Blockchain and sensible Web3

COSC312 / COSC412

Learning objectives

- Explain how Web3 seeks to build decentralised systems
  - Likely relies on **peer-to-peer networking** (decentralised)
  - Uses open blockchain systems such as bitcoin, Ethereum

- Gain a high-level view of **blockchain approaches** and beyond cryptocurrencies, e.g., how they support **decentralised autonomous systems**

- Can sketch what **NFTs** are & how they use blockchains

Nodes in bitcoin network

- There are four main roles nodes can take on:
  - **Network**—all nodes help routing within the p2p protocol
  - **Wallet**—manage keys that show ownership of transactions
  - **Miner**—participate in the proof-of-work block verifications
  - **Blockchain**—can carry the full blockchain
- Bitcoin Core reference client contains all four functions
  - Miners may leave out wallet
  - Lightweight wallet only has wallet and network components
  - Some nodes may store blockchain, but not do mining

Content of bitcoin transactions

- **No persistent coins**: serial numbers are transaction hashes
- Transaction specifies a **number of inputs and outputs**, with inputs usually previous transactions
  - can **output back to yourself**, thus pocketing 'change'
  - remainder of input, after subtracting output, is **transaction fee**
- Since all transactions are in the blockchain:
  - can search back in time to find transaction:
  - either **genesis block** (50 bitcoin) or a **coinbase mining reward**

bitcoin: anonymity, privacy and value

- bitcoin has been discussed as being anonymous
  - This makes little sense—the **entire ledger is available publicly**!
  - However it is true that public keys need not be identified
- **Linkability concerns**: metadata may allow subsequent determination of wallet's owners
  - Large state organisations likely want to do this,
    - *e.g.*, law enforcement
- State players globally are key to bitcoin value

bitcoin scalability challenges

- Originally, blocks had no size limit, but that risks DoS
  - Added a limit that **blocks can only be 1 megabyte** at most
- Blocksize limit has **caused scalability problems**:
  - Provides for fewer than ten transactions per second
  - Around ten minutes to add a block to blockchain
  - Thus bitcoin transactions **can take hours to confirm**
- Segregated Witness (SegWit) approx. doubles size
  - Moves witness signature out of transaction blocks

Many more aspects of bitcoin not discussed

- bitcoin blocks also include **management parameters**:
  - *e.g.*, **version numbers** to allow the protocol to be modified
  - Versioning is very important given that the protocol behaviour is the fundamental basis on which cryptocurrencies are built

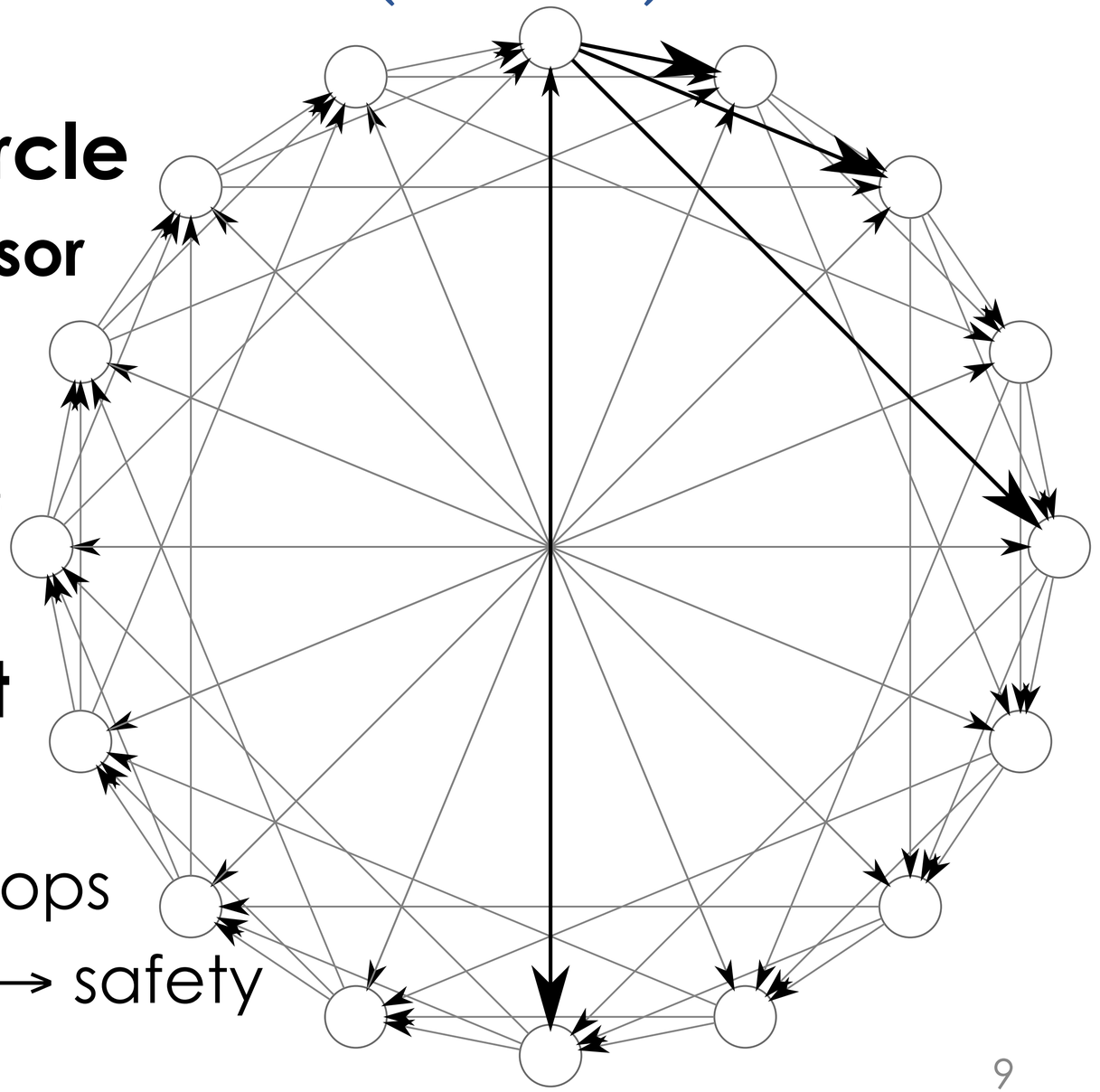
- bitcoin specifies transactions with a **scripting language**
  - P2PKH—'**pay to public key hash**' is a common transaction
  - 'multisig' transactions allow m-of-n public key sign-off
  - **Smart contracts can be encoded**, beyond money transfer

Peer-to-peer networking for scalability

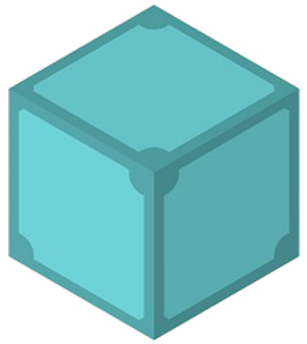
- No central server: clients do message routing
  - (But uses the Internet, thus **depends on IP**, etc.)
- To join network: new client **connects to seed** nodes
  - Can then grow local knowledge of global client set
- Example peer-to-peer structure: **distributed hash table**
  - Hash data items; use hash as position within number space
  - Assign clients responsibility for ranges of that number space
  - Reliable even as clients join and leave (churn) over time

‘Chord’ distributed hash table (DHT)

- Clients + keys **arranged in circle**
  - Every client knows their **successor**
  - Client also has ‘**fingers**’ further ahead in key space
    - Note four emphasised fingers of top-centre client
- Look up key by finding **client that precedes** that key
  - Can reach any key in $\mathcal{O}(\log n)$ hops
  - Assign **multiple clients per key** → safety



IPFS—the InterPlanetary File System



- Provides **decentralised data storage**
  - Aims for **high availability** (anti-censorship, global replication)
  - Decentralisation avoids reliance on ‘big tech’, or single servers

- Location of data (and replicas) **based on its content**
  - Request data via a cryptographic hash of that data
  - Data is divided up into **immutable blocks**
  - Interplanetary Naming System (IPNS) supports **mutable objects**
  - **Peer-to-peer infrastructure** for finding / reading / writing data

Blockchain aside from bitcoin

- Increasingly **blockchain services** are being offered independently of cryptocurrencies such as bitcoin
  - **Blockchain as a Service** is offered on the commercial cloud
- There is **much hype**, and often gaps in understanding
  - Some existing approaches rebadged as ‘blockchain’
- bitcoin helped show ways in which **decentralised systems can appear to form distributed consensus**

Different sorts of blockchain designs

- **Permissionless** (open) systems—bitcoin, Etherium, *etc*.
  - Any node can join or leave the blockchain at any time
- **Permissioned**—there is control over who participates
  - Can use algorithms like Paxos or RAFT to form consensus
  - … similar sorts of closed systems existed previously
- Other axis is **public** / **private**
  - sovrin is a permissioned+public blockchain managing identity
  - hyperledger is a permissioned, private blockchain

Open, decentralised consensus algorithms

- **Permissionless blockchains**: consensus over open set
  - Nakamoto consensus is term for bitcoin's consensus algorithm
  - As discussed, bitcoin uses proof-of-work to support consensus
    - Nifty but for hugely destructive environmental effect
  - Nakamoto consensus also involves the '**longest chain**' rule

- Ethereum now uses proof-of-stake (explained soon)
  - Was bootstrapped from previously using proof-of-work

Proof of space

- As the name suggests: **demonstrate allocating space**
  - … as opposed to demonstrating doing computational work
- One approach: **graph pebbling**
  - prover stores large graph to demonstrate commitment
  - verification needs to be cheap compared to proof generation
- Another approach: **plotting of precomputed solutions**
  - *e.g.*, could use proof-of-work style problem with stored guesses
  - can then raise difficulty level during proof-of-space
- Criticism: messed up supply chain for storage devices!

Proof of stake

- Validators are selected **based on their stake**
  - *i.e.*, selected validators will hold lots of the cryptocurrency
    - May have been required to hold this for some minimum duration
  - it's against their own financial interests to behave maliciously
- Various potential attacks:
  - **Nothing-at-stake**—malicious validator builds on every fork
    - Improved approaches require security deposits from validators
  - **Long-range attacks**—attackers recreate alternate history
    - Mitigations involve, *e.g.*, checkpoints; invalidating old keys
  - **Overcentralisation**—incentive to raise stake → centralisation

Web3 and decentralised applications

- Web3 aim build **decentralised computing** platforms
  - Tone is sometimes even stronger, *i.e.*, anti-central

- **Executable contracts** rather than transfer of currency
  - bitcoin already shows practicality of scripting language
  - bitcoin facilitates agreement of future events (& cancelation)

- Always ask: **is blockchain really needed?** Alternatives?

Proposed Web3 example applications

- **Supply chain management**: tracked asset transfer
  - Particular with respect to pharmaceuticals
  - Many organisations; common goal; fraud impractical
- Microgrids and neighbourhood **electricity trading**
- Government storage of records (*e.g.*, health records)
  - **e-democracy** and **voting** (how could that go wrong?)
- **Collecting royalties** for performances…
- Legal and financial processes, *e.g.*, **conveyancing**

Web3/crypto: does it avoid central control?

- Web3/crypto doesn't depend on big-tech or big banks
- … but there are many dependencies often ignored:
  - Need **access to computing equipment** *i.e.*, supply chain
  - Need to have **power infrastructure** (solar bitcoin mining: hard)
  - Need Internet service provider (ISP) and **network infrastructure**
  - Crypto needs **an exchange** to gain any real-world cash value
    - Exchanges almost certainly attract **government regulation**

- More pragmatic/efficient to embrace central control?

Ethereum aims to effect dapps (distributed)

- Ethereum aims to build a **global computing platform**
  - Cannot be shut down easily
  - Can scale up and down
  - Resistant to censorship and other interference

- **Ethereum Virtual Machine**
  - Platform on which code executes

- Usually need some sort of bridge to other web APIs

Blockchain scheme governance

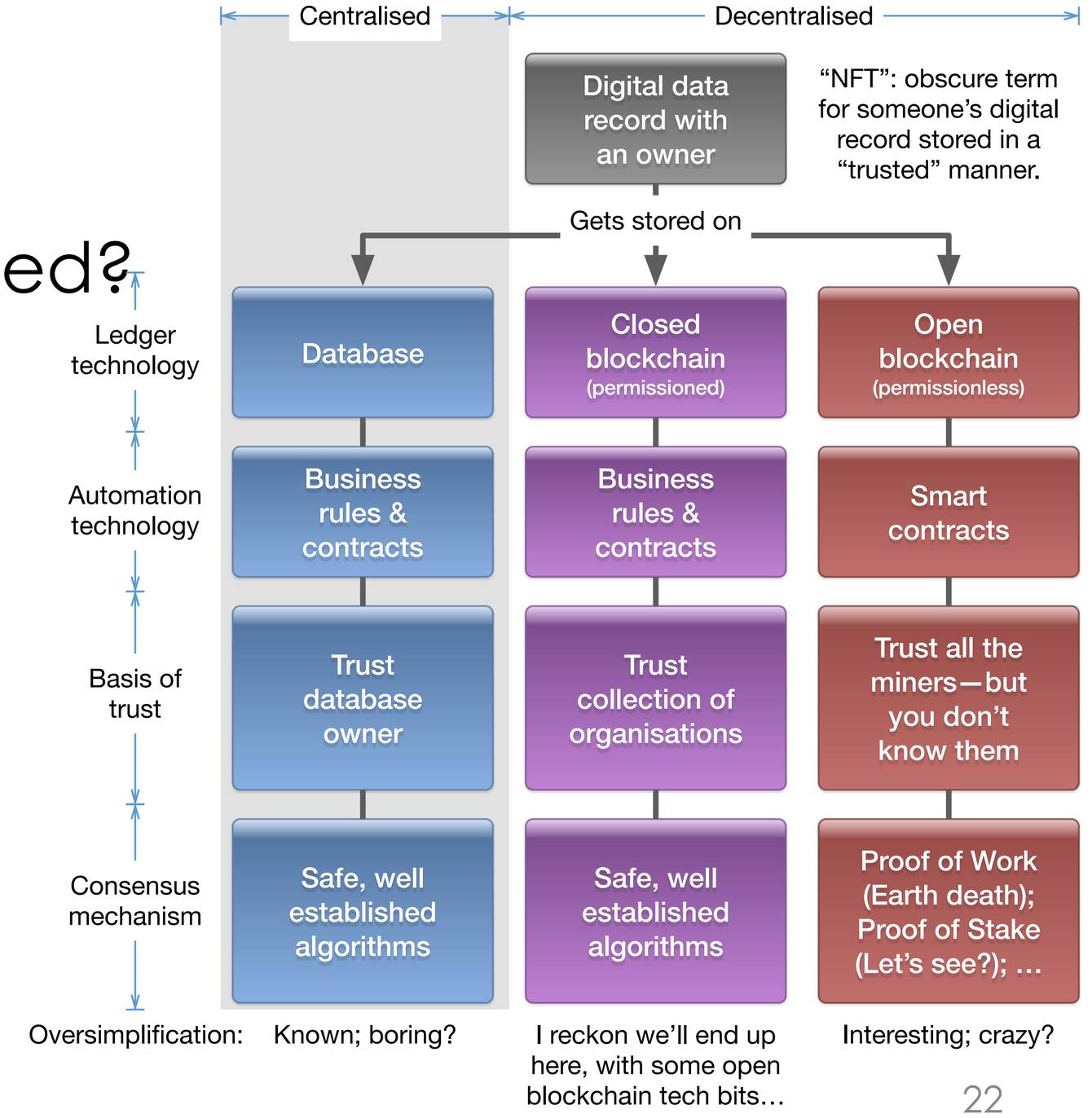
- What if a **protocol vulnerability** is discovered?
  - Say a **hacker steals resources** worth millions of dollars
  - Entire blockchain system can agree to **rewind history**?
  - … but this is a capability blockchain systems seek to give up
  - Alternatively end up **showing lack of real decentralisation**?
- Ethereum *e.g.*: **Decentralized Autonomous Organization**
  - Raised $150m crowd-sourced funding; DAO was ~15% of ether
  - **Code had vulnerabilities**; hacker siphoned off a third of DAO
  - Soft-fork and hard-fork resolutions discussed; hard-fork done

NFTs—non-fungible tokens

- **Cash is fungible**—individual coins are interchangeable
- NFTs are just **unique digital records owned** by someone
- NFTs are usually stored on blockchains
  - Thus **record of ownership** is decentralised and cooperative
- Smart contracts can record NFT **transfer of ownership**
- Blockchains don't suit storing lots of data
  - Thus NFTs often encode a **URI to target object**
  - … but then there is no particular value to NFT's uniqueness

NFT characterisation

- **Blockchain NFTs**: really need?
  - Existing financial systems can be improved to lower friction within transactions
- Decentralised Identifiers:
  - **W3C DID standard**
  - Help unify different technology that achieves similar results



In summary

- Bitcoin demonstrated **decentralised consensus** in an open world: including permissionless blockchains
- Web3 aim: build **decentralised apps** (dapps) & **storage**
  - Depends on peer-to-peer functionality at low levels
  - Embraces many forms of blockchain, *e.g.*, Ethereum
  - Goes beyond cryptocurrency use
- **NFTs** are a particular use of blockchains
  - … mostly using open blockchains, but might not need to