Blockchain Technologies

Adithya Bhat

Outline

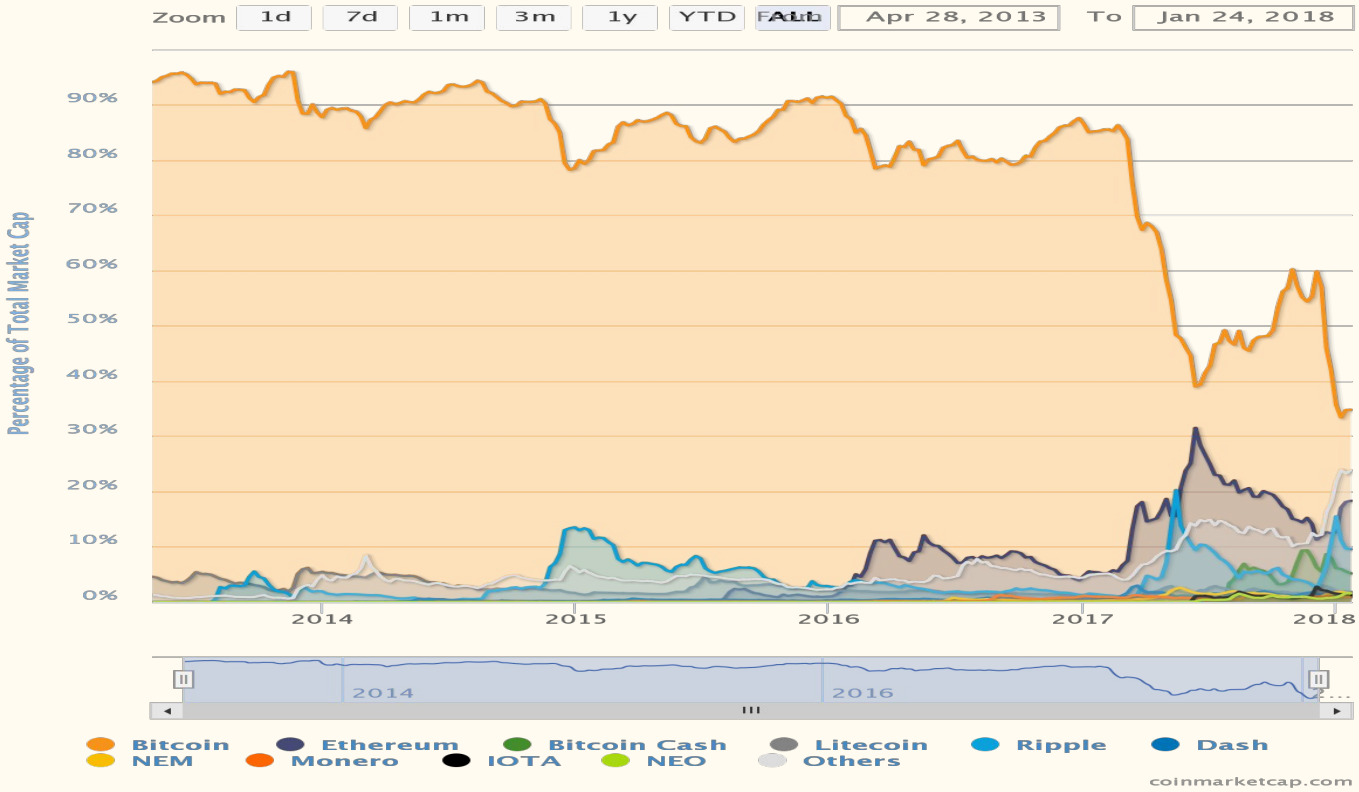
Things that will be covered today!

- Coin Exchange and Economics
- Cryptocurrencies outline
- Problems in Cryptocurrencies
- BitCoin
- Ethereum
- Ripple
- IOTA
- Privacy and De-anonymization Attacks

Cryptocurrencies

- A type of digital currency
- Backed by
  - Public Key Cryptography
  - Cryptographic Hash Functions
- Usually
  - Limited in supply
  - Decentralized
  - Publicly verifiable
  - Privacy
- Relatively new and cannot be regulated by any Government\
- Not asset backed

Overview of Market Capitalization (till yesterday)



Coin Exchanges

- Supply and Demand
- Match buyers and sellers
- Based on orders
- Market Order (buy/sell within range)
- Limit Order (buy/sell above/below price)
- Usually hold your coins for you
- Prone to leakage, insider trading, etc

Problems in Cryptocurrencies

Problems in Cryptocurrencies

1. Double Spending Problem
2. Transaction Fees
3. Transaction Throughput
4. Scalability
5. Consensus Problem/ Byzantine Generals Problem
6. Aging Crypto Algorithms
7. Quantum Computers

Byzantine Generals Problem

The Problem

- **Generals = Computer Components**
- **Each division of Byzantine army is directed by its own general.**
- **There are n Generals, some of which are traitors.**
- **All armies are camped outside enemy castle, observing enemy.**
- **Communicate with each other by messengers.**

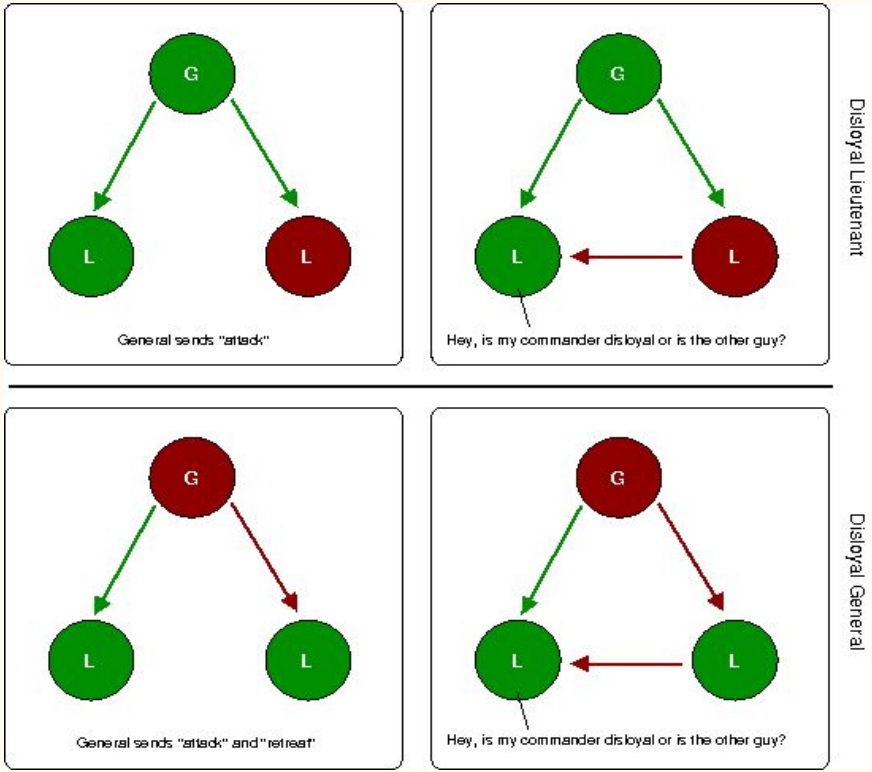
Requirements:

- **G1: All loyal generals decide upon the same plan of action**
- **G2: A small number of traitors cannot cause the loyal generals to adopt a bad plan**
- **Note: We do not have to identify the traitors.**

Reduction of General Problem

- Byzantine Generals Problem (BGP):
  - A commanding general (commander) must send an order to his n-1 lieutenants.
- Interactive Consistency Conditions:
  - IC1: All loyal lieutenants obey the same order.
  - IC2: If the commanding general is loyal, then every loyal lieutenant obeys the order he sends.
- Insight: We can restrict ourselves to the problem of one general sending its order to others.
- Note: If General is loyal, IC2 $\Longrightarrow$ IC1.
- Original problem: each general sends his value v(i) by using the above solution, with other generals acting as lieutenants.

Results



Impossibilty Result:

For a system with 3m+1 nodes, m traitors can be tolerated.

BitCoin

BitCoin

Satoshi Nakamoto: The Boss!

Started in 2007.

Code -first, paper later policy.

Missing since 2013 (probably dead!)

Father(kind of) of cryptocurrencies and market leader

Blockchain and incentivized against corruption

Some Key Features

- Prevents Double Spending
- Idea of blockchain
- Mining blocks
- Geometric Progression of Block Rewards
- 10 minute/block and 4(avg.)-7(max) transactions/second
- Uses Merkle trees for state storage

Working

Cue Website!

Hashing

Digital Signatures

Automatic Difficulty Resetting

Mining blocks

Coinbase transaction vs Normal Transaction

TCP/UDP Network

Let tsum = Number of seconds taken to mine last 2016 blocks

Tnew=tsum×T/(14×24×60×60)

- Recall that probability of success in single trial is $(T+1)/2^{256}$

Ethereum

Ethereum Features

- Uses GHOST protocol for consensus
- Uncle blocks
- Ethereum Virtual Machine
- Gas
- Smart contracts
  - Solidity
  - Multiple Clients

Other Popular Cryptocurrencies

Ripple

Key features:

- Cross border payments
- Uses XRP
- Uses ripple consensus algorithm
- Use rippling
- Designed specifically for banking and trading
- Based on havala trading

IOTA

Some of the key features

- Generation 3 cryptocurrency
- Tangle Technology for consensus
- Uses Post Quantum Crypto
- Designed for IoT Devices
- ZER0000 Fees

Other Cryptocurrencies of Interest

ZCash

- Privacy is guaranteed
- Uses zk-SNARKS
    - Zero Knowledge Succint Non-interactive Arguments of Knowledge
- Uses concepts of MPC to generate random number
- The generators have so much power that they can create coins out of thin air

AlgoRand

- Very Powerful
- Based on randomly elected validators
- Patented by MIT (thank you Micali)
- Scalable and Decentralized

Hyperledger

- Consorium based blockchain
- Contains predefined validators and orderes
- Open sourced and under active development
- Supports customized functionality
- Scalable and Decentralized

Concerns and Attacks

Concerns around Blockchains and Cryptocurrencies

- Quantum Computers
- Identity based (Sybil attacks)
- Pollution/Power Consumption
- Unregulated
- Moving towards centralization (few powerful miners)
- Resistant to changes
- Forking is a huge problem!
- Ageing algorithms

Attacks on Cryptocurrencies

DAO Attack

Ethereum contract kill

Loss of Keys and Stolen Key attacks

Collapsing of exchanges

References

- https://coinmarketcap.com/charts/
- http://lamport.azurewebsites.net/pubs/byz.pdf

Thank You!