Blockchain

Part – I: Introduction

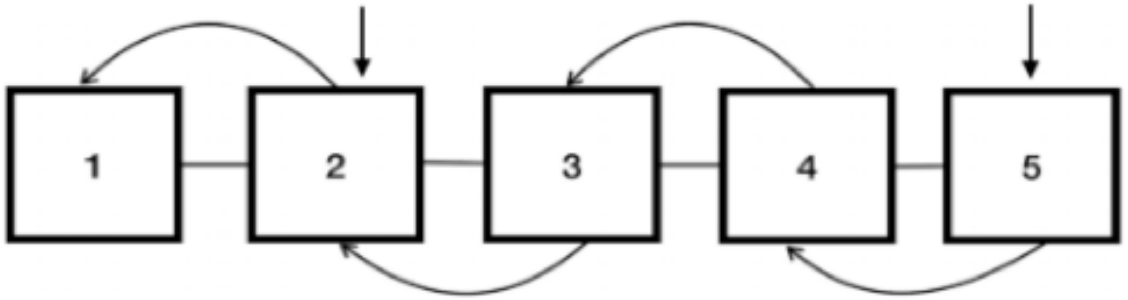
Credits: Several of the slides borrowed from Prof. Ari Juels, Jacobs Technion-Cornell Institute and Prof. Aggelos Kiayias, The University of Edinburgh

What is Blockchain?

- From a bird's-eye view it is a data structure: ''linked-list'' with specific properties
- It is a "distributed" database of "records" of all events that have been executed and shared among participating "parties"

Every block except the first one contains the hash of the previous block (pointer)

Blocks store cryptographically secure information (validated by nodes)

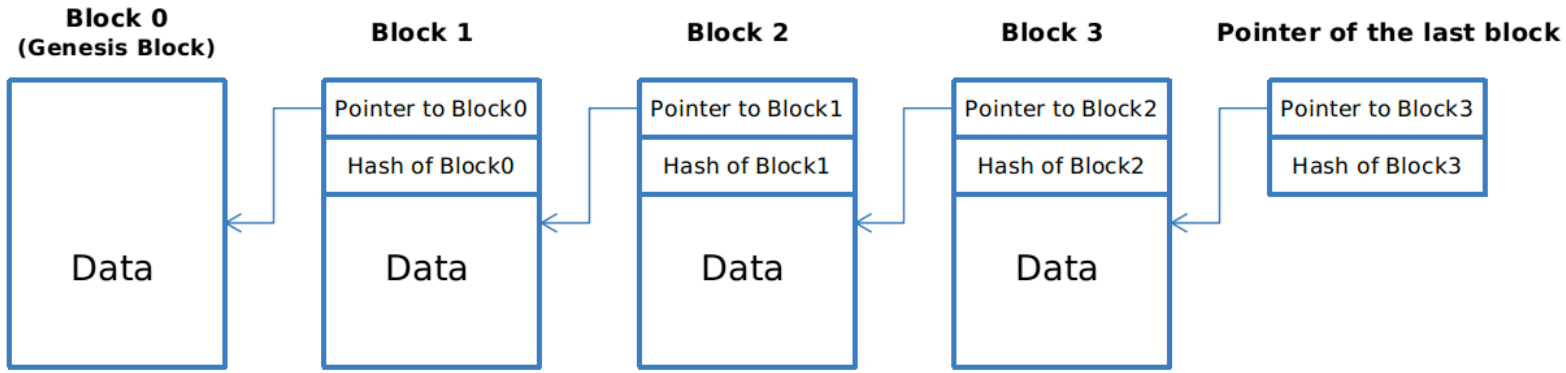


A blockchain has a linked list structure

https://hackernoon.com/databases-and-blockchains-the-difference-is-in-their-purpose-and-design-56ba6335778b

What is Blockchain?

- List of records (*blocks)*
- that are linked using *cryptography*
- Each block generally contains
  - a cryptographic hash of the previous block,
  - a timestamp,
  - data



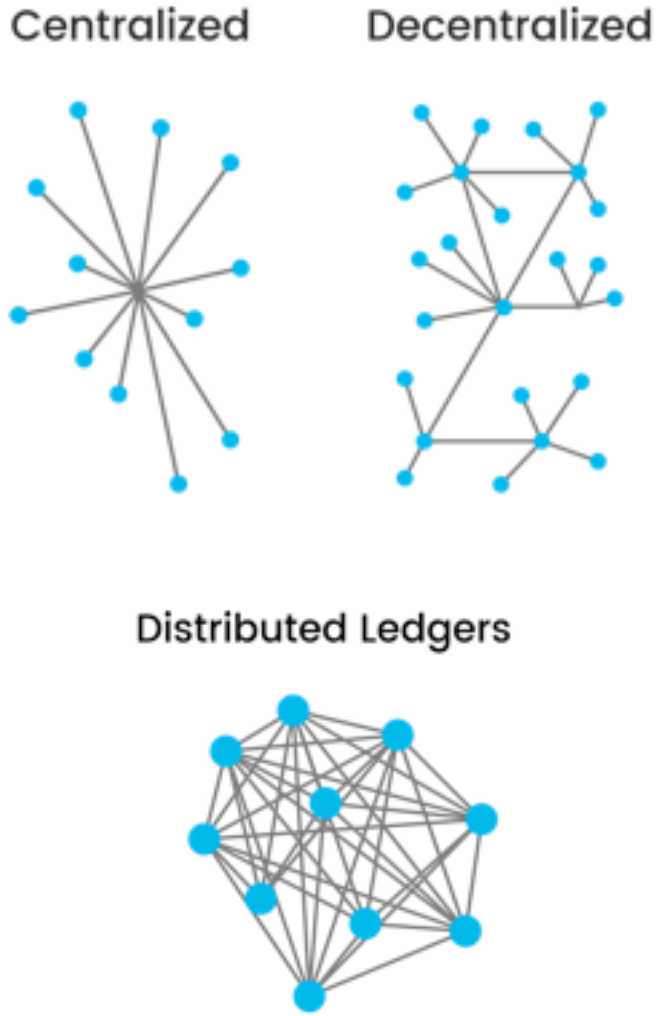
https://medium.com/@zhaohuabing/hash-pointers-and-data-structures-f85d5fe91659

Limitations of Distributed Databases

- The limitations of distributed databases:
  - Trust
  - Low fault-tolerance
  - Complexity
  - Costs
  - Immutability
  - Transparency

Network topologies

- Centralized –> central control over data (prone to single point of failure)
- Decentralized –> multiple central owners that control the data
- The distributed ledger is shared and updated with every incoming event among the nodes connected
  - No central server
  - No central control over data



What do we get from moving centralized to distributed ledgers?

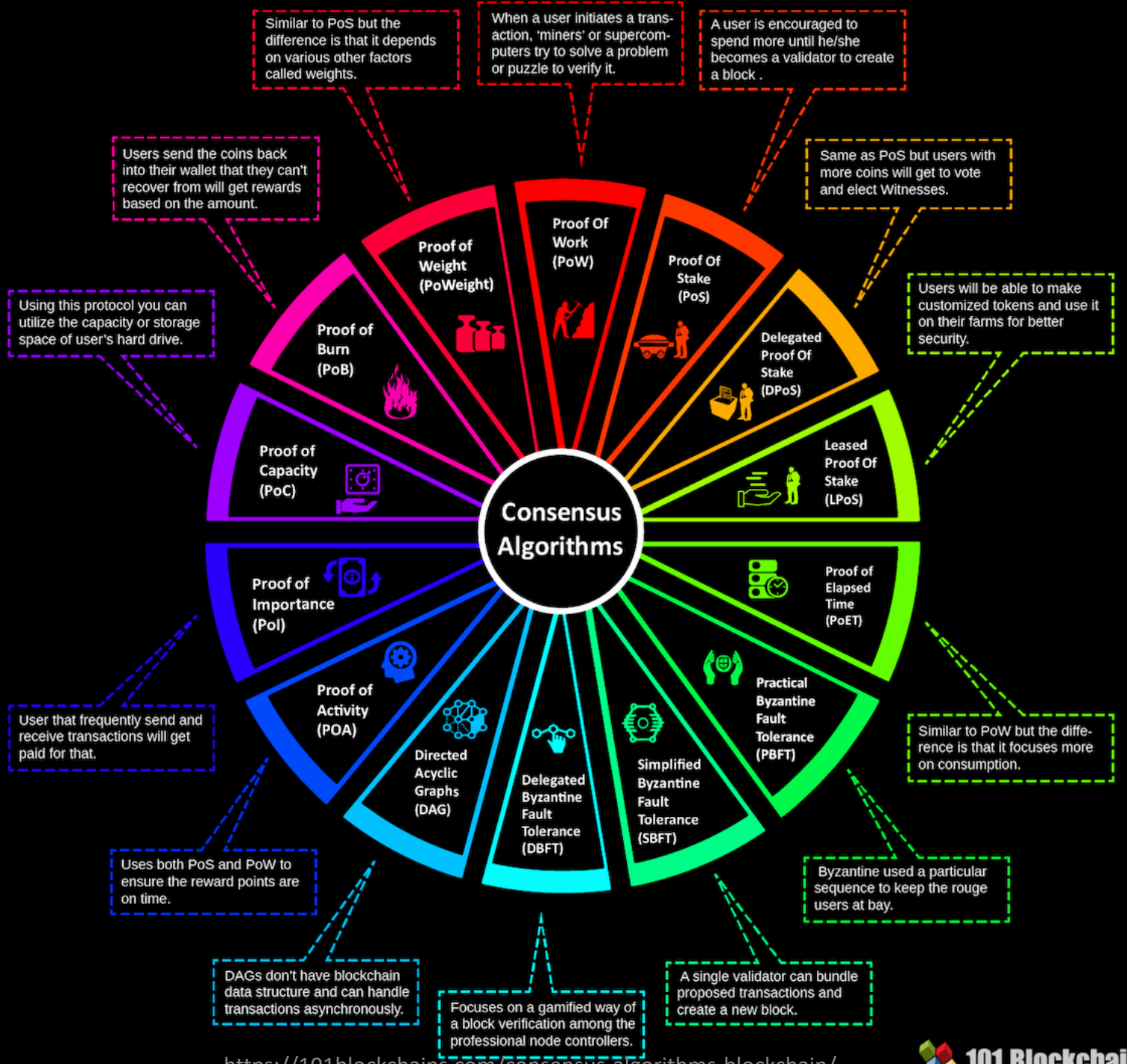
- Transparency
- Distributed trust (trust is distributed among all parties)
- Fault-tolerance (no more single-point failures)
- Costs
- Immutability

Transparency in Blockchain

- **Transparency:** Every participant has a copy of the current blockchain data
  - They have access to all blocks added to the structure so far

Distributed Trust in Blockchain

- **Consensus:** All network participants must agree that an event to be added to chain is valid.
- This is achieved through the use of consensus algorithms
  - Many different consensus algorithms



https://101blockchains.com/consensus-algorithms-blockchain/

101 Blockchains

Fault tolerance

Byzantine fault tolerance

- Assume some nodes and the network may be actively malicious
  - They might be able to prevent honest nodes from communicating not reply at all or send different messages to different nodes
- Fundamentally need **N=3f+1 for consensus**, where f is *faulty nodes*
  - f out of N might not reply => Need to proceed with N-f or 2f+1
  - f out of the N-f might be malicious => Need majority
    - N-2f > f => N>3f or N=3f+1
- Can be relaxed to N=2f+1 under various stronger assumptions

Public (permissionless) vs Private (permissioned) Blockchains

- Consideration of who's able to *write* that data.

Public Blockchains

- Anyone can participate (write to blockchain)

Private Blockchain

- Participants are predefined, known, and trusted
  - Many of the mechanisms are not needed – or rather they are replaced with legal contracts

Open vs Closed Blockchains

- Consideration of who's able to *read* that data.

Open Blockchains

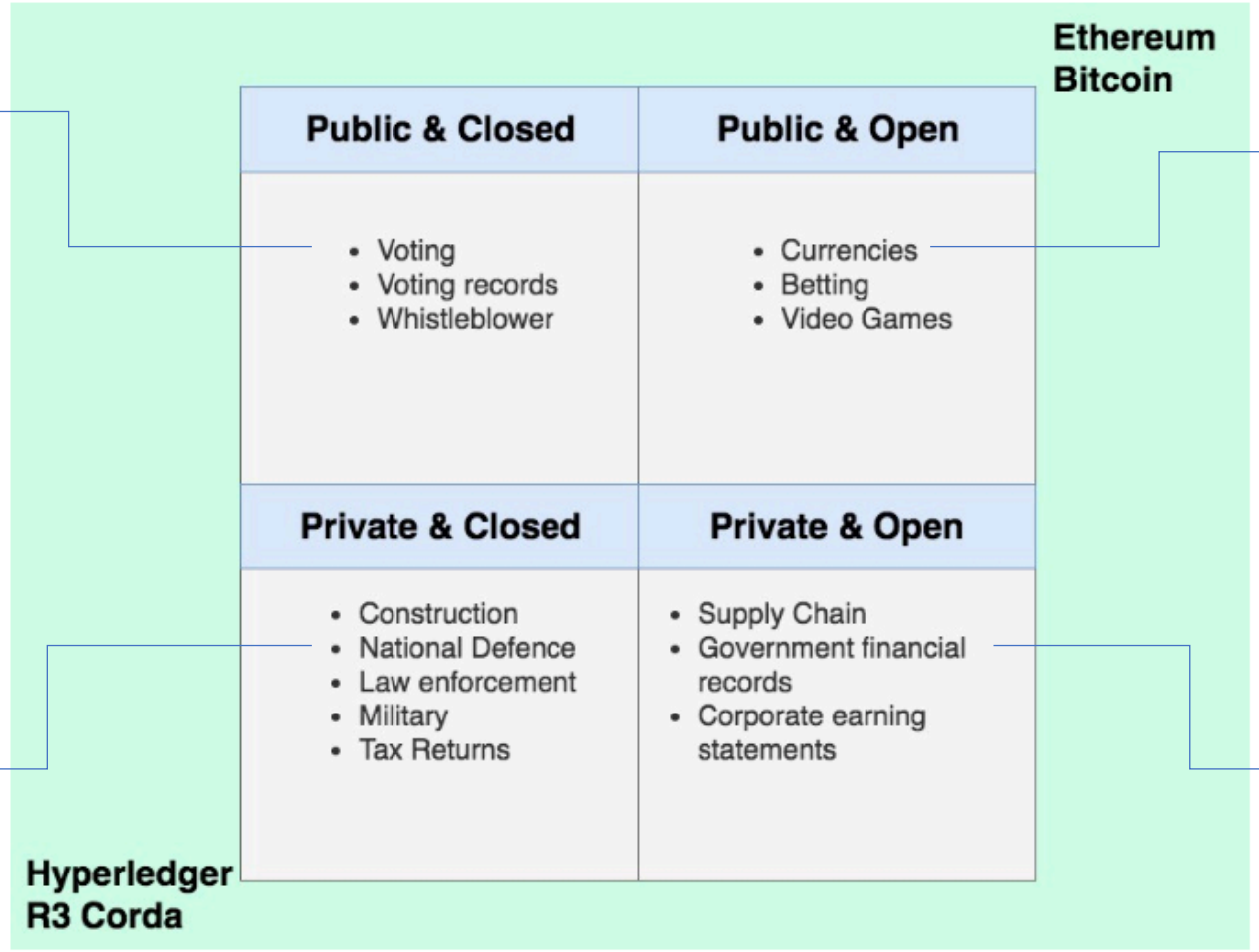
- Anyone can access the blocks and read

Closed Blockchain

- Only a predefined group (i.e., industry, government etc.) can access the blocks and read

Public/Private and Open/Closed Blockchains

People freely vote (write to blockchain) but cannot read because of ballot confidentiality!



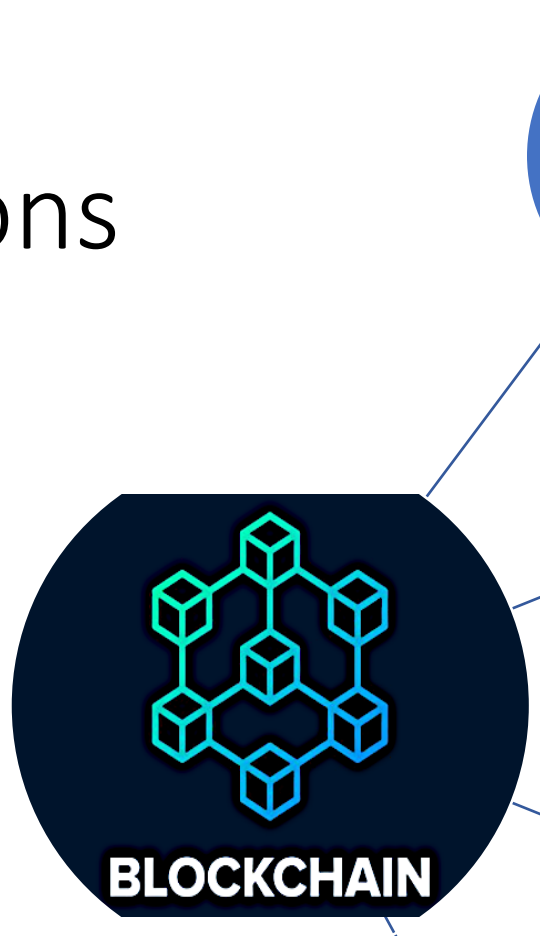
Participants free to make transactions (write to blockchain) and read all transaction history/verify

Sensitive applications! Only permissioned people have read/write rights

Only permissioned people can write financial records, everyone is free to read the current blocks of financial records

https://medium.com/coinmonks/public-vs-private-blockchain-in-a-nutshell-c9fe284fa39f

Applications



- Smart Contracts
  - Wagers
  - Digital Rights
  - Escrow
- Digital Currency
  - E-commerce
  - Microfinance
  - Global payments
  - Remittance
- Record Keeping
  - Healthcare
  - Ownership
  - Voting
  - Intellectual Property
- Securities
  - Crowdfunding
  - Debt
  - Equity
  - Private Markets

Summary

- Distributed ledgers use blockchain protocols as one main means of implementation
- The blockchain is a distributed database that satisfied unique set of safety and liveness properties
- To understand it better, we can focus on one of its successful application: Bitcoin!