KEYSTAMP

An open-source Proof-of-Compliance standard on the blockchain

November 27th 2017
Toronto, Canada

Invented at RegHackTO
by Existence

OSC ONTARIO SECURITIES COMMISSION

Abstract

We propose an new open-source standard, Keystamp, for allowing financial services participants to prove irrefutably the actions they took and knowledge they had at a specific point in time. It is a complete cryptographic key management infrastructure and allows for the seamless integration of blockchain technology in an easy-to-use workflow. We specifically implement Proof-of-Compliance (PoC) in the context of "know-your-customer" policies, or any other context where establishing that information was obtained by certain parties at a certain time is required.

It provides a digital trail of unforgeable signatures and timestamps that provides irrefutable evidence that someone had certain information, took action or participated in specific events at specific points in time.

It is also a Proof-of-Knowledge institution for the digital economy, since this open-source system can be used by anyone, for free, to prove that he possessed any data at any time. It can be used for mediation in civil disputes (contracts) by the general public since proofs are easy to verify.

Purpose and social impact

The purpose is to foster trust through disruptive technologies. We aim to increase social cohesion in the digital economy, providing an entirely digital institutional framework of trust for the digital economy.

Keystamp has the potential to enormously decrease the costs of compliance and audit for financial institutions, technology providers, governments, and any institution that needs trust and hierarchical authorizations. It increases transparency and saves money to the taxpayers.

Technology stack

Our technology stack consists of:

1. **A public key infrastructure web application**
2. **An API for signature, validation and timestamping engines**
3. **Cryptographically-enforced data and rights access permissions**
4. **Gateway connection to blockchain P2P network**
5. **Issuance of unforgeable digital certificates**
6. **Hierarchical and deterministic encryption**
7. **Abstraction layer for complex cryptographic libraries**
8. **Telephone verification (2FA) and traditional KYC**
9. **A graphical interface for internal and regulatory compliance**
10. **Built-in compliance tools for financial advisors**

Cryptographically-enforced permissions

We use BIP32 Bitcoin key architecture for cryptographically-enforced access permissions. The issuing authority generates a master private key which it uses to perform digital signatures. It derives sub-keys (hardened keys) that the authority can assign at will. That authority can also to the same, and assign keys at a lower level.

Our innovations

1. Hierarchical encryption and access control

We private keys not only for signing data but also as encryption passwords for storing data. This means that when the lower sub-keys encrypt data, all the levels above can decrypt it. It’s a one way function. As such, only the issuing authority has access to all the data, and permissions are hierarchical, perfect for institutions such as financial regulators.

2. Decentralized and trustless

The same private keys can be used to issue or receive any blockchain asset, from securities to obligations, gift cards, vouchers, etc. When those innovations become mainstream, the validation of transactions will be trustless perfectly synced with cryptographic identities.

All of these cryptographic identities can be linked to legal identities in a centralized government or institutional database. It is possible to use distributed storage networks like IPFS to store data.That database acts as a reference index for pseudonymous keys.

Timestamping

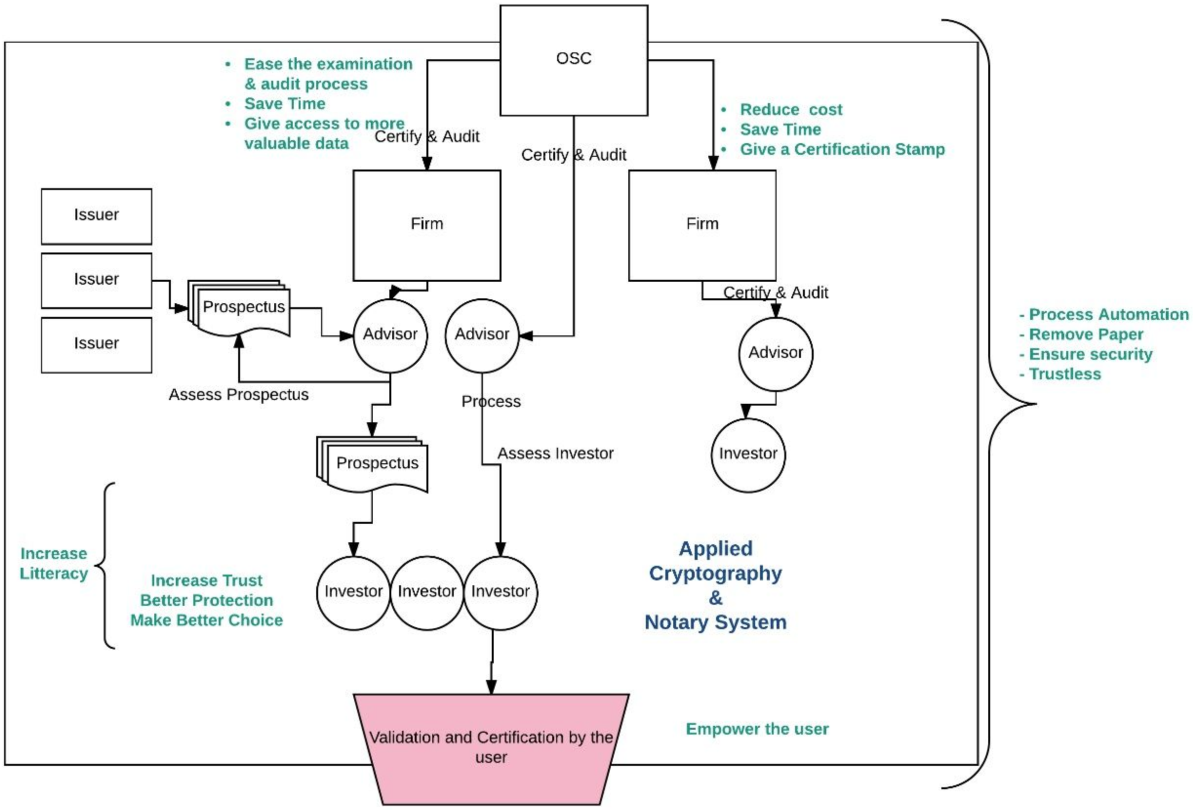
To prove that data existed at a certain time, we can hash the data, leaving a tiny fingerprint. That fingerprint is then signed by the holder of a key, along with a message providing context. If the key is associated to a legal identity, this is irrefutable proof that a person or organization said something or had some information.

Context and use-case

This technology is extremely useful to prove that the proper due diligence was made, the proper disclosures were understood, and proper documents were received and validated, etc.

Our use-case revolves around three types of financial relationships that are under the purview Ontario Securities Commission:

- The “know-your-customer” process initiated by financial advisors for assessing the risk profile of their investing clients.
- The delivery of data by the producers or sellers of investment products to financial advisors.
- The assessment of the risk profile of the investment products by financial advisors at time at which advice is given to investing clients.



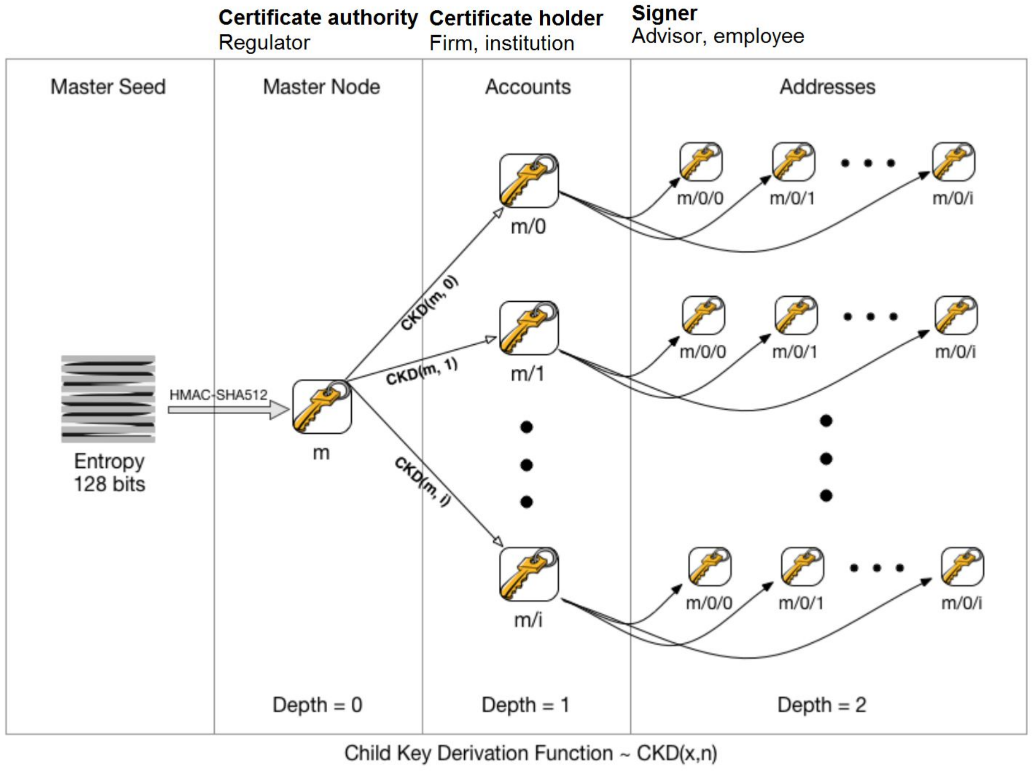
Significance and innovation

Keystamp if the first project to leverage the BIP32 key architecture of Bitcoin, invented by Gregory Maxwell, the CTO of Blockstream, not only for cryptographic signatures or the issuance of cryptographic certificates but also for cryptographically enforced access permission to certain data. This access takes the form of a novel use of BIP32 to achieved hierarchical public key encryption for messages. We achieve this by using the private keys as encryption passwords.

Since the higher level keys can derive the keys of the lower level keys:

- The regulator can decrypt all the data
- The firm can decrypt the data of all its subordinates
- Subordinates can encrypt data for reporting purposes

Bitcoin extended public key (BIP32) architecture



We leverage the public key encryption algorithms on which the identity system of the blockchain is built, as well as the immutable and trustless nature of blockchain timestamps.

One of the main benefits of the blockchain is that it can provide independently auditable cryptographic proof that a certain set of data existed at a specific period in time. Because of the blockchain proof-of-work algorithm, data embedded in the blockchain is entirely immutable.This is what is referred to as “notarization”. In addition, public key encryption makes possible irrefutable digital signatures. By combining the two, we can prove that a set of data was “signed” by a person or organisation at a certain point in time. We can leverage those technologies in the context of compliance to increase trans

The standard process

1. The issuing authority (e.g. regulator) generates a master private key using the Bitcoin BIP32 standard. It is from this key that all subsequent keys in the infrastructure are derived.

- The issuing authority generates (derives) hardened keys for each of the “subordinates” in the hierarchy. This can mean the relationship between regulators and financial services firms.

This means that anybody can independently verify that a certain firm has been accredited by the regulatory authority, as long as the firm is using the Keystamp protocol.

Customization: the issuing authority could decide not to derive hardened keys, which means that all the certificate holders would be aware of each other and thus track each other’s transactions on the blockchain and be able to verify each other’s signatures.

- Each institution (or person) such as an advisory firm derives extended public keys, again hardened or not, for each other subordinate, such as individual employees and advisors of an advisory firm.

- Each advisor uses a new key, derived from his extended key, to cryptographically sign documents and compliance data.

Compliance data consist of any data used to prove that certain compliance policies were followed. This includes KYC, due diligence, internal audits, release form, consent forms, contracts, etc.

- Every time an advisor engages in the “know-your-customer” process, the advisor presents evidence of the KYC process, risk assessment, disclosures and all relevant data to the end-user. Examples include:
  - Risk assessment forms
  - Recorded video and audio
  - Email and chat exchanges
  - Disclosures, declarations, fee tables
- The end user provides his consent that he agrees that the information presented by the advisor accurately reflects the KYC and disclosure process that was completed by the advisor by either digitally signing, validating with phone sms verification or any other traditional remote KYC methods.
- A data bundle including the compliance data as well as the end-user’s consent proof (signature or SMS validation log) is hashed using SHA-256.
- The hash is signed by the private key of the person that wishes to prove that he has knowledge of the data.
- The data is encrypted with that same private key, and is stored securely for the right keyholders to access.
- The data can be stored in distributed storage networks such as IPFS, maidsafe, or secure cloud storage.

- The signed hash is stored in the Bitcoin blockchain using OP_RETURN.
- This proves that at the same time the compliance data, the user consent and the advisor's signature of that data and consent existed at a certain point in time.
- If a single byte of data is changed in the compliance data or the user consent proof, the hash will be modified unpredictably. By comparing the compliance hash of the original document on the blockchain with the compliance hash that is presented, we can immediately prove that they are the same (or not), and so that it existed at the time of the block in which it was included.
- We return a blockchain receipt which includes
  - The hash of compliance data
  - The hash signature
  - The advisor's public key
  - The blockchain txid
  - Link to the encrypted original file
- Using the open-source tools we provide, anybody can verify the signatures and the timestamp thanks to the science of public key encryption and blockchain technology.

More Information and resources:

Website: keystamp.io:3000
git: https://github.com/existencelabs/keystamp-client
git: https://github.com/existencelabs/keystamp-api

Fully Functional Backend API for Notarization and Validation of keystamps
git: https://github.com/shayanb/keystamp-crypto

whitepaper: https://github.com/existencelabs/keystamp-whitepaper.git

Contact
francis@existencelabs.com
phil@existencelabs.com