CSE446: Blockchain & Cryptocurrencies

Lecture – 6: Money and Cryptocurrency

Inspiring Excellence

Agenda

- Cryptocurrency
- Distributed Ledger/Blockchain concept
- Bitcoin

Crypto-currency

- Based on cryptography
- Derives trust from mathematical properties/algorithms/systems
- Based on established, trusted cryptographic primitives NOT from chemical/physical properties
- NOT from coercive (imposed) Legal Tender statutes
  - Legal tender is a medium of payment recognised by a legal system to be valid for meeting a financial obligation

Fiat money vs Crypto-currency

- Holder has ownership
  - Like any Fiat money, a crypto-currency is a bearer instrument
  - But provides better security as it is important to prove ownership
- No other records kept as to identify an owner
- Easy to keep anonymous
- Hard or impossible to replace if lost or stolen

https://upload.wikimedia.org/wikipedia/en/9/94/1000_Bangladeshi_taka_Obs_2011.jpg

Bitcoin

- Decentralised, Distributed, Voluntary
- No central issuing or verification authority, no “Bitcoin Corp”
  - Bitcoin Foundation (bitcoinfoundation.org)
  - Growing numbers of of entrepreneurs accepting or basing new business concepts on Bitcoin
- Relative to other bearer instruments (currency or fiat currency)
  - Easier to transport anywhere in the world
  - Easier to secure, even provides better security
- Relative to other electronic currencies
  - Immune to sovereign censorship, shutdown, or confiscation
  - Immune to inflation and bank defaults

Bitcoin challenges

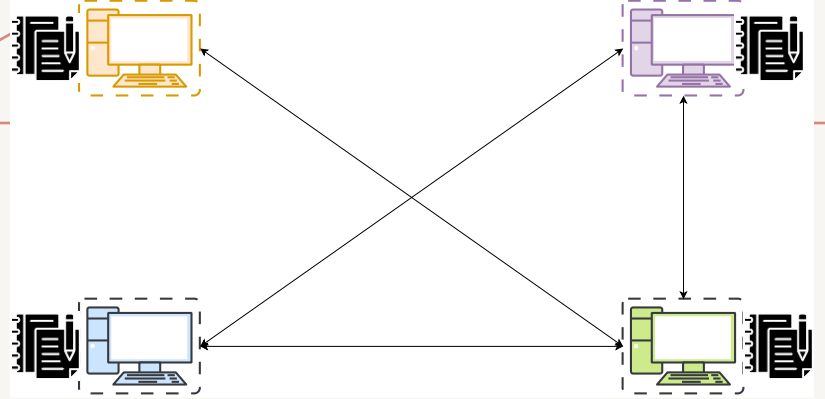
- Creation of a virtual coin/note
  - How is it created in the first place?
  - How do you prevent inflation? (What prevents anyone from creating lots of coins?)
- Validation
  - Is the coin legit?
  - How do you prevent a coin from double-spending?
- Trust on third-parties
  - Rely on proof instead of trust
  - Verifiable by everyone
  - No central bank or clearing house

Bitcoin challenges

- Creation of a virtual coin/note
  - How is it created in the first place?
  - How do you prevent inflation? (What prevents anyone from creating lots of coins?)
  - Is the coin legit?
  - How do you prevent a coin from double-spending?
- Trust on third-parties
  - Rely on proof instead of trust
  - Verifiable by everyone
  - No central bank or clearing house

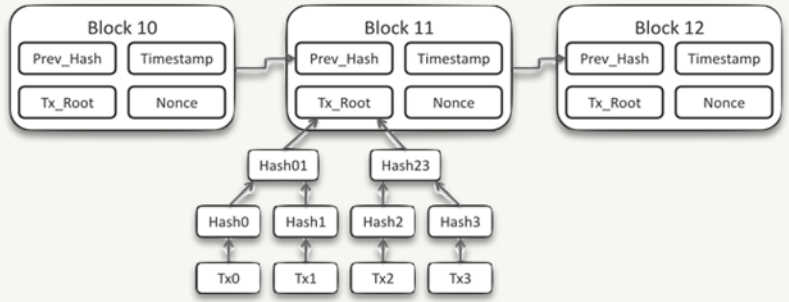
Blockchain/Distributed Ledger is the solution

Distributed Ledger



- A general ledger is the heart of any banking and financial institutions
- To tackle the centralised trust issues
  - dissolve the centralised trust, replace it with a decentralised trust
- One way: distribute the ledger over as many entities as possible
  - Hence the notion of distributed ledger
- Slight difference in meanings between blockchain and distributed ledger
  - A blockchain is just an example of a distributed ledger

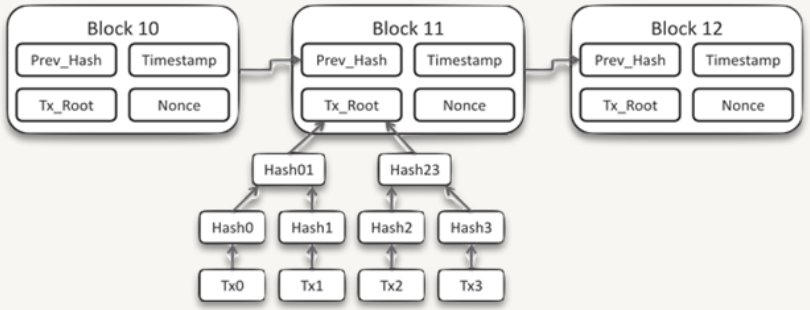
Blockchain

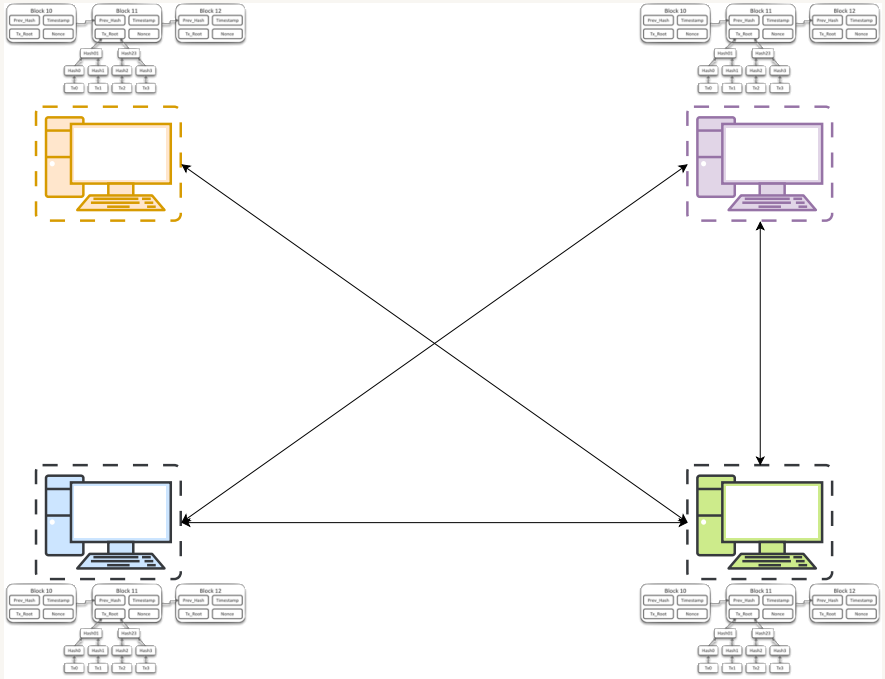


- The blockchain is a distributed record of transactions structured in a specific way
- These transactions are grouped together following specific sets of rules
  - These groups are known as Blocks
- Blocks are the linked together with specific rules, thus forming the chain
- Blockchain is a chain of blocks, where each block maintains a specific data structure

Blockchain

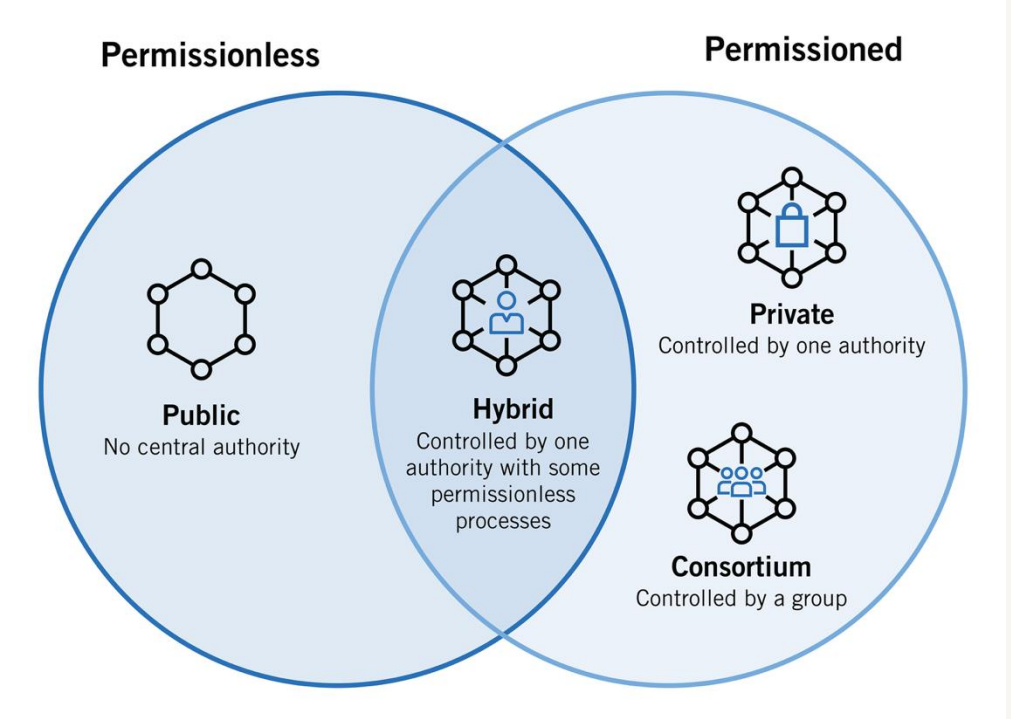
Even though a blockchain is a just a data structure, however, it implies a distributed data structure





Blockchain types

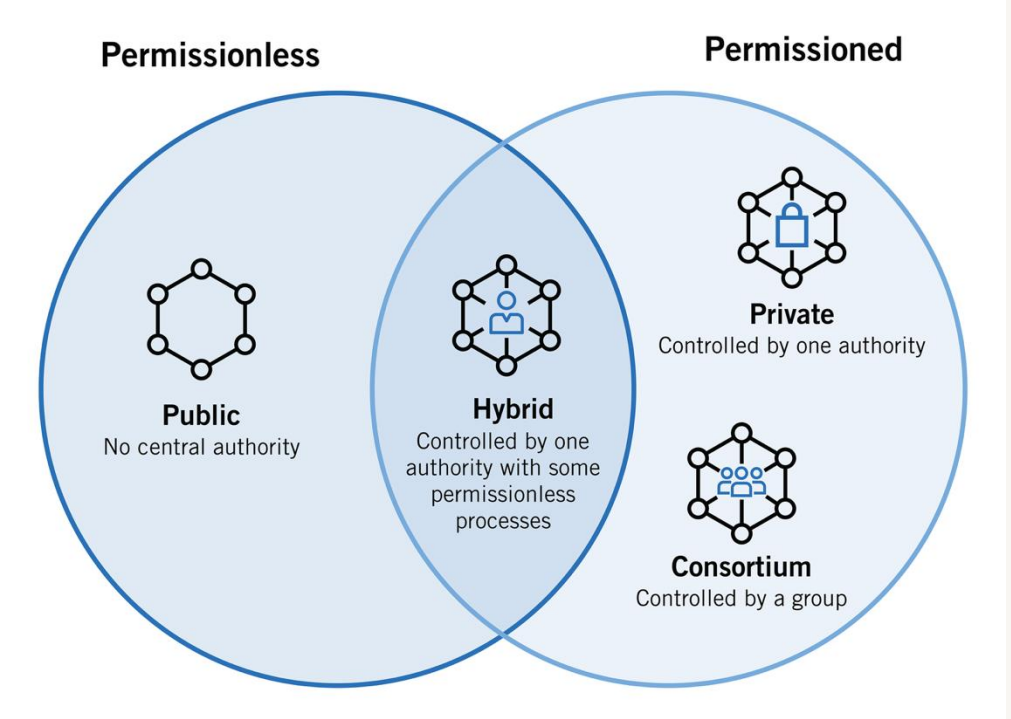
- Depending who can access (read) or write data from/to a blockchain, there could be four types of blockchain
  - Public (permissionless) blockchain
  - Private (permissioned) blockchain
  - Hybrid blockchain
  - Consortium blockchain



https://www.foley.com/en/insights/publications/2021/08/-/media/images/insights/publications/2021/08/22mc35029-blockchain-graphic--permissions06.png

Public blockchain

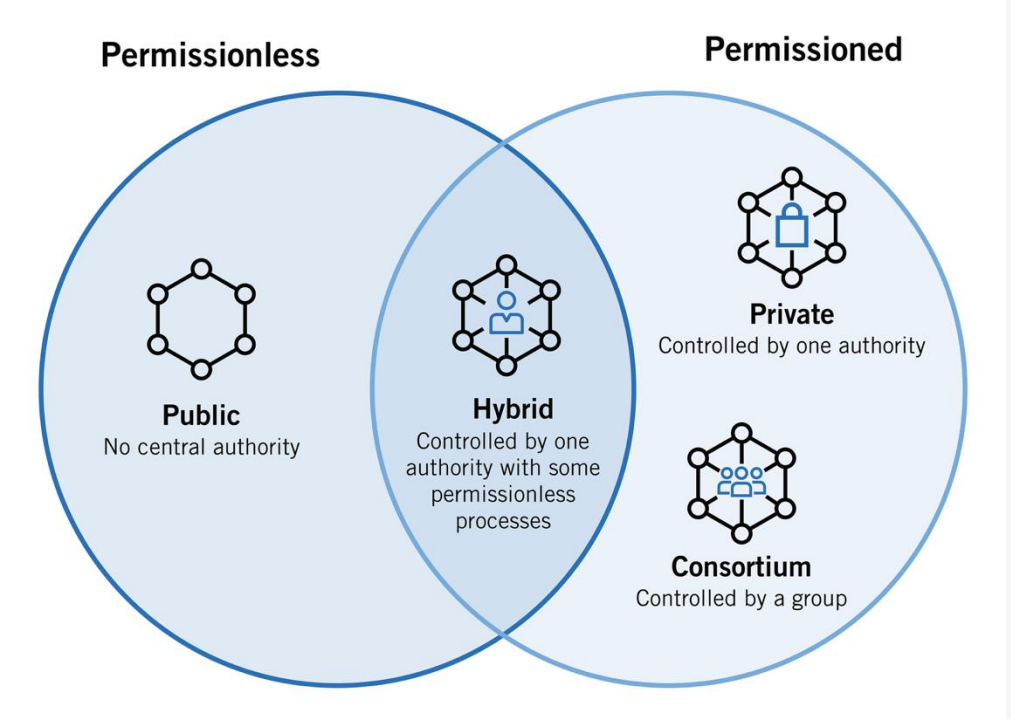
- A public blockchain is an open blockchain which allows everyone to join in the network
- Everyone can write into the blockchain following specific rules
- All data can be read by all
- Everyone can verify all data in the blockchain
- No one is trusted & there is no central authority
- Almost all crypto-currency blockchains are public, e.g. Bitcoin, Ethereum, Solana, Cardano



https://www.foley.com/en/insights/publications/2021/08/-/media/images/insights/publications/2021/08/22mc35029-blockchain-graphic--permissions06.png

Private blockchain

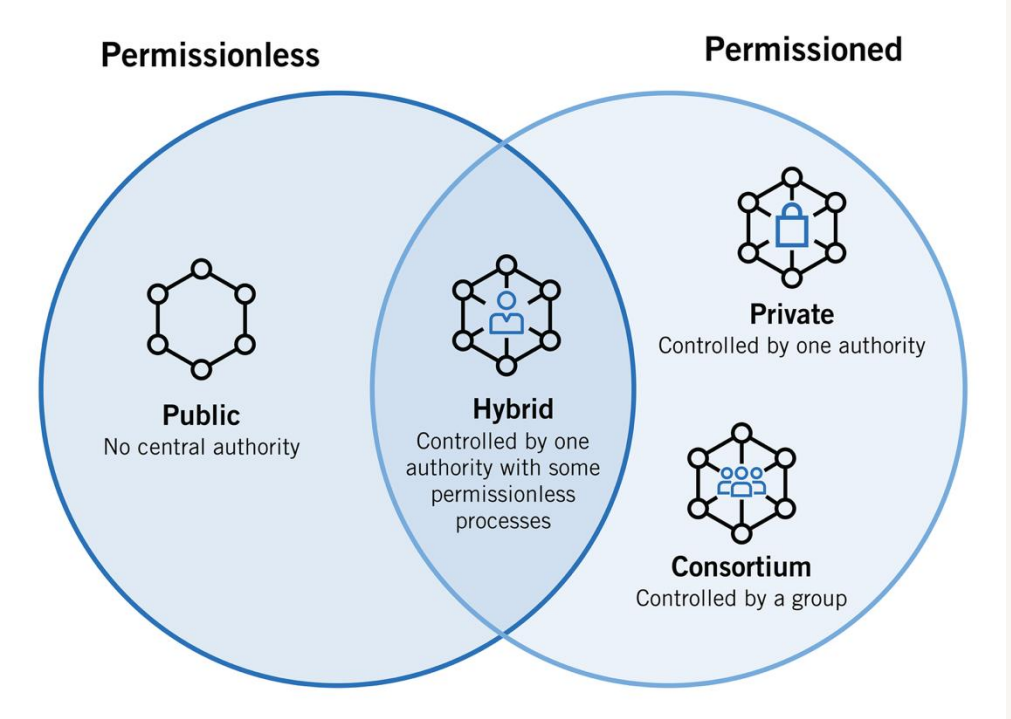
- A private blockchain is controlled by a single authority (e.g. a bank or an org)
- The network is private and set up between trusted partners (e.g. different bank branches)
- Sets own rules and regulations
- Restricted read/write access so that only authorised parties can participate
- Examples: Hyperledger Fabric, Hyperledger Sawtooth, Corda, etc.



https://www.foley.com/en/insights/publications/2021/08/-/media/images/insights/publications/2021/08/22mc35029-blockchain-graphic--permissions06.png

Hybrid blockchain

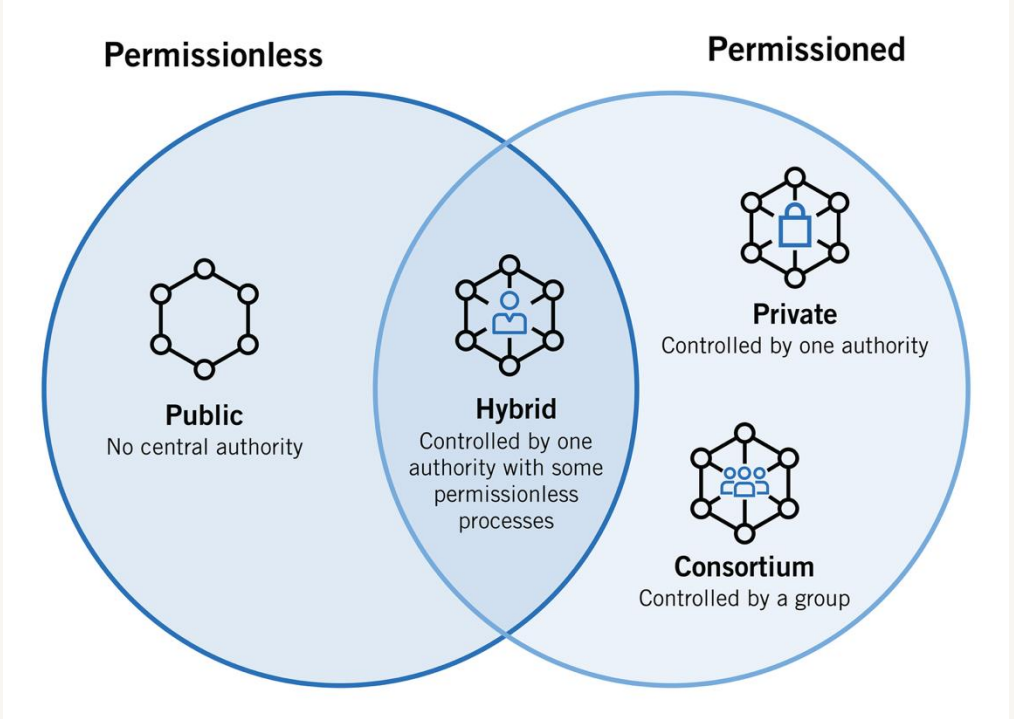
- A hybrid blockchain is a combination of public and private blockchain
- It is usually controlled by a central authority
- The authority sets up the rules
- Everyone can read data from the blockchain
- Write access is restricted
- Examples: LTO Network, Sovrin



https://www.foley.com/en/insights/publications/2021/08/-/media/images/insights/publications/2021/08/22mc35029-blockchain-graphic--permissions06.png

Consortium blockchain

- It is a private blockchain controlled by a set of private entities (e.g. a consortium of banks in Bangladesh)
- They set up their own rules and regulations
- Read and write access are controlled and are only allowed to the authorised entities
- Can be set up with private blockchains



https://www.foley.com/en/insights/publications/2021/08/-/media/images/insights/publications/2021/08/22mc35029-blockchain-graphic--permissions06.png

Summary

Types	Read	Write
Public	All	All
Private	Restricted	Restricted
Hybrid	All	Restricted
Consortium	Restricted	Restricted


THANK YOU
QUESTIONS?