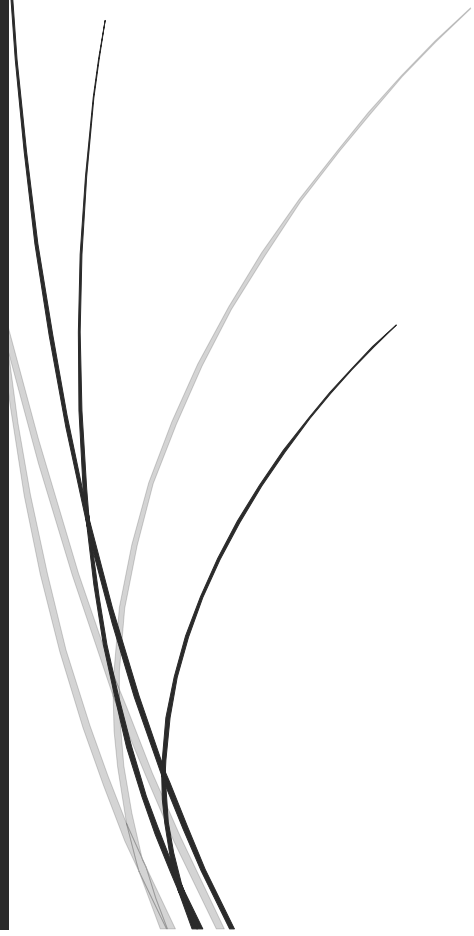
WhitePaper

# DNA

**DNA Network is a link between blockchain and the real world.**



Joye

# INDEX

## SUMMARY

Over the past few years, blockchain has been looking to solve real-world problems and introduce traditional markets as incremental markets. However, many projects have failed in their attempts due to the following main reasons:

- Blockchain relies on oracles to obtain information. However, centralized or multi-centralized oracles are vulnerable to attacks and malicious operations. If the accuracy of the original data cannot be ensured, the practical application of blockchain technology will lose its value.
- There is currently a lack of effective technical solutions to ensure that the physical objects corresponding to the data on the blockchain have not been replaced or counterfeited.

As a bridge between the new generation of blockchain and the real world, DNA is a blockchain application that puts real-world tangible assets (luxury goods, ceramics, calligraphy and paintings, antiques, handicrafts, crafts, etc.) on the chain to solve the above problems. Two revolutionary technical solutions were launched to solve the problem. First, a microscopic fingerprint image magnified by N (N ≥ 180) times on the surface of the physical object is captured through an "intelligent forensic instrument" and uploaded to IPFS storage. The information is then aggregated through a real-name authenticated public chain account and minted into NFT. When verifying, take a microscopic image of the same location and the same multiple of the physical object, and compare it with the fingerprint image of the NFT using an artificial intelligence algorithm to ensure that the physical object corresponding to the data on the chain will not be forged or replaced and that the blockchain oracle will easily receive it. The problem of original data accuracy caused by attacks or subjective evil will bring trillions of real-world assets into the blockchain world.

## BLOCKCHAIN HISTORY

As early as decades ago, the concept of decentralized digital currency was proposed. In the 1980s and 1990s, anonymous electronic cash protocols began to emerge, most of which were based on Chaumian blinding technology. These protocols offer currencies with a high degree of privacy,

but because they all rely on a centralized intermediary, they have not caught on. In 1998, computer engineer Wei Dai published a paper on "B-money", proposing the idea of creating money by sending digital currency through a set of untraceable digital pseudonyms and achieving decentralized consensus. In 2005, Hal Finney introduced the concept of "reusable proofs of work", which combined the ideas of b-money and computationally difficult hashes proposed by Adam Back. Hashcash puzzle for creating cryptocurrencies. However, this concept again fails due to its reliance on trusted computing as the backend. Although none of these concepts have been widely used, they laid an important foundation for the advent of Bitcoin.

### 1.1 THE BIRTH OF BITCOIN, THE FIRST CRYPTOCURRENCY

On November 1, 2008, Satoshi Nakamoto published a white paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System", detailing the powerful functions of the Bitcoin blockchain network. This day is regarded as an important milestone in the history of blockchain development, paving the way for the subsequent rise of blockchain. The birth of Bitcoin represents the creation of decentralized credit based on mathematical algorithms and cryptography principles.

### 1.2 BITCOIN'S INNOVATIVE CONCEPT

Bitcoin combines a very simple node-based decentralized consensus protocol with a proof-of-work mechanism. Nodes gain the right to participate in the system through a proof-of-work mechanism, packaging transactions into "blocks" every ten minutes, creating an ever-growing blockchain. Nodes with more computing power have greater influence and are much more difficult than creating a million nodes.

### 1.3 THE ARRIVAL OF BLOCKCHAIN 2.0-ETHEREUM

At the end of 2013, Vitalik Buterin proposed a "next-generation cryptocurrency and decentralized application platform" inspired by Bitcoin. Ethereum provides a blockchain with a built-in mature Turing-complete language, allowing developers to easily build and deploy scalable, distributed applications (DApps) for blockchain in finance, energy, artificial intelligence,

etc. Applications in intelligence, agriculture, entertainment IP, big data and other fields have laid a solid foundation.

## 1.4 SMART CONTRACT

The concept of smart contracts comes from cryptologist Nick Szabo, who provides the following definition: “A set of commitments specified in digital form, including an agreement by each party to fulfill other commitments”. The main purpose of a smart contract is to automatically execute the terms of the agreement after specified conditions are met. On the blockchain, a smart contract is defined as “automatically executing code that enforces the terms of an agreement between parties.” Compared with traditional contracts, smart contracts do not rely on a trusted third party to operate, thus reducing transaction costs. The biggest feature of smart contracts is their immutability and deterministic components. Once deployed, smart contract code is immutable and although the contract can be deleted, the transaction history remains embedded in the blockchain in which it resides. The results of a contract are the same for anyone who runs it, not even the creator of the contract has exclusive rights to it. The birth of smart contracts has ushered in the vigorous development of credit rules.

## 1.5 BLOCKCHAIN 3.0-OPENING A CHAPTER IN A NEW ERA

If Bitcoin is seen as the birth of blockchain, Ethereum enables blockchain to run applications. So what will the next generation of blockchain technology be? Some people believe that it breaks through the impossible triangle and continuously improves the security, performance and scalability of the public chain. For example, in 2018, the EOS mainnet was launched, claiming to process more than 100,000 transactions per second (TPS), far exceeding Ethereum's 50TPS, but in the end Ethereum won. This shows that what restricted the next generation of blockchain technology at that time was not breaking through the impossible triangle. Improving the underlying technology could not bring about more application scenarios and usage scenarios. This must still belong to the category of blockchain 2.0. If blockchain 1.0 is a blockchain used by geeks, and blockchain 2.0 is a blockchain used by a few people, then 3.0 should make blockchain applications popular to the vast majority of people in real society. , opening an era of credit construction with

extensive public participation. However, many blockchain implementation projects have not been successful in recent years. The main reason is that they cannot solve the problem of blockchain application implementation.

# PROBLEMS WITH BLOCKCHAIN IMPLEMENTATION

In recent years, the encryption market has experienced a rapid explosion, with the number of projects and the amount of funds increasing hundreds of times. This rise is not accidental, but because blockchain truly solves the pain points of traditional applications and meets market needs. However, according to the most recent year's data, the market has clearly regressed. One of the fundamental reasons is that the current encryption market mainly relies on stock competition. The development of the encryption market has reached a bottleneck. Therefore, it is urgent to expand outward, embrace the real society, link with the real society, and introduce incremental markets. However, in the past few years, many projects have tried hard to embrace the real society and use blockchain to solve real-world problems, but they have all failed in the end. The main problems faced by these projects are oracles (the channel through which the blockchain communicates with the real world) and KYC issues.

## 2.1 ORACLE PROBLEM

### 2.1.1 What is an oracle?

In the blockchain environment, oracles are an important concept that provide information from the real world to the blockchain. The word oracle can also be translated as "oracle". This concept comes from Greek mythology and refers to a person who can communicate directly with God and predict the future. In ancient times, people often faced a lack of information when making decisions and sought incomprehensible knowledge from oracles. By analogy to the blockchain environment, the role of oracles is similar to ancient oracles. They play the role of connecting the blockchain with the real world, converting real-world information into usable data for the blockchain. An oracle is not a specific program or device, but a concept that can include any mechanism that provides external data to the blockchain. These mechanisms can be operated by humans or can be data provided by automated systems or sensors. Oracles pass real-world information to smart contracts, enabling

them to make accurate decisions and perform corresponding operations based on external data. In general, the role of the oracle in the blockchain is to provide information from the real world to the blockchain so that smart contracts can operate more intelligently and flexibly. By analogy with the concept of oracles, we can better understand the role and importance of oracles in the blockchain.

#### 2.1.2 Why do you need an oracle?

If the smart contract does not handle crypto exchanges, but instead handles decentralized mechanisms involving weather, stock prices, or political events, a gateway from the outside world is needed. Due to the consensus mechanism of the blockchain, external information cannot be provided along with the transaction data because other nodes would detect the information coming from "untrusted" sources. Therefore, information from the real world should come from a single source of third parties whose reliability is indisputable for all nodes: oracles.

Oracles typically do not insert information directly into the blockchain, but instead collect and store data from the real world. When a smart contract needs to process external data, the code calls the correct information from a trusted oracle. Oracles can be IoT systems such as sensors and detectors, ERP platforms, or in the case of private data, people operating directly on the blockchain. Oracles act as bridges, converting external and non-deterministic information into a format that the blockchain can understand. Examples of data collected by oracles include lottery winners, natural disasters and risk measurements, prices and exchange rates of physical/crypto assets, static data (such as fingerprint information for products), dynamic data (such as time measurements), weather conditions, geolocation and Traceability information, and events in other blockchains.

#### 2.1.3 Oracle problem

**1. Non-standard data issues**

When an oracle cannot be fully automated, agent intervention is often required to determine whether the observed behavior is correct. This is because some behaviors or data are not standardized, cannot be verified, and require subjective human judgment to evaluate. This uncertainty is called the "oracle non-standard problem".

**2. Failure, attack or subjective malicious issues**

In the case where the oracle is reliable and cannot be destroyed, there are two situations that will cause the data it provides to still be at risk of being tampered with:

Situation 1: The data provided by the oracle machine is credible and verified. Due to the failure of the oracle machine itself or being attacked, the data uploaded to the smart contract is tampered with and cannot operate correctly.

Scenario 2: The oracle machine itself commits evil and uploads tampered data to the smart contract.

From a game theory approach, it can be proven that the higher the value of the smart contract, the higher the incentive for the oracle to be destroyed.

3. The problem of the connection between physical objects and digital assets

When physical assets are mapped to the blockchain through smart contracts, how the physical objects are linked to digital assets (whether art, cars, or houses) is also the core issue that restricts the entire blockchain from embracing the real world. As for physical on-chain issues, we can also divide them into two categories based on the delivery method.

a. Physical objects need to be subject to supervision and assisted delivery in the jurisdiction in which they are located, and they are subject to other things besides smart contracts (such as courts, government agencies). This means trusting something other than smart contracts. For example, if a smart contract involves the transfer of a house property between two agents, the code does indeed exchange certificates between the parties. The previous owner can refuse to leave the home. Without the involvement of a third party (such as a court) that oversees smart contracts, their execution cannot indeed be ensured.

b. Physical objects (crafts) that do not require jurisdictional supervision and are directly traded by individuals. There is no guarantee that the physical object corresponding to the blockchain data is the physical object that has not been replaced or counterfeited.

## 2.2 ACCOUNT REAL-NAME ISSUE

### 2.2.1 What is an Ethereum account?

In Ethereum, an account is a user's identity and is used to store digital assets and smart contracts. Ethereum accounts are divided into two types: Externally Owned Account (EOA) and Contract Account (Contract Account).

①External accounts are controlled by private keys and can send transactions and execute smart contracts.

②Contract accounts are controlled by logic programming in the code. It has no associated private key and cannot execute itself. Although smart contracts can activate other smart contracts, the initial input can only be provided by EOA, and smart contracts can perform operations after receiving transactions from EOA

### 2.2.2 Anonymity and privacy issues

In traditional social activities, names are a window for people to understand each other. Authorization for contracts can be determined through signatures and biometric materials. In the development of the Internet, anonymity has brought about a series of problems, such as illegal transactions and cyber violence, so the Internet has gradually implemented a real-name system. However, the real-name system also raises security and privacy concerns, because personal private data is controlled by Internet giants, who can monitor users' online activities.

Currently, most blockchain projects still use the account system of Bitcoin and Ethereum, in which the identity is a public and private key system with a string of hash values. The anonymity of the blockchain mainly comes from the lack of correlation between addresses and individuals, and the fact that individuals can have multiple addresses. However, this anonymity is actually a kind of "pseudo-anonymity", similar to the "vest" on the Internet. Others have no way of knowing how much of your blockchain assets you have and who you have transferred to. On the blockchain network, only transfer records can be found, but the identity behind the address cannot be directly found. But once you know who the corresponding person is behind the address, you can find all its related transfer records and assets. Therefore, blockchain cannot achieve complete anonymity or complete real-name identification. It is

important to note that blockchain technology can provide better privacy protection and identity management solutions. For example, some projects are studying the use of technologies such as zero-knowledge proofs to achieve stronger privacy protection, so that transactions can be accepted by verification and verifiers while protecting privacy.

To sum up, the anonymity of blockchain is relative. It can provide a certain degree of privacy protection, but it is not completely anonymous. In the process of blockchain development, we need to weigh the balance between privacy protection and identity management to ensure the security of personal data and the improvement of user experience.

#### 2.2.3 The digital world lacks connectivity with the real world

Satoshi Nakamoto once said: "I don't agree that real names are unnecessary. This may be true for Bitcoin, but for blockchain, real names are precisely the biggest challenge faced by blockchain in the field of identity authentication."

There are weaknesses in the blockchain account system. It cannot directly correspond to personal identities in the real world, cannot verify that digital assets belong to real individuals, and is difficult to connect with real social service networks. This is a key issue that hinders the implementation of blockchain in real-world applications.

In industries such as finance and art that require strong identity verification, the lack of user identity verification (KYC) will cause the entire system to fail to operate healthily. In order to solve this problem, many blockchain projects have adopted the following methods for KYC:

①Use a centralized organization to perform user identity verification (KYC):

This method still relies on a centralized third-party organization to perform user verification, and there is a risk of leakage and abuse.

②Use a decentralized organization to perform user identity verification (KYC):

In order to protect the security and privacy of users, this method basically does not store user information and is only used to verify whether they are real people, which cannot meet the needs of strong identity verification.

To achieve seamless connection between blockchain and the real world, the problem of identity verification needs to be solved. DNA is researching

how to achieve strong authentication while protecting user privacy. For example, using technologies such as zero-knowledge proofs can provide better privacy protection and identity verification solutions. At present, blockchain technology is still developing and improving, and solving the identity verification problem is an important step in realizing the implementation of blockchain in real-life applications.

# AN ORACLE BASED ON VISUAL SENSORS

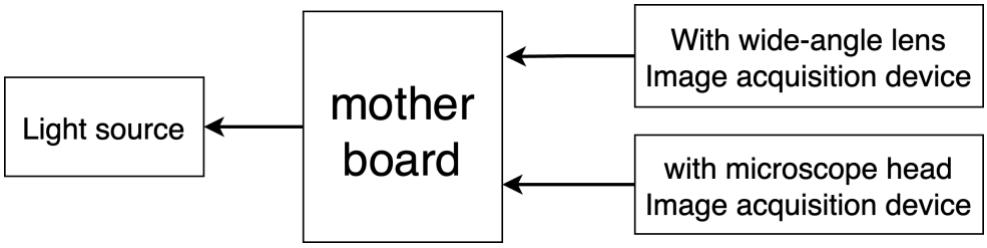
## 3.1 TECHNICAL SUMMARY

Through the "intelligent forensic instrument", you can take a local image of the physical surface of the product that is magnified N (N > 180) times to generate a fingerprint image. These fingerprint images can be uploaded to a centralized server or decentralized storage, and all the information is aggregated and minted into NFTs (non-fungible tokens). During authentication, the verifier can take a locally magnified image of N (N > 180) times at the same location on the surface of the object, and compare it with the fingerprint image previously stored on the chain. Artificial intelligence algorithms are used to compare micro-detailed images to ensure the correspondence between the data on the chain and the physical object.

## 3.2 TECHNICAL IMPLEMENTATION

### 3.2.1 Intelligent forensic instrument

The intelligent identification instrument is a portable intelligent electronic microscope device that is used with a mobile phone to automatically scan and collect microscopic images of the surface of an object. Includes: image acquisition device with wide-angle lens, light source device, image acquisition device with microscope lens, housing, Bluetooth wifi module and gyroscope.




### 3.2.2 Scanner working principle

The smart forensic instrument can be used after being connected to a mobile phone. When in use, the image acquisition device with a wide-angle lens is used as an image positioning device, and the user is guided in real

time to position the image acquisition device with a microscope lens by searching for image templates in continuous images. After arriving at the accurate position, the microscopic image of the surface of the object is collected, so that microscopic images of the same position on the surface of the object can be collected at different times or by different users, so that the consistency verification of the object itself can be achieved through image comparison technology.

#### 3.2.3 Accurately locate the surface position of the object

Obtain at least two image sequences of different scales or different sizes of the same target area on the object surface to form a manual guidance image group to guide the user to direct the camera towards the target area on the object surface, and then use intelligent algorithms to capture the video frames in the video frames captured by the camera. Automatically search for image positioning templates to capture accurately positioned images of object surface positions.

#### 3.2.4 Minting NFT (ERC721)

Casters can use the "intelligent forensic instrument" to magnify the image of the object's surface by at least 3 times. Make sure the focus is accurate and the image is clear when shooting. Then, upload these captured images and videos (photos of items, videos, fingerprint images, positioning images) to the decentralized server (return to IPFS link) to obtain the data link. Next, link the data with other data of the NFT, including timestamp, metadata, minter, etc., and encapsulate it in NFT to complete the casting of the NFT.

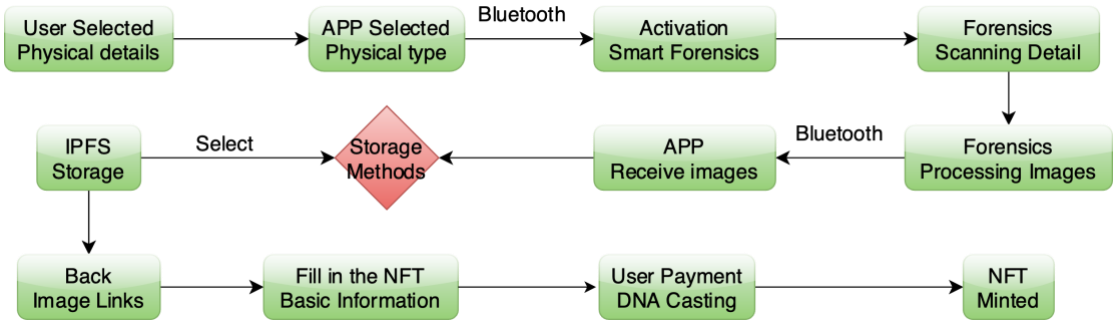
### 3.3 WORKFLOW

#### 3.3.1 Casting process

①Use "intelligent forensic instrument" to collect fingerprint data and positioning data on the surface of objects

②Upload fingerprint data and positioning data to the decentralized server and return the positioning link

③Encapsulate all data and write the signature to complete the casting of NFT




### 3.3.2 Verification NFT process

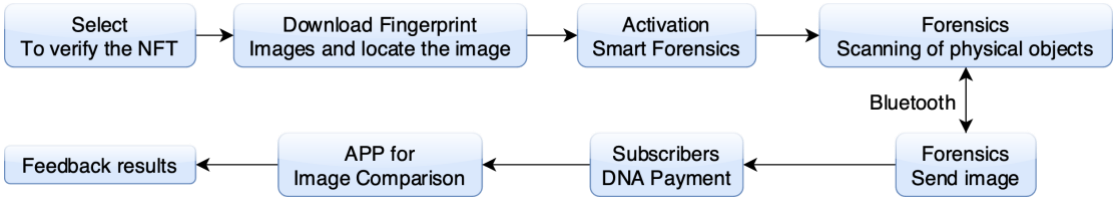
①The verifier queries the NFT information that needs to be verified

②The verifier downloads fingerprint data and automatic positioning data on the server or decentralized storage

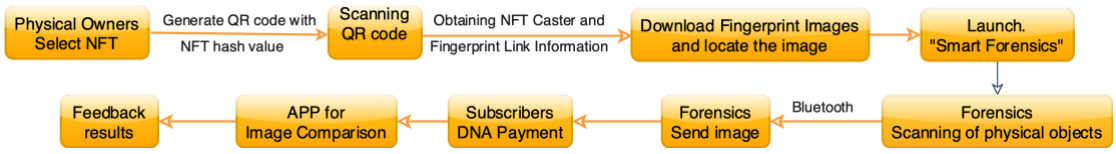
③The verifier takes an image of the surface of the object magnified N times in the same way as the caster.

④The machine automatically compares the image taken by the verifier with the downloaded fingerprint image, and feeds back the result

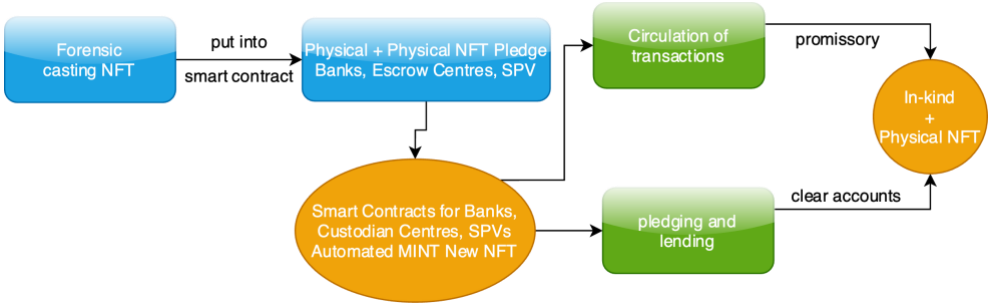
**Verification process of physical NFT, own NFT yourself**




**Verification process of physical NFT, others own NFT**




**DNA linkage RWA process**



# DNA.PASSPORT

## 4.1 TECHNICAL SUMMARY

DNA Passport is an online + offline identity aggregation dApp built on Ceramic Network. Users can collect various identity certificates called stamps from Web2 and web3 authenticators; stamps are provided by various Web2 and Web3 authenticators , including Google, Facebook, Bright ID, ENS and Proof of Humanity. Passport aggregates stamps and aggregates the real-name authentication information provided by offline users on the chain through MyID. For example, Li Lei provides identity information off-chain and binds various online identity verifiers to aggregate various information through his wallet. chain. Users only need to know the information of the user corresponding to the account through the wallet account.

## 4.2 BRIEF DESCRIPTION OF DID

DID is the abbreviation of "Decentralized Identity". As a digital identity that does not require verification by a centralized organization, it gives users a new opportunity to control their own rights. Currently, the main problems DID solves include ownership (user's data and identity management rights) issues and the absence of native Web3 identities. In response to the above two questions. DNA DAO will launch its DID product - DNA Passport by combining on-chain + off-chain identity verification. Following the launch of the "intelligent forensic instrument", DNA DAO's physical copyright system will also evolve from a centralized platform to a decentralized protocol.

## 4.3 PROBLEMS WITH DID

### 4.3.1 Ownership issues

Since the Internet does not provide users with a native identity layer, digital identities are issued by websites and applications. The silo approach may have worked for the early days of the Internet, but now that the number of Internet users has reached billions, the drawbacks of the silo approach have become increasingly apparent. Creating usernames and passwords is increasingly becoming the mainstream paradigm for identity proofing, even though it is increasingly considered an insecure model; and the average person has to manage more and more passwords, which inevitably leads to

poor user experience. What’s more, users don’t actually own their online identities, but rather rent accounts from a company or centralized entity. Therefore, online identities are prone to risks of illegal intrusion, manipulation, censorship, or loss.

#### 4.3.2 The absence of native Web3.0 identity

“Today, Web 3.0 is more about expressing transferable, financialized assets than an encoding of social trust relationships. However, many core economic activities, such as unsecured loans and building personal brands, are built on On a lasting, non-transferable relationship. In less than a decade, Web3.0 has created an unprecedented unique and flexible parallel financial system, bringing a complex and open ecosystem to financial transactions, and then , the economic value of financial transactions is generated by humans and their relationships. Since Web3 lacks the foundational elements to represent this social identity, it fundamentally relies on the centralized Web2 structure it seeks to transcend, thus replicating its limitations "——"Decentralized Society: Looking for the Soul of Web3"

### 4.4 TECHNICAL IMPLEMENTATION

#### 4.4.1 MyID introduction

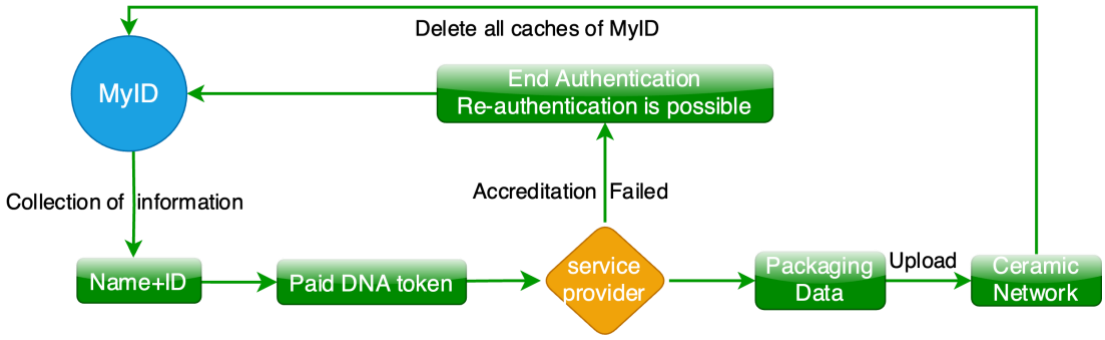
MyID is an off-chain user information collection verifier. The collected information mainly includes: user name, identity ID and other information. It aggregates the information collected and allows users to upload it to the DNA.Passport tool

#### 4.4.2 MyID workflow

①The user uses the wallet to log in to MyID and fill in personal information

②Choose at least 2 face recognition service providers (Ant, Baidu) for real-name authentication

③After passing the real name, the personal information filled in by the user will be encrypted and uploaded to the chain and the cache will be cleared.




#### 4.4.3DNA Passport Features

**information autonomy**

Verified through open web standards such as DID and VC, it contains personally identifiable information, WEB2 account information, and WEB3 information. All information in the user's Passport can be modified, added or deleted at the user's discretion.

**Cross-chain verification**

Verify data across multiple blockchains for composable, interoperable identities. This means that users only need to hold a DNA Passport to have a Web3 network pass.

#### 4.4.4 DNA PASSPORT technology implementation

DNA Passport is a decentralized user identity information aggregator. Its main working logic is:

①Confirm the user's identity (name, identity ID) through the information uploaded by KYC under the MyID chain

②Prove the user's social status or the social label of this user that everyone agrees on through the web2.0 social network.

DNA Passport is an identity verification application developed on the Ceramic blockchain network. Ceramic is an off-chain sovereign data network that maps decentralized identifiers (DIDs) into user-controlled data flows. Data on Ceramic is public, permissionless, and verifiable, unlocking information access and interoperability across all platforms and services on the web.

The DNA Passport SDK consists of a set of databases distributed on NPM to help developers interact with Ceramic Passport data on NPM.

@DNA/passport-sdk-writer – Writes authenticated DIDs to the Ceramic Passport stream.

@DNA/passport-sdk-reader – Read from any Passport stream (on Ceramic).

@DNA/passport-sdk-verifier – Verify the contents of a passport.
Anyone can read the data on Ceramic. If you know the user's blockchain address, DID or Ceramic Stream ID, you can obtain data from Ceramic, and people can read the user's Passport information, but only the user himself can go to Passport. Write data in it. An app only obtains permission when the user signs a message using the wallet to grant the app access (such as when the user connects to the DNA Passport app). Passport requires a user's unique wallet signature to allow write operations, and only applications that want to write to a user's PassPort need to ask the user to sign these messages.

## 4.5 DNA PASSPORT PERSONAL VERSION BACKEND


## 4.6 INTRODUCTION TO DNA PASSPORT ENTERPRISE EDITION

### 4.6.1 DNA node

The corporate version of Passport cannot submit information to the chain alone. Information needs to be submitted by the DNA node. To apply for a DNA node, you only need to pledge a certain amount of DNA to the community (as long as a company or institution signature application is submitted, the deposit is non-refundable). The specific value will be announced by the community at that time. Nodes submit corporate or institutional signature applications to the community, and the community approval time is 7 days. During the 7-day publicity period, community members can verify the authenticity of the signature application. After the publicity period, it will be automatically reviewed and uploaded to the chain.

### 4.6.2 DNA node income

After the company and institution signature application submitted by the node is passed, they will take a commission from the fee for minting NFT (5%-20% of the floating pipeline income, which is determined by community voting).

### 4.6.3DNA PASSPORT Enterprise Edition


# DNA DAO

## 5.1 TOTAL ISSUANCE

There are two tokens in the DNA ecosystem, DNA and RNA

**RNA is a management token with a total upper limit of 1 billion and a non-constant quantity. It is used to realize the management rights of the DNA ecology. Management rights include community proposal voting, income distribution voting, and node income voting.**

**DNA is a fuel token with a total amount of 1 billion and a constant quantity, which is used to control DNA ecological resources. Mainly used for casting NFT, verifying NFT and node staking**

In the DNA ecology, 1 billion pieces of DNA have been generated, but RNA has not been generated, and the number is initially zero. Users pledge DNA to their wallet address through the "entrusted voting smart contract" to obtain RNA. RNA cannot be traded or transferred, and will be automatically destroyed upon expiration to redeem DNA. The rules for generating RNA from DNA pledge are as follows:

Staking for 36 months: DNA: RNA 1:1

Staking for 12 months: DNA: RNA 1:0.3

Staking for 6 months: DNA:RNA 1:0.14

Staking for 1 month: DNA: RNA 1:0.02

## 5.2 TOKEN USAGE

### 5.2.1 DNA usage scenarios

①Minting physical NFT requires consuming DNA

②Becoming a node (enterprise and institutional submitter) requires pledging DNA

③Scanning and verifying physical NFT requires consuming DNA

④DNAPASSPORT signature application requires DNA

⑤Producing RNA requires pledging DNA

⑥Purchasing various physical objects requires DNA

### 5.2.2 RNA's rights and interests

①Verify that 70% of the physical NFT income is divided according to the proportion of RNA holdings

②60% of the income from minting NFT is divided proportionally

③Participate in community proposal voting

④Foundation ecological investment token airdrop

⑤Annual 3% airdrop (community support plan)

## 5.3 Token distribution

①The development team receives 20% DNA tokens, of which 10% tokens (unlocked monthly, issued in 3 years)

②Private equity, blockchain VC, community DAO, various public chain investment departments, incubators (seed round, round A, round B, round C) coinlist, etc. 20% tokens

③The community owns 60% of the tokens

## 5.4 DNA black hole combustion mechanism

10% of the fee for each verification of a physical NFT will be automatically entered into the black hole address, and 10% of the fee for each physical NFT minted will be automatically entered into the black hole address. If a node

does evil, the node's future income and part of the node's deposit will be confiscated and burned.

## CHANGES DNA TECHNOLOGY BRINGS TO THE INDUSTRY

### 6.1 Anti-counterfeiting and traceability

In recent years, consumers have frequently encountered counterfeit goods and food safety issues, and how to ensure the authenticity of products and avoid being deceived has become a problem that people cannot cure. Blockchain technology seems to have brought new hope for commodity traceability with its characteristics of information transparency, non-tamperability, and traceability.

In the past few years, many anti-counterfeiting traceability projects based on blockchain public chains or consortium chains have emerged, but they have not become popular. The main reason is that these projects still use traditional methods and only use blockchain technology for storage. They do not fully utilize the characteristics of blockchain and do not solve the problems of traditional solutions. There have been many anti-counterfeiting methods in the past, including radio frequency identification, QR codes, barcodes and near field communications. Product-related information is recorded through QR codes or barcodes, such as the supervision code on the carton. We can scan the external QR code for basic authentication before purchasing, and the data in the box is associated with the outside after consumption. However, these anti-counterfeiting technologies using blockchain cannot fundamentally solve the problem of counterfeiting by copying and transferring anti-counterfeiting marks.

Although the application of blockchain technology can ensure the anti-counterfeiting and traceability of data in the circulation process, when applying blockchain technology to physical anti-counterfeiting and traceability, there is still a key issue that has not yet been resolved, that is, how to ensure that the physical object corresponding to the data is Not replaced or counterfeited. There is currently no existing technology that provides a good solution. However, with the introduction of DNA microscopic scanning technology, this critical problem has been solved.

By magnifying N times (N >180) at the production end, a partial image of the physical surface of the product is taken, the partial image is uploaded to

decentralized storage, and all information is summarized and minted into NFT using a real-name account. During authentication, consumers read the NFT information and magnify it N times (N >180) to take a partial image of the same position on the surface of the physical object. Microscopic image recognition technology and blockchain technology are used to achieve anti-counterfeiting and traceability of physical products.

### 6.2 NFT

With the development of cryptocurrency, non-fungible tokens (NFT) have gradually attracted people's attention. NFT is a digital asset. Unlike traditional cryptocurrencies, each NFT is unique, so they can represent unique, irreplaceable items such as artwork, music, virtual real estate, etc. NFTs are usually built on blockchain technology, which makes them decentralized and non-tamperable.

Throughout 2018, the global transaction volume of NFT was only US$473,000, but by 2022, three years later, this number had soared to more than US$40 billion. As international first-tier companies such as Walmart, McDonald's, and Visa begin to get involved in the NFT field, more and more celebrities, athletes, and KOLs have also begun to participate in transactions. NFT has become a mainstream investment method.

Although the application of NFT can help us track the production time and circulation history of a specific product, it cannot track its social origin for us, nor can it provide a rich social background. This has led to a lot of abuse and fraud in the current NFT field, such as copying original digital artworks and distributing them in different markets. This major issue also caused Web3 participants to suffer huge capital losses. Even the largest NFT trading centers are still trying to find ways to solve these security issues. In addition, the price maintenance of NFT depends on the consensus of the community. Once there is a problem in the community, the value of NFT will plummet.

However, NFT, as the cornerstone of the next generation Internet, is far more than digital collections and PFP (Profile Picture). It is actually "Everything", it can be data, it is the mapping of the physical world in the virtual world, it can be used as a carrier for asset securitization, it can also be combined with the real economy, and it can even play a huge role in private domain traffic management. Therefore, we have seen that many Web2

companies around the world, such as Starbucks, Nike, LV, Gucci, Disney, etc., are trying to use NFT to further build their own membership systems and brand culture. Once blockchain technology (such as DNA) establishes a communication bridge with the real world, the application of NFT technology in the real economy will become possible, and the potential of this market is immeasurable.

### 6.3 Real World Asset RWA

Real World Asset Tokenization (RWA) is the process of converting real-world asset ownership (such as U.S. Treasury bills, real estate, or art) into digital tokens on the blockchain. This tokenization can increase the liquidity of assets, enable fractional ownership, and expand investment channels. However, the security of RWA tokenization depends on regulatory compliance and the trustworthiness of the platform.

RWA tokenization offers several advantages, such as increasing liquidity in traditionally illiquid assets, providing opportunities for fractional ownership, and democratizing investment opportunities that were previously only available to wealthy individuals or institutional investors. The RWA tokenization market is expected to grow significantly, with industry estimates predicting a market value of $4 trillion to $16 trillion by 2030.

However, RWA tokenization currently relies heavily on enforcement by legal regulatory agencies, and the real-world situation is very complex. For example, when a smart contract involves the transfer of real estate between two agents, the code can indeed exchange certificates of equity between the parties. However, the previous owner may refuse to leave the house and even rent it out on a lease basis for 20 years. Even if a third party overseeing a smart contract (such as a court) is involved, its execution cannot be ensured. Therefore, in the process of promoting RWA tokenization, the challenges posed by these real-world complexities need to be solved.

Obviously, it will take time to promote and improve RWA, but for movables (antiques, calligraphy and paintings, luxury goods, artworks, handicrafts, watches, ceramics, souvenirs, stamps, etc.), DNA can be implemented without legal supervision. The specific implementation method for bearer delivery is as follows:

1. Customers deposit physical objects into the custody center, and the custody center needs to pledge a certain amount of token DNA.
2. The customer deposits the NFT into the custody center, and the custody center verifies whether the NFT matches the physical object.
3. Physical objects are matched, and the custody center issues new NFTs signed by the custody center to customers (customers can use the new NFTs to redeem old NFTs and physical objects)
4. Customers tokenize new NFTs, deposit them into smart contracts to generate interest-bearing ERC20 tokens, or pledge new NFTs to obtain stable coins and other financial operations.
5. If the customer defaults, the other party can directly deliver the customer's NFT and find the custody center to redeem the physical object. The exchange of physical objects by the custody center is anonymous and can be redeemed with the NFT signed by the custody center.

**6.4 Decentralized mall**

In the thousands of years of human society, some people are as tall as mountains, but some people are extremely despicable, and trust has always been a problem that has been difficult to solve for thousands of years. Satoshi Nakamoto has completely solved the trust problem in human society by using mathematical methods. , and has been running stably for 14 years. No matter when and where you are, you can trust the data generated on the chain. Throughout the past ten years, the essential reason why the implementation of blockchain has not been effectively promoted is There is currently a lack of effective blockchain oracle mechanism to connect the real world and the blockchain network, giving people the illusion of a blockchain scam! Imagine that Li Lei, who is far away in Seattle, USA, directly purchases a postage painting from Xiao Ming in China through the blockchain network. He does not need to worry that Xiao Ming, who has never met, is a liar, and Xiao Ming does not need to worry about Li Lei. No money will be given after receiving the goods! Point-to-point transactions can be easily completed without any third-party platforms such as Amazon or Alibaba, and without worrying about the other party's character. For the time being, this is called Liao's conjecture.

### 6.4.1 What is a decentralized mall?

In blockchain technology, users' transactions no longer rely on centralized third-party institutions, but are based on trust in machines, mathematical algorithms and smart contracts. This means that users no longer need to rely on any Leviathan institution, but can fully trust the technology itself.

For example, users can put products on the shelves in a decentralized mall without worrying about malicious exchanges or malicious refunds. Consumers can purchase goods without worrying about buying fakes. This is because blockchain technology provides transparent, tamper-proof transaction records and microscopic image comparison technology combined with signatures, so that every transaction on the blockchain can be tracked and verified, and the data on the chain corresponds to the physical object.

### 6.4.2 Logistics - A method to prevent tampering of packages

Place the item inside the box and seal it, then affix an unforgeable label to the box and sign the seller's name. Next, the unforgeable characteristics of the tag are extracted as fingerprint data, stored and transmitted to the smart contract. During the receiving process, the recipient obtains the fingerprint data of the product and compares it with the fingerprint data to be shipped. At the same time, the recipient obtains the fingerprint data of the outer packaging box, compares it with the smart contract, and uploads it to the express company's own server. During the express delivery stage, first confirm the integrity of the packaging box and verify that the label on the packaging box is intact. Then, the extracted fingerprint data is compared with the fingerprint data of the smart contract to determine whether the packaging container has been opened. Through the above process, the security and integrity of the transaction process can be ensured. Buyers can tell whether someone has ever opened the packaging container by verifying the integrity of the box and the intactness of the label, as well as the consistency with the extracted fingerprint data. This approach combines physical closure and unforgeable features of the label, as well as verification of fingerprint data, to provide buyers with a higher level of assurance that the item has not been tampered with or taken apart during shipping.

### 6.4.3 Implementation of decentralized mall technology

1. Pending order object

Order objects include: companies (certification required), individual artists (certification required), individuals (certification not required)

2. Transaction process

### 6.5 Decentralized business marketing

Physical NFT rights and interests are operated offline and decentralized: In traditional offline merchant operations, merchants mostly adopt closed operations to users to protect customers. This method intensifies the fragmentation of user rights and interests. Member rights and interests are everywhere, and each member’s rights and interests are everywhere. An account system, each account system stores a copy of user privacy information. At the same time, business giants hinder the development of small and medium-sized enterprises and technological innovation through their monopoly on users. Through physical NFT comparison technology, all credible data in the entire life cycle of physical objects can be analyzed. Based on the anonymous user's consumption ability and past equity write-off (NFT redemption) situation, it can further reflect the user's economic strength, consumption distribution, and consumption habits. This kind of precision marketing can bring more business opportunities to enterprises, especially central enterprises and creative enterprises, while protecting user privacy. The larger the amount of data, the more precise the marketing. All merchants jointly create data and jointly use data. Decentralized data and a decentralized direct marketing system can put all enterprises on the same starting line, allowing enterprises to spend more energy on products and services. At the same time, trustworthy public data created by decentralized co-creation will be high-quality raw materials for the development of AI and can cultivate new productivity.