Thursday, 4 June, 2020

The Bridge

Beacon chain: Conductor of the ETH 2.0 orchestra

Abstract

- *Beacon chain implementation aims to ensure that validators are playing by the rules while proposing the blocks in Proof of Stake design*
- *ETH 2.0 design aims to increase processing power by having multiple blockchains (shards) processing transactions parallelly. Beacon chain is crucial for communication among different shards*

Introduction

Ethereum 2.0, sometimes referred to as Serenity, is a major protocol upgrade for the Ethereum network. Ethereum has long been dogged by scalability issues. With every node required to verify and execute every transaction, problems arise when the system is overloaded. Ethereum has been using a Proof-of-Work (PoW) mechanism since its inception. However, the rollout of Ethereum 2.0 will cast this aside to make way for a new Proof-of-Stake (PoS) mechanism. Improvements in this rollout will pass through three major phases, and the beacon chain is fundamental to the process.

Phase 0

This is when the beacon chain will be implemented. Scheduled to be released on 30th June 2020, it will introduce the new PoS consensus mechanism, as well as store and manage the registry of validators[1].

Phase 1

This second phase will integrate shard chains (explained below), which will help improve Ethereum's scalability and is slated for 2021.

Phase 2

The third phase of Ethereum 2.0 is scheduled for 2022. It implements eWASM[2], a new and enhanced virtual machine.

A musical analogy aids understanding here. In Phase 0, the conductor (Beacon Chain) of an orchestra gets on stage. In phase 1, the instruments (Shard Chain), are arranged on the stage. Finally, in Phase 2, the musicians (transactions and smart contracts) come into play, bringing life to the orchestra. This article focuses on the beacon chain. However, to understand how it will facilitate migration to Ethereum 2.0, we first need to get to grips with sharding. This is because the beacon chain will manage the sharding system, not to mention managing and storing states of validators.

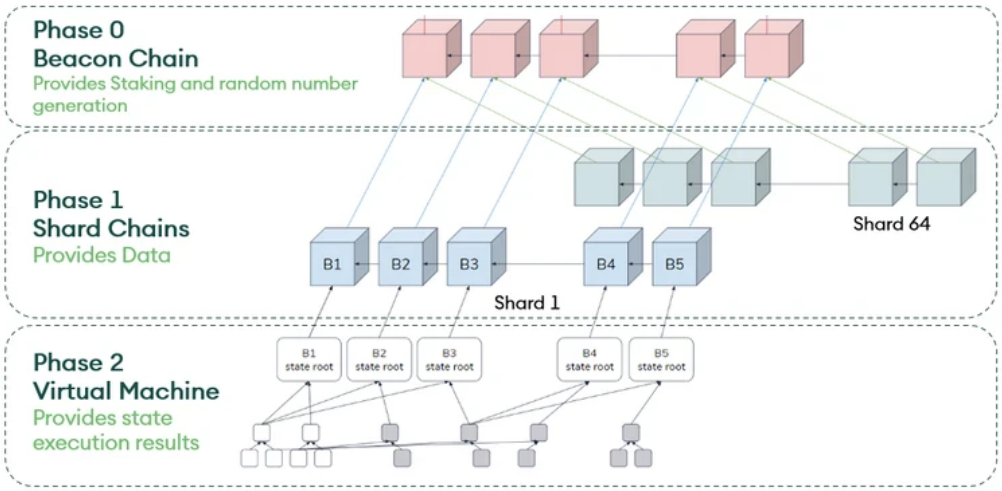
What is sharding?

Three key components comprise a blockchain system: decentralization, security, and scalability. Public blockchains are good at two out of the three parameters mentioned. This is known as the blockchain Trilemma. So far, Ethereum has been sufficiently secure[3] and decentralised but lacks desired scalability. Sharding is an attempt to improve this scalability shortfall.

The word sharding comes from taking a database and separating it into multiple logical databases that can still communicate with each other. Put simply, Ethereum takes this concept but applies it to its blockchain which is a form of a database. So, the Ethereum 2.0 blockchain will be split, like lots of mini databases, into 64[4] different shard chains. More may be deployed over time as the hardware scales. They all live separately but need the beacon chain to communicate with one another. As a result, transactions, data storage, and processing occur in parallel with each other, improving performance by a factor of the number of shards.

The figure below illustrates how sharding and PoS come together in a single design. The beacon chain manages the PoS protocol for itself, unifying all the 64 shard chains. That means at least 64 times the throughput of Ethereum 1.0, and more data by a factor of several hundred.

Figure 1: Ethereum 2.0 Architecture



Source: SEBA Research, Ethereum blog

Beacon Chain: Facilitating Ethereum 2.0 Migration

The migration involves two primary considerations, with the beacon chain crucial in the process - moving the ether (ETH) itself; and moving the state of the chain.

In Phase 0, Ethereum 1.0 users will be given the option to lock their ETH in a contract, with the same amount of new asset called Beacon ETH (BETH or ETH2) then credited to them on the beacon chain. Once completed, it can be staked on the Ethereum 2.0 chain to earn rewards. There will be a **one-way bridge** for the ETH migrating to Ethereum 2.0. That means it cannot be sent back.

During phase 0, ETH2 will be used only by validators on the beacon chain. The PoS blockchain gets funded ETH2 in two ways. The first way is by depositing ETH to a deposit contract (ETH1.X[5] contract) which burns the deposited ETH and mints the same amount of ETH2 on the beacon chain. The second way will be as a reward for validating the beacon chain (in Phase 0) and to validate shard chains (starting in Phase 1). Except for asset migration and asset creation, there are five key functions of beacon chain, all of which are pivotal to the success of the migration.

Beacon Chain's Major Functions

✔ *Crosslink Management*

The beacon chain processes crosslinks, which link together the entire sharded system. Crosslinks are a set of signatures from a committee[6] attesting to a block in a shard chain, which can be included in the beacon chain. Crosslinks serve as the primary way through which the beacon chain becomes aware of the shard chains' updated statuses. They also play an infrastructural role in cross-shard communication, which describes instances where a transaction needs to be shared between two or more shards.

✔ *Randomness provision*

When sharding a blockchain, the key challenge presented is security. Validators spread out across shards so that a single shard could not be taken over by a bad actor. This is partly achieved through validator shuffling, wherein a pseudo-randomly chosen committee of validators is assigned to each shard block. The beacon chain is responsible for providing this to the rest of the system, and this random shuffling makes it very unlikely for a shard to be attacked.

✔ *Validator management*

The beacon chain is required to maintain the set of nodes[7] that keep the Ethereum 2.0 network running. To join the beacon chain validator set, the ETH owner sends their staking amount (32 ETH) to a contract on the current PoW chain. Once the validity of the transfer has been checked, it can be detected by the beacon chain client[8]. When selected, the active validators take part by proposing blocks on the beacon chain. Note also that when the shard chains are implemented in Phase 1, the validators will be able to propose blocks on their respective shards.

✔ *Managing Committees*

Committees are formed by a randomly selected group of validators appointed by the network to validate the blocks on each shard. The committee's votes on which blocks represent the chain's actual history are crucial for maintaining security on the PoS blockchain. By counting votes (also known as attestations) from its committee, the beacon chain can confirm its history, otherwise known as finality[9].

✔ *Overseeing Rewards and Penalties*

The beacon chain will keep track of validator deposits, updating them too. If a validator fails to follow the rules, they are sanctioned through system removal and slashing[10]. The beacon chain also removes validators if their deposit dips under 16 ETH.

Conclusion

As is clear, the role played by the beacon chain in facilitating migration to Ethereum 2.0 will be thorough and pivotal. Not only does it serve as the basis for the new PoS mechanism, but it also will facilitate communication between the shard chains and crosslinks. Now, after years of effort, the much-heralded beacon chain is expected in the coming months. And with the conductor's baton in hand, it will just be a matter of time before the Ethereum 1.0 we know so well becomes just another shard among shards.

[1] Validators are people who stake on Ethereum's PoS network in return for rewards.

[2] The Ethereum WebAssembly (eWASM) will replace the current Ethereum Virtual Machine (EVM) and is a restricted subset of WASM that has been adapted just for the Ethereum network.

[3] As we have not observed any takeovers or rollbacks we can assume that it is sufficiently secure

[4] The number of shard chains Ethereum will support is still a discussion within the community. In our explanation we assume that there will be 64 shard chains, however this is subject to change.

[5] ETH1.X is a codename for all the Ethereum main net upgrades to be adopted in the upcoming months

[6] The network appoints a randomly selected group of validators to form a committee to validate blocks on each shard

[7] The network appoints a randomly selected group of validators to form a committee to validate blocks on each shard

[8] A beacon chain client is responsible for managing the state of the beacon chain, validator shuffling, and other tasks.

[9] Finality implies finalisation of all previous blocks, back to the genesis block mined in 2015

[10] If validators fail to follow the protocol, they will have their deposits “slashed” (confiscated)

Authors

Yves Longchamp
Head of Research
SEBA Bank AG

Ujjwal Mehra
Research Analyst
B&B Analytics Private Limited

Saurabh Deshpande
Research Analyst
B&B Analytics Private Limited

research@seba.swiss

Disclaimer

This document has been prepared by SEBA Bank AG ("SEBA") in Switzerland. SEBA is a Swiss bank and securities dealer with its head office and legal domicile in Switzerland. It is authorized and regulated by the Swiss Financial Market Supervisory Authority (FINMA). This document is published solely for information purposes; it is not an advertisement nor is it a solicitation or an offer to buy or sell any financial investment or to participate in any particular investment strategy. This document is for distribution only under such circumstances as may be permitted by applicable law. It is not directed to, or intended for distribution to or use by, any person or entity who is a citizen or resident of or located in any locality, state, country or other jurisdiction where such distribution, publication, availability or use would be contrary to law or regulation or would subject SEBA to any registration or licensing requirement within such jurisdiction.

No representation or warranty, either express or implied, is provided in relation to the accuracy, completeness or reliability of the information contained in this document, except with respect to information concerning SEBA. The information is not intended to be a complete statement or summary of the financial investments, markets or developments referred to in the document. SEBA does not undertake to update or keep current the information. Any statements contained in this document attributed to a third party represent SEBA's interpretation of the data, information and/or opinions provided by that third party either publicly or through a subscription service, and such use and interpretation have not been reviewed by the third party.

Any prices stated in this document are for information purposes only and do not represent valuations for individual investments. There is no representation that any transaction can or could have been effected at those prices, and any prices do not necessarily reflect SEBA's internal books and records or theoretical model-based valuations and may be based on certain assumptions. Different assumptions by SEBA or any other source may yield substantially different results.

Nothing in this document constitutes a representation that any investment strategy or investment is suitable or appropriate to an investor's individual circumstances or otherwise constitutes a personal recommendation. Investments involve risks, and investors should exercise prudence and their own judgment in making their investment decisions. Financial investments described in the document may not be eligible for sale in all jurisdictions or to certain categories of investors. Certain services and products are subject to legal restrictions and cannot be offered on an unrestricted basis to certain investors. Recipients are therefore asked to consult the restrictions relating to investments, products or services for further information. Furthermore, recipients may consult their legal/tax advisors should they require any clarifications. SEBA and any of its directors or employees may be entitled at any time to hold long or short positions in investments, carry out transactions involving relevant investments in the capacity of principal or agent, or provide any other services or have officers, who serve as directors, either to/for the issuer, the investment itself or to/for any company commercially or financially affiliated to such investment.

At any time, investment decisions (including whether to buy, sell or hold investments) made by SEBA and its employees may differ from or be contrary to the opinions expressed in SEBA research publications.

Some investments may not be readily realizable since the market is illiquid and therefore valuing the investment and identifying the risk to which you are exposed may be difficult to quantify. Investing in digital assets including cryptocurrencies as well as in futures and options is not suitable for every investor as there is a substantial risk of loss, and losses in excess of an initial investment may under certain circumstances occur. The value of any investment or income may go down as well as up, and investors may not get back the full amount invested. Past performance of an investment is no guarantee for its future performance. Additional information will be made available upon request. Some investments may be subject to sudden and large falls in value and on realization you may receive back less than you invested or may be required to pay more. Changes in foreign exchange rates may have an adverse effect on the price, value or income of an investment. Tax treatment depends on the individual circumstances and may be subject to change in the future.

SEBA does not provide legal or tax advice and makes no representations as to the tax treatment of assets or the investment returns thereon both in general or with reference to specific investor's circumstances and needs. We are of necessity unable to take into account the particular investment objectives, financial situation and needs of individual investors and we would recommend that you take financial and/or tax advice as to the implications (including tax) prior to investing. Neither SEBA nor any of its directors, employees or agents accepts any liability for any loss (including investment loss) or damage arising out of the use of all or any of the Information provided in the document.

This document may not be reproduced or copies circulated without prior authority of SEBA. Unless otherwise agreed in writing SEBA expressly prohibits the distribution and transfer of this document to third parties for any reason. SEBA accepts no liability whatsoever for any claims or lawsuits from any third parties arising from the use or distribution of this document.

Research will initiate, update and cease coverage solely at the discretion of SEBA. The information contained in this document is based on numerous assumptions. Different assumptions could result in materially different results. SEBA may use research input provided by analysts employed by its affiliate B&B Analytics Private Limited, Mumbai. The analyst(s) responsible for the preparation of this document may interact with trading desk personnel, sales personnel and other parties for the purpose of gathering, applying and interpreting market information The compensation of the analyst who prepared this document is determined exclusively by SEBA.

Austria: SEBA is not licensed to conduct banking and financial activities in Austria nor is SEBA supervised by the Austrian Financial Market Authority (Finanzmarktaufsicht), to which this document has not been submitted for approval. France: SEBA is not licensed to conduct banking and financial activities in France nor is SEBA supervised by French banking and financial authorities. Italy: SEBA is not licensed to conduct banking and financial activities in Italy nor is SEBA supervised by the Bank of Italy (Banca d'Italia) and the Italian Financial Markets Supervisory Authority (CONSOB - Commissione Nazionale per le Società e la Borsa), to which this document has not been submitted for approval. Germany: SEBA is not licensed to conduct banking and financial activities in Germany nor is SEBA supervised by the German Federal Financial Services Supervisory Authority (Bundesanstalt für Finanzdienstleistungsaufsicht), to which this document has not been submitted for approval. Hong-Kong: SEBA is not licensed to conduct banking and financial activities in Hong-Kong nor is SEBA supervised by banking and financial authorities in Hong-Kong, to which this document has not been submitted for approval. This document is not directed to, or intended for distribution to or use by, any person or entity who is a citizen or resident of or located in Hong-Kong where such distribution, publication, availability or use would be contrary to law or regulation or would subject SEBA to any registration or licensing requirement within such jurisdiction. This document is under no circumstances directed to, or intended for distribution, publication to or use by, persons who are not "professional investors" within the meaning of the Securities and Futures Ordinance (Chapter 571 of the Laws of Hong Kong) and any rules made thereunder (the "SFO"). Netherlands: This publication has been produced by SEBA, which is not authorised to provide regulated services in the Netherlands. Portugal: SEBA is not licensed to conduct banking and financial activities in Portugal nor is SEBA supervised by the Portuguese regulators Bank of Portugal "Banco de Portugal" and Portuguese Securities Exchange Commission "Comissao do Mercado de Valores Mobiliarios". Singapore: SEBA is not licensed to conduct banking and financial activities in SIngapore nor is SEBA supervised by banking and financial authorities in Singapore, to which this document has not been submitted for approval. This document was provided to you as a result of a request received by SEBA from you and/or persons entitled to make the request on your behalf. Should you have received the document erroneously, SEBA asks that you kindly destroy/delete it and inform SEBA immediately. This document is not directed to, or intended for distribution to or use by, any person or entity who is a citizen or resident of or located in Singapore where such distribution, publication, availability or use would be contrary to law or regulation or would subject SEBA to any registration or licensing requirement within such jurisdiction. This document is under no circumstances directed to, or intended for distribution, publication to or use by, persons who are not accredited investors, expert investors or institutional investors as defined in section 4A of the Securities and Futures Act (Cap. 289 of Singapore) ("SFA"). UK: This document has been prepared by SEBA Bank AG ("SEBA") in Switzerland. SEBA is a Swiss bank and securities dealer with its head office and legal domicile in Switzerland. It is authorized and regulated by the Swiss Financial Market Supervisory Authority (FINMA). This document is for your information only and is not intended as an offer, or a solicitation of an offer, to buy or sell any investment or other specific product.

SEBA is not an authorised person for purposes of the Financial Services and Markets Act (FSMA), and accordingly, any information if deemed a financial promotion is provided only to persons in the UK reasonably believed to be of a kind to whom promotions may be communicated by an unauthorised person pursuant to an exemption under the FSMA (Financial Promotion) Order 2005 (the "FPO"). Such persons include: (a) persons having professional experience in matters relating to investments ("Investment Professionals") and (b) high net worth bodies corporate, partnerships, unincorporated associations, trusts, etc. falling within Article 49 of the FPO ("High Net Worth Businesses"). High Net Worth Businesses include: (i) a corporation which has called-up share capital or net assets of at least £5 million or is a member of a group in which includes a company with called-up share capital or net assets of at least £5 million (but where the corporation has more than 20 shareholders or it is a subsidiary of a company with more than 20 shareholders, the £5 million share capital / net assets requirement is reduced to £500,000); (ii) a partnership or unincorporated association with net assets of at least £5 million and (iii) a trustee of a trust which has had gross assets (i.e. total assets held before deduction of any liabilities) of at least £10 million at any time within the year preceding the promotion. Any financial promotion information is available only to such persons, and persons of any other description in the UK may not rely on the information in it. Most of the protections provided by the UK regulatory system, and compensation under the UK Financial Services Compensation Scheme, will not be available.