Blockchain and cryptocurrency
Lecture goals

- Blockchain and traditional client-server architecture
- Characteristics of Blockchain
- Cryptocurrencies and initial coin offering
- Consensus mechanism and crypto-economics
- Blockchain types and smart contracts
- Blockchain platforms
  - Bitcoin
  - Ethereum
  - Hyperledger fabric
Blockchain

- Blockchain is a **decentralised distributed ledger technology** that runs over a **peer-to-peer (P2P)** network

Centralised  

Distributed
Traditional client-server vs Blockchain architecture

Image source: https://mlsdev.com/blog/156-how-to-build-your-own-blockchain-architecture
Blockchain structure

Form a *chain* by connecting each *block to previous block* by a *unique cryptographic hash*.
Blockchain - Who invented it?

- **Bitcoin**
  - Digital cryptocurrency
  - Authored in whitepaper in 2008 by Satoshi Nakamoto and launched in 2009
  - Devised the first blockchain database to keep transactions records

- **Satoshi Nakamoto**
  - Pseudonymous person or persons
  - Maybe an organisation
  - Two years later (April 2011) *disappears* from the web
Satoshi Nakamoto - Who is he?

- Satoshi Nakamoto - Japan
- Helger Lipmaa - *Estonia*
- Self-proclaimed Satoshi Nakamoto (Craig Wright - a fraud)
Satoshi Nakamoto?
Milton Friedman speaking about e-Cash in 1999
Blockchain before Bitcoin

Bitcoin is built on earlier work:

- Peer-to-peer/distributed computing
- Cryptography and Merkle Tree
- Cryptographically linking blocks
  - Stuart Haber and W. Scott invented in 1991
- Smart contracts
  - Nick Szabo in 1997 introduced the idea of smart contracts
- Digital currency
  - Nick Szabo in 2005 introduced *bitgold* as a form of digital money
Blockchain before Bitcoin

Bitcoin is built on earlier work:

- Peer-to-peer/distributed computing
- Merkle Tree
- Cryptographically linking blocks
  - Stuart Haber and W. Scott Stornetta invented in 1991
- Cryptography
- Smart contracts
  - Nick Szabo in 1997 introduced the idea of smart contracts
- Digital currency
  - Nick Szabo in 2005 introduced bit gold as a form of digital money

What different Satoshi Nakamoto did in Bitcoin cryptocurrency?
Blockchain before Bitcoin

Bitcoin is built on earlier work:

Decentralised distributed *consensus mechanism* and *incentive layer*
- Proof of work
- Crypto mining
- Crypto economics

Satoshi put together the already available technology along with consensus mechanism and introduced an incentive layer
- It overcomes the *centralisation* and *double-spending issues* in digital currency

- Nick Szabo in 2005 introduced bit gold as a form of digital money
Characteristics of Blockchain
Characteristics of Blockchain

- Distributed nature
- Decentralised / dis-intermediate
- Immutable ledger
- Tamper-evident
- Pseudo-anonymity
- Provenance
Distributed nature

- Peer-to-peer (P2P) network
  - Reliability
  - Greater security
  - High performance
  - Reduce cost
  - Nodes act as server as well as client

- Participants nodes
  - Distributed trust

- Distributed ledger
  - Redundancy, share and synchronize transactions/blocks
Decentralised (Dis-intermediary)

- No *centralised authority* to control the network or operations
- No *trusted-third party* to settle the transaction between two parties
- Transparent
Immutable ledger

- Append only
- Cannot delete / edit
Tamper-evident

- Minor change in a transaction will invalidate the complete ledger
Pseudo-anonymity

- Blockchain is not anonymous
- Pseudo-anonymity
  - *Disguised identity*
  - Linked to public address
    - No one will get to know the person actual name or other sensitive information
  - Increase confidentiality
Provenance

- Data provenance is a historical record
- Originates who made changes to it over time
- It validates if product/service is authentic
- Improve quality control and auditing
Cryptocurrencies & Consensus mechanisms
Cryptocurrencies

- Cryptography-based digital money/currency
- Exchanges of assets (funds) without third-party or centralised control authority (e.g., banks or other financial institutions)
Bitcoin

- Satoshi Nakamoto authored in 2008 and implemented in 2009
- First cryptocurrency
  - Satoshi refers to the smallest denomination of bitcoin (BTC)
  - 1 BTC = $10^8$ satoshi (1,000,000,00 satoshi)
- First implementation of blockchain technology

Currently, Bitcoin is the most traded cryptocurrency. Bitcoin market value is $212.51B (26th August, 2020)
Ethereum (Ether)

- The emergence of Ethereum took the blockchain to next level, usually relate to a *Blockchain 2.0*
- **Smart contracts** in their platform
- Ethereum introduces the Ether cryptocurrency
  - Wei refers to the smallest denomination of ether (ETH)
  - 1 ETH = $10^{18}$ wei (1,000,000,000,000,000,000 wei)
- **Vitalik Buterin** invented in 2015
Altcoins

- All the cryptocurrencies alternative to Bitcoin are called Altcoins
- Forks of Bitcoin
  - Bitcoin XT
  - Bitcoin cash
  - Bitcoin Gold, etc
- Small changes in Bitcoin and launch own cryptocurrency
  - Litecoin
- Defining own rules and Blockchain network
  - XRP (Ripple)
- Focusing on some particular problem solution
  - Storj - Decentralized cloud storage
  - Augur - Decentralized prediction market platform
Forks

- Blockchain *split/diverges* into two paths. There are two types of forks:
  - **Hard Fork**
    - Rule changes - usually a big change in consensus mechanism
      - (e.g., block size, mining algorithm, consensus protocol)
    - Contentious Hard Forks
      - It occurs when a significant portion of full nodes disagrees about which version of the software to run
  - **Soft Fork**
    - Software updates - minor changes that keep compatible with the older version
      - (e.g., hash address)
  - Not all forks are *intentional*, *accidental forks* could happen also
Forks

- Blockchain split/diverge into two paths. There are two types of forks:
  - **Hard Fork**
    - Rule changes - usually a big change in consensus mechanism
      - (e.g., block size, mining algo, consensus protocol)
    - Contentious Hard Forks
      - It occurs when a significant portion of full nodes disagrees about which version of the software to run
  - **Soft Fork**
    - Software updates - minor changes that keep compatible with the older version
    - (e.g., hash address)
- Not all forks are intentional, accidental forks could happen also
Initial Coins Offerings (ICOs)

- Mostly ERC20 tokens
- Raise funds
  - To provide some service, app or as an investment opportunity
- Top ICOs based on raised funds
  - **EOS** - $4.1 B
    - Smart contracts
  - **Telegram** - $1.7 B
    - Encrypted messaging & Blockchain ecosystem
  - **Dragon coin** - $320 M
    - Decentralized Currency for Casinos
- Many involved in *scams* or some *ponzi* schemes
Phases of launching an ICO

- Ideation phase
- Competitors analysis
- Legal side research
- Write a white paper
- Create ICO token
- Launch a website
- Marketing
Estonian ICOs project

- WePower
- *Lexit*
- *Polybius*
Consensus mechanism

Decision-making process

- Define the state of the ledger
- Dynamic way of reaching an agreement in a group
Proof of work (PoW)

Mining-based consensus mechanism

- Bitcoin and Ethereum
- Energy-waste
- Try to solve computational puzzle
Proof of stake (PoS)

Hold/Lock crypto assets to participate in consensus process

- Validators
- Needs assets
- Energy-efficient
- Ethereum migrating to PoS
Practical byzantine fault tolerance (PBFT)

Based on Byzantine generals problem

- Malicious nodes must not be greater than or equal to one-third of all the nodes in the system
  - According to the problem, \(3n+1\) generals deal with \(n\) traitors
- Number of nodes increase, the system becomes more secure
Other consensus mechanisms

- Delegated Proof of Stake (DPoS)
- Proof of Elapsed Time (PoET)
- Proof of Authority (PoT)
- Crash Fault Tolerance (CFT)
Crypto mining

Transactions are verified and added to the blockchain ledger.

- Nodes (Miner nodes, Full nodes, Validators nodes)
- Crypto economics
- Crypto puzzle
- Mining difficulty level
- Nonce and role of nonce
- *Crypto mining equipment*
Crypto mining equipment

Mining hardware to solve complex crypto puzzle.
Crypto wallets

- Store public and private keys
- Send and receive cryptocurrency
- Track the cryptocurrency balance
- Wallet could be:
  - Paper wallet
  - Hardware wallet
  - Software wallet
Blockchain types

- **Permissionless / public**
  - Requires no permission to join the Blockchain network
  - Open to all and transactions are visible to everyone
  - More transparent but slow transactions speed

- **Permissioned**
  - Requires permissions to join the Blockchain network
  - Only pre-defined nodes can participate in consensus mechanism
  - Fast, privacy oriented but less transparent

- **Private / Hybrid**
  - Controls and network governance assigned to one designated authority
  - Blockchain activity is only visible to chosen participants
  - More privacy oriented, scalable but less decentralised
Smart contracts

Smart contract is a digital contract

- *Piece of code* exists in a Blockchain network
- Execute when certain conditions meet
  - For example, self-execute when conditions/terms meet between buyer and seller
- Reduce the need of a trusted-third party, enforcement costs, fraud losses, malicious and accidental exceptions
Decentralised autonomous organisation (DAO)

DAO manage the governance of the business

- Interconnected *web of smart contracts*
  - Automate all its essential and non-essential processes
  - Eliminate central points of weakness, middlemen, and unaligned stakeholder interests
- Ultimate goal of DAO is to *eliminate human input*
Off-chain and on-chain storage

● Off-chain data
  ○ Off-chain data is any non-transactional data that is too large to be stored in the blockchain efficiently, or, requires the ability to be changed or deleted
    ■ For example, images, videos, word or PDF documents etc
  ○ Off-chain data storage reduces the storage requirements

● On-chain data
  ○ Transaction related data
  ○ Reference of an off-chain stored data
  ○ Bitcoin allows 1 Mb data per block
  ○ Ethereum allows 20-30 KB data per block
How funds transfer in dis-intermediary environment?

For example, Bob wants to send money to Robert in Blockchain-based dis-intermediary environment.
Blockchain platforms
Blockchain platforms

Blockchain platforms are growing after the emergence of Bitcoin and smart contracts:

● **Bitcoin**
  ○ Purely a cryptocurrency platform, an example of permissionless Blockchain

● **Ethereum**
  ○ Decentralised applications (dApps), an example of permissionless Blockchain

● **Hyperledger-fabric**
  ○ Decentralised applications (dApps), an example of permissioned Blockchain

● **Corda**
  ○ Main focus on financial-based decentralised applications (dApps), an example of permissioned Blockchain

● **Multichain**
## Comparison of Blockchain platforms

<table>
<thead>
<tr>
<th></th>
<th>Bitcoin</th>
<th>Ethereum</th>
<th>Hyperledger-fabric</th>
<th>Corda</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type</strong></td>
<td>Permissionless</td>
<td>Permissionless</td>
<td>Permissioned</td>
<td>Permissioned</td>
</tr>
<tr>
<td><strong>Smart contract</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>SC language</strong></td>
<td>Scrypt</td>
<td>Solidity</td>
<td>Go</td>
<td>DAML</td>
</tr>
<tr>
<td><strong>Consensus</strong></td>
<td>PoW</td>
<td>PoW, PoS (migrating)</td>
<td>PBFT, CFT</td>
<td>Transaction validity &amp; uniqueness</td>
</tr>
<tr>
<td><strong>Cryptocurrency</strong></td>
<td>Bitcoin (BTC)</td>
<td>Ether (ETH)</td>
<td>No official cryptocurrency</td>
<td>No official cryptocurrency</td>
</tr>
<tr>
<td><strong>Transactions/s</strong></td>
<td>7 TPS</td>
<td>8-9 TPS</td>
<td>Thousands</td>
<td>Thousands</td>
</tr>
<tr>
<td><strong>Confidentiality</strong></td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Applications</strong></td>
<td>Cryptocurrency only</td>
<td>Multiple applications</td>
<td>Multiple applications</td>
<td>Financial applications</td>
</tr>
</tbody>
</table>
Bitcoin network

- **Bitcoin P2P protocol**
  - Nodes interconnect in a mesh network with a flat topology
  - No server, no centralised service or hierarchy

- **Bitcoin core**
  - *Reference client*
  - Contains wallet, miners, full Blockchain database, network routing node

- **Extended bitcoin network**
  - Combination of different protocols
    - Bitcoin P2P protocol
    - *Stratum protocol*
    - Pool-mining protocol
  - Pool servers, pool mining nodes and lightweight wallet clients
Bitcoin network

- **Nodes**
  - Mining nodes, full nodes, thin/light nodes, validator nodes

- **Transaction pools**
  - Mempool
    - Maintains *unconfirmed* list of transactions
    - Transactions are known to Bitcoin network but not yet added in Blockchain
  - Orphan pool
    - *Missing parent* of the transaction
    - Transaction store temporarily
    - When parent arrive, then transaction move from orphan pool to mempool
Bitcoin node network discovery

When a new node boots up, it must discover other bitcoin nodes on the network in order to participate.

- Establish a TCP connection
- Initial handshake
- Address propagation
- Synchronising the blockchain
Bitcoin node network discovery

When a new node boots up, it must discover other bitcoin nodes on the network in order to participate.

- Establish a TCP connection
- *Initial handshake*
- Address propagation
- Synchronising the blockchain
Bitcoin node network discovery

When a new node boots up, it must discover other bitcoin nodes on the network in order to participate.

- Establish a TCP connection
- Initial handshake
- **Address propagation**
- Synchronising the blockchain
Bitcoin node network discovery

When a new node boots up, it must discover other bitcoin nodes on the network in order to participate.

- Establish a TCP connection
- Initial handshake
- Address propagation
- *Synchronising the blockchain*
Bitcoin block and Blockchain

- **Genesis block**
  - First block of the chain

- **Blockchain size**
  - Approx. **286 GB** and increasing

- **Full nodes amount**
  - Approx. **9,000 to 10,000** full nodes

- **Block structure**
  - Block size
  - Header
  - Transaction counter
  - Block content

*Image source: A Decentralised Approach to Task Allocation Using Blockchain*
Ethereum network

- **Ethereum P2P protocol**
  - Nodes interconnect in a mesh network with a flat topology
  - No server, no centralised service and hierarchy

- **Ethereum virtual machine**
  - Stack-based virtual machine that executes bytecode
  - Handles smart contract deployment and execution

- **Ethereum clients**
  - Go-ethereum (Geth) - Golang implementation and developed by Ethereum Foundation
  - Parity Ethereum - Rust implementation and developed by Parity Tech

- **Nodes**
  - Full nodes, light nodes, archive nodes
Ethereum node network discovery

- Geth continuously attempts to connect to other nodes
- Geth finds peers through discovery protocol
  - In discovery protocol, nodes are gossipping with each other to find out about other nodes on the network
  - The peer discovery algorithm is based on the kademlia protocol
- Geth use bootstrap nodes
  - Bootstrap nodes maintain a list of all nodes that connected to them in a period of time (predefined temporal value, for example last 24 hours)
  - Bootstrap nodes are special nodes that provide the connection information
- The connecting peers then synchronize with the peers
Ethereum block and Blockchain

- **Genesis block**
  - First block of the chain

- **Blockchain size**
  - Approx. 159 GB and increasing
  - Ethereum archive nodes size is approx. 4 TB

- **Full nodes amount**
  - Approx. 8,000 full nodes

- **Block structure**
  - Header
  - Ethereum account state
  - Block content

*Image source: A Platform Architecture for Multi-Tenant Blockchain-Based Systems*
Hyperledger fabric network

- **Organisation**
  - Entity which has access to channels and can issue identities to participants
  - Governs one or more network peers and depends on a membership service provider

- **Channels**
  - Channels allow a specific set of peers and applications to communicate with each other

- **Membership Service Provider (MSP)**
  - Provides an abstraction for membership operations
    - Issuing certificates,
    - Validating certificates
    - User authentication
Hyperledger fabric network

- **Peer**
  - Host ledgers and smart contracts
- **Orderer**
  - Keep consistent Ledger state across the network. Creates the block and delivers that to all the peers

Hyperledger fabric block and Blockchain

- **Genesis block**
  - First block of the chain

- **Blockchain size**
  - Depends on the organisation operations

- **Nodes amount**
  - Configurable

- **Block structure**
  - Header
  - Data
  - Metadata

Image source: LedgerGuard: Improving Blockchain Ledger Dependability
Lecture goals

● Blockchain and traditional client-server architecture
● Characteristics of Blockchain
● Cryptocurrencies and initial coin offering
● Consensus mechanism and crypto economics
● Blockchain types and smart contracts
● Blockchain platforms
  ○ Bitcoin
  ○ Ethereum
  ○ Hyperledger fabric