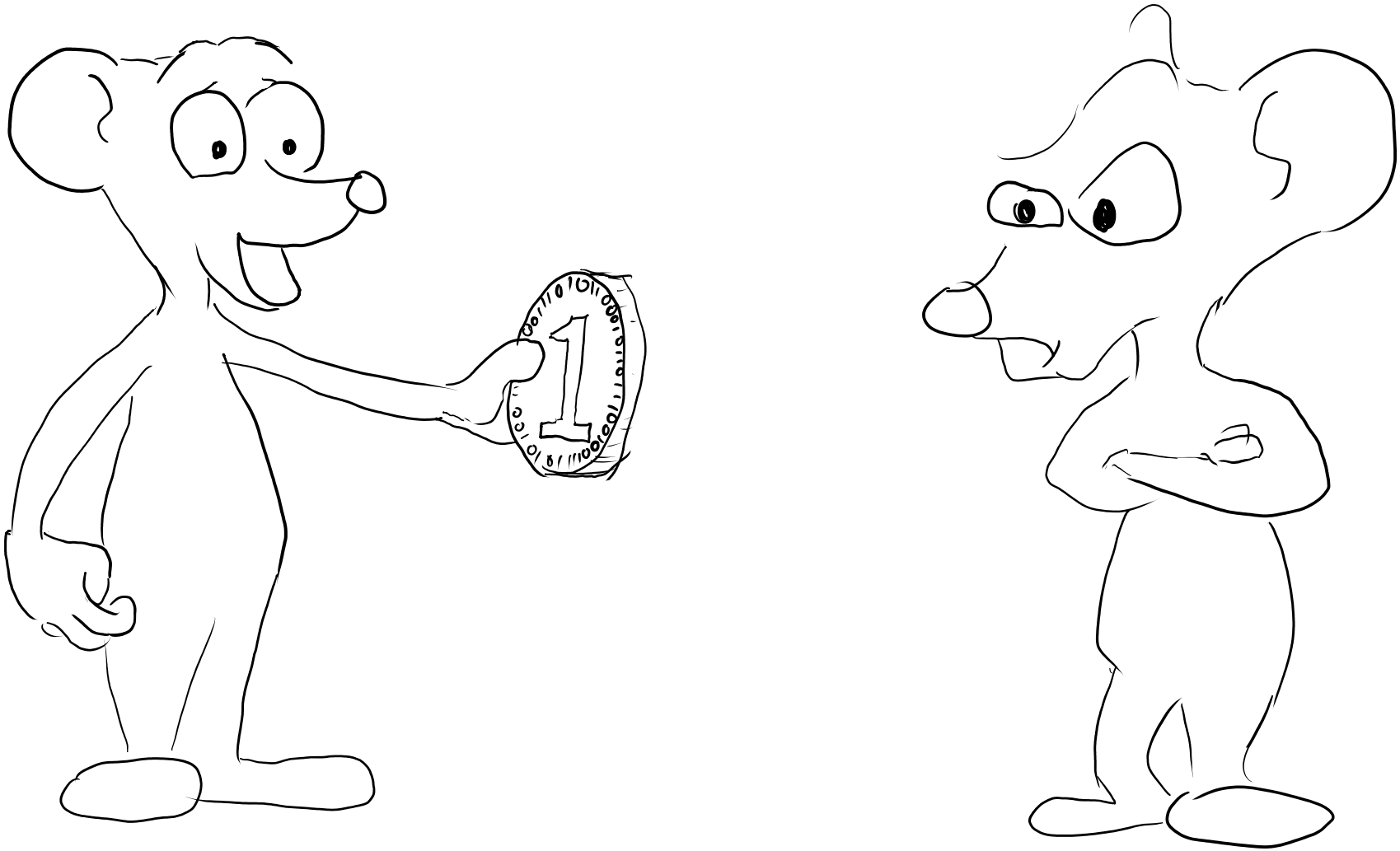
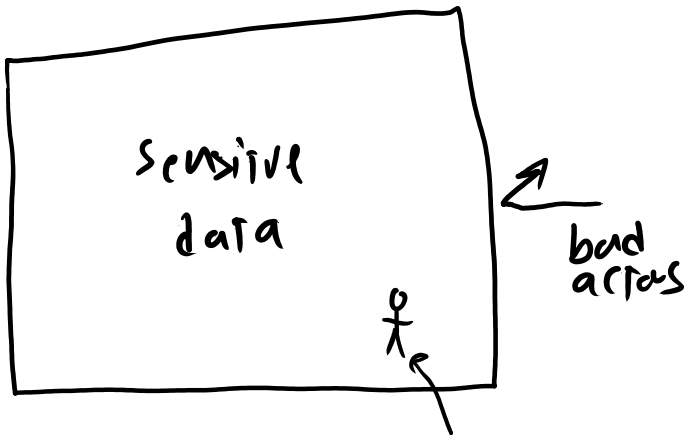

1

Authorization

Firewall ---- may be hybrid ---- fine-grained Access Control List



- user1: read
- usr2: read, write
- User3: change who can access
- User4: nothing

Principle of least privilege

↳ many people are unhappy

↑ small as possible

Trade off

Security

Usability

Block chain

Cryptocurrency

indelible ← cannot delete, edit, reorder anything

distributed ← no one agent in charge; consensus

ledger ← structured list of entries

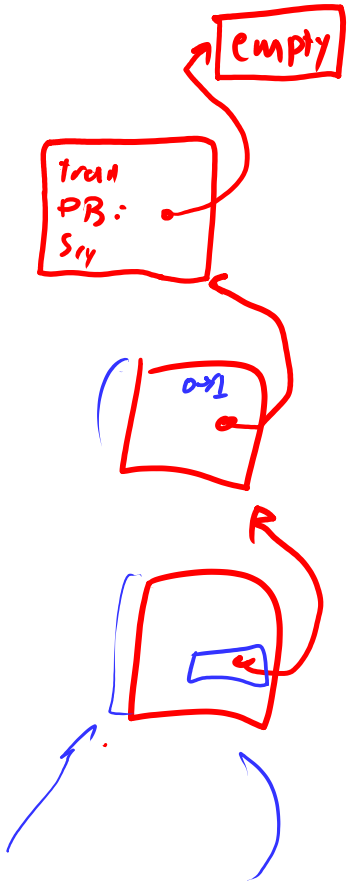
add to ↑ end of but not edit

Block chain

Block:

- Transaction User1 gives $3 to User 2
- Previous block: hash
- Signed: user1

Hash ←



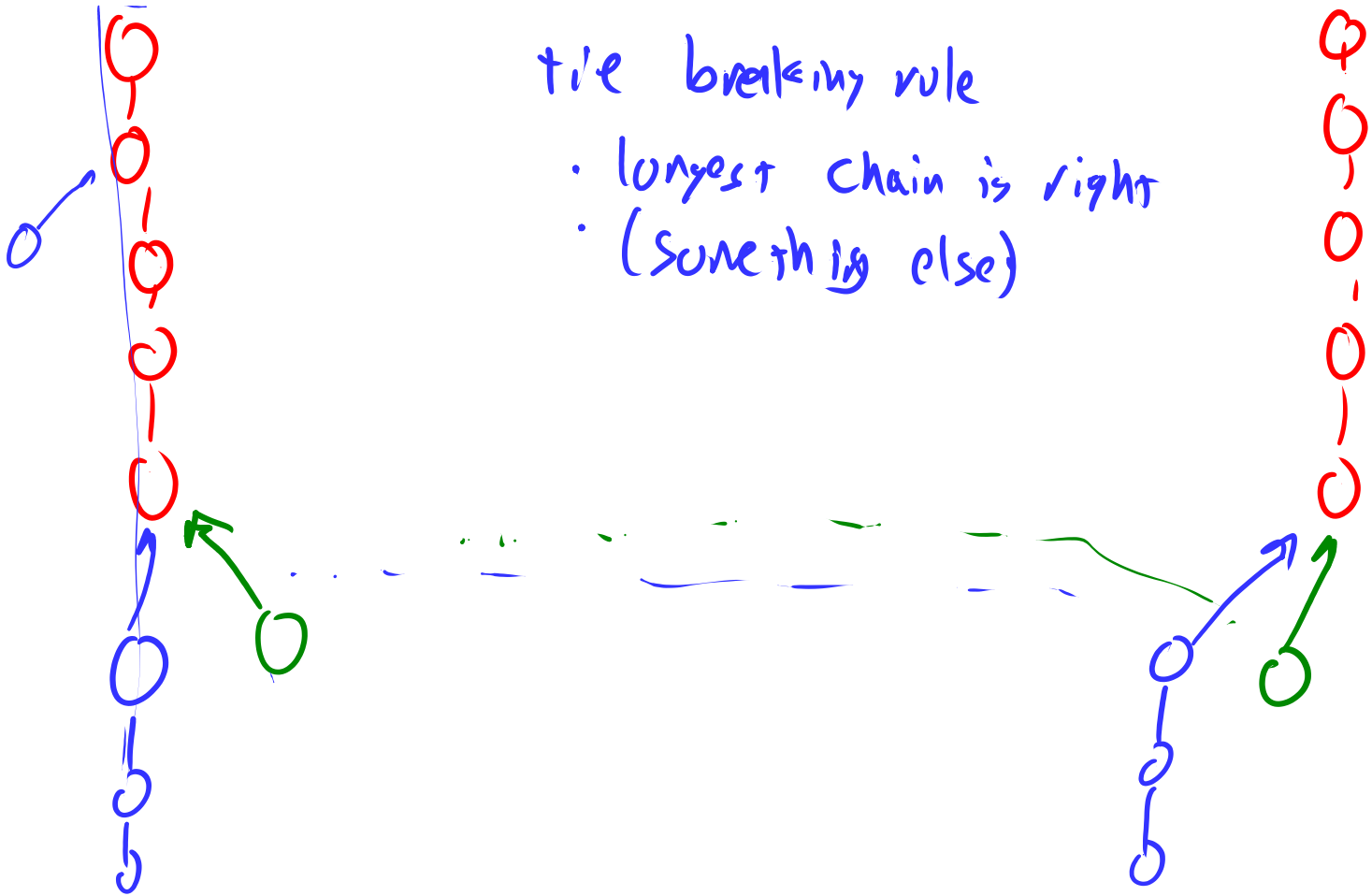
To use:

- each have engine blockchain

1. make block at end of chain & share with everyone

2. recieve a block: check valid, add to chain

Conflicting blocks



Malice

Bitcoin

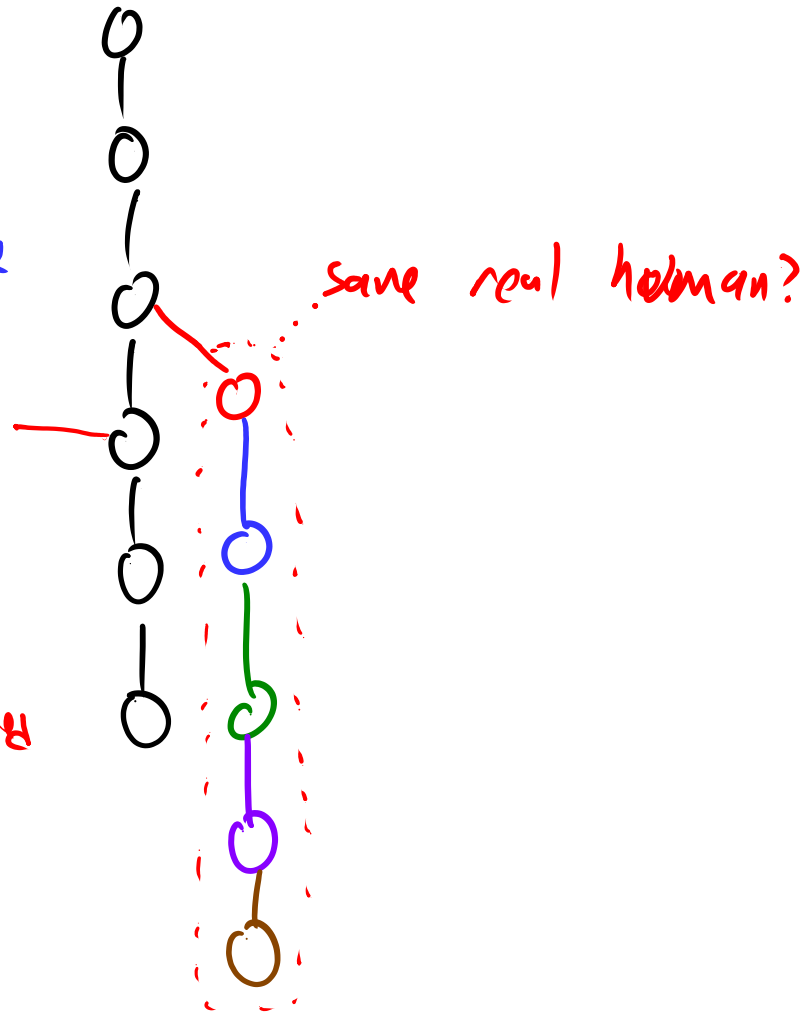
- Proof of Work
  = each block's hash must be small in value

- Proof of Stake
  = enter a raffle to add a block

Ethereum

- non-anymous users

Ripple



Currencies are Backed by —

- Government: taxes, fee, fines ... any to govt
- Crime: ransomes