# Project Proposal: Authenticating and Signing Administrative Documents on the Blockchain

## 1. Project Overview

The project aims to build a blockchain-based system that allows public or private institutions to authenticate and sign administrative documents. Each document will be minted as an NFT containing a cryptographic hash, ensuring authenticity, integrity, and easy verification.

## 2. Objectives

- Allow any citizen or organization to verify the authenticity of an administrative document instantly.
- Reduce fraud and forgery.
- Facilitate the storage and verification of official documents without intermediaries.
- Prove the integrity of documents over time.

## 3. Proposed Technical Approach

- Minting an NFT for each document on the Tezos blockchain.
- Storing the document's hash in the NFT metadata.
- Storing the full document securely via IPFS.
- Providing a public verification interface.
- Strict validation of authorized issuers through a registration and whitelist system.
- Easy verification for users via QR code or document ID.

## 4. Constraints and Requirements

- Issuer Verification (only authorized institutions).
- Secure Document Hashing (SHA-256).
- Use of decentralized storage (IPFS).
- Standardized Metadata Format.
- Legal Recognition.
- Easy User Accessibility.
- Cost Control (low fees).

## 5. Potential Attack Vectors and Countermeasures

- Fake Issuer Attack: KYC and whitelisting verified institutions.
- Document Swap Attack: Always verify hashes and use IPFS.

- Revoked Document Reuse: On-chain revocation list.
- Identity Theft: Hardware wallets and multi-signatures.
- Metadata Tampering: Hashing metadata on-chain.
- Blockchain Spam: Economic deterrents and access controls.

## 6. Expected Benefits

- Increased trust.
- Greater transparency.
- Lower operational costs.
- Faster processes.
- Inclusion for remote areas.
- Scalability to other sectors.

## 7. Conclusion

Blockchain authentication of administrative documents will enhance institutional trust, reduce fraud, and simplify access for users. This proposal outlines a robust system leveraging Tezos blockchain, NFT technology, and decentralized storage to achieve these goals.