
Smart Contracts

Outlines

- **What is a Smart Contract?** Advantage
- of Smart Contracts Applications of
- Smart Contracts Other Use Cases and
- Characteristics

What is a Smart Contract?

A **smart contract** is a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract.

- What Nick Szabo proposed in 1994:
 - A **smart contract** is a computerized transaction protocol that executes the terms of a contract.
- IBM:
 - **Smart contracts** are lines of code that are stored on a blockchain and automatically execute when predetermined terms and conditions are met.
 - **Chaincodes**

What is a Smart Contract?

- Characteristics of smart contracts
 - Simply computer programs that acts as agreements where the terms of the agreement can be programmed with the ability to self-execute.
- A primitive ancestor of smart contracts
 - Vending machine: Coins in and soda out.
- More sophisticated ones



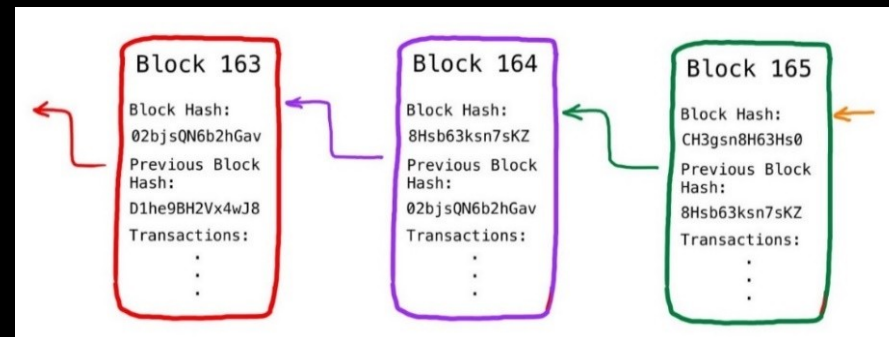
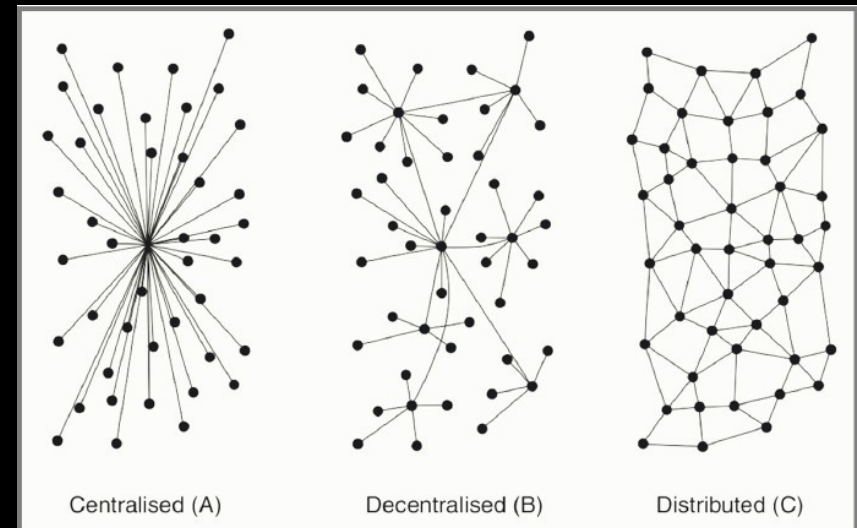
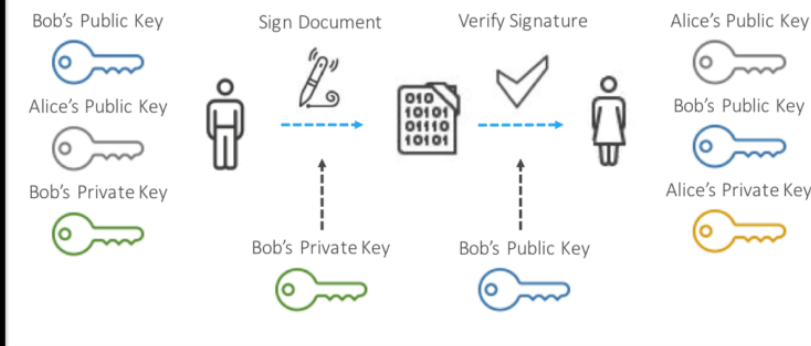
Significance of Smart Contracts on Blockchain

A *distributed, append-only ledger of provably signed, sequentially linked, and cryptographically secured transactions that's replicated across a network of computer nodes, with ongoing updates determined by a software-driven consensus.*

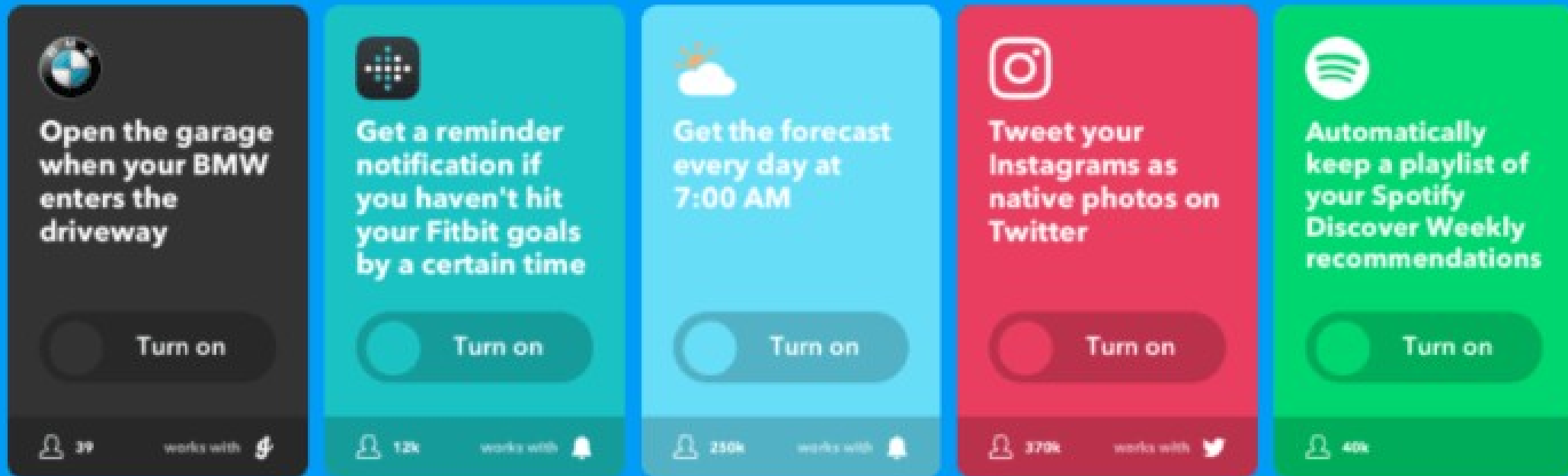
Smart contract on blockchain:

1. Immutability (irreversible)
2. Security
3. Can be more transparent

Signing with asymmetric encryption



An Example of a Kind-of-Smart Contract



Advantages of Smart Contract

Characteristics of smart contracts on blockchain:

1. Immutability (irreversible)
2. Security (in the sense that the blockchain does not fail easily)
3. Transparency

- Compared to traditional contracts:
 - High certainty of contract terms
 - Can be more transparent (subject to debate)
- Additional benefits over other digital contracts:
 - Contracts can be immutable and irreversible
 - Can be more transparent

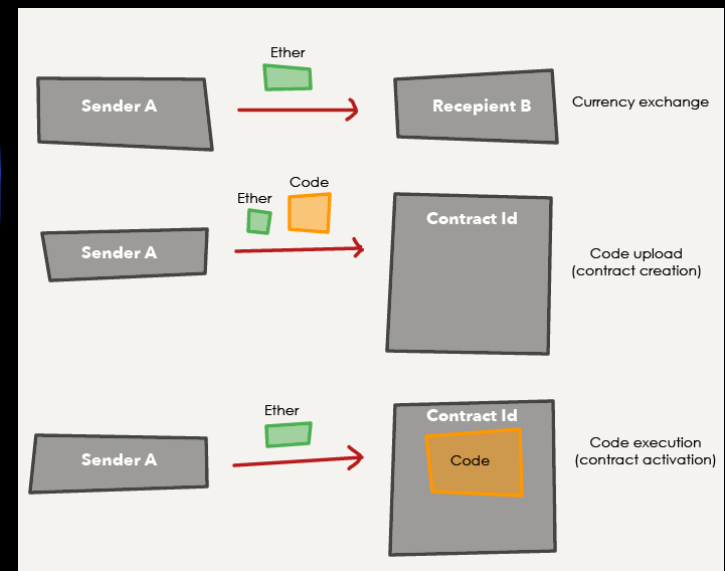
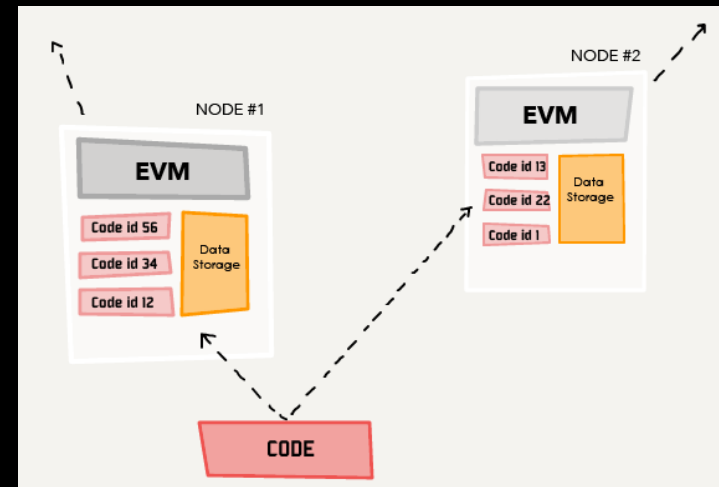
How Do Smart Contracts Work?

- Ethereum

1. **Send** the application to the system, the code and associated data is **replicated** around the network.
2. Once stored, the Ethereum Blockchain assigns **a unique address** to reference the uploaded code.
3. **Execute** the code by calling the program at that **address**.

Ethereum has three types of transactions:

- a) Transfer of **Ether**
- b) Creating a smart contract
- c) Transaction with a smart contract (activate a smart contract)



Outlines

- What is a Smart Contract? Advantage
- of Smart Contracts **Applications of**
- **Smart Contracts** Other Use Cases and
- Characteristics

Use Case of Smart Contracts

- Current use cases
 - Banking and financial service contracts
Money transfer; flight delay insurance; securities trading, clearing and settlement
 - Prediction markets Replacing escrow
 - services
 - Token sales: Initial Coin Offering, Securities Token Offering

Use Case

“Future” use case

- Transfer of assets registered on blockchain
- Tangible assets (land, house, vehicles)
- Copyrighted contents (music, etc)

