Issuing Blockchain-verified Certificates

Supervisor
Dr. Abhinesh Kaushik

Indian Institute of Information Technology, Lucknow

February 28, 2023

Group Members

- Ashna Agrawal - LCS2020028
- Palak Goel - LIT2020030
- Soumya Baheti - LIT2020040
- Anjali Chaudhary - LIT2020061

Introduction

Our project focuses on building an immutable certificate generation system. The procedure of issuing the digital certificate is as follows :

- IIITL or the Certificate issuing authority will feed the college data in the certificate template.
- Issuer will fill in the required details and submit the form.
- Now the issuer will approve the transaction charges in Metamask.
- The certificate along with the corresponding hash is generated.
- Each certificate will have a unique hash key which can be used to validate the authenticity of the certificate.

Problem to be Solved

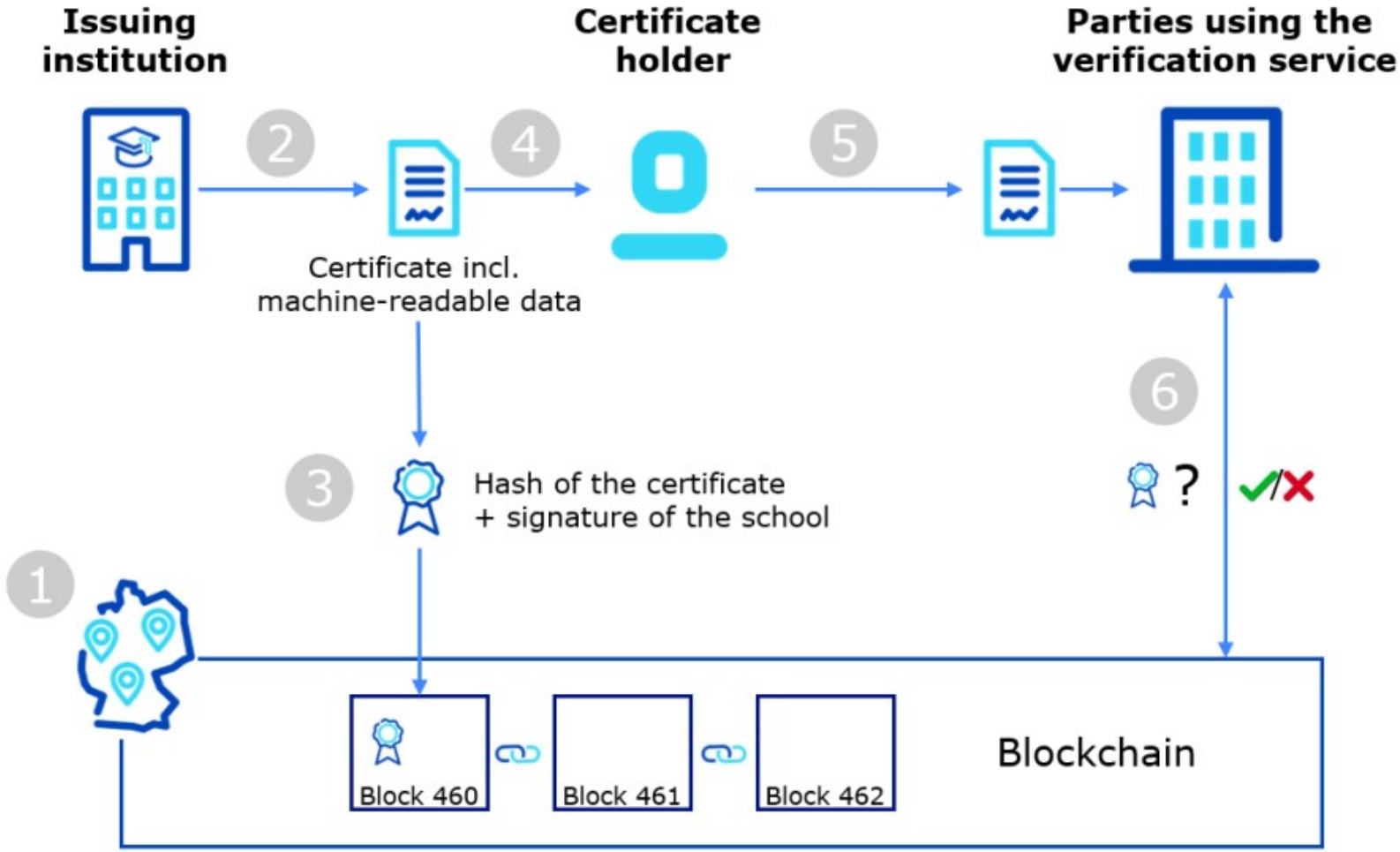
- Document verification is a complex domain that involves various challenging and tedious processes to authenticate. This leads to uncertainty and doubt regarding the credibility of the document source.
- Traditional records are usually held as paper files that can deteriorate over time and are vulnerable to loss or theft.
- To make the data more secure and safe, everything needs to be digitalized with the principle of Confidentiality, Reliability, and Availability. All of these can be achieved using Blockchain, which solves the problem of counterfeiting certificates.
- By storing the records as digital certificates, the issuer can also safeguard them from damage and destruction.

Blockchain

- Blockchain is an online ledger that provides decentralized and transparent data sharing.
- The goal of blockchain is to allow digital information to be recorded and distributed, but not edited.
- New blocks are always stored linearly and chronologically at the “end” of the blockchain.
- After a block has been added, it is extremely difficult to go back and alter the contents of the block unless a majority of the network has reached a consensus to do so.
- Hence, a blockchain is the foundation for immutable ledgers, or records of transactions that cannot be altered, deleted, or destroyed.

Motivation

At present times, Blockchain technology is gaining more attraction due to its distributed ledger feature. Every record in this ledger is secured by rules of cryptography which makes it safer and tamper-free. While searching more about the topic, we came across an article titled "IIT Kanpur awards blockchain-based digital degrees to eliminate forgery", which motivated us to create a web app that issues blockchain-verified certificates for our college.


Issuing institution
Certificate holder
Parties using the verification service
2
4
5
Certificate incl. machine-readable data
6
3
Hash of the certificate + signature of the school
?
1
Block 460
Block 461
Block 462
Blockchain

Tech-Stack

- Ethereum
- Solidity
- Metamask
- Truffle
- Ganache
- NodeJS
- React

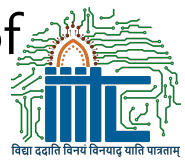
Ethereum

- Ethereum is a technology for building apps and organizations, holding assets, transacting and communicating without being controlled by a central authority.
- It has its own cryptocurrency, Ether, which is used to pay for certain activities on the Ethereum network.
- Ethereum is programmable, it means that you can build apps that use the blockchain to store data or control what your app can do.
- It makes use of smart contracts which are simple computer programs which exectute when triggered by a transaction from a user.

Truffle

Truffle framework uses Ethereum Virtual Machine, thereby enabling flexible and straightforward smart contract

- Truffle has in-built capabilities for compilation, integration, and deployment of smart contracts.
- We need truffle to convert the Solidity code into machine-readable code that can be deployed on Ganache blockchain.
- Truffle smart contract development is easier with support for writing deployment scripts.
- The network management features in the Truffle development framework can help you deploy applications to any number of private and public networks.



Challenges

- Blockchain was a new technology for us. The main challenge we all faced was to learn and implement a dApp using blockchain.
- Choosing the technology that was compatible with each other and finding resources on them.
- Work distribution and collaboration among the group members.
- Difficulty in finding ethereum-faucets for mining ether on ethereum testnets, as for each transaction some amount of ether was required.

Conclusion

- Creating immutable ledgers is one of the main values of Blockchain.
- This behavior helps us to achieve a system in which all the process is transparent and unchangeable.
- Our System automates the process of generating Certificates and reduces the manual work needed for the verification of the same.
- Students are also at comparatively low risk of losing the certificate.
- By using an additional hashing algorithm we are decreasing the percentage of data being tampered with. This will help us preserve the data and create transparency.

Future Work Plan

Till the end of this semester,

- We will be able to generate and revoke blockchain-verified certificates.
- The unique id associated with the issued certificate will be sent to the student via email.
- Any person can view the certificate on our website using a unique certificate id.

References

- A. Gayathiri, J. Jayachitra and S. Matilda, "Certificate validation using blockchain," 2020 7th International Conference on Smart Structures and Systems (ICSSS), Chennai, India, 2020, pp. 1-4, doi: 10.1109/ICSSS49621.2020.9201988.
- Khan, S.N., Loukil, F., Ghedira-Guegan, C. et al. Blockchain smart contracts: Applications, challenges, and future trends. Peer-to-Peer Netw. Appl. 14, 2901–2925 (2021). https://doi.org/10.1007/s12083-021-01127-0
- C. BouSaba and E. Anderson, "Degree Validation Application Using Solidity and Ethereum Blockchain," 2019 SoutheastCon, Huntsville, AL, USA, 2019, pp. 1-5, doi: 10.1109/SoutheastCon42311.2019.9020503.

Thank You

Now let us look at the demo of our project