NuLink Whitepaper 2.0

May 1, 2023

Abstract

NuLink provides privacy-preserving technology for decentralized applications via APIs. We enable and make it easy for developers, startups, small businesses and enterprises to build their own applications with all the best security and privacy practices.

1. Introduction

NuLink network is a decentralized solution for web3 privacy-preserving applications developers to implement best practices and best of breed security and privacy. The NuLink platform provides endpoint encryption and cryptographic access control. Sensitive user data can be securely shared from any user platform to cloud or decentralized storage, and access to that data is granted automatically by policy in Proxy Re-Encryption or Attribute-Based Encryption. To verify the data source, data users can utilize Zero-Knowledge Proof. Additionally, for advanced privacy-preserving use cases, NuLink utilizes Fully Homomorphic Encryption (FHE) to provide customized enterprise-level data computation services.

1.1 Background

In 2006, British mathematician and entrepreneur Clive Humby famously said “Data is the new oil”. He was, of course, referring to the immense opportunities for anyone who could tap data’s fundamental value. Today, businesses across the spectrum understand that data is the key to maximize business value. From autonomous driving (Tesla, Waymo) to content makers (Netflix, HBO), from e-commerce (Alibaba, Amazon) to financial markets (Robinhood, Coinbase) – almost all businesses are mining data to fuel innovation and growth.

At the same time, data can cause irreparable damage to businesses, reputations and people’s lives if sensitive information leaks in a data breach. For example, the number of data breaches in healthcare has been increasing year after year, affecting millions of people including children. In just one instance, hackers who gained access to the records of a Finnish mental health startup in 2020 extorted money from the patients enrolled with the startup.

In many cases, even though the law requires companies to implement data protection (for example, Europe's GDPR or General Data Protection Regulation that is known as the toughest privacy and security law in the world), businesses regardless of size – enterprise, small or medium businesses or startups – often find it difficult to protect their users' data. The reasons for this are many and include the following:

- The means of privacy protection are diverse and the technology is complex. Depending on the particular scenario, it is often necessary to use a combination of one or more crypto technologies. There is a high technical threshold and not all businesses have the resources or capacity to provide this.
- It is difficult to ensure the secure storage of data. Plain text storage, an attack on a centralized server, and other issues may all lead to a data breach.
- Due to the lack of universal solutions, the implementation of privacy protection schemes requires high costs in terms of time, money and technology.

Finding a solution to these data privacy problems is the motivation behind NuLink.

NuLink has the following core characteristics: It integrates a variety of crypto technologies, is decentralized, easy to implement, and open source. We aim to offer an out-of-the-box solution that lowers the threshold of having a privacy protection scheme in application for all kinds of business. NuLink will offer everything needed including data encryption, key & storage management, inter-blockchain deployment and privacy computing.

1.2 Our Technologies

NuLink is building a robust technology foundation by integrating top-tier technologies. The platform offers technical solutions that fall into three primary categories:

- Data Availability: NuLink utilizes advanced cryptographic techniques such as Zero Knowledge Proof to ensure the availability of data in ciphertext form.

- Privacy-preserving data sharing: The general method is to encrypt data and let the data owner control access to it. The technologies include decentralized encrypted storage, proxy re-encryption, identity-based encryption and attribute-based encryption, etc.
- Privacy-preserving data computing: This involves the integration of certain privacy computing capabilities into smart contracts. The technologies used include multi-party secure computing, homomorphic encryption and so on.

These three categories of technical solutions enable NuLink to provide privacy-preserving applications across numerous fields, including Decentralized Finance (DeFi), healthcare, web3 social networks (SocialFi), Digital Rights Management, and more.

2. Design Philosophy

2.1 Architecture

The NuLink network integrates the Application Layer, the Cryptograph Layer, the Storage Layer, the Blockchain Layer and the Watcher Network.

Figure 1: NuLink Network

1. The Application Layer: The Application Layer acts as an interface between the system and the application, facilitating direct communication with the application while also liaising with the Cryptography Layer to validate access to the application's confidential information.
2. The Cryptograph Layer: The Cryptography Layer carries out cryptographic functions for the Application Layer, such as generating keys, encrypting, decrypting, and other related tasks. It also connects to the Storage Layer to facilitate the uploading and downloading of encrypted privacy data.

3. The Storage Layer: Our platform's Storage Layer is a secure network created for the purpose of storing confidential data in encrypted form. At present, we utilize IPFS (InterPlanetary File System) as the primary decentralized storage network. Nonetheless, we intend to incorporate additional storage networks like S3 in the coming times.
4. The Blockchain Layer: The Blockchain Layer is responsible for managing staking node registration and service requests within the blockchain system. As of now, only Ethereum is supported for staking node registration. Nevertheless, users can still make service requests in other blockchain systems, such as Binance Smart Chain, Polygon, Polkadot, Arbitrum, Aptos or Sui.
5. The Watcher Network: The Watcher Network is a relayer network that transfers staking node information from Ethereum to other blockchain systems. To ensure its decentralization and security, the Watcher Network is maintained under an on-chain governance mechanism (DAO).

Through a unified API integration, NuLink users can access a range of privacy-preserving services, storage, and blockchain solutions. Staking nodes have the opportunity to earn NuLink's token (NLK) by offering privacy-enhancing services in the Cryptography Layer, providing decentralized storage solutions in the Storage Layer, and relaying data from Ethereum in the Watcher Network.

2.2 Crypto Primitives

The core product provided by NuLink is decentralized privacy-preserving technology, which is an organic combination of blockchain and cryptography technologies. The crypto primitives involved include Proxy Re-Encryption (PRE), Fully Homomorphic Encryption (FHE), Zero-Knowledge Proof (ZKP) and so on. This section will introduce these crypto primitives and the schemes used by NuLink, and explain how these work in NuLink systems.

2.2.1 Zero-Knowledge Proof

Zero-Knowledge Proof (ZKP) means that the prover makes the verifier believe that a certain conclusion is correct without providing any useful information to the

verifier. Zero-Knowledge Proof was first proposed by S Goldwasser et al in 1989. It has the following three properties:

1. **Completeness:** If both the prover and the verifier party are honest and follow every step of the proof process, then the proof must be successful and the verifier must accept the prover.
2. **Soundness:** No one can forge a new proof and successfully make it pass verification.
3. **Zero Knowledge:** After the verification process, the verifier verifies that the prover has the knowledge but does not get any information about that knowledge. From the point of view of the prover, they did not breach privacy.

Figure 2: *Zero-Knowledge Proof (ZKP)*

By whether the participants need to interact or not, Zero-Knowledge Proof can be divided into Interactive Zero-Knowledge Proof and Non-Interactive Zero-Knowledge Proof or NIZK. NIZK is suitable for decentralized scenarios. The commonly used NIZK schemes are zk-SNARK, zk-STARK, Bulletproofs, PLONK, Supersonic, Malin and so on. Each scheme has its own advantages and we can choose the appropriate one depending on the different scenarios involved.

ZKP provides an additional layer of security and privacy for users by providing publicly verifiable proof, making sure that users of the NuLink network can easily verify that their data is being correctly stored and processed.

2.2.2 Proxy Re-encryption

Proxy re-encryption (PRE) is a type of public-key encryption (PKE) that allows a proxy entity to transform or re-encrypt data from one public key to another, without having access to the underlying plain text or private keys. The proxy re-encryption operation process is as follows:

Figure 3: *Proxy Re-encryption (PRE)*

1. Publisher Alice encrypts the data m with her own public key into c_A, then Alice sends the ciphertext c_A to the proxy and generates a re-encryption key for her, which is calculated by Alice herself.

2. Next, the proxy uses the re-encryption key to convert the ciphertext c_A into a ciphertext c_B that can be decrypted by Bob with his secret key and sends it to Bob. The proxy only provides computing conversion services and cannot get plaintext.

3. Bob decrypts the plaintext m that Alice wants to share securely.

Proxy re-encryption plays a role in private data sharing in NuLink. Specifically, NuLink uses the Umbral Proxy Re-Encryption Scheme. Umbral is a threshold Proxy Re-Encryption scheme following a Key Encapsulation Mechanism (KEM) approach. It is inspired by ECIES KEM, and the BBS98 proxy re-encryption scheme. With Umbral, Alice – the generic name for data owners in NuLink KMS (Key Management System) – can delegate decryption rights to Bob for any ciphertext intended to her through a re-encryption process performed by a set of N semi-trusted proxies. When at least t of these proxies (out of N) participate by performing re-encryption, Bob is able to combine these independent re-encryptions and decrypt the original message using his private key.

Using Umbral, NuLink can not only easily realize single-user to single-user private data sharing – we emphasize again that Umbral is a threshold scheme – NuLink can also realize single-user to multi-user private data sharing.

2.2.3 Identity-Based Encryption and Attribute-Based Encryption

Both identity-based encryption (IBE) and attribute-based encryption (ABE) are public key encryption schemes that control access rights. The former can specify the identity information of the recipient, while the latter can specify the attributes of the receiver. NuLink uses these two technologies to achieve more functional data sharing.

Using public key encryption to transmit data has certain shortcomings and risks. For example, the public key is generally a series of meaningless random numbers. If the public key is used incorrectly in the encryption process, the ciphertext cannot be decrypted by the correct receiver. At the same time, it is likely to disclose the information to the wrong user, or even to malicious users. In fact, in real life, there is such an attack method: malicious users deceive the sender and replace the receiver's public key.

IBE solves this problem by binding the user's identity information directly to the public key. It is similar to an ideal email system: If you know someone's identity, you can send them a letter that only they can read. You can authenticate their signature.

Figure 4: *Attribute-Based Encryption (ABE)*

On this basis, ABE has made a further functional expansion. If we define attributes as the characteristics of things or information, policy is the relationship between these features. Then IBE uses the simplest policy and attribute matching, that is, authenticating identity attributes. In ABE, there are more diverse choices of attributes and policies. ABE is generally divided into two categories. KP-ABE (key policy) embeds the policy into the key and the attribute into the ciphertext. CP-ABE (ciphertext policy) embeds the policy into the ciphertext and the attribute into the key. These two schemes have a dual relationship in structure, so analogy transfer is often carried out in the scheme design, but they are very different in their specific application scenarios.

NuLink chooses CP-ABE, because the policy is embedded in the ciphertext. This means that the data owner can decide which attributes can access the ciphertext

by setting the policy, which is equivalent to making an encrypted access control for this data whose granularity can be refined to the attribute level.

2.2.4 Fully Homomorphic Encryption

Fully Homomorphic Encryption (FHE) refers to the ability to calculate ciphertext without the private key. That is to say, for any valid f and plaintext m, there is a special property $f(Enc(m)) = Enc(f(m))$.

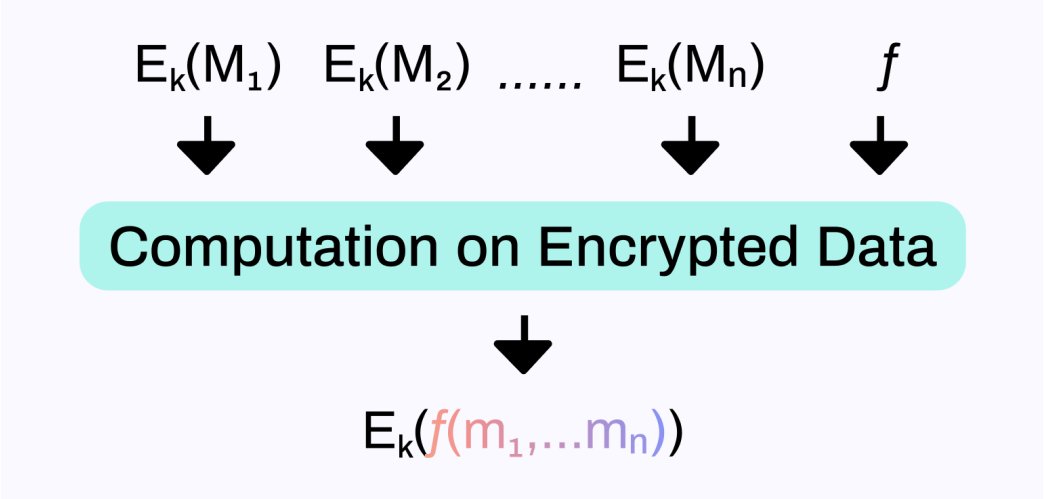

Figure 5: *Fully Homomorphic Encryption (FHE)*

FHE is known as the holy grail of cryptography. This problem was proposed by Rivest in 1978. Thirty-odd years later, in 2009, Craig Gentry constructed the first FHE scheme.

At present, secure and efficient FHE schemes are based on the LWE problem and Ring-LWE problem on lattice. They are anti-quantum and can provide sufficient security even in the post-quantum era.

Fully Homomorphic Encryption is restricted by efficiency, which mainly depends on the operation mode of ciphertext. While FHEW and TFHE cryptosystems are more suitable for dealing with boolean logic operations, BGV, BFV and CKKS are more suitable for batching and calculating affine transformations. For nonlinear

arbitrary functions, the latest PBS technology has a good efficiency performance. Therefore, NuLink will build different FHE algorithms to improve efficiency.

Fully Homomorphic Encryption has a wide range of theoretical and practical applications, especially in decentralized privacy-preserving products.

Nodes in the system whose computing power is not strong enough can store their data in the Storage Layer in the form of ciphertext. When data computing is needed, the user initiates computing authorization to the computation nodes. The computation nodes carry on the corresponding ciphertext operation to get the encrypted result, the user downloads the result and decrypts it, and then the final plaintext result can be obtained. In the whole process of computing, only the owner of the data has the ability to decrypt, so users can be guaranteed data privacy.

We need to emphasize that this can be used as a component of multi-party secure computing, rather than just completing the proxy computation of two parties.

2.3 Solutions

2.3.1 Data Availability

At our core, we are committed to safeguarding data privacy. One of our primary objectives is to address the issue of data availability, which is typically divided into two parts. Firstly, we strive to provide consumers with the means to ascertain that the seller has the required data before making a request. Secondly, we aim to establish a mechanism for verifying the authenticity of the data in its encrypted form.

Within the NuLink network, Zero-Knowledge Proof is used to ensure that all functional nodes, including storage nodes, computing nodes, and proxy nodes, have publicly verifiable data processing and computing operations. At the same time, prior to authorizing data access, the data owner is required to present a Zero-Knowledge Proof. This proof verifies that the encrypted data is aligned with its plaintext counterpart, irrespective of the encryption scheme in use. This approach endows NuLink networks with enhanced flexibility.

2.3.2 Data Sharing

An additional challenge we need to address is how to maintain data security during transmission to other parties. Specifically, We must ensure that data remains uncompromised during transmission, and that it is only accessible to authorized individuals approved by the data owner.

NuLink addresses this challenge by leveraging proxy re-encryption, identity-based encryption, and attribute-based encryption. Initially, data is encrypted at the user-end, and access to the data is granted to authorized parties using the PRE, IBE, or ABE algorithms. Receivers can then decrypt the data using their private key as appropriate. Throughout this process, only the data owner and authorized parties can access the original data, ensuring its confidentiality and security.

2.3.3 Data Computing

The last issue we are trying to address is privacy concerns related to data computation. In certain scenarios involving edge computing or machine learning, the individual who owns the data may only wish to grant access for computing purposes on a specific model. As a result, the authorized party would only receive the computed result and not the original dataset.

NuLink will utilize FHE technology to enable privacy-preserving data computation. This approach leverages the unique property of Fully Homomorphic Encryption, which enables calculations to be performed on ciphertext. Initially, the dataset will be encrypted and transmitted to the computing providers. The computing providers will then execute the desired computation, such as a prediction model for machine learning. Ultimately, the encrypted result will be returned to the authorized party for decryption.

2.4 Workflow

For example, user A has database D, and user B wants to use A's database for machine learning computing. User A provides data, but does not want any participant

(including B) to have access to their database, requiring that B can only access the calculation results.

- **Setup:** When entering the network, the Cryptograph Layer generates a symmetric key and a homomorphic key pair for all users. The public key will be open. These keys can be updated at any time, and the user's ciphertext data needs to be updated synchronously.
- **Application Layer:** User A uses the Application Layer to select the data computing service and authorizes the Cryptograph Layer. At the same time, A sends a transaction to the Blockchain Layer, specifies the nodes on which it requests the service, and pays the service fee.
- **Blockchain Layer:** Checks and broadcasts transactions in the corresponding blockchain.
- **Cryptograph Layer:** The Cryptograph Layer interacts with the Storage Layer, encrypts the database with the symmetric key, encrypts the symmetric key with the homomorphic public key, and uploads a ciphertext. The advantages of symmetric encryption are high encryption and decryption efficiency, small size and low bandwidth occupation. At the same time, the Cryptograph Layer initiates a computation request to the computing nodes.
- **Computing Network:** The computing nodes will receive the ciphertext and perform homomorphic decryption first. This operation can convert the symmetrically encrypted ciphertext into homomorphic encrypted ciphertext and continue its machine learning calculation. The correctness and security of the calculation are guaranteed by homomorphic encryption technology. The calculation results are in ciphertext form, which can only be decrypted by user A so the computing node sends a re-encryption request to the Proxy Network.
- **Proxy Network:** The Proxy Network is the union of several Proxy nodes who will provide proxy re-encryption services. At this point, the ciphertext will be converted into a new ciphertext that user B can decrypt directly. This is guaranteed by proxy re-encryption technology. For proxy re-encryption requests in Polkadot or other ecosystems, we build the Watcher Network.

- **Watcher Network:** The Watcher Network will relay the information of staking nodes from Ethereum to other ecosystems. When this happens, the proxy re-encryption implemented through NuLink network can be reflected in other ecosystems.
- **Cryptograph Layer (B side):** In this step, the ciphertext is transmitted to the Cryptograph Layer on the B side, and the computing result can be obtained after decryption.
- **Application Layer (B side):** After receiving the calculation result sent by the Cryptograph Layer, the Application Layer can show it to B.

Figure 6: *Workflow*

3. Participants

The NuLink network consists of two primary groups of participants: Service Providers and Service Users. Service Providers are nodes that offer a range of services within the network and can be further classified as Proxies, Computing Providers, Watchers, or Storage Providers, depending on the type of service they offer. Users are participants who utilize various resources within the NuLink network and can be grouped as either Data Providers or Data Consumers. The following parts furnish a comprehensive explanation of each participant type and their corresponding functions in the network.

1. **Proxies:** Proxies within the NuLink network are responsible for supplying re-encryption services. To achieve this, they must register and stake NLK tokens for a defined duration. Proxies earn compensation for their services, which includes NLK tokens and other tokens based on the blockchain they serve. In the event that they breach the protocol, Proxies are liable to be 'slashed'.
2. **Computing Providers:** Computing Providers in the NuLink network provide privacy computing services. They are required to stake a proportional amount of NLK tokens for a specific duration and stay online to obtain rewards. The rewards comprise NLK tokens, including a fixed reward and service fees received

during the service period. Similar to Proxies, Computing Providers are susceptible to being 'slashed' for non-compliance with the protocol.

3. **Watchers:** Watchers are nodes with the responsibility of transmitting registration details of Service Providers from Ethereum to other blockchains. The Watcher Network will be under the supervision of an on-chain governance mechanism (DAO). To qualify for the Watcher election, candidates must stake NLK tokens. Watchers receive rewards in Ethereum for monitoring NuLink's staking contract and conveying up-to-date information to other blockchain systems. Similar to Proxies and Computing Providers, Watchers can be 'slashed' if they breach the protocol.

4. **Storage Providers:** Storage Providers in the NuLink network offer decentralized storage services and capabilities. Additionally, the network has the potential to support third-party decentralized storage, and rewards are provided in NLK tokens as an incentive.

5. **Data Provider:** Data Providers in the NuLink ecosystem are the rightful owners of data and can safely share it with Data Consumers by utilizing the network's privacy-preserving data sharing capability. Moreover, they can also offer their data for a computing model provided by Data Consumers via the privacy-preserving data computing functionality. Data Providers compensate Service Providers through service fees and may charge Data Consumers for access in the off-chain channel (similar to the merchant-tax model, where the merchant pays the tax and the consumer bears it by increasing the product price).

6. **Data Consumer:** Data Consumers within the NuLink ecosystem obtain data. They have the option to either directly request Data Providers to share their data or utilize a computing model that securely uses the Data Provider's data. Data Consumers can engage in on-chain or off-chain trading with Data Providers, with a future plan for an on-chain trading market.

4. Token Economics

4.1 Purpose

The NuLink token serves as an incentive for nodes to offer privacy-preserving services to the entire system and to uphold on-chain governance. Through the tokenomics design, all participants of the decentralized network contribute to the NuLink network in a sustainable manner. This design guarantees the following aspects:

1. Security of the system
2. Sustainable development of the system
3. Protection of the interests of all parties
4. Building a thriving multi-ecosystem encryption service.

4.2 Token Functions

In the NuLink network, NLK tokens serve several primary functions, including:

1. **Collateral**: In the NuLink network, Providers such as Proxies, Watchers, Computing Providers, and Storage Providers are required to stake NLK tokens as collateral in order to offer their services and receive corresponding rewards. However, by doing so, they also assume the potential risk of having their staked NLK tokens slashed as a penalty for violating the protocol.
2. **Benefits**: In the NuLink network, Providers such as Proxies, Watchers, Computing Providers, and Storage Providers are incentivized to offer high-quality services by receiving staking benefits in the form of NLK tokens. By providing proper and reliable services, Providers can earn rewards in NLK tokens.
3. **Fees**: In the NuLink network, NLK tokens are utilized as service fees for users who require secure data storage, secure data sharing, or secure data computing services. These users must pay the corresponding Providers using NLK tokens in exchange for access to the desired services.

4. **Voting:** NLK tokens play a critical role in the on-chain governance mechanism (DAO) of the NuLink network, specifically in the election and voting process. Holders of NLK tokens can cast their votes on proposals related to the network's development and operation. This use case emphasizes the importance of NLK tokens as a means of participating in the decision-making process of the NuLink network.

4.3 Token Distribution and Mining mechanism

NuLink's token symbol is NLK. The total supply of NLK is 1 billion and it will be generated in five categories: Foundation (15%), BD & Community Incentivization (15%), Core Team Incentivization (15%), Pre-sale (25%) and Stake Mining(30%).

Figure 7: *Token distribution and usage*

The process of token generation in the NuLink network will occur in three distinct periods:

1. **Genesis phase:** The Genesis phase refers to the timeframe from the token generation event (TGE) to the launch of the NuLink mainnet.

2. **Ascension phase:** The four-year period following the launch of the NuLink mainnet is known as the 'Ascension Phase'. During this period, Providers can stake NLK tokens and receive additional rewards in NLK tokens for providing reliable services to the network.

3. **Zenith phase:** The 'Zenith phase' refers to the third phase of the NuLink network that follows the Ascension phase. Its specific details will be determined by the DAO in advance. Nonetheless, Service Providers will continue to be crucial to the network and stake NLK tokens to provide reliable and secure services and gain rewards. This phase is expected to further solidify the position of the NuLink network as a leading provider of secure and decentralized data services.

4.3.1 Genesis phase

The Genesis phase is a crucial period for the NuLink network, as it sets the foundation for the future growth and development of the platform. During this phase, the various categories involved in building and promoting the network will begin to release their respective portions of work.

The Foundation category plays a critical role in the Genesis phase, as it establishes the legal and organizational framework for the network. This includes setting up the governance structure, defining the roles and responsibilities of the different parties involved, and ensuring compliance with regulatory requirements.

Business Development & Community is another essential category during the Genesis phase. It is responsible for building partnerships and relationships with other companies, promoting the platform to potential users, and creating a strong community around the network. This category's work is crucial for the network's success, as it helps to drive adoption and build a robust ecosystem around the platform.

The Core Team category is responsible for the technical development of the NuLink network. They will be working on the network’s core features, including the cryptographic primitives, smart contracts, etc. Their work will lay the foundation for the mainnet launch and the network's future development.

Finally, the Pre-sale category is responsible for marketing and selling the initial tokens that will be used on the NuLink network. This category's work is critical, as it helps to fund the network's development and creates a community of early adopters who are invested in the network's success.

It is important to note that mining will not start during the Genesis phase but will instead begin after the mainnet launch. The preparation period during the Genesis phase is essential to ensure that the NuLink network launches successfully and is well-positioned for future growth and development.

4.3.2 Ascension phase

The predetermined release schedule will be followed to release the remaining locked portions of the Foundation, Business Development & Community, Core Team, and Pre-sale categories. Once the mainnet is launched, stake mining will commence using 30% of the total NLK tokens for this category. By the end of four years, all one billion NLK tokens will have been generated, and the NuLink network will move into the Zenith phase.

Service Providers on the NuLink network are rewarded through two means: staking profit and service bonus. Staking profit serves as an incentive for Providers based on their staked amount and is generated through the stake mining process. On the other hand, service bonus is intended to encourage Providers based on their performance and is generated from the service fees paid by Data Providers to the system.

4.3.2.1 Staking profit distribution

To begin staking on the NuLink network, a staker must first select a service to provide, choosing one role from the four categories (Proxies, Computing Providers, Watchers, and Storage Providers). Staking rewards earned by the staker will be distributed among these roles and will depend on both their staking amount and the service they offer.

During each epoch, the NuLink network will assess a staker's contribution based on their valid staking amount. If a staker is not providing the service during a specific period of time within the epoch, their contribution will not be considered valid for that period. Consequently, their valid staking amount will only take into account the period in which their service is online. This amount can be calculated as:

$$s_i^V = \frac{L_i}{E_j} * S_i$$

s_i^V: valid staking amount of staker i

L_i: duration of the service the staker i provide for the current epoch

E_j: total duration of the current epoch j

S_i: staking amount of the staker i

And here $\frac{L_i}{E_j}$ is called the living ratio of staker i in epoch j,and is initially set to 1 for all stakers. Once the online checking mechanism is deployed, it will be updated accordingly.

Figure 8: *Valid staking amount*

The valid staking quota attributed to staker i is determined by the proportion of their valid staking amount to the overall valid staking amount in the relevant category, and it can be calculated as follows:

$$P_i = \frac{s_i^V}{\Sigma_j s_j^V}$$

P_i: the valid staking quota of the staker j

s_i^V: valid staking amount of staker i

s_j^V: valid staking amount of staker j, here Σ_j means summary of all staker from the same category in the current epoch.

The staking profit allocated to a staker j is proportional to his valid staking quota and the staking reward assigned to a particular category. This can be computed as follows:

$$R_j^S = \sigma_i * B_k * P_j$$

R_j^S: the total staking profit allocate to a staker j

σ_i: the system adjust coefficient. σ_1 is the reward portion for Proxies, σ_2 is the reward portion for Computing Providers. σ_3 is the reward portion for Watchers. σ_4 is the reward portion for Storage Providers. The staker j needs to choose one when he starts staking. And we have $\sum_{i=1}^{4} \sigma_i = 1$

B_k: the base Reward for current epoch k. And we have $\sum_{k=1}^{210} B_k = 300,000,000$,which means the total mining reward for the Ascension Phase is 30% of the total supply.

P_j: the valid staking quota of the staker j

Figure 9: *The staking profit distribution*

4.3.2.2 Service bonus distribution

Each time a user utilizes a service on the NuLink network, they are required to pay a service fee that is collected by the NuLink Treasury account. Initially, the NuLink Foundation manages this account, but it will be later shifted to NuLink DAO. The collected fees are classified as service bonus and are periodically distributed to the service providers. The period, referred to as a batch, will consist of several epochs and its length will be determined by DAO at a later stage.

The total service bonus of one batch will be divided into three parts:

1. Stakers (80%): This part will be given to the stakers according to their reputations in the near history.

The reputations can be quantified as:

$$V_i = \frac{N_g}{N_t}$$

V_i: the reputation score of staker i in the current batch.

N_g: the count of good behavior epochs in the current batch. We will set a threshold living ratio, and good behavior means the living ratio of staker i is higher than the threshold in an epoch (the threshold is set to 0.8 at the beginning, and DAO can change it later).

N_t: the count of the total epoch of the current batch.

The bonus of service provider i can be calculated as:

$$R_i^B = \frac{V_i}{\Sigma_j V_j}$$

R_i^B: the service bonus allocated to the staker i

V_i: the reputation score of staker i in the current batch

V_j: the reputation score of staker j in the current batch, here Σ_j means summary of all staker in the current batch

2. NuLink Foundation (15%): This portion will be given to the NuLink Foundation to maintain the sustainable development of the system.

3. Burning (5%): This portion will be burned to reduce the total supply of NLK tokens.

4.3.3 Zenith phase

In the Zenith phase, NLK tokens will be generated exclusively through the process of stake mining. However, the staking mechanism to be employed must be determined in advance by the NuLink DAO, which is elected by the community.
During this phase, the NuLink DAO will play a crucial role in network governance, ensuring that it remains decentralized and responsive to the requirements of its users. By empowering the community to select its leaders and determine the staking mechanism, the NuLink network will be able to adapt to evolving market trends and remain at the forefront of innovation in the decentralized data services industry.

5. On Chain Governance (DAO)

NuLink utilizes a Decentralized Autonomous Organization (DAO) to govern different aspects of the project, including token distribution, network upgrades, and decision-making procedures. The NuLink DAO is a democratically structured organization where all NLK holders are members. Meanwhile, each member's voting power is proportional to their staked NLKs. This ensures a fair and decentralized decision-making process that is not under the control of a single entity or individual. A quorum threshold model is employed to determine the number of votes required for a proposal to be approved. NuLink Foundation retains the power of explanation.

The DAO voting process consists of four main steps: Proposal, Approval, Referendum, and Execution:

1. **Proposal:** In this first step, any member of the DAO can submit a proposal for consideration. The proposal should outline a specific action, such as a network upgrade or token distribution. The proposal must also include a detailed explanation of the proposal's purpose and expected impact.
2. **Approval:** Once a proposal is submitted, it moves to the Approval stage. During this stage, members of the DAO can vote to approve or reject the proposal. Each

member's voting power is determined by their staked NLKs. To pass, a proposal must reach a quorum threshold.

3. **Referendum:** If a proposal does not reach the quorum threshold during the Approval stage, it moves to the Referendum stage. During this stage, the proposal is opened up to the entire community for voting. This stage allows for a more democratic decision-making process and ensures that all community members have a voice in important decisions.
4. **Execution:** Once a proposal has been approved and passed, it moves to the Execution stage. During this stage, the action outlined in the proposal is carried out. For example, if the proposal was for a network upgrade, the development team would implement the upgrade according to the proposal's specifications.

Overall, the voting process is designed to promote transparency, fairness, and decentralization in decision-making within the NuLink community. By allowing members to have a say in important decisions, the DAO ensures that the network remains responsive to the needs and interests of its users.

6. Application Scenario

6.1 Encrypted NFTs Trading Market

In order to conduct secure NFT trading, the transaction is divided into two parts. The payment and the transfer of NFT ownership needs to be completed on-chain. The NFT transmission needs to be completed synchronously and securely under the chain. Alice first encrypts and uploads her NFT resources to the NuLink network through NuLink’s proxy re-encryption function so that the NFT can be safely transmitted to Bob. The encrypted NFT data of Alice and Bob are written into the blockchain by mint operation. This step completes the transfer of the NFT ownership on the chain.

Figure 10: *Encrypted NFTs trading market*

6.2 Privacy-Preserving Social Network

A Privacy-Preserving Social Network can be built on the NuLink network. The user could start an end-to-end encrypted group messaging, and members can easily be added or removed from the chat by granting or revoking access. The NuLink solution will avoid the overhead of encrypting and sending messages multiple times individually to each participant. Furthermore, the user can also share a post only with a certain group of people without worrying about information leaking, especially to the owner of the social network.

6.3 Decentralized Digital Rights Management

The Decentralized Digital Rights Management platform can be deployed on the NuLink network. The owner of a digital asset can register their ownership in blockchain. After registration, they can encrypt their digital asset and publish the encrypted version of their digital asset in the storage network. Those who want to buy this digital asset could pay the owner in exchange for temporary access to the digital asset. In the whole process, only the owner and the buyer can access the digital asset.

6.4 Electronic Health Records Sharing

A robust Electronic Health Records Sharing platform can be constructed upon the NuLink network. The patient who owns the health records and encryption keys is the data provider. Their health records will be encrypted and stored in a decentralized storage network. The patient will have control over who will access their data. They can grant secure access to others such as hospitals or insurance companies.

6.5 Automotive Data Sharing

A car owner or user needs to be able to share their car data with a third party — perhaps an insurance company so that they can get reduced insurance premiums or a MaaS (Mobility as a Service) company to resolve a dispute. Obviously the data owner will not want any other third party to access their data during the transfer process.

Right after the data has been read out from the OBD port, the data will be encrypted from the endpoint and sent over the air to the enterprise level server, through

NuLink’s proxy re-encryption function. The encryption key will be granted to the insurer or MaaS company automatically before the car owner even starts the car.