DRAFT

LegalNFT: Document Signing and Notarization NFT Service Using Blockchain Technology

Jordan Stojanovski

January 27, 2022

Abstract

We describe LegalNFT, a document management, signing and notarization service, which encapsulates legal agreements into Non-fungible Tokens (NFTs). This allows safe electronic storage and communication of the documents, signing and encryption using software and/or hardware devices. The completed agreements are recorded on a public blockchain and immutable decentralized storage, and encapsulated into NFTs which can be appraised and traded on the open market in a centralized or decentralized manner.

Introduction

NFT is simply a denotation of an unique asset recorded on a blockchain. The ERC 721 standard for NFTs merely describes an interface for identification, ownership and transfer, but does not specify details about handling the contents or legal terms of the NFTs. Data storage is extremely expensive, and the NFT mainly points to a separate place where the NFT content is stored or specified. It is desirable that such storage is immutable and decentralized in order to match the properties of the blockchain storage.

The NFTs have found usage as recorded artwork and as such have gained tremendous popularity in the blockchain world. Some NFTs may be overpriced due to hype, but some genuinely represent unique items with great value.

LegalNFT is a system which allows attachment of legal agreements to the NFTs. This allows protection, describing the legal terms of the NFT as well as encapsulating any legal agreement or record into the NFT. These terms can specify identification of a physical object, and/or a legal obligation attached to the NFT. As such, the NFT can be valued/appraised and traded on the open markets. The development of Decentralized Finance (DeFi) would allow such trade to be completed without human intervention, regardless of intent to impede it or compete with it in an unfair manner. This could create a mass market for trading anything that is legally described as ownership or liability.

There are various electronic document signing services on the market. Some make it easy to sign documents by identifying the signers via email addresses, and accepting their signatures by clicking on an “Agree” button. This may be acceptable for documents that do not carry financial burden or large obligation, but it presents a problem when stakes are larger.

Various institutions in different countries appear as digital certificate signing authorities, allowing the citizens to digitally sign documents. This is cryptographically safe, but somewhat inconvenient, as there is no universal way to sign free-form documents. Instead this method is mainly used for signing already computerized workflows, such as payment transactions.

Private companies that facilitate document signing try to capture the market by storing the documents and trying to lock the users into repeat business. Many private companies try to monetize user’s data and bury user’s content into the terms and conditions in exchange for free usage or discounts. This imposes security risks from malicious actors. As such, many legislations forbid or at least attempt to forbid storage of the data outside of their premises or country.

This presented an opportunity to develop a system which allows the user to cryptographically sign documents, record them in an encrypted unalterable storage, allowing the user or institution to be a sovereign owner of the data. This gives the user independence from big technology companies. In addition the timestamped record and NFT encapsulation opens a possibility to appraise and/or trade these agreements.

Philosophical principles

- LegalNFT is based solely on distributed and open-source technologies. No private company or government should be able to lock the users into using proprietary technologies in order to access their data.
- The users of LegalNFT are the sovereign owners of the data. No institution, private or governmental would have a backdoor to access or alter the data without the user's consent. The user could only surrender access willfully in case of voluntary publication or court subpoena.
- LegalNFT shall never advise the user to succumb to the least resistance in order to break the above principles.

Distributed Autonomous Organization - DAO

LegalNFT itself shall become a Distributed Autonomous Organization (DAO). Initially the founding members would control all processes and internally make all decisions. In the second stage membership shall be tokenized on the blockchain, each token representing a share of power in the decision making process. Such tokens can be acquired by usage of LegalNFT,

participation in its development and demonstration of authority by jurisdictions, such as governments.

The LegalNFT DAO members shall be able to propose actions and vote on such proposals. Once the proposals are voted, the actions should be executed in a safe distributed manner.

Technologies Used

The web user interface is using React.js and JavaScript which are open-source and do not require financial compensation for open-source projects. The web front end is served from IPFS, which is a distributed, content addressable and censorship-free system. The web site URL is secured by the Ethereum Name Service (ENS) domain, which provides translation from the web site name to IPFS addressing. ENS is uncensorable. Since the content of the web site is stored in an immutable storage, each time a new version is created, the ENS domain name shall be updated to point to the latest version. This shall be governed by the LegalNFT DAO.

The cryptographic tools rely on open source technologies. No keys are stored in any LegalNFT system, and the user is solely in charge of safeguarding their own keys. LegalNFT merely provides suggestions for safeguarding, backup and storage of such keys. The cryptographic methods are based on Elliptic Curve Cryptography, utilizing the same Elliptic Curve as the Ethereum blockchain. This allows the LegalNFT keys to be stored in Ethereum Web3 software wallets such as MetaMask or hardware wallets such as Ledger or Trezor.

Once the documents are signed, they are accessible via IPFS, but encrypted with the document owners' public keys, and thus only decryptable by the owners' private keys.

As IPFS is a document delivery system and does not guarantee document storage, the user is responsible for storing and safeguarding the relevant documents. Note that the user cannot alter those documents, as they are content-addressable, signed by the appropriate parties and registered on the blockchain. To store the documents the user is given a choice of one of the following:

1. Use the FileCoin distributed system to store the documents. Storage is guaranteed through distributed proof of space-time and incentivized by the FileCoin cryptocurrency. This assures competitive storage pricing through the FileCoin built-in auction system, as well as privacy, as no participant in the system is aware of the content of the data stored.
2. Store the documents on a private IPFS server(s). IPFS provides document "pinning" on user's storage.
3. Store the documents using a publicly available commercial IPFS pinning service such as Pinata. This is valuable in cases where there is a requirement for a "responsible party" for storage of the documents.
4. Store the documents in a proprietary manner using any storage of choice, as long as they are not altered. If the documents are no longer accessible via IPFS (not pinned, no FileCoin storage), the user can re-publish them, and since they are content-addressable, they will assume the original address.

Storage of the data only provides safety against loss, and therefore does not allow access to unencrypted data.
As documents are signed, the digital signatures along with the signed documents are encrypted and stored in an IPFS accessible storage, organized in a folder. However, to provide a timestamp on the actual signing of the documents, the entire folder along with its contents is hashed and recorded on Ethereum or any Ethereum compatible public blockchain, uncontrollable and unalterable by private entities or governments. This avoids censorship of the data and manipulation by private entities. In addition it avoids excessive infrastructure cost and also makes the cost of the system proportional to its usage.

Diverse and International Acceptance

Various jurisdictions rely on courts, notaries and apostles. Private institutions have their own document signing systems.

In order to stimulate cooperation LegalNFT provides a free-form container for parts of the agreement. This allows not only agreements with complete wording and identification of the signing parties, but also agreements derived from templates. For example a template for a vehicle lease agreement could specify the general terms of the agreement, identifying the parties involved by their aliases/roles. Then separate small documents could identify the parties, their public keys and some specific parts of the agreement, such as price, term length etc. This container can be digitally signed by the agreement signers, making it immutable as a whole. Then the signed agreement can be “notarized” by recording it to the blockchain as NFT.

In addition, this free-form container allows fulfillment of various requirements by different jurisdictions. For example if the jurisdiction mandates identification of the user’s public key/address by signing using a certificate, such signed statements can be put into the container as part of the agreement. Even if the jurisdiction mandates signing of the whole document using a specific kind of certificate (issued by specific authority), such signature can be placed in the container.

The above system of trust already has worldwide acceptance. However, it is up to the specific private entities or jurisdictions to accept signatures and signing certificates signed by specific authorities. For example, one country may accept official documents signed by signers whose certificates are signed by one of that country’s Certificate Authorities, but not accept others. In addition, a Certificate can be signed by multiple Certificate Authorities and as such used in multiple jurisdictions which have such inter-organizational or international agreements.

To avoid clutter in their court systems, many countries have adopted the system of notaries. However, notaries in various countries have different powers, authorities and recordkeeping requirements. In order to accept a notarized document in another country, a notarized document has to get an Apostille issued by courts, or special “super-notary” institutions. This in turn creates clutter in international document acceptance and trade. LegalNFT can streamline this system if pairs of jurisdictions agree to accept each-others users’ documents signed in a

specific acceptable way defined by consenting jurisdictions. This would be achieved by the free-form container of documents in LegalNFT. The convenience of signing the documents using the Elliptic Curve signatures used by Ethereum is only an option. The user can sign documents using any mechanism and then turn them into an NFT as a timestamped record.

User Experience

The user would access LegalNFT via its website. There, a signing ceremony can be initiated, in which the user decides who will bear the expenses and the rules of engagements, such as

- How and whether the document is encrypted
- How many parties shall sign and who they are
- Is the signature valid only after all parties sign
- Who has access to the signatures
- Restrictions of document storage mechanisms/venues.

Next the user shall make payment for the services. This shall be a small one-time fee with one-time setup or automated by third parties.

Once the signing ceremony is initiated, it’s the responsibility of the user to communicate it to the other parties involved. This could be email, secure or public messaging etc., but all based on the user's will and not enforced by LegalNFT. LegalNFT would allow the user to store communication links for streamlining of the process, which the user voluntarily submits.

Users communicate in several rounds, refining the document and discussing it independently of LegalNFT. Once they decide to sign, the signatures are recorded and temporarily stored. Upon completion of the signing ceremony, each party is offered a storage mechanism from the allowed list generated upon creation of the ceremony. One party can decide to use one venue while another a separate venue, according to their appetite of trust and safety. The storage of documents is independent from the “notarization” on the blockchain, which merely creates an NFT that points to the signed documents container.

The documents are accessible to each user according to the storage venue they chose, as well as the user's authority and ability to decrypt them. This can present a proof of signing, timestamp (retrieved from the blockchain) and jurisdiction (retrieved from the signing certificates’ Certificate Authority which is attached to the signature or simply stored in the documents container as one of the free-form documents).

Importantly, the user does not depend on any third party in order to prove that they or their counterparty signed the document defined by the ceremony, and present the document and proof of signing to the appropriate jurisdiction or private entity.

Vendor Independence

As big technology companies have grown out of proportion, in order to provide “free” services, they lock the user into relinquishing ownership of their personal information, documents and activity data. The user loses control where that data is disclosed, sold and even stolen / “hacked”. Most jurisdictions have not caught up with legislation to make the holders of personal and other sensitive information responsible for its mishandling. In addition, powerful tech companies are “lobbying” against such legislation, as it would erode the value of the data in their possession.

Some countries strictly limit the location of storage of personal information, but that is mostly for verification of credibility and good standing and prevention of illicit activities by users. Yet, none of that is for protection of user’s privacy and sovereignty of their personal information.

LegalNFT is open source. There is no “security by obscurity” in any of its components. Everything is based on sound cryptographic methods. The data format is not only disclosed, but it is stored in a simple IPFS directory structure format. Even if LegalNFT ceases to exist, no data is lost but merely convenience of handling that data. We make extra effort not to lock the user into using LegalNFT exclusively, but try to attract them by convenience.

Despite the open format, data sovereignty is assured by the strong cryptographic methods. Unless the user willingly discloses the decryption keys, it is next to impossible to “hack” the data and steal it. This sounds like a bold claim, but it is easily achievable as LegalNFT never stores clear text data because we have no intention of monetizing that data.

In addition, eventual customer contact lists would never be mixed with the LegalNFT document storage, as this storage never reaches LegalNFT’s “premises”. All payment shall be processed via cryptocurrencies, which would render storage of payment method information such as credit card numbers unnecessary.

We are hoping to penetrate the market via openness as opposed to vendor locking.

Business Model and Tokenomics

This part is still in development. It is simple to put together, but instead of making decisions incompatible by eventual funding source, we would work together with the funding source to seal the options.

As there are many open initiatives for user data sovereignty and independence from big tech, it is possible to get grants from public funding. The European Union is actively searching to fund such solutions.

As LegalNFT is not locking the user into its exclusive usage, it can still be a commercial product and yet appeal to public institutions. As such, we would create a blockchain based business model. Payment for LegalNFT services would be achieved using a “Token” with limited circulation (or at least issuance).