COMSM0019: Internet Economics and Financial Technology

Lecture 18: Blockchain & Cryptocurrencies II

John Cartlidge

john.cartlidge@bristol.ac.uk

Bitcoin: BTC

Bitcoin Blockchain
1st Generation DLT

- Transactions

Ether: ETH

Etherium Blockchain
2nd Generation DLT

- Transactions
- Smart contracts / DApps

ADA: ADA

Cardano Blockchain
3rd Generation DLT

- Transactions
- Smart contracts / DApps
- Multi-layer / Efficient

There are now three generations of distributed ledger technology (DLT). These are examples of some of the most popular in each generation. The true "*value*" of these technologies is in the blockchain protocols that underlie the coins, not the price the cryptocurrency is currently trading at.

Not all DLTs are created equal…

Generation 1: Bitcoin

Initial release Jan 2009

- Pros:
  - Low-cost transactions (no intermediary profits)
  - No central government control (a *libertarian* currency)
- Cons:
  - Energy intensive (proof-of-work)
  - Initially designed for record keeping / transactions only, so hard to build more complexity (such as smart contracts) on top of the framework

Generation 2: Etherium

Released July 2015

- Designed to be more than just a platform for transactions
- Developments:
  - **Smart contracts:** Solidity, a Turing Complete contract-oriented programming language for smart contracts runs on the Etherium Virtual Machine (EVM)
  - **Decentralised applications (DApps):** open-source software platforms implemented on the blockchain, each with an individual token

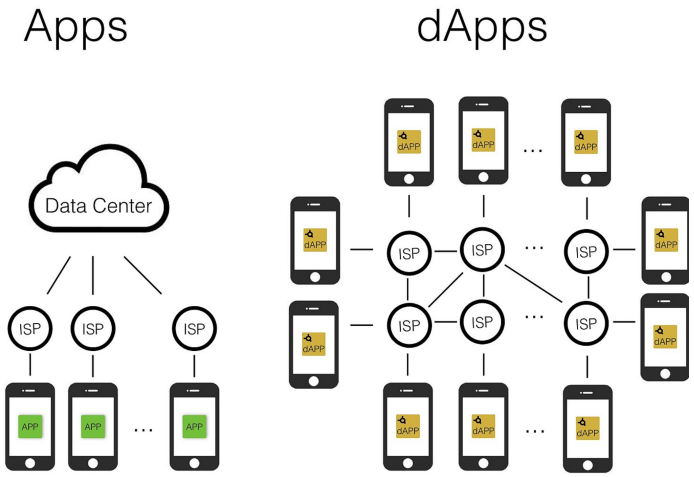
https://www.ethereum.org/

3rd Generation: Cardano

Founded in 2015, ADA token launched Sep 2017. Still under development.

- Third generation blockchain designed from the ground-up to solve problems observed in earlier generation DLTs
  - Use of academics and peer-review for design process (for the first time)
- Developments:
  - **Multi-layer**: separate token/transactions from code/contracts
  - **Efficient and secure**: proof-of-stake (Ouroborous protocol)
  - **Permissioned and Permisionless:** enables private networks

ADA: ADA
Cardano Blockchain
3rd Generation DLT



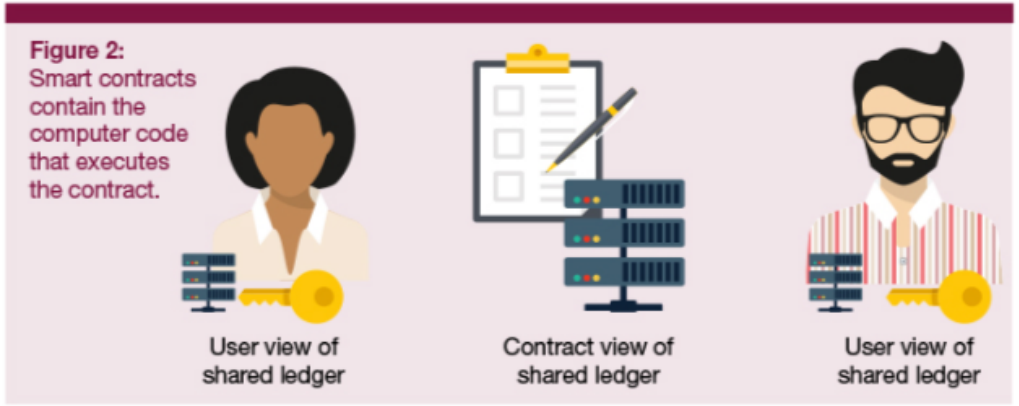
Smart Contracts & Distributed Apps

Self-executing contracts with terms of agreement written into code which exists in the distributed blockchain

What is a *smart* contract?

- If a blockchain is the database, then the smart contract is the application layer that makes much of the promise of block chain technology a reality
- **Smart contracts** are contracts whose terms are recorded in code instead of legal language.
- Most conventional contracts have no direct relationship with the code that executes them
- In many cases the paper contract is archived, and the software will execute an approximation of the contract's terms written in computer code
- A smart contract is useful when machines, companies or people want to create a digital agreement, with cryptographic certainty that the agreement has been honoured in the ledgers of all parties to the agreement

Further Reading: https://github.com/ethereum/wiki/wiki/White-Paper#applications



Example: smart contract/DApp for Airbnb rentals

- An electronic door-lock uses a smart contract to control the entry pin of a rental apartment
- When a holidaymaker books the apartment, they are issued with a unique door-entry pin code
- The smart contract views the ledger and only activates the pin code once the payment has been received, and only for the duration of the rental period
- Payment funds are only transferred to the owner when the pin code is first used by the holidaymaker
- If the contract allows a 90% refund for a no-show, then if the pin code is not used on the first day, it expires and 90% of the rental fee will be returned to the holidaymaker and 10% will be released to the owner.

(Not street-) smart contracts

Real-world contracts are not always as simple as following a “rule” that can be executed in code. This limits the potential applications for smart contracts.

(Not street-)smart contracts

A critique by Karen Levy: *"Smart contracts are based on a thin conception of what law does, and how it does it"*

Contracting Practice	Social Aim
Writing or acceding to *unenforceable terms*	Set expectations for future behavior, including behavior outside the formal purview of the contract
Writing or acceding to *purposefully vague* terms	Facilitate stable and flexible long-term relations
Willful *nonenforcement* of enforceable terms	Provide a strategic resource for operating "in the shadow of the law"

Summary:

- Smart contracts are useful for the more simple "transactional" contracts that are easily encoded as "rules" and we should see innovations in these areas;
- But, we should not over-hype their ability to replace our current legal frameworks around contract law. There are *natural limitations* to smart contracts

LEVY, Karen E. C.. Book-Smart, Not Street-Smart: Blockchain-Based Smart Contracts and The Social Workings of Law. **Engaging Science, Technology, and Society**, [S.l.], v. 3, p. 1-15, feb. 2017. ISSN 2413-8053. Available at: https://estsjournal.org/index.php/ests/article/view/107.

The DAO

The world's first Decentralised Autonomous Organisation (DAO)

The DAO

An idea with potential for a revolutionary business disruption!

- Decentralised business model for commercial and non-profit enterprises. Equity Crowdfunded, stateless, with no directors.
- Investors own DAO tokens that give rights to vote on projects. Money can be pulled by investors until time of first vote.
- Legal structure registered in Switzerland (law allows money to be taken from unknown source, as long as you know where it is going)
- Code of DAO open-source. Transparent: everything done by code, which anyone can see and audit

How did it perform? Did it change the world of business forever?

- **May 2016**: Largest crowdfunded campaign in history. $150m Ether value raised in 28 days (11,000 investors; equivalent to 14% of all ether tokens in existence)
- **Early June**: A paper showed security vulnerabilities (recursive calls) in The DAO
- **17th June**: Exploitation of vulnerability in The DAO code led to 1/3 of DAO funds being siphoned off. Thankfully, most of the money was recovered due to a 28 day holding period enforced in the smart contract. However, the incident led to a hard fork of Etherium (ETH) – the original fork containing hack was renamed Etherium Classic (ETC)
- **End 2016**: The DAO delisted from major cryptocurrency exchanges such as Kraken.

WARNING: The Wild West *Revisited*

Like many new technologies with high potential value, cryptocurrencies and DLTs are learning through failures, frauds, and fragile legislation. Tread with care until the landscape matures...

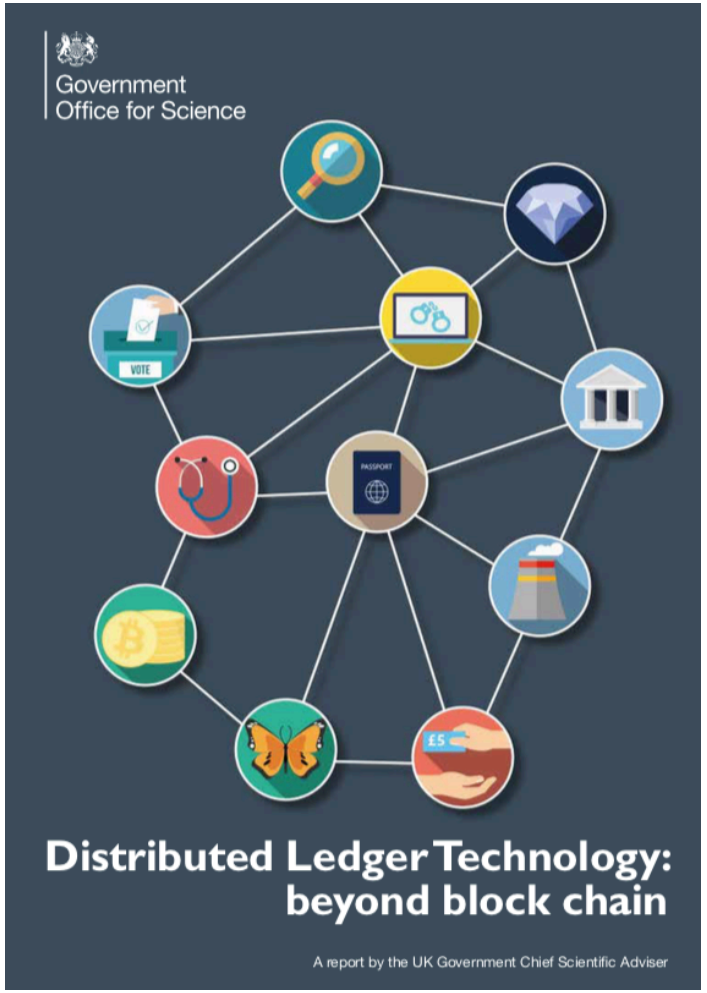
Smart contracts: applications & vision

Despite these “teething troubles”, there is still a lot of interest in smart contracts and DApps...

A UK Government report on future directions suggested a seemingly endless number of application areas, including…

- Food, Financial Services, Energy, Pharmaceuticals, Health, Aerospace, Aviation, Telecommunications, IT, Transport, Utilities, Agriculture, Oil and Gas…

It’s likely that smart contracts and DApps ***will*** have a significant impact in future years, but there will be many failures (and fraud) along the way

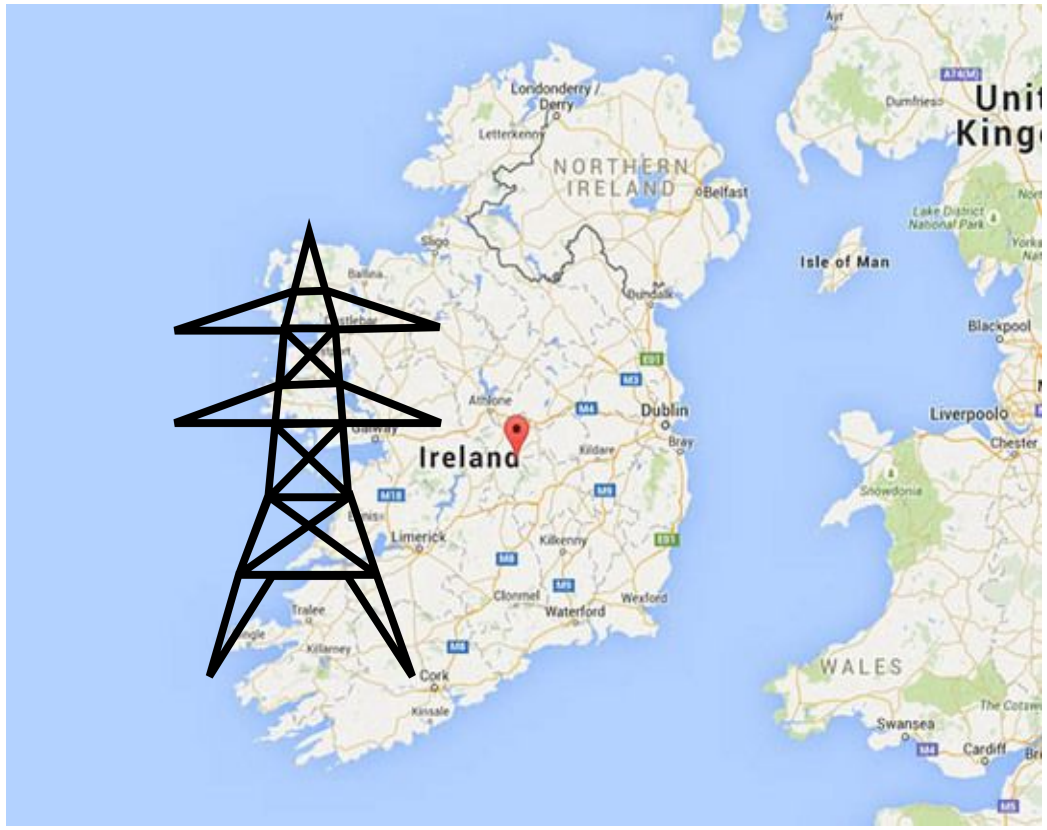


Proof-of-stake

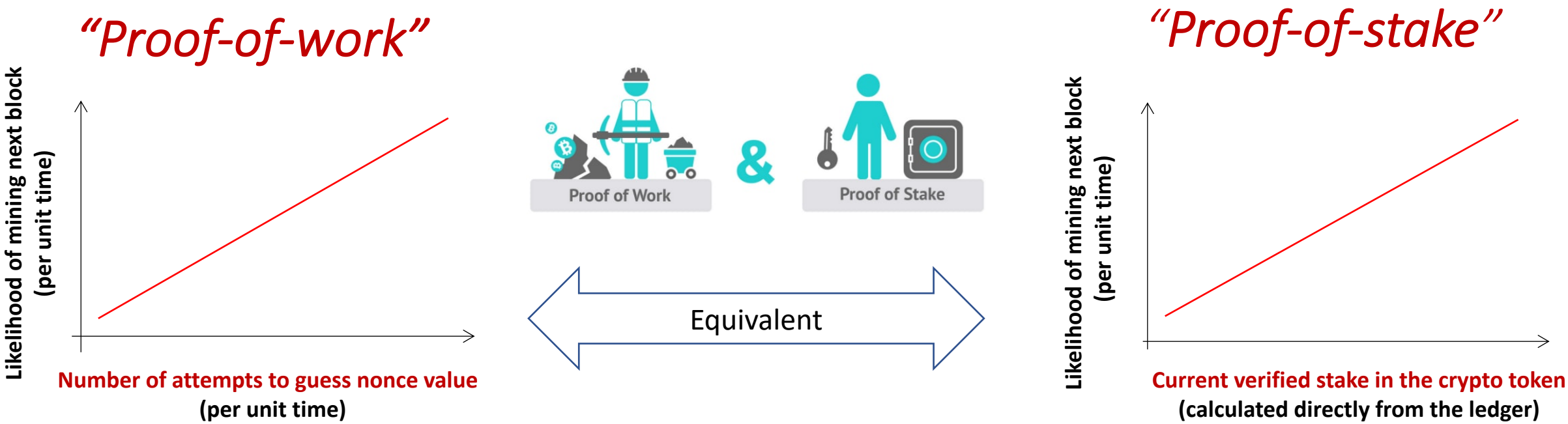
Who mines the next block?

An efficient alternative to proof-of-work

“Proof-of-work”



- Proof-of-work is extremely costly
- Global Bitcoin mining has an estimated energy usage equivalent to the country of Ireland
- Energy is used in proof-of-work purely so there is a fair process of selecting the next miner
- *Surely there must be a more efficient (and equally secure) alternative?*

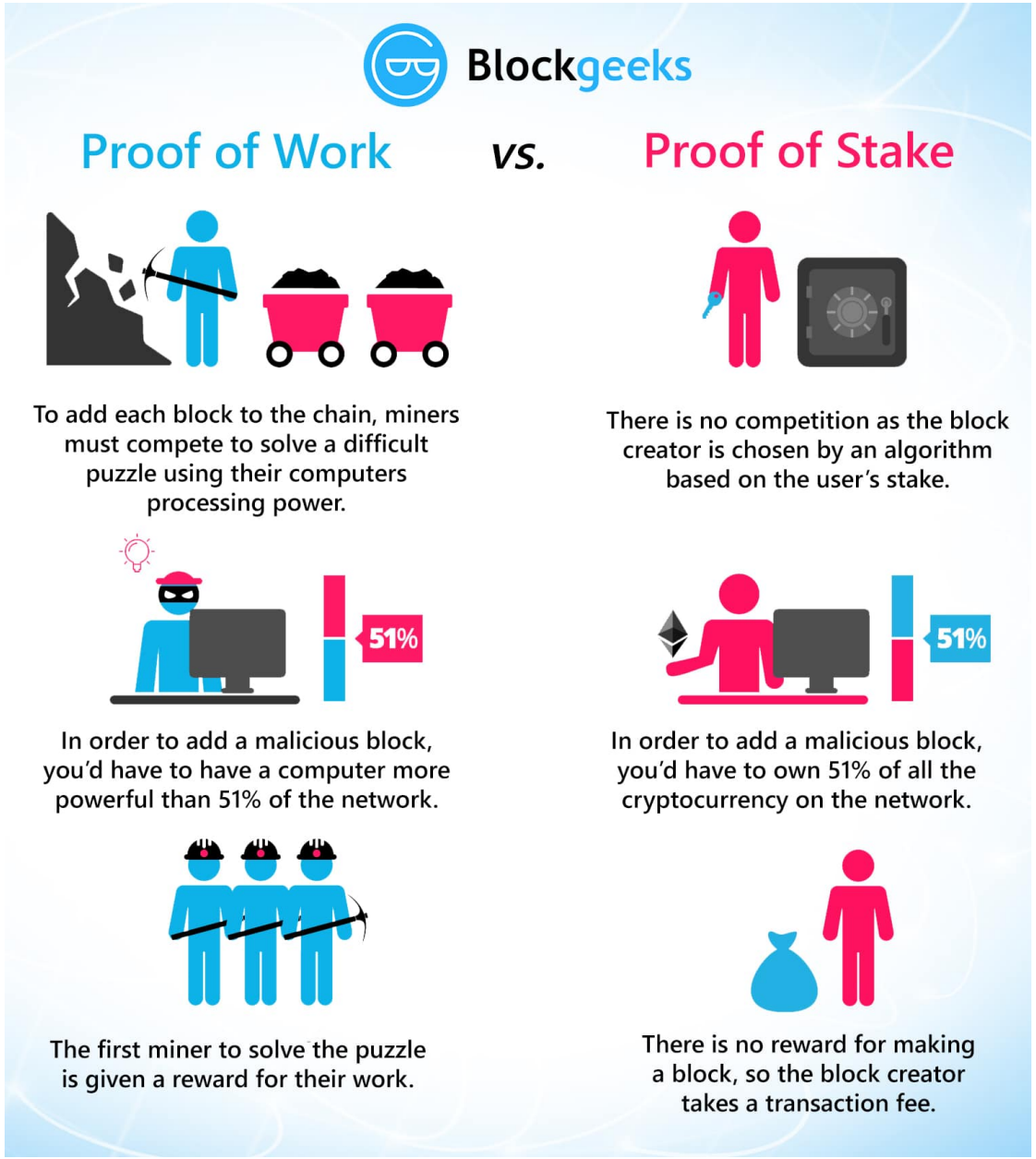


Proof-of-work:

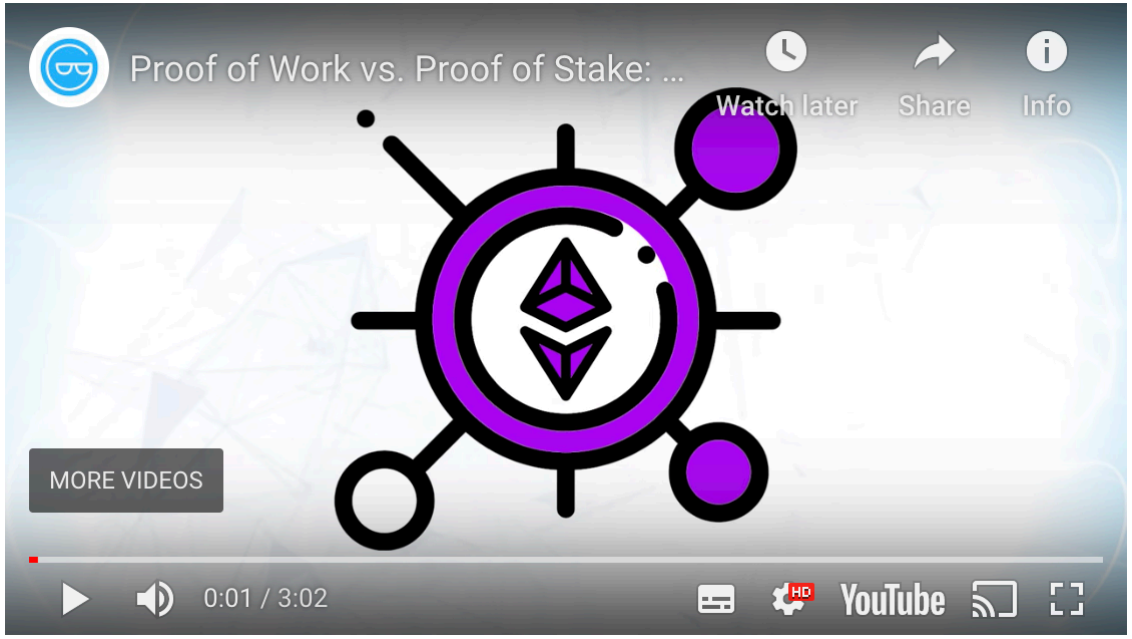
- An exhaustive process, with no clever short-cut available
- Therefore, every "guess" has an equal chance of success
- More guesses gives more chance to mine the next block: i.e., the likelihood of being the next miner is proportional to number of guesses attempted
- Also, the number of attempts is proportional to the compute resources given to the task; and compute resources cost money
- So, essentially, ***the likelihood of mining the next block is proportional to the money a miner is committing to the task of mining***…

Proof-of-stake:

- An ***efficient alternative (equivalent) to proof-of-work***
- Calculate each miner's "stake" in the cyptocurrency by using the ledger to count the verified tokens the miner owns
- Simply select the next miner, ***m***, at random with probability equal to the ratio of ***m***'s stake to the total stake of all miners
- As long as the stochastic (i.e., *random*) process selecting the next miner is "fair", we have a system that is equivalent to proof-of-work (and ***as secure as proof-of-work***), without the wasteful need of actually doing the work. *Bravo!*



https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/



Watch this 3-minute video: https://youtu.be/-C19r0UsYws

"A greener and cheaper form of consensus"

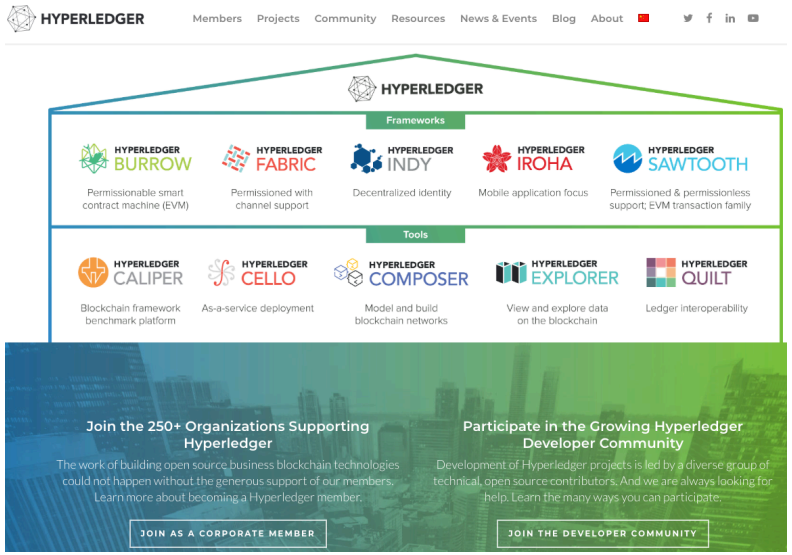
Ouroborus

- Proof-of-stake protocol backbone for the **Cardano** blockchain
- To be secure, stakeholder selection *must* be *truly random*
- **Innovation**: secure multiparty implementation of a coin-flipping protocol
- Ouroborus is the first proof-of-stake shown to be provably secure (with security equivalent to Bitcoin's blockchain)
- Presented at Crypto 2017
- Permits *permissioned* and *permissionless* ledgers via token distribution

https://www.cardano.org/en/ouroboros/

Link has one-hour video lecture by the algorithm creator

A Trivial Aside: The ouroboros is an ancient symbol depicting a serpent or dragon eating its own tail. It is often used as an emblem of infinity. Fans of the sci-fi sitcom, *Red Dwarf,* may recall that, as a baby, Lister was left by his parents in a box under a pool table in the Aigburth Arms pub, Liverpool. On the box was written OUROB ORUS. The barmaid who found him thought his parents couldn't decide whether to call the baby Robert or Russell ("our Rob, or Russ"). The Aigburth Arms was at one time my local pub and I played pool there often. Unfortunately, I never discovered a time-travelling baby. https://en.wikipedia.org/wiki/Ouroboros_(Red_Dwarf)



Hyperledger

Open-source standard for cross-industry blockchain technologies. A global collaboration hosted by The Linux Foundation

Hyperledger: A blockchain “standard”

Launched 2016 by 30 founding corporate members, hosted by Linux Foundation

Vision:

Hyperledger as a business blockchain umbrella

- Of the 70+ open source organizations the Linux Foundation has launched, Hyperledger is the fastest growing.

To advance cross-industry blockchain technologies

- An “*operating system*” for marketplaces, data-sharing networks, micro-currencies, and decentralized digital communities.
- Potential to reduce cost and complexity of getting things done in the real world.
- Open Source, collaborative software development to ensure transparency, longevity, interoperability and support required to bring blockchain technologies forward to mainstream commercial adoption.

https://www.hyperledger.org/

Hyperledger Goals

Create enterprise grade, open source, distributed ledger frameworks and code bases to support business transactions

Provide neutral, open, and community-driven infrastructure supported by technical and business governance

Build technical communities to develop blockchain and shared ledger POCs, use cases, field trails and deployments

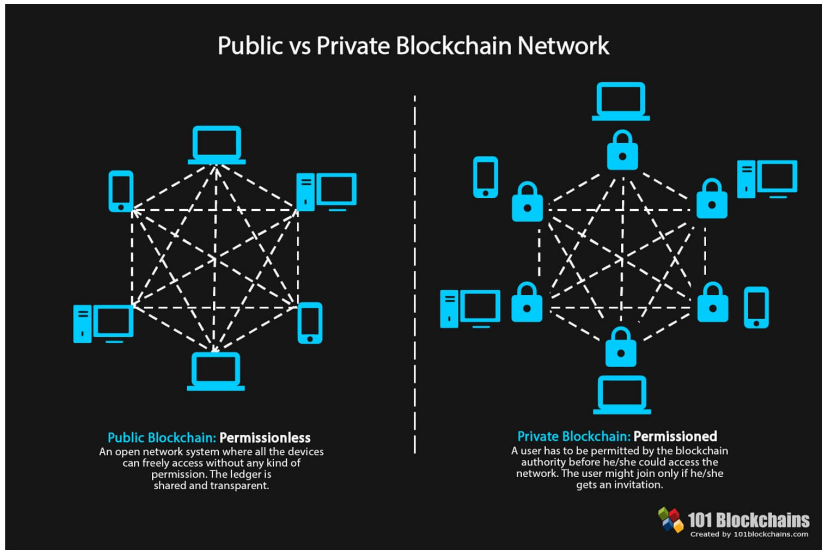
Educate the public about the market opportunity for blockchain technology

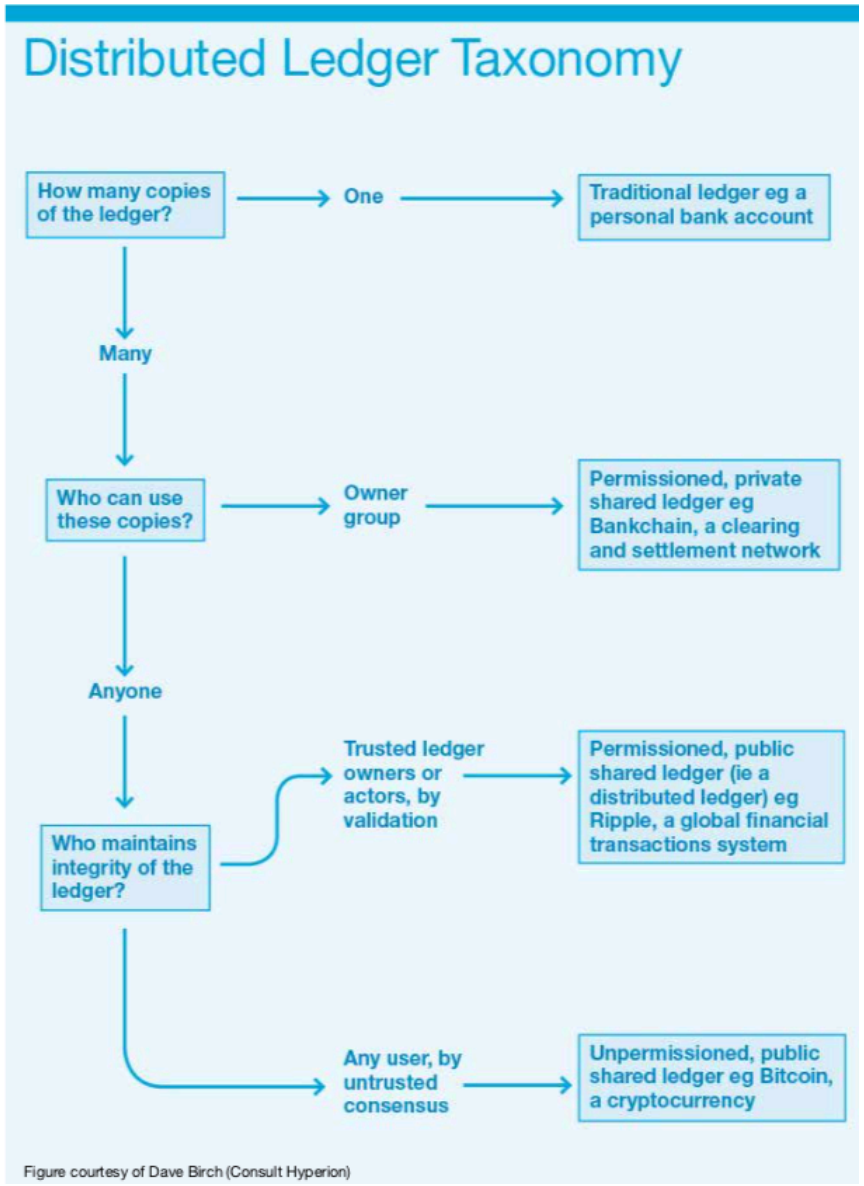
Promote our community of communities taking a toolkit approach with many platforms and frameworks

Permissioned Ledgers

Permissioned ledgers have one or many owners. The ledger's integrity is checked by a limited consensus process carried out by trusted actors (e.g., company, banks, government departments). Maintaining a shared record is much simpler than the consensus process used in *unpermissioned* ledgers, therefore permissioned ledgers are usually faster.

Hyperledger Fabric is an open source enterprise-grade permissioned DLT platform, designed for enterprise contexts





Bitcoin and Ethereum are ***public permissionless*** DLTs.

A glimpse of the future?

Shared Ledger Database

Blockchain allows multiple different parties to securely interact with the same universal source of truth

Finance

Streamlined settlement, improved liquidity, increased transparency and new products/markets

Healthcare

Unite disparate processes, increase data flow and liquidity, reduce costs and improve patient experience and outcomes

Supply Chain

Track parts and service provenance, ensure authenticity of goods, block counterfeits, reduce conflicts

Summary:

- There is great hype around DLTs
- Significant advances:
  - Smart contracts / DApps
  - Efficient/secure proof-of-stake
  - Hyperledger open-source standards
- Is the hype justified?
  - *Wait and see.*
  - *There will be failures along the way…*

Example questions

Q.1: What is the name of the *proof-of-stake* protocol used in the *Cardano* blockchain?

[1 mark]

Q.2: Name a *permissioned* Distributed Ledger Technology.

[1 mark]

Q.3: What is, or was, *The DAO?*

[3 marks]

Q.4: What is *proof-of-stake* and how does it compare with *proof-of-work*? Describe the advantages and disadvantages of both.

[6 marks]