SSLChain – SSL certificates management using a blockchain

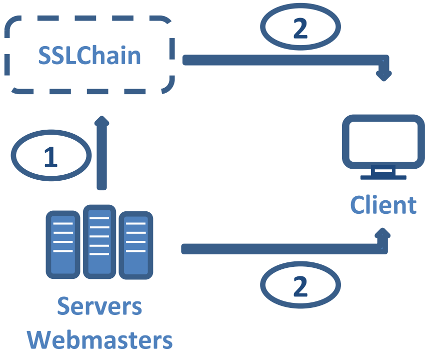
SSLCHAIN

Sslchain : an innovative way, taking advantage of blockchain technology to manage SSL certificates without trusted third party

Proposal and added value

- Currently, secure connexions use SSL certificates **exclusively issued by Certificate Authority. Sslchain offers an alternative** way to manage these certificates taking advantage of blockchain technology.
- Certificates would no longer have to be signed by a third-party authority but would be stored in a blockchain to ensure their **integrity** and their **permanent accessibility**.
- The main advantage of Sslchain lies in its low running cost : **thanks to the blockchain technology, it is a market with a very low transaction costs.**

Flow sheet



1 **Certificate registration,** with low costs, securely, publicly, unchangeable, by the webmasters.

2 **Certificate verification** allowed by the client's comparison of the certificate sent by the website and the one stored in the blockchain. If the certificates are equals, encrypted exchanges can start.

Benefits and Business Plan

- SSL exchanges are used by most websites in the world. So, the potential market of an **alternative way to manage SSL certificates** is huge and the competition non-existent. To propose a strong alternative using a blockchain wille therefore make it possible to compete the certificate authorities. Furthermore these last have high rates prices to sign the certificates (tens of dollars a year) whereas a transaction in Sslchain only costs few dollars. **Compete with these trusted third party proposing an innovative offer at a lower price** is achievable.
- Sslchain major asset is that it uses a blockchain. This technology allows to store certificates in a **secure, decentralized and public** way. So that the SSL certificate safety does not depend on a third-party authority.

Proof-Of-Concept description

- Sslchain is based on an **Ethereum SmartContract** that allows to interact with the blockchain. Two main features have been developed:
- **Creation of new certificates**
  - Check that for one domain, there is only one valid certificate in the blockchain.
- **Consult a registered certificate**
  - The certificates stored in the blockchain are searchable via the application. Their presence in the blockchain ensure their **integrity**.

Team and continuation

- Student at Ensimag, computing and mathematics engineering school
- In order to further develop my project, an internal feature of web browser should be developed to allow the verification of a certificate received from a website requesting the blockchain. So the client would have the same comfort as now. Furthermore, a system to allow online payment for the webmasters should be developed so that they don't have to own Ethers.