Abstract :Ethereum is one of the most important part of blockchain technology ,the core of it is smart contracts.In the recent years ,Ethereum's smart contract ecosystem has experienced several major security events in its development, exposing vulnerabilities and design flaws in smart contracts, and driving improvements in contract development and management.We propose to find a new technology to reduce vulnerabilities in smart contracts and decreases the risk of incurring losses

Ethereum is an open source public blockchain platform with smart contract functions. In essence, Ethereum is a public database that keeps permanent records of digital transactions. The operation of Ethereum is based on blockchain technology, a decentralized and decentralized distributed ledger technology[1], which consists of a series of chronological data blocks, each containing a certain number of transaction records and the hash value of the previous data block to form a chain structure . This chain structure makes data impossible to tamper with, not changed or deleted if it is added to the blockchain.

Compared with the bitcoin,working principle of Ethereum is similar, but the function of Ethereum is more flexible in the Ethereum work process. At first, Users send transactions or deploy smart contracts via their wallets, then Transactions and smart contracts are validated by the nodes in the network and executed in the Ethereum Virtual Machine (EVM), verify the execution of the smart contract.The validated transaction and contract results are packaged into blocks and added to the blockchain[2].

Ethereum allows developers to write smart contracts and deploy them on the blockchain. Arguably we can say smart contracts are essentially a core component of Ethereum. Smart contract use programming language to convert the contract terms into a program that can be run . After the smart contract program starts to be executed on the blockchain, it will leave permanent records on the blockchain, and the records cannot be tampered with.Which makes the transaction process transparent and open, ensuring the legality of the contract execution.The encrypted execution of smart contracts in Ethereum relies on the Ethereum Virtual Machine (EVM)[3]. The EVM is the core of the Ethereum network and is responsible for executing the smart contract code. All nodes will run the EVM and verify the execution results of the contract. This distributed execution method ensures the reliability and security of smart contracts, as any tampering with the contract will be discovered and rejected by other nodes. Smart contracts do not need third-party intermediaries. When certain conditions are met, they operate automatically and execute completely in accordance with the programs written in the Solidity language, which can prevent fraud and third-party interference. Thus, transaction costs and risks can be reduced[4].

Hash functions play an important role in Ether, where transactions and blocks are encrypted and verified using hash algorithms.Hash function is an algorithm that creates a fixed-length and unique hash value from a message of arbitrary length.Hash algorithm has three characteristics: uniqueness (collision resistance), unidirectional performance, and avalanche effect.Uniqueness means that the hash value of any information is unique and the same hash values do not appear.Unidirectional performance means that it is extremely difficult to launch the original information according to the hash value to ensure the security of the information.The avalanche effect means that the hash value changes dramatically even if the information changes minimally[5].

Currently, two hash algorithms are mainly used in Ethereum:SHA-256 and Keccak-256,to ensure the security of digital currency production[5]. The SHA-256 algorithm inputs the data and goes through a series of complex logical and mathematical operations to eventually output a 256-bit hash value.In Ethereum, the more widely used is Keccak-256.Keccak-256 is an encryption function that is part of the SHA-3 series.It uses a unique sponge structure and consist of an absorption phase and a squeezing phase. In the absorption phase, the input message is divided into chunks and processed by a substitution function; in the squeezing phase, the output is extracted from the state by repeatedly applying the same substitution function[6]. The Keccak-256 is widely used in Ethereum, including address generation, smart contracts, mining, and blockchain security.In address generation, the user's wallet address is generated by hash processing of its public key using Keccak-256.In smart contracts, Keccak-256 is used to validate digital signatures, generate random numbers, and ensure the integrity of the data.In mining, Keccak-256 is used in Ethereum's proof of Workload (PoW) algorithm, where miners need to solve a complex mathematical problem involving Keccak-256 hash operations to compete for accounting rights[7].

Although Ethereum is one of the main forces of blockchain technology, with the continuous development of blockchain technology and the continuous upgrading of user needs, Ethereum is still facing technical bottlenecks, mainly reflected in the following aspects:

1. Restricted extensibility

throughput bottleneck: The Ethereum network has a limited throughput, i. e., a limited number of transactions that can be processed in a unit of time.This results in periods of high demand, such as the NFT boom and the rise of DeFi apps, where networks are prone to congestion, surging transaction costs, and declining user experience[8].

Delay bottleneck:Delay is the time elapsed from submitting the transaction to the time when the transaction is confirmed and included in the blockchain.The delay problem of the Ethereum network also affects its scalability.Longer confirmation time and blockchain synchronization time increase the waiting time for transactions and reduce the efficiency of the network[9].

1. Smart contract security:

Smart contracts are one of the core features of Ethereum that allows users to execute automated contracts on the blockchain.However, the security issue of smart contracts is also one of the technical bottlenecks facing Ethereum.Since the code of smart contracts is difficult to modify once deployed, any security breach can lead to serious consequences, such as fund theft and data leakage.In addition, the complexity of smart contracts also increases the risk of security vulnerabilities.

1. Consensus mechanism:

Ethereum currently uses a consensus agreement of proof of work (Proof of Work, PoW) and proof of equity (Proof of Stake, PoS), but it is still mainly PoW. This consensus protocol has a high guarantee of security, but there are also some problems.For example,the PoW consensus agreement could lead to network congestion and higher transaction costs.It also requires a lot of computing resources and power consumption, which is detrimental to environmental protection and sustainable development.

1. Privacy:

Ethereum's transaction data is open and transparent, which helps to increase the transparency and traceability of transactions.However,it also raise the risk of privacy leakage.Some sensitive information, such as user identity, transaction amount, and so on, may be used by malicious attackers for illegal activities.

For the current defects of Ethereum, there are three directions that can be used as future breakthrough points:

1. The Proof of Interest (PoS) mechanism：

We can turn proof of work (PoW) to proof of equity (PoS),to reduce energy consumption and increase transaction speed.However, how to ensure that the network remains highly security and operates steady under the PoS mechanism and keep the degree of decentralization of the network,it still needs to be supported by newer technological breakthroughs[10].

1. Blockchain sharding technology:

In order to improve the throughput and scalability of the Ethereum network, we can try sharding technology which divide the blockchain network into multiple smaller parts.Each parts of blockchains can deal with transactions and store datas independently .But it will face a lot of problem to realize the sharding technology ,such as how to ensure that the communication and datas are identical between parts[11].

1. Layer 2：

Layer 2 solutions are an additional network layer built on top of the main Ethernet network,in order to deal with more transactions and reduce the burden of the main net.We can improve the scalability and performance of Ethereum by optimize the transaction processing process and improve the transaction efficiency[12].

REFERENCES

1. Yueyue DAI,Ke ZHANG,Yan ZHANG. Blockchain empowered 6G[J]. Chinese Journal on Internet of Things, 2020, 4(1): 111-120.
2. The Basic Concepts and Workings of Ethernet

<https://blog.csdn.net/weixin_39372311/article/details/141484391>

1. What is Ethereum Virtual Machine (EVM) in Blockchain?

<https://medium.com/@orderlynetwork/what-is-ethereum-virtual-machine-evm-in-blockchain-e7db57167bea>

1. What are Smart Contracts? Applications of Smart Contracts[inoutcode/ethereum\_book](https://github.com/inoutcode/ethereum_book) <https://blog.csdn.net/tyxjolin/article/details/129823905>
2. The Wonderful Use of Hash Algorithms in Ethernet

<https://learnblockchain.cn/article/867>

1. What is Keccak256? Exploring the Cryptographic Hash Function and Its Use in Cryptocurrencies<https://www.nervos.org/knowledge-base/what_is_keccak256_(explainCKBot)>
2. Data Structures and Algorithms Used in Ethernet - Hash Functions - keccak256<https://blog.csdn.net/qq_28053637/article/details/136571740>
3. The current dilemma facing Ether (ETH)<https://baijiahao.baidu.com/s?id=1808738261085987198>
4. Ethernet's scalability crisis: exploring bottlenecks in the execution layer<https://blog.csdn.net/feeltouch/article/details/140633326>
5. What is Proof of Stake (PoS)<https://m.163.com/dy/article/HARV5O9105535G1Y.html>
6. Ethereum sharding technology<https://zhuanlan.zhihu.com/p/37991389>
7. Ethernet Layer 2 at a glance<https://www.chinaz.com/2024/0520/1617722.shtml>