crypto.com

Ethereum 2.0

An Introduction

August 2020

Research and Insights

DeFi Report

Senior Research Analyst
Kendrick Lau

RESEARCH DISCLAIMER

This report alone must not be taken as the basis for an investment decision. The user assumes the entire risk of any use made of this information. The information is provided merely complementary and does not constitute an offer, solicitation for the purchase or sale of any financial instruments, inducement, promise, guarantee, warranty, or as an official confirmation of any transactions or contract of any kind. The views expressed therein are based solely on information available publicly/internal data/other reliable sources believed to be true. This report includes projections, forecasts and other predictive statements which represent Crypto.com's assumptions and expectations in the light of currently available information. These projections and forecasts are based on industry trends, circumstances and factors which involve risks, variables and uncertainties. Opinions expressed therein are our current opinion as of the date appearing on the report only.

No representations or warranties have been made to the recipient as to the accuracy or completeness of the information, statements, opinions or matters (express or implied) arising out of, contained in or derived from this report or any omission from this document. All liability for any loss or damage of whatsoever kind (whether foreseeable or not) which may arise from any person acting on any information and opinions contained in this report or any information which is made available in connection with any further enquiries, notwithstanding any negligence, default or lack of care, is disclaimed.

The reports are not for public distribution. Reproduction or dissemination, directly or indirectly, of research data and reports of Crypto.com in any form is prohibited except with the written permission of Crypto.com. Persons into whose possession the reports may come are required to observe these restrictions.

Contents

1. Executive Summary

Welcome to our Macro Report on Ethereum 2.0 (ETH 2.0), a multi-year system upgrade to the Ethereum network, the first phase of which is expected to launch at the end of 2020, bringing with it a new consensus algorithm.

Key Takeaways

- ETH 2.0 will implement two main features, Proof-of-Stake and Sharding, to improve the security and scalability of the network;
- Proof-of-Stake is a much more efficient and arguably fairer method to distribute transaction validation responsibilities and rewards versus Proof-of-Work, which disproportionately rewards large miners and consumes copious amount of energy on wasteful calculations to secure the network;
- Sharding, although complex, is one of the most promising methods to add scalability to a blockchain network and in tandem with layer 2 scaling solutions, which can increase scalability by a factor of hundreds, if not thousands;
- ETH 2.0 will be rolled out in three phases. Phase 0, to be released in December 2020, will only implement the Beacon Chain. Phase 1 will include sharding. It is not until Phase 2 in 2022 where dApp functionality will be enabled and Ethereum's dApps can be migrated over to ETH 2.0 shard chains;
- Validator returns can range from 2% to 20% depending on the number of validators participating in the network, but returns will likely be on the higher end at launch;
- Becoming a validator can be technically challenging, although third party service providers will provide staking services on day one;
- Being a validator to earn rewards can be attractive, but there are risks to consider – primarily, ETH staked will be locked up for at least one year, until the launch of Phase 1 in 2021.

2. Introduction

As Ethereum celebrates its fifth birthday, we are a step closer to the launch of ETH 2.0 (code-named "Serenity"), a system-wide upgrade that will change how the blockchain fundamentally operates. These changes include a shift to proof-of-stake (PoS), the implementation of sharding, and an improved virtual machine, the Ethereum WebAssembly (eWASM).

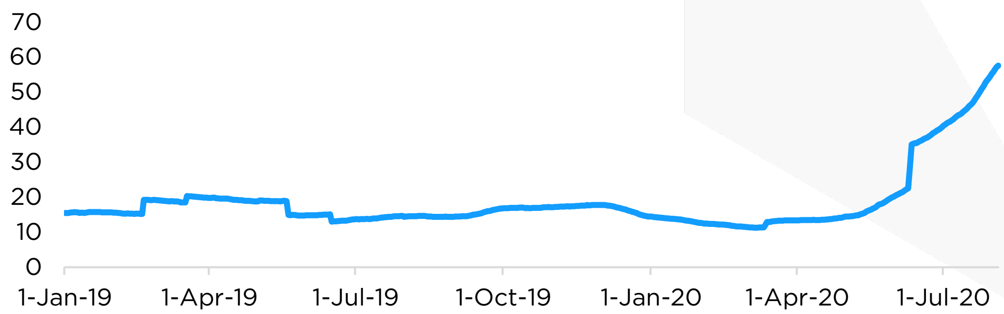
Ultimately, these upgrades will make Ethereum more efficient and bring improved throughput compared to the current limit of 10-15 transactions per second, allowing dApps to operate with less latency and at lower network costs.

2.1 Ethereum's Current State

Ethereum is the second largest cryptocurrency by market capitalization, and the most popular blockchain network smart-contract enabled platform. In Q2 2020, the total transaction volume on the Ethereum network reached an all-time high of US$14.3 billion, with 768 active dApps and 1.51 million users. This rapid growth in dApp usage recently has been driven by the rapid rise of decentralized finance, or DeFi.

This extreme popularity, however, comes at the cost of ever-increasing transaction fees, or gas prices as they are known in the world of Ethereum. Based on gas price data on etherscan.io, average gas prices have gone up by over 400% in the past few months. This means a simple token transfer using 21,000 gas could cost $0.5 on average, while a more complex transaction, such as using a decentralized exchange, could cost as much as $15-20!

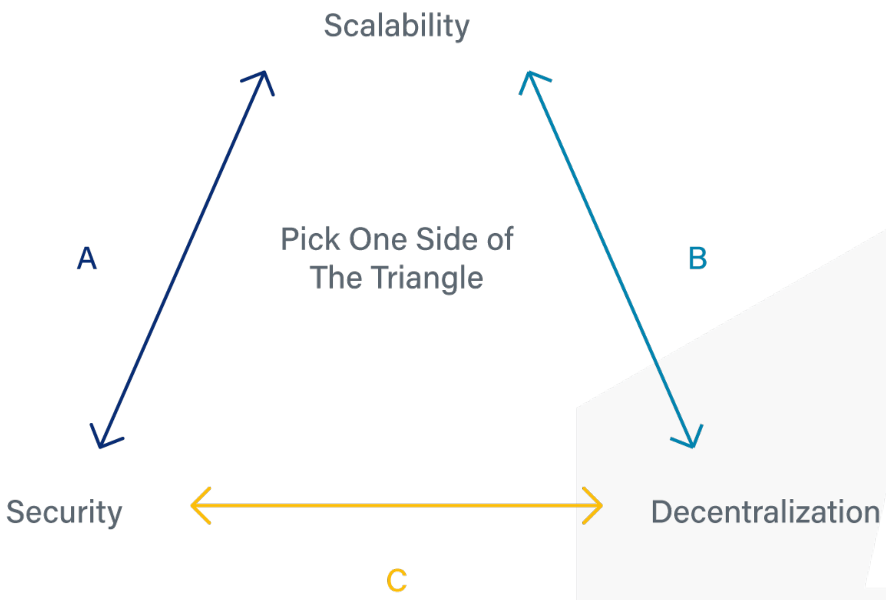
90-Day Rolling Average Gas Price (Gwei)



Source: Crypto.com Research

2.2 The Scalability Trilemma

Ethereum's founder Vitalik Buterin recognized this problem from early on. They noticed that there are severe tradeoffs when choosing between scalability, security, and decentralization, and where two can be satisfied, satisfying all three is very difficult. This concept is called the Scalability Trilemma (read more about blockchain scalability here). Ethereum 1.0 had security and decentralization as its main design axioms, and as a result, scalability was sacrificed.



Source: Crypto.com University

Note that the scalability trilemma is only an observation instead of a formal mathematical proof.

Decentralization

Decentralization refers to the degree of diversification in ownership, influence and value in the blockchain. Cryptocurrencies are in general “decentralized” since there is no single party that can govern the whole network. However, decentralization is more a spectrum instead of a binary “yes or no”, as we have seen different levels of decentralization in various projects like Bitcoin, Ethereum, Ripple, EOS, etc.

Security

Security refers to the level of defensibility blockchain has against attacks from external sources, as well as the resistance of the system to tampering. There are many attack vectors in a blockchain system, including double spending attack, sybil attack, DDoS attack and 51% attack, etc. In general, more freedom (i.e. free entrance / exit of the network) results in higher decentralization but lower security, since it is hard to verify the identity for the new participants where they can be owned by a single malicious entity or collude together to cause harm to the network.

Scalability

Scalability determines the capacity of the network including number of nodes in the network, the number of transactions that the network can process, how fast the network can process and so on. The term scalability is sometimes confusing because Bitcoin's blockchain is in fact scalable upon new participants joining the network. The PoW system will automatically adjust the difficulty and the network can tolerate any number of nodes that exist in the network.

3. ETH 2.0 Main Features

ETH 2.0 attempts to make Ethereum much more scalable and efficient while retaining or even improving its security and decentralization. Proof-of-stake will make the entire network more energy efficient and decentralized, while sharding will vastly improve scalability and throughput. In this section, we will describe the consensus algorithm behind ETH 2.0 as well as sharding.

3.1 Proof-of-Stake

In this section, we will describe the key differences between proof-of-work (PoW) and proof-of-stake (PoS), the two primary consensus algorithms used by cryptocurrencies. If you don't understand how consensus algorithms work, you can refer to our article on Blockchain consensus.

Consensus Algorithm	Consensus Mechanism	Opportunity Cost for Validators
Proof-of-Work	Solve computationally intensive cryptographic equations	Hardware and electricity costs
Proof-of-Stake	Validators propose and vote on transactions	Staked collateral

Proof-of-Work

PoW uses computationally intensive calculations and cryptography to ensure that only real transactions are validated, which is the algorithm behind Bitcoin and Ethereum 1.0. Since PoW requires expensive hardware and copious amount of electricity, miners are disincentivized from acting dishonestly and undermining the network, since these investments will be lost if they do so.

Every time a transaction is broadcasted to a PoW network, miners race to solve a cryptographic puzzle to generate a "hash," which can be used by other miners in the network to verify that the transaction is valid. Once a hash has been generated, the new block is added to the existing blockchain, and this update is distributed across the network, becoming part of the canonical ledger. The first miner to generate the hash receives rewards in the form of the blockchain's native cryptocurrency.

The cryptographic difficulty and ease of hash verification make it such that an attacker would have to control a significant portion of the computing power of the network in order to create fraudulent transactions – known as the "51% attack."

Proof-of-Stake

While PoW has been successful at securing the state of many blockchains, the computationally intensive nature makes it very energy inefficient and expensive to run. In fact, Vitalik Buterin stated in this blog post from 2014 that PoW essentially requires the burning of computational power on useless calculations to secure the network.

By forgoing the energy-intensive mining process, PoS is a much more energy efficient and environmentally friendly process than PoW. The staked collateral replaces the energy-intensive process as a disincentive to protect the network from attack. Because of the lack of energy consumption on the part of validators, the rewards do not need to be as high in PoS systems as in PoW.

PoS networks, on the other hand, relies on validators to stake large amount of assets on the network before they are able to partake in transaction validation and claim rewards for doing so. This collateral at risk makes it such that if a validator acts dishonestly, their assets can be taken away by the network. Instead of competing on speed and energy to generate a hash, validators in PoS systems compete on the amount of collateral staked.

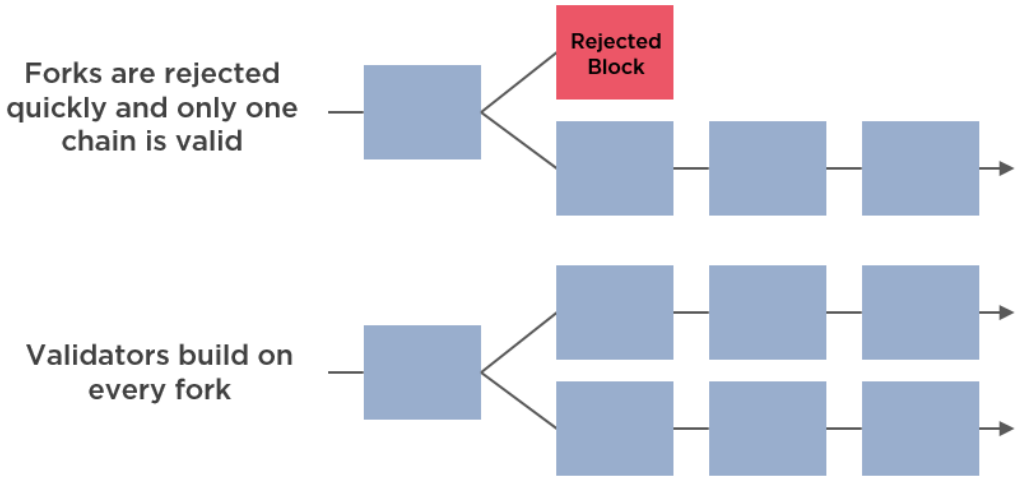
Subsequently, the economics in PoS systems must be well-designed to ensure that validator nodes are sufficiently incentivized to perform the work that secures the network. We will go over the economics of ETH 2.0 in the later section.

The “Nothing at Stake” Problem

Typically, only one block will be presented to validators at any time, so there will be no dispute over which block is valid. However, during times of high network traffic, multiple blocks may appear simultaneously.

As a result, it is in validators’ economic interests to participate in every fork, since they can earn rewards on whichever fork ends up winning. As a result, consensus could be difficult to build, leading the network vulnerable to double spend attacks. If you would like to read more about the “nothing at stake” problem, we have it prepared here.

The diagram below shows two scenarios. The first shows an ideal scenario of how the network handles forks, and the second shows how the network under the “nothing at stake” problem would proceed in case of a fork. As you can see, no consensus is reached and the network is in disarray since there are two valid forks proceeding simultaneously.



Source: Crypto.com Research

Casper, ETH 2.0’s implementation of PoS, eliminates the problem of “nothing at stake” by using a simple solution, to make the blockchain aware of other forks that are present, and which validators are voting on which blocks. If a validator is caught participating in more than one chain, that validator’s staked Ether will be slashed as a penalty.

Benefits of Proof-of-Stake

As alluded to above, there are a number of benefits to proof-of-stake over proof-of-work:

- **Energy efficient:** PoS systems do not require the consumption of large amount of electricity to secure the network.
- **Lower token inflation:** Because validators do not have to spend money on electricity, fewer new tokens need to be minted to reward validators.
- **Reduced centralization risks:** In proof-of-work, economies of scale make it such that miners with the biggest pool of mining hardware will win a disproportionate amount of rewards, which over time leads to centralization in mining pools.

  In proof-of-stake, however, rewards are distributed proportionally due to the nature of the voting system, which means that each validator's returns will be the same in percentage terms and no benefit can be gained by staking more.
- **Economic penalties for dishonest validators:** the network confiscates the collateral of attackers, while in PoW only energy is lost in attempting an attack. Vlad Zamfir, lead project manager of Casper, put it best when he said, "Imagine a version of the proof-of-work where if you participate in a 51% attack your mining hardware burns down".

Casper: Technical Details of PoS in ETH 2.0

For ETH 2.0, the proof-of-stake system is called "Casper." To begin with, time in ETH 2.0 is split into epochs and slots. Each slot is 12 seconds, and an epoch is 32 slots (6.4 minutes).

At the start of each epoch, the system randomly assigns each slot in that epoch to a randomly selected validator, who becomes the block proposer, and organizes validators into committees of 128 members at a minimum. The block proposer's role is to select a block to append to the existing blockchain in each slot, after which committees vote to append this to the main chain if the block is valid.

ETH 2.0 will have a minimum validator count of 16,384, who must each stake 32 ETH each. The reason for this number is to prevent committees from becoming corrupted by potential attackers. Even in a hypothetical scenario that an attacker controls one-third of all 16,384 validator nodes, there is a vanishingly low chance that the same attacker could control more than two-thirds of a randomly selected committee of 128 validators (this probability is around one in one trillion). In this way, the integrity of the overall network can be maintained.

Validators must also vote in a two-thirds majority to *finalize* blocks, after which nothing can be done to revert the chain to an earlier state.

3.2 Sharding

Currently, the Ethereum network can only process around 10 transactions per second, which is a severe limitation when network traffic is high, since transaction fees are also prohibitively high. The main reason for this low throughput is that every node must process every transaction. While this does improve the security and finality of the entire blockchain, it comes at the cost of speed.

Sharding is the scaling solution chosen by the Ethereum community as the best option to achieve long term and massively increased scalability, by removing the need for every node to verify every transaction. In the most basic form of sharding, the network is split into multiple blockchains that run separately, with each shard having its own set of validators and transaction history.

According to the most recent project specifications, ETH 2.0 will split the network into 64 shards, with each shard being able to handle as much traffic as the current Ethereum network.

Cross-Shard Communications

Although sharding improves network throughput, Ethereum will not achieve full functionality unless shards can communicate with one another. It would not be useful if each shard operated completely independently of other shards. This raises the question of how shards will communicate and transact with one another.

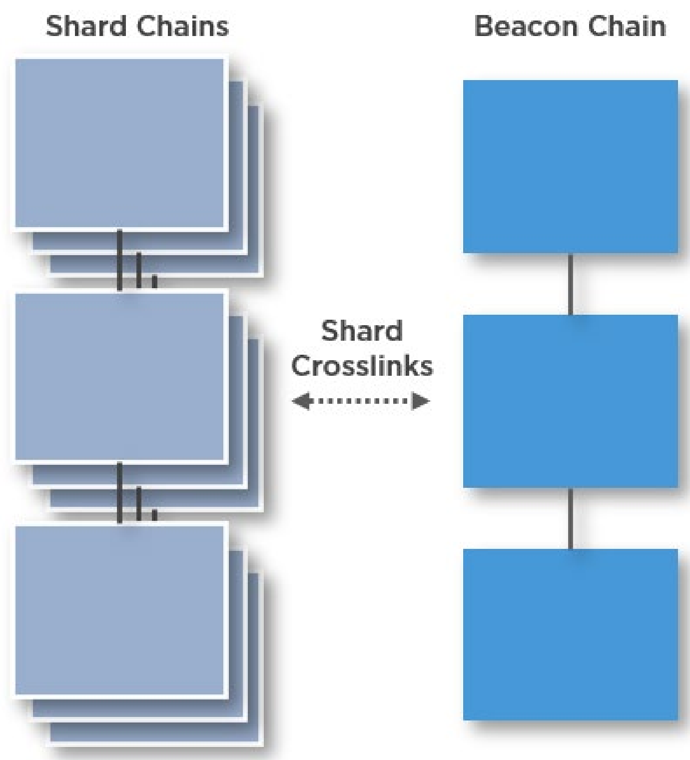
At Devcon 2018 in Prague, Ethereum co-founder Vitalik Buterin explained cross-shard communications in the following way:

> *“Imagine that Ethereum has been split into thousands of*

islands. Each island can do its own thing. Each of the islands has its own unique features and everyone belonging on that island i.e. the accounts, can interact with each other AND they can freely indulge in all its features. If they want to contact with other islands, they will have to use some sort of protocol."

At the center of the network will be the Beacon Chain, which is responsible for coordinating validator activities, and more importantly, to store information about state changes in all other shards.

A randomly selected committee of minimum 128 validators will be assigned to attest to each block in a shard chain. Once this happens, a crosslink can be formed and the Beacon Chain can then be updated about the status of shards. As blocks become finalized on the Beacon Chain, the corresponding shard blocks will also be finalized.



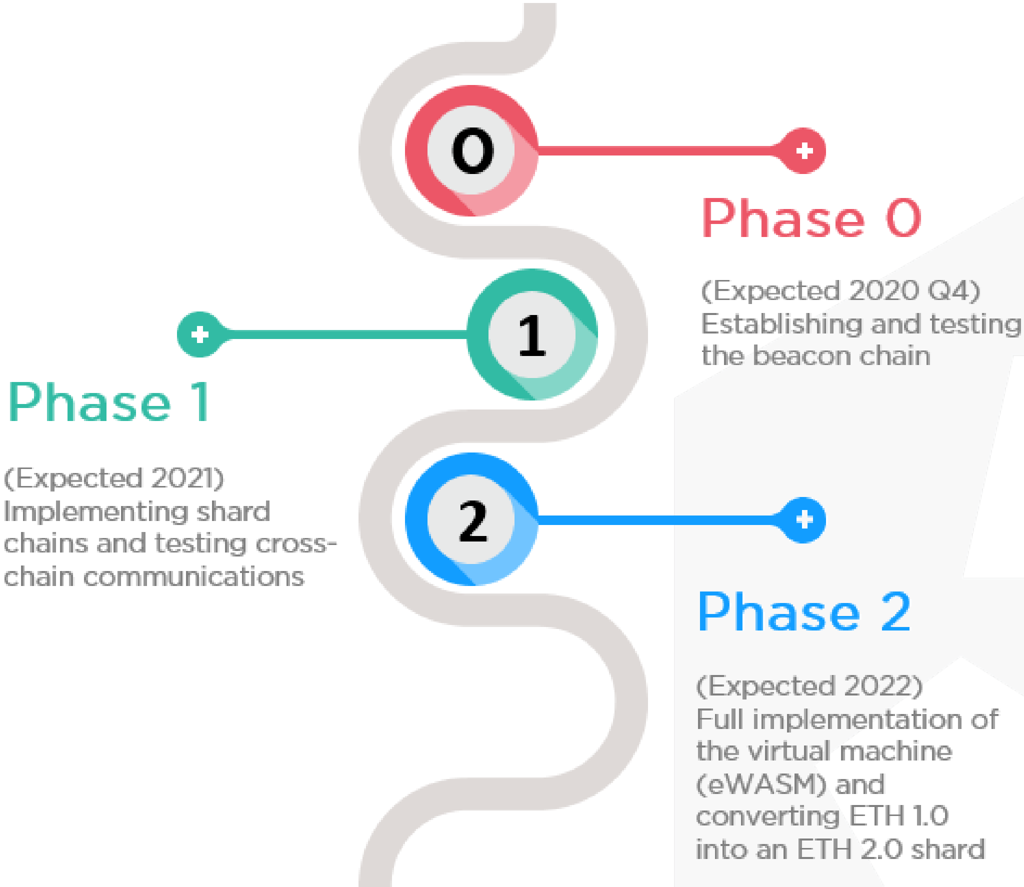
Source: Crypto.com Research

To learn more about sharding, you may also refer to our University article here.

3.3 Phases of Implementation

Although ETH 2.0 has launched its public testnet already, the fully functional version of Ethereum with dApp functionality and sharding won't be live right away. Instead, ETH 2.0 will be launched in phases, since replacing the widely used Ethereum blockchain is a complex process that must be managed carefully.

ETH 2.0 Schedule



Source: Crypto.com Research

Phase 0: Beacon Chain (Expected in December 2020)

Phase 0 will implement the Beacon Chain for ETH 2.0, which will serve as the central backbone of the entire network, managing proof-of-stake for itself and all of the shard chains.

The purposes of the Beacon Chain are as follows:

- Store information about validators and their stakes, while ensuring that all validators have a minimum 32 ETH staked
- Select block proposers for each shard in each slot
- Organize validators into committees to vote on the validity of proposed blocks
- **Distributing rewards and imposing penalties to validators.** The Beacon Chain is also responsible for monitoring the behavior of the validators. Rewards are given to the validators as an incentive for acting in line with the rules. On the other hand, malicious behaviors, such as voting on two chains at once, will lead to a penalty (slashing) where some of their staked collateral is deducted. In egregious cases, they can even get thrown out of the system entirely.
- **Establish the mechanism to determine finality and enable crosslinks between shards.** The current state of each shard is recorded in a Beacon Chain block as a crosslink. When the Beacon Chain block has been finalized, the corresponding shard block is considered finalized. The other shards can depend on it for cross-shard transactions.

In Phase 0, ETH 2.0 will not be able to support smart contracts and dApps. In fact, its only functionality will be to establish transfers of ETH from Ethereum 1.0 chain, and to test the proof-of-stake system is working as intended.

All Ether on the Beacon Chain in phase 0 will be shifted from a one-way transaction to a deposit contract living on the ETH 1.0 network. The deposit contract is watched by every validator on the network, who will submit the deposits to the Beacon Chain to update the list of validators.

Phase 1: Sharding (Expected in 2021)

After the Beacon Chain is established and deemed to be working as intended, Phase 1 will implement sharding. 64 shard chains will be established, and the Beacon Chain will begin organizing validators into committees to validate transactions on each separate shard in each slot and epoch.

Phase 1 is primarily concerned with testing the mechanisms of sharding, and will not deal with account balances. Instead, the Beacon Chain will treat shard chain blocks as simple collections of bits with no structure or meaning.

Phase 2: State Execution (Expected in 2022)

Until Phase 2, no smart contract functionality or dApps will be able to run on ETH 2.0. Phase 2 is when the functionality of the entire network will come together, allowing dApps to be deployed.

A new and upgraded virtual machine called Ethereum WebAssembly (eWASM) will also be introduced. eWASM is similar in functionality to today's Ethereum Virtual Machine (EVM) – it will be able to support account balances, smart contracts, and so on. One major upgrade anticipated with the eWASM is that developers will be able to deploy dApps coded in any programming language, not just Solidity.

4. ETH 2.0 Economics

Validators on ETH 2.0 will be rewarded for securing the network and validating transactions. How does one become a validator, and what kinds of returns should they expect?

4.1 Becoming a Validator

Anyone with 32 ETH can become a validator once Phase 0 is officially launched later this year. Currently, the latest testnet available for staking is the 'Medalla' testnet. Note that testnet Ether (gETH) has no value and is only for the purpose of testing the network.

Once Phase 0 is officially launched later this year, however, we expect that the process to becoming a validator will be very similar to the process that the existing testnets use.

Below, we will detail the process to become a validator using Prysm, one of the most popular ETH 2.0 clients. Another popular client is Lighthouse. Please note that these details pertain to the 'Medalla' testnet, and upon Phase 0 launch the procedure is subject to change.

Step 1: Install the Client

Follow the documentation for Prysm or Lighthouse to install the requisite client. Windows, Linux, MacOSX are supported.

Step 2: Get Ether (or testnet Ether)

Validators require at least 32 ETH in order to run a node on the network. For the Medalla testnet, you can request for gETH on the Medalla testnet through Prysm's Discord channel.

Step 3: Complete the Onboarding Process

Follow the directions in the ETH 2.0 launchpad to get your validator public/private keys and deposit your 32 ETH.

Step 4: Import Validator Accounts into Prysm/Lighthouse

Follow the respective client's directions (Prysm or Lighthouse) to import your validator accounts.

Step 5: Start Beacon Node and Validator Clients

Run the beacon node connected to the Medalla testnet. It will begin to sync with other nodes and will be ready for you to connect to it.

Step 6: Wait for Validator Assignment

Please note that it may take from 5-12 hours for nodes in the ETH2 network to process a deposit. In the meantime, leave both terminal windows open and running; once the node is activated by the ETH2 network, the validator will immediately begin receiving tasks and performing its responsibilities. If the chain has not yet started, it will be ready to start proposing blocks and signing votes as soon as the genesis time is reached.

To check on the status of your validator, we recommend checking out the popular block explorers: beaconcha.in by Bitfly and beaconscan.com by the Etherscan team.

4.2 Alternative Staking Arrangements

If running a validator node is not for you, because you are either not technically up to the challenge, or because you don't want to bother with the hassle, fear not! There are many service providers already lined up to help users with staking before the actual ETH 2.0 launch.

4.3 Staking Economics

The ETH 2.0 upgrade will bring switch from PoW to PoS. This means that instead of miners competing for a block reward, validators will be paid to perform assigned rules and secure the network. As a result, it is extremely important to strike a balance in validator incentives to ensure the security of the network.

If the incentive to stake is too low, the network will not reach the minimum number of validators needed to maintain cross-shard consensus. If the incentive is too high, the network is overpaying for security and inflating at a rate that is detrimental to the economics of the network and other token holders.

Staking Rewards

Rewards for ETH 2.0 validators will vary based on the amount of ETH staked at any point in time. If the ETH staked is low, the return rate per validator increases to incentivize additional validators to join the system. Similarly, as the amount of assets staked by validators increases, the rewards also decrease.

The schedule below shows the returns that can be earned by stakers at various validator pool sizes.

ETH validated	Max annual issuance	Max annual return rate
1,000,000	181,019	18.10%
3,000,000	313,534	10.45%
10,000,000	572,433	5.72%
30,000,000	991,483	3.30%
100,000,000	1,810,193	1.81%
134,217,728	2,097,152	1.56%

The numbers above can also be reduced by the following:

- Validators going offline will incur penalties to their rewards, and if 33% go offline at once, this leads to “finality leaking” (where block finality cannot be reached due to lack of a 2/3 supermajority) and additional penalties for offline validators are imposed.
- Validators getting stakes slashed due to malicious behavior.
- Transaction fees being burned due to EIP 1559, which aims to burn the majority of transaction fees in order to improve token economics and network fees for all users.

Staking Risks and Costs

In return for staking rewards, validators also bear some risks and costs:

Risk/Cost	Max annual issuance
Computing and Maintenance	Users will need to run a validator client and beacon node. This will require at least a Raspberry Pi 4, or a low specification PC. In addition to electricity costs, users will also have to bear the cost of broadband internet.
Capital Acquisition and Lockup	User will need to acquire and stake the 32 ETH in the deposit contract, which will be locked in Phase 0, until Phase 1 is launched.
Code Risk	There are risks of staking software failure or security vulnerabilities that can result in lost of funds
Security Risk	Users are responsible for the security of their validator clients. If their client is hacked due to a security failure, there is no way to recover funds.

5. Summary

In summary, ETH 2.0 in its completed form will implement a massively scalable blockchain network that is capable of running dApps at a much greater scale and lower transaction fees than the current Ethereum network.

Key Takeaways

- ETH 2.0 will implement two main features, Proof-of-Stake and Sharding, to improve the security and scalability of the network;
- Proof-of-Stake is a much more efficient and arguably fairer method to distribute transaction validation responsibilities and rewards versus Proof-of-Work, which disproportionately rewards large miners and consumes copious amount of energy on wasteful calculations to secure the network;
- Sharding, although complex, is one of the most promising methods to add scalability to a blockchain network and in tandem with layer 2 scaling solutions, which can increase scalability by a factor of hundreds, if not thousands;
- ETH 2.0 will be rolled out in three phases. Phase 0, to be released in December 2020, will only implement the Beacon Chain. Phase 1 will include sharding. It is not until Phase 2 in 2022 where dApp functionality will be enabled and Ethereum's dApps can be migrated over to ETH 2.0 shard chains;
- Validator returns can range from 2% to 20% depending on the number of validators participating in the network, but returns will likely be on the higher end at launch;
- Becoming a validator can be technically challenging, although third party service providers will provide staking services on day one;
- Being a validator to earn rewards can be attractive, but there are risks to consider – primarily, ETH staked will be locked up for at least one year, until the launch of Phase 1 in 2021.

6. References

Bitfly. (n.d.). *Open Source Ethereum 2.0 Beacon Chain Explorer.* Retrieved from https://beaconcha.in/

Das, R. (n.d.). *Ethereum 2.0-Beacon Chain Explained.* Retrieved from https://medium.com/coinmonks/ethereum-2-0-beacon-chain-explained-70287fc9901b

Das, R. (n.d.). *What to expect in Ethereum 2.0.* Medium. Retrieved from https://medium.com/coinmonks/what-to-expect-in-ethereum-2-0-779dfe970642

Ethereum Foundation. (n.d.). *Ethereum 2.0 Specs.* Github. Retrieved from https://github.com/ethereum/eth2.0-specs

Etherscan. (n.d.). *Beaconscan.* Retrieved from https://beaconscan.com/

EthHub. (n.d.). *Ethereum Roadmap*. Retrieved from https://docs.ethhub.io/ethereum-roadmap/ethereum-2.0/eth-2.0-phases/

Hoffman, D. (n.d.). *EIP 1559: The Final Puzzle-Piece to Ethereum's Monetary Policy.* Medium. Retrieved from https://medium.com/@TrustlessState/eip-1559-the-final-puzzle-piece-to-ethereums-monetary-policy-58802ab28a27

Kim, C. (n.d.). *Ethereum 2.0: How It Works and Why It Matters.* Coindesk Research. Retrieved from https://www.coindesk.com/research/reports/ethereum-2-0-how-it-works-and-why-it-matters

Lighthouse Book. (n.d.). Retrieved from https://lighthouse-book.sigmaprime.io/intro.html

Masnavi, S. (n.d.). *Ethereum 2.0: Medalla, the Final Public Testnet, Goes Live.* CryptoGlobe. Retrieved from https://www.cryptoglobe.com/latest/2020/08/ethereum-2-0-medalla-the-final-public-testnet-goes-live/

Prysmatic Labs, Inc. (n.d.). *Prysmatic Labs official documentation portal.* Retrieved from https://docs.prylabs.network/docs/getting-started/

Quantstamp Labs. (n.d.). *Understanding Phase 0, The Current Stage of ETH 2.0 Development.* Retrieved from https://quantstamp.com/blog/understanding-phase-0-the-current-stage-of-eth-2-0-development

Schwarz, C. (n.d.). *Ethereum 2.0: A Complete Guide. Casper and the Beacon Chain.* Medium. Retrieved from https://medium.com/chainsafe-systems/ethereum-2-0-a-complete-guide-casper-and-the-beacon-chain-be95129fc6c1 crypto.com

e. contact@crypto.com