

■
NEC IS A LAYER-2 ON-CHAIN AGGREGATOR BASED
ON THE CORE CONCEPT OF ETHEREUM
EXPANSION. IT IS COMMITTED TO BUILDING A
MODULAR, UNIVERSAL, AND HIGHLY FLEXIBLE
EXPANSION FRAMEWORK FOR ETHEREUM.

NiEW WHITE PAPER



NiEW
ERA

2021 EXPANSION
FRAMEWORK

CATALOGUE

01 Abstract 01

02 Nomenclature 06

Decentralized application (= DApp)

DAO

Digital identity (digital identity)

Web3

Transaction fee (transaction fee)

Light client (light client)

solidity

EVM

A Distributed Hash Table, DHT)

Workload proof (proof-of-work)

Proof of rights and interests (proof-of-stake)

Consensus (consensus)

Sharding (sharding)

Protocol (protocol)

Merkle Patricia tree

03	Project background	12
	The Birth of the Next Generation Internet: Web 3.0	
	Challenges faced by Ethereum	
	The Layer-2 solution	
04	Project introduction	15
	Introduction to NEC	
	Core advantage	
	Think tank team	
05	Ecological governance model	18
	Comprehensive application ecology of expansion and aggregation	
	Decentralized governance (DAO)	
	Decentralized ecological management system	
06	Ecological application	22
	New financial payment system	
	DeFi (decentralized finance)	
	Community currency	
	Blockchain game	
	Electronic voting	
	NFT casting	
	NEC wallet	

07	Technical architecture	32
	Under-chain verification of NEC	
	SPOR point-to-point encrypted storage	
	Design of data governance structure	
	I/O streaming protocol (GSIOP)	
08	Extension & Agreement	37
	NEC Assets Cross-chain Bridge	
	Save	
	Consensus	
	Without leadership	
	Asynchronous	
	Byzantine fault tolerance	
	Network security hypothesis	
09	Token allocation	38
10	Appendix	42
	Risk warning	
	disclaimer	

ABSTRACT

Today's Internet is stateless-participants can't keep their own status, and can't transfer their status between each other in a native way. The blockchain technology pioneered by Bitcoin provides us with a way to preserve state in a digital native way. In the ecosystem of cryptology currency and blockchain, This new basic ability has been given the title of Web 3.0. Ethereum is currently the second largest network in the world, and its market value has exceeded 40 billion US dollars. Ethereum aims to become a global distributed network for implementing point-to-point contracts. In other words, Ethereum is a "global computer that cannot be stopped". In 2020 and early 2021, The actual use cases of Ethereum ecosystem have exploded, and the problem of Ethereum expansion has become increasingly prominent. The utility of blockchain network carrying DAPPs and DeFi platform needs to be expanded and implemented to maintain. Every operation of Ethereum needs to be handled by most nodes to reach a consensus on the chain, which leads to the low throughput of the current blockchain.0 has been difficult to meet the use and development needs of users. On December 1, 2020, Ethereum started the online mileage of 2.0. The new roadmap of Ethereum 2.0 is the framework of "executable PoS beacon chain+data fragmentation +Layer2". In order to realize thousands of times of throughput brought by Ethereum ahead of time, Layer 2 will push Ethereum 2.0 into use. With the launching milestone of Ethereum 2.0, Numerous protocols will be officially launched, and Layer2 is making up the last piece of puzzle for the popularization of Ethereum web3 technology paradigm, making it possible for web3 and traditional web2 technology to compete on the same platform.

NEC(New Era) is a Layer-2 chain aggregator based on the core concept of Ethereum expansion, which does not affect decentralization and utilizes the existing developer community and ecosystem. It is an offline/side chain extension solution for existing platforms, which can provide scalability and excellent user experience for DApp/ user functions.

NOMENCLATURE

Decentralized application (= DApp)

Services that operate out of centralized trust institutions. An application that allows end users/resources to interact, reach agreements, or exchange information directly without the middleman.

DAO

Decentralized autonomous organizations. DAO is a type of contract (or a set of contracts) in the block-chain, which can make rules, enforce or automate some organization-level work including organization management, fund raising, practical operation, expenses and expansion.

Digital identity (digital identity)

A group of transactions signed with the same public key that can be verified defines the behavior of digital identity. In many real scenes (such as voting), it is hoped that the digital identity can be consistent with the real identity. How to ensure this non-violence is still an unsolved problem.

Web3

The exact definition of Web3 is still being discussed, but it generally refers to the network composed of various connectable devices, decentralized services and applications, logical storage of online information and artificial intelligence applications.

Transaction fee (transaction fee)

That is, gas cost, is the amount of etheric currency that needs to be paid to miners in order to execute your transaction.

Light client (light client)

It allows users to execute and check transaction execution in a low-capacity environment without running a client program of Geth.

solidity

Solidity is a high-level development language with syntax rules close to Javascript. It is designed to compile the code of Ethereum virtual machine.

EVM

Ethereum Virtual Machine, which is the decentralized core computing platform of Ethereum platform.

A Distributed Hash Table, DHT)

Distributed hash table is a decentralized distributed system, which can provide lookup services similar to hash table functions. DHT stores key and value pairs, and any node in the network can get the corresponding value efficiently through a specific key.

Workload proof (proof-of-work)

A mathematical value that can prove that a computational problem that consumes resources and time has been solved. Generally, it appears in the abbreviation "PoW".

Proof of rights and interests (proof-of-stake)

An alternative method of mining operation requires miners to prove that they have a certain amount of network currency by answering questions. This is based on the principle that miners should not try to destroy a network in which they have interests. Proof of rights and interests generally appears in the abbreviation "PoS". Compared with PoW, PoS can reduce the waste of computing power, But it can also provide extra security for the network.

Consensus (consensus)

Refers to the unanimous approval of all nodes in the network about the status of Ethereum network.

Sharding (sharding)

The process of dividing the space of possible accounts (contracts also belong to accounts) into subspaces, such as the first digit of their digital addresses. This enables contracts to be executed on 'chips' instead of the whole network, thus making transactions completed faster and providing a stronger scalability.

Protocol (protocol)

A standard used to define the method of exchanging data over a computer network.

Merkle Patricia tree

Merkle Patricia tree provides a cryptographic verification data structure, which can store all (key, value) bindings. They are completely predictable, that is, Patricia tree with the same (key, value) binding will ensure that all bytes under it are the same, so there will be the same root hash. It provides $O(\log(n))$ complexity for inserting, searching and deleting, and it is easier to understand and implement with coding than a more complex alternative based on comparison, such as red-black tree.

PROJECT BACKGROUND

The Birth of the Next Generation Internet: Web 3.0

On the 50th anniversary of the birth of the Internet, Tim Berners Lee, the inventor of the world wide web, is worried about the future of the Internet. He raised the issue of increasing centralization. This power imbalance violates the original design principles of the Internet, because the design principle of the Internet is to achieve the goal of information decentralization. In recent years, technology giants, including Facebook and Google, have overturned the original design principles of the Internet, enveloping data on closed platforms. The value of the whole ecosystem of Web 2.0 is more based on the company and platform based on the protocol. Participants can't keep their own state, nor can they transfer their state to each other in a native way. Only 7% of the generated data is actually stored. And over time, the proportion is still declining and is expected to drop to 5% in the next five years. However, the current cloud storage infrastructure is still proving unable to keep up.

Blockchain technology pioneered by bitcoin provides us with a way to preserve state in a digital native way. In the ecosystem of cryptocurrency and blockchain, this new basic capability has been given the title of Web 3.0. The vision of Web 3.0 is to make all applications, data and use cases of the Internet fully verifiable. Increasing the ability to verify means that a centralized intermediary, such as a bank or a large technology company, who controls your money or your data, can ask them to back up that data and prove that their actions on that data are accurate. With the development of related infrastructure, developers all over the world will develop products and start businesses on Web 3.0, turning an open financial system from a vision to a reality.

Challenges faced by Ethereum

Ethereum is now the world's second largest network, with a market value of over \$40 billion. Ethereum aims to become a globally distributed network for the execution of point-to-point contracts. In other words, Ethereum is the "unstoppable global computer." More importantly, Ethereum has become the most widely used blockchain protocol in the world, settling more than \$6 billion a day. Ethereum is more than just a cryptocurrency. It is a "world computer" and the "value layer" of the Internet. It allows people to develop apps and products using "currency" written in code. If Web3 continues to grow, Ethereum will become a new settlement layer of the Internet, all types of transactions, whether it happens on Ethereum or another blockchain, or even visa, it will turn to Ethereum to exchange funds and keep safe and unforgeable records.

In 2020 and early 2021, the actual use cases of the Ethereum ecosystem have exploded. Analyst James Wang highlighted Ethereum's progress this year in his article [Ethereum announcements first quarter 2021 results](#)

INDEX	2020 Q1	2021 Q1	YEAR-ON-YEAR GROWTH
TRANSACTION VOLUME (US\$ BILLION)	\$33	\$713	2,065%
TRANSACTION FEES (MILLIONS OF DOLLARS)	\$8	\$1,699	20,158%
AVERAGE TRANSACTION FEE (USD)	\$0.06	\$7.63	12,617%
DAILY ACTIVE ADDRESSES (DRY)	354	607	71%
ETH PLEDGE AMOUNT (MILLION ETH)	0	3.6	-
DEX TRADING VOLUME (US\$ BILLION)	\$2.3	\$177.0	7,596%
TOTAL VALUE OF DEFI LOCK-UP (US\$ BILLION)	\$0.8	\$52	6,400%
STABLECOIN TRADING VOLUME (US\$ BILLION)	\$7.1	\$41.9	488%
WRAPPED BTC (BTC)	1,777	170,024	9,468%
NFT ART SALES (MILLION DOLLARS)	\$0.7	\$396	56,163%
ETH SUPPLY (MILLION)	110.3	115.3	5%

Figure 1: James Wang, Ethereum announcements first quarter 2021 results

From May 1 to May 22, the two largest Ethereum DEX, uniswap and sushiswap alone, handled \$78 billion in transactions.

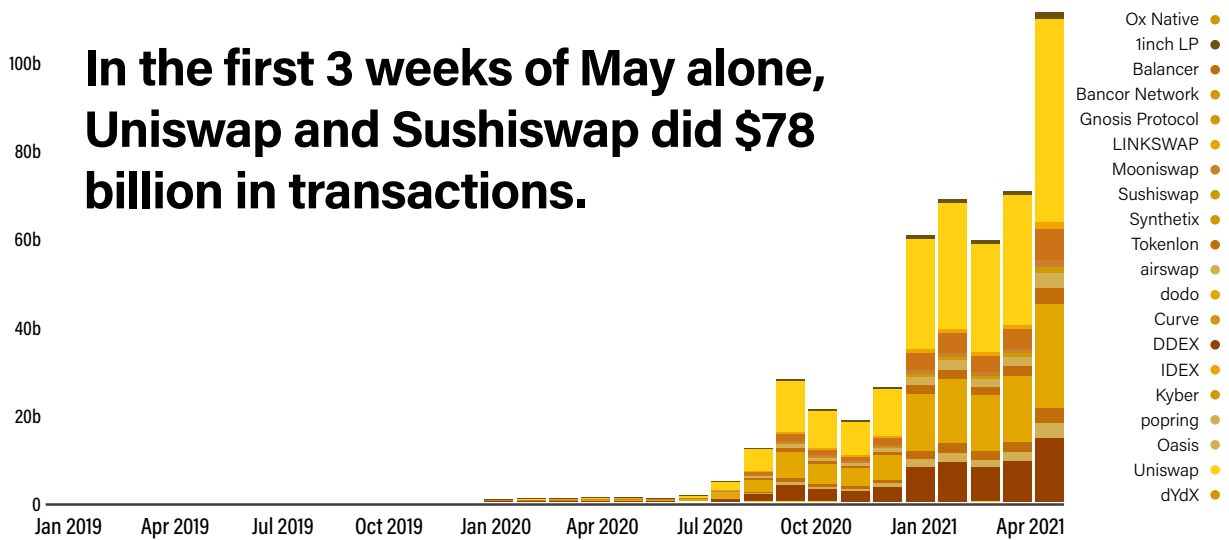


Figure 2: the growth trend of Ethereum's defi applications since 2021

With the increasing demand of dApps based on Ethereum, there are more DeFi, more NFTs, more DAOs and more games. At present, when the Ethernet network is busy, the transaction speed will be affected, which makes the user experience of some types of Dapps very poor. As the network becomes busy, the price of Gas is also rising, because transaction senders bid against each other. This makes it very expensive to use Ethereum. Every operation in Ethernet workshop (transfer, NFT casting, ERC-20 contract generation) must be performed by every node in the network. This sets a basic limit on the transaction throughput of Ethereum: it cannot be higher than the speed of data obtained from a single node.

The current Ethereum system has the following challenges:

Slow transaction speed: For some use cases (such as blockchain games), the current transaction processing time is not feasible. Currently, the Ethereum blockchain processes about 19 transactions per

second. By contrast, Visa handles about 1,700 transactions.

Transaction cost is high: using decentralized application based on blockchain (dapps) becomes very expensive. At present, a simple transaction requires about \$5 in Gas fee. The article "The Great Online Game" written by Jack Butcher is cast into an NFT, and its casting and auction cost nearly \$1,000.

High energy consumption: Mining based on POW consensus needs a lot of electricity.

Ethereum Ecology needs a solution that can handle more transactions without increasing the load of a single node.

The Layer-2 solution

Any improvement to scalability should not be at the expense of security and decentralization. The transaction that should have been processed on the main chain of Ethereum, namely Layer 1 (L1), should be transferred to Layer 2 (L2) for processing, and then the result should be sent back to L1 for confirmation from L2. This solution is called Ethereum Layer 2. The Layer 2 solution on Ethereum is designed to help applications expand by processing transactions under the Layer 1 chain. Layer 1 is the basic consensus layer of standards. At present, thousands of transactions are settled at this layer. The scalability scheme built on Ethereum without any modification to the underlying Layer 1 protocol is called Layer 2 scheme. These schemes can handle transactions without interacting with the Ethereum network, and anchor their security on Layer 1 of Ethereum through intelligent contracts. Multiple Layer 2 schemes can be run on Ethereum without everyone upgrading the underlying infrastructure. Compared with Layer 1, it can improve throughput, reduce costs and improve user experience. At present, Ethereum can only process about 15 transactions per second on its Layer 1, while the extended solution based on Layer 2 can greatly increase the number of transactions to 2,000-4,000 transactions per second, which has exceeded the processing capacity of Visa-1,700 transactions per second. Therefore, we believe that L2 scheme is the key for Ethereum to win mainstream users.

There are many expansion schemes of Layer2 in etherfang, including side chain, State Channel, Plasma, ZK Rollup, optimal rollup, Validium, etc. See the following table for the current mainstream Layer-2 solutions and their advantages and disadvantages:

	State Channels	Sidechains	Plasma	Optimistic Rollups	Validium	Zkrollup
Examples	Pisa,celer	Skale,poa	Omg,matic	Ovm,fuel	StarkeX	Zksync,loopr
Security						
Liveness assumption (e.g. watch-towers)	Yes	Bonded	Yes	Bonded	No	No
The mass exit assumption	No	No	Yes	No	No	No
Quorum of validators can freeze funds	No	Yes	No	No	Yes	No
Quorum of validators can confiscate funds	No	Yes	No	No	Yes	No
Vulnerability to hot-wallet key exploits	High	High	Moderate	Moderate	High	Lmmune
Vulnerability to crypto-economic attacks	Moderate	High	Moderate	Moderate	Moderate	Lmmune
Cryptographic primitives	Standard	Standard	Standard	Standard	New	New
Performance / economics						
Max throughput on ETH 1.0	1..∞tps*	10k+tps	1k..9k Tps*	2k Tps*	20k+tps	2k Tps
Max throughput on ETH 2.0	1..∞tps*	10k+tps	1k..9k Tps*	20k+tps	20k+tps	20k+tps
Capital-efficient	Yes	Yes	Yes	Yes	Yes	Yes
Onchain tx to open new account	No	No	No	No	No	No
Usability						
Withdrawal time	1 Confirm	1 Confirm	1 Week ¹ (?)	1 Week ¹ (?)	1..10 Min ⁷	1..10 Min ⁷
Time to subjective finality	Instant	N/A(Trusted)	1 Confirm	1 Confirm	1..10 Min	1..10 Min
Client-side verification of subjective finality	Yes	N/A(Trusted)	No	No	Yes	Yes
Instant tx confirmations	Full	Bonded	Bonded	Bonded	Bonded	Bonded
Other aspects						
Smart contracts	Limited	Flexible	Limited	Flexible	Flexible	Flexible
EVM-bytecode portable	No	Yes	No	Yes ⁶	No	No
Native privacy options	Limited	No	No	No	Full	Full

0. Some researchers do not consider them to be part of L2 space at all, see

<https://twitter.com/gakonst/status/1146793685545304064>

1. Depends on the implementation of the upgrade mechanism, but usually applies.

2. Complex limitations apply.

3. To keep compatibility with VM throughput must be capped at 300 TPS

4. This parameter is configurable, but most researchers consider 1 or 2 weeks to be secure. Depends on the implementation. Free in zkSync, high in Loopring.

6. While theoretically possible, a PoC for feasibility of fraud-proofs for arbitrary EVM-bytecode has yet to be demonstrated.

7. Can theoretically be accelerated with liquidity providers but will break the capital-efficiency.

Figure 3: Layer2 expansion scheme of Ethereum and its advantages and disadvantages

At present, many Layer 2 solutions have been launched, and Layer 2 solutions have grown into the golden track in the web3.0 era. As of May 2021, two mainstream L2 models -- ZK Rollups and optimal rollups-- have been protecting cryptocurrencies worth more than 300 million dollars.

PROJECT INTRODUCTION

With the coming of Web3.0 era, the tide of decentralized data network is rising. In the past few years, we have witnessed the power of this reform movement to adjust the economic incentive mechanism. In this reform, Ethereum has the best DApp development tools and infrastructure at present. With the continuous growth of web3, Ethereum will become a new settlement layer of the Internet. However, after the explosive growth of DeFi since 2020, the performance of Taifang was overwhelmed, and the transaction cost tens of dollars or even hundreds of dollars. The capacity problem and efficiency problem of Ethereum made this avenue of blockchain world crowded and difficult, which made blockchain developers using Ethereum smart contracts and related tools miserable. In 2020, Hyden Adams once said on Twitter: "I'd like to state the fact that we will waste 420k USD every day on UNISWAP, which means that 150M USD will be wasted on gas every year. It's not ridiculous, it's a fact". These pain points have seriously affected the comprehensive development of Ethereum ecology, and Ethereum expansion track has risen rapidly and become the focus of the market.

The new roadmap of Ethereum 2.0 is the framework of "executable PoS beacon chain+data fragmentation +Layer2". In order to realize thousands of times of throughput brought by Ethereum in advance, Layer 2 will push Ethereum 2.0 into use. Under this background, the Ethernet Layer-2 aggregator NEC came into being. The aggregator of Layer 2 solution can not only improve the scalability of NFT projects, Moreover, it can bring a large number of users in DeFi system to excellent NFT projects and bring value.

Introduction to NEC

NEC (New Era) is a Layer-2 chain aggregator based on the core concept of Ethereum expansion, and is committed to building a modular, versatile and highly flexible expansion framework for Ethereum. Its core component is SDK, a modularized and flexible development framework, which supports the construction and connection of two mainstream expansion paths: Secured chains, or two-layer chain, which can rely on the security of Ethernet network. There is no need to establish its own authentication mechanism. In addition to the main chain completed at present, other Layer 2 expansion schemes will be supported in the future, such as Optimal Rollers, zk Rollups, Validium, etc., which will make NEC truly become the Layer 2 aggregator on Ethereum chain.

NEC proposes a decentralized and configurable two-tier side chain network, which provides storage function and supports transactions with high throughput, low cost and low delay. This system is the configuration and deployment of Byzantine fault-tolerant side chains with high throughput, compatibility with Ethereum virtual machines, support for storage, and can prove security. A subscription-based decentralized network is provided. The side chain of each certificate of interest is highly configurable, which is composed of nodes pledging NEC certificate on Ethereum main network, and its consensus mechanism uses asynchronous Byzantine fault-tolerant protocol.

Core advantage

Overall improvement of network performance: based on the consensus mechanism of rights certification, it becomes a blockchain network with extremely fast processing speed; It has strong scalability and can shorten the network congestion time by ~ 5S ADN 1,0000+TPS; Supporting WEB3 technology can improve its throughput.

Ultra-high compatibility: fully compatible with web3js interface API of Ethereum. This means that the website or service interacts with the Ethereum network. Web3 tries to empower users and regain the value they create. Fully compatible with EVM, DAO and smart contracts, it provides developers with comprehensive options to test and build explicit distributed applications. One-click DApp migration tool can exchange and utilize information widely in the ecosystem.

Eco-reward: In NEC's network, it also provides end users with the choice of participating and passively earning considerable income. ETL pledge shows such a characteristic, which allows users to keep NEC network stable by pledging tokens and getting rewards. The APY (annual return rate) provided by NEC for users is as high as 18%.

Wallet application: In the wallet application planned by NEC, it can provide good services for those who want to hold, send or receive funds easily. It can easily connect hardware wallets and provide a seamless experience.

Think tank team

NEC project is developed by several Turing Prize winners as consultants and directed by Ethereum technical team, which is jointly promoted by many geek technical enthusiasts and teams around the world. NEC is also a decentralized global geek community with the mission of connecting blockchain enthusiasts all over the world and providing users with blockchain services and infrastructure. NEC Technology Research Laboratory gathers core developers such as Ethereum and EOS, as well as top talents in blockchain, big data, cloud computing and other technical fields, and has comprehensive R&D strength with global competitiveness. The overall R&D strength is strong, with a number of financial product experts and safety experts, and equipped with an international-level risk control team.

ECOLOGICAL GOVERNANCE MODEL

Comprehensive application ecology of expansion and aggregation

From the perspective of industry ecology, NEC is a cross-chain comprehensive application ecology that combines DeFi, NFT, blockchain games, community currency, community autonomy DAO and various DApp application scenarios, and is committed to providing the most valuable digital asset services for every user, while helping the coordinated development of blockchain technology and various applications.

From the perspective of blockchain industry, NEC is an extensible Layer-2 aggregator with distributed technology as its core, and it is an industrial alliance of innovative technologies and blockchain application involving business enterprises. It also serves the basic ecology of C-end users and B-end users based on blockchain and intelligent network and relying on relevant technologies, data, products and scenarios of participants. NEC can effectively support asset release, transfer and exchange. Internal smart contracts can directly support online hosting, crowdfunding and other business models, and most financial core businesses can be supported at the core level. Specific personalized business scenarios can be customized through the side chain and tied (anchored) to Ethereum to realize various rich applications.

Decentralized governance (DAO)

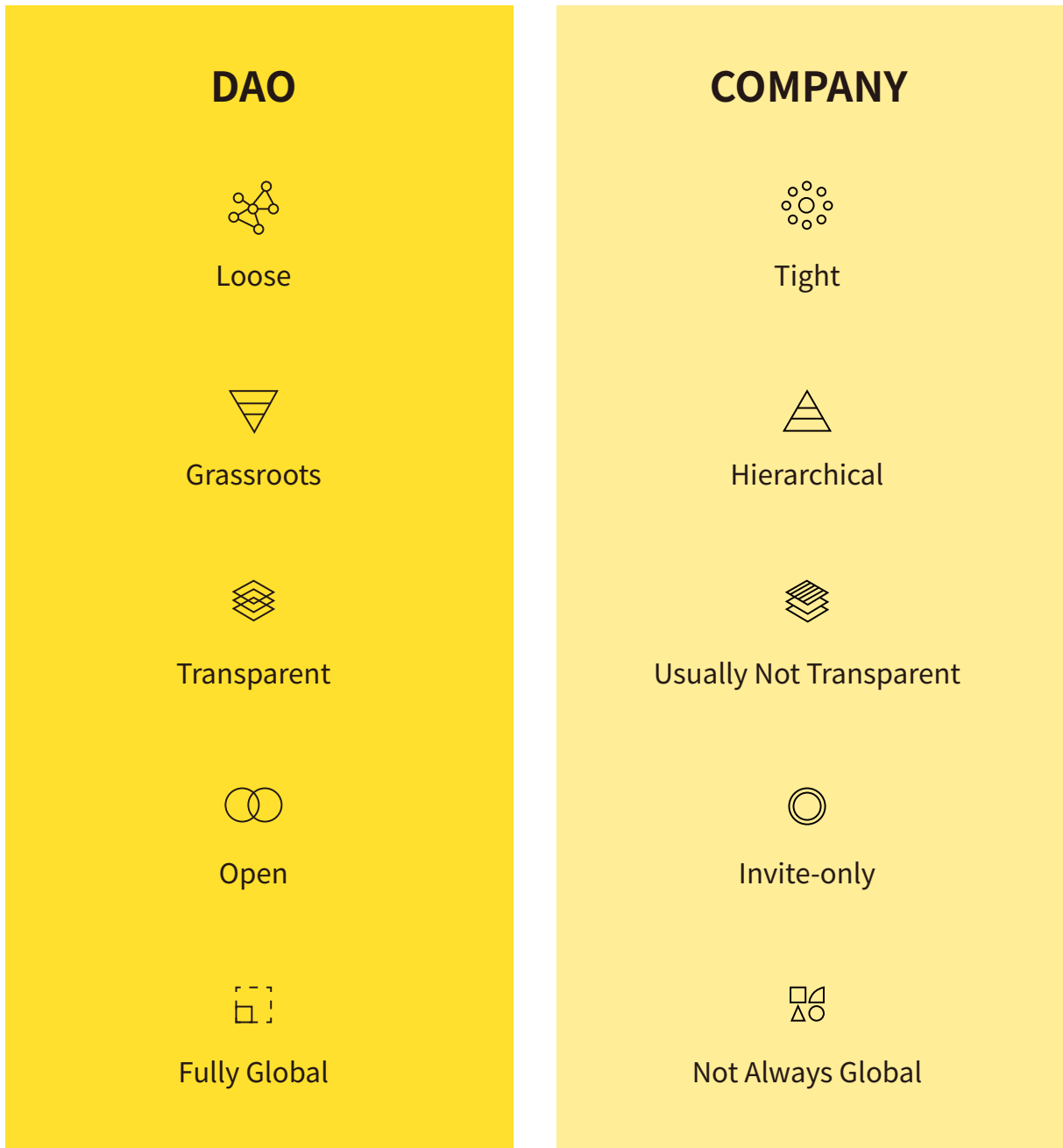


Figure 4:DAO vs Company. Source: Aragon

The decentralized chain operation of NEC is inseparable from the governance of DAO. DAO, as a decentralized autonomous organization, keeps running through intelligent contracts, and encodes transac-

tions and rules in the blockchain. It has various advantages and realizes openness, justice, no intervention and autonomous operation, but it has no legal entity. Chain voting and management of decentralized autonomous organizations. The consensus with POSDAO is a kind of DAO. Verifier is a distributed autonomous group that provides benefits and gains benefits based on participation benefits. DeFi project can use DAO governance mechanism running on the platform, such as proposal and voting system, community fund collection and so on.

NEC will ensure the release and development of its own ecological applications until the NEC community is established to maintain itself completely decentralized. NEC Eco's DAO governance adopts the incentive mechanism of general certification, which will be used as the value storage carrier to capture and solidify the growing value of the protocol network.

Decentralized ecological management system

As a decentralized ecology, NEC is supported by a completely transparent decentralized autonomous system. This structure enables each NEC holder to clearly understand all technical construction and value transfer within the ecological foundation, and fully reflects the public trust value of blockchain. All decisions in NEC are based on the referendum decision of the holder of the certificate. All technical updates are publicized by the community. This completely decentralized management system will completely avoid the disadvantages of centralized management of traditional institutions. It provides excellent and trust-free solutions for centralizing the management's exclusive rights, tampering with data and making decisions on the group's direction alone.

In order to ensure the fairness and smooth circulation of NEC's value and prevent the occurrence of large-scale control and black-box operation in the history of blockchain, NEC not only centralizes autonomous management from the root, but also hires financial auditing, analysis, investment and other practitioners from many global core financial institutions to join the Financial Supervision Council. Provide professional supervision and guidance from a financial perspective.

ECOLOGICAL APPLICATION

New financial payment system

Instead of the foundation of the Internet-based financial system, this financial system has the ability of being completely open and untrusted, and NEC can be used to pay quickly and effectively. P2P payment blockchain can replace the current expensive, slow and bank-driven process.

DeFi (decentralized finance)

Solve the problem of high gas cost in Ethereum, and be able to use existing Ethereum intelligent contracts and tools. Developers can transplant their existing DApp based on Ethereum in a short time, which greatly improves the performance and reduces the cost. Include DeFi applications-especially DEX such as Uniswap, because that high gas fee overshadow the transaction volume, Transferring assets to NEC (and bridging them) greatly reduces gas charges.

Community currency

Community Integration Currency (CIC) is a local currency and service used to pay for goods. CIC cannot replace the national currency; They are supplementary currencies used to support local trade. CIC provides a medium for daily expenditure and trade, while allowing individuals to save money (which

may be volatile or scarce) for interaction between nationals and large enterprises and government agencies outside the direct community. CIC supports and empowers communities to create jobs, develop social plans, and support trade infrastructure by establishing decentralized local banking. Blockchain technology supports CIC's local currency exchange platform by providing transparent functions based on Web. Local currency can be traded in one way and another based on exchange rate—all users need is a mobile phone and a customized wallet application. Fast speed and strong stability.

Blockchain game

Cryptography is not the only use case of blockchain technology. Experts say that games will become the first practical use case of blockchain, reshaping the industry and making games more immersive than before.

Electronic voting

Voting is a process that needs process integrity very much. The result of voting must be correct, and there must be a transparent process to ensure this, so that everyone can believe that the result is correct. There should be no possibility of successfully interfering with anyone's willingness to vote or preventing their votes from being counted. NEC guarantees the integrity of voting process based on blockchain technology, which can be used for governance and chain voting, and provides a free and open democratic way. When every vote can be verified and tamper-proof, users will know that their votes are submitted and count the results. This is essential for participation, and for small communities, Petitions and local governance (as well as DAO), this is correct because of the larger communities (such as national elections). For the sake of effectiveness, there are basically no restrictions, voting is very easy, anonymity is allowed, scalability for users is very cheap (therefore, no one is excluded), and it has ideal functions to

run from smart phones. Voting must be traceable in real time and can be reviewed by any entity. Through fast and cheap processing, our platform is very suitable for many different fair and transparent voting procedures. Now, the demand for this technology is more obvious than ever. And we are very happy to see the new innovation blockchain voting related to digital and digital technology on the platform.

NFT casting

NFT is a unique and non-interchangeable asset cast in the chain. NFT is creating interesting use cases in digital art, collectibles, ticketing, games, digital ownership and other fields. Each NFT has its own unique attributes that can be tracked and unchangeable. NFT artists can sell their works directly to collectors. The authenticity and quantity of cast works can be verified by anyone at any time. The platform can also be set to allow royalties to be collected in future resale events. Proof of ownership is easy to verify, which is important for ownership records, domain names and other assets.

Like other alternative assets (cryptocurrencies), token owners can fully control and manage their own assets without relying on third parties. The high cost of gas in Ethereum makes it too expensive to cast and trade NFT on the main network. The platform solves this problem by casting, trading and storing NFT. Once the value is determined and/or access to Ethereum is required, you can use TokenBridge to transfer unique assets and all associated metadata to Ethereum. This system provides a fast and cheap way to create and manage NFT in the whole blockchain ecosystem.

NEC wallet

The development team is working hard to build an easy-to-use Plasma wallet mobile application, which is integrated with WalletConnect to ensure secure storage of keys, intuitive access to functions provided

by NEW ERA based on Ethernet Layer2, and seamless link from DApps to browser. Users can interact with DApp on browsers and more devices in the future, While still keeping its key securely in the mobile wallet.

—OpenNEW ERA-Ethernet light client based on POS network

OpenNEW ERA is the fastest, lightest and safest Ethereum client developed based on fast PoS network without license, which has lightweight identity protocol and stability protocol. It uses the Rust programming language. It is licensed under GPLv3 and can be used for all Ethereum requirements. Particularly, Lightweight identity protocol means that it can match the public key with the hash value of mobile phone number, thus allowing cryptocurrency to be sent to any mobile phone number, which eliminates many barriers to cryptocurrency transactions. A simple smart phone can act as a node in the NEW ERA network, which is realized by fast synchronization of ultra-light clients.

Clean, modular code base, easy to customize

Advanced client based on CLI

Minimum memory and storage space

Use Warp Sync to synchronize in hours, not days

Modularity, which can be easily integrated into your service or product.

TECHNICAL ARCHITECTURE

Under-chain verification of NEC

The throughput of the basic Ethereum blockchain is the same, and the second layer solutions are all operated under the chain instead of on the Ethereum blockchain, while still ensuring sufficient security and immutability.

- **layer 2** refers to systems built “on top” of layer 1.
- layer 2 scaling solutions increase ethereum’s effective transaction throughput by performing some operations “off chain”
- These solutions do not typically require a hard fork, they are implemented as smart contracts.

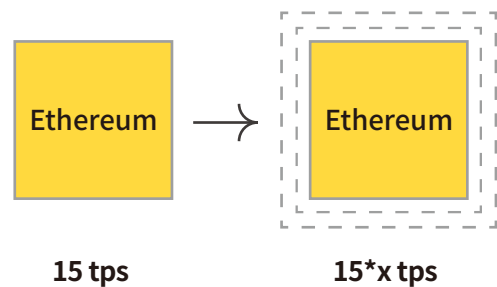


Figure 5: Ethereum Layer 2 solution

NEW ERA exists in the form of Ethereum intelligent contract, and interaction with the software under the chain does not require changes to the basic protocol. NEW ERA allows the application based on Ethereum to still be verified on the main chain. Once a specific operation is verified, it is small enough to be executed on the Ethereum main chain. Therefore, Applications can also use calculations that are too expensive to do on the chain. For example, verifying the simple payment verification (SPV) certificate from other blockchain can make Ethereum smart contract "check" whether the transaction has occurred in another chain (such as Bitcoin or dogecoin).

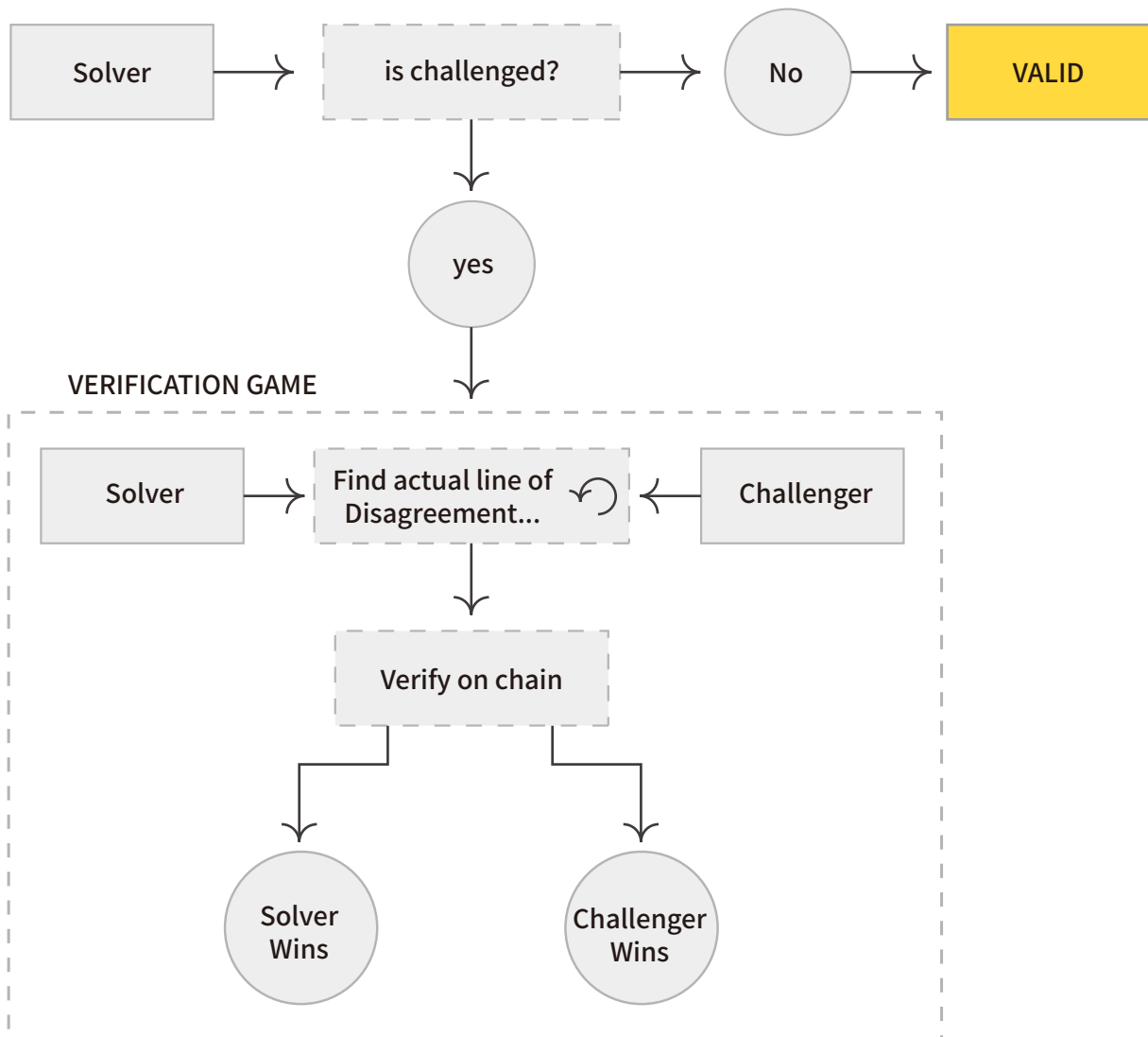


Figure 6:NEW ERA Simplified Concept Map

Imagine that you have some expensive calculations (like SPV proof) that need to be part of your application. You can't just regard it as a part of Ethereum's main chain intelligent contract, because the computation cost of SPV certification is very expensive. Remember, it is very expensive to do any calculation directly on Ethereum. Because each node has to process this operation in parallel. The block of Ethereum has an upper limit of available gas, which sets an upper limit for the total amount of calculations that all transactions in the block can perform. The computational cost of an SPV proof is very high. Even if it is the

only transaction in a block, the gas value it needs is many times the limit of the gas value of a single block. But, you can pay others a small fee and put the calculation out of the chain. The person who receives your money is called the solver. First, the solver pays the security deposit in the smart contract. Then, you describe to the solver the calculations they need to perform. They do the calculations and return the results. If the result is correct (mostly within one second), their deposit will be returned. If it turns out that the solver didn't perform the calculation correctly—that is, they had fraudulent operations or made mistakes, then they lost the deposit.

NEW ERA uses an economic mechanism called "verification game" and the verification game is executed in a chain, so it can't just calculate the results.

SPOR point-to-point encrypted storage

NEC needs to build a data storage platform that can be encrypted and shared. First of all, we need to ensure that the encrypted and shared files themselves can be proved to be storage integrity, rather than being unrecoverable after storage. Based on this choice, we need a reliable and effective way to verify the integrity of file storage and the related proof that it can be retrieved completely.

NEC chooses the representative SPOR algorithm here, which provides a complete theoretical system that can prove security and verify the integrity of file storage. We can use this storage integrity verification algorithm to provide important auxiliary information for NEC style consensus algorithm to be introduced later, so as to achieve organic integration and complementary advantages.

This part of auxiliary information provides the corresponding weight in the later chain governance, that is to say, our governance is not a simple bet and an offline governance mode. We use the storage integrity verification algorithm to audit the contribution of storage nodes in the chain, and combine the online governance mode of betting to optimize and maintain the stability of the system step by step.

The advantage of this method is that it will not be disturbed by some uncertain factors. Spor (Sentinel Proof of Retrieval), an algorithm of traditional POR, detects the verifiability of data by setting up a specific document fingerprint. File fingerprint is a block with random value, and it is indistinguishable from file block by encryption. SPOR protocol structure includes the following three parts:

Establishment phase:

The verification node v encrypts the file f , and implants the file fingerprint into the random position of the file f , wherein the check value of the fingerprint is randomly constructed. Let $F\sim$ be the document after fingerprint implantation.

Verification phase:

In order to verify that the storage node holds the file F , the node V selects the location of some fingerprints in F , and requests the storage node to return the corresponding fingerprint values.

Safety phase:

Because the file f is encrypted and the fingerprint value of the file is random, the storage node cannot distinguish the fingerprint from a certain part of the original file. Therefore, we realize the following characteristics: if a storage node deletes or modifies a part of a file entity, there is a high probability that the corresponding part of its fingerprint will also be modified. When the verification node queries and verifies enough fingerprints, it can detect whether the storage node modified or deleted the file entity.

Suppose a document contains b blocks: $[1], \dots, [b]$.

Coding functions require the following four steps:

Error correction: we cut the file f into k blocks. For each part, we use (n, k, d) error correction code c , so that each part is expanded into n blocks, and a new file $f' = [1], \dots, [b]$ is generated, which contains $b' = bn$ blocks.

Encryption:

We apply symmetric key cryptography to f' and get a new file f'' . Because the file needs to be restored when the storage node deletes or damages the file block, the data block needs to be encrypted independently, that is, the password can run independently on the text block.

Create file fingerprints:

Let: $\{0,1\} \times \{0,1\} \rightarrow \{0,1\}$ be a simple one-way function, and then a group of file fingerprints $\{f_i\}_{i=1}^b$ can be calculated with $\text{pass} = (k)$. Apply the above file fingerprint to f'' and get the file f''' .

Replacement:

Let: $\{0,1\} \times \{1, \dots, b'\} \rightarrow \{1, b'\}$ be a pseudo-random permutation. We apply g to the file f''' , and get the output file F .

Design of data governance structure

Governance structure, as an indispensable link between the preceding and the following in the consensus, is also the main difference from the Internet. If the verification in the system can be proved within a specified time in a consistent network, then in an available network, Every node in the system needs to broadcast according to a specific data governance structure in order to maintain the fault-tolerant characteristics of the whole system. In NEC's data governance structure, we can design the following governance methods through the additional information obtained in the storage network:

- Each storage node needs to bet before it can enter the system contribution storage unit;
- After storage, rank through the comprehensive weight of the combination of stored contribution and bet;
- The 101 nodes with high ranking perform blocking actions in the public chain. The selection of the 101 nodes is based on the study of successful PoS cases. Compared with the 21 nodes of DPoS in EOS, the 101 nodes have inclusiveness to the newly added nodes and increase the difficulty of flood attack on the newly added nodes;
- In each round of Committee block-out, the way of block-out in turn will be used, and there will be more rounds of nodes with high ranking. The existing blocking operation is divided into rotating blocking and random number blocking. In Ouroboros, random numbers are encrypted and communicated, so blocks are made according to a specific random number, because it is judged that PoS is not necessarily a good node. NEC finds out good nodes through chain governance and polls them by storing additional information that data can be retrieved. Through NEC, the block can be made faster, because the operation of random number communication is omitted;
- Large nodes can choose small nodes to contribute storage for themselves.

Under this governance structure, every storage node needs to make a bet to enter the system if it wants to start contributing to the system. In the design, the storage node needs to be relatively stable. This mechanism that adds a threshold to the admission mechanism can be partially screened when selecting the primary node, because when the data needs to be stored, the storage space he needs and the mapping backup space need relatively robust storage nodes to ensure that they can be retrieved later.

Because committee members are ranked by the comprehensive weight of storage contribution and bet amount, the nodes in the chain system need to be recognized by both the storage network and the public chain before they can be accepted by the committee. That is to say, it is not completely feasible to enter the market only by pledge. The contribution ranking in the storage network ensures that the nodes that contribute to the system can stay in the Committee for a long time, thus avoiding that only the pledged nodes stay in the Committee for a long time.

Large nodes can encourage more small nodes to participate in the storage construction of the storage network with their own small profits by letting small nodes contribute storage; At the same time, big nodes can also improve their rankings in this way. This participation mechanism can give medium-sized nodes and large nodes a chance to play games. Although for large nodes, medium nodes, small nodes have different division of labor, but there is a fair part in the overall mechanism design. Medium-sized nodes can compete with large nodes, and small nodes can sell their own storage parts to get extra block rewards.

I/O streaming protocol (GSIOP)

In the data storage of blockchain, the size limitation of storage on the chain and the inability of self-certification of data under the chain have always been the bottleneck of DApp design. NEC itself has an entrance from outside the chain to the chain, and the storage part is responsible for this part of the function. Therefore, the data holder can initialize on NEC, the practice of storing data under the chain

through NEC streaming protocol to mark data outside the chain.

Compared with the existing prophetic machine mode and the original direct storage on the chain, it can guarantee the ownership and privacy of data with larger storage space. Through such a mark, NEC streaming protocol is to achieve multi-party file changes and ensure privacy through encrypted storage. This is also the design of NEC, which always thinks that the information stored in DApp needs to be private (i.e. undisclosed). GSIOP is to customize the encrypted storage part into a widely used protocol by using the characteristics of NEC storage, so as to achieve the special functions brought by relevant encryption algorithms while encrypting the data stream for access by NEC.



1/0 Streaming protocol

In the practical use of blockchain, it is difficult to guarantee the data size on the chain and the synchronization of the data under the chain. In other words, if the data is kept in the chain, the data size must be considered. Since the data that each block can keep is limited, increasing the data size will affect the block size. Although the size of the data does not need special consideration, But the synchronization of data needs special treatment.

That is to say, if the data does not have any confirmation mechanism, it cannot be directly uploaded. First of all, whether the data under the chain can guarantee the confirmation, because the identity under the chain is not unique, it is difficult to judge whether the uplink operation after the identity under the chain is confirmed by the credible part; Secondly, When the data under the chain can be uploaded, it can be processed by different nodes for many times. Because the data is open, it is difficult to sort out which parts are available.

For example, a malicious node can change a public data through accounts A, B, and C without any punishment. Even if the accounts A, B, and C are prohibited from being changed at the same time, a new account D will be maliciously operated. Therefore, users before uploading data under the chain need to be differentiated. Current solutions include offline solutions based on lightning network and lightning network. When the data link goes down to the uplink, it is similar to self-verification first and then let the nodes on the chain verify. On the lower chain of the chain, it is provided in a way similar to centralization.

We prefer to transmit the data under the chain through a protocol, and then synchronize this part of the data in the chain through isomorphism. To put it simply, it is to give the next data channel in the chain. Users only need to initialize the data on NEC, and then the rewards and punishments are solved through chain governance.

GSIOIP is a protocol scheme that ensures the reliability of storage under the chain by encryption. Firstly, the account number selectivity is made to the modifiable person when the data initializes the storage unit by encryption algorithm, which is divided into data owner, data partial modifier and data supervisor.

They correspond to three users with different roles in the data. The owner of the data has the key of full modification, and the owner has the operation of full modification. This part of the data is maintained by the owner in the system, so the data can be related to a specific storage address, and the data has the choice of privacy.

Part of data changer, which is selected by the data owner to change the relevant part of data. Data can be segmented so that different people can change different parts, and the address of data changer corresponds to the data change action, so that people who have problems with data change can be found.

Data inspector, who has the right to view data without changing it, plays a role in the whole system to eliminate the false data uploaded by relevant bad addresses. In the first version, GSIOP first changed the value of uint, and for this function, the first kind of application can be extended, that is, an encrypted side chain system. The data owner is the user holding NEC in this system, and he can use NEC across chains by locking. Information about another chain using NEC can be accepted and encrypted and stored in the storage network by using a user whose account has account information in another chain other than NEC as a data part modifier.

Finally, the whole node of the other chain acts as a supervisor, and he can see that there is information coming in this way and store the intermediate steps. At last, when users want to withdraw the remaining NEC, they only need to call all the relevant stored information to ensure simple cross-chain operation. In later versions, GSIOP will provide the calling and changing operation of string. Related functional extension applications will also be written later. Due to the addition of related storage functions, NEC has made corresponding changes in smart contracts and virtual machines. NEC will add opcodes and related types and instructions to existing stack virtual machines in a way compatible with existing EVM.

EXTENSION & AGREEMENT

NEC Assets Cross-chain Bridge

NEC makes use of the communication ability between L1 and L2, and transfers any form of Ethereum assets (including Ether, ERC20, ERC721, etc.) between L1 and L2 without trust. When transferring assets from L1 to L2, the assets are deposited in a NEC bridge contract on L1, and then an asset of the same amount is cast on L2 and deposited in the designated address; When assets are transferred back from L2 to L1, the assets will be destroyed on L2. Then the same amount of assets will become available in the bridge contract of L1.

Transactions initiated by L1 to L2 are first stored in inbox with transaction parameters such as calldata, callvalue and gas info. When the transaction fails to be executed for the first time, it will be put into the "retry buffer" of L2, which means that anyone can redeem the bill by re-executing the transaction for a certain period of time (usually a challenging period, i.e. about one week). There is no time limit for the retry transaction from L2 to L1, and it can be carried out at any time after the end of the dispute period.

This mechanism is mainly designed to deal with such a scenario: when a user wants to deposit a token from L1 into L2, they will first deposit these tokens into the bridge contract of L1, and at the same time cast the same token on L2. Suppose that the transaction on L1 has been completed, but the transaction on L2 has failed due to insufficient handling fee, which will lead to a serious problem: the user's token on

L1 has been transferred out, However, tokens were not received on L2. In fact, these tokens were locked in L1's contract. The user (or anyone else) can re-execute the transaction with enough handling fee within one week and finally get token on L2 through the mechanism of retryable bill.

The following are the basic steps of NEC asset cross-chain bridge:

L1 ->L2

The user initiates a Deposit transaction from L1

Assets are deposited in L1 contract, and transactions are deposited in Inbox in batches

The transaction is executed at L2, and the casting assets are transferred to the designated address

If the transaction fails, the transaction is stored in the retry buffer of L2, and the user can initiate a retry in a challenge period

L2 -> L1

The user initiates a Withdraw transaction in L2

L2 chain packages the transactions collected in a certain period of time, generates Merkel tree, and publishes the root node as OutboxEntry to L1 Outbox

The user or anyone can perform Merkel verification on the root node and transaction information

After the challenge period, the user can complete the transaction at L1, and if the transaction fails, the user can initiate a retry

Save

In order to expand the potential application scenarios, NEC has improved the current EVM to realize the storage of larger files. The modifications include increasing the specifications of blocks (allowing each block to contain more data) and directly accessing the file system of each node through a fileStorage precompiled intelligent contract. Users in the network can now divide files into 1MB "chunks", and submit them to the fileStorage smart contract and store them in the file system of each node in a continuous way. Files in the network can also be deleted by renting, so as to ensure that the network can reallocate resources when the state is congested and extra storage performance is needed.

Consensus

When developing consensus algorithm, it is very important to consider malicious participants, botnets, distributed denial of service (DDoS) attacks, malicious firewalls, etc., which will interfere with network communication. At the same time, the ratio between the support of any large network for high throughput information and the downtime of network nodes is very important. In view of the above reasons, NEC currently adopts Moustefaoui et al. A variant of al , because it provides a lot of ideal and necessary functions for truly decentralized and high throughput networks. This protocol enables a leaderless, asynchronous and Byzantine fault-tolerant network to be realized.

Without leadership

At present, in many decentralized/distributed consensus protocols, a leader will be selected in each round to present some data (that is, a block) for the network to run consensus and reach consensus. NEC implements another consensus protocol, in which all virtual child nodes can propose blocks, and only those virtual child nodes that receive the vast majority of signatures ("a threshold") are eligible to submit

to the blockchain. No leadership not only eliminates collusion among network participants, but also ensures that all participating virtual sub-nodes have fair opportunities to propose blocks.

Asynchronous

In the asynchronous timing model, there is no fixed limit or expectation for the information transmission time of the network. When sending information, the virtual child nodes in the network do not expect to receive a reply immediately, and execute an exponential information return process. They try to resend the information with long interval but not yet received a reply. This model accurately captures the current running state of the Internet-nodes in the network will always fail and information will always be lost.

Byzantine fault tolerance

Byzantine Fault Tolerance (BFT) is the security standard of distributed systems. BFT system ensures that nodes in the network can always reach the same consensus with less than 1/3 malicious nodes. Nodes regarded as "malicious" in the network may exhibit various behaviors, including but not limited to false reports, collusion and refusal to participate. In various implementations of BFT, Asynchronous Byzantine Fault Tolerance (ABFT) is the most powerful. This is because they can cope with the possibility that the information between honest participants is delayed or cannot be sent to the intended recipient, which is not uncommon in similar Internet environments.

Network security hypothesis

This protocol assumes that the network is an asynchronous system with the guarantee of final transmission, which means that it assumes that all virtual sub-nodes are connected with each other by a reliable communication link, which may be very slow, but will eventually transmit information. This asynchronous model is similar to Bitcoin and Ethereum blockchain. It reflects the state of modern network-temporary network differences are normal, but they will be solved in the end. In practice, the ultimate delivery guarantee is realized as follows: when the information is exponentially returned, the sending virtual child node will make multiple attempts to deliver the information to the receiving virtual child node until the delivery is successful.

TOKEN ALLOCATION

NEC is the original token of NEW ERA. NEC is used as POS staking currency, and the currency holder can get the ecological incentive of NEVERA, which is not limited to:

NEC cross-chain bridge handling fee: In the case of cross-chain transactions, bridges are required to connect blockchain. Entry and exit fees charged when transactions move between EVM are based on blockchain. The expenses are allocated to the verifier and the principal and their mortgage rate.

Staking Award: In NEW ERA's network, it also provides end users with the choice of participating and passively earning considerable income. Users pledge tokens and get rewards to keep NEW ERA's network stable, and the APY (annual return rate) provided by NEW ERA for users is as high as 18%.

Token name: NEC

Issued total amount: 600000000

Allocation scheme:




STRATEGIC PLANNING


The upgrade of New Era is divided into several stages like the second floor of Ethereum. We are divided into stage 1, stage 2, stage 3 and stage 4. More subsequent upgrades will be continuously updated according to the progress of the second floor of Ethereum


▶ Stage 1 (February-May 2021)

- **February 2021**
 - Support solidity language and compiler
- **March-April 2021**
 - To develop an asset cross chain bridge based on Ethereum layer 2 protocol, developers can use new era to make seamless cross chain experience a part of their DAPP.
 - ① Fast access and exit between Ethereum and L2 system;
 - ② L2-l2 switching, completely bypassing Ethereum;
 - ③ Arbitrage between defi applications on different chains;
 - ④ Construct cross chain DEX aggregator;
 - ⑤ More general cross chain smart contract calls.
- **May 2021**
 - The new era Cross Chain Protocol simplifies the handling of fees, and users can transfer money without holding a specific token.

A grey triangle pointing right, followed by the text "Stage 2 (June-December 2021)".


-  **June 2021**
 - Issuing governance token \$NEA to open private placement and Ido

-  **July-August 2021**
 - Decentralized NFT streaming media platform launched to support NFT transactions
 - Online mainstream exchanges start trading publicly
 - Open pos mining

-  **October-December 2021**
 - Deploy real-time cross-link communication function Space-fold compatible with Ethereum Layer 2, which can be "folded" to Ethereum Layer 2 solutions such as xDai, Optimality, Matic, SKALE and Arbitrum.
 - The New Era cross-chain wallet is launched, and through the state channel technology, assets can be freely transferred between the second-layer network of Ethereum (including zkRollup) and the fragments of ETH 2, and even other public chains (compatible with EVM), without waiting for a long exit time.

A vertical blue line with a grey triangle pointing right at the top, followed by the text "Stage 3 (January-December 2022)".

-  **January-February 2022**
 - Global recruitment of New Era authentication node
-  **March-May 2022**
 - The distributed cloud storage function for cloud mining and hosting space is online
-  **June-July 2022**
 - Global recruitment of distributed cloud storage provider nodes (cpu, memory and processor)
-  **August-September 2022**
 - Distributed cloud storage platform supports users to host programs such as Wordpress and Magento
-  **October-December 2022**
 - Support Go,Nodejs.Python and other languages for development

 **Stage 4 (2023 and beyond)** **2023 and beyond**

- Pay close attention to the development of Ethereum Layer 2 technology, realize cross-slice transfer and contract call, and build an execution environment to support the construction of extensible applications on Ethereum 2.0.
- NEC DAO Global Community Autonomy Alliance was established to reach a vision consensus and promote community autonomy.
- NEC ecological start; Gradually improve ecological application, integrate market resources, and carry out business cooperation on a global scale.

APPENDIX

Risk warning

There are various risks in the development, maintenance and operation of NEC, many of which are beyond the control of NEC developers. In addition to other contents described in this white paper, please fully understand and agree to accept the following risks:

market risk

NEC's price is closely related to the whole market situation in digital currency. If the overall market situation is low or there are other uncontrollable factors, NEC's price may remain undervalued for a long time even though it has good prospects.

Regulatory risk

As the development of blockchain is still in its early stage, there are no relevant regulatory documents in the world about the pre-requirements, transaction requirements, information disclosure requirements, lock-in requirements and so on. Moreover, it is unclear how the current policy will be implemented, and all these factors may have an uncertain impact on the development and liquidity of the project. Blockchain technology has become the main regulatory object in major countries in the world. If the regulatory body intervenes or exerts influence, NEC may be affected by it. For example, the use is restricted by laws and regulations, and NEC may be restricted, hindered or even directly terminated.

Competitive risk

At present, there are many projects in the blockchain field, and the competition is fierce. There is strong market competition and project operation pressure. Whether NEC projects can break through many excellent projects has been widely recognized, which is not only linked to their own team ability and strategic planning, but also influenced by many competitors in the market, and may face vicious competition.

Risk of brain drain

NEC has gathered a talented team with both vitality and strength, and attracted senior practitioners of blockchain and technology developers with rich operations. In the future development, the possibility that NEC as a whole will be negatively affected due to the departure of core personnel and conflicts within the team cannot be ruled out. The accelerated development of cryptography or the development of science and technology, such as quantum computer, will bring the risk of cracking to NEC platform, which may lead to the loss of NEC data.

In the process of project update, there may be loopholes, which will be repaired in time after being discovered, but there is no guarantee that it will not cause any impact. Other unknown risks at present, besides the risks mentioned in this white paper, there are also some risks that have not been mentioned or anticipated by the founding team. In addition, other risks may suddenly appear, Or in the form of a combination of various risks already mentioned. Participants are invited to fully understand the team background, know the overall framework and ideas of the project and participate rationally before making participation decisions.

Disclaimer

This document is only used to convey information, and the contents of the document are for reference only. It does not constitute any suggestion, instigation or invitation to sell stocks or securities in NEC and its related companies. This document does not constitute or be understood as providing any trading behavior, nor is it any form of contract or commitment. In view of the unpredictable situation, The goals listed in this white paper may change. Although the team will try its best to achieve all the goals of this white paper, all individuals and groups who purchase NEC will take their own risks. The document content may be adjusted in the new white paper with the progress of the project, and the team will announce the updated content to the public by posting announcements on the website or the new white paper. This document is only for the specific object who actively requests to know the project information to convey information, and does not constitute any future investment guidance, nor is it any form of contract or commitment.



niEW
ERA