DISTRIBUTED LEDGERS

Ledgers: foundation of accounting, currently mostly centralized control
- Facilitates data integrity, faster access and control
- Updated through transactions (atomic, durable and consistent)

Distributed Ledgers (DL): no central authority controlling data
- Transactions: should be also atomic, durable and consistent
- Less performant as agreement mechanisms are required
- Replicated securely across geographic locations, to do so:
  - Consensus formation mechanisms, p2p protocols, crypto infrastructure

Blockchain: a type of DL which uses blocks to maintain shared state
CONSENSUS MECHANISMS

Allow secure data state update according to state transition rules
Facilitate agreement for data consistency, incentivize honesty

Approaches (all rule what is a valid block):
  - Byzantine Fault Tolerance
  - Proof of Work / Stake

Bizantine Fault Tolerance:
  - Mathematical verification of messages
  - Tolerates ~ 1/3 dishonest or absent participants
  - Ex.: functioning network with 1 out of 4 faulty nodes
  - Ensure a minimum number of nodes reach consensus about the sequence and result of transactions before appending them to the shared ledger

Bitcoin: consensus based on Proof of Work
How a Bitcoin transaction works

Bob, an online merchant, decides to begin accepting bitcoins as payment. Alice, a buyer, has bitcoins and wants to purchase merchandise from Bob.

1. **Creating a new address**: Bob creates a new Bitcoin address for Alice to send her payment to.

2. **Submitting a payment**: Alice transfers bitcoins from her wallet to Bob's new address.

3. **Verifying the transaction**: The transaction is verified by the network, ensuring it is legitimate.

4. **Transaction confirmed**: The transaction is added to the blockchain, completing the process.
CONSENSUS MECHANISM

Proof of Work (Mining)
- Participants only accept valid block if its hash is less than target number (difficulty)
- To find valid hash, miners guess and check hashes
- When found, broadcast valid block to network
- Solution includes reward for miner, incentivize honest behaviour
- Other participants verify the solution before accepting it
- Difficulty adjusted to desired block frequency
- Computationally expensive (high energy use)
  - Discourage cheating
  - Problem: low transaction volume
MINING (IN ETHEREUM BLOCKCHAIN)

The answer to the guess is a block, which contains:
- List of transactions (updates to the system)
- Hash of the most recent block
- Random number nonce (number used once to do hash guessing game)
- Miner reward (transaction of reward to winner node, only valid if block accepted by the network)

The longest block chain is acknowledge as the correct one, and the way to secure rewards, thus incentivising coordination.
1. You sign your transaction
2. You send your transaction

3. Your transaction goes to a MEW node...

4. ...who put it the pool of all signed transactions
   IF YOUR TX IS PENDING, IT'S IN THE POOL

5. Miners pick transactions from the pool
   HIGH GAS PRICES PICKED FIRST!

6. Miners then put transactions in a block and add it to the chain
   ONCE IN THE BLOCKCHAIN, YOUR TX IS PERMANENT!

https://steemit.com/ethereum/@n-ur/behind-the-scene-on-how-myetherwallet-works-simple-illustration
Miners of last 1000 blocks

- Ethermine
- f2pool
- SparkPool

Uncles mined in the last 1000 blocks

- Ethermine
- Nanopool
- f2pool

Direct link
Uncle link

Valid transactions in the pool: 117652 (showing 500 max)
Ether value in the pool: 78849 (39,740,385.43 USD)

http://ethviewer.live/
PUBLIC AND PRIVATE BLOCKCHAINS

Classification depending on permission levels

Public or permission-less: allow anyone to join as a trust-less participant, anyone can read/write data

- Pseudo-anonymous transactions, addresses of participants are public but not necessary linked to an identity
- Transaction processors must invest financially to prevent fraud
  - For instance through Proof of Work
  - Incentivised by direct economic reward (cryptocurrency)
- Cost digital currency to process transactions
- Censorship resistant (anyone can access and record transactions)
- Examples: Ethereum (public) or Bitcoin
PUBLIC AND PRIVATE BLOCKCHAINS

Permissioned or Consortium: only verified participants are allowed
- Block validator identities are known allowing punishment of dishonest actors
- Different consensus mechanisms are possible that achieve higher transaction throughput than in public ones
- Example: Alastria (https://alastria.io)

Private or sandboxes: for rapid application development, instant deployment and single-enterprise deployment solutions
- Prototyping and learning
# Blockchain Platforms

<table>
<thead>
<tr>
<th></th>
<th>Ethereum</th>
<th>Hyperledger</th>
<th>Bitcoin</th>
<th>Corda</th>
<th>Ripple</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Consensus Algorithm</strong></td>
<td>Proof of Work (Proof of Stake)</td>
<td>PBFT</td>
<td>Proof of Work</td>
<td>BFT or RAFT</td>
<td>Ripple Protocol</td>
</tr>
<tr>
<td><strong>Network Size</strong></td>
<td>Global</td>
<td>Limited</td>
<td>Global</td>
<td>Limited</td>
<td>Limited</td>
</tr>
<tr>
<td><strong>Protocol Implementation(s)</strong></td>
<td>Go, C++, Python, Haskell, Java, Rust, Ruby, JavaScript</td>
<td>Go, Java</td>
<td>C++, Java</td>
<td>Kotlin, Java</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Consortia</strong></td>
<td>Enterprise Ethereum Alliance</td>
<td>Hyperledger Foundation</td>
<td>N/A</td>
<td>R3</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Native Digital Currency</strong></td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Built-in Smart Contracts</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td><strong>Blocks</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td><strong>Mining</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td><strong>Public/Private Interoperability</strong></td>
<td>Public, Private/Permissioned, Permissionless</td>
<td>Private/Permissioned</td>
<td>Public/Permissionless</td>
<td>Private/Permissioned</td>
<td>Private/Permissioned</td>
</tr>
<tr>
<td><strong>Developer Community Strength</strong></td>
<td>30X</td>
<td>X</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

*Source: Consensys Academy*
THANK YOU FOR YOUR ATTENTION

QUESTIONS?

ROBERTO GARCÍA
http://rhizomik.net/~roberto/

Frankfurt, June 19th, 2019