Cryptech

# Abstract

Cryptech is a cryptographic protocol that allows one or more signors and a notary to create an immutable, timeless, and self-evident proof on a blockchain that a certain document was signed and notarized at a certain time by a certain signor using digital signatures and a blockchain.

[overview of method/algorithms]

# Introduction

[context of real estate transactions]

[current approach]

[Cryptech benefits]

# Approach

First, a pair of private/public keys is generated by the signor.

[assumptions – blockchain(consensus/public/private)]

[assumptions – cryptography(Diffie-Hellman/al Ghamal/RSA)]

Our goal is to create an immutable record on the blockchain containing proof that:

1. Signor S signed
2. Document D at
3. Time T

# Part A: The Signor

It is essential to store the proof of the Signor’s identity. Given the anonymity of public keys, this problem becomes extremely difficult in practice. However, in this paper we present an approach that takes help of a credible notary who signs some identity proof of the signor. For example, a notary could verify the driver’s license in person and then link that person’s public key to the digital signature that attests the validity of the signor’s identity.

## The Identity Problem and Notaries

Digitally verifying identity has always been a tricky problem. The main challenge is to link the signor’s public key, which is anonymous, to the signor’s government identity for legal purposes. We can solve this problem by using the notary’s identity. For this, however we must assume that the notary themselves are authenticated. In our protocol, we have the notary sign the digital identity of the signor using the notary’s private key. This implies that the signature can be validated using the notary’s public key by anyone.

# Part B: The Document

This part of the record is proof that the document is indeed the one that was signed by the signor. This is verified by presenting the original document, and comparing its SHA-256 hash with the one stored on the blockchain.

# Part C: The Time

The time of signing must be provable too. If a certain signature is published on the blockchain at time T, it necessarily implies that the document was signed at time T\* < T. In other words, the document was created before or at time T.

# Protocol

We will now describe the protocol in steps using variables. Let’s say that we have a single signor, notary, and document. The goal is to digitally sign the document while capturing the verification of the signor’s identity by the notary. This digital signature would be pushed onto the blockchain, where it would persist, creating a timeless, self-evident proof that signor S signed document D at time T.

## Setup

1. Let there be a signor X, who has private-public key pair (, ) produced from an NaCl cipher box. Let i be X’s government identification number, SHA-256 hashed.
2. Let N be a notary with private-public key pair (, ). The identity of the notary is assumed to be linked to their private key, which is picked from a pre-selected authentic pool of private keys.
3. Let H be the SHA-256 hash of some secret document D. In our case, this document would be a legal contract to be signed by the signor.
4. Let there be a public blockchain that is fairly decentralized. In our case, we use Apollo, by Factom. Factom gives us an endpoint that allows to push a message (“Entry”) with some metadata/context. Let E be the entry and c be the context.

## Verifying the Signor X’s Identity

1. The notary’s job to validate X’s identity i in person. This is done by obtaining the digital identification number on a valid government photo ID, hashing it once the person’s identity can be verified. We now have a verified i, the hashed identity of X.
2. The notary then creates a digital signature using the notary’s private key and i, the hashed identity of X. This signature is a token that can be used to validate X’s identity by anyone. If X had to prove that notary N has verified their identity, they could provide N’s public key , along with their original identity number. Anyone who wanted to verify X’s identity in person would validate the photo ID, hash the ID number, and verify with and . If the digital signature is valid, then private key did in fact sign .

## Signing the Document D

1. We have now verified X’s identity by having it digitally signed by the notary to get . We have also obtained the hash of document D, H. Now, X creates a digital signature with message H with their private key along with the nonce . The nonce is encrypted along with H while creating the signature, and it always contained in the first 24 characters of the signature.
2. We now have a signature that can be verified with , , and . Since we have shown that is sufficient proof that validated , is now sufficient proof that identity signed document D. If challenged, X can provide to the challenger. The first step would be verifying given and . If is a valid signature, it means that signor X’s identity is verified. The next step is to verify using . A valid implies that document D was in fact signed by X.

## Publishing the Signature at time T

1. Now, we have which by itself is sufficient proof that X signed D. All that is left is the time component. To prove this, we use the blockchain. The blockchain is considered to be an immutable public database for our purposes. We push signature along with as context in the entry E.
2. If someone challenges X, the entry E is sufficient proof that D was signed by X before or at time T, which is the time it was published to the blockchain. can be obtained from E, and given , it can be proved that X signed D. The verification can be done without using any Cryptech protocol – any challenger need only obtain from the blockchain entry and , which is public information. X can provide their photo ID and document D. The SHA-256 hash and the blockchain are assumed to persist.

# Protocol Function Pseudocode

# Proof of Completion and Security

Claim of X: Identity i signed document H with the blessings of notary N at the time t

The only evidence required is B.

Evidence: Bitcoin block address B

Public keys are no secret and can be freely shared

Public information: Public keys U\_n and U\_x

Proof that X's claim is true:

* Check where time of claim t is +/-10mins of the time bitcoin block hash B was created.
* Get chain id C and entry hash E from B.
* V\_n, V\_x, V\_i = verify\_sign\_notary(C, E, H, U\_x, U\_n, S\_n, i).
* If and only if V\_n, V\_x, V\_i are all true, that is sufficient legal proof of X's claim