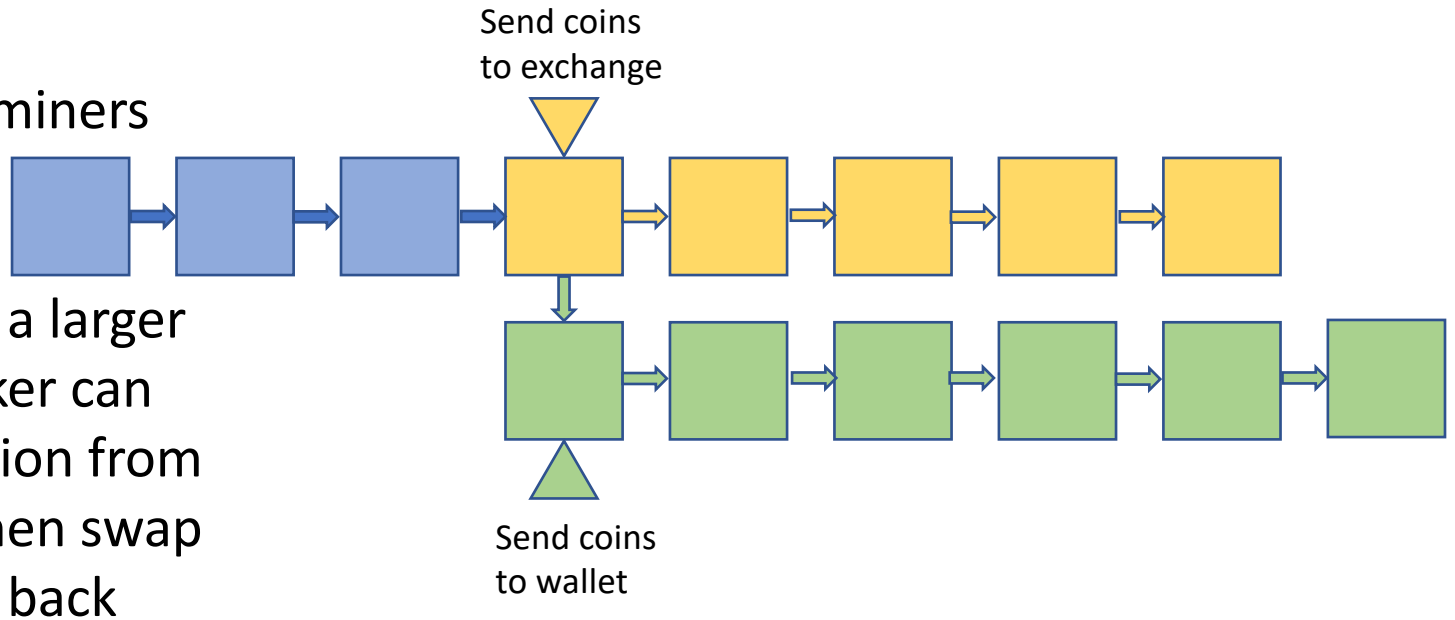
But First – The 51% Attack

- A successful 51% attack was performed against the Bitcoin Gold fork
- Money was stolen from exchanges via double-spend attacks
- With 51%+ of the network hash power
  - Can make blocks faster
  - Can interfere with other miners
  - With the ability to create a larger valid side-chain the attacker can wait until block confirmation from the vendor is obtained, then swap chains and effectively roll back transactions, hurting the vendor



```
MM"""""""""`M   dP   dP
MM  mmmmmmmM   88   88
M`      MMMM d8888P 88d888b. .d8888b. 88d888b. .d8888b. dP    dP 88d8b.d8b.
MM  MMMMMMMM   88   88'  `88 88ooood8 88'  `88 88ooood8 88    88 88''`88''`88
MM  MMMMMMMM   88   88    88 88.  ... 88       88.  ... 88.  .88 88  88  88
MM        .M   dP   dP    dP `88888P' dP       `88888P' `88888P' dP  dP  dP
MMMMMMMMMMMM
```

History

- Founded/Invented by Vitalik Buterin
- Proposed in late 2013
- Crowd sale between July and August 2014
- Released July 30th 2015
- 11.9 million coins (13%) “premined” and distributed
- The DAO was hacked in June 2016
- A fork to remedy the situation dissolved the DAO and split the blockchain into ETH (Ethereum) and ETC (Ethereum Classic)

Overview

- A platform for launching decentralized/distributed applications on a blockchain vs just a distributed ledger like Bitcoin/Litecoin/Dogecoin
- Instead of having to create a new blockchain for every application and build up a network for security they can just deploy on the Ethereum blockchain
- p l a t f o r m
- Miners execute code in exchange for transaction fees pegged to the amount of execution required (“gas limit”) and the price per unit of execution (“gas price”)

Terminology

- **Smart Contract (DApp)** – a piece of computer code placed on the blockchain, to be executed under certain conditions and with certain outcomes. The contracts are public and accessible to all (sort of)
- **Ethereum Virtual Machine (EVM)** – a Turing-complete virtual machine in which the execution takes place
- **Solidity** – the programming language used for writing smart contracts
- **Gas** – an internal pricing mechanism that tie ETH to units of work
- **Gas Price** – the price the sender is willing to pay per unit of gas (hourly rate), this allows miners to prioritize jobs
- **Gas Limit** – the upper limit on how much work the sender is willing to pay for (hours of work requested), this prevents runaway execution or inadequate compensation

EVM

- A runtime environment for smart contract code
- Isolated environment on the host computer
- Every node has an EVM
- EVMs in C++, Go, Haskell, Java, JavaScript, Python, Ruby, Rust, and WebAssembly ← which could be very interesting
- Contracts are compiled to EVM bytecode and executed by nodes (miners)

DApps and DAOs

- DApp – Distributed Application
  - Application code deployed to the blockchain
    - Immutable
    - Decentralized
    - Tamper-proof
    - Only as secure as the authors make them

- DAO – Distributed Autonomous Organization
  - “A DAO consists of one or more contracts and could be funded by a group of like-minded individuals. A DAO operates completely transparently and completely independently of any human intervention, including its original creators. A DAO will stay on the network as long as it covers its survival costs and provide a useful service to its customer base” Stephen Tual, former CCO Ethereum

Working with Ethereum

- https://brave.com/
- https://metamask.io/
- https://www.myetherwallet.com/
- https://etherscan.io/
- https://cryptozombies.io/

Sources

- https://en.wikipedia.org/wiki/Ethereum
- https://en.wikipedia.org/wiki/The_DAO_(organization)