BlockChain based certificate verification platform

Axel Curmi, Frankie Inguanez

Institute of Information & Communication Technology, MCAST IICT

Introduction

Satoshi Nakamoto, out of a need to secure transactions for cryptocurrencies, introduced a new concept of how we could store transaction data without the need for a centralised point of authority. Nakamoto described this system as an ongoing chain of hash-based proof-of-work [1], nowadays known as the blockchain. The blockchain is considered to be the next revolutionary technology ever since the internet was first introduced, as it is constantly challenging us to change the way we use technology in our daily lives [2].

Hypothesis & Questions

In this research we set out the hypothesis: the integrity of certificates, be it academic or medical, should ideally be in a decentralised system, that will be more reliable, autonomous and have the ability to survive beyond the lifetime of the issuing institution/entity.

- Can the same system be extended for medical and/or other purposes with more sensitive information?
- Is the blockchain proposal more reliable than normal systems?
- Is the proposal limited to one network or can it cross different blockchain networks?

Research Stages

We have opted to split this research into three stages:

❶**Technology Familiarisation:** where a prototype is created using the blockchain for the verification of academic certificates;

❷**Privacy Enhancement:** a second prototype is created which will hold important medical health records of patients, with a main focus on the privacy concerns/issues;

❸**Market Acceptance:** a study is performed to gather user and corporate acceptance as well as the possibility of having inter blockchain network communication.

Technology Familiarisation

Privacy Enhancement

Market Acceptance

Technology Familiarisation

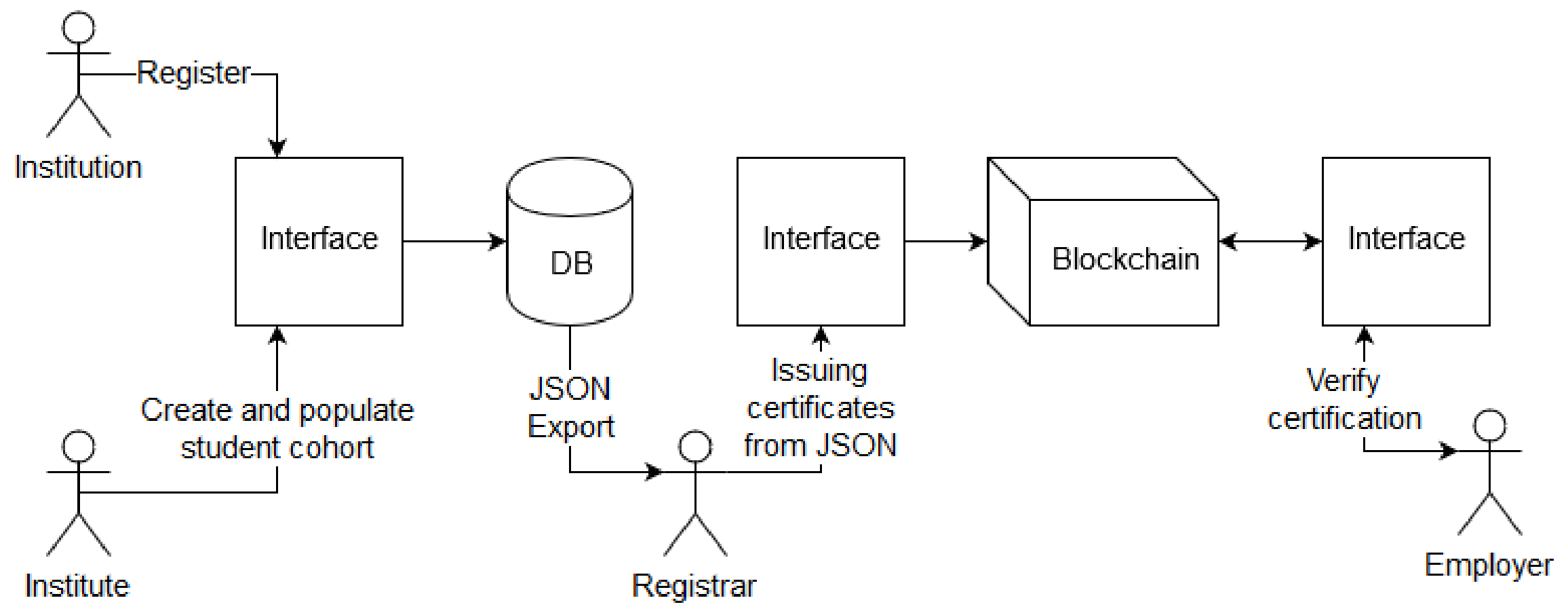


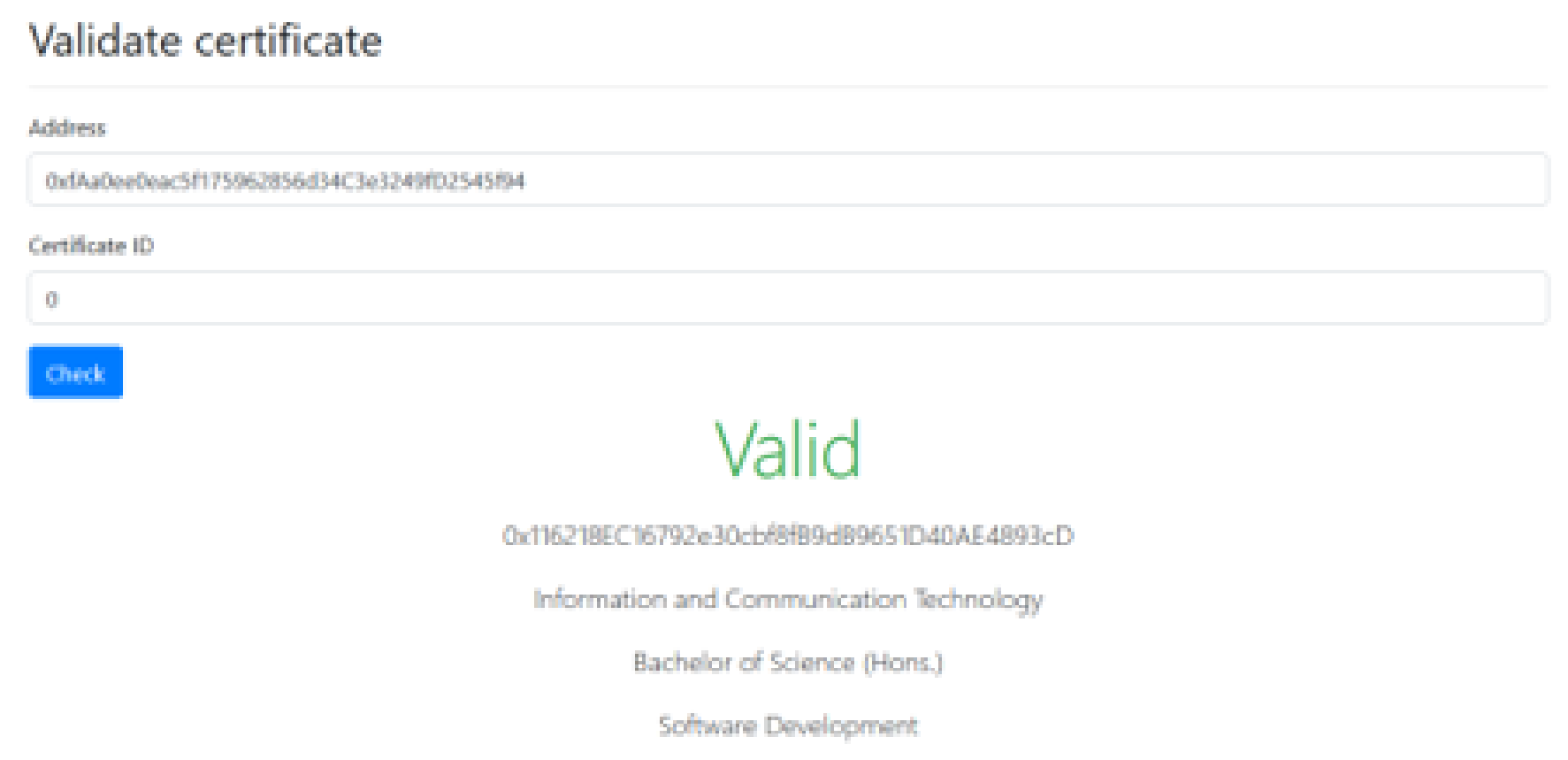
Figure 1: The three phases of the technology familiarisation stage

❶**Institution registration:** In order to start issuing certificates with this platform, the issuing entity firstly has to register itself with us and stored in an off-chain storage. Once registered, the owner of the platform has to deny or approve the entity's registration.

❷**Issuing of certificates** Once the issuing entity is approved, they can now login into their account and do a number of things off-chain and on the blockchain, such as:

- Create cohorts (off-chain)
- Add students to cohorts (off-chain)
- Download JSON populated with data input
- Issue certificates to students (blockchain)

❸**Certificate viewing and validation:** Anyone looking to check the validity of any certificate can do so by simply inputting the id of the certificate holder and the certificate id. In doing so a message will appear showing an error message if the certificate does not exist, otherwise the certification details are shown.



Validate certificate

Address

0xfAa0ee0eac5f175962856d34C3e3249fD2545f94

Certificate ID

0

Valid

0x116218EC16792e30cbf8fB9dB9651D40AE4893cD

Information and Communication Technology

Bachelor of Science (Hons.)

Software Development

Figure 2: A valid certificate

Privacy Enhancement

Repurpose prototype for medical sector

- Doctor's recipe
- Personal medical records

Privacy is the main focus of this stage as medical information cannot be made public. Permissioned blockchain networks, such as Hyperledger Fabric, and cryptography techniques will be researched and considered for this stage to make sensitive data private.

Market Acceptance & Inter-blockchain communication

- Quantitative data to be collected from the general public by using online surveys.
- Qualitative data will be collected from interviews with corporate users for corporate acceptance.

Lightning networks [3] will also be a focus of research in this stage as they provide practical solutions to problems such as scalability and transactional speed.

Evaluation

- **High security & Reliability**
- **Scalability** is an issue.
- **Certificate count per block** is limited as there is a maximum number of bytes which can be stored in a single block.
- **Low transaction speed** when compared to transaction companies like VISA and PayPal. However this limitation does not affect this platform as operations are not time critical.
- **Loss of account credentials**

Conclusion

This research confirms that anything which is considered valuable, such as certificates, can be stored on the blockchain, and thus being immutable and incorruptible. Thus it is being proposed that in the next stage of this research, focus is given to securing the data and controlling user access. It is being also recommended to investigate the combination of blockchain and off-chain storage structure, similar to what was implemented in [4], in order to implement an advanced medical health recording system which would also allow end users to opt-in and opt-out from having their medical data used by medical researchers. This research has not investigated on how the validity of documents on the blockchain is verified, yet this needs to be addressed in the subsequent phases. The blockchain technology is a very recent and emerging technology which is met with mixed feelings and understanding by the general public.

References

[1] Satoshi Nakamoto.
Bitcoin: A peer-to-peer electronic cash system, 2008.

[2] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and C. Yang.
The blockchain as a decentralized security framework [future directions].
IEEE Consumer Electronics Magazine, 7(2):18–21, March 2018.

[3] The Raiden Network fast, cheap, scalable token transfers for ethereum.
Accessed: 28/06/2018.

[4] Guy Zyskind, Oz Nathan, et al.
Decentralizing privacy: Using blockchain to protect personal data.
In *Security and Privacy Workshops (SPW), 2015 IEEE*, pages 180–184. IEEE, 2015.

[5] Jesse Yli-Huumo, Deokyoon Ko, Sujin Choi, Sooyong Park, and Kari Smolander.
Where is current research on blockchain technology?âĂŤa systematic review.
PloS one, 11(10):e0163477, 2016.