### Dsign

### Decentralized Signature

2022/12/05

### Brief Introduction

Dsign is a new type of electronic contract signing platform that permanently stores digital contracts on a blockchain network. As the third generation of electronic signature platform, electronic contracts have a more powerful legal effect through the blockchain network and biometric system.

We guarantee the feasibility of the signature through asymmetric encryption. We have created a completely new on-chain protocol, and every information of the contract cannot be tampered with. Using DID and bioinformation to bind wallet, the contract management system based on Etherchain and Arweave has 0 Gas cost with strong privacy performance.

**Why is innovation needed**

Our vision is to subvert the traditional signature industry through brand new technology. Traditional electronic signatures will verify personal information based on mailboxes and mobile phones. Traditional electronic signatures are easily forged due to security and depository models.

1. The mobile phone number do not represent the user itself, in some parts of Europe and the United States, the mobile phone number is not bound to the real physical identity information. This creates the risk of information abuse. Even in some areas, such evidence is not used as a user's identification.
2. At the email level, e-mail address is currently the main identity authentication. But it only applies to anonymous digital accounts and cannot act as authentication like an ID. E-mail can be registered by anyone and resemto the existence of a web domain name. And for the login and registration of email, there is often no physical identity certificate and biological authentication, even if certain specific identity information is bound, email does not have a real secure ownership.

**Strong identity system**

Anyone who knows an email password can log in to an email account. Contracts signed using email completely reduce the legal effect, especially when personal information is sold outside. When the same password is used in a large number of web pages, the email key cannot be fully guaranteed.

Based on the above situation, we conceived a completely new identity system. An imtamable binding is made around the digital identity, biological information and ID information. Digital identity is generated by the tamper-proof blockchain wallet public and private keys, which represents the user's imtamable identity. And the advantage of this identity is that it does not have to pay high GAS fees like NFT, and maintains an imtable, unique attribute. The private key represents the user's own password, and no third party can master the user's content.

When we sign traditional and important contracts face to face, we all hope that the identity of the other party is true, and the ID identity and the signer themselves are consistent. We even want the other party to guarantee the validity, and each page ensures that the content is free from tampering. But everything can be done by on-chain protocol.

The user's identity can be determined by his real biometric features and legal entity credentials. Based on face recognition and fingerprint authentication, the electronic signature platform can thus fully define the real signer of each contract signed. Thus avoiding the occurrence of certain fraud.

**What is an electronic signature, and how is its market**

Electronic signature refers to the data message contained in electronic form, used to identify the identity of the signer and indicate the content approved by the signer. DocuSign has more than one million users and more than a billion transactions. With electronic signature infrastructure construction and block chain technology development, and benefit from the third party electronic signature platform actively cooperate with enterprise service software, electronic signature enterprises will products and partners of software integration, build enterprise service ecological closed loop, promote electronic signature service user scope, promote the world electronic signature industry scale expansion.

The global digital signature market is worth $3 billion in 2021. The forecast period has a compound CAGR of 36.1%, and the market is expected to grow from $4.05 billion in 2022 to $35.03 billion in 2029.

Many countries have issued a number of encouraging policies related to the application of electronic signature to promote the improvement of electronic signature infrastructure services. Many national regulations emphasize the legal effect of electronic signature, encourage the lattice industry to adopt electronic signature products, and lay a good development environment for the application of electronic signature. Electronic signature infrastructure is becoming increasingly mature and perfect, electronic signature has the characteristics of efficient contract management, strong credibility and so on, to meet the needs of enterprise information management, small, medium and micro enterprises will successively adopt electronic signature products, the new generation of electronic signature agreement will fully penetrate into all industries.

**Why a blockchain is needed**

Extensive Internet access has changed almost every aspect of human life, and a large portion of human contracts are done on the Internet and done electronically, and it is always in our pocket. While the Internet has a amazing impact on social organizations, some basic laws about the system still exist. The main information is the transient of the information stored on the network, which can change or disappear at any time. And its inevitable centralized risk, platforms and third parties can view users' content based on the background.

In this paper, we present a sister network that is seamlessly integrated with the World Wide Web, providing an archive of permanent encryption validation for the Internet. The archive makes use of a new blockchain-derived data structure called blockchain weaving, and a new access proof algorithm. In Arweave, it is the storage infrastructure on the blockchain. It brings many benefits:

Contracts can permanently exist on the chain and the user can access the signer's own contract through the dashboard with the private key. User privacy is well guaranteed, and there is no need to constantly pay monthly subscriptions like traditional platforms. Instead, paid permanent storage provides more free and cheaper access to contracts.

More secure, each signed "message" contains the content of the contract text, signer information, time information. All of this data is packaged and encrypted on the chain, and thanks to the Merkel tree's network mechanism, nothing in the contract can be tampered with since then.

Blockchain technology enables us to improve the security of electronic signatures, and blockchain provides a distributed ledger that cryptography ensures that data can not be tampered with and forged. Its number of broadcasts, content bookkeepers, and backup nodes is much higher than traditional cloud storage. Blockchain technology has the characteristics of imtamable, non-denial, and multi-party participation, highly meeting the storage needs of third-party electronic signatures. Third-party electronic signature enterprises combine blockchain technology with storage business to form blockchain storage application, which can improve the anti-tampering and anti-counterfeiting ability of storage data, and improve the security and reliability of third-party electronic signature.

**Why we choose Arweave?**

First, let's solve the simple question: Why use Arweave to store contracts? The answer is simple: the data on the Arweave cannot be deleted or changed. IPFS and AWS have only three node backups, and Arweave has far more backups stored on the chain.

We can also ask this question in another way: Why not use IPFS or AWS? IPFS is not ideal, and although it uses content addressing to ensure that the contract is not changed, it cannot guarantee that your data will not be deleted. For example, if you use IPFS, a fixed service, it is removed if your data is not accessed within 6 months. For a contract, it is entirely a tailbreaker. For another example, nft.storage promises "indefinite" storage but in its terms and conditions below. Whenever the Protocol Labs, Inc. Continue to provide free storage for NFT, data will be free on IPFS.Protocol Labs, Inc. Terminate the N F T at its sole discretion. Rights of storage, N. C. Protocol Labs, and decided to end up with the NFT. The storage Project. Before termination, Protocol Labs will provide users with a 90-day notification via email, giving users enough time to arrange to store their data in other ways.

**What makes Dsign different?**

Dsign will not only become a dApp similar to our traditional electronic signature platform, but it will also do something that the traditional platforms can't do:

Permanent contract storage: The data truly exists on the chain and is constantly globally synchronized by a large number of nodes.

immutability: timestamp, identity, and contract contents are encrypted and packaged on the chain.

Service Continuity: Ensure sustainable execution through the protocol and managed by the developer community through DAO.

One payment: Thanks to the on-chain storage protocol, there is no monthly payment. For each contract, you only need to pay for storage once, and you can always preview it on the dashboard in the future.

Contract Privacy and Data Ownership: the users browse the contract only through the private key, and it is executed by the agreement, and the third book and the platform cannot read the user's privacy.

Trusted identity: Automatically binds identity and biological information to the wallet, thus signing a contract, and there is no need to worry about leaking real information through privacy protocol.

**Dsign's competitors**

The EthSign protocol is applicable to the ICO / The VC's tokens are automatically distributed and executed. But without a biological identity and a real ID, it is not suitable for traditional contracts.

DocuSign: The contract cannot be kept permanently, and users need to pay continuously. Without biological authentication and can easily lead to contract forgery, the legal effect of the content is not the strongest.

**Conclusion**

Users' demand for contracts is unchanged, and there are still a large number of users using paper contracts. What blocks the generalization of electronic contracts is the opacity of identity and trust, and the security of mechanisms. Once Dsign starts, it becomes a decentralized, universal electronic signature agreement that will sign electronic contracts in a secure, decentralized, and trusted way. Through the identity asymmetry of traditional electronic contracts, and without Gas costs.

We are very excited about the possibilities that Dsign brings to the Arweave ecosystem and the entire blockchain industry, including building new users away from traditional bastions.

*Dsign will be an enhanced, uncracked, and permanently stored electronic signature platform in the web3 era, and we can't wait!*