Blockchains & Crypto

alchemy | 2022

Blockchains

Purpose of Blockchain

- With a blockchain we can decentralize where code runs and agree on the output
  - There is no single owner of the code's execution*
    - The code always runs as programmed
    - The code is transparently verifiable

**developers can choose to write privileged code*

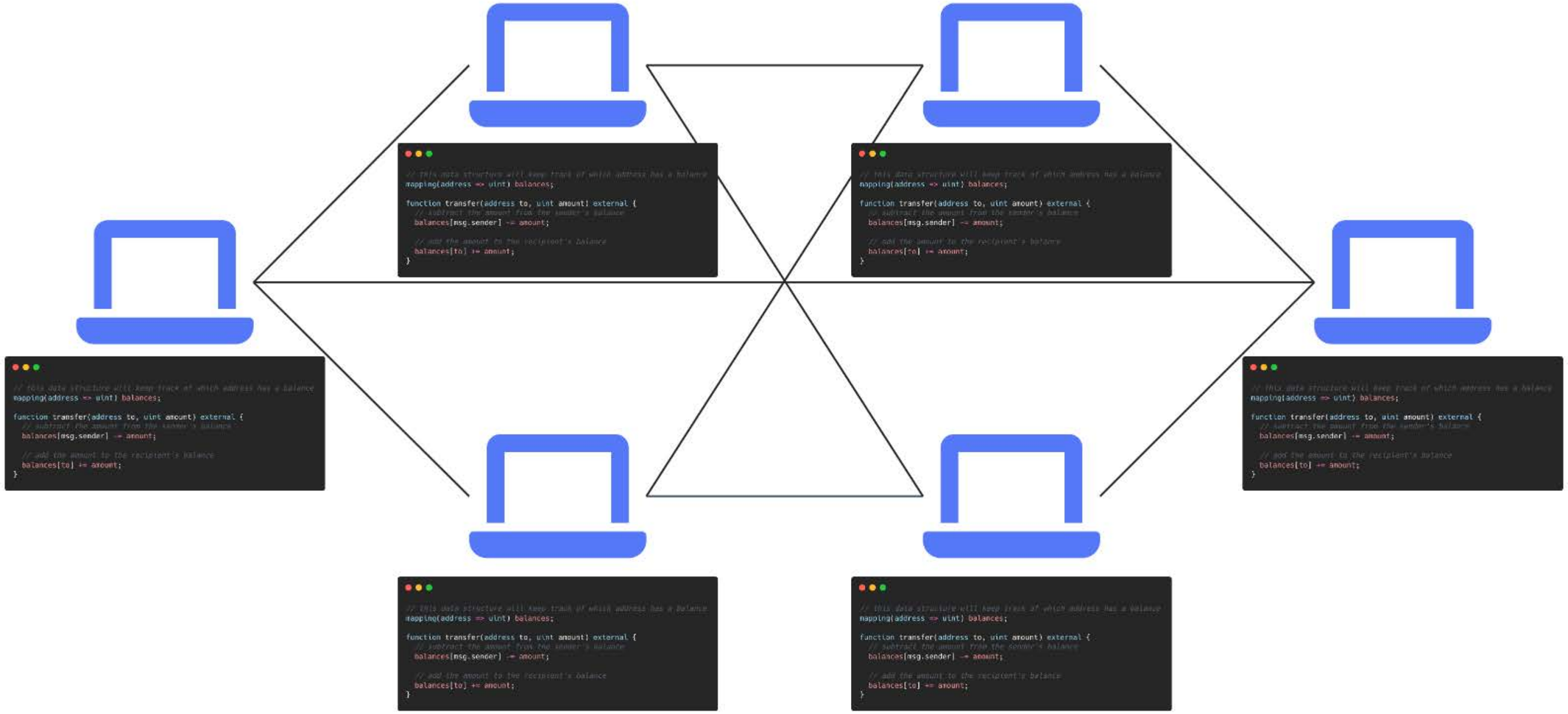
Purpose of Blockchain

```
// this data structure will keep track of which address has a balance
mapping(address => uint) balances;

function transfer(address to, uint amount) external {
  // subtract the amount from the sender's balance
  balances[msg.sender] -= amount;

  // add the amount to the recipient's balance
  balances[to] += amount;
}
```

Is this code decentralized? 🤔

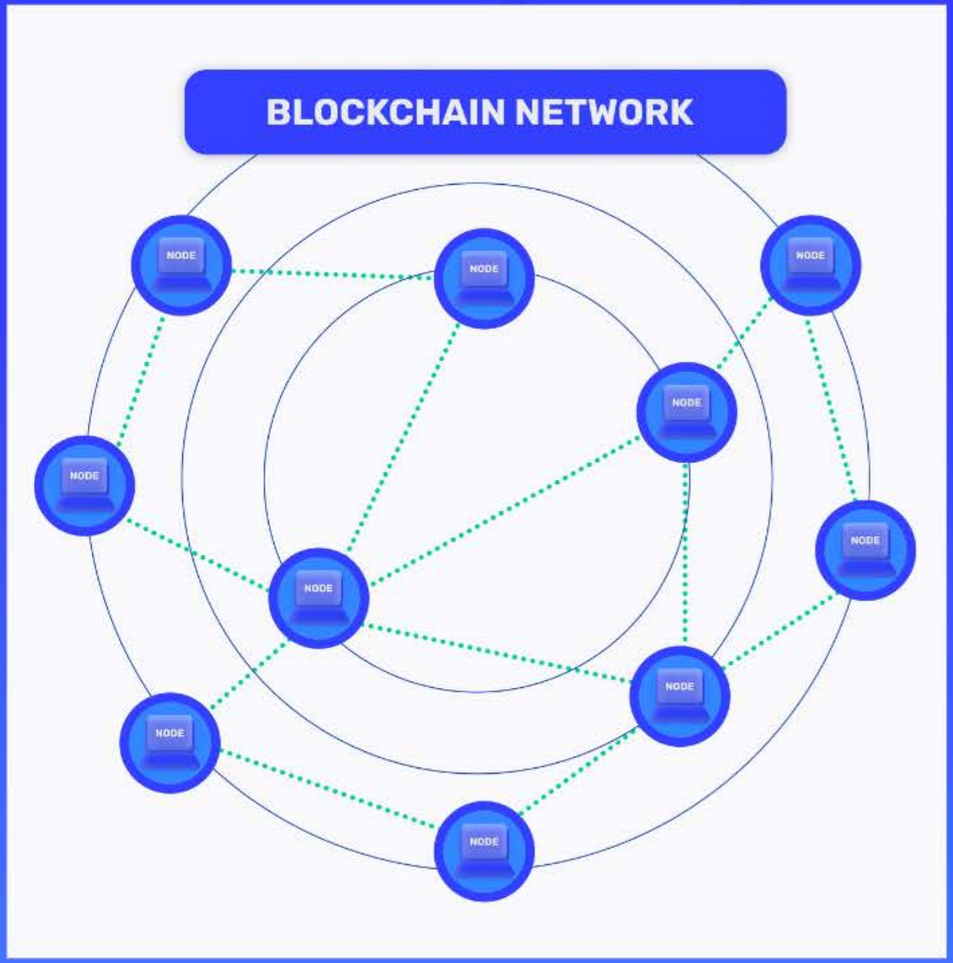
depends where the code is deployed, unless deployed to decentralized blockchain like Ethereum

Code Decentralization



Blockchain Network

- Blockchain: protocol connecting these machines
- Each machine or “node” in the network will run code as it is written
- The blockchain enforces these rules
- Since the program is enforced, it is called a “smart contract"



Bitcoin: the first! ₿

- Bitcoin was the first successful blockchain and cryptocurrency 💸
- But, there was much research and many attempts before it! 🧑‍🔬
- Most of the components were discovered already. 🤯

How does it work? 🤔

- **Proof of Work** - Security 🔒
- **Mining Rewards** - Financial Incentives 💰
- **Public Key Cryptography** - Authentication 🔏
- **Linked Data Structure** - Chronology ⌛
- **Peer to Peer Network** - Permissionless 🌐

☝️ These components work together in concert.

Decentralization emerges from a properly setup network. 🌋

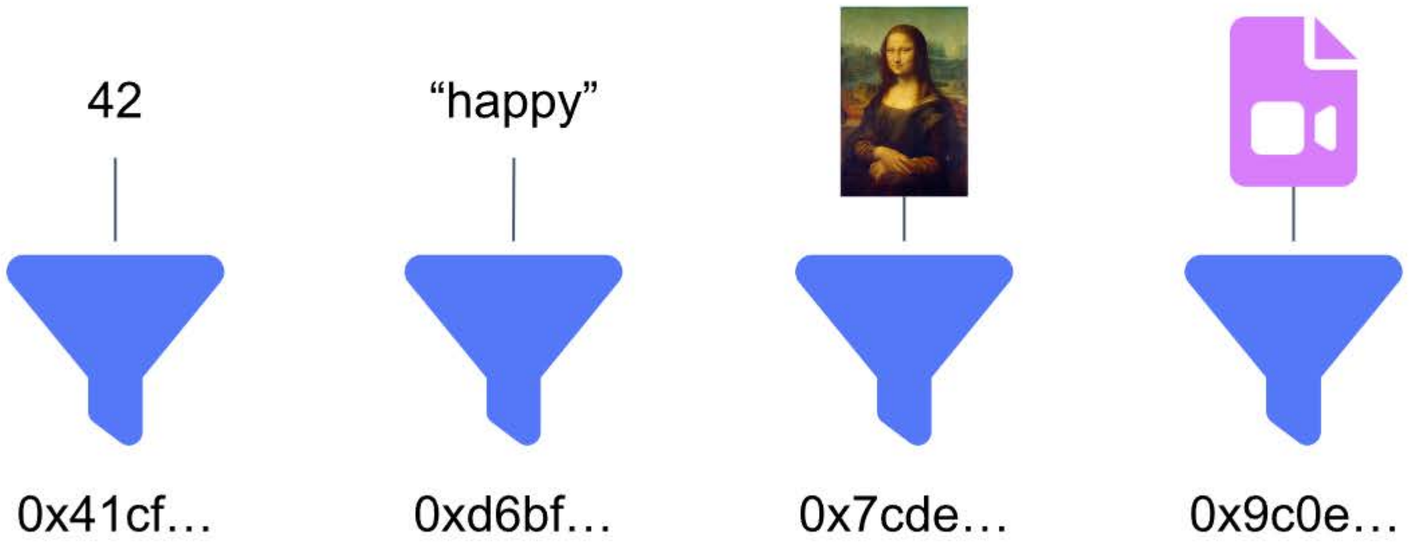
Crypto

Crypto 🔒

- Way before cryptocurrency, there was crypto
- Two important primitives for our purposes:
    - **Cryptographic Hashes**
    - Public Key Cryptography

Hash Function

- Hash: Give me some input, big or small and I'll give you a fixed size output
    - Input can be any type of data: number, string, image, video, etc..



Cryptographic Hash Functions 🔒

A cryptographic hash is a function with these properties:

- 🔮 **Deterministic** 结果是确定的
- 🎲 **Pseudorandom** 结果不能预测，随机的
- ➡️ **One-way** 要知道结果match哪一个input，只能一个一个试
- 🏎️ **Fast to Compute**
- 💥 **Collision-resistant** 重叠几率小（output有2^{256}种可能性）

SHA256 is one-such function which provides a 256 bit output

Cryptographic Hash Functions 🔒

Two important use cases for Hash functions for us:

1. Commitments (Protocol & Smart Contract)
2. Proof of Work

Next:

Try Hashing