Blockchain

A technical primer

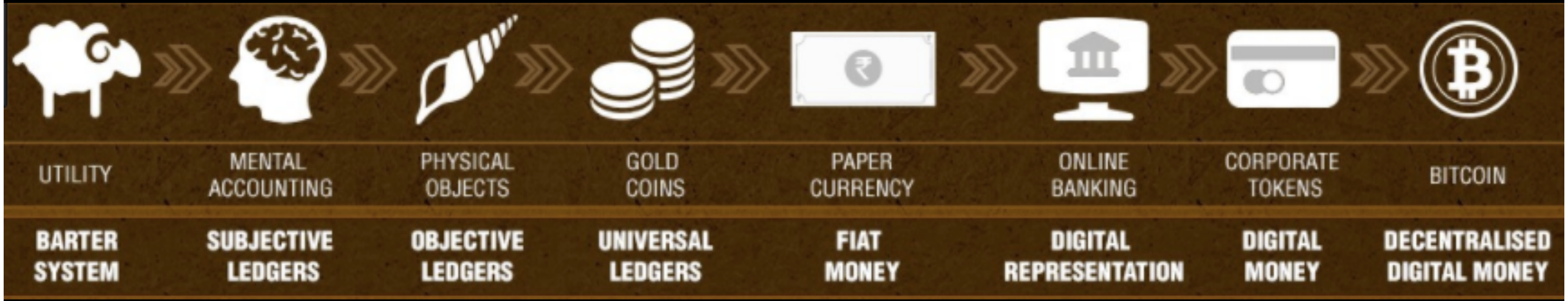
- Rahul Jadhav

Before we begin…

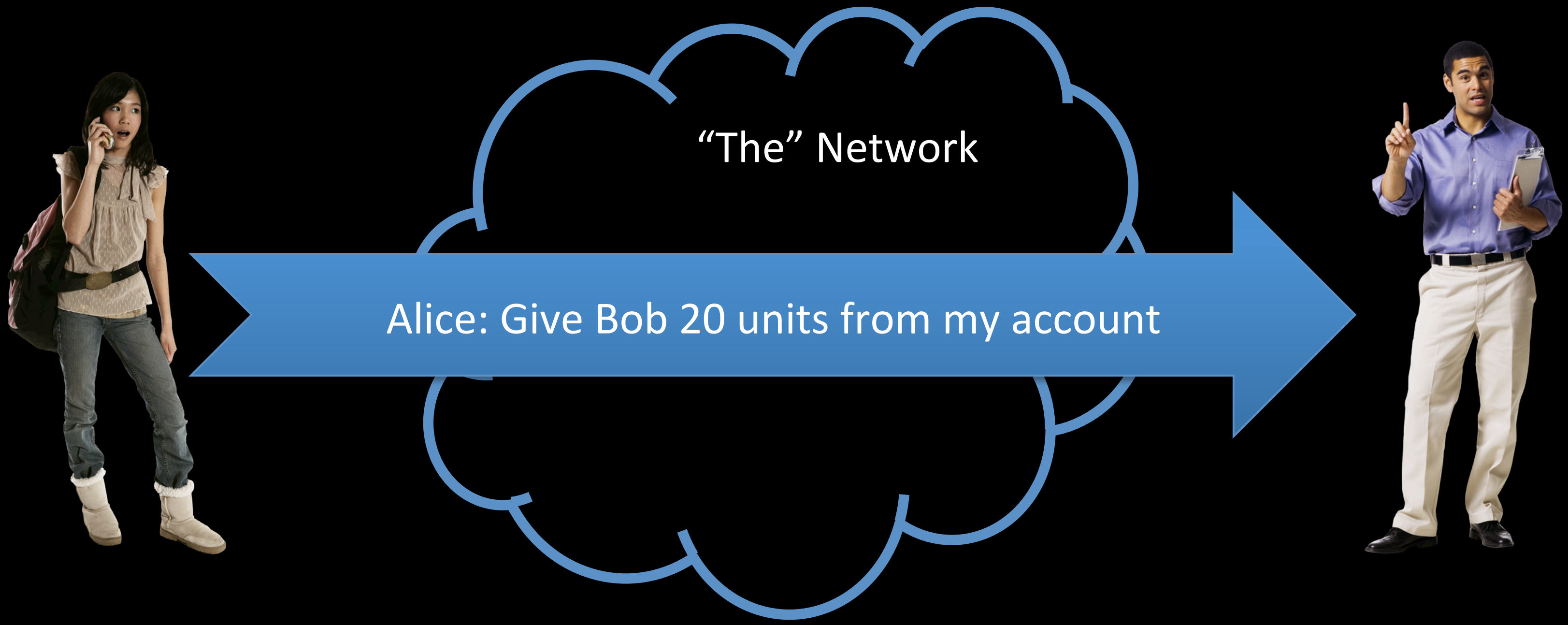
- Public/Private key
- Hash Function (SHA256 in our case)
- Digital Signatures
- Distributed P2P network
- Merkel Trees

Before we begin…

- It’s important to understand
  - What’s a CryptoCurrency?
  - At what point money became centralized?



Some background…



“The” Network

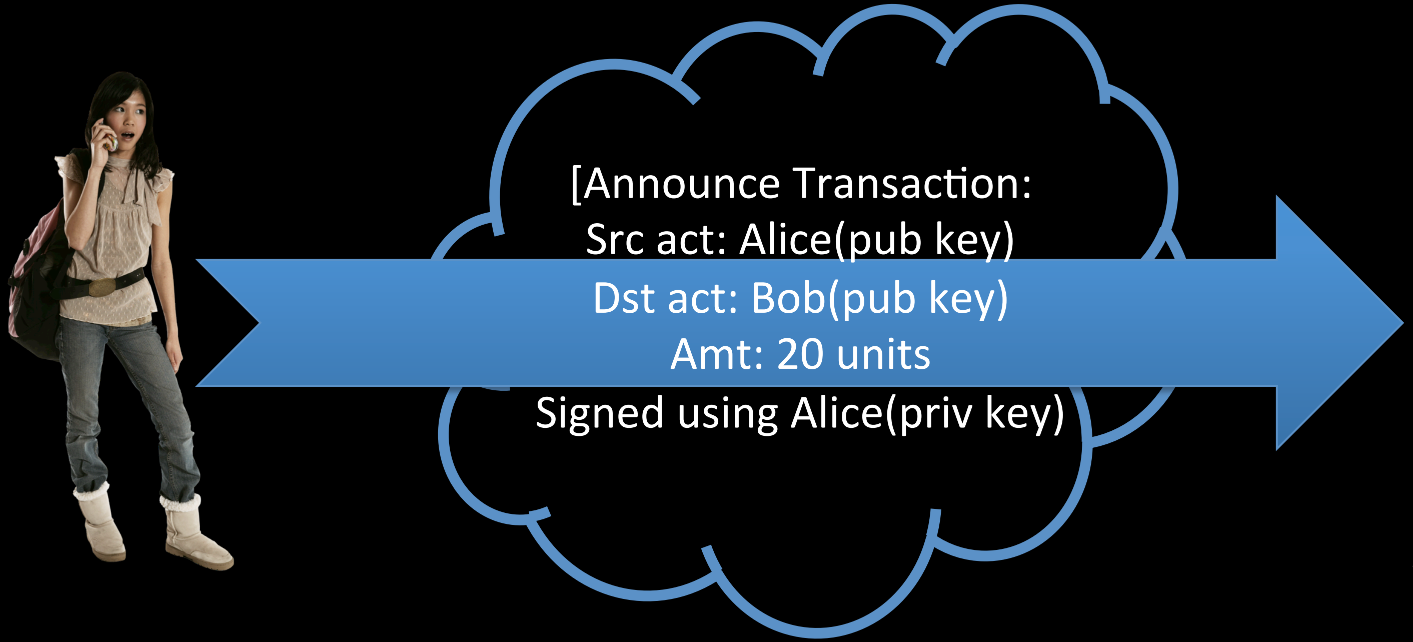
Alice: Give Bob 20 units from my account

- Currency characteristics
  - Universal acceptability
  - Recognized Issuer - Government
  - Account Management - Banks
  - Wallet Management - Users

CryptoCurrency - Challenges

- How to issue new currency?
  - No physical mint
- Where to store the transactions?
  - No central authority
- How to ensure transactions cannot be tampered?
- Transaction initiation:
  - How to ensure that the source account has enough funds?
- How would users identify each other?

But it can be trivially solved…



[Announce Transaction:
Src act: Alice(pub key)
Dst act: Bob(pub key)
Amt: 20 units
Signed using Alice(priv key)

Ponder… Immutability

- Even though the network can't change the value, they can still delete the transaction at later point of time.
  - But you can use Merkel trees to make it immutable

Another Problem … Consensus

- Who has the right set of transactions?
  - How will "The Network" decide?

Still unanswered…

- Where did Alice got her 20 units from in the first place?
  - Where is the mint?

Now lets talk blockchain

- For a truly open cryptocurrency, we need an backend: BlockChain
- A Distributed ledger which is
  - Immutable, Tamperproof
  - You can’t delete the transactions nor modify
  - But everyone can see the transactions
  - Network together decides which is the right set of transactions

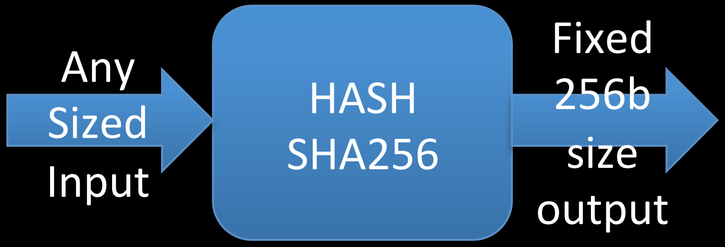
Further about blockchain…

- Trustless open network
  - Anyone can participate. Does not need permission from any central authority or from the network itself for participating.
  - All you have to do is play by the rules
  - Most importantly the rules are part of the software which is open sourced.

Unraveling the mystery…

HOW DOES BLOCKCHAIN GET THESE CHARACTERISTICS?

Hash function Primer



- Any size input → Fixed size output
- Same input → Same output
  - Anyone can use the same input with the same hash function and get the same output
- Slight change in input → Complete change in output

Hash Primer

```
~:rahuljadhav$ for((nounce=0;nounce<10;nounce++)); do echo
"rahularvindjadhav$nounce" | shasum -a 256; done

50add82e952c0576d92b9f427fc08018654c948b4217be7deb6b7e404a05f368  -
f100f16b5d61df9c66c0b5b6153ffc64563528a62bcb28305d02b35600f5726e  -
eacc0436420aab21881c81cac310bf14b5b6db3c532eddc93c68835dadd09571  -
74d1523faa9585a43246ff35d55f72f4495274307b1512866beba4454050f3fd  -
5fe6d82026120c90598910c1db9d6f10b3140d75cf2db0f4b91d994ef6443723  -
0d0d2bcbfab885864b8290e228ed81d1f52870c6f6f897f4152213a4e1c6909d  -
5c989d795d929617bc45acb590f00af8adb7caa0125fc8410f2de5fdd5db5a56  -
10f24a6b4328f592576e7638802db4089178d6bf9ae617e769bf9e2725037c9e  -
d5e4dbe86edc500671efe92af27bfbae4f5abda494b004a0c671de087abb51ed  -
f5080d2391ff0bf6ad424f4acfc98846690d9938bd436aaa9d422e901ec3d586  -
```

Hash Primer

- What is the probability that the first bit is zero for any HASH output?

Hash Primer

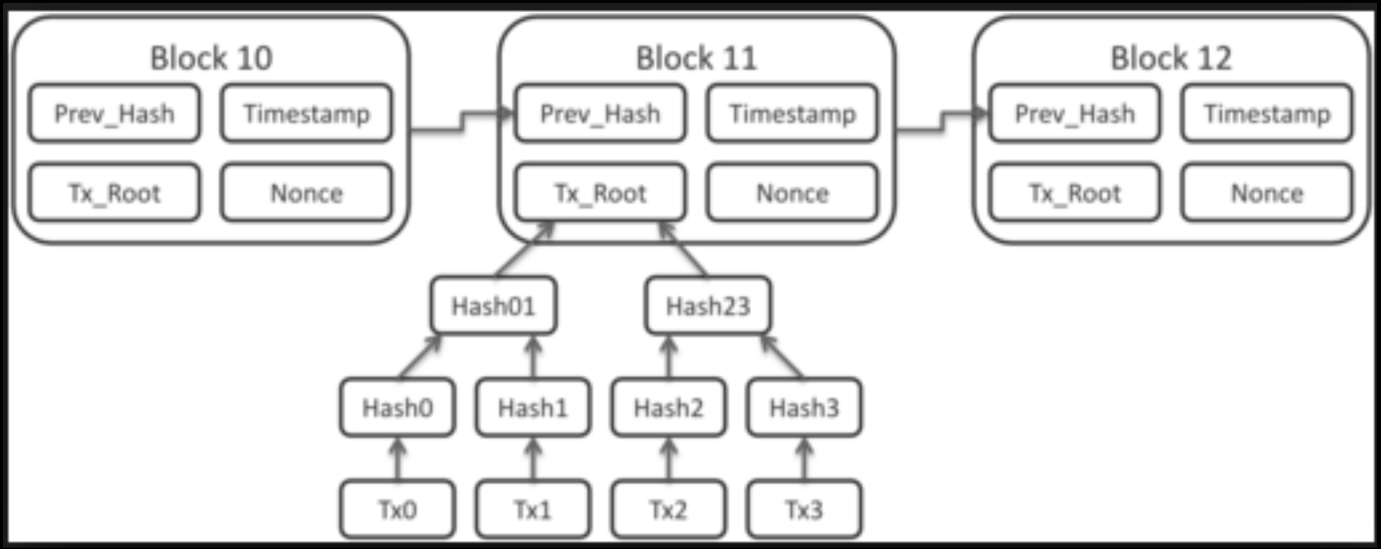
- What is the probability that the first 40 bits are zero for any HASH output?
- Introduce Difficulty Target…

Introducing Mining or Proof of work…

- A Miner assembles a set of transactions and starts mining with an objective
  - To find a nounce which will satisfy the difficulty target.
- How does PoW map to approx time?
  - PoW, a moving target because of advancements in computing platforms
  - PoW of avg 10 minutes prevails on public blockchain

What does a block contain?

- Daisy-chained blocks
  - – Single bit change in any previous blocks will result in whole chain getting invalidated
- Genesis Block – First block mined



Miner’s Fee

- Concept of Coinbase
  - Value slashing of a coinbase
- Collecting transaction fees
  - Implications of having transaction fees
- Electricity/Maintenance cost vis-à-vis coinbase earnings
  - Mining bases shifting to China
  - Shifting to colder places where heat dissipation is easier
  - Tremendous improvements in hardware mining

Question

- Why is having a difficulty target which maps to physical time so important?
- PoW is what provides immutability characteristic to Blockchain.

Question

- What happens if two or more miners mine the same block number at relatively similar times?
  - Note that miners decide which transactions to select by themselves.
- Did it ever happened that multiple branches kept on increasing at the same height?
  - Highly improbable, but it happened. Why?

Achieving Consensus

- Understanding chain branches
- Consensus: Maps to longest branch
- How to decide that the branch is long enough?

Fallout of Consensus mechanism

- Transaction CONFIRMATION time
  - Transactions from unaccepted branches are as good as not processed
- Different apps may choose to have different confirmation times

Miner’s Computational Race

- Why does it makes sense for miners to abandon the current block if someone else solves it first?
- Mining future blocks in advance: There is no way miners can start mining future blocks because of the dependency on previous block header.

Empty Block Mining Issue

- Miners can choose to mine a block with empty transactions
  - Why would miners do that?
    - Adding transaction to the block means validating them
    - Checking if there are duplicates
    - All this takes time
  - Relation to coinbase value which will drop over a period of time.

Double Spending Issue

- What is Double Spending?
- How is Double Spending possible?
- Why Confirmation time so important?
  - How does it tackle double spending issue?

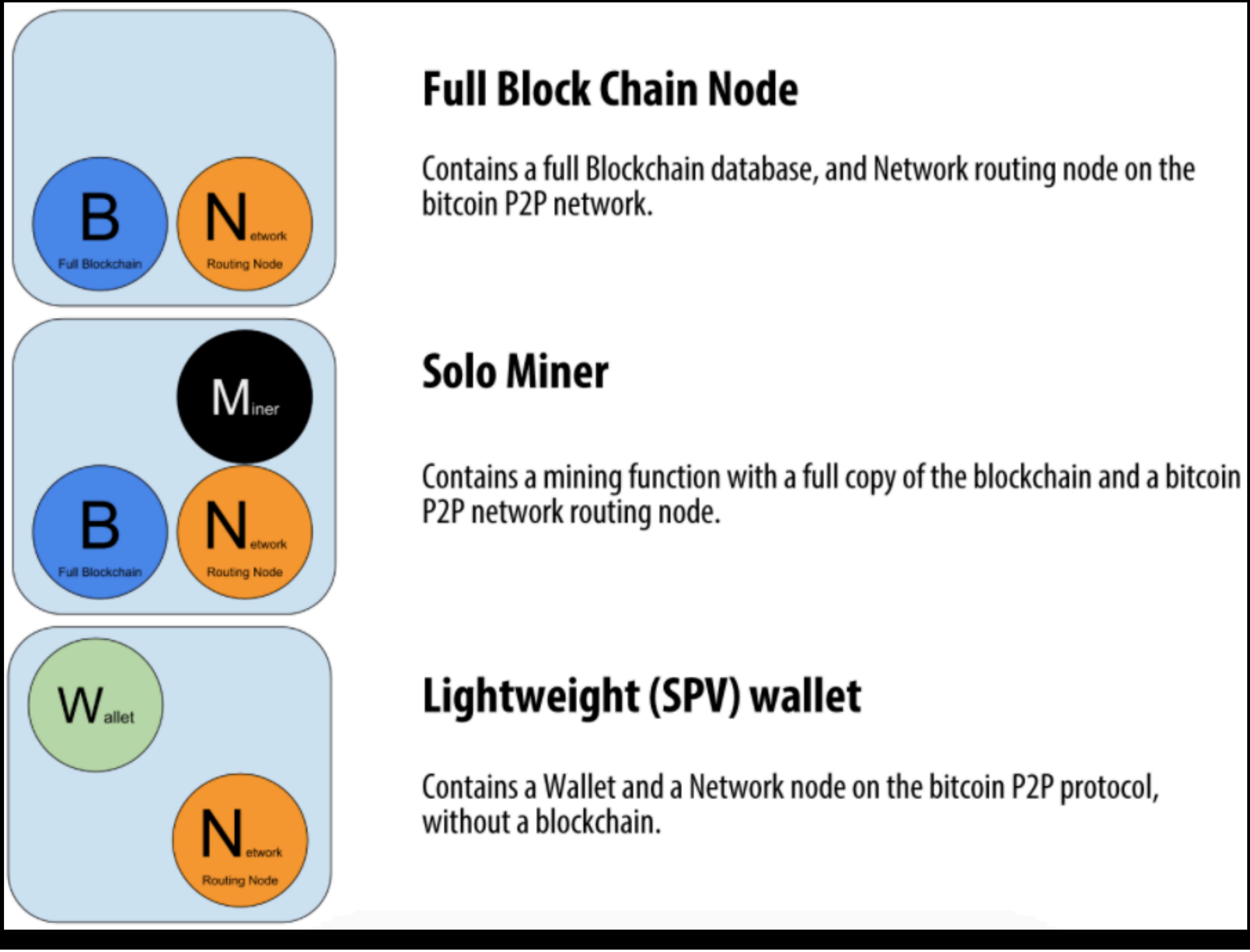
Understanding elements in blockchain network

BLOCKCHAIN NODE TYPES

Functions within blockchain network

- Full Blockchain Ledger
- Mining function
- Network Routing Node
- Wallet

Nodes within blockchain network



Full Block Chain Node

Contains a full Blockchain database, and Network routing node on the bitcoin P2P network.

Solo Miner

Contains a mining function with a full copy of the blockchain and a bitcoin P2P network routing node.

Lightweight (SPV) wallet

Contains a Wallet and a Network node on the bitcoin P2P protocol, without a blockchain.

Limitations of Public Blockchain

- <<Talking about the blockchain which is utilized by BitCoin>>
  - – Ltd txn processing capability
    - Resulting in longer confirmation wait time
    - Increasing transaction fee
  - – Increase in ledger size over time
    - With 1K txn size per block, we have 150 GB ledger size today.
  - – PoW burns electricity
  - – Privacy issue … anyone can track your spending
    - Mapping a public key to an identity is non-trivial

Miscellaneous

FAQS

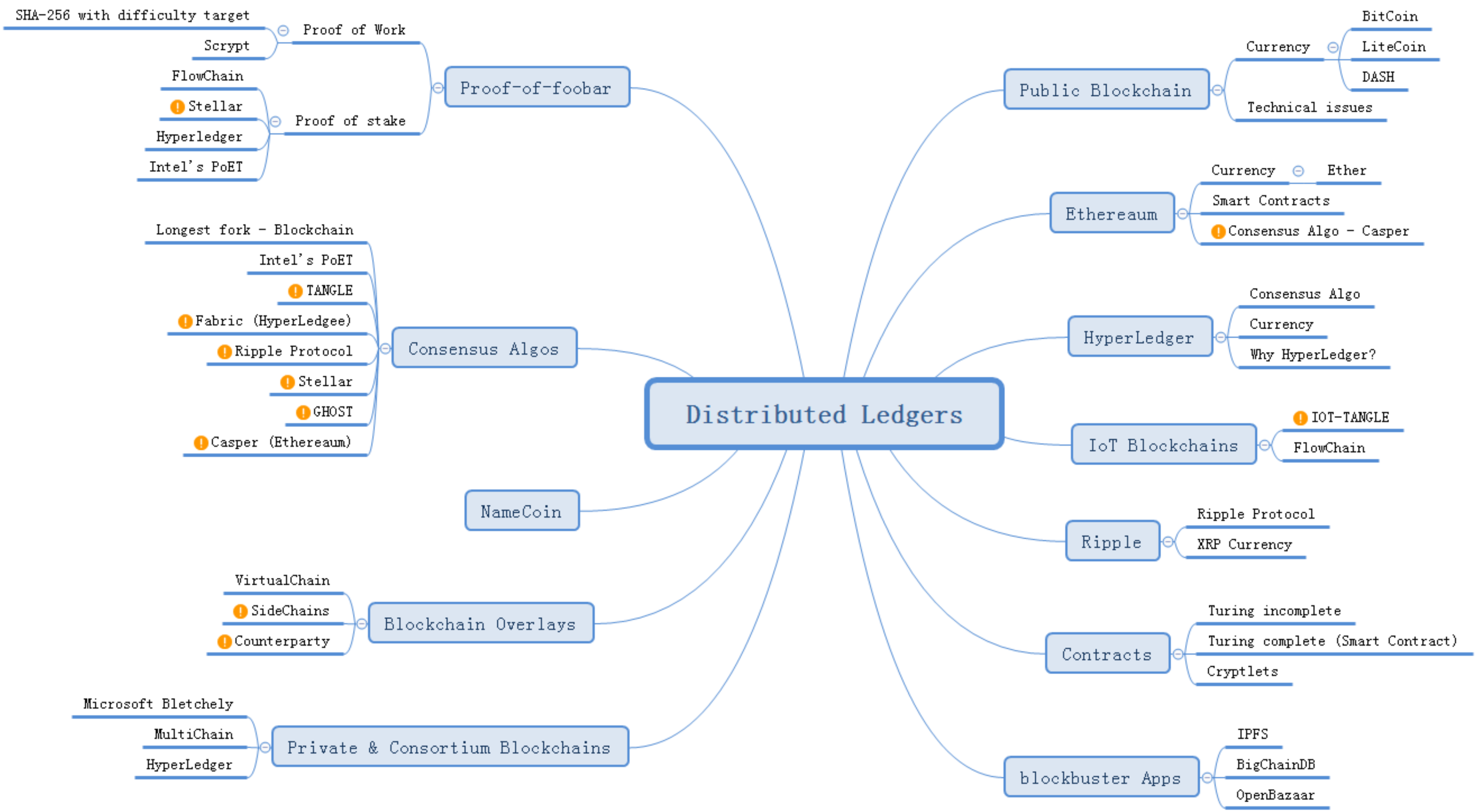
FAQs

- What is public vs private blockchain?
- What is Bitcoin-Cash fork?
- What is HyperLedger?
- What are ICOs?
- What is Blockchain-As-A-Service (BaaS)?
- What is Ethereum and how is it different from Bitcoin network?
- Why does IoT and blockchain goes hand in hand?
- What is Proof-Of-Stake?

FAQs

- What is Microsoft Bletchely Project?
  - Microsoft's strategy for BaaS
- What are governments doing about it?
  - Taxation rules in India?
  - ICO regulations?
- What are DAOs (Decentralized Autonomous Organizations)?
- Was there a fraud in such systems?
  - What steps were taken for recovery?
  - 50mn DAO virtual currency siphoned off.

My MindMap



- Distributed Ledgers
  - Proof-of-foobar
    - Proof of Work
      - SHA-256 with difficulty target
      - Scrypt
    - Proof of stake
      - FlowChain
      - Stellar
      - Hyperledger
      - Intel’s PoET
  - Consensus Algos
    - Longest fork - Blockchain
    - Intel’s PoET
    - TANGLE
    - Fabric (HyperLedgee)
    - Ripple Protocol
    - Stellar
    - GHOST
    - Casper (Ethereaum)
  - NameCoin
  - Blockchain Overlays
    - VirtualChain
    - SideChains
    - Counterparty
  - Private & Consortium Blockchains
    - Microsoft Bletchely
    - MultiChain
    - HyperLedger
  - Public Blockchain
    - Currency
      - BitCoin
      - LiteCoin
      - DASH
    - Technical issues
  - Ethereaum
    - Currency
      - Ether
    - Smart Contracts
    - Consensus Algo - Casper
  - HyperLedger
    - Consensus Algo
    - Currency
    - Why HyperLedger?
  - IoT Blockchains
    - IOT-TANGLE
    - FlowChain
  - Ripple
    - Ripple Protocol
    - XRP Currency
  - Contracts
    - Turing incomplete
    - Turing complete (Smart Contract)
    - Cryptlets
  - blockbuster Apps
    - IPFS
    - BigChainDB
    - OpenBazaar