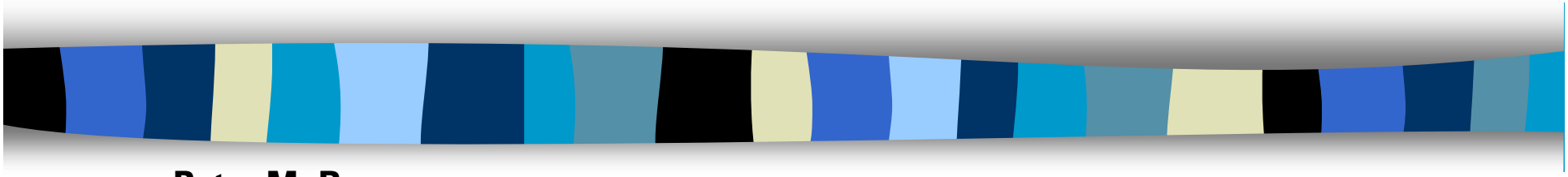
7CCSMDLC: Distributed Ledgers & Cryptocurrencies

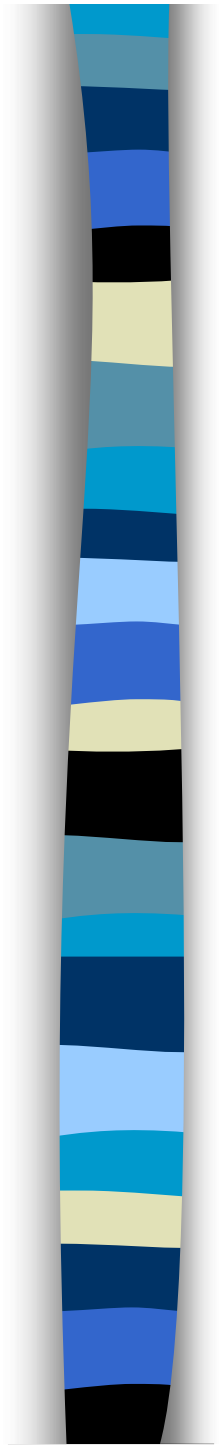
Lecture 7: Applications and Ecosystems



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

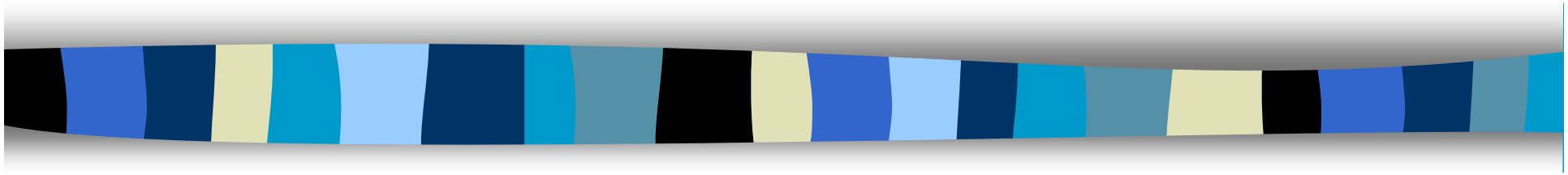
Email: peter.mcburney@kcl.ac.uk
Bush House Central Block North – Office 7.15

2020



Outline

- Applications of blockchain technolgy
  - Ignoring cryptocurrencies
- Challenges
- Guidance on the Group Project



Applications

DLTs – Evolving thinking over last few 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.

What are main benefits

- Shared state
  - Different organizations needing the same data
  - Eliminates the need for data reconciliation between companies
- Stateful (history kept)
- Immutability of stored data
- Unique allocations /co-ordinated allocation
  - Solution to double-spend problem
- Witnessing of transactions
- Immediate settlement for digital assets.

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.

Types of Applications

- Record keeping
  - Identity records
- Records of transactions
  - Exchanges of ownership of assets
  - Chains of custody
  - A global protocol
- Promises and commitments
  - If X happens, then I will do Y
  - eg, Futures & options contracts, trade finance
- Smart contracts
  - Self-executing programs
  - A local protocol.

Non-blockchain technical solutions exist

- For instance,
  - Centralized databases with Public-Key-Identity and secure communications

- But there are non-technical issues with this solution

  - Who holds and manages the central database?
  - Do you trust them?
  - Can they hold this database legally (ie, does it breach anti-collusion laws?)
    - Eg, some jurisdictions may not allow sharing of prices.
  - Will they require payment?
  - How can you secure the central database against attack?
  - How can you ensure the host of the central database does not exploit the data commercially?
  - How do you ensure that only the parties to a transaction see the data for that transaction, or even know of its existence?

List of applications

- Identity records
  - France Education Ministry / Gradbase
  - KYC/AML
  - Land registries
- Provenance
  - Everledger / DeBeers
- Personalized access to med records
  - Dovetail Lab (now EMIS)
- Corporate governance
  - Crowdcube explored
- Insurance
  - Real-time insurance adjustment - InsurWave
  - DAO for insurance pool - NexusMutual
- Trade flows
  - Vakt / Komgo
- RegTech
  - FCA.

Education Degrees & Certificates

- Who
  - French Ministry of Education
  - Gradbase (www.gradba.se) (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
- Expected 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.

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 ?)
- Expected Benefits
  - KYC/AML checks would be more efficient & faster
  - Reduction of duplication of work
- Challenges
  - Different requirements in different sectors/ different applications.

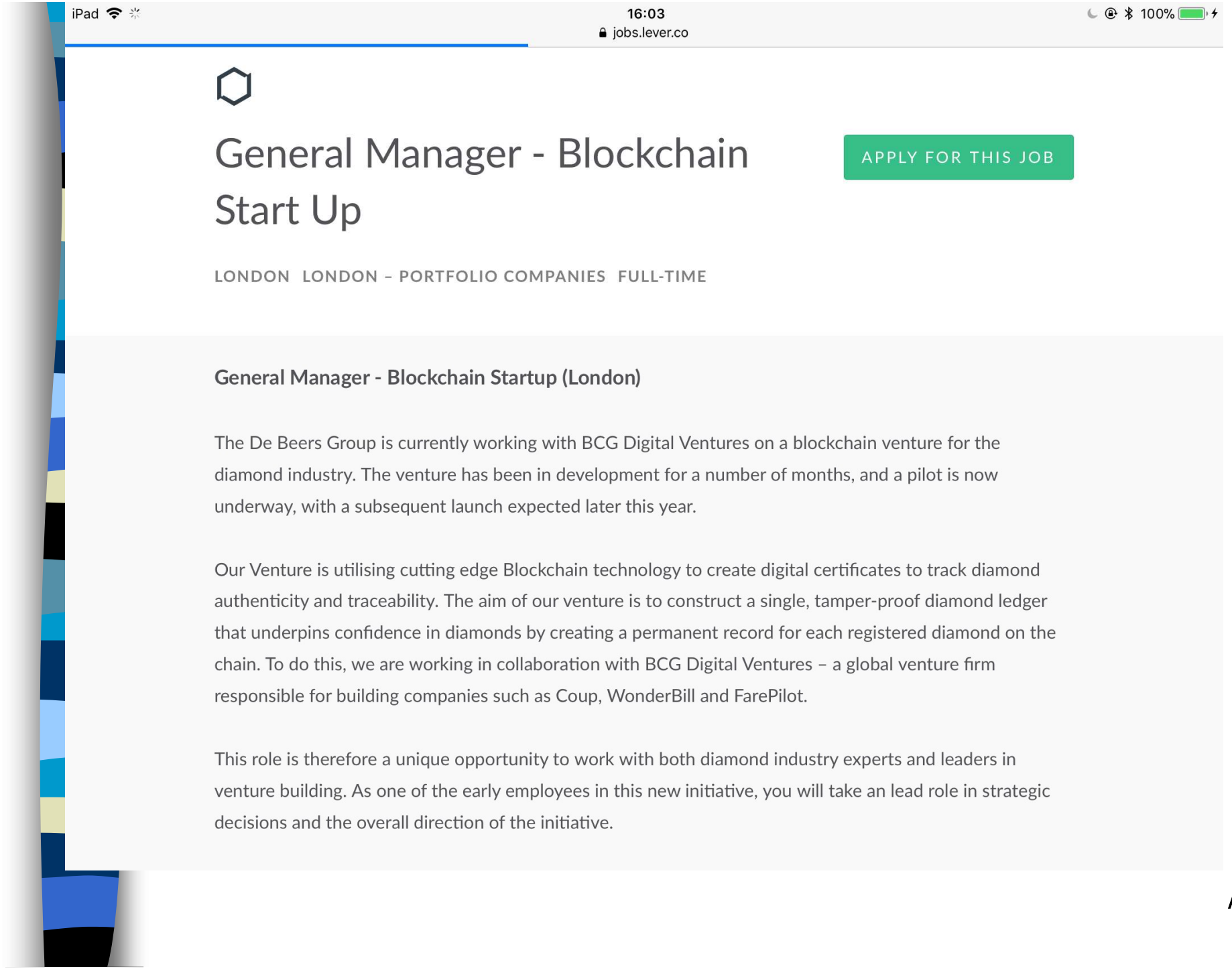
Land Registers

- Who
  - Government land registers
- Motivations
  - To enable fast, efficient access to land-ownership information
- Expected Benefits
  - Faster, cheaper, easier access to land registry data
  - Monetization of land assets via tokenization
- 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
- 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 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/EMIS

- Who
  - Dovetail Lab: www.dovetaillab.com (now 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
- Expected Benefits
  - To ease and speed approved sharing of personalhealth records
- Challenges
  - Getting access to health record data
  - Working with NHS
  - Consumer adoption.

DOVETAIL

Smart contracts for shareholders rights – prototype

- Who
  - Crowdcube
  - UK's largest portal for crowd funding

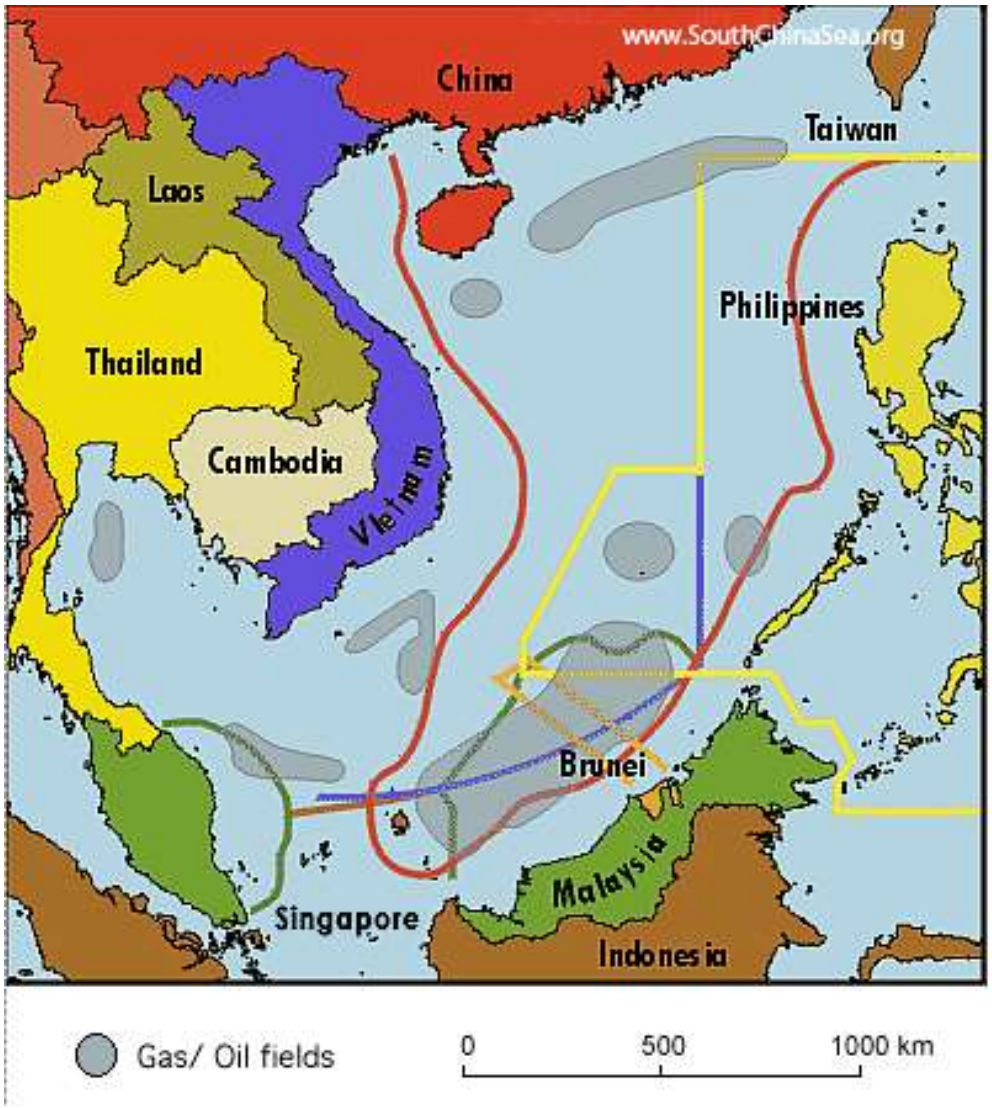
- What
  - Voting via blockchain
  - Smart contracts for shareholder rights
  - To automate shareholder voting for SMEs
- Why
  - Current system messy (paper + Excel)
- Challenges
  - Ensuring smart contracts are reliable and unhackable
  - Many users will not be technically sophisticated.

Real-time insurance recalibration

- Who
  - InsurWave (insurwave.com)
    - Consortium of Maersk, EY, MS Amlin, Guardtime, etal
- What
  - Real-time automated insurance adjustment
  - Uses GPS, 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.

Example: Competing claims in South China Sea



Insurance mutual pool

- Who
  - Nexus Mutual (UK start-up)

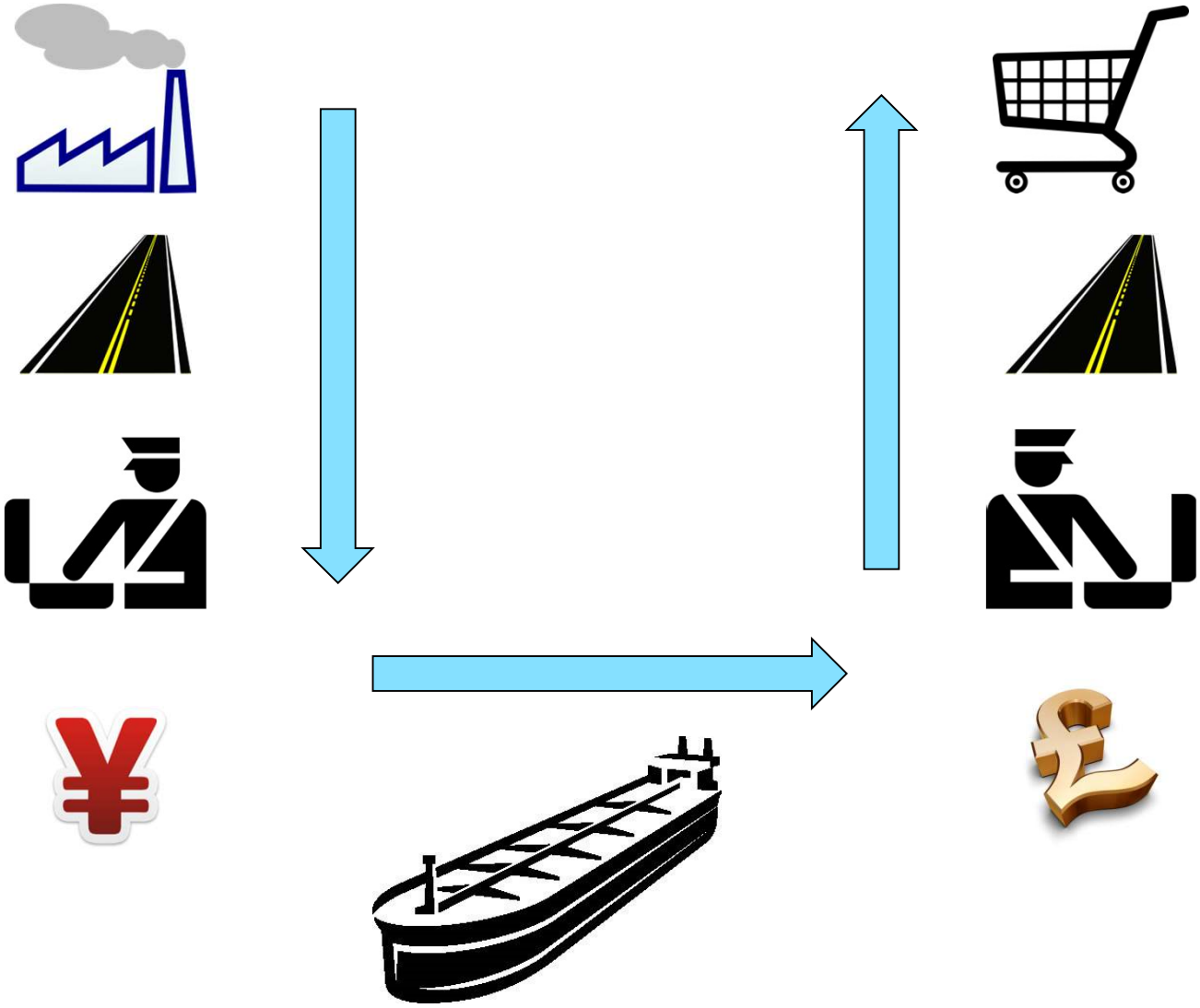
Nexus Mutual

- 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.

Application: Trade Finance



Post-trade workflows for energy commodity trades

- Who
  - Vakt (vakt.com)
  - Consortium of banks, energy companies & energy commodity traders
- What
  - Blockchain platform for management of post-trade activities
- Why
  - To enter shared data just once
  - To monetize data
  - To automate activities
  - To solve double-spend for resources
- Challenges
  - Balance of data sharing with privacy
  - No platform is exactly right.

VAKT

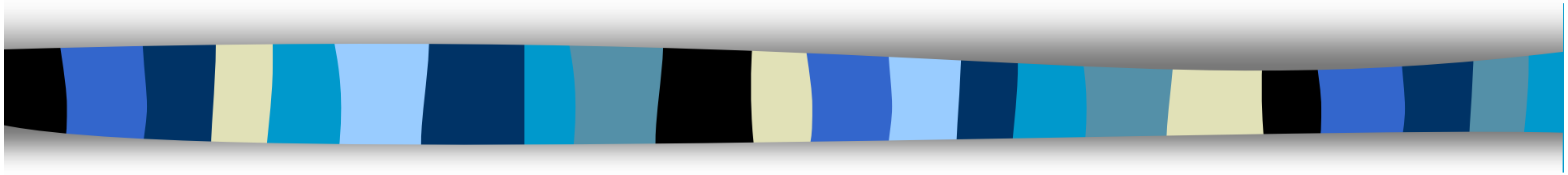
Shell

MERCURIA
ENERGY GROUP LTD

ING BANK

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.

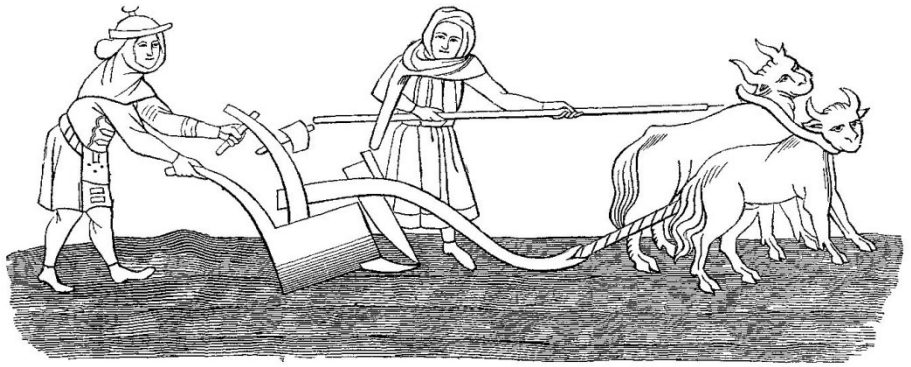


Challenges

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 (eg, Zerocash protocol)

- 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: around 350K (max 450K)
  - 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-monitoring, self-repairing, self-optimizing, etc
  - Example in mobile telecoms: *"No G after 5G!"*

Comparison of WWW and Blockchains

Launch period	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
2018-2025	Blockchain & Distributed Ledgers	Agreement on shared information & actions Stateful Shared State	Joint-Action Society	Identity records Chains of custody Insurance	BPE/BPR across organizations

Team Projects

- You are asked to explore a topic in depth.
- You need to make a brief presentation on it (5 minutes) and write a technical report.

- The technical report should be written in narrative form (ie, sentences, not bullet points) and describe what you did. Use of diagrams and tables is encouraged.
- The report should be about 10 pages long (ie, about 3000 words), not including the cover page, contents page, the references and any appendixes.
  - If you develop code, please include a listing in an appendix.

- The cover page should include the project title, your team name, and the names & K-numbers of all the team members.

Team Project Deadlines

Deadlines:

- Team presentations in lecture on 26 March 2020 or by video.
  - 5 minutes
  - 1 person to present
- Team Reports due: Monday 30 March 2020 at 16.00
  - Submit 1 report per team on KEATS
- Team reports are marked (see next page)

Team Reports (due 30 March at 16.00)

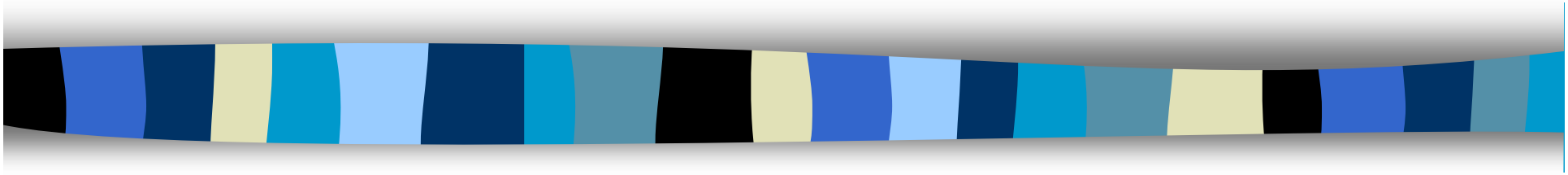
- Marks allocated: 20% of the module total

- I am looking for:
  - Evidence that you explored a topic in detail or developed a prototype
  - Criteria for assessment:
    - Rigour
    - Clarity
    - Initiative & Creativity
    - Action-orientation

  - Justify your assumptions, your conclusions and/or your design choices
  - You should also include a summary of what your team learnt in doing this project.

  - This is a technical report
    - ie, it is not a presentation, and not an essay.

Thank you!



peter.mcburney@kcl.ac.uk