CMPSC 390
Ethereum and Smart Contracts. Altcoins.

Janyl Jumadinova

Credit: Authors of "Mastering Bitcoin" and "Bitcoin and Cryptocurrency Technologies"

February 2, 2021

Transferable Benefits of Bitcoin

- Pseudonymous, cryptographic identities allow for accountability.

Transferable Benefits of Bitcoin

- Pseudonymous, cryptographic identities allow for accountability.
- Democratic decisions made through consensus protocol that doesn't require trust.

Transferable Benefits of Bitcoin

- Pseudonymous, cryptographic identities allow for accountability.
- Democratic decisions made through consensus protocol that doesn't require trust.
- Immutable ledger of truth.

Transferable Benefits of Bitcoin

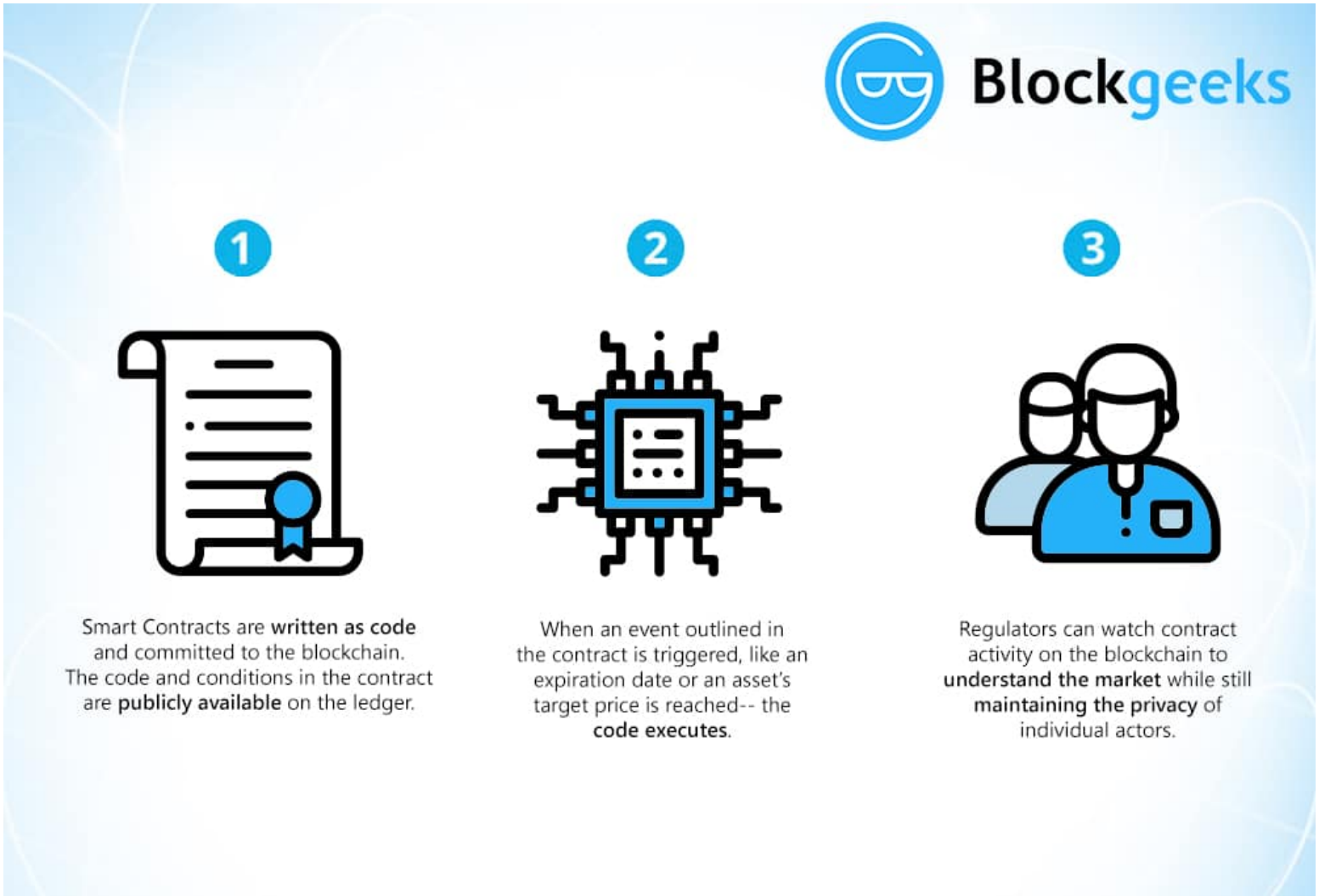
- Pseudonymous, cryptographic identities allow for accountability.
- Democratic decisions made through consensus protocol that doesn't require trust.
- Immutable ledger of truth.
- Uncensorable, cannot be controlled by any one party.

Transferable Benefits of Bitcoin

- Pseudonymous, cryptographic identities allow for accountability.
- Democratic decisions made through consensus protocol that doesn't require trust.
- Immutable ledger of truth.
- Uncensorable, cannot be controlled by any one party.
- Distributed: no central point of failure.

Smart Contracts

Code that **facilitates**, **verifies**, or **enforces** the negotiation or execution of a digital contract.



Ethereum

https://ethereum.org

Ethereum

https://ethereum.org

Ethereum is a decentralized platform designed to run smart contracts:

- Distributed computer to execute code.

Ethereum

https://ethereum.org

Ethereum is a decentralized platform designed to run smart contracts:

- Distributed computer to execute code.
- Account-based blockchain.

Ethereum

https://ethereum.org

Ethereum is a decentralized platform designed to run smart contracts:

- Distributed computer to execute code.
- Account-based blockchain.
- Transactions == state transaction function.

Ethereum

https://ethereum.org

Ethereum is a decentralized platform designed to run smart contracts:

- Distributed computer to execute code.
- Account-based blockchain.
- Transactions == state transaction function.
- Ethereum's native asset is called ether: – Basis of value in the Ethereum ecosystem.

Ethereum

- **Block creation time**: $13sec$ (Ethereum) vs $10min$ (Bitcoin)
- Ethereum price:

Bitcoin vs. Ethereum

	Bitcoin	Ethereum
Ticker	BTC	ETH
Smallest Unit	1 Satoshi = 0.00000001 BTC	1 Wei = 0.000000000000000001 ETH
Purpose	Be a global decentralized payment system.	Be a decentralized supercomputer to power DApps from around the world.
Max Supply	21,000,000	No fixed supply
Block Reward	12.5 BTC (halving every 210,000 blocks)	2 ETH
Consensus Algorithm	Proof-of-work (POW)	POW now but will move on to POS using Casper Protocol
Throughput	7-8 tps	15-20 tps
Miner Fees	Collects transaction fees	Collects Gas fees

Ethereum Accounts

User owns private keys to an account.

Ethereum Accounts

User owns private keys to an account.

- Externally Owned Accounts:
  - Owned by some external entity (person, corporation, etc.)
  - Can send transactions to transfer ether or trigger contract code.
  - Contains: Address, Ether Balance.

Ethereum Accounts

User owns private keys to an account.

- Externally Owned Accounts:
  - Owned by some external entity (person, corporation, etc.)
  - Can send transactions to transfer ether or trigger contract code.
  - Contains: Address, Ether Balance.
- Contract Accounts:
  - "Owned" by contract.
  - Code execution triggered by transactions or function calls (msg).
  - Contains: Address, Associated contract code, Persistent storage.

Ethereum Smart Contracts Purposes

Ethereum Smart Contracts Purposes

- Store and maintain data.
  - Data represents something useful to users or other contracts.
  - Ex: a token currency or organization's membership.

Ethereum Smart Contracts Purposes

- Store and maintain data.
  - Data represents something useful to users or other contracts.
  - Ex: a token currency or organization's membership.
- Manage contract or relationship between untrusting users.
  - Ex: financial contracts, insurance.

Ethereum Smart Contracts Purposes

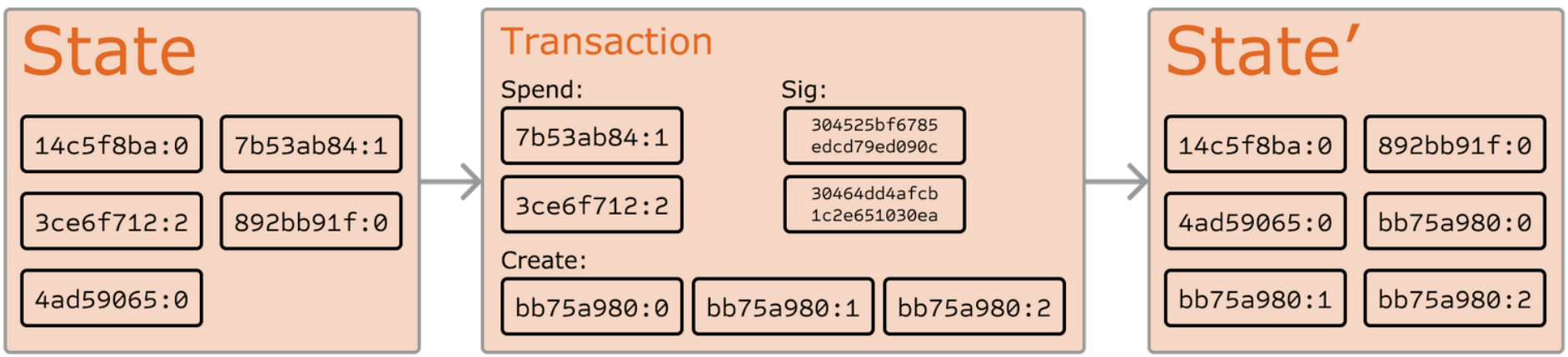
- Store and maintain data.
  - Data represents something useful to users or other contracts.
  - Ex: a token currency or organization's membership.
- Manage contract or relationship between untrusting users.
  - Ex: financial contracts, insurance.
- Provide functions to other contracts.
  - Serving as a software library.
- Complex Authentication.

Ethereum Mining

1. Download the entire Ethereum blockchain.
2. Verify incoming transactions and Run Smart Contract code invoked by transactions.
3. Create a block.
4. Find a valid nonce.
5. Broadcast your block.
6. Profit!

Ethereum Mining

- Ref: https://ethereum.org/en/whitepaper/



Altcoins

Ref: https://coin360.com/

Features of altcoins

- Better (or different) security.
  - Mining puzzle.

Features of altcoins

- Better (or different) security.
  - Mining puzzle.
- Contract/platform features.

Features of altcoins

- Better (or different) security.
  - Mining puzzle.
- Contract/platform features.
- Different parameters and monetary policy: inflation, inter block time.

Features of altcoins

- Better (or different) security.
  - Mining puzzle.
- Contract/platform features.
- Different parameters and monetary policy: inflation, inter block time.
- Community or common interest support

Litecoin

https://litecoin.org/

- Litecoin launched in September 2011.
- Memory-hard mining puzzle.

Dogecoin

https://dogecoin.com/

- Launched in December 2013.
- Culture - tipping, charity, sponsorship.

Explore Alcoins

https://www.coingecko.com

- Select one Altcoin.

Explore Alcoins

https://www.coingecko.com

- Select one Altcoin.
  - When and why was it created?
  - What are its features?
  - What is its current status?