Proposal Demonstrator II

for Validicity

by Göran Krampe

Introduction

This document describes phase 2 of constructing the Validicity chain-of-custody information system. These are the main goals with this iteration:

- Add a minimal mobile application, working both on iOS and Android published on app stores
- Make a minimal Chainpoint (or other) integration to enable regular anchoring of selected parts of the information in the Bitcoin and Ethereum public ledgers
- Make the minimal functionality of a Query tool that can query the system and verify Chainpoint proofs

The overall purpose is for these parts to be included in a live demo and presentation of the system.

Mobile application

The mobile application is built using Flutter and will include the following functions:

- Startup splash with Validicity logo
- Mandatory first login screen using username and password
- Basic preferences of the application:
  - Language selection
  - Color theme
  - Ability to explicitly create keys and register public key in server
  - Current Project selection (among the projects the user has been given access)
- List of Samples in Project
  - Detail view of Sample
  - Sample Event log view which is a direct view of the block chain
- QR code scan ability to find Sample
- NFC scan ability, including entering text comment, to create Event

We are postponing the issue of account recovery (if you have forgotten username and/or password) since this needs to be discussed and is not essential for demonstrating the system.

To support a full demonstration we also need to have ability in Validicity Tool to:

- Create an Organisation
- Create Users in this Organisation (to use in mobile app)
- Create a Project in this Organisation
- Assign this Project to the Users created

And we need to publish the application on Android PlayStore.

Chainpoint Research

There are different solutions available in the area of using public ledgers, such as the crypto currency ledgers or similar ledgers, to create and verify “timestamp proofs”. The one presented earlier, **Chainpoint**, is an open solution developed by Tierion but there are more variants out there.

- https://tierion.com/ - The company that developed Chainpoint and the leader
- https://chainstamp.io/ - Offering similar service, although looks “not updated”
- https://opentimestamps.org/ - A very similar competing alternative to Chainpoint
- https://originstamp.com – A paid service from a company in Switzerland
- https://factom.com – Competitor to Tierion but seems abandoned
- https://stampery.com – Was started and released at similar time as Tierion
- https://chainpoint.org – The open standard created by Tierion and fully Open Source

There are also a long list of services that offer “proof of existence” via a website, where you upload a document/hash and get a proof. These are typically not marketed as “platforms” to integrate with:

- https://block.co/
- https://www.blockcerts.org/
- https://www.proofofexistence.com/

Factom is a competitor to Tierion but several things are indicating that Factom is not successful and largely “abandoned” while Tierion is going strong and has secured partnerships with both Microsoft and Phillips etc. Neither is really interesting for Validicity, but a good future for Tierion secures further development of Chainpoint and thus makes it a safer choice. However, it should be noted that we only “plug in” Chainpoint as one alternative that can be changed down the road.

Opentimestamps is a one man show (Peter Todd) and similar to Chainpoint. However, Tierion seems to be more “in order” and actively developed.

Stampery built several consumer focused services and is also similar to Tierion/Opentimestamps, but a proper company. Stampery have however acknowledged that Chainpoint is the strong “standard” and wants to follow it as well as possible. Stampery also uses “non standard” Merkle trees.

Finally, Tierion and Chainpoint is properly “developer focused” which is what we want here, not a consumer oriented product. I feel confident that Chainpoint is the way to go – at least to begin with. This ensures we can anchor in the **Bitcoin** and the **Ethereum** ledgers. Also, Tierion has worked intensively with Microsoft:

> *“Chainpoint is now available on Microsoft Logic Apps and Microsoft Flow. Developers can now anchor data to Bitcoin when creating workflows between enterprise systems and popular applications, including Salesforce, Office 365, Twitter, Dropbox, and Google services.”*

Chainpoint Integration

A minimal Chainpoint integration involves:

1. Design database to store proofs and how they relate to the other data
2. Decide when proofs should be requested, for example at every sample submission? Takes 15 seconds, then up to 2 hours to be fully confirmed.
3. Construct hashes of data we would like to anchor
4. Make a call to a Chainpoint gateway
5. Get a proof back and store it in the database
6. Ability to show and verify proofs – add that capability to Validicity Tool

Relevant links:

- https://medium.com/tierion/how-to-create-and-verify-a-chainpoint-proof-eba52a7700e3
- https://github.com/chainpoint/chainpoint-gateway/wiki/Gateway-HTTP-API
- https://github.com/chainpoint/chainpoint-cli

Timetable

The following is a step by step breakdown with time estimations:

1. **24 hours**. First version of mobile application
2. **4 hours.** Make release on Android PlayStore. Postpone AppStore.
3. **24 hours**. Construct first Chainpoint integration
4. **16 hours**. Build first Query tool able to perform simple queries
5. **8 hours**. Add Chainpoint proof verification to Query tool
6. **8 hours**. Prepare presentation and demo of Demonstrator II

In summary, if we disregard time to demonstrate and other meetings etc, 10 full days should be enough to reach Demonstrator II.

NOTE: In order to save some time I suggest waiting with AppStore publishing, it’s usually a fairly boring but time consuming activity that usually takes 4-8 hours to pull through. Android PlayStore is easier.