Bitcoin

- A protocol that keeps track of unspent transaction outputs, like a ledger
- Each node on the decentralised network maintains a copy
- This allows each user of the protocol to verify transactions themselves
  - Eliminates the counterparty risk of centralization

Bitcoin

- Why does Bitcoin have value?
  - Because someone is willing to exchange $$$, goods, or services for it!

- Scarcity
  - Only 21M BTC will ever be created

- Transparency
  - No means of obfuscating transactions on the network

Bitcoin

Inside of a Transaction

- A signed tx is broadcast to the network saying saying account 1 is sending account 2 1 BTC

- The tx is then added to the Mempool to await validation

- A miner will add the tx to a proposed block, which is then broadcast to other nodes

Bitcoin

Inside of a Transaction

- The other nodes will verify all of the info in the block (txs) meets the consensus rules of the protocol

- Once the block has been verified, it will be added to the chain and become a part of the history of the ledger

- The miner to propose the successful block receives a reward

Bitcoin

Bitcoin vs Banks; benefits of decentralisation

- Bitcoin is a open source protocol

- Not operated or maintained by any central group of authority

- Allows for “trustless” peer to peer value transactions