January 31, 2023

Share

Web3's Next Narrative? – Things to Know About the Ethereum Shanghai Upgrade

BEOSIN
Blockchain Security
Web3's Next Narrative? – Things to Know About the Ethereum Shanghai Upgrade

The Ethereum Shanghai Upgrade, also known as the next new narrative of Web3 by many media, is currently one of the most discussed hotspots.

In March 2023, Ethereum will launch the expected Shanghai upgrade. As of press time, this upgrade mainly includes EIP-3540, EIP-3651, EIP-3670, EIP-3855, EIP-3860, EIP-4895, EIP-4200, EIP-4750 and EIP-5450, while the much-anticipated EIP- 4844 will be postponed to May-June for update.

In Ethereum ecosystem, we often hear the word "EIP", so what does this word mean?

EIP stands for Ethereum Improvement Proposal, which is the collective name for a set of standards and protocols that are recommended for use on the Ethereum platform. The specific standards and protocols it contains are related to the core protocols, client APIs, smart contract standards, etc. of Ethereum. Each EIP contains the definition of a certain standard or protocol.

Let's first understand a few of the standards that will be involved in the Ethereum Shanghai upgrade.

EIP-3540

This EIP is mainly an update for the EVM Object Format (EOF) contract bytecode, introducing an extensible and version-controlled container format for EVM. The separation of code and data is achieved by adding markers for code and data to the contract bytecode. This separation is particularly beneficial for on-chain code validators, which can distinguish between code and data. (Reference:

Related Project

Related Project S Score

Learn More

Guess you like

Beosin - Global rity Report 202

January 05, 2023

Blockchain Secu hly Recap of Ja

February 01, 2023

Beosin and Coi d Into A Strateg

February 01, 2023

A Recap of Beo NiFT Web3 Sec

February 02, 2023

Join the commun to discuss.

EIP-3651

The main purpose of the EIP is to change the "COINBASE" address from a cold address to a hot address. Currently, COINBASE direct transactions are becoming increasingly popular because they allow conditional payments, which provide benefits such as implicit cancellation of transactions. However, the price of access to COINBASE is too high because COINBASE was originally introduced in EIP-2929 under the access list framework to carry out gas calculations based on the cost of access to cold addresses, which is relatively high compared to the cost of access to hot addresses. (Reference: https://eips.ethereum.org/EIPS/eip-3651)

EIP-3670

This EIP mainly works with the above EIP-3540 contract creation when introducing code validation. Contract bytecodes containing truncated PUSH data or undefined instructions are rejected. (Reference: https://eips.ethereum.org/EIPS/eip-3670)

EIP-3855

This EIP mainly adds the PUSH0 instruction, which serves to press the constant 0 into the stack. Currently, there are only PUSH1-PUSH32 instructions that press 1 byte to 32 bytes into the stack, and pressing constant 0 into the stack requires the PUSH1 0 instruction, which consumes 3 gas in runtime and an additional 2 bytes of storage cost 2*200 gas. A constant 0 is currently pressed onto the stack, and the addition of the PUSH0 instruction saves a certain amount of gas. (Reference: https://eips.ethereum.org/EIPS/eip-3855)

EIP-3860

This EIP mainly modifies the maximum value of initcode. The current maximum value of initcode was set to MAX_CODE_SIZE: 24576 in EIP-170. In EIP-3860, the new maximum value of initcode is MAX_INITCODE_SIZE = 2 * MAX_CODE_SIZE = 49152. This doubles the maximum contract size and allows contracts to have richer functionality. However, the cost per byte of initcode will add 0.0625 gas, and the cost of deploying gas to the contract will increase slightly. (Reference: https://eips.ethereum.org/EIPS/eip-3860)

EIP-4895

This EIP is mainly for activating pledged withdrawals from the Ethereum beacon chain. (Reference: https://eips.ethereum.org/EIPS/eip-4895)

EIP-4200

increases the complexity of code analysis. The main benefits of these static instructions are reduced gas costs (at deployment and execution time) and better analysis properties. (Reference: https://eips.ethereum.org/EIPS/eip-4200)

EIP-4750

This EIP is primarily an optimization of code. It is mainly based on the above EOF format (EIP-3540) and introduces the ability to include multiple code segments in the bytecode, each representing a separate subroutine or function. Two new opcodes, CALLF and RETF, are introduced in the bytecode to be responsible for calling and returning such subroutines or functions. In addition, the EIP also introduces the JUMPF instruction to perform jumps to such subroutines or functions. (Reference: https://eips.ethereum.org/EIPS/eip-4750)

EIP-5450

This EIP mainly changes the validation process of the code and optimizes the network. While EVM currently performs a large number of validity checks for each executed instruction, such as overflow, gas sufficiency, etc., this EIP will enable contracts to perform the relevant validation at deployment time, thus reducing the number of such validations performed while the code is running. (Reference: https://eips.ethereum.org/EIPS/eip-5450)

Major Categories of the Shanghai Upgrade

1. EVM detail optimization

There are mainly two detailed improvements to the EIP: EIP-3651 and EIP-3860.

The EIP-3860 can alleviate the problem that some complex contracts have to be split into multiple contracts before they can be deployed to the mainnet due to the byte code length limitation of smart contracts, and the introduction of this EIP will significantly increase the richness and diversity of smart contract functions.

2. Withdrawal from beacon chain

It is mainly realized through EIP-4895.

At present, the number of ETH staked on the beacon chain is over 15 million, accounting for nearly 13% of the total amount of Ethereum in circulation.

validator_index (validator data), address (withdrawal target address) and amount (number of ETHs), which will be actively pushed to the execution layer. A new field withdrawals will also be defined in the execution layer, which holds a list of withdrawal objects that will be added to the list of withdrawals after the execution load gets a withdrawal object. After verification, then the number of amounts of Ethereum will be added to the addres, so as to achieve the withdrawal of Ether.

3. Bytecode improvements

There are six main bytecode-related improvements to EIP, namely: EIP-3540, EIP-3670, EIP-3855, EIP-4200, EIP-4750 and EIP-5450.

This type of upgrade mainly adds some new bytecode instructions, including: PUSH0, RJUMP, RJUMPI, RJUMPV, CALLF, RETF, JUMPF. It also classifies bytecodes, adds bytecode markers for distinguishing bytecode types, and modularizes bytecodes of each type. On the other hand, the validation mechanism of bytecode has been updated, and the network and usage cost have been optimized.

This part of the upgrade is the main part of the Shanghai upgrade, which will have a relatively large impact on the Ethereum virtual machine system.

Beosin will include all the instructions in this Shanghai upgrade into Beosin VaaS - the smart contract formal verification tool.

What is the Ethereum Scalable Solution?

On the other hand, the much-anticipated EIP-4844 has been postponed to May-June this year, featuring the introduction of a new transaction format of "blob-carrying transactions", a data type specifically designed for L2 data transfers.

Rollups are a scale-out solution that is the only de-trusted scale-out solution for Ethereum in the short, medium and possibly long term. In recent months, the cost of transferring data from L2 to L1 has been high, and Rollups have clearly reduced the transaction costs for many Ethereum users, with Optimism and Arbitrum having 3-8x lower costs than the Ethereum base layer itself. ZK rollups even have features that cost 40-100 times less than the Ethereum base layer.

However, even these fees are too expensive for many users. In the long run, data sharding is a good solution to rollups' own shortcomings, adding 16MB of dedicated data space to each block of a chain using rollups. However, the implementation and deployment of the data sharding feature will take a long time to achieve.

The EIP provides a solution by implementing a new transaction type, "blob-carrying transactions", which is designed to host the original transaction compression data of L2, equivalent to the previous calldata. The calldata does not actually need to be executed by L1 to incur gas charges. The new transaction type blob will not be read by EVM like calldata, but will remain in the consensus layer and be deleted after a 30-day delay. In simple terms, the previous calldata data is kept in the consensus layer and not sent to the execution layer as before, thus incurring high gas fees, which is why Rollup fees can be reduced. (For more information: https://eips.ethereum.org/EIPS/eip-4844)

If you have need any blockchain security services, please contact us:

Website **Official Twitter** **Alert** **Telegram** **LinkedIn**

Stay up-to-date on our latest offerings, tools, and the world of blockchain security.

Contact@beosin.com

Resources

- Security Incident
- Research Report
- Event Update
- Partnership Announcement
- Resources

Company

- About Us
- Terms and Conditions
- Privacy Policy
- Channel Verification

Product&Service

- EagleEye
- KYT
- VaaS
- Malicious Websites Identification
- Smart Contract Audit
- Blockchain Security Audit
- Cryptocurrency Tracing

Solution

- Compliance
- Smart Contract Security

Socials

- Beosin Twitt
- Beosin Alert
- Telegram
- Linkedin
- Medium
- Discord