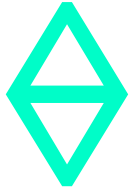


Web3: Ethereum and the next evolution of the Web



Luke Hedger – JAAK

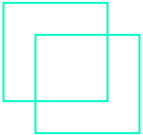
Origin Story

- Spies
- Monopolies
- Cypherpunks



Agenda

1. Web2 vs Web3, Centralisation vs Decentralisation
2. The decentralised web
3. Experimenting with Ethereum



Web 1, 2, 3

- Web 1.0 (1980s to early 2000s)
 - Open protocols (TCP/IP, HTTP, SMTP) maintained by the Internet community (W3C, IETF)
- Web 2.0 (mid 2000s to present)
 - Software/services built on open protocols, data silos, vendor lock-in
- Web 3.0 (the future?)
 - Open network protocols, shared data layer, blockchains

Aspects of decentralisation

	Centralised	Decentralised
Architectural	Company HQ	CDNs, BitTorrent, Blockchain
Political	Company CEO, CDNs	Blockchain
Logical	Blockchain	BitTorrent



Imperial cult of ancient Rome



500 years Rome largest city
in the world

5 million square kilometres
of territory

70 million subjects

21% of the world's
population

1,500 years long

1 emperor

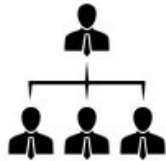
Ant colonies

- Centralised

Global information



Local behaviour



- Decentralised

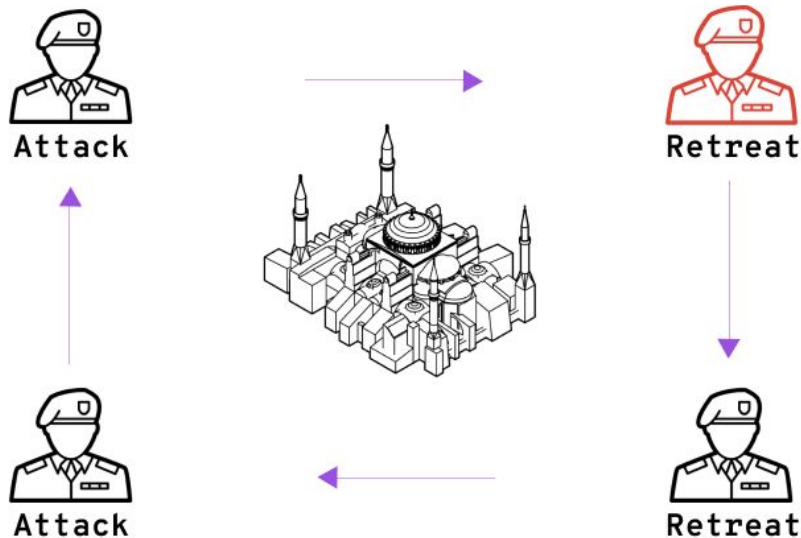
Global behaviour



Local information



Byzantine Generals

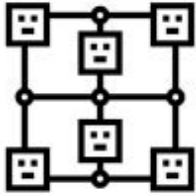


Attack or Retreat?
Consensus?

The Byzantine Generals Problem

Leslie Lamport, Robert Shostak, Marshall Pease (1982)

The decentralised web



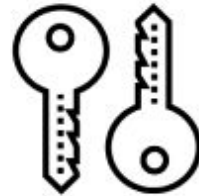
Open networks

Public protocols



Shared data

Cryptography



In practice

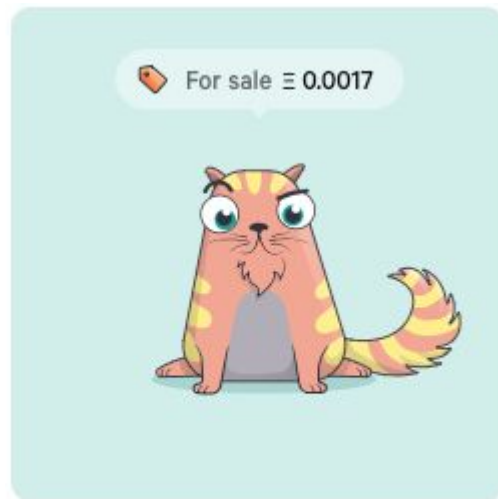
- Data: **KORD** (IP), Ocean (AI)
- Governance: **DAOs**, Wikipedia
- Communication: Secure Scuttlebutt

Ethereum:

- Money: ICOs
- Games: **CryptoKitties**
- Registries: Decentraland



KORD



Kitty 380010 · Gen 22 · Sluggish



Decentralised stack

• Computation



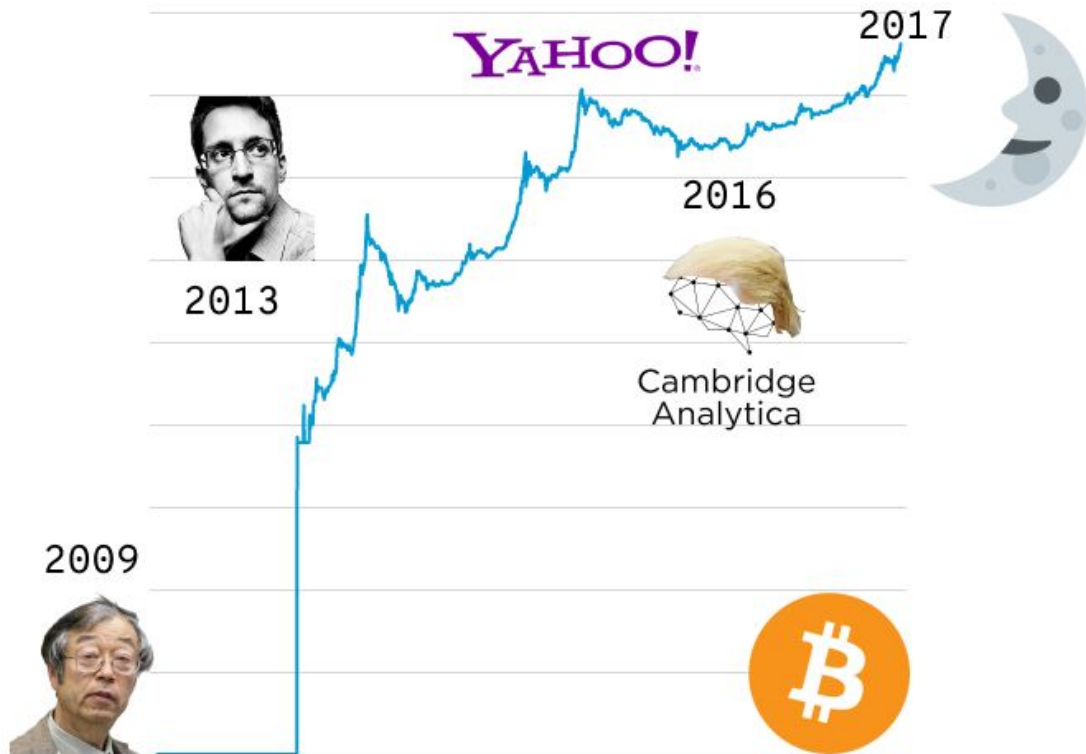
• Storage



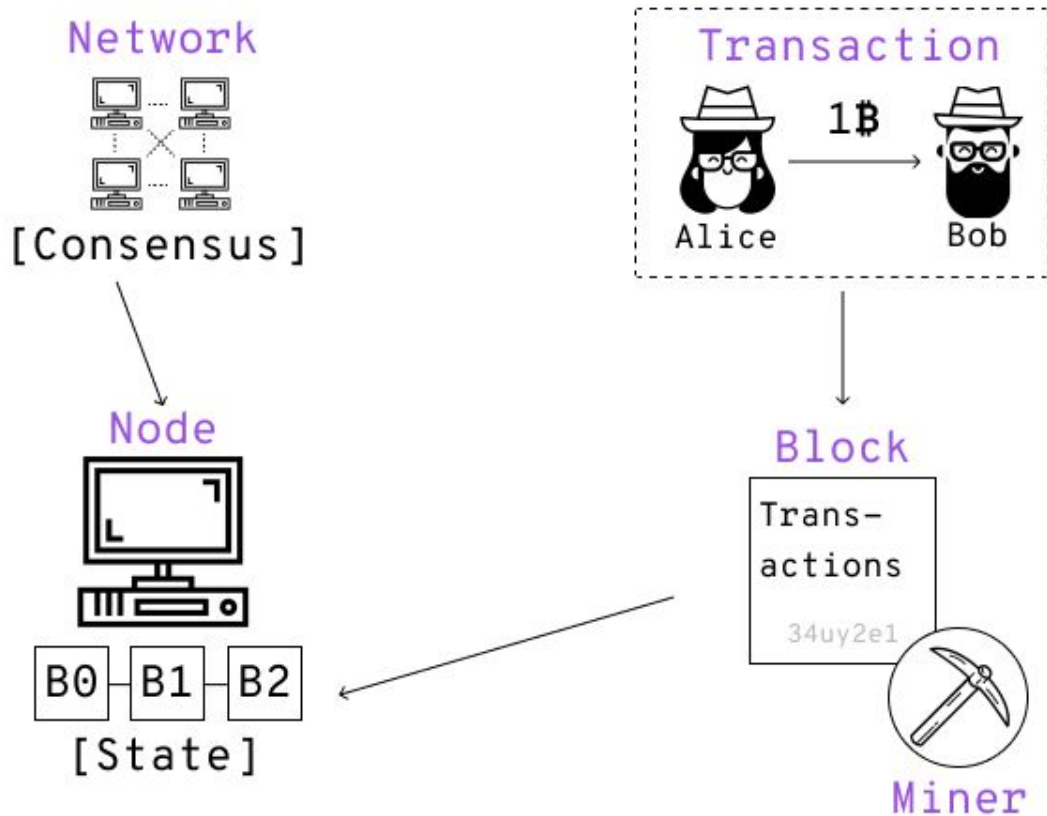
• Hosting



HODL



Blockchain



Ethereum



Alice

castVote("YES")



Smart Contract

API

castVote(vote)
getVotes()

State = { votes }



Swarm



Smart contracts

- A **contract** is “a voluntary arrangement between two or more parties”
- A **smart contract** is “a computer protocol intended to facilitate, verify, or enforce the negotiation or performance of a contract”

Wikipedia



HelloWorld.sol

```
pragma solidity ^0.4.23;

// import './SomeContract.sol';

contract HelloYou {
    event Hello(address indexed you);

    function sayHello() public {
        address _person = msg.sender;

        emit Hello(_person);
    }
}
```



```
pragma solidity ^0.4.23;

contract Vote {
    enum VoteType { NO, YES }

    mapping(address => bool) voters;

    uint YesVote;
    uint NoVote;

    function castVote(VoteType _vote) public {
        // TODO
    }
}
```

```
function castVote(VoteType _vote) public {  
    require(uint(VoteType.YES) >= uint(_vote));  
  
    address voter = msg.sender;  
  
    if (voters[voter] == true) { revert(); }  
  
    voters[voter] = true;  
  
    if (VoteType(_vote) == VoteType.YES) {  
        YesVote = YesVote + 1;  
    } else {  
        NoVote = NoVote + 1;  
    }  
}
```

```
import web3 from 'web3.js'

const abi = [ ... ]

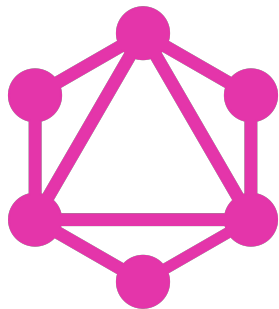
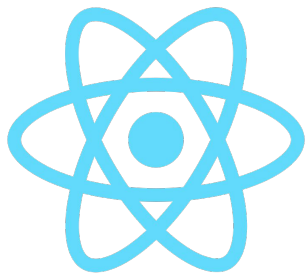
const address = '0x123456789'

const Vote = new web3.eth.Contract(abi, address)

Vote.methods.castVote.send('YES')
```



Decentralised applications (really just applications) 🤪



Next steps

Crossing Over to Web3: bit.ly/crossing-over-web3

Hashnode: hashnode.com/n/ethereum

Spectrum: spectrum.chat/ethereum

GitHub: github.com/lukehedger

KORD: kord.network



“If you asked people in 1989 what they needed to make their life better, it was unlikely that they would have said a decentralized network of information nodes that are linked using hypertext.”

— Farmer & Farmer

Credits

- Hagia Sophia by Lluisa Iborra from the Noun Project
- marshal by H Alberto Gongora from the Noun Project
- Computer by Smalllike from the Noun Project
- Pickaxe by Lucas fhñe from the Noun Project
- hipster by Oksana Latysheva from the Noun Project
- networking by Smalllike from the Noun Project
- C-3P0 by Arthur Shlain from the Noun Project
- Data by Daily icons from the Noun Project
- Key by Nikita Kozin from the Noun Project