Ethereum 2.0

Solange Gueiros

Montevideo

dez/2019

THE
LATIN AMERICAN
BITCOIN & BLOCKCHAIN
CONFERENCE 2019

About me...

- São Paulo - Brazil
- BSc Computer Science, Pedagogy
- Doing MSc in Digital Currencies
- Developer for more than 20 years
- Won AirSwap award at EthNewYork – may/2019
- Won Waves award at EthBerlin – aug/2019

About me…

- Teacher at Blockchain Academy
- Developer evangelist at IOVLabs

- I do not work at the Ethereum Foundation
- Everything here is my own research and personal opinions

Ethereum context

What is this

- Smart contract platform
- Open-source
- Public
- Own currency: Ether or ETH.

Current status

The scalability problem

- “world computer”
- with around 15 transactions per second ?!?!?
- Visa and others can handle

  up to 40,000 transactions per second.

Ethereum Roadmap

Ethereum Roadmap

- Frontier – Proof of Concept – jul/2015
- Homestead – Developer-ready
- Metropolis – Current
- Serenity – next

Hard forks

Hard forks in Ethereum

- Most of them do not break the chain
  - (Exception: The DAO)
- They are updates and improvements
- The miners / validators only need to update the client version

Hard forks in Ethereum

- This year (2019):
  - Constantinople
  - Istanbul

Constantinople

Constantinople

- 27-28 feb 2019

- block number 7,280,000
- https://etherscan.io/block/7280000

- 4 EIPs – Ethereum Improvement Proposal

Istanbul

Istanbul

- 08 dec 2019

- block number 9,069,000
- https://etherscan.io/block/9069000

- 6 EIPs – Ethereum Improvement Proposal

Istanbul

- 2 new OpCodes
  - Chainid
  - Selfbalance
- 9 new precompiled contracts
- Gas changes
  - Some things cost more, other cost less

Istanbul

- Security fixes
- Improve resilience to denial-of-service attack

Istanbul

- Make layer 2 solutions based on SNARKs and STARKs more performant
- Enable Ethereum and Zcash to interoperate
  - verify the Equihash PoW

Istanbul

- Big step to move away from PoW to PoS algorithm
- Align the costs of opcodes to computational costs

Ethereum 2.0

All the same!

- Eth2
- Serenity
- Ethereum 2.0

Ethereum 2.0 Goals

- Improve:
  - Decentralization
  - Resilience
  - Security
  - Simplicity
  - Longevity

- By Ethereum researcher Danny Ryan

Serenity

Serenity

- Casper - Proof of Stake
- Sharding - Scalability
- eWASM - A new Ethereum Virtual Machine

Serenity Road Map

- Phase 0: Beacon Chain (Q1/2020)
- Phase 1: Shard Chains (2021)
- Phase 2: eWASM (New Ethereum Virtual Machine) (2021)
- Phase 3: Continued Improvement (2022)
- (the official wiki suggests 6 phases / sub-stages)

Serenity Road Map

- it’s not a change that will happen overnight
- It can have delays and changes along the way.

- As with every software, there is no final version;
- there is always improvements and fixes that need to be done.

Phase 0

Phase 0

- Beacon Chain
- Casper: Proof of Stake
- ETH2: the new Ether
- RANDAO

Beacon Chain

Phase 0 - Beacon Chain

- The Beacon Chain will be a separate blockchain from the main Ethereum blockchain.
- This new chain will have a Proof of Stake (PoS) consensus algorithm
- and it will run in parallel to the main PoW Ethereum blockchain.

Phase 0 - Beacon Chain

- Initially, the blockchain will be created for simplicity
- and will not support smart contracts or accounts.
- It will manage the Casper Proof of Stake protocol for itself and all of the shard chains.

Phase 0 - Beacon Chain

- managing validators and their stakes;
- nominating the chosen block proposer for each shard at each step;
- organizing validators into groups / committees to vote on the proposed blocks;

By Ben Edgington - Blockchain engineering at PegaSys, ConsenSys

Phase 0 - Beacon Chain

- applying the consensus rules;
- applying rewards and penalties to validators;
- being an anchor point on which the shards register their states to facilitate cross-shard transactions.

By Ben Edgington - Blockchain engineering at PegaSys, ConsenSys

Casper

Phase 0 – Casper

- Proof of Stake consensus
- Postponed before:
  - Use of Casper to replacement Ethash consensus has been postponed several times
  - Delay the difficulty bomb and the obsolescence of PoW

Phase 0 – Casper - PoS

- Casper FFG = Friendly Finality Gadget

- Finality =
  - once a particular operation has been done…
  - it will be forever in history
  - nothing can revert

ETH2

Phase 0 - ETH2: the new Ether

- new asset for stakers (validators)
- to be used on the Beacon Chain
- to migrate their ETH from the Eth1 chain to the Eth2 chain

Phase 0 - ETH2: the new Ether

- It will be created using two methods:
  1. As a reward for validating the Beacon Chain (and shards after Phase 1).
  2. Purchasing it for 1 ETH by any user via a registration smart contract at Eth1 chain.
     - The contract refers to it as a deposit.

Phase 0 - ETH2

- Currently there is no way to withdraw or transfer ETH2 from the Beacon Chain in Phase 0.
- Once deposited in the Eth1.x registration smart contract, the ETH1 is burned.
- Beacon Chain validators watch this contract and submit deposit information to the Beacon Chain, which then issues ETH2 to the depositors.

Phase 0 - ETH2

- Pay attention: they will NOT be able to migrate this ETH2 back (for now).
- Because they could be earning interest paid in ETH on the Eth2 chain.

Phase 0 completed: ETH1 and ETH2

- Two active Ethereum chains:
  - Eth1 chain - current, PoW main chain
  - Eth2 chain - new Beacon Chain, PoS

RANDAO

Phase 0 - RANDAO

- RANDAO – random numbers
- A way to combine contributions (individual random numbers) provided by many participants into a single output number.
- This will be used to organize validators into block proposers and committees.

Clients - Beacon Chain

- Are currently being developed
- Separately from standard Ethereum clients: Geth, Parity, Pantheon, et al.

Phase 0 - Beacon Chain

- Beacon Chain might not seem useful.
- But is the first component of Ethereum 2.0 to be delivered.
- It is the foundation of the entire system.

Phase 0 - Beacon Chain

- During Phase 0, all user transactions and smart contract computations will still occur on the Eth1 chain
- ETH2 is transferable (to and from shards) only in end of Phase 2

Phase 1

Phase 1

- Shard Chains
- Crosslinks

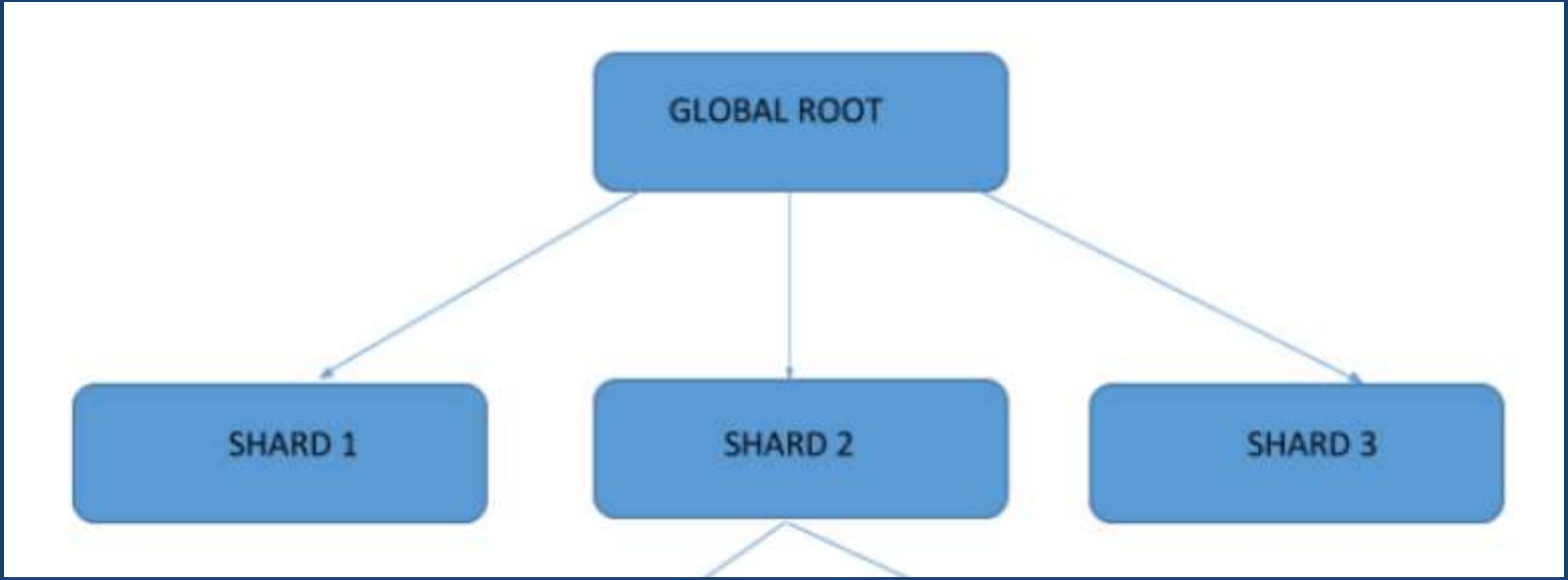
Shard Chains

Phase 1 - Shard Chains

- Sharding is a scalability technique
- That allows parallel transactions throughout
- Allowing process many transactions concurrently

Phase 1 - Shard Chains

The network will be divide across multiple shards



Phase 1 - Shard Chains

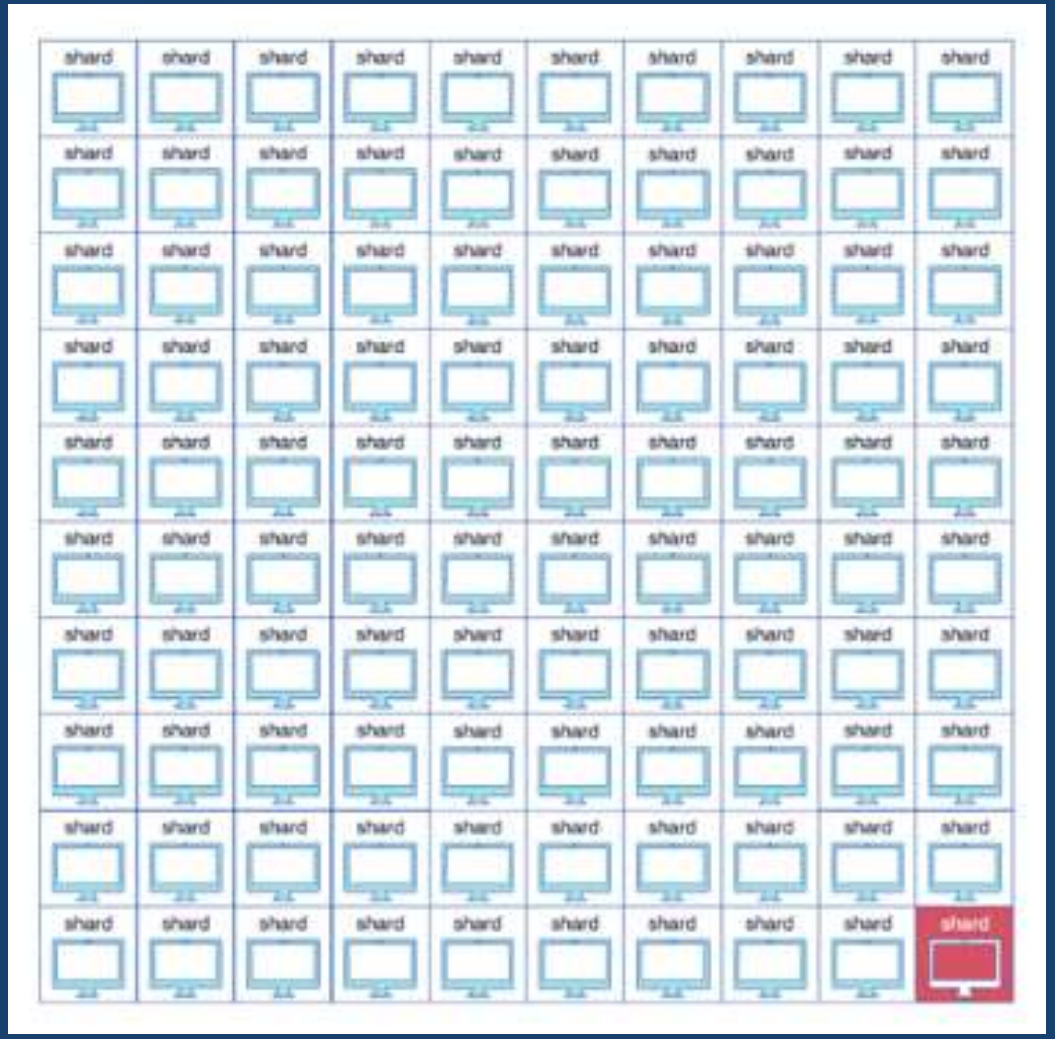
- Phase 1 does not specify shard chain state execution or account balances.
- A trial run for the sharding structure.
- It will not scale with shards yet.
- The Beacon Chain will treat shard chain blocks as simple collections of bits with no structure or meaning.

Phase 1 – Be careful

- Each shard can be validated with a small group of validators.
- Which makes it easier for a 51% attack
- As they only need 51% computing power (or stake) of the shard they are in, instead of the whole network.
- Higher centralization

Phase 1 – Shard attack

- Solution:
  - validators don’t choose which chain they validate



Phase 1 – Shard Chains

- Validators will not approve any smart contract, account or asset.
- The Eth1 and Eth2 chains will still operate in parallel after Phase 1.

Crosslinks

Phase 1 - Crosslinks

- Crosslinks are a set of signatures from a committee
- Also is an infrastructure for asynchronous cross-shard communication.

Phase 1 - Crosslinks

- Attesting to a block in a shard chain, which can be included into the Beacon Chain.
- Crosslinks are the way which the Beacon Chain "learns about" the updated state of shard chains

Phase 1 - Crosslinks

- Time by time, the current state (the “combined data root”) of each shard gets recorded in a Beacon Chain block as a crosslink.
- When the Beacon Chain block has been done, the corresponding shard block is considered finalized
- And other shards know that they can trust on it for cross-shard transactions.

Phase 1 – for all

- In Phase 0, 1, and 2 the main PoW chain (Eth1) will remain live while testing and do the transition to Eth2 chain.
- This means that rewards will be paid to both Ethereum 2.0 validators as well as the normal PoW block rewards.
- More inflation at beginning but…
- Will decrease as the PoW chain is been deactivated.

Phase 2

Phase 2

- eWASM (New EVM)
- Execution Environments (EEs)

eWASM

EVM - Ethereum Virtual Machine

- The EVM is the heart of the Ethereum network
- It is the part that handles smart contract deployment and execution.

Current EVM – The problem

- It processes transactions sequentially.
- With the PoS and Sharding changes, it need to process transactions in parallel
- The current EVM will not be suitable for this.

Phase 2 - eWASM (New EVM)

- Each shard will manage a virtual machine based on eWASM.
- It'll support accounts, contracts, state, and other abstractions that we are familiar in solidity.

Phase – for all

- The entire system will start to come together.
- I hope tools like Truffle, Solc, Ganache will support eWASM in Phase 2.

Execution Environments

Phase 2 - Execution Environments (EEs)

- EE can be constructed in many ways:
  - a UTXO-style chain
  - a Libra-style system
  - a fee market relayer
  - and others.

Phase 2 - Execution Environments (EEs)

- Every shard has access to all execution environments
- And has the ability to make transactions within them
- As well as run and interact with smart contracts.
- Fees is still in research and development.

And... dApps?

Phase 2 – About dApps

- A dApp will have to choose what shard it wants to be on.
- That decision is important!
- Cross-shard communication differs on Eth2 as it is not synchronous which means some compose may be lost between shards

Phase 2

- About accounts and smart contracts…
- When and how it will be migrated to Ethereum 2.0?
- It is an open question yet…

Phase 3

Phase 3 - 2022

- Cross-shard transactions
- Lightweight clients
- Super-square charting
- Closer ties

Conclusion

Conclusion

- Need to move all the things which are in Ethereum now
- How to do it?
- Big challenge!!!

Contact

https://www.linkedin.com/in/solangegueiros/

Contact

- blockchainacademy.com.br
- iovlabs.org

- solangegueiros@gmail.com
- https://medium.com/@solangegueiros
- https://www.linkedin.com/in/solangegueiros/
- twitter, facebook, instagram: solangegueiros

References

- https://docs.ethhub.io/ethereum-roadmap/ethereum-2.0/eth-2.0-phases/
- https://medium.com/swlh/a-comprehensive-view-of-ethereum-2-0-serenity-5865ad8b7c62
- https://eth.wiki/en/roadmap/istanbul
- http://eips.ethereum.org/