Blockchain + IPFS Data Storage

—

FIDUCE

Overview

Working with real estate loans can be very exhausting and may consume a lot of precious time because of the tons of papers which all sides should collect, validate and provide.

Also, human mistakes in documents validation can never be 100% avoided, without mentioning personal data leaks.

With the combination of mobile application, blockchain and smart-contracts, cryptography and secured data storage it is possible to simplify and improve security of the mortgage, selling or purchasing processes of the real estate objects.

Mobile application will provide the comfortable and understandable user interface, which would be available for all relevant parties and where these parties can perform needed actions (for example, sign the documents), check the status of the deal and know who is responsible on which step of the deal.

Smart-contracts would guarantee that the law-regulated process is clear and no speculations can be performed because decisions are accepted by a code using strict instructions. And Smart-contracts would automate the whole process from the beginning of the deal till the final handshake.

Blockchain distributed ledger would guarantee that all records can’t be changed and all history would be accessible anytime and anywhere.

Cryptography would be used to encrypt customer’s personal data and store it in the distributed file storage - IPFS.

Goals

1. Automate the document flow for the mortgage loans
2. Make an GDPR-compliant system for distributed personal data storage
3. Develop transparent and trusted system which allows to check history or the current deals in real time by the relevant parties.

Proposed High-Level Specifications

The whole system would consist of three main parts:

- Mobile application
- Blockchain and smart-contracts
- Distributed data storage (IPFS)

Mobile application

Mobile application would be the entry point for all participants of the system. It would receive the user's data from user's account and OCR scanners (it would be the oracle, so Oraclize would be used to work with this data).

For the user, it would serve as the initial point of the deal and application would allow the user to track the status of the deal.

The same is for all relevant parties - each side can upload own documents, sign them, add new information and track the status. Detailed specification would be designed after the analysis of the mortgage loan process.

Also, mobile application would initialize the smart-contracts execution (starting the deal).

Blockchain and smart-contracts

Smart-contract would guarantee that the whole process is following the strict rules, all documents are valid and protect all participants from the speculations and mistakes.

The mortgage process consists of many steps of documents providing, verification, comparing, etc. So, smart-contracts would rule this chain of actions and trigger another event after the successful previous one, or notify all relevant parties about the actions which need to be undertaken in order to proceed further in this chain of events.

Detailed specification would be described after the analysis of the current business logic and legislation.

Blockchain will serve as the immutable ledger of the all records in the system. This functionality would give all participants to check the history of the deals.

Also, references to the encrypted files, which are stored in the IPFS, would also be recorded in the blockchain in order to know which document was used for which deal and on what step.

Distributed data storage (IPFS)

Different solutions for storing data were concerned: IPFS, Storj, Sia, Maidsafe, Filecoin (solution from the developers of IPFS, not released yet). But all of them, except IPFS, requires cryptocurrency as a payment for using the distributed storage. It is made to guarantee the immutability of the stored data. Public IPFS doesn't have such mechanism by default, so IPFS cluster is the best solution.

IPFS cluster - it is a group of nodes which is set to listen only the participants of the one group of nodes. So the solution for the distributed data storage is to keep own nodes and store the encrypted personal data there.

Other features

It is mentioned that the system requires own token as the loyalty program. But, it is also mentioned that Ethereum blockchain should be private. In this case own tokens would be closed inside the private network and wouldn't be tradeable.

These tokens can be transferred only between the participants of the system.

If it is OK then private Ethereum would be used.

OCR scanners would provide the system with the private data of the users. To deal with external systems like these scanners Oraclize would be used. This will allow us to automate the process of adding scanned documents to the IPFS through the blockchain.

Very important topic - encryption.

It is feasible to encrypt the data by the public key and decrypt it using the private one. But the detailed requirements for the access level and permissions for other participants are required to describe the encryption process in details.

Technologies stack

For the mobile application would be used cross-platform framework - Ionic.

Solidity for the smart-contracts development.

Private Ethereum and Node.JS would serve as a backend and encryption server.

Oraclize would deal with the incoming from OCR scanners data.

IPFS Javascript RESTful API would be utilized for the data storage.