What is this Ethereum Thing Anyways?

Waterloo Ethereum Developer Meetup September 25th, 2018 Hernando Castano

What is Ethereum?

"Open blockchain platform that lets anyone build and use decentralized applications that run on blockchain technology."

http://ethdocs.org/en/latest/introduction/what-is-ethereum.html



That's All Folks!

Presentation Overview

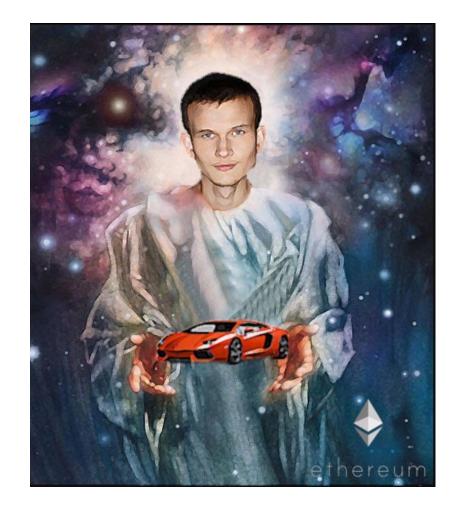
- A Brief History of Ethereum
- How Does it Work?
- Ecosystem



History of Ethereum

Vitalik-Lambo-Jesus

- In 2011 Vitalik Buterin saw a need Bitcoin to include a usable scripting language
- Wrote the Ethereum Whitepaper in November 2013
- Work on Ethereum begun in 2014
 - Dropped out UWaterloo for this
- Crowdfund happened in 2014, raising \$18 million



The Vitalik Buterin Show



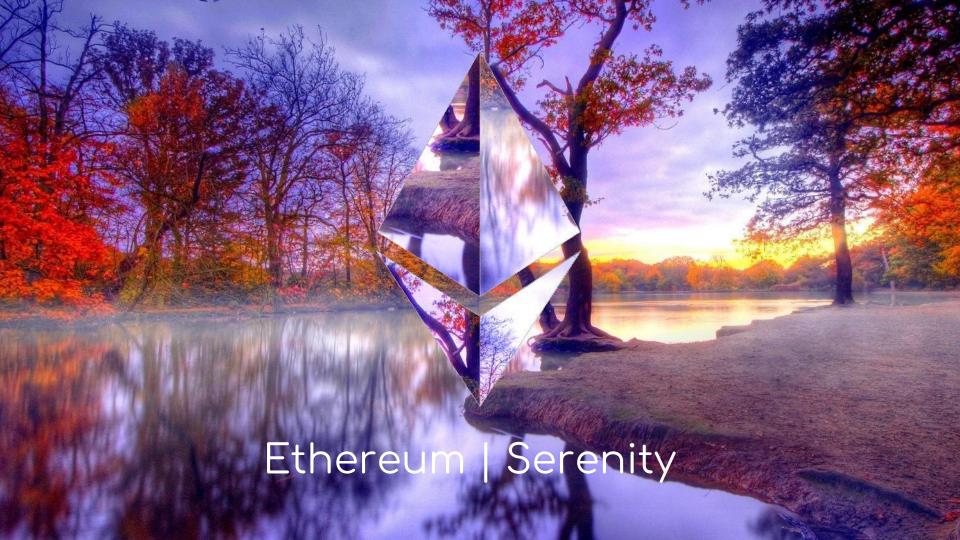
https://www.reddit.com/r/ethtrader/comments/6ecxfu/the vitalik buterin show everybody gets a lambo/

Ethereum Network Releases









How Does it Work?

ENTERPRISE ETHEREUM ARCHITECTURE STACK APPLICATION DAPPS **EXPLORERS, MONITORING & BI APPLICATIONS INFRA CONTRACTS &** NETWORK GOVERNANCE IDENTITY RBAC **TOKEN STANDARDS** ETHEREUM NAME SERVICE **STANDARDS** SMART CONTRACT SMART CONTRACT LANGUAGES FORMAL VERIFICATION TOOLS TOOLING PERMISSIONS & WALLETS KEY MANAGEMENT HSM PERMISSIONING / AUTHENTICATION **CREDENTIALS** INTEGRATION & ENTERPRISE MANAGEMENT SYSTEMS INTEGRATION LIBRARIES **DEPLOYMENT TOOLS** CLIENT INTERFACES **ORACLES** JSON-RPC INTER-CHAIN PRIVACY / SCALING PRIVATE TRANSACTIONS OFF-CHAIN (TRUSTED EXECUTION) **PRIVACY** ON-CHAIN SCALING ON-CHAIN (LAYER 2) OFF-CHAIN (COMPUTE) **CORE BLOCKCHAIN** ON-CHAIN PRIVATE STATE STORAGE/LEDGER ON-CHAIN PUBLIC STATE ON-CHAIN STORAGE OFF-CHAIN STORAGE **EXECUTION EVM** SYNC PRECOMPILED CONTRACTS TRUSTED EXECUTION CONSENSUS **PUBLIC CONSENSUS PRIVATE CONSENSUS NETWORK NETWORK PROTOCOL** DEVP2P **ENTERPRISE P2P** LEGEND Yellow Paper Public Ethereum Application Laver Enterprise Ethereum All Yellow Paper, Public Ethereum, and Application Layer components may be extended for Enterprise Ethereum as required.

All Yellow Paper, Public Ethereum, and Application Layer components may be extended for Enterprise Ethereum as require
8 2008 Enterprise Ethereum All ance

The Ethereum Stack

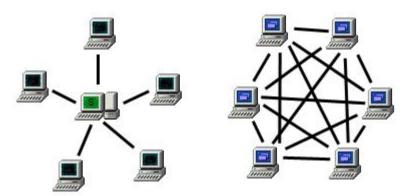
https://entethalliance.org/wp-content/uploads/2018/05/EEA-Architecture-Stack-Spring-2018.pdf

Networking Layer

- How communication between nodes on the network occurs
- Nodes talk to each other directly
- Ethereum uses *devp2p*
 - Peer Discovery
 - Transport (RPLx)
 - Application Layer (devp2p)

Server Based Network

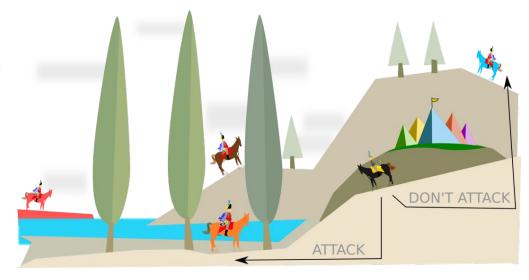
Peer to Peer Network



https://medium.com/@alberthu/wtf-is-peer-to-peer-4b865d29e44e

Consensus Layer

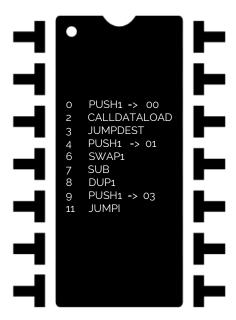
- Algorithm used to agree on the state of the network
- Ethereum uses a Proof-of-Work algorithm called Ethash
- Some testnets use
 Proof-of-Authority algorithms
 - O Kovan => Aura
 - Rinkeby => Clique



(Yes, I know this is for a BFT consensus algorithm, not a POW one) https://hackernoon.com/a-hitchhikers-guide-to-consensus-algorithms-d81aae3eb0e3

Ethereum Virtual Machine (EVM)

- Compute layer of Ethereum
 - o Runtime environment for smart contracts
- Turing complete (ish)
 - Computation is bounded by gas
- Completely deterministic
- Word size of 256-bits (unlike the typical 32/64-bits)
 - Better for cryptographic operations
- Lots of fun details in the Yellow Paper



https://www.kisspng.com/png-ethereum-virtual-machine-blockchain-smar t-contract-1302259/

https://github.com/CoinCulture/evm-tools/blob/master/analysis/guide.md

JSON-RPC

- Lightweight protocol for sending/receiving requests
- Used in Ethereum space when sending commands to a remote node
 - Querying blockchain data
 - Sending transactions
- How things like Metamask* talk to the blockchain

```
// HTTP POST
curl https://mainnet.infura.io/ \
    -X POST \
    -H "Content-Type: application/json" \
    -d '{"jsonrpc":"2.0","method":"eth_blockNumber","params": [],"id":1}'

{
    jsonrpc: "2.0",
    id: 1,
      result: "0x5c174e"
}
```

https://infura.io/docs/api/get/eth_blockNumber

Smart Contracts

- Immutable pieces of code that live on the blockchain
- Do exactly what they are programmed to do
 - Even if they're programmed wrong!
- Various smart contracting languages
 - Solidity Most popular
 - Vyper Up and coming

```
pragma solidity ^0.4.0;

contract SimpleStorage {
    uint storedData;

    function set(uint x) public {
        storedData = x;
    }

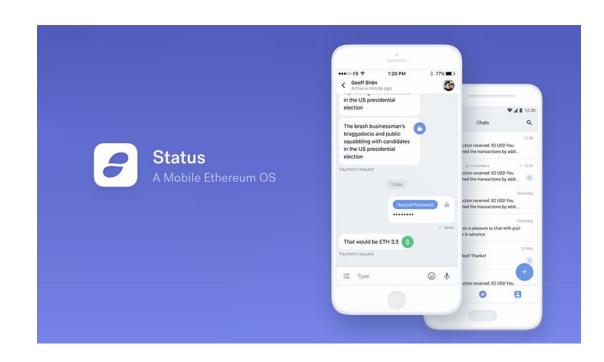
    function get() public view returns (uint) {
        return storedData;
    }
}
```

https://solidity.readthedocs.io/en/v0.4.24/introduction-to-smart-contracts.html

Ecosystem

Status.IM

- Instant Messaging
- Run dApps on your phone
- Manage crypto funds
- Live on mainnet with a v0.9x
 mobile app



MakerDAO

- Best known for their stablecoin, Dai
 - o 1:1 Peg with USD
 - Backed by ETH (for now)
- Collateral loans
 - Collateral Debt Positions (CDPs)
- Governance
 - Recently had first Foundational Vote



For Real Now. That's all Folks