Kaduna Polytechnic Graduate Certificate Verification System Using Blockchain Technology.

Idris, B.*, Abubakar, M.*, Lawal R. L.*, Akande H. F.**

*Department of Computer Science, Directorate of ICT Centre Kaduna polytechnic, Kaduna state, Nigeria

**Department of Chemical Engineering, Directorate of ICT Centre Kaduna polytechnic, Kaduna state, Nigeria

Abstract — Universities and other educational institutions issue graduation certificates as one of the most important documents for graduates. A certificate is a proof of the qualification of a candidate and can be used to apply for a job or other related issues. Today, it is popular to forge important documents like certificates, identity cards, and passports. It is expensive and time-consuming to check certificates using traditional methods. The purpose of this paper is therefore to suggest a theoretical model that can provide a potential solution for the issuance and validation of educational certificates using blockchain technology. The blockchain technology includes multiple functions including hash, public/private key cryptography, digital signatures, peer-to-peer networks and work proof. The model uses different elements to formulate the block divided into key processes: the issuance of a digitally signed academic certificate and the confirmation of the academic certificate. The proposed model showed that the blockchain technology could leverage Kaduna Polytechnic certificate authentication. It fulfils all the conditions necessary for a modern verification system for certificates. It also addresses the holes and obstacles in the existing methods for checking the validity of educational certificates.

IJSER

Keywords – *Metmask, Ethereum, authentication, hash, cryptography.*

1. INTRODUCTION

As stated by Warasart & Kuacharoen (2012) in their work titled Paper-Based Document Authentication Using Digital Signature and QR Code, institutions issue certificates to students who have completed graduation requirements. They further stated that a graduation certificate is mostly in the form of a paper-based document as an electronic document cannot effectively replace a physical certificate. According to Chen (2017), the advent of advanced and cheap scanning and printing technologies has increased the falsification of certificates. This threatens the integrity of the holder of the certificate and the university which issued the certificate.

The analysis and review of the document has therefore become important tasks. The graduation certificate presented by the graduate must be validated that the holder is the rightful

owner or that the certificate is genuine. In addition, a certificate of graduation must be checked to ensure that its content is correct and that the certificate originates from a reputable source.

Research carried out by Singhal (2015) showed that educational institutions are working in various ways to counter fraud and forgery. Most of the techniques, however, take time because they are manual and require human interaction.

During the process, a great deal of time will be spent either approaching the university to validate a certification or waiting for a university to confirm that the certificate is legitimate, and that the data is correct. This process can be extremely laborious and costly, especially if a company needs to check several hundred applicants ' certificates.

This work therefore seeks to propose a solution for the authentication of educational certificates using blockchain technology.

Stuart Haber and W. Scott Stornetta (1991), two researchers who aimed to develop a system where document time stamps could not be manipulated with, initially proposed blockchain technology. Blockchain did not have its first real-world application until almost two decades later, with the debut of Bitcoin in January 2009.

Satoshi Nakamoto (2008) postulated the idea of Bitcoin Blockchain. A blockchain is the foundation of the Bitcoin protocol. Satoshi Nakamoto, the digital currency's pseudonymous founder, described it as "a new electronic cash system that is totally peer-to-peer, with no trusted third party" in a research paper introducing the digital currency. The blockchain technology is perfect as a new infrastructure that preserves and shares learning accomplishments and authenticates them.

Tengyu Yu (2016) described a blockchain as a decentralized database that is extensively used to record transactions. The transaction is added to a block that already contains records of numerous transactions whenever a consensus is obtained among different nodes. For a transaction to connect to a block chain, the block carries the hash value of its previous counterpart. The blocks are all linked together to form a blockchain.

We created a decentralized application and designed a certificate system based on the Ethereum blockchain in this research. A web-based interface is integrated in the system to serve as the interface between the users (School administrators, graduates and third-parties) and the Ethereum block-chain using Metmask and Solidity. Because it is incorruptible, encrypted, and trackable, as well as allowing data synchronization, this technology was chosen. The technology improves the efficiency of processes at each stage by incorporating blockchain technologies. The system reduces paper consumption, lowers administration expenses, avoids document counterfeiting, and delivers accurate and trustworthy information on digital certificates.

IJSER

The blockchain is a multi-functional hybrid software comprising hash, public and private key cryptography, digital signatures, peer-to-peer networks, and work evidence. Each is clarified as follows.

Hash

A hash is a fixed length short code. The input of data from a report into a hash generator results in a hash output containing a number of digits. Then this hash forms a unique identification. It results in the same hash value by entering the same data into the hash generator. According to Nomura Research Institute(2016), a small difference such as changing a single letter of text in data input results in a completely different hash. Figure 1 shows the mechanism of generating a hash.

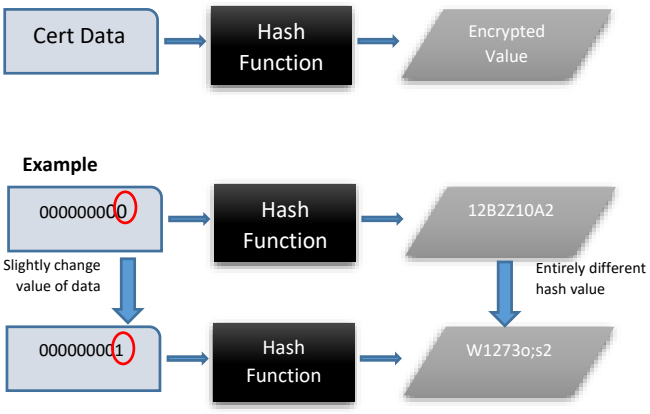


Figure 1. Blockchain hashing.

In Figure 1, it can be seen that a small change in the input of the data will result in a very different hash. This hash feature can be used to detect any data falsification and is used for encryption purposes in a blockchain system.

Public and Private Keys

This blockchain feature is based on the principle that different keys are created to encrypt and decrypt. In a blockchain, the public-key cryptographic approach is always used to create a private key for private use and a public key for public use as shown in Figure 2.

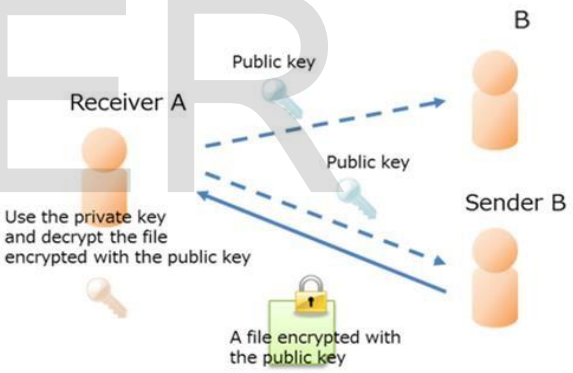


Figure 2: The Public Key Encryption

Thompson (2017) stated that this approach differs from the symmetric key cryptographic system which uses the same key for both encryption and decryption and where the delivery mechanism must be protected to the relevant party. Public key cryptography only enables the safe transmission and retrieval of files when the verifying party generates both a private and a public key and sends the public key to the recipient in advance. If the verifying

IJSER

party retains the confidentiality of the private key, the transaction's protection will be maintained even though the public key will be easily accessible to everyone.

Digital Signatures

As show by Chiyevo, both the hash and the cryptographic methods of the public key are used to establish a system of digital signature that can be used to verify the validity of data sent over the Internet. The digital signature is created by using the sender's public key to encrypt the hash value of the file sent to the verifying party. The report will also be uploaded to the verifier online. The verifier will use the data in the file to produce a hash value. Additionally, the verifier uses its private key to decode the digital signature and retrieve the hash value. It ensures that the electronic signature is genuine if the two hash values matched, and the data contained in the certificate has not been altered.

Peer-to-Peer (P2P) Network

X. Technologies (2017) stated that a software or network architecture that shares tasks, work, or files among peers. Peers are network members with fair operational rights and resources. Each computer or client on the network is called a node in a P2P network and consists of a P2P node network.

Ethereum

Ethereum is a decentralized, open platform with Turing completeness and support for a variety of derivative applications. Ethereum is used to generate the majority of smart contracts and decentralized autonomous entities.

Ethereum would be the global computer system if the Bitcoin blockchains were deemed a global payment network. It provides a platform on which developers can build applications. Ethereum and those developers work together to build and maintain the infrastructure.

Ethereum Virtual Machine (EVM)

The Ethereum Virtual Computer (EVM) is a decentralized virtual machine that uses a worldwide network of public nodes to run scripts. Using a high-level language called Solidity, developers direct the EVM to execute programs.

Solidity

The programming language Solidity is used to create smart contracts.

Smart Contracts

A smart contract, also known as a crypto contract, is a computer program that governs the direct transfer of digital money or assets between two parties under specific conditions.

Ethash

The proof-of-work function of Ethereum-based Blockchain currency is called Ethash. It is a hash function that belongs to the Keccak family, which also includes the SHA-3 hash

IJSER

functions. Ethash, on the other hand, is not a SHA-3 function and should not be confused with it.

MetaMask

MetaMask is a browser extension that allows you to access Ethereum-enabled distributed applications, or "Dapps." The addon injects the Ethereum web3 API into the JavaScript context of every website, allowing Dapps to read from the blockchain.

Node JS

Backends are written in Node JS, which is also in charge of supplying frontend pages, assets, and user authentication through JWT (Json Web Token). It also includes web3 as a requirement, allowing us to run solidity code on the frontend.

Remix IDE

Remix IDE is a web and desktop program that is free source. It promotes a quick development cycle and includes a large number of plugins with user-friendly interfaces. Remix is utilized for the full contract development process as well as a learning and teaching environment for Ethereum.

The Remix IDE is part of the Remix Project, which provides a framework for plugin-based development tools. Remix Plugin Engine, Remix Libs, and, of course, Remix-IDE are among the sub-projects.

Remix IDE is an open-source application that allows you to write Solidity contracts directly from your browser.

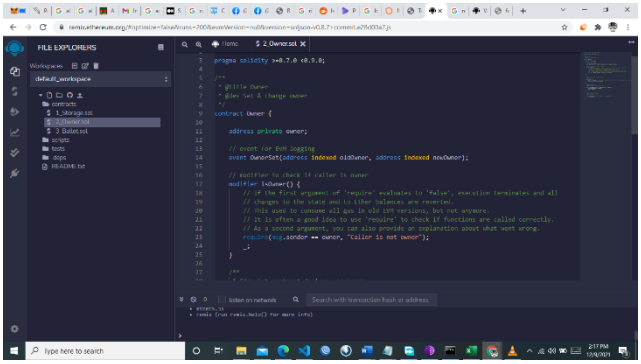


Fig 3 Remix IDE

Code Igniter

Code Igniter is used to develop our frontend, and it has the goal of creating a better user experience in the frontend for the end user by giving features such as no page reloading on page switch and quick site loading.

Bootstrap

Bootstrap is a powerful front-end framework for building modern webpages and web applications. It's open-source and free to use, however it comes with a plethora of HTML and CSS templates for UI elements like buttons and forms. JavaScript extensions are also supported by Bootstrap.

MySQL

MySQL DB is a database that is used in this project to store information about users and

IJSER

their authentication in an encrypted format, as well as information about their session.

IPFS

The InterPlanetary File System is a distributed file system that uses a peer-to-peer network to store and share data. In a global namespace connecting all computing devices, IPFS uses content-addressing to uniquely identify each file.

2. Literature Review

Holt (2006) proposed an approach for storing logs in an encrypted format that is difficult to modify and can be easily identified if it is modified. He focused on the security elements by breaking down the log production and verification processes. However, this system has a setback which is the fact that the log resides on a server or few servers which makes it possible to target those servers and modify the logs with the advance hacking skills. The log, in itself, is difficult to modify but not impossible.

Trong Thua Huynh and Dang-Khoa Pham (2019) introduced Blockcerts, a blockchain-based application linked with the open badge ecosystem, is the first notable use case for holding a hash of certificates. Blockcerts is a middleware that allows you to issue and retrieve certificates over the Internet. Employees can acquire a verifiable, tamper-proof version of their certificate that they can share with employers and other organizations via a wallet. Blockcerts, on the other hand, has several disadvantages. Blockcerts ties itself to the Bitcoin market at fluctuating rates by connecting to the Bitcoin network, making the requirements for granting certificates uncertain. Furthermore, as the Bitcoin network grows in size, the cost of adding a new node to the network increases.

Sutton and Samavi (2017) delivered a paper titled "blockchain enabled privacy audit logs," which focuses on data integrity and authenticity using the linked data technique. This work struggles to secure the audit log but not the certificate itself.

Both Mozilla Open Badges and Badgr (2012) provided unified solutions for managing a student's whole educational history by aggregating all digital certificates received at various academies and linking them to a single identity. Despite the fact that these solutions do not utilize blockchain, they demonstrate how to combine numerous certificates into a student's identification. However, it lacks immutability.

A study carried out by Chiyevo (2015) showed that blockchain technology removes the need for credentials verification by educational organizations. Since certificates issued on the blockchain can be verified automatically,

IJSER

educational organizations are no longer required to commit resources to this task.

Public key infrastructure (PKI) replaces the central authority with a very stable decentralized architecture that increases the durability of the network due to the numerous block duplicates where the signatures are stored. Blockchain decentralization forbids third parties from modifying or removing block-kept transactions unless they violate the proof-of-work condition that validated them. Blockchains also offer independent time stamping, which increases security.

Chiyevo further stated that in circumstances where passwords will expire, it is necessary to have a correct timestamp. In response to a key leak, the issuer must also rotate issuing keys on a regular basis for protection. While deciding whether a record was released by a particular issuer during key validity, an independent timestamp is required. Blockchain signatures are independent of file format as opposed to many PKI schemes.

3. Methodology

This project varies from other Ethereum based certificate verification in the sense that it does not only verify the authenticity of the certificate but check the existence of similar certificates. This handles a loophole in other similar researches. A compromised personnel in the certificate administration department may re-enter another certificate into the blockchain since the first entry is immutable, and when the second certificate is verified, it will be found to be authentic however in a situation where all previous entries resurface, then a red flag will be raised.

The system has three categories of human elements, the administrator, graduate, and inquiring party.

Administrator: is responsible for the generation of the certificates and takes responsibility for the content of the certificate with is logged as part of the transaction. This will make the administrator cautious in carrying out his/her duties.

Graduate: the graduate will have access to the certificate upon login. Ideally, a hard copy will be issued to the graduate by the Institution which has the hash of the blockchain transaction containing the graduates record and meta-data. The certificate serial no. can also be used to verify a certificate and it returns the hash key as well.

Inquiring party: This is the person or company that is interested in the integrity of the certificate. The inquiring party is most likely an employer or an institution for further carrier progression. The graduate may also inquire if he/ she deems fit.

System design and architecture

IJSER

The system's application will be built on the Ethereum platform and run by the Ethereum Virtual Machine (EVM). Smart contracts will be employed in the backend. The smart contract was created in the Solidity programming language.

The commands are compiled by default compiler in Remix IDE, during the compilation process, some gas is decreased from the ether balance which would be prompted by Meta-mask.

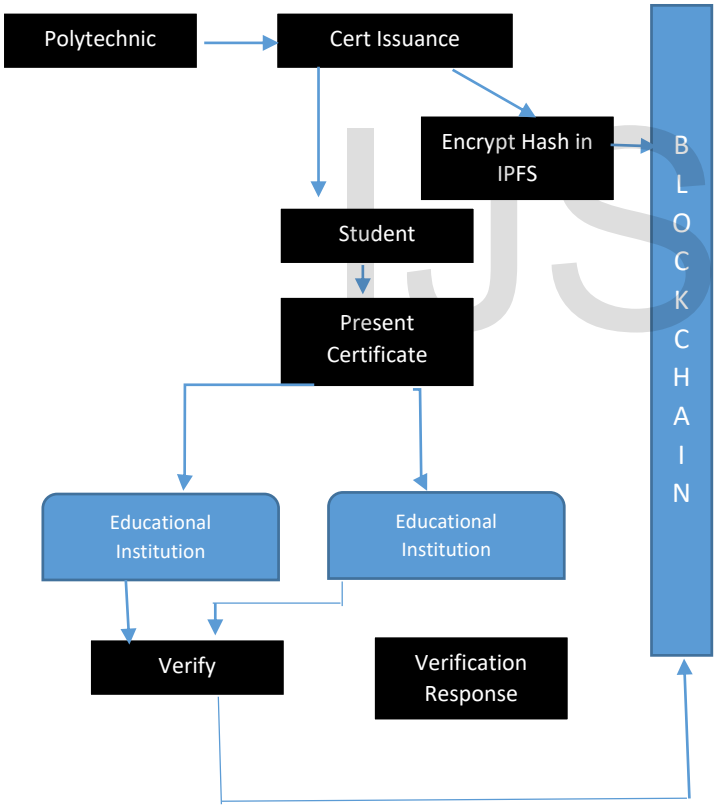


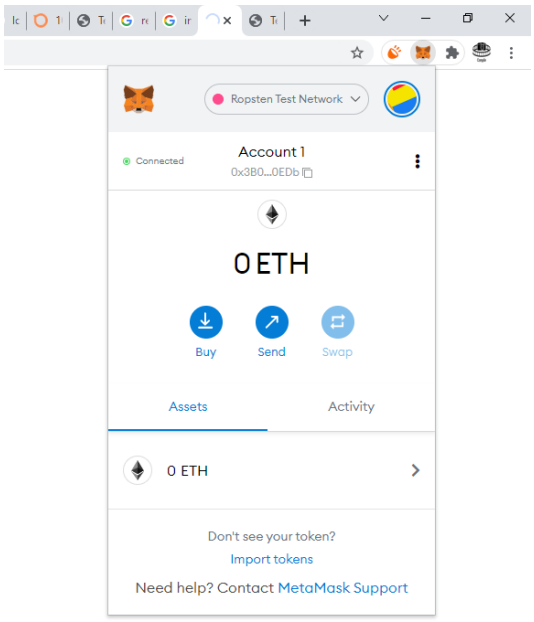
Fig 4. System architecture

The school (Kaduna Polytechnic) will issue certificates, have system access, and be able to submit certificates to IPFS storage via the web interface as shown in Fig 4. The graduated students are the second group, when students meet certain criteria, the authorities will issue a certificate via the Blockchain. Students will be able to inquire about any certificates they have obtained after they have gotten their certificate.

With the use of the certificates digital signature (cert SN number) and Quick Response code (of the transaction hash), the company or graduate's employer will be the user who can request for information about the document's originality, authenticity, and integrity. The interface in Fig. 9 serves as the point where both students and inquiring companies or institutions will verify the authenticity of the certificate.

System Process

All of the operations are carried out utilizing HTML and JavaScript on a webpage which is the front end. The front-end cannot communicate with the Ethereum blockchain the way conventional programmes communicate with databases via backend programmes like PHP or Python. A web3 technology called Metamask is the API through which the frontend communicates with the smart contracts to send and retrieve data to and from the Ethereum blockchain. Metamask also shows the amount of ether that is available for transactions. Each transaction(i.e. operation on the blockchain guided by the smart contract) requires some ethers. The Metamask will prompt the user for approval of the transaction before the transaction is carried out.



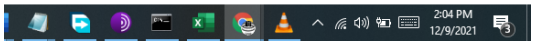


Fig 5. Metamask

The Polytechnic must generate certificates and sent to the Interplanetary File System (IPFS). IPFS is used to generate hash values for each certificate, which were then put in blockchain. Students can examine their certificates on a webpage during verification and, if necessary, download the hash from the blockchain, as indicated in the sequence diagram (Fig 6).

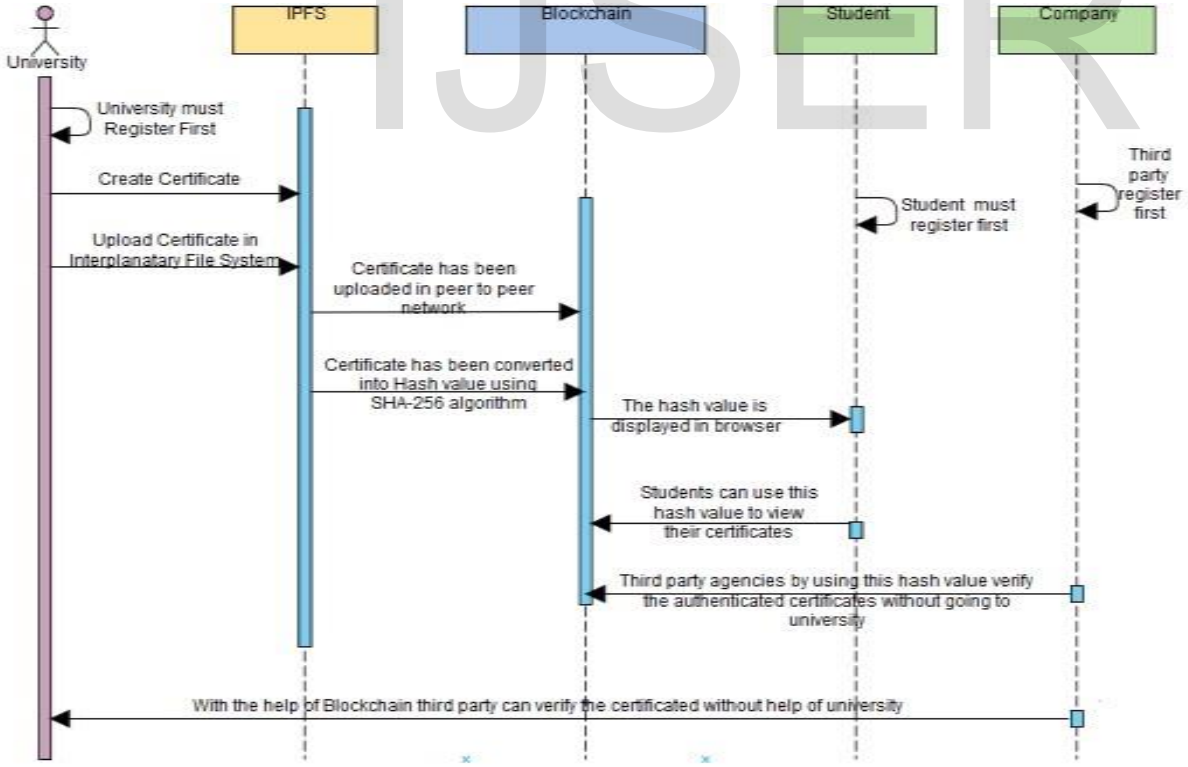


Fig 6. Certificate Creation, IPFS Entry and Addition of Certificate to Blockchain

IJSER

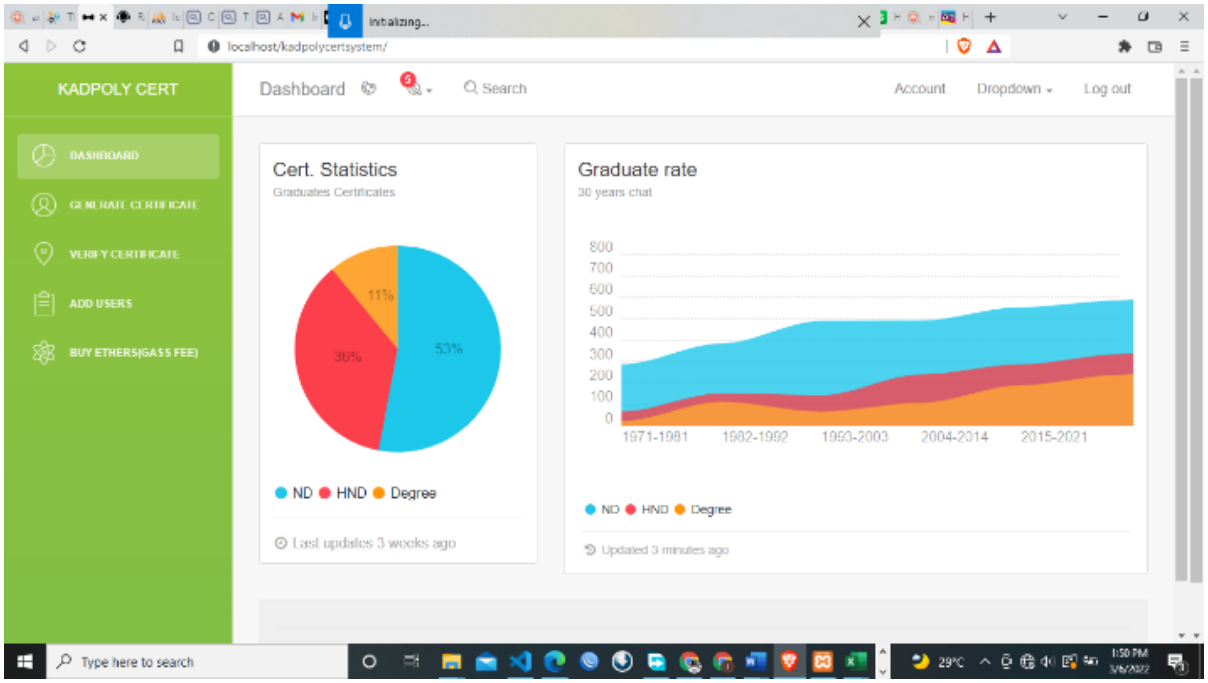


Fig 7. The Dashboard of the Front-end Web Page.

IJSER

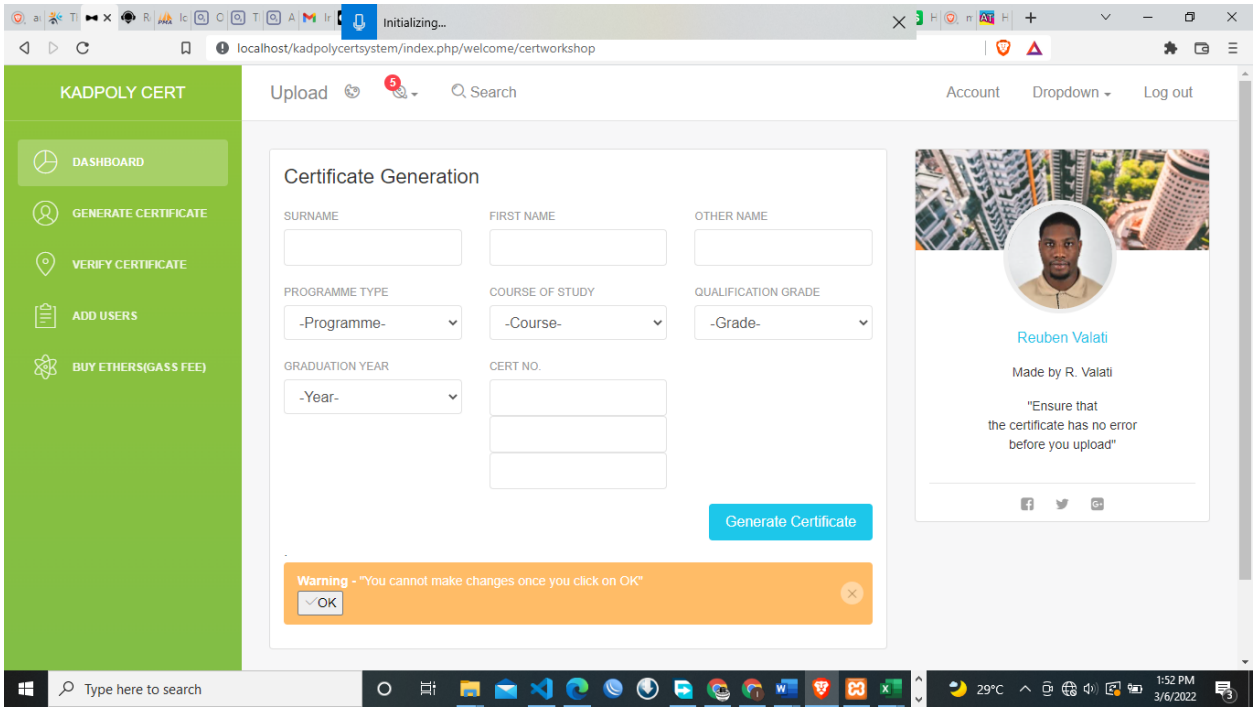


Fig 8. Certificate Generation Page.

IJSER

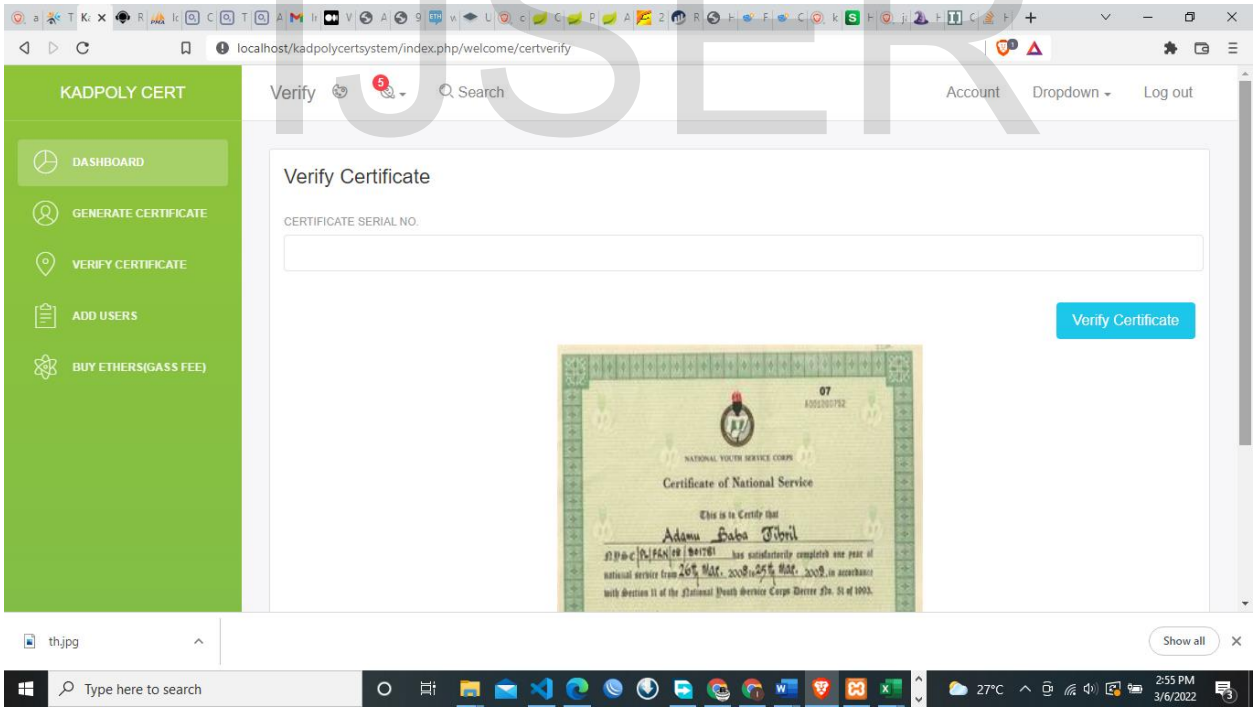


Fig. 10. The Hash Value of a student retrieval.

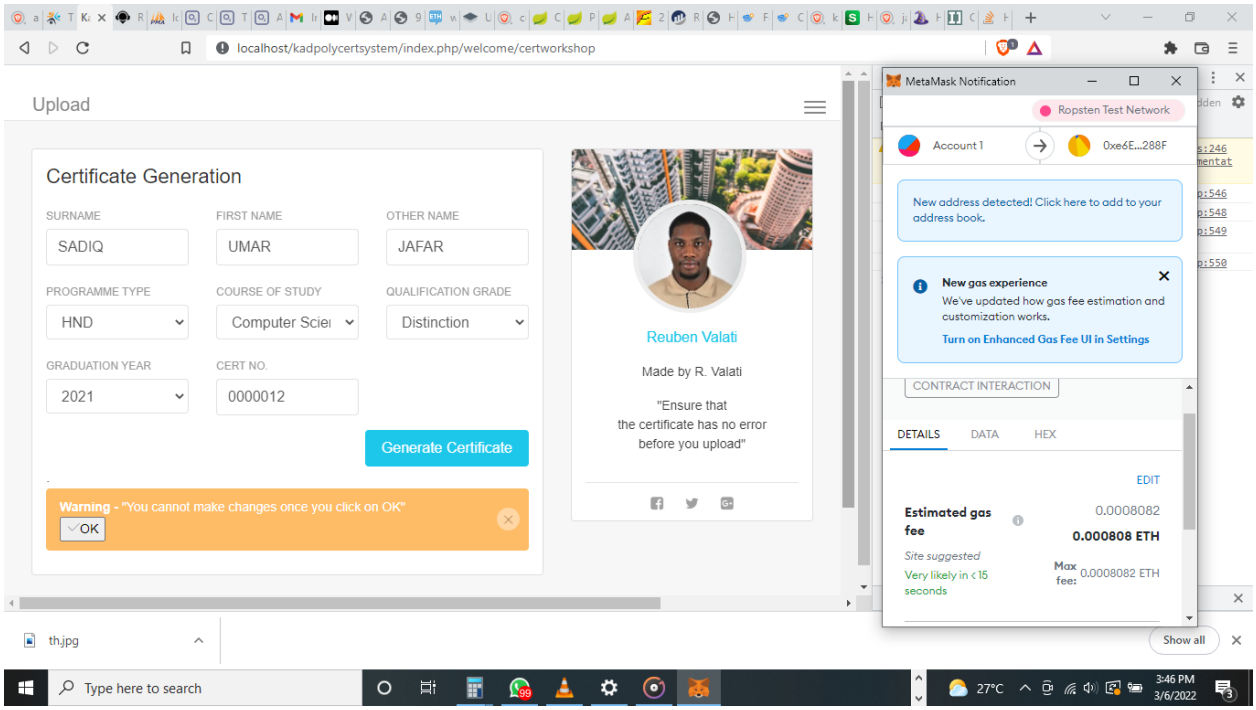


Fig 11. Metamask prompt for gas fee for certificate generation transaction.

IJSER

4. Result

The findings of this study show that after the Polytechnic generates the certificate for each and every transaction, some ether is used in Metamask (Fig.11) and the certificates are stored in IPFS, with the resulted hash value displayed on a webpage during verification (Fig. 10) using the SHA-256 algorithm, and the certificate can be viewed during the verification process as shown in Figure 10.

5. Discussion

The following are some of the facts of our implementation:

Only the Polytechnic can generate the certificates and push to the Ethereum blockchain because only the users that have been created with access can will be allowed by the test-user integrity contract on the blockchain. Unlike on a conventional database, the users, like the certificate, are immutable.

It is also worth knowing that some cost will be incurred in the form of gas, the Ethereum blockchain involves the use of an extremely large number of peer-to-peer servers and the mining process requires a lot of processing power. This is why the Institution will have to buy ether-gas just like air-time for text messaging. As you send messages, your

airtime reduces, similarly as you add certificates to the block chain, the gas reduces.

The inter-planetary file system does what it does best, it keeps record of the certificates and distribute it to all computers on the network on a peer-to-peer bases.

Once the certificate is successfully added to the chain, the generated hash value representing the certificate is sent to the web page via MetaMask.

The graduate and employer of the graduate or any other relevant body that is deemed fit to verify the certificate can do so as explained earlier.

6. Conclusion

One of the key values of Blockchain is the creation of immutable ledgers. This characteristic aids us in creating a system in which all processes are transparent and immutable. Our system streamlines the process of creating certificates and decreases the amount of manual effort required to verify them. Students also have a low chance of losing their certificate. We can reduce the percentage of data that is tampered with by utilizing an additional hashing technique. The certificate's hash is kept in the blockchain, while the original document is kept in the Inter Planetary File System (IPFS). This will aid in data preservation and transparency.

IJSER

REFERENCES

[1] A. Singhal, “Degree Certificate Authentication using QR Code and Smartphone,” vol. 120, no. 16, pp. 38–43, 2015.

[2] E. Chiyevo Garwe, “Qualification, Award and Recognition Fraud in Higher Education in Zimbabwe,” *J. Stud. Educ.*, vol. 5, no. 2, pp. 119–135, 2015.

[3] M. Warasart and P. Kuacharoen, “Paper-based Document Authentication using Digital Signature and QR Code,” no. Iccet, 2012.

[4] Nomura Research Institute, “Survey on Blockchain Technologies and Related Services,” 2016.

[5] Nakamoto, S. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf

[6] S. Balasubramanian, R. Prashanth Iye, and S. Ravishankar, “Mark sheet verification,” *2009 3rd Int. Conf. Anti-counterfeiting, Secure. Identify. Commun. ASID 2009*, 2009.

[7] S. Thompson, “The preservation of digital signatures on the blockchain - Thompson - See Also,”

Univ. Br. Columbia iSchool Student J., vol. 3, no. Spring, 2017.

[8] T. Healy, S. Cote, J. Helliwell, and S. Field, "The Well-Being of Nations - The Role of Human and Social Capital," *Oecd*, p. 118, 2002.

[9] X. Technologies, "Blockchain imperative for educational certificates," *Xanbell Technologies*, 2017.

[10] Z. Chen, "Anti-Counterfeit Authentication System of Printed Information Based on A Logic Signing Technique."

IJSER