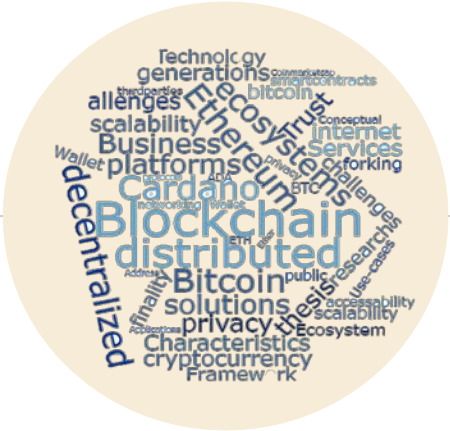
The three blockchain technology generations?



Hello!

I am Mark van der Pasch

Master student TU/e

Blockchain internship @ Rabobank

Fintech & Innovation, BAL

‘How to qualify public unpermissioned blockchain technologies and why are these not wide-scale adopted for business use cases?’

Blockchain types

Who is allowed to validate in the consensus process?

Permissionless

Permissioned

Who is allowed to access and participate in the network?

Public

Private

Characterisation framework:

Public permissionless blockchains:

Service characteristics:

Functionality

Level of Privacy

Level of Trust

Level of Interoperability

Level of Scalability

Governance

Technology characteristics:

Internal design considerations:

Network design

Consensus mechanism

State machine architecture

Complementary protocols:
2nd layer solutions

How to qualify Bitcoin as a set of technology characteristics:

Network Design

Distributed peer-to-peer

Consensus mechanism

PoW based on SHA-256

State machine architecture:

Coding language: Golang, C++
Smart contract execution: Native
Data structure: transaction based (UXTO)
Block size: 1MB, 1,8 MB for SegWit block.
Block release time: ~600 seconds
Block header data structure: Binary merkle tree with SegWit support

Complementary protocols (2nd layer):

Interchain: i.e. decentralized exchanges

Offchain protocols: Lightning (state channel protocols)

How to qualify Bitcoin as a set of services characteristics:

Functionality

Native: Cryptocurrency, Turing incomplete smart contracts and SegWit

Add-on: i.e. Lightning, Decentralized exchanges

Level of Scalability

Maximum throughput: 3.3 – 7 tx/sec

Latency: ~10 minutes

Transaction costs: ~1.1 USD (25-4-18)

Level of Trust:

Security: High

Finality: No absolute finality

Liveness: High

Level of Privacy:

User level privacy: Pseudonymous

Transaction level privacy: Open and accessible

Level of Interoperability:

Currently poor native interoperability

Governance

Incentives: depends per stakeholder type.

Mechanism for coordination: Off-chain BIP & mailing list, On-chain Miners to implement changes.

How to qualify Ethereum as a set of technology characteristics:

Network Design

Distributed peer-to-peer

Consensus mechanism

Ethash PoW mechanism

State machine architecture:

Coding language: Solidity, Serpent, LLL, Vyper & Bamboo
Smart contract execution: EVM
Data structure: State (account-Block release timbased), Transactions and Receipts
Block size: ~8000000 gas
Block release time: ~12 seconds
Block header data structure: Merkle patricia trees and uncle blocks

Complementary protocols (2nd layer):

Interchain: i.e. decentralized exchanges

Offchain protocols: i.e. Raiden network (state channel protocols)

How to qualify Ethereum as a set of services characteristics:

Functionality

Native: Ether Cryptocurrency, Turing complete smart contracts

Add-on: endless applications

Level of Scalability

Maximum throughput: 31.66 Tx/sec

Latency: ~12 seconds

Transaction costs: ~.50 USD (25-5-18)

Level of Trust:

Security: High

Finality: No absolute finality

Liveness: High

Level of Privacy:

User level privacy: Pseudonymous

Transaction confidentiality: Open and accessible but zkSNARKs

Level of Interoperability:

Poor native interoperability

Governance

Incentives: depends per stakeholder type.

Mechanism for coordination: Off-chain: EIPs and ERCs, On-chain: Gas limit voting

What are the challenges of Ethereum?

Functionality

Native: Ether Cryptocurrency, Turing complete smart contracts

Add-on: endless applications

Level of Scalability

Maximum throughput: 31.66 Tx/sec

Latency: ~12 seconds

Transaction costs: ~.50 USD (25-5-18)

Level of Trust:

Security: High

Finality: No absolute finality

Liveness: High

Level of Privacy:

User level privacy: Pseudonymous

Transaction confidentiality: Open and accessible but zkSNARKs

Level of Interoperability:

Poor native interoperability

Governance

Incentives: depends per stakeholder type.

Mechanism for coordination: Off-chain: EIPs and ERCs, On-chain: Gas limit voting

1st layer method to solve the challenges: (Casper)

Ethereum Casper PoS implementations

Pros:
Level of Trust
Finality

Level of scalability
Lower electricity cost > Lower network costs

Cons:
Centralized validation <1500ether minimum stake.

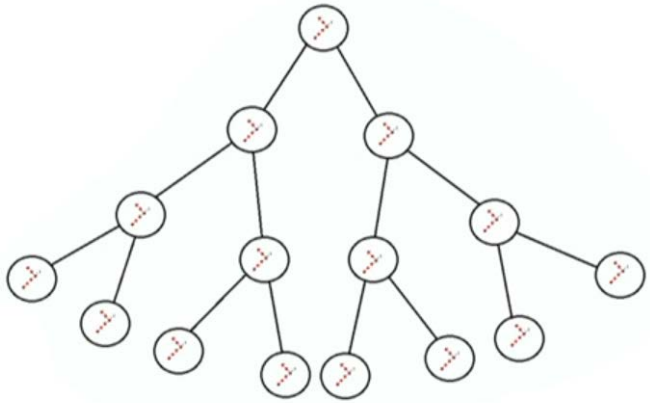
Transformation PoW → PoS

2 step process:

Casper Friendly Finality Gadget (FFG):
Hybrid PoW/PoS
Implemented on alpha testnet since 1st of Januari 2018.
Each 50th block is finalized by PoS.

Casper Correct by Construction (CBC):
PoS consensus mechanism
BFT by-block consensus mechanism

1st layer method to solve the challenges: (Sharding)



Ethereum Sharding implementations

Hierarchical way of splitting network resources

Pros:
Level of scalability
Higher throughput
Load balancing

Cons:
Longer finality time for low-level shards

Node Hierarchy:

- *Super-full node:* This type of node downloads the complete chain including all shards. This node should validate everything.
- *Top-level node:* This type of node processes all main chain blocks, and has light-client access to all shards. It can still check whether a new transaction is valid in all shards.
- *Single-shard node:* This type off node acts like a top-level node, but also downloads a complete shard chain and can validate blocks on that chain.
- *Light-node:* This type of node works like a current light-client, and only verifies all block headers and main-chain blocks.

2nd layer method to solve the challenges: (Payment channels)

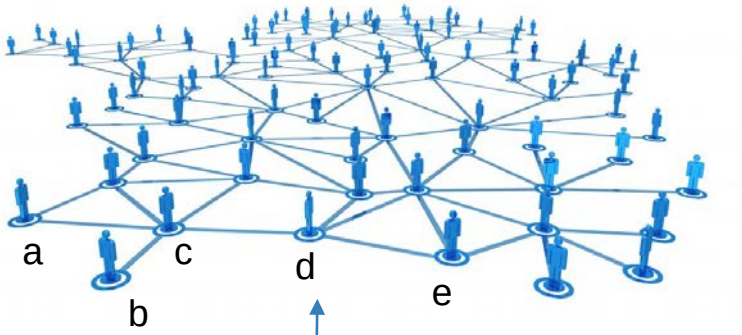
Raiden Network (Ethereum)
Lightning Network (Bitcoin)

Pros:
Level of Scalability
Low cost transactions
High Throughput

Higher level of Privacy

Level of Interoperability
Cross chain atomic swaps

Cons:
Current centralized operators
Depends on availability



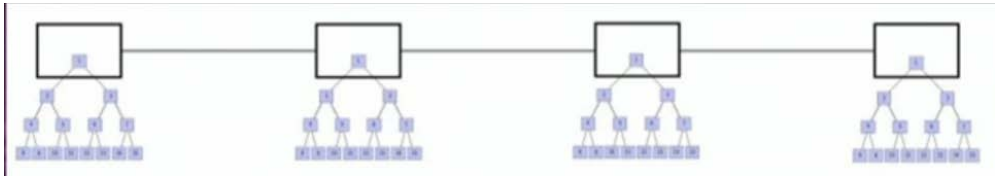
2nd layer method to solve the challenges: (Plasma)

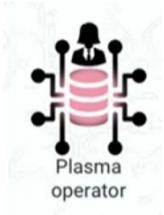
Plasma -> design pattern for scalability on top of Ethereum.

Pros:
Level of Scalability
Ultra high throughput
Applications specific plasma chains.

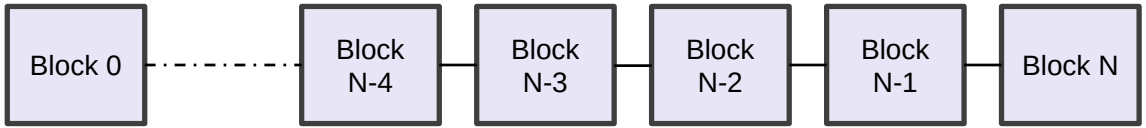
Level of Privacy

Cons:
Centralized plasma operator*
*** limit power of plasma operator**





Settlement in smart contract on-chain



What are the challenges of Ethereum?

Functionality

Native: Ether Cryptocurrency, Turing complete smart contracts

Add-on: endless applications

Level of Scalability

Maximum throug
31.66 Tx/sec

Latency: ~12 seconds

Transaction costs: ~.50 USD (25-5-18)

Level of Trust:

Security: High

Finality: No absolute finality

Liveness: High

Level of Privacy:

User level privacy: Pseudonymous

Transaction confidentiality: Open and accessible but zkSNARKs

Level of Interoperability:

Poor native interop ilit

Governance

Incentives: depends pe
stakeholder type.

Mechanism for coordination:
Off-chain EIPs and ERCs,
On-chain: Gas limit voting

Generations Blockchain:

- Generation 1 → (Cryptocurrency) Blockchains
- Generation 2 -> (Universal) Blockchain Platforms
- Generation 3 or beyond-> (Universal) Blockchain Platforms with some form of governance regulation?

Debating topics:

- Are governance challenges currently influencing the wide-scale adoption of blockchain for business use-cases?
- How should these governance challenges be solved? i.e. on-chain, off-chain or by external “Third-parties”
- Others.....