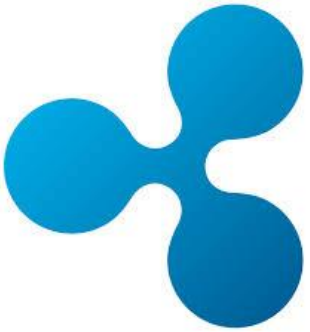
Cryptocurrencies & Smart Contracts

What they are…

… and what they aren't







What is a Cryptocurrency?

- Define it by its basic properties:
  - Ownership: Each coin "belongs" to someone
    - Requires their permission to transfer
  - Consensus: everyone agrees where the money is.
    - Easy to get with "real" coins
  - Irreversibility: past transactions cannot be changed
  - Scarcity: we can't create arbitrary amounts of money
- What makes a currency a **crypto**currency?
  - Distributed
    - No need to trust single entity
  - **Permissionless**

Cryptocurrency in a Nutshell

- Digital signatures:
  - Coins are “owned” by a public key
  - Transfer requires a signature – must know corresponding secret key
  - Well-established cryptographic primitive
- Why aren’t signatures enough?
  - No instantaneous broadcast
  - Different users see events in different order
  - Transaction order is critical!
- So how do we agree on the “correct” order?
  - Democracy! Majority decides…

Cryptocurrency in a Nutshell 

- We're done? Not quite…
  - How many votes do you get?
  - No verifiable IDs on the Internet
- Nakamoto's solution:
  - Prove you spent CPU power in order to vote
  - New assumption: majority of CPU power is honest
- In more detail:
  - We run a "puzzle lottery":
    - first person to solve generates "block" (and next puzzle)
    - determines tx order since previous block

"On the Internet, nobody knows you're a dog."

What Cryptocurrency **isn't**

- It's not **private**
  - Every transaction appears on a "public ledger"
- It's not **cheap**
  - No inherent lower limit for centralized (permissioned) transaction cost
  - Proof-of-work gives a minimum cost for transactions
- It's not **fast**
  - E.g. Bitcoin currently at <5 transactions per second
- Solving these problems is a work-in-progress…

Smart Contracts?

- “Coin with code”
  - The code is the contract

- Standard coin code:
  - “anyone who knows secret key can claim this coin”

- More advanced:
  - “anyone who knows two out of three keys can claim coin”

- Even more advanced:
  - If you give an input to this program and it says ok, you can claim coin