Eth 2.0 Roadmap
& Overview

M Junaid

Phases

Phase 0 (PoS) Testnet Launched

- can deposit ETH and start staking
- no user level functionality except transferring ETH bw accounts on PoS chain (Q: beacon chain?)

Phase 1 (Data Sharding) 99% developed

- shard chain go live
- only verifying data has been published?, not verifying Tx, not running smart contracts, not verifying validity of Txs,
- can hold 2.6 MB/sec of data
- no smart contracts, just data availability verification, usable for certain kinds of layer 2 constructions, eg ZK rollup

Phases

Phase 2 (state execution)

- accounts , smart contracts, etc enabled on shard chains
- full functionality now available
- eWASM
- Execution Environments (EEs) (developer will chose)
- EEs within a shard can be constructed in whatever way a developer sees fit - there could be an EE for a UTXO-style chain, a Libra-style system, an EE for a fee market relayer and beyond.
- Do note that the concept of execution environments is still in heavy research and development
- Q: inter shard interaction, smart contract living bw shards?

Phase 3 (STARKS, further scaling)

- upgrades to consensus (Casper CBC)
- upgrades to scaling (STARKs)

Chains

Eth1 Chain

|

Beacon chain

| |

| |

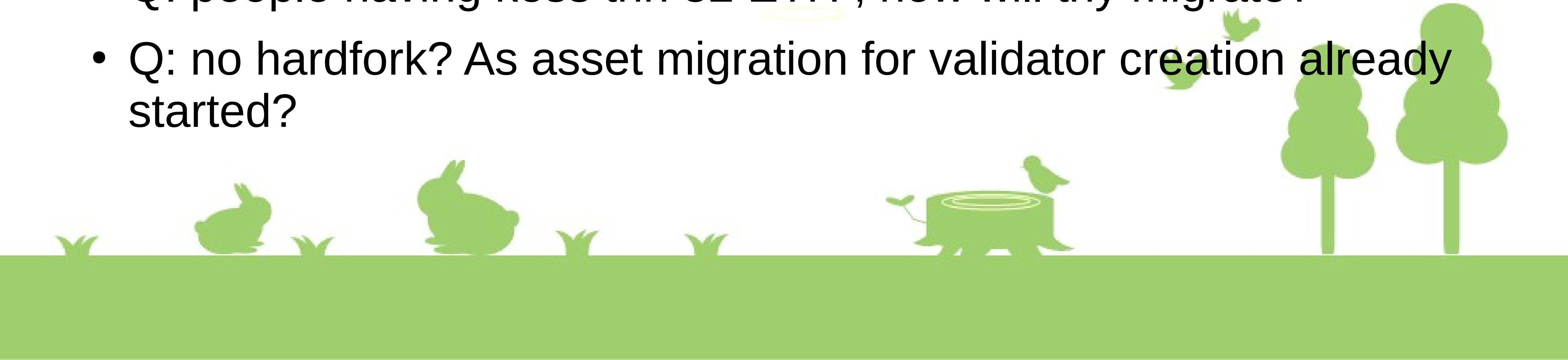
Shard 1   Shard 1024

- Q: shard blocks and beacon blocks generated independently?

Beacon chain

- Manage consensus, it stores information: active validators in system, acts as central chain, so shard chains plug data into this beacon chain, it is new chain, but its extension to eth 1.0 eco system, manage validators pool, and consensus between them

- There is bridge that allows to take ether/other assets from eth 1.0 to beacon chain then into shards (eth 2.0 NW)
- Q: state migration ?
- Q: people having kess thn 32 ETH , how will thy migrate?
- Q: no hardfork? As asset migration for validator creation already started?



Bridge:

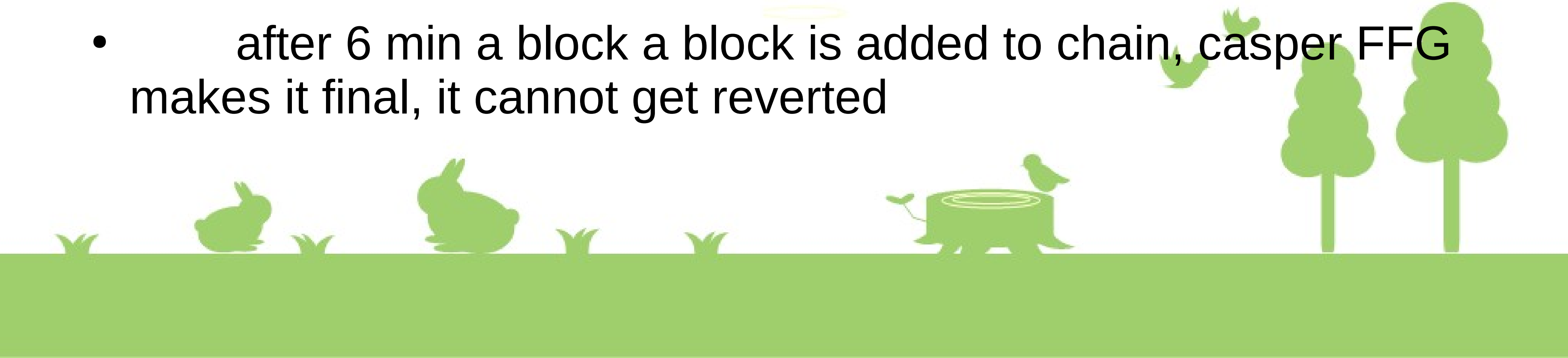
- Min 32 ETH deposit in contract: generate a merkle proof
- Idea: ETH pool contract and reward distribution.
- Then feed that merkle proof into beacon chain (validators pool)
- It is 1 way burn

Beacon chain working

- time on beacon chain is split in ~6 min epoch,
- each epoch have 64 slots
- during each slot there is a block on beacon chain
- each block is signed first by single block proposer, and then it is approved by large set of validators (1/64 th of entire validator set)
- goal is rapidly propose and rapidly agree on new blocks that are being added to beacon chain

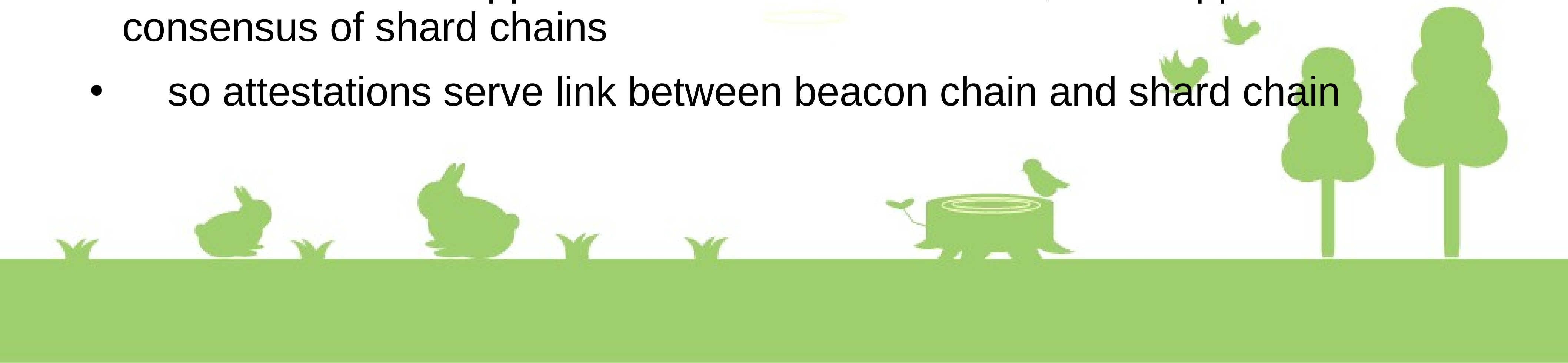
Attestation

- every block is attested by 1/64 th validators in whole validator set.
- (Q:6 sec block, not per epoch?)
- (security of shards)
- in less time block finalization, 3 sec larg num of signatures
- casper FFG algo running in background as well for consensus-
- its purpose if to give finality to block
- after 6 min a block a block is added to chain, casper FFG makes it final, it cannot get reverted



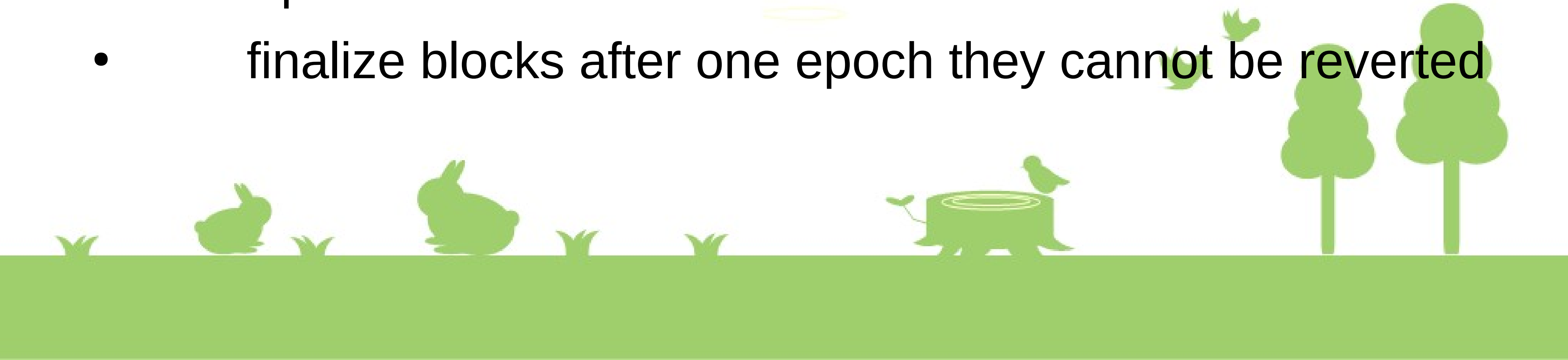
Attestation

- during each epoch, every validator is randomly assigned to one shard,
- there are 1024 shards in total,
- there are TX happening on each shards
- its job of assigned validator to validate data in shard for 6 min
- if data is correct, validator will report , at what current block that shard is
- Q: attestation per block per shard? Attestation per epoch, for finality in beacon chain?
-
- so attestations support beacon chain consensus, also support consensus of shard chains
- so attestations serve link between beacon chain and shard chain



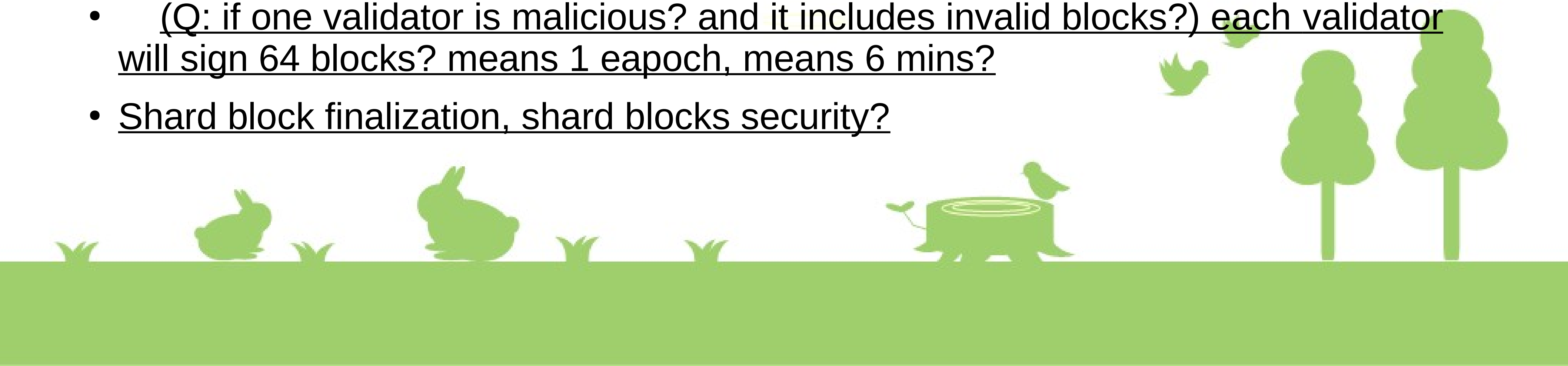
Consensus

- LMD GHOST fork choice algo (Q: for shard blocks finality along with validator signs?)
- it is able to manage NW latency + allow to manage rapid confirmation for many incoming messages in parallel
- for eth 1.0 current is longest chain algo, but that cant handle security if many parallel fast blocks are coming
-
- Casper FFG finalization:
- finalize blocks after one epoch they cannot be reverted



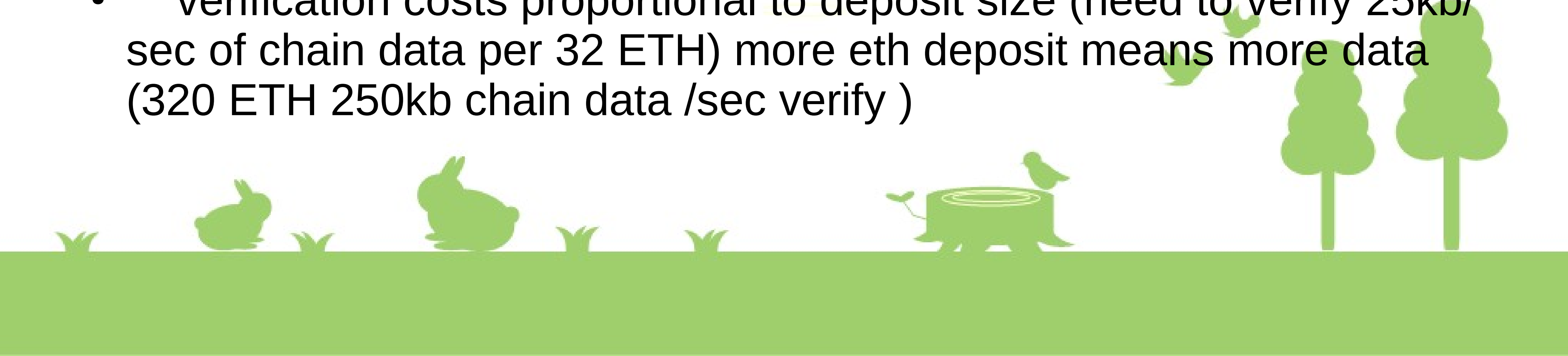
Crosslinks

- 1024 shards
- capacity of each shard is same as eth 1.0 chain
- people will do Tx etc as normal
- people will have accounts in shards
- (Q: are state unique per shard, if so then how can I transfer state/value between shards to other accounts etc)
- (Q: if value transfer bw shards, will it take 1 epoch 6min?) If state is not global bw shards? Then how to transfer value in less time?
- from beacon chain, validators are randomly assigned shards for blocks finality, for short time, its random sampling for security.
- (Q: if one validator is malicious? and it includes invalid blocks?) each validator will sign 64 blocks? means 1 eapoch, means 6 mins?
- Shard block finalization, shard blocks security?



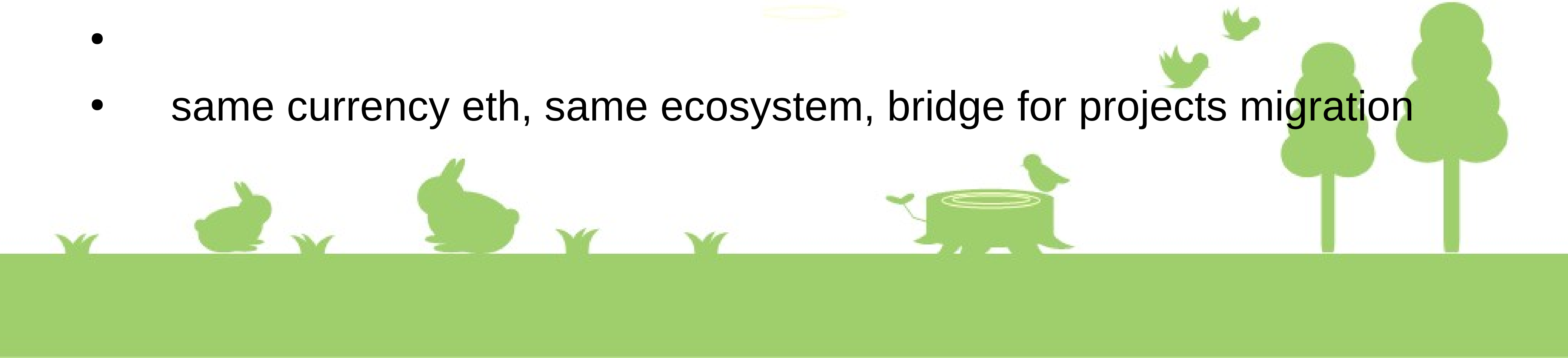
Stakes

- >= 32 eth deposit in bridge and wait for few hours then you will be active validator
- then you sign blocks using cryptographic key
- max rewards: 2~6% of deposit value per year
- if validator are offline then reward will reduce, (10% offline , 20 to 30% reduction in reward)
- its not passive interest: you have to keep node up
- if validator doing any thing wrong: it will be punished
- verification costs proportional to deposit size (need to verify 25kb/ sec of chain data per 32 ETH) more eth deposit means more data (320 ETH 250kb chain data /sec verify)



Eth 2.0

- pos, Sharding > high num of Tx per sec,
- economic based consensus
- goal: no mining pool, no staking pool, no centralization
- if you have 32 eth you will be able to do on laptop
- if you have higher deposit you will need very very powerful server for validation
-
- new technologies: BLS aggregation, proof of custody, casper FFG, optimized merkle proofs, phase3_ data availability, casper FFG,
-
- same currency eth, same ecosystem, bridge for projects migration



Discussion Points (Qs)

- shard chain clients will be same like eth 1.0 clients with instant seal by validator?
- if I have 1000 ETH and I want to be validator but only using laptop, its not possible, it will encourage me to not become validator! as it need powerful server!
- ways: becoming contributors in existing 2.0 nodes developments, develop own?

Detailed Phases 2k19

- Phase 0: PoS beacon chain without shards
- Phase 1: Basic sharding without EVM
- Phase 2: EVM state transition function
- Phase 3: Light client state protocol
- Phase 4: Cross-shard transactions: see here and more.
- Phase 5: Tight coupling with main chain security: here and more.
- Phase 6: Super-quadratic or exponential sharding

https://github.com/ethereum/wiki/wiki/Sharding-roadmap#strongphase-3strong-light-client-state-protocol