SSLChain – Management of SSL certificates

SSLCHAIN

> ▶ **Sslchain: an innovative way to manage SSL certificates without third party by taking advantage of the Blockchain technology**

Proposal and added value

- The secure connections use **SSL certificates which are exclusively managed by Certificate Authorities**. **SSLchain is an alternative** solution to manage certificates by taking advantage of the Blockchain technology.
- The certificates would no longer need to be signed by a third party, but would be stored in a Blockchain, in order to ensure their **permanent integrity and accessibility.**
- The SSL Chain comparative advantage come from its low cost: **thanks to the technology Blockchain, it is a market with almost zero costs.**

Flow sheet
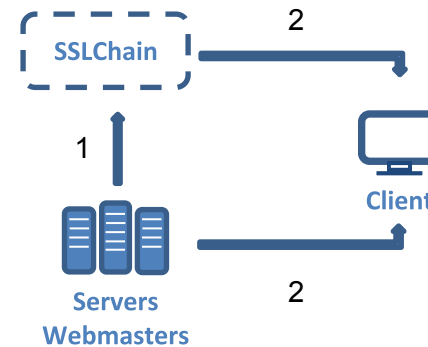
1. Saved the certificate by the webmasters in a secured, public, decentralized, tamper proof, accurate and inalterable way.

2. Checked the certificate by comparing the certificate sent by the webmaster and the one available in the Blockchain. If the certificates are identical, the information can be shared.

Benefits and Business Plan

- **The market is large:** SSL connections are used by almost all internet websites in the world which means the potential market is very large.
- **The competition is low**: Until now nobody tried to propose a viable alternative to replace the certification authorities by using an innovating technology.
- **The comparative advantages are important:**
  i) **Lower price**: The certification authorities charge high fees to sign certificates (dozens of euros every year), but a transaction in the SSLchain project would cost only few euros.
  ii) **Higher data integrity**: SSLchain allows to stock the certificates with a secured, public, decentralized way. The integrity of the SSL certificates do not longer depend on a third party.

Proof-Of-Concept description

- Sslchain is based on a **SmartContract Ethereum** which can be used to interact with the Blockchain. Two main functionalities are developed:
- **Created new certificates**
  - Checked there is an unique valid certificate for a given period and a given domain.
- **Viewed the saved certificates**
  - The certificates in the Blockchain can be viewed through the application. The fact they are in the Blockchain ensures data integrity.

Team and continuation

- Student at ENSIMAG, a school for computing and mathematical
- « In order to pursue my project development it would be necessary to develop a functionality with the main web browsers to directly check the received certificate through a Blockchain request. The client would then have the same comfort than now. Besides a secure online payment facility should be set up to let the webmasters buying their certificates in euros without Ethers.