NuLink Whitepaper 1.1

November 13, 2021

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 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. For the data user on the other side, Zero-Knowledge Proof can help them verify the data source. In more advanced privacy-preserving use cases, NuLink uses Fully Homomorphic Encryption to customize 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

By integrating best-in-class technologies we are building a strong technology foundation. The technical solutions provided by NuLink cover three main categories.

- To ensure the availability of data in ciphertext form. The crypto techniques used here mainly include Zero Knowledge Proof.
- 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, which 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 kinds of technical solutions can provide privacy-preserving applications in many fields, such as Decentralized Finance (DeFi), healthcare, social networks, Digital Rights Management, etc.

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.

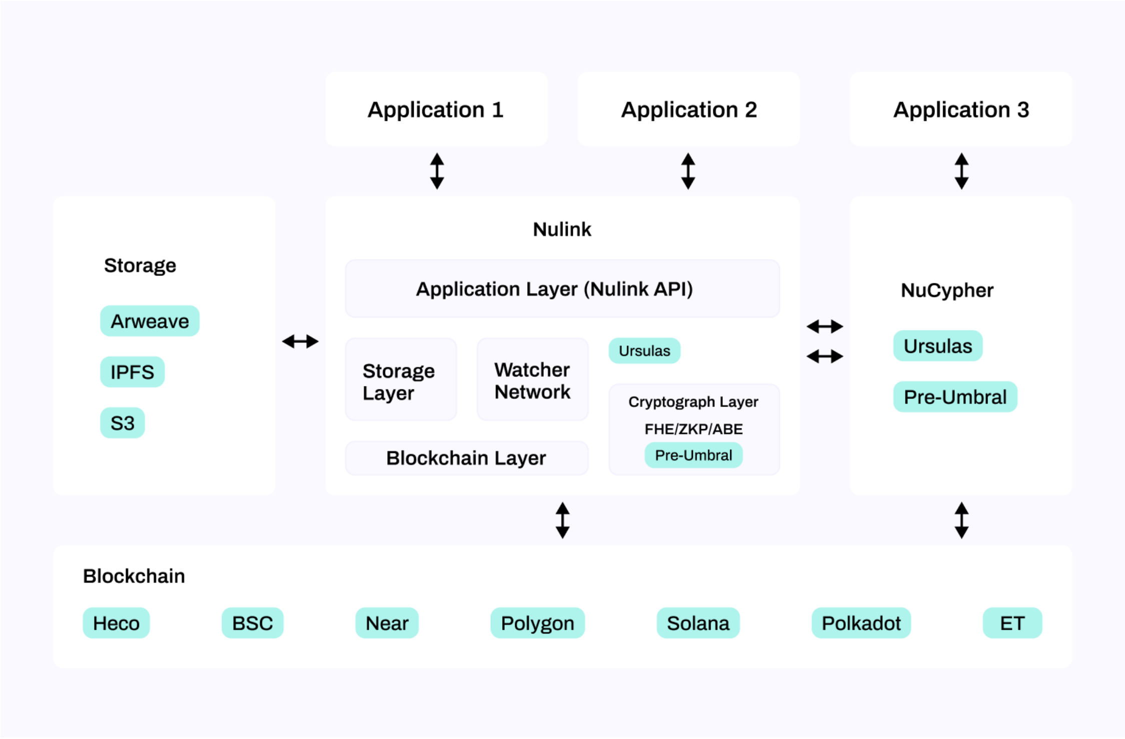


Figure 1: NuLink Network

1. The Application Layer: The Application Layer is an abstract interface layer that directly interacts with the application. The Application Layer also needs to interact with the Cryptograph Layer to grant authorization of the application's privacy data.
2. The Cryptograph Layer: The Cryptograph Layer is an entity that handles cryptographic operations on behalf of the Application Layer. The cryptographic operations include key generation, encryption, decryption, etc. The Cryptograph Layer also needs to connect to the Storage Layer and is responsible for uploading and downloading the encrypted privacy data.
3. The Storage Layer: The Storage Layer is a storage network that can be used to store encrypted privacy data. Currently, we support IPFS (InterPlanetary File System) as our decentralized storage network. Other storage networks such as Swarm and S3 will be available soon.
4. The Blockchain Layer: The Blockchain Layer is the blockchain system that can handle the proxy registration and re-encryption request management. Currently, proxies can register in Ethereum only. However, the user could send their requests to other blockchain systems such as Polkadot and Solana.
5. The Watcher Network: The Watcher Network is a relayer network that relays the information of proxy nodes from Ethereum to other blockchain systems. The Watcher Network will be maintained under an on-chain governance mechanism (DAO) to guarantee its decentralization and security.

NuLink users can simply integrate into one single API and get access to multiple storage and blockchain solutions. Miners can get NuLink's token (NLK) in the Storage Layer by providing decentralized storage services and also in the Watcher Layer by relaying information from ETH.

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, Fully Homomorphic Encryption, Zero-Knowledge Proof 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 or 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.

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.

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:

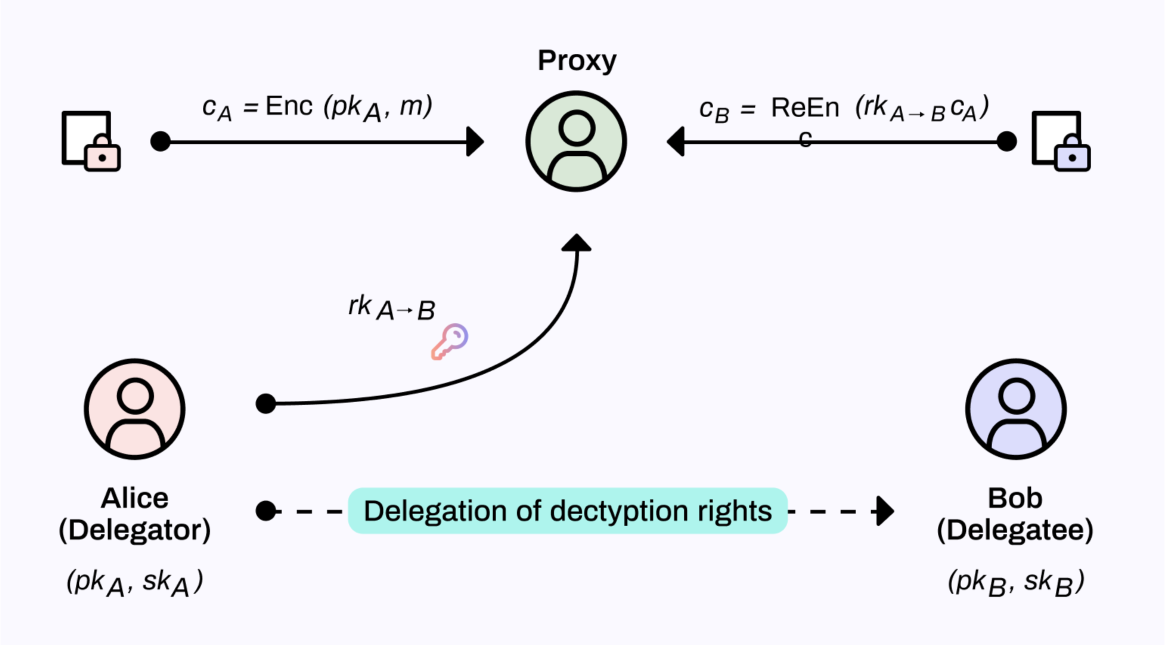

Proxy
c_A = Enc (pk_A, m)
c_B = ReEn ($rk_{A \to B}$ c_A)
c
$rk_{A \to B}$
Alice
(Delegator)
(pk_A, sk_A)
Delegation of dectyption rights
Bob
(Delegatee)
(pk_B, sk_B)

Figure 2: Proxy Re-encryption

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 NuCypher's 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 NuCypher 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.

Identity-based encryption 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.

On this basis, attribute-based encryption 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 $f(Enc(m)) = Enc(f(m))$.

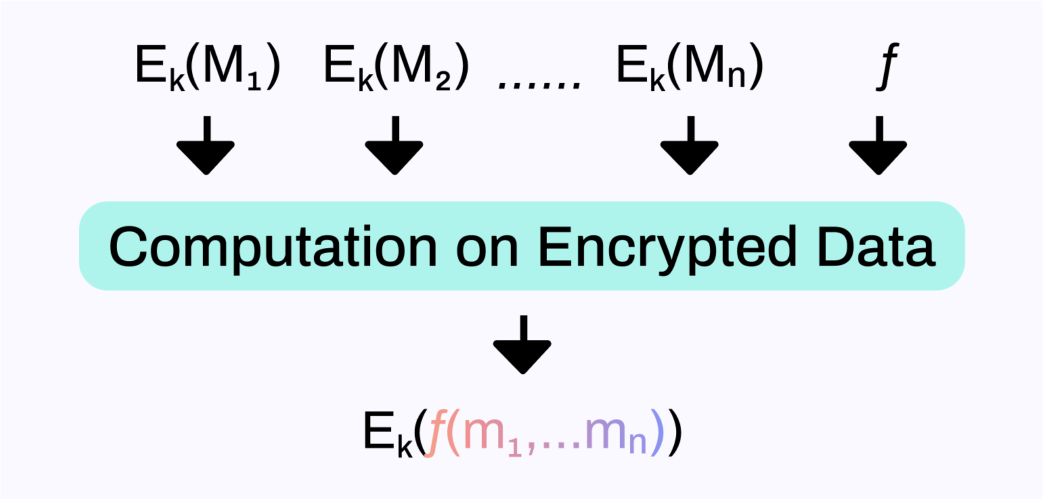


Figure 3: Fully Homomorphic Encryption

Full homomorphic encryption 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 fully homomorphic encryption scheme.

At present, secure and efficient fully homomorphic encryption 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.

At present, 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 fully homomorphic encryption 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

As a platform focused on data privacy, the first thing we need to solve is the problem of data availability. This problem is often divided into two parts: the first is how consumers can determine that the seller has the data they need before purchasing, and the second is how to verify that the data in the ciphertext state is true.

In the NuLink network, these two problems can be solved by Zero-Knowledge Proof technology: the data owner needs to provide Zero-Knowledge Proof before data authorization. In fact, the method of proof in the ciphertext data state is consistent with that in the plaintext state, which is independent of the encryption scheme used. This provides higher flexibility for NuLink networks.

2.3.2 Data Sharing

The data sharing functionality of NuLink is realized by bridging the proxy re-encryption technology to the blockchain system. This is a feature that NuLink will deploy first, and IBE and ABE will be added to this solution later. This solution can be applied in many scenarios.

First, Alice calls the Application Layer through APP on the IoT device, selects the proxy re-encryption service and authorizes. On Alice's NuLink side, after receiving the authorization, the Application Layer invokes the Blockchain Layer to initiate and verify the transaction, and transfers data to the Cryptograph Layer. The Cryptograph Layer interacts with the Storage Layer to perform encryption operations and upload the encrypted data. The encrypted data obtained at this step can only be decrypted by Alice. In order to convert it into ciphertext that can be decrypted by Bob, we implement proxy re-encryption through Ursula nodes deployed by NuCypher. After re-encryption, the encrypted data will be sent to the Cryptograph Layer in Bob's NuLink side and can be decrypted directly.

2.3.3 Data Computing

The data computing functionality of NuLink will be realized by bridging the fully homomorphic encryption technology to the blockchain system in the future.

It takes advantage of the property that full homomorphic encryption can be used to calculate ciphertext, that is, the user selects the data computing service in the Application Layer. After receiving the authorization, the Cryptography Layer homomorphic encrypts and uploads the user's data to the Storage Layer. The computing node of the Blockchain Layer will access the data and perform the specified calculation (such as machine learning model prediction, etc.). Finally, the ciphertext result is returned to the Storage Layer, and the Cryptography Layer accesses the ciphertext result, which is decrypted and returned to the user. We will add MPC (multi-party computation) to this solution later.

2.4 Work flow

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:** At present, the Proxy Network we use is NuCypher's Ursula network. In the future, we will build NuLink's own Proxy Network according to

our requirements. For proxy re-encryption requests in ETH, through Ursula nodes deployed on ETH by NuCypher, we can directly 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 Ursula nodes from Ethereum to other ecosystems. When this happens, the proxy re-encryption implemented through Ursulas 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.

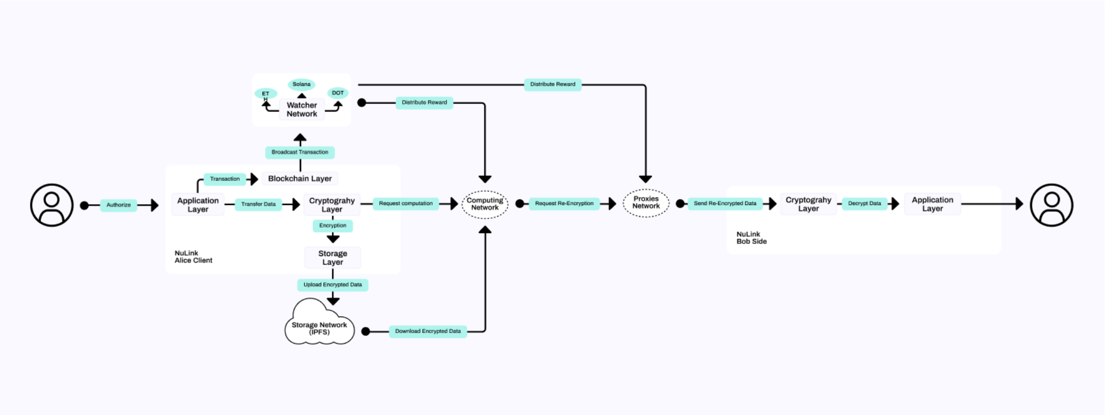


Figure 4: Work Flow

3. Participants

There are multiple participants in the NuLink network. They can be classified into two major categories: Providers and Users. “Providers” are nodes that provide different services in the NuLink network. According to the type of service provided, Providers can be classified as Proxies, Computing Providers, Watchers, Storage Providers. “Users” are participants who use various resources in the NuLink network and can be classified as Data Providers and Data Consumers. Below, we elaborate on these terms.

1. **Proxies:** In the NuLink network, Proxies play the same role as the Ursula nodes in NuCypher. They need to register and stake NuCypher (NU) tokens for a certain period. They will provide re-encryption service for users in the locking period. They can get rewards in return for their services. Their rewards include two components: NU tokens as a constant reward and other tokens as a service fee depending on which blockchain the Proxies serve for (Ethers in Ethereum and NLKs in other blockchain). Proxies will get slashed if they violate the protocol.

2. **Computing Providers:** Computing Providers are nodes that provide homomorphic encryption services in the NuLink network. They are required to stake a corresponding amount of NLK tokens for a certain period and stay online in order to obtain a reward. The rewards are distributed in NLKs and are composed of two parts: A constant reward, and service fees collected in the service period. The Computing Providers also bear the risk of being slashed if they violate the protocol.

3. **Watchers:** Watchers refer to the nodes that take responsibility for relaying the registration information of Proxies from Ethereum to other blockchains. NuLink will build an on-chain governance mechanism (DAO) to manage the Watcher Network. Candidates who are willing to become Watchers need to stake NLKs first to be eligible for the Watcher election. The tokens from candidates who win the election will be locked for an epoch and stay online for the whole epoch. Those who fail in the Watcher election can retrieve their staked NLKs. Watchers are requested to monitor NuCypher’s staking contract with Ethereum and deliver the updated information of Proxies to several blockchain systems (Polkadot, Solana, Near, etc). They can get a constant rate of reward by providing such a service. Watchers will be subject to the slash-in-case-of-misbehaviour rule as well.

4. **Storage Providers:** Storage Providers are nodes in the network that provide decentralized storage capabilities and storage services for the NuLink network. The NuLink network supports third party decentralized storage and will incentivize the storage network in NLKs.

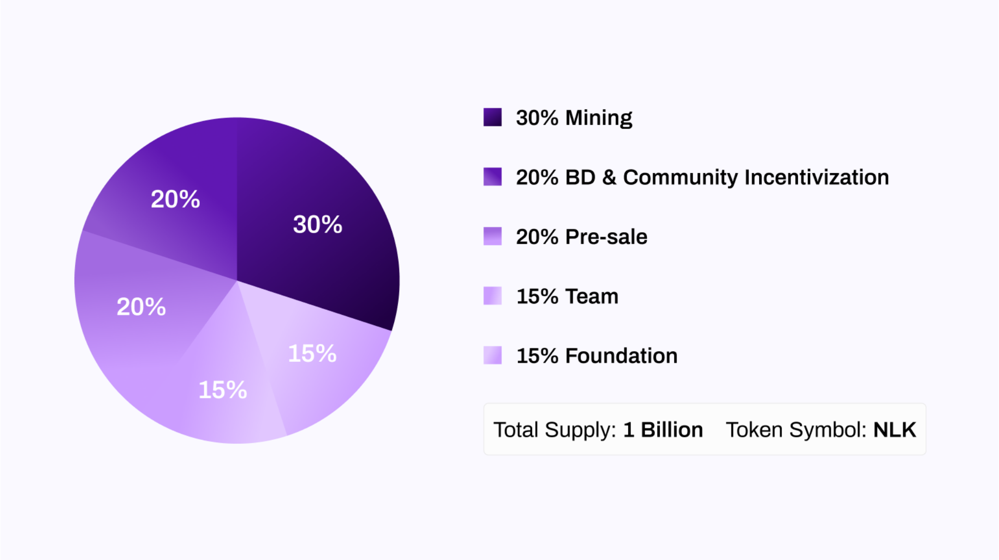
5. **Data Provider:** A Data Provider is the owner of the data in the NuLink Ecosystem. They can share their data securely with Data Consumers using the privacy-preserving data sharing functionality of the NuLink network. They can also provide their data for a computing model provided by Data Consumers through the privacy-preserving data computing functionality. We need to mention here that Data Providers need to pay service fees to Providers and could charge Data Consumers for this portion in the off-chain channel.

6. **Data Consumer:** A Data Consumer is the receiver of the data in the NuLink Ecosystem. They can request the Data Provider to share the data directly or can provide a computing model to use the Data Provider's data in a secure manner. They can trade with Data Providers in exchange for the access of data either on-chain or off-chain. NuLink plans to provide an on-chain trading market in the near future.

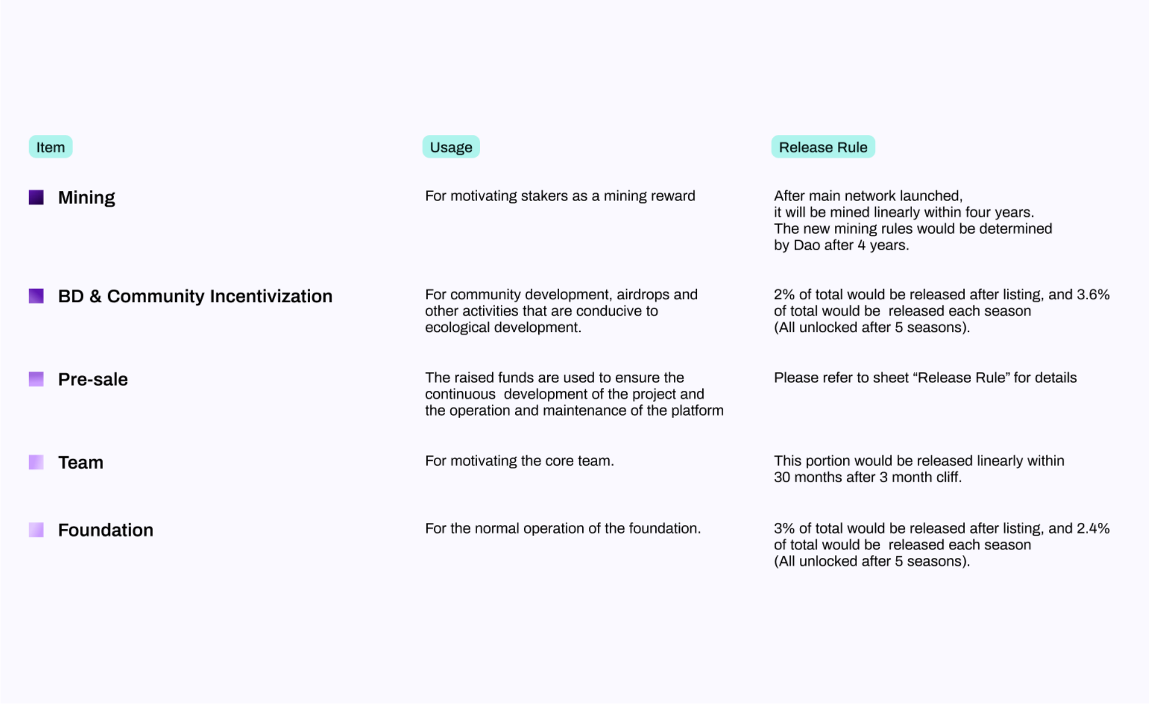
4. Token Economics

4.1 Token Generation and Distribution

NuLink's token symbol is NLK. The total supply of NLK is 1 billion and it will be generated in two stages: pre-allocation and stake mining after the mainnet launch.



The pre-allocation of NLK can be classified into four categories: Foundation (15%), BD & Community Incentivization (20%), Core Team Incentivization (15%) and Pre-sale (20%). After the mainnet is launched, the remaining 30% of the total supply will be mined by Providers in the NuLink network within four years. After four years, the new mining rules will be determined by the on-chain governance mechanism (DAO) maintained by the community. The detailed information of the token distribution can be found in the following scenarios: For NLK tokens generated before the NuLink mainnet, smart contracts will be provided to allow NLK holders to transfer tokens to the mainnet at a one-to-one ratio after the mainnet goes live. In the mainnet stake mining mechanism, if a node is found to be malicious or providing unstable service quality, it will be penalized. Their NLK tokens will be slashed, with a portion directly destroyed and the rest sent to a treasury account maintained by DAO. Also, for any service-related transaction in the NuLink network, a portion of basic fees will be destroyed, and the remainder will be distributed to the Providers.



Item	Usage	Release Rule
■ **Mining**	For motivating stakers as a mining reward	After main network launched, it will be mined linearly within four years. The new mining rules would be determined by Dao after 4 years.
■ **BD & Community Incentivization**	For community development, airdrops and other activities that are conducive to ecological development.	2% of total would be released after listing, and 3.6% of total would be released each season (All unlocked after 5 seasons).
■ **Pre-sale**	The raised funds are used to ensure the continuous development of the project and the operation and maintenance of the platform	Please refer to sheet "Release Rule" for details
■ **Team**	For motivating the core team.	This portion would be released linearly within 30 months after 3 month cliff.
■ **Foundation**	For the normal operation of the foundation.	3% of total would be released after listing, and 2.4% of total would be released each season (All unlocked after 5 seasons).

4.2 Token Functions and Values

In the NuLink network, NLK tokens have the following main functions. They will be:

1. Used as the staking collateral for different kinds of Providers (Proxies, Watchers, Computing Providers, Storage Providers). Providers need to stake NLKs in the NuLink network to provide services and obtain benefits. Meanwhile, they will bear the risk of NLK slashing in the case of a penalty.
2. Used as the staking benefits for different kinds of Providers (Proxies, Watchers, Computing Providers, Storage Providers). If the Providers provide proper services in the NuLink network, they will be rewarded with NLKs.
3. Used as the NuLink network's service fees. Users in NuLink who want to use the service (secure data storage, secure data sharing or secure data computing) need to pay fees to the corresponding providers.
4. Used in the election and voting of the on-chain governance mechanism (DAO). NLK is used to vote on proposals.

NLK is the utility token of the NuLink network. Its value is positively correlated to the scale of the NuLink network. The demand and value of NLKs may increase in the following scenarios:

1. When more decentralised apps (DApps) are developed in the NuLink network ecosystem and more users will use the NuLink network.
2. When more DApps are developed in the NuLink network ecosystem and the commercial applications built on these (encrypted NFTs trading market, secure sharing of data collected by IOT devices, joint medical data analysis, financial encrypted data prediction, inquiry of credit history, privacy-preserving social network, decentralized digital rights management, etc) will lead to an increase in the demand for NLKs.
3. When the total amount of NLKs in circulation will decrease because they are being used or locked up in the network. For example, while staking or voting for on-chain governance.
4. When events take place that cause the total amount of tokens to reduce. This includes slashing, transaction fees, token burning, etc.

5. Application Scenario

5.1 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.

5.2 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 for 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.

5.3 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.

5.4 Encrypted NFTs

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.

5.5 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.

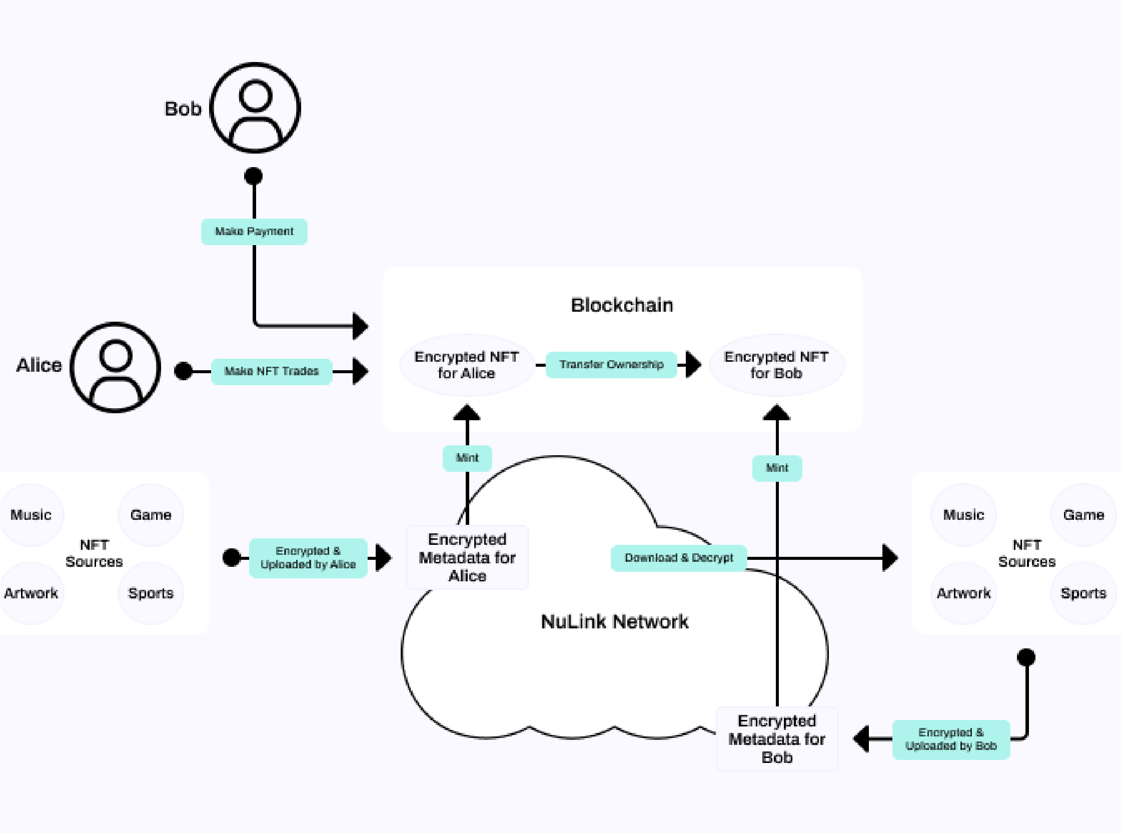


Figure 5: Encrypted NFT

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.