BBCHAIN: Trustworthy Distributed Document Verification System

Rodrigo Q. Saramago
Supervision: Hein Meling, Leander Jehl, Veronica Estrada-Galiñanes
Department of Electrical Engineering and Computer Science, University of Stavanger

Forskningsrådet
The Research Council of Norway

Universitetet i Stavanger

Background

Until today certified documents are mostly based on paper and the verification process is expensive, time-consuming, and prone to human error and fraud [2]. Besides that, the solutions that makes use of digital signed versions require third-party central authority.

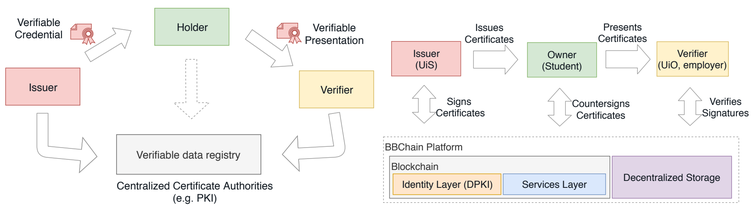

Fig. 1: Common centralized approach and the decentralized solution based on W3C standard[1]

Current Problems

- Bureaucracy and lack of interoperability between issuers and verifiers.
- How to verify the owner of a public key?
- Centralization of information (central authorities).
- Users don't have control of their data.

Available Technologies

- Blockchain → Integrity, redundancy, cryptographic immutability, transparency, smart contracts
- Biometrics → User's unique public identifier

How take advantage of these technologies?

The goal of this work is to build a trustworthy distributed system to ensure authenticity and integrity of documents by effectively combining blockchain and biometrics technologies.

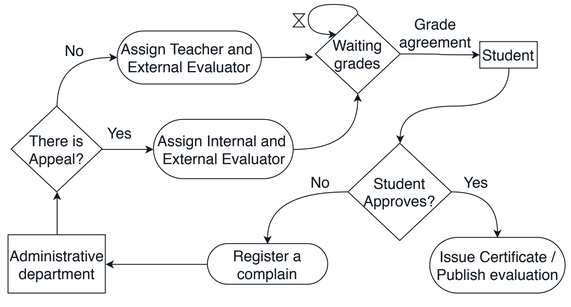

Fig. 2: Simplified UiS evaluation process

Proposal

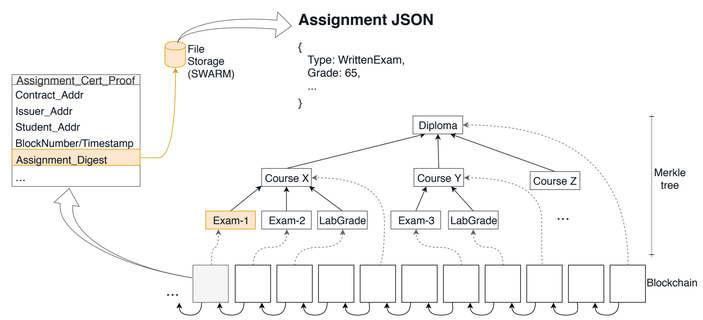

Fig. 3: The Diploma construction

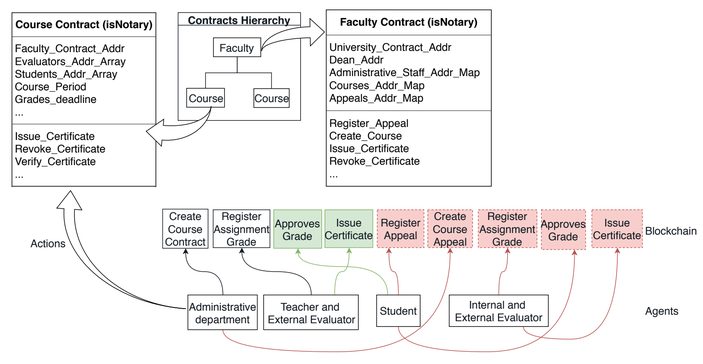

Fig. 4: The student evaluation process

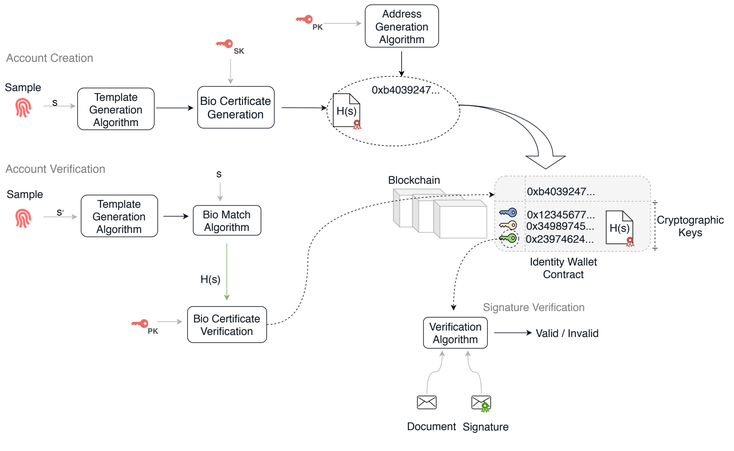

Fig. 5: Identity and signature verification process

Advantages

- Institution modeled as a group of employees.
- Users endorse the trust in the institutions.
- Enables transparency of institutions procedures and easily fraud detection.
- Less human error prone, potentially reducing cost and complexity.
- Establish relation between real and digital identity (biometrics).
- Key-management through smart contracts.
- Improves emission and verification process of digital documents.
- Can globally scale and don't relies on any central authority.
- Gives to users control of their digital identities and documents.

Challenges

1. Data stored on contracts are public → Zero-Knowledge (ZoKrates)[3].
2. Data emitted on events/logs are public.
3. Tracking user activities.
4. Cross-matching information between services.
5. Risk of censorship.
6. Smart contracts limitations (Gas costs, Oracle problem)
7. Require encrypted files on storage/wallet.
8. Biometrics match accuracy (template exchange/Fuzzy signature[4])

References

[1] World Wide Web Consortium. *Proposal Specification of Verifiable Credentials.*

[2] World Economic Forum. *The Known Traveller Unlocking the potential of digital identity for secure and seamless travel.*

[3] Ethereum Foundation. *Toolbox for zkSNARKs on Ethereum.* Available at `https://github.com/Zokrates/ZoKrates`.

[4] Kenta Takahashi et al. "Signature schemes with a fuzzy private key". In: *International Journal of Information Security* (Feb. 2019).