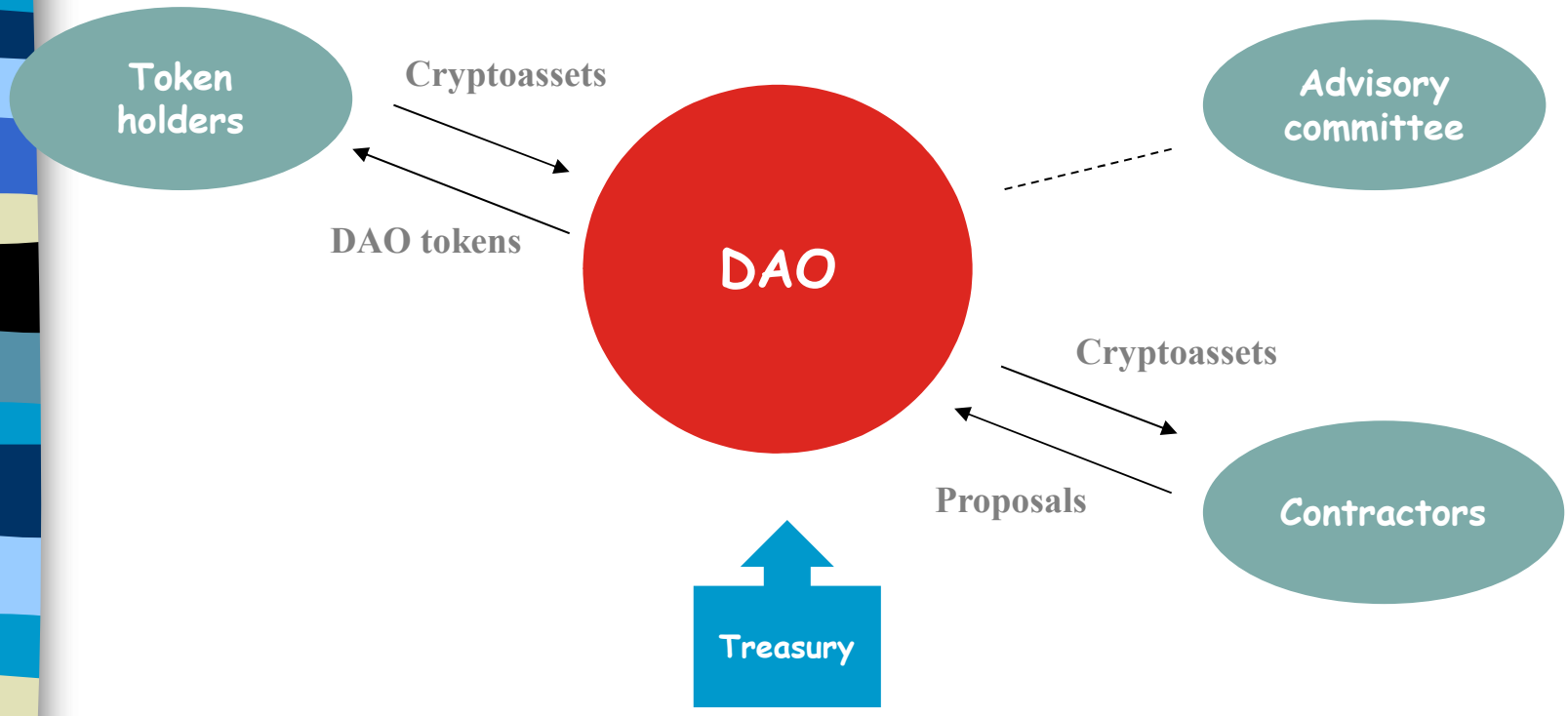
DeFi – Decentralized Finance

- DeFi is founded on the premise that financial services can be delivered without having a centralised operator
  - Smart contracts are used to facilitate P2P provision of financial services without any centralised party intermediating transactions or arrangements

- DeFi has proven popular
  - in exchanges (also known as DEXs)
  - where participants swap cryptoassets directly against one another
  - in yield farming arrangements (where strategies such as automated market making and lending have generate yields on stored cryptoassets) and
  - in payments, insurance and derivatives

- Popular DeFi applications include:
  - UniSwap, Aave, Compound, MakerDAO, MetaMask, Nexus Mutual.

Decentralized Autonomous Organizations (DAOs)



What are DAOs?

- Novel type of technology-mediated organisational structure involving multiple participants
  - A DAO typically uses or facilitates the creation & maintenance of blockchain, smart contracts, or open source software systems

- They are a way of organising people, or social coordination or collaboration technology, with potential to reduce transaction costs
  - The community members are usually anonymous

- The term “DAO” does not necessarily represent any particular type of organisational structure

- Some DAOs include a recognised legal form or incorporated entity.

Where are DAOs commonly used?

- DAOs are important in the context of cryptocurrency tokens and decentralised finance ecosystems
- Many are involved with the development of code that is used to create smart contracts
- DAOs usually employ smart contracts to automate or program some elements of their internal activity. Often those smart contracts are open-source and are themselves deployed to open-source blockchain systems
- Examples of DAOs include social structures or organisations involving multiple participants created for investment purposes - including to invest in or trade cryptotokens and non-fungible tokens (NFTs), as well as fundraising, crowdsourcing or charitable purposes
- Many DAOs are also involved in software engineering — developing, modifying and maintaining open source software infrastructure (such as blockchain systems or decentralised finance applications), and in relation to the governance of these developments.

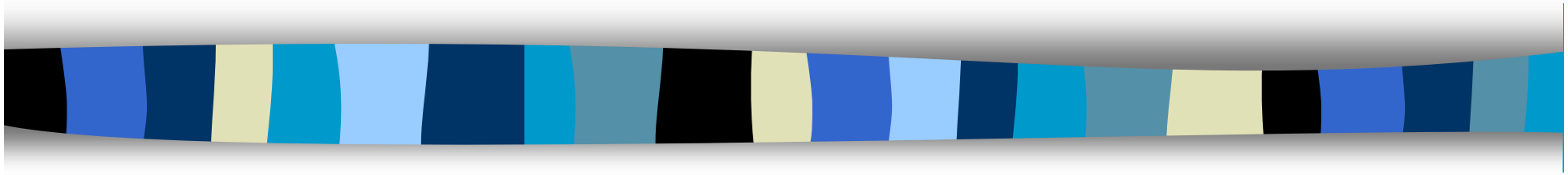
DeFi Example: Aave

- Launched: November 2017, as ETHLend
  - Rebranded as Aave (Finnish for “ghost”) in September 2018
  - Founder & CEO: Stani Kulechov
- A decentralised protocol on Ethereum to allow lending and borrowing of cryptocurrencies, without a centralised intermediary
  - Users deposit funds into liquidity pools, which can be then lent out to other users
  - Borrowers pay interest on loans, and Lenders receive interest
  - Borrowers require collateral in cryptocurrency
    - Collateral not needed for *Flash Loans* (borrowing and repayment in same transaction block)
- All managed by smart contracts
- Governance by the community of token holders, via a governance token AAVE (launched October 2020)
  - In March 2025: 183 K token-holders (maybe not all distinct people)
- Currently holding pool of some US$ 7.1 billion (equivalent)
- Aave also has a stable coin GHO (launched August 2022)

Insurance mutual pool

Nexus Mutual

- Who
  - Nexus Mutual (UK start-up)
- What
  - Mutual insurance organization running over blockchain
  - Providing smart contract cover
  - Earthquake cover
  - Smart contracts to automate claims assessment & payment
- Why
  - To automate insurance (a DAO for insurance)
  - To harness wisdom-of-the-crowd for insurance
- Challenges
  - Regulation (UK Prudential Regulation Authority)
  - May need national licences to operate
  - Quantifying risk for novel products.

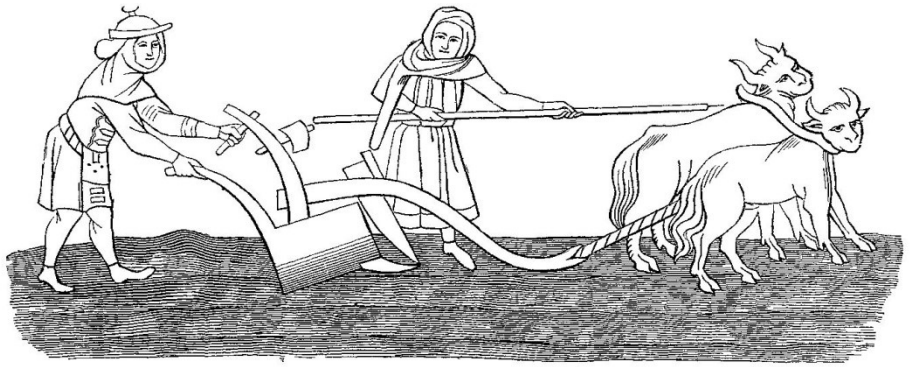


Challenges

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



Implementation Challenges

- Organizational challenges
  - Managing stakeholders
  - Managing revocation and cancellation
  - Business Process Engineering/Re-engineering
    - Especially for inter-organization workflows
  - Governance of the Distributed Ledger
- Legal and Regulatory aspects
- Technical
  - User friendliness
  - Managing multiple DLs
  - Integration with legacy systems
  - Production readiness
    - eg, security, compliance & monitoring requirements, analytics capabilities
    - William Mougayar: 18-24 months to resolve!

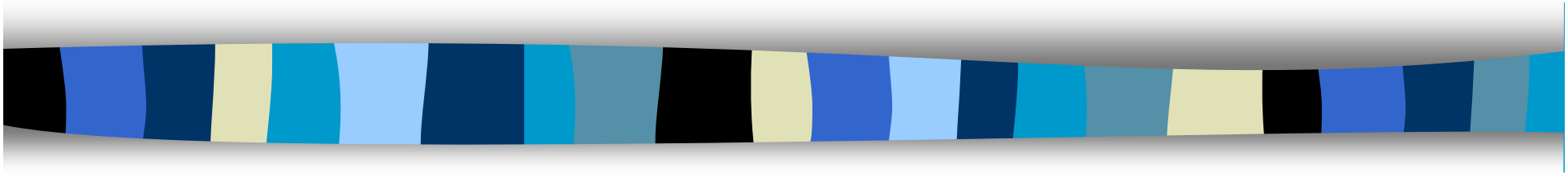
Key Technical Challenge: Scaling

- Current DLT Blockchain not adequate for most financial applications
  - Number of Bitcoin transactions per day: under 300K
  - Credit card transactions: 300 million per day (100 billion pa)
- How to scale?
- One possible solution: **Sharding**
  - Does everyone have to witness every transaction?
  - Split the space of accounts into sub-spaces
  - Each sub-space gets its own set of witnesses (validators)
- **Side-chains**
  - Private blockchains with occasional posting to a larger chain (eg, Bitcoin)
  - Everledger (diamond blockchain).

From smart objects to smart societies

- Smart contracts
  - eg, self-executing futures contracts
- Programmable combinations
  - of existence records, smart contracts, transaction records, etc
  - for multiple participants
- Autonomic and self-organizing systems
  - Self-* systems (self-star systems)
    - » self-monitoring, self-repairing, self-optimizing, etc
  - Example in mobile telecoms: *"No G after 5G!"*

Thank you!



peter.mcburney@kcl.ac.uk