Blockchain Project Report

Name: Prakash Veer Singh Tomar

Stream: CSE AIML

Enrollment ID: 12020002016009

Class Roll No. : 2

Blockchain for Notary Services: Examine the potential of blockchain for digital notarization and document verification.

Author: Prakash Veer Singh Tomar

Date: 6th October, 2023

Github: https://github.com/lonewolf235/Smart-Contract-for-Notary

Blockchain technology has immense potential for digital notarization and document verification. Its key strengths lie in immutability and transparency. Blockchain stores a secure and tamper-proof record of documents, creating an unchangeable history that can be easily verified by authorized parties. This ensures the integrity and authenticity of digital files, making it ideal for notarization. Moreover, the decentralized nature of blockchain reduces reliance on centralized authorities, enhancing security and accessibility. As a result, blockchain offers a robust and efficient solution for verifying the authenticity of documents and ensuring their long-term validity, with applications ranging from legal contracts to intellectual property protection.

Notary Public Smart Contract

Introduction

The Notary Public Smart Contract is a blockchain-based solution designed to act as a digital notary public service on the Ethereum blockchain. It leverages the

immutability and transparency of blockchain technology to provide a secure and tamper-proof method for protecting the integrity of digital documents and files. This smart contract offers a versatile platform that extends beyond simple notarization, enabling parties to associate with records and collectively safeguard their interests.

Use Cases

The Notary Public Smart Contract caters to a range of use cases, including but not limited to:

1. File Integrity Protection

The primary function of this smart contract is to protect the integrity of digital files and documents. It achieves this by creating a unique cryptographic fingerprint (hash) of the file, which is stored on the Ethereum blockchain. Any subsequent changes to the file will result in a different hash value, making it evident if the document has been altered.

2. Copyright Proof

Content creators, such as artists, photographers, and writers, can utilize this smart contract to establish copyright proof for their creative works. By notarizing their files on the blockchain, they can provide undeniable evidence of ownership and the creation date of their work, which can be crucial in copyright disputes.

Record Creation

Creating a new notarized record is a straightforward process, but it involves essential details to ensure the record's security and longevity. The key components of record creation include:

1. File Hash

A crucial aspect of notarization is the generation of a cryptographic hash of the file being protected. This hash acts as a unique digital fingerprint for the document. It is important to note that most hash functions return a hexadecimal representation of the hash value. To store this value on the smart contract, it must be converted into a `uint256` data type. Typically, each pair of hexadecimal characters corresponds to one byte. It is recommended to use robust hashing functions like SHA256 for optimal security.

2. Parties Associated with the Record

A distinctive feature of this smart contract is its ability to accommodate multiple parties associated with a single record. Parties can be individuals, organizations, or any relevant entities. The parties' Ethereum addresses are collected in an array, allowing for a flexible and inclusive approach to notarization.

3. Expiration Timestamp

Every notarized record has a specified expiration timestamp, represented as a Unix timestamp. The Unix timestamp is a numerical value that denotes a specific point in time. Users can find the current Unix timestamp on external websites or applications, such as UnixTimestamp.com. The expiration timestamp defines the duration of the record's validity, after which it will no longer be considered valid.

Upon successfully creating a record with these details, the smart contract generates a unique record ID. This record ID serves as the key for future access to the notarized document.

Example of record creation:

```
createRecord(2142131241, ["address#1", "address#2", "address#3"], 2523910141)
```

Record Acceptance

Before a notarized record becomes valid, it must be accepted by all parties associated with the record. This acceptance process is crucial, as it ensures that all involved parties acknowledge and agree to the contents and validity of the document. The acceptance is facilitated by the `acceptRecord` function, which requires parties to call the function from their respective Ethereum addresses and provide the record ID as an argument. Only after all parties have accepted the record does it attain validity.

Record Verification

The core function of the Notary Public Smart Contract is record verification. Parties associated with a particular record can utilize the `verify` function to confirm the integrity of the notarized file. However, this function can only be invoked from an Ethereum address that is listed as a party on the specific record. Verification involves comparing a provided hash value with the hash stored in the record. If the two hash values match, the function returns `true`, indicating that the document's integrity has

been maintained. Conversely, if there is a mismatch, the function returns `false`, signaling potential tampering.

Record Validity

A notarized record is deemed valid when it satisfies two critical aspects:

1. Time Aspect

The time aspect of validity is determined by the record's expiration timestamp, denoted as `validUntil`. For a record to be considered valid, the current timestamp (as represented in Unix time) must be less than the `validUntil` timestamp. This ensures that the record has not exceeded its defined validity period.

2. Party Aspect

The party aspect of validity emphasizes the collective agreement and acceptance of all parties associated with the record. All parties must have invoked the `acceptRecord` function to indicate their consent and acknowledgment of the document. Only when every party has accepted the record does it achieve full validity.

This dual validation mechanism, encompassing both time and party aspects, reinforces the security and reliability of the notarization process. It protects the interests of all parties involved and upholds the integrity of the notarized documents.

In conclusion, the Notary Public Smart Contract is a robust and versatile solution for securing and notarizing digital documents and files on the Ethereum blockchain. Its features, including multiple party support and comprehensive validation checks, make it a valuable tool for a wide range of use cases, from file integrity protection to copyright proofing. By leveraging the capabilities of blockchain technology, this smart contract brings transparency and trust to the notarization process, ensuring the long-term integrity of valuable digital assets.