Liqueth

LITEPAPER

Table of Contents

CoinDCX

Executive Summary

The announcement of Ethereum 2.0 in 2020 took the cryptocurrency community by storm. The next generation of Ethereum network that everyone had been waiting for was finally round the corner and was going to be launched very soon. The reason for this upgrade ranged from improving the throughput and the enhancement of the network but the main reason was scalability. For a long time now, people had been complaining about the low number (~15) of transactions per second and this had time and again affected the network. People started realizing the worth of Ethereum, when in 2017 many projects created their tokens on Ethereum and raised funds through ICOs and also when CryptoKitties became a huge hit which also led to the congestion in the Ethereum network[1], causing gas prices to rise and transaction prices to soar.

Since the announcement of Ethereum 2.0 or Eth2 or Serenity, many people have staked the required 32 ETH to become a validator. There are many who wish to be a validating node but they either do not hold 32 ETH required to be a node or lack the knowledge required for setting up the system or cannot devote their time while online.

As a support to the Ethereum network upgrade, CoinDCX, India's largest and safest cryptocurrency exchange and top liquidity aggregator has partnered with Staked to provide staking facilities to anyone and everyone who holds at least 0.1 ETH in their CoinDCX wallet[2]. Along with staking facilities, CoinDCX will also be launching Liqueth (LQTH) - the ETH backed token. With almost a million-dollar worth of ETH already staked on CoinDCX, the LQTH tokens will be generated in a 1:1 ratio of the ETH staked through CoinDCX. LQTH is an ERC-20 token and will be minted only when the ETH locked in CoinDCX is sent for validator creation. This litepaper contains more details about Ethereum 1x, the reasons behind Ethereum 2.0, how Ethereum 2.0 functions, the various challenges that people had to face with the conditions mentioned, and finally the solution that CoinDCX is providing to the community. This litepaper also contains a description of the Ecosystem and the Roadmap of the token.

---

1   "CryptoKitties is causing ethereum network congestion — Quartz." 4 Dec. 2017, https://qz.com/1145833/cryptokitties-is-causing-ethereum-network-songestion/. Accessed 15 Jan. 2021.
2   "CoinDCX Promises to Launch ETH-backed Token on …." https://blog.coindcx.com/coindcx-promises-to-launch-eth-backed-token-on-reaching-1-million-in-eth2-staking/. Accessed 15 Jan. 2021.

Introduction

The Ethereum network is one of the largest and most widely used public, open-source blockchain networks in the world that was built to allow developers to create and deploy decentralized applications using smart contracts. Described as "a secured decentralized generalized transaction ledger",[3] the Ethereum network was launched on July 30, 2015. Since then, the Ethereum community has been working tirelessly to become a decentralized global computer that could one day replace the centralized applications that we use in our everyday life.

When the Ethereum network was first launched in 2015, the long-term roadmap of the project was envisioned in 4 phases. Each phase in this roadmap is defined by a set of various Ethereum Improvement Proposals (EIPs). The Ethereum community either accepts or rejects the EIPs when put forward to them. These proposals help to create guidelines that will later be followed by everyone involved with Ethereum. For example, the current release of Ethereum is called Constantinople and was created through a total of four EIPs designed to improve the network's security, privacy, and scalability.

The Turing completeness of the Ethereum network provides an abstract layer that allows everyone to establish their own rules for ownership, transaction formats, and functions for state transfer. This is accomplished by the incorporation of intelligent contracts, a series of cryptographic rules that are only enforced if those conditions are met. This also means that the Ethereum network can solve any reasonable computational problem as long as there is enough computing power and time to do so. This also means that Ethereum also provides a larger possibility of products but it also leads to greater complexity.

The first release of the Ethereum network was called Frontier. This was used to build Dapps, mine Ether, and generally experiment with the new platform. The network was then upgraded to Homestead. This provided many improvements to the protocols that would become the foundations of future upgrades and increased transaction speed. The third and current stage of Ethereum, Metropolis, has two releases, namely Byzantium and Constantinople.[4]

3   "Ethereum Yellow Paper - GitHub Pages." https://ethereum.github.io/yellowpaper/paper.pdf. Accessed 15 Jan. 2021.
4   "Ethereum 2.0: A Complete Guide. This article briefly … - Medium." 4 Jun. 2019, https://medium.com/chainsafe-systems/ethereum-2-0-a-complete-guide-d46d8ac914ce. Accessed 15

CoinDCX

Byzantium was released in October of 2017 and is lighter, faster and more secure than the previous versions. Some specific upgrades include more predictable gas prices and easier programming for developers. Byzantium also improves privacy by allowing Ethereum developers to perform efficient on-chain verification of zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments Of Knowledge). Although at first glance, the zk-SNARKs acronym may seem complicated, the system uses a relatively simple concept, that of a zero-knowledge proof. This is a method that can prove the truth of a statement without revealing anything else beyond what that statement is trying to prove. The Byzantium update also updated a mining adjustment called a "difficulty bomb" that will make mining more difficult over time in anticipation of the transition to a proof of stake system.[5]

Constantinople is meant to further build on these improvements. Although the original release date for Constantinople was set for November of 2018, Ethereum leaders and developers decided to postpone its release until 2019. The fork was finally released on February 28, 2019, at block 7,280,000.

Despite sure great advancements in technology, the Ethereum network has time and again been criticized for the increasing congestion in the network. For Ethereum to be considered as a truly decentralized global computer, it needs to make more transactions per second rather than just 15 - 20 transactions per second (TPS). The fourth and tentatively final stage of Ethereum is Ethereum 2.0 or Serenity. There have been multiple network upgrades but ETH 2.0 will be the largest and the most comprehensive update that has ever been implemented by the Ethereum community.

Thus upgrades will take place in different phases over a span of 2 years, although the timeline may be subject to change. We will try to understand why ETH 2.0 is so important but before that, we will go through the different problems that led to such a situation.

This litepaper has highlighted the different reasons why ETH 2.0 was needed, the challenges faced by the community, how ETH 2.0 changes the scenario and how CoinDCX has supported this upgrade by providing its solution to the crypto community.

5   "Ethereum 2.0: A Complete Guide. This article briefly ... - Medium." 4 Jun. 2019, https://medium.com/chainsafe-systems/ethereum-2-0-a-complete-guide-d46d8ac914ce. Accessed 15 Jan. 2021.

Problems with ETH

The single most important issue that Ethereum faces is network scalability. With more than 3,000 decentralized apps (Dapps) at the time of writing,[6] the Ethereum network needs to process a really high number of TPS. The Dapps on Ethereum ranges from gaming to decentralized finance (DeFi), gambling, marketplaces, social media, and more. All these are dynamic in nature and need quick transactions to take place. For an exchange on Ethereum to work as quickly as Nasdaq (which executes thousands of transactions per second), Ethereum surely needs a network upgrade that can support this.

With each passing day, more and more Dapps have been added to the network and this has led to an on-going increase in the number of transactions generated on the network and an increase in the cost of these transactions. This has made the Ethereum network slower, with more pending transactions being stored in the mempool or the txpool.

For the network to achieve mass adoption and better performance, there have been multiple upgrades that could help increase the scalability in the network. After investigating several other options, the Ethereum team settled on a process called sharding as the best solution for network scalability. Off-chain solutions like plasma chains and state channels will also likely be used to take the load off of the main network and further increase scalability. Before we discuss these under Eth2, let us understand the problems that the current Ethereum network was facing.

The most obvious issue that has been addressed by the network is the efficiency and the environmental sustainability of the Ethereum blockchain network. The Ethereum network currently relies on the Proof of Work (PoW) consensus mechanism where all nodes on the network compete with each other to mine a block, to get mining rewards and the transaction fees for the transactions stored in the block. While Proof of Work is a highly secure consensus algorithm, the fact that this mechanism takes up a lot of resources in the form of electricity and other resources is something that has made everyone very concerned about it.[7] Today miners in the PoW mechanism keep

6   "State of the DApps — DApp Statistics." https://www.stateofthedapps.com/stats/platform/ethereum. Accessed 15 Jan. 2021.

7   "The Problems That Ethereum 2.0 Proof-of-Stake Aims to Solve ...." 26 Oct. 2020, https://medium.com/better-programming/the-problems-that-ethereum-2-0-proof-of-stake-aims-to-solve-5361c155461a. Accessed 15 Jan. 2021.

CoinDCX

running the hash functions to get a hash value that will help them store transactions on the blockchain. This makes the system computationally very expensive. Instead of working together to validate a transaction, miners compete with each other and that leads to a loss of large amounts of electricity, which also means that only the miner who wins the race gets the reward for it, others do not.

Another important issue addressed by the community is the bottleneck around its Ethereum Virtual Machine (EVM). The EVM is essentially the underlying structure of Ethereum that executes code and allows the network to function correctly. It is responsible for the internal state of the Ethereum network and for all of its computations, ensuring accuracy, balancing of account information, maintaining the gas prices, addresses and block information. The EVM also keeps a track of block information, storage state, account state and runtime environment information. The EVM is primarily responsible for dealing with all Ethereum smart contracts which are written in Solidity/Vyper and compiled into a unique EVM bytecode. The contracts are then executed by each node on the network. deals with all Ethereum smart contracts which are written in Solidity/Vyper and compiled into unique EVM bytecode. The contracts are then executed by each node on the network.

ETH2 - The Solution

The two major changes that will be seen on Ethereum are the transition of the network's consensus mechanism from the Proof of Work consensus mechanism to the Proof of Stake (PoS) mechanism and the addition of shares to the Ethereum mainnet.

The shift from a PoW to PoS mechanism called Casper will seek to solve the efficiency and sustainability issue of the Ethereum network. This transition will become increasingly important because of the difficult bomb mining adjustment that was introduced in 2017 through the Byzantium update. The bomb will make mining Ether more and more difficult until it will eventually become infeasible. This device was introduced in anticipation of Serenity's transition from PoW to PoS and is yet another reason why the update is so important for the Ethereum community.

Casper will be implemented on Ethereum in a way that will use Ethereum's current PoW proposal mechanism to introduce new blocks onto the blockchain. If two blocks are proposed simultaneously, validators are only rewarded for betting on one chain, so it only makes sense to bet on the original chain, as this is the one that is most likely to succeed.[8]

More importantly, Casper introduces a mechanism that will instantly confiscate the entire stake of any validator who tries to support an invalid chain by validating more than one block at a time. Should a validator maliciously attempt to compromise the network (i.e. validate incorrect data history), all or some of their 32 staked ETH will be slashed (more about penalties later). Users can submit evidence of voting on the wrong chain by miners to penalize incorrect votes. Casper, therefore, handles the nothing at stake problem by introducing a wrong-voting penalty to the protocol.

The final major issue that will be addressed by Eth2 is speed and usability. This is related to but not the same as, the issue of scalability that will be addressed by sharding. The introduction of sharding should remove the most significant bottleneck for transaction speed and throughput. To ensure that the Ethereum Virtual Machine is able to maintain its speed and perform tasks as per its expectations, ETH2 has

8   "Everything You Need to Know About Ethereum 2.0 - Medium." 10 Dec. 2020, https://medium.com/london-blockchain-labs/everything-you-need-to-know-about-ethereum-2-0-bc9c2d101778. Accessed 15 Jan. 2021.

CoinDCX

been set in place to include Ewasm (Ethereum wasm) to the network. Wasm is a W3C Community Group open standard instruction-set that is currently being developed by engineers from Google, Mozilla, Microsoft and Apple. In addition to increasing speed and throughput. Ewasm will increase the security and usability of the Ethereum network, and bestow several other benefits.[9]

In addition to the shift from PoW to PoS and including shards to Ethereum mainnet, Serenity has two long-term design goals created in anticipation of potential issues that may arise in the future. The first is to design the release in such a way that the network will be able to remain live in the event of a major partition or if a very large percentage of nodes go offline simultaneously. In his talk at Devcon 2018,[10] Ethereum developer Justin Drake explained how the team wants Eth 2.0 to be able to "survive world war three" or a similar situation in which up to 80 percent of nodes go offline at once.

The other contingency that Eth 2.0 anticipates is the advent of quantum computing. There is currently an ongoing tech race between the United States, China, and other major powers and corporations to be the first to invent a production quantum computer. At this point, the question is not if, but when. Whenever they do come along, quantum computers will be exponentially more powerful than even the most advanced traditional computers. This will render most existing cybersecurity, including encryption and blockchain tech, relatively defenseless and easily hack-able. It is therefore important for new and future blockchain networks to do everything possible (within the limits of traditional binary computing) to protect against the eventuality of quantum computers. The final design goal for Eth 2.0, as laid out in the Ethereum GitHub repo is- "to select all components such that they are either quantum secure or can be easily swapped out for quantum secure counterparts when available.[11]

9   "Ethereum 2.0: A Complete Guide. Ewasm. | ChainSafe - Medium." 31 Aug. 2019, https://medium.com/chainsafe-systems/ethereum-2-0-a-complete-guide-ewasm-394cac756baf. Accessed 15 Jan. 2021.
10   "Devcon4 Mainstage - Justin Drake - YouTube." 2 Nov. 2018, https://www.youtube.com/watch?v=zqL_cMlPjOI. Accessed 15 Jan. 2021.
11   "Ethereum 2.0: A Complete Guide. This article briefly ... - Medium." 4 Jun. 2019, https://medium.com/chainsafe-systems/ethereum-2-0-a-complete-guide-d46d8ac914ce. Accessed 15 Jan. 2021.

How does ETH2 work?

As discussed before, Eth2 will lead to a shift from PoW to PoS protocol alongside the addition of shards to Ethereum mainnet. It is necessary to understand how the entire network will function once these changes get implemented.

In this section, we will be discussing the different features of the Eth2 network.

Proof of Stake (PoS)

A shift to the PoS consensus mechanism would allow ETH holders to stake their tokens on the network to participate in the transaction validation process and earn rewards in return.

The contract for Eth2 must collect an initial 16,384 deposits of 32 ETH each, a total of 524,288 ETH, to proceed with the Phase 0 launch of Ethereum 2.0. These funds will be locked in the contract as a security deposit of being given access to the network and its validation procedure. Any malicious activity from these validators will lead to a penalty being imposed on their stake. This is how we expect the security of the network to be maintained.[12]

Since validation depends on the ETH staked in the network and not the computing power needed, as in the case of Proof of Work, no validator would want to act against the interest of the blockchain that would lead them to lose their funds and a possibility of a reduction in the price of each token if people start believing that the network is under attack.

Attacking the network also means that a validator would need to have a very high stake in the network. Having a high stake and performing an attack means that these attackers could even lose their whole funds, thus making such attacks expensive. This process is called slashing.

The only major drawback of PoS is that there could still be validators who stake a lot more than the others, thus having more influence in the network and getting more

---

12   "Everything You Need to Know About Ethereum 2.0 - Medium." 10 Dec. 2020, https://medium.com/london-blockchain-labs/everything-you-need-to-know-about-ethereum-2-0-bc9c2d101778. Accessed 15 Jan. 2021.

CoinDCX

staking rewards. As more people stake on the network, the annual percentage rate (APR) keeps decreasing. This might not be that advantageous for those validators who stake fewer funds, thus making the entire process again "not-so decentralized". Moreover, having a larger stake in the network also means that the network could be attacked.

Staking on Ethereum will work in a similar way as it works on any other PoS blockchain. You will validate only as many transactions as your stake in the network. For example, if you have staked 4 tokens in the network of 100 tokens, then you will only validate 4% of the new blocks and receive the rewards for those transactions recorded in the blocks.[13]

Slots and Epochs

The validators on the network will be responsible to validate transactions and also propose new shard blocks. If they are not chosen to propose a new block then they can make sure that everything in the proposed block looks right.

A minimum of 128 validators (called a committee) is needed to attest every shard block. Every shard block is to be proposed and validated by this committee in a time-frame known as a slot. Each slot is 12 seconds and an epoch contains 32 slots adding to 6.4 minutes. Once the validation process is complete for the epoch, the committee is broken up, and a new set of validators will be chosen using a pseudo-random process RANDAO. This is done so that malicious validators don't have any control over the final outcome of new proposed blocks.[14]

A slot is therefore a chance to add a block to the Beacon Chain. Every 12 seconds, one Beacon Chain block and 64 shard blocks (as the current Eth2 has plans for 64 PoS shards) are added when the system is running optimally. Slots are similar to block time but some slots can remain empty too.

Although real shards are not introduced until Phase 1, validators participate in the consensus of the assigned shard to vote for the shard's head. The validator links the shard head to the beacon block for a slot and as mentioned earlier, they police each

13   "Everything You Need to Know About Ethereum 2.0 - Medium." 10 Dec. 2020, https://medium.com/london-blockchain-labs/everything-you-need-to-know-about-ethereum-2-0-bc9c2d101778. Accessed 15 Jan. 2021.
14   "The Beacon Chain Ethereum 2.0 explainer you ... - ethos.dev." 16 Jun. 2020, https://ethos.dev/beacon-chain/. Accessed 15 Jan. 2021.

other and are rewarded for reporting other validators that make conflicting votes or propose multiple blocks.

Proposing and attestations

One validator will be pseudo-randomly selected for each slot to propose a block. In Phase 0, the main role of the proposing validator will be to collect all the attestation votes and any whistleblower activities into a block. If the selected validator fails to propose a block in time, then the network will progress without a block for that slot. Validators will only learn about which slot they can propose a block at the beginning of an epoch.

At least 16 committees will be assigned the slot for which they need to submit an attestation vote 1 epoch in advance. Attestations are weighted by a validator's effective balance with a maximum ceiling of 32 ETH. For example, if validators A, B and C have 16 ETH, 32 ETH and 48 ETH respectively, their attestation vote weights will be 20% (= 16/[16 + 32 + 32]), 40% (= 32/[16 + 32 + 32]) and 40% (= 32/[16 + 32 + 32]).[15]

There are three types of attestation votes that a validator will submit.

- **LMD-GHOST vote to determine the current height of the chain**
  Your validator needs to vote on what the head of the chain is (the most recent block). This is referred to as the head vote.

- **Casper FFG votes to finalize blocks**
  Your validator needs to vote on whether they agree with the most recent checkpoint. Once ⅔ of attesting validators agree, the blocks prior to that checkpoint becomes justified. This is referred to as the target vote.

- Your validator also needs to vote on **whether they agree with the most recently justified checkpoint**. Once ⅔ of attesting validators agree, the justified blocks prior to this checkpoint become finalized. This is referred to as the source vote.

In summary, it will take at least one epoch, 6.4 minutes, for blocks to become justified and at least two epochs, 12.8 minutes, for blocks to become finalized.

---

15   "Deeper dive into Ethereum 2.0: Part 1 | stakefish - Medium." 8 Sep. 2020, https://medium.com/stakefish/deeper-dive-into-ethereum-2-0-part-1-93c475a18735. Accessed 15 Jan. 2021.

CoinDCX

If finalization does not happen for 4 consecutive epochs, a mechanism called the inactivity leak will kick in, penalizing validators that have stopped submitting Casper FFG votes. This penalization will persist until finalization can be achieved on the network. [16]

Joining and exiting as a validator

Once you have 32 ETH on a validator node, you can signal your intention to start validating. After your intentions are relayed to the network, you are placed in the activation queue. Only 4 validators can be activated per epoch in order to prevent the validator set from changing too rapidly. Once it is your turn, your validator will get added to the active set in 4 epochs (≈ 25.6 minutes).

Validators who have been active for at least 256 epochs (≈ 27 hours) can signal to the network to initiate a voluntary exit from the active validator set. Once the message has been relayed to the network, the validator will be put at the end of the exit queue. There is a limit to how many validators can exit per epoch, similar to the limit on activations per epoch. If there are no validators in the exit queue, it will take at least 5 epochs (= 32 minutes) for the validator to exit. It will take another 256 epochs (≈ 27 hours) before any ETH balance becomes withdrawable. In Phase 0, validators that have exited from the active validator set will have no option to join again.

Slashing

In order to prevent malicious behaviors, specifically those that could fork the network, Ethereum 2.0 uses a mechanism called slashing. Your validator can be slashed for the following reasons.

- Proposing two different blocks in a single slot[17]
- Submitting two different Casper FFG attestations in a single epoch
- Submitting a Casper FFG attestation that completely surrounds another Casper FFG attestation

16   "Deeper dive into Ethereum 2.0: Part 1 | stakefish - Medium." 8 Sep. 2020, https://medium.com/stakefish/deeper-dive-into-ethereum-2-0-part-1-93c475a18735. Accessed 15 Jan. 2021.

17   "eth2.0-specs/beacon-chain.md at dev · ethereum … - GitHub." https://github.com/ethereum/eth2.0-specs/blob/dev/specs/phase0/beacon-chain.md. Accessed 15 Jan. 2021.

CoinDCX

For posing a threat to the network, the offending validators will have their effective balance slashed. In addition to this balance reduction, the slashed validators will have a longer than average withdrawal delay. Typically, after exiting, validators would only need to wait 256 epochs (≈ 27 hours) to withdraw their ETH balance. For slashed validators, they will need to wait for 8,192 epochs (≈ 36 days) before the remaining ETH balance becomes withdrawable. In Phase 0, validators that have been ejected will no longer be able to join the active validator set.

Forced ejection as a validator[18]

There are two cases where a validator will be forced to exit from the active validator set. We have already discussed the first one in the Slashing section above, but we'll cover another scenario where a validator could be forcefully ejected from the active set.

- **Getting slashed**

    As discussed previously in the Slashing section, validators getting slashed will be automatically put into the exit queue.

- **Validator balance falling to 16 ETH or below**

    If a validator's effective balance falls to 16 ETH or below for whatever reason, the network will automatically put the validator in the exit queue. The process will look a lot similar to a voluntary exit. Once the network observes a balance of 16 ETH and under, the validator will be put at the end of the exit queue. If there are no validators in the exit queue, it will take at least 5 epochs (= 32 minutes) for the validator to fully exit. It will take another 256 epochs (≈ 27 hours) before any ETH balance becomes withdrawable.

Rewards, Penalties and Slashing

A key unit of account that will frequently appear is **base_reward**.

$$base\_reward = \frac{64 \ x \ \textit{Effective Balance on Validator}}{¼ \ x \ \sqrt{\textit{Total ETH Staked Network}}}$$

18   "Deeper dive into Ethereum 2.0: Part 1 | stakefish - Medium." 8 Sep. 2020, https://medium.com/stakefish/deeper-dive-into-ethereum-2-0-part-1-93c475a18735. Accessed 15 Jan. 2021.

Staking rewards

There are three ways a validator can get rewarded.

Proposer rewards

After you successfully propose a block as a validator, your rewards will be based on:

_Number of Attestations Included x ⅛ x base_reward_

Attestation rewards

After you submit attestation votes as a validator, your rewards will be based on:

$$3 \text{ x base\_reward} + \tfrac{7}{8} \text{ x base\_reward x } \frac{1}{\textit{Number of slots delayed}}$$

Whistleblower rewards

Once a slashable offense is observed and gets reported, the whistleblower and the block proposer who includes the whistleblower's report will be rewarded.[3] Some of the rewards are diverted to the proposer in order to incentivize a swift inclusion of slashing events to the network.

Whistleblower:

$$\tfrac{7}{8} \text{ x } \frac{\textit{Slashed validator's effective balance}}{512}$$

Proposer including the whistleblower's report:

$$\tfrac{1}{8} \text{ x } \frac{\textit{Slashed validator's effective balance}}{512}$$

Penalties

Penalties are relatively minor compared to slashing and will not result in validators getting kicked out. There are two ways that validators will be penalized.

Offline penalty (either submitting incorrect attestations or missing attestations):

3 x base_reward

Inactivity leak penalty - a mechanism that kicks in if the network is unable to reach finality for 4 consecutive epochs. All validators who are offline, effectively causing the finality delay, will see their balance decrease over time so that the network will have enough participating stake to reach ⅔ majority attestation votes and achieve finality:

Effective balance x Number of epochs finality is delayed x $\dfrac{1}{16,777,216}$

Slashing

Slashing has some severe consequences. As a reminder, there are three ways a validator can get slashed: proposing two different blocks in a single slot, submitting two different Casper FFG attestations in a single epoch and submitting a Casper FFG attestation that completely surrounds another Casper FFG attestation. The amount of ETH that gets slashed is identical for all three instances.

Amount slashed on the first block where a validator is found guilty:

$\dfrac{Effective\ balance}{32}$

Amount slashed 4,096 epochs (≈ 18 days) after the validator is first found guilty:

$\dfrac{Effective\ balance\ \ x\ \ Total\ ETH\ slashed\ during\ the\ simliar\ period}{Total\ Staked\ ETH}$

Amount slashed every epoch until the validator gets ejected from the active set in 8,192 epochs (≈ 36 days):

3 x base_reward

Phase 0 of ETH2

The Beacon Chain was launched on December 1, 2020. It is an overarching chain that will ensure that the data on the shards has the most up-to-date data, reward validators for proposing new blocks and punish them for their malicious behavior. There will not be any shard chains operational as there is nothing that needs to be in sync. Its role initially will only be to bring all validators onboard.

This chain will have Casper finality, a random number generator to shuffle validators, and simulate crosslinking in the non-existent shard chains. ETH will continue to receive upgrades and operate alongside the Beacon Chain.

The first implementation of Casper will use Ethereum's current PoW proposal mechanism to introduce new blocks onto the blockchain. If two blocks are proposed simultaneously, validators are only rewarded for betting on one chain, so it only makes sense to bet on the original chain, as this is the one that is most likely to succeed.[19]

More importantly, Casper introduces a mechanism that will instantly confiscate the entire stake of any validator who tries to support an invalid chain by validating more than one block at a time. Should a validator maliciously attempt to compromise the network (i.e. validate incorrect data history), all or some of their 32 staked ETH will be slashed (more about penalties later). Users can submit evidence of voting on the wrong chain by miners to penalize incorrect votes. Casper, therefore, handles the nothing at stake problem by introducing a wrong-voting penalty to the protocol.

Phase 1: Shard Chains

Phase 1 will add a basic structure of sharding to Ethereum 2.0. This is necessary from a scalability point of view. This phase is expected to start with 64 PoS shards but they will not support accounts or smart contracts right away.

Along with shard chains, cross-references will also be introduced in Phase 1. Cross-references will allow to record and finalize the state of each shard on Beacon Chain. Ultimately, cross-references will serve as the basis for transactions between shards in later phases.

19   "ETH 2.0 Explained: Staking, Sharding, and Scaling ... - Medium." 24 Jun. 2020, https://medium.com/interdax/ethereum-2-0-explainer-e996ac7dc006. Accessed 15 Jan. 2021.

CoinDCX

Phase 1.5: Mainnet to Shard

Everything until Phase 1.5 will be done on the Proof of Work blockchain. It is only when the mainnet becomes the shard in Phase 1.5 will the transition to PoS take place. We expect this transition to be seamless and to happen sometime in 2021.

Phase 2: Fully Formed Shards

The fully formed shard of Phase 2 is expected to be seen beyond 2021. Shards should be fully functional chains that will then be compatible with smart contracts and be able to communicate with each other more freely. Developers may even be able to design shards in their own ways.

Genesis of ETH2

The genesis of Eth2 was based on the condition that there must be 16,384 validators (128 validators in each 128 committee), with each validator staking 32 ETH on the Eth2 smart contract. The condition was met on November 24, 2020 and this led to the launch of the genesis block on December 1, 2020.

Problems related to Ethereum 2.0

Although becoming a validator in a PoS mechanism is cheaper than being a miner in a PoW protocol, the fact that not many people own 32 ETH or are willing to stake at least 32 ETH (~ $16,480 at ~$515 per ETH) is also true. This leads to problems of fungibility. Another issue is facing technical issues on the network. Imagine staking 32 ETH and losing some or all of it because you did not deposit it correctly.

Users will also have to stake their ETH for a very long duration, something that many might not be willing to do. It is okay for people who have deep pockets, but this will again lead to the centralization of power in the network, where only rich people stake large amounts of ETH and earn rewards. A majority of the people who wanted to do it and had enough funds to take the risk of staking have staked so far. This is because of the risk associated with staking your tokens for a long period of time.

CoinDCX

CoinDCX's Solution

CoinDCX aims to solve the staking challenge by providing a smart contract-driven solution. Not only will the users be able to stake any number of ETH greater than 0.1 ETH, they will also be given a token called Liqueth (LQTH) which will be backed by the ETH staked on CoinDCX. This token will address liquidity locking challenges, protect from inactivity leaks and slashing penalties by making an infrastructure that is up and running on the server and driven by smart contracts. The token mint function is called once the ETH is locked on the Pooling Hub. As soon as the pooling hub value is in multiples of 32 ETH, pooling hub calls batching contract for the creation of validator. The batching contract will send the funds in multiples of 32 ETH to the validators. These batching contracts can send up to 5000 ETH in a single transaction on the ETH blockchain.

There are various parts of the ETH 2.0 token solution we will explain them in this section:

- Deposit Contract: The Deposit Contract is a smart contract and the primary mechanism to transfer funds from an ETH account to an ETH2 validator. It specifies who is staking (ETH address that makes the deposit), who is validating (validator public key), the amount of stake (minimum of 32 ETH), and who can withdraw the funds (withdrawal key pair).

- Validator: A validator participates in the proof-of-stake consensus for the ETH2 protocol. Each validator on ETH2 must have a minimum of 32 ETH staked in order to vote for new blocks and earn rewards.

- Batching Contract: Our partners - Staked have developed and open-sourced a batching contract to save our users on gas costs and deposit multiple validators with a single on-chain transaction. It enables users to deposit up to 185 validators (~6K ETH) in a single deposit, offering the convenience of signing a single transaction rather than 185 distinct transactions.

- Reporting: This will take note of user-level rewards generated on the ETH 2.0 validator and help users take payouts of the funds on a periodic basis.

- User panel: This is the panel where the user will be able to withdraw his funds or see how much is accumulated so far.

- Profit Amplifier: This is a special function enabled on the entire DCX product ecosystem against the usage of tokens. If the user holds the token or uses some of the services with the token he is entitled to receive extra rewards in the ecosystem.

ETH 2.0 Token Ecoystem
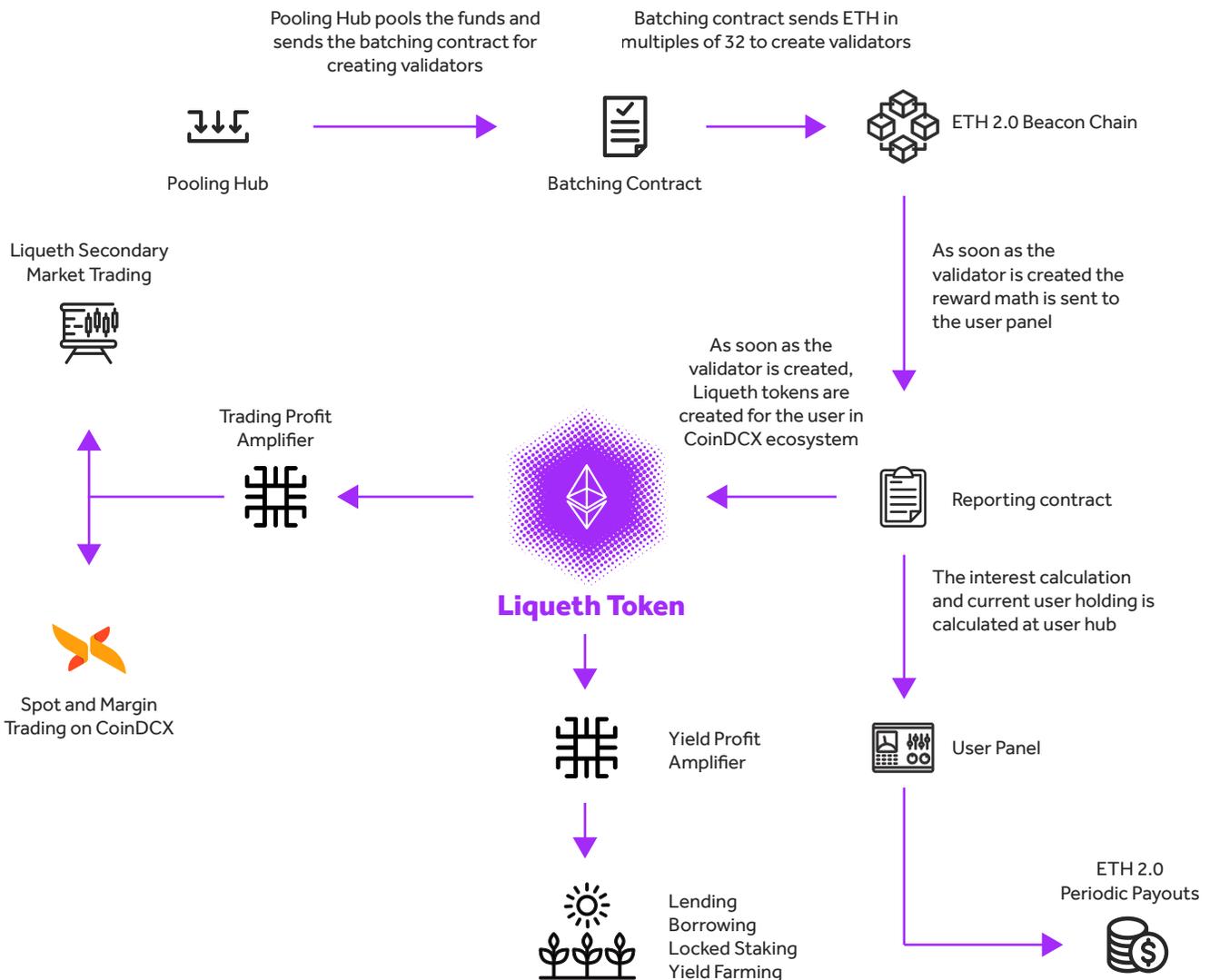
Liqueth (LQTH) - The ETH backed token

Liqueth (LQTH) - The ETH-backed token is a bond-backed token based on proof of staking reserve protocol i.e the tokens will be generated in a 1:1 ratio of the Ethereum staked through the validator. The token will be an ERC-20 token and will be minted only when the ETH is locked in CoinDCX and sent for validator creation. Here are some of the properties of the token:

- Fair Mined/Minted - Each token is backed by Ethereum is the reserve.
- No Founder of team rewards- No token is generated extra for founders or team working on the project.
- Burns 1:1 with Ethereum at the time of unlocking of Ethereum.
- Holding the token is similar to holding Ethereum for the long term but with some extra interest rewards and platform rewards.

As the name suggests, the most important utility of the token is liquidity! Liqueth (LQTH) will be pegged to Ethereum's price and tradable on CoinDCX markets. Other token utility includes:

- A periodic payout to all the holders based on their token holdings.
- Reduced fees when paying through the token- Users will get fee discounts when used as a medium to pay trading fees.
- Use as collateral in Margin- The token can be used as collateral in margin trading.
- Lower interest rates while using the token as collateral: Lower rates of interest charged after 24 hours in the open position when paid through token.
- Airdrop Farming- All the token holders will get an additional airdrop for participating in all the campaigns CoinDCX conducts.
- The additional yield on other locked staking products: CoinDCX has already announced its partnership with some of the most promising Defi and staking providers in the industry. The token HODLers will be given early access to the products along with additional yield which will quickly help them multiply their rewards as compared to those who do not hold LQTH tokens.

CoinDCX

Ecosystem

The community lies at the heart of Liqueth's ecosystem. This ETH backed token enables the community to take advantage of staking rewards from the blockchain along with the benefits provided by CoinDCX and its partners to boost the trading profits. Here are some of the activities conducted by CoinDCX to develop and nurture Liqueth's ecosystem. Several activities will be performed by our partners and the community, exclusively for all the Liqueth (LQTH) token holders.

Activities by CoinDCX:

- Onboard new partners to provide additional yield benefit to the Liqueth (LQTH) token holders.
- Provide fee discounts
- Enable lending and borrowing mechanism
- Provide discounts on Margin
- Create a secondary market to trade tokens
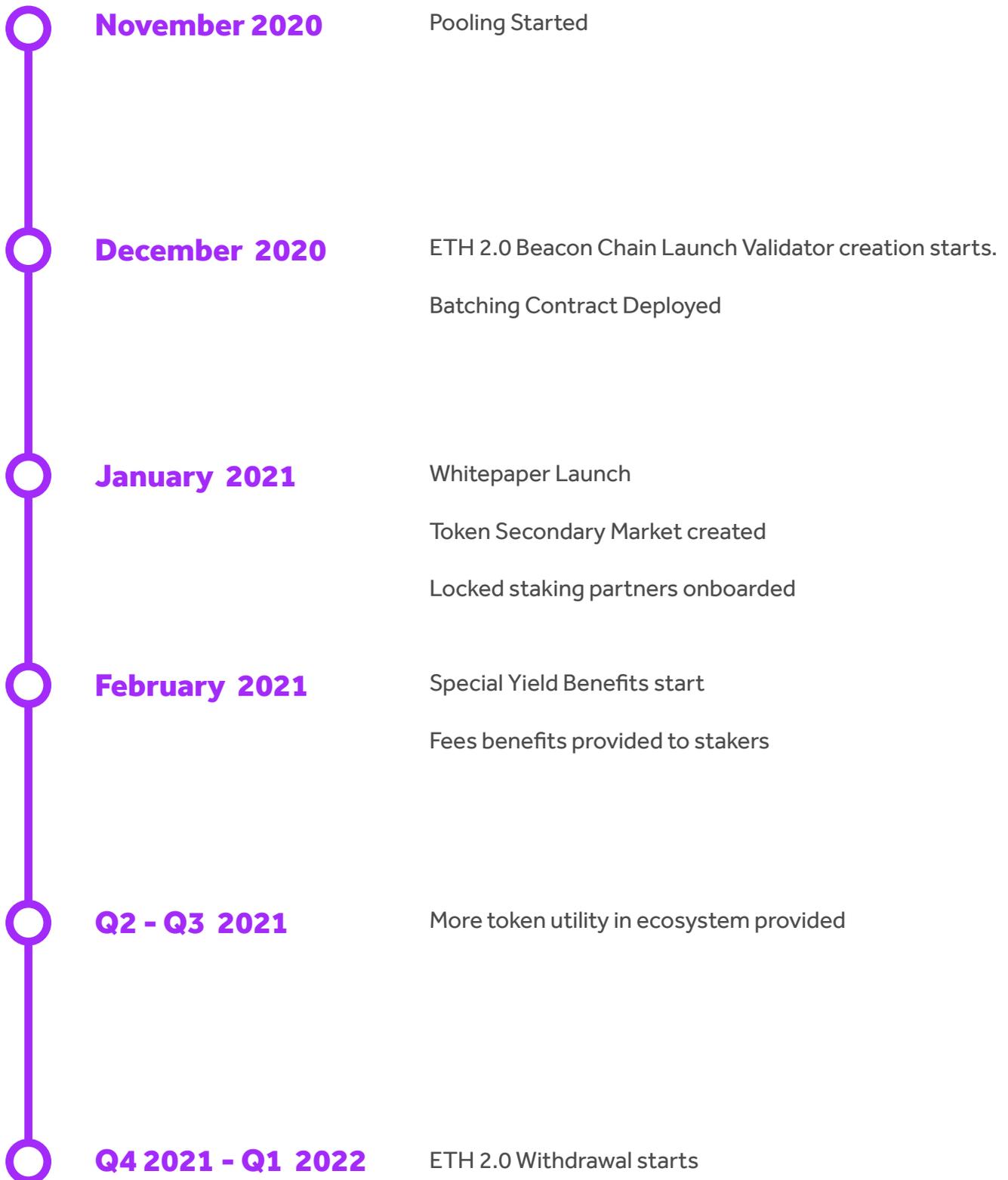
Activities by Partners:

- Provide special benefits to all the Liqueth (LQTH) token holders and give access to exclusive activities conducted for these token holders only.

Activities by Community:

- Participate in activities run by CoinDCX communities to get access to special benefits.
- Get exclusive rewards for participating in Community-run events, airdrops and much more.

Roadmap

November 2020   Pooling Started

December 2020   ETH 2.0 Beacon Chain Launch Validator creation starts.

                           Batching Contract Deployed

January 2021   Whitepaper Launch

                           Token Secondary Market created

                           Locked staking partners onboarded

February 2021   Special Yield Benefits start

                           Fees benefits provided to stakers

Q2 - Q3 2021   More token utility in ecosystem provided

Q4 2021 - Q1 2022   ETH 2.0 Withdrawal starts

CoinDCX

About CoinDCX

CoinDCX is India's largest and safest cryptocurrency exchange and top liquidity aggregator in the world. The exchange has instant deposit and withdrawal facilities. The versatile wallet structure provides the best fee structure in the industry. Established in 2018, the exchange is today deemed by many market participants as India's most trustworthy cryptocurrency exchange.

CoinDCX offers users a single-point access to a diverse suite of crypto-based financial products and services:

Insta -   Provides fiat onboarding from INR to crypto
Spot -   Gives access to trade cryptocurrencies across 500+ markets
Margin -   With up to 6x leverage trades across more than 250 markets
Lend -   Decentralized lending service wherein users can earn upto 14% APR
Stake -   Users can earn passive income by staking their cryptos
Futures -   Maximize trading potential with leverage up to 20x

The exchange has a powerful yet simple interface that provides fast and reliable trading experience for professional and novice customers alike. CoinDCX is backed by world-class security processes which include a safe & instant KYC verification process and insurance cover to safeguard users' funds.

For more information, visit https://coindcx.com/