Blockchain-based academic certificate credentialing system for Asia Pacific University

Lim Gin Keat
School of Computing
Asia Pacific University of Technology and Innovation (APU)
Kuala Lumpur, Malaysia
lionellimgk98@gmail.com

Lee Kim Keong
School of Computing
Asia Pacific University of Technology and Innovation (APU)
Kuala Lumpur, Malaysia
kimlee@apu.edu.my

***Abstract*— Certificates play a significant role in business education and professional development. Individual records of learning become essential for the professional careers of individuals. Consequently, it is critical that such records are kept inaccessible long-term and tamper-proof ledgers. A blockchain records transactions in a verifiable and permanent manner, so it is very appropriate to store certificate fingerprints or other educational items. Blockchain exposes certificate forgery and promotes the history of learning. The Blockchain-Based Academic Certificate Credentialing System could be a feasible solution in this research for issuing, validating, and sharing certificates in a digital format using blockchain technology. Therefore, the aim of this research paper is to propose a theoretical model and develop a Blockchain-Based Academic Certificate Credentialing System that can support counterfeit protection as well as secure access and management of academic certificates according to the needs of learners, education institutions, and employers using Blockchain technology. Using the characteristics of blockchain technology offer including hash, public& private keys, cryptography, digital signature, peer-to-peer networks and smart contracts. Conclude into an academic certificate credentialing system that meets all the aims and objectives, offer a faster, more straightforward and more secure way to issue the academic certificate and aiding the process of validation and verification.**

***Keywords*— Blockchain, academic certificate management, smart contract**

I. Introduction

Academic certificates are the standard that determines whether the student has achieved certain learning requirements and are until today mostly on paper or other physical formats. The Academic certificate includes several statements which consist of the kind of qualification or academic title that is attested, information of the issuer university, name and signature of the certifier who has validated the facts and certify that the certificate qualification is true and most importantly the basic information of the receiver or learner. Learners or students are still receiving a hard paper copy of certificate from Asia Pacific University of Technology and Innovative nowadays. The paper certificates have their advantages as it is difficult to forge due to the build-in security features that came with it. Moreover, the paper certificates can be easily store and bring out to show them to any employers or for any purpose. However, there are some disadvantages such as employers as a third parties have to manually verify the paper certificate manually and the need for certification authorities to maintain the registry and database of certificates.

Based on multiple studies, the idea of providing an alternative to paper certificates is to utilize blockchain technology to create digital certificates that are cryptographically signed. In cope with a recent news report by The Star [1], stated that an estimated one in 20 potential hires in Malaysia has fake qualifications while one in 10 has credentials from unaccredited institutions, a corporate fraud investigation agency found. Hence, the digital certificates that utilize blockchain technology can provide counterfeit protection for certificates, ease the verification process of certificates as even the certification authority will no longer exists and the certificate should be confidential so that it can only be viewed by authorized persons with a time-limited validity. Potentially, reduce the incidence of certificate forgeries and ensure that the security, validity and confidentiality of the academic certificate can be improved. Nicosia University is the first university that uses blockchain technology to handle the certificates of students acquired from MOOC platforms. [2] In addition, the Massachusetts Institute of Technology (MIT) and the Learning Machine company worked together to develop a digital Blockchain-based online learning badge. Students who have participated in MIT Media Lab projects and passed the test will receive a credential that will be held in a blockchain network. [3]

In this research paper, the research will analyses deeper about the disruptive potential of the blockchain technology for education from journals and articles made by other developers. Focus on the relevance of blockchain technology to education, to understand its components for blockchain technology to be adapted for educational use. In addition to that, there will also be a comparative analysis between the similar system of academic certificate credentialing system utilizing the blockchain technology, in terms of its functionalities, system architecture, process and so on.

II. Literature Review

A. *Current process flow of awarding academic certificates to students in most academy institutions*

In the current situation, the certificate authorities in each respective universities or institutions managing their student's data, learning courses titles and other relevant information as well as the important exam result using MS Excel sheet. When the students graduated from the universities or institutions, the authorities will issue a paper academic certificates to the graduates. Whereby the authorities will retrieve the data and examination result from their legacy system, the process for the authorities to search for the academic information of the students might take a long time and troublesome. At present, most universities and institutions have built-in security features in their academic certificates. When graduates go for a job interview the graduates must bring along the paper academic certificate. Then, the employer must contact the universities or institutions for the authentication and validation of the certificate, which is consider time-consuming and troublesome process.

B. Blockchain

1) Definition

Under the pseudonym Satoshi Nakamoto, the white paper for Bitcoin was published in 2008 [4]. Nakamoto introduces Bitcoin, an electronic payment network inside a peer-to-peer network that doesn't require users to trust any other entity. There were other systems for making safe electronic payments in a peer-to-peer network at the time, but none of them solved the issue of double spending without a trusted third party. The issue of double spending means one user could make numerous payments on the same asset.

The solution is simple with a trustworthy third party involved; the recipient simply asks them if the asset was previously spent. [4] By designing what he called a "block chain," Nakamoto solved this problem. The term blockchain is used a lot nowadays. The term comes from the data being stored in blocks, where each block contains the previous block's hash value and thus a chain is formed.

Narayanan et al. [5] describe that the structure of a blockchain looks like a linked list with hash pointers. Each of the block on the block contain hash of the transaction and the previous block’s hash value. This data structure proves to be a tamper-evident log, the blockchain can only append new block but it is impossible to alter or delete the existing data.

Iansiti and R. Lakhani [6] define a blockchain with the sentence below:

> *“... blockchain is an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way.”*

There are four basic properties of the blockchain technology:

a) Distributed Database – each node or network users act like a database or an entity itself.

b) Peer-to-peer transmission. Each of the transmission is transmitted between two independent nodes. There are no intermediate and central nodes.

c) Irreversibility of Records and Security. When a transaction is added to the database, the transaction cannot be altered. This is because of the blockchain's chain structure. The blockchain is secure against tampering and the data is immutable.

d) Computational Logic. Transactions can be programmed according to algorithms and rules to occur automatically.

Blockchain is a decentralized distributed ledger with itself own rule’s collection where data are store in each of the node on the blockchain in the network.

A blockchain’s basic data structure look like just what it describes it is like a block chained together interconnected among each other. In each of the block consist of the transaction data along with the timestamp with it, each of the block’s transaction can be verified using its own hash value. The blockchain is open and data can be publicly viewed but once it entered the data in the block cannot be revoked or deleted which helps to prevent forgery. Moreover, each of the block is interlinked together with the previous block with the hash value preceding block. If one of the block data is changed in the blockchain, the hash value of that block will also be changed. [7]

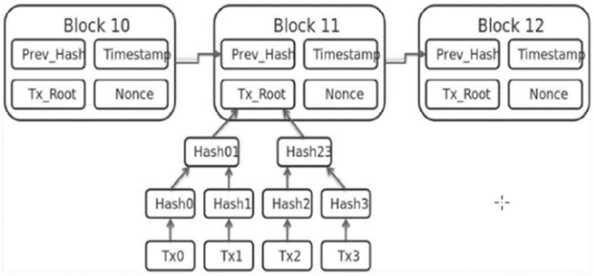


Fig. 1. Basic structure of blockchain. [7]

2) Public & Private Blockchain

a) Public Blockchain

Public Blockchain is permissionless, which allows anyone can simply join and get access to the network and perform read, write, or participate within the blockchain. The entities are decentralized, where it does not have a single entity controlling the network. The data on the blockchain network will be impossible to modify or alter once they have been validated on to the blockchain.

b) Private Blockchain

Private blockchain requires permission to gain access control to the blockchain network, which restricts the people that can participate in the blockchain network. There can be one or more than one entitles controlling the network, which is represented as a reliance on the third parties to transact.

c) Similarities

Both public and private blockchain function only as an append-only ledger where the record appended on the blockchain cannot be altered or deleted, which considers them as immutable records. Each of the entities on the network node in both of these blockchain has the complete replica of the ledger over the peer-to-peer networks of entities. The records in both of the blockchain network are verified by the considerable level of the immutability of the provided blockchain network until a majority of the blockchain participants have agreed on the record, considering it to be valid and reached consensus.

d) Differences

A private blockchain is much lighter and provides transactional throughput in the order of the magnitude compare to the public blockchain. The level of access granted on both of the blockchain networks are different where anyone can join and access control on the append and verify the process of a public blockchain. On the other hand, private blockchain only allows access to authorized entitles to join and gain control access on the network. A public blockchain is more decentralized, whereas a private blockchain is more centralized.

The transaction process time on a private blockchain will be much shorter due to the less authorized participants in the private blockchain. This is because public blockchain has more nodes to manage, and the transaction will only process at a much slower pace as a consequence, it will also consume more computational resources to perform the transactions. A public blockchain is more secure and trustless between its network nodes due to the decentralization and active participants having a higher nodes numbers on the network, it is nearly impossible to have "bad actors" to perform attacks on the system to gain full control over the consensus network. [8]

3) Public Key Cryptography

The use of this tool is to develop protocols that prevent a third parties from viewing the private data. In nowadays the cryptography has a combination of the disciplines of math, computer science, physics, engineering, and more. [9]

Some important terms are defined below:

a) Encryption: Encoding data into an unreadable format

b) Decryption: Reserving encryption – converting encrypted data into its original form.

c) Cipher: An algorithm for performing encryption or decryption, usually a well-defined set of steps that can be followed.

In every blockchain application, public key cryptography has been using and involving the generation of private key, with the use of the pair of a public key and a private key to perform different tasks. Using the public key to perform encryption so that only the decryption process can only be done with a unique and specific private key. The process can maintain the authenticity of document.

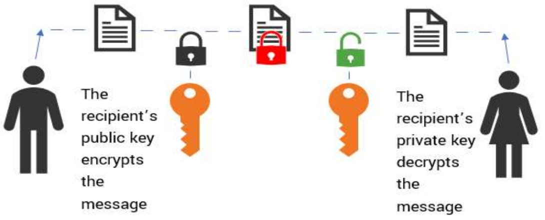

The recipient's public key encrypts the message
The recipient's private key decrypts the message

Fig. 2. Public key cryptography process

4) Hash Function

A function that takes any length of a string input and produces a fixed length of string accordingly to the type of encryption used. If a hash function like H is applied to the message like m and the resulting outcome would be the value of h. Based on the deterministic and requires a little of computational power. H(m) = h

5) Smart Contract

Smart Contract is a digital contract that contains the business logic and functionality formulated to be executed by the computer system if been called. A smart contract can also be like a person that is trusted with assets holding temporarily and follow the order when being programmed.

[10] A smart contract is used to run in the Ethereum blockchain platform with the uses of ETH, a type of token used in Ethereum, users can create many different services, applications, or contracts with it. [11]

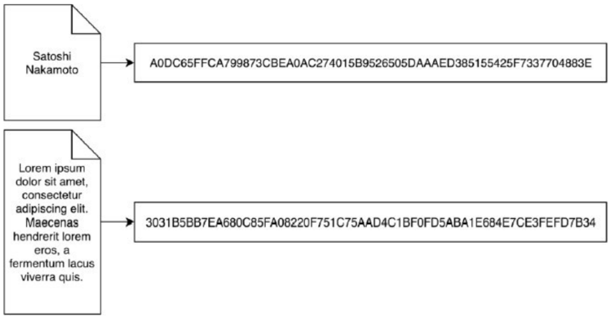

Satoshi Nakamoto
A0DC65FFCA799873CBEA0AC274015B9526505DAAAED385155425F7337704883E
Lorem ipsum dolor sit amet, consectetur adipiscing elit. Maecenas hendrerit lorem eros, a fermentum lacus viverra quis.
3031B5BB7EA680C85FA08220F751C75AAD4C1BF0FD5ABA1E684E7CE3FEFD7B34

Fig. 3. Two messages and their corresponding SHA-256 hash value.

Counterfeit academic certificates have been a longstanding worrying issue in the academic system. For a very long time, the needs of standard and certification have existed to ensure quality and purpose is fulfilled. An academic certificate is a standard that determines whether the student has achieved specific requirements on academic standards. Currently, the Asia Pacific University of Technology and Innovative University is still distributing certificates in the form of hard copy. Graduated students that apply for jobs at any private or public company sector have to produce those hard copies of certificates.

In contrast, the organizations or companies have to verify all the certificates manually, which could be a very time-consuming process. By any chance, there could also where a counterfeit academic certificate that is not legit may get unnoticeable by the verifier during the verifying process. Recently there has been an article by The Star (2019) [1], stated by the director of Akhbar & Associates, this agency undertakes background checks on potential hires for companies, said that 5% to 7% currently in the workforce have fake degrees while 10% to 15% have their degrees from unaccredited universities.

Counterfeit certificates can be easily purchased online at a low cost instead of paying a hefty price and undergoing a long process in getting a legit academic certificate. With the counterfeit certificate, buyers can find different curative narratives of their experiences for different purposes. Besides that, human tends to make a mistake where importing data and analyzing results from legacy systems is an important first feature for certification authorities, wrong information might be inserted into the paper certificate.

The student has to apply a new copy from the university and have to wait a couple of days to receive it, which might cause inconvenient and time-consuming for the students. Currently, employers only receive copies of the learner's paper certificates, occasionally notarized copies. In the first circumstance, employees can only prove the validity of the copies by requiring the authenticity and validity of the certificate from the issuing university, which is a time-consuming and costly process.

The main aim of this research is to develop a Blockchain-Based Academic Certificate Credentialing System that can support counterfeit protection as well as secure access and management of academic certificates according to the needs of students, university, and employers using Blockchain technology. The objectives of this research are:

- To lower the cost of paper academic certificate by replacing it with digital certificates store in the blockchain.
- To improve the productivity of administration staff as a digital certificate can be created in a much shorter time than a paper certificate.
- To ease the verification process whereby inserting the URL link of the applicant digital certificate, an employer can get an immediate get an authentication response.
- To allow easy tracking for the existing student record of a digital certificate by the administration staff.

III. SIMILAR SYSTEM

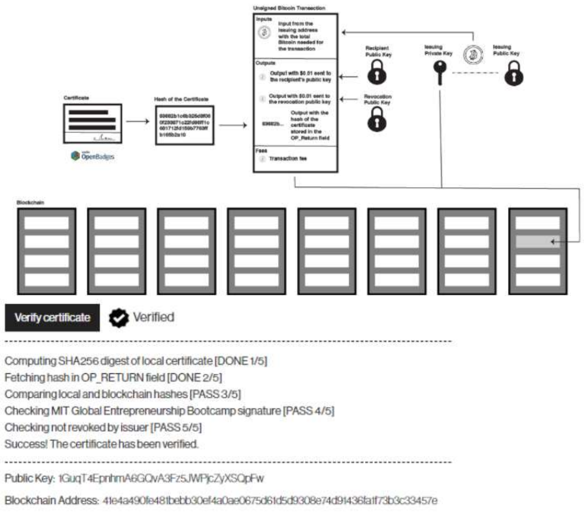
A. Blockcerts

BlockCerts is an open-source software tool that is developed by the researchers in the MIT Media Lab, which uses blockchain technology and Open Badge specification that allow users to issue, share, view, and verify the digital certificates for the academic purpose of non-academic achievements. [12] The aim of this system is to prevent fraud and support the management of various certificates and achievements. This system has already been deployed at the MIT University where they issue certificates for achievements, for example, the participants of the MIT's Global Entrepreneurship Bootcamp.

How BlockCerts work is that it consists of three repositories or tools for performing their digital certificates, which are Cert-schema, Cert-issuer, and Cert-viewer, each of them describes the mandatory data fields or standards for the digital certificate documents. On the specification of the Open Badges, Cert-issuer will be issued on the blockchain, which Cert-issuer will convert the certificate documents into hash value and perform a transaction using bitcoin from the issuer's address to the recipient's address on to the blockchain. Then which the Cert-viewer can view and verify the digital certificates that are place on the blockchain. [13]

The flow of the system architecture is relatively simple, starting from the issuer creates a digital document of the certificate with the necessary information needed on the document (e.g., recipient's name, issuer's name. issue date) based on the structure standard of the Open Badges. After that, the issuer will cryptographically sign the digital certificate with their private key, which adds the signature to the digital certificate itself.

The recipient or student will receive a copy of the digital certificate that allows the student to store the digital copy in any electronic devices or even print a hard copy for himself. Next, in order to place the digital certificate onto the Blockchain, the issuer will create a hash of the cryptographically signed digital certificate and perform a bitcoin transaction using the Cert-issuer tool to store the hash into a new block and chain it onto the blockchain. Now, the authenticity and legitimacy of the digital certificate will be stored onto the blockchain, in which students can now share the digital certificate to the employer to perform verification. Using the Blockcerts system, the employer can verify or compare the hash of the presented digital certificate with the hash value stored in the blockchain to verify the certificate content and check the cryptographic key used to sign the certificate correspond to the issuer's key to verify the issuer. [12]


Unsigned Bitcoin Transaction
Inputs
Input from the issuing address with the total Bitcoin needed for the transaction
Outputs
Output with $0.01 sent to the recipient's public key
Output with $0.01 sent to the revocation public key
Output with the hash of the certificate stored in the OP_Return field
Fees
Transaction fee
Recipient Public Key
Issuing Private Key
Issuing Public Key
Revocation Public Key
Certificate
OpenBadges
Hash of the Certificate
Blockchain
Verify certificate
Verified

```
--------------------------------------------------------------------------------
Computing SHA256 digest of local certificate [DONE 1/5]
Fetching hash in OP_RETURN field [DONE 2/5]
Comparing local and blockchain hashes [PASS 3/5]
Checking MIT Global Entrepreneurship Bootcamp signature [PASS 4/5]
Checking not revoked by issuer [PASS 5/5]
Success! The certificate has been verified.
--------------------------------------------------------------------------------
Public Key: 1GuqT4EpnhmA6GQvA3Fz5JWPjcZyXSQpFw
Blockchain Address: 41e4a490fe481bebb30ef4a0ae0675d61d5d9308e74d91436fa1f73b3c33457e
```

Fig. 4. Overview of the digital certification architecture.

B. EduCTX: A blockchain-based education credit platform

[13] have proposed a system named EduCTX, which is a Blockchain-Based Global Higher Education Credit Platform and Ecosystem. The system concept is built based on the European Credit Transfer and Accumulation System (ECTS). In which by implementing the existing ECTS system in the EduCTX system to create a globally trusted higher education credit assigning and recording system and to shorten the shortcomings of the ECTS system.

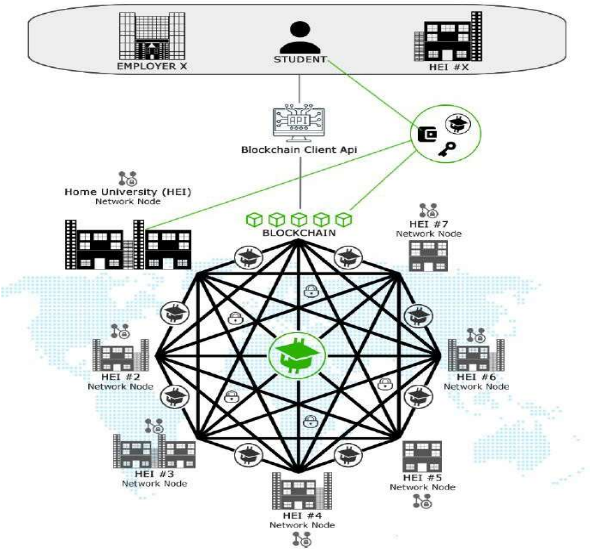


Fig. 5. Proposed EduCTX platform. [14]

The EduCTX initiative or ecosystem, students' achievements, or ECTS credits will be defined as ECTX tokens. There will be three types of stakeholders or users on the platform, 1. Student or Recipient that achieves the ECTX tokens 2. University or Higher Education Institute (HEI), who will be rewarding the tokens 3. Employer or HEI, who will verify the ECTX tokens of the Students or Recipients.

[13] The type of blockchain structure that EduCTX has chosen is the ARK Blockchain, mainly for their open-sources and the flexibility of the different programming languages supported by it. The process starts by a Higher Education Institute (HEI) joining the EduCTX blockchain network, which it then must first be recognized by the existing HEI members on the blockchain network. Then only the new HEI can create a blockchain wallet and set up a new node on the blockchain network.

When a new student enrolls in the HEI, a 2-2 (Keys of HEI and Student) multi-signature wallet will be created for the student to store his or her results and achievements ECTS credits information. Therefore, the institution's admins can transfer the correct number of ECTX tokens from the HEI's wallet to the student's 2-2 multi-signature wallet.

On the other hand, the ECTX tokens that are transferred to the students cannot be transferred to others' wallets. When then a student completed his certificate course, he or she sends the blockchain wallet address and collect a script to a prospective employer. The employer will perform the verification of the student's academic credit achievements or course completion through the blockchain web API. Using the technology of Delegated Proof of Stake (DPoS) consensus protocol to perform append information on to the blockchain that does not require computation resources as in Proof-of-Work (PoW) protocol in the bitcoin network and no random peer (HEI) can simply join the private blockchain network without the permission from the existing peer which provide a more secure and tamper-proof network. [13]

IV. SYSTEM ARCHITECTURE

The proposed system is built upon a technology stack called MERN stack and the Ethereum Blockchain. Under the hood of MERN stack are M – MongoDB as a local database, E – Express.js as a back-end API framework, R – Reacts.js as a library for building the user interface, and N – Node.js as a node manager, more details of the libraries used are mentioned in the Chapter 3 technical research. The front-end will be coded with HTML, CSS, and JavaScript to allow the user to interact with the Blockchain-Based Academic Certificate Credentialing System.

Furthermore, connecting to the MERN stack is the Ethereum blockchain this is where the generated certificates will be stored and be verified in the chain of blocks. With the use of blockchain principles, the composition of the technology already consists of several existing functions, including the hashing function, public and private key cryptography, and proof of work. Combined with these elements to formulate the blockchain, the features in this proposed system can be categorized into two-part, including issuing a Digital Academic Certificate and verifying the Digital Academic Certificate.

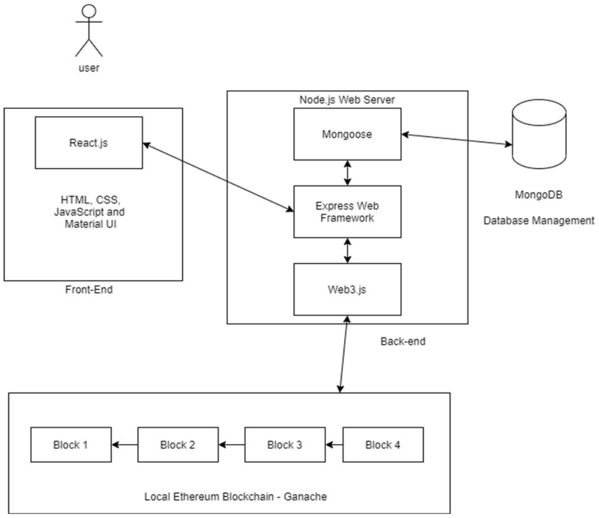


Fig. 6. System architecture of the proposed system

V. ANALYSIS OF THE PROPOSED SYSTEM

A. Issuing the Digital Academic Certificate

1) Hash Generation – the use of the SHA-256 hash generator will be used to generate hashes because it is publicly an open-source tool and very reliable. Converting any string of data into the SHA-256 hash.

2) Public and Private keys – the use of the public key and private key will be issued to the university. In turn, the public key will be in the form of a URL link to the students, and the private key will be kept confidentially.

3) Digital Signature – to perform the digital signature mechanism, both of the hash generation and public-key cryptographic will be put in use, which will validate the authenticity of information over the internet. The digital signature will first be encrypted with the hash value of the certificate file being sent to the student with the public key of the university. The private key will only be kept confidential by the university in MongoDB for the verification process, where it will decrypt the digital signature and extracted the hash value. In order to put in comparison to the two-hash values to verify the authenticity of the digital certificate and the data in it.

4) Timestamping – provide another layer of security to the digital certificates. The use of generating timestamps is the consideration of the entire time taken with precise day, month, and year to be stamped into the digital certificate and digital signature as a block of data that then be encrypted to produce a code on which data the document was issued.

5) Digitally Signing the Certificate – the digital signature on the digital certificate will be composed of the four elements mentioned above, including (i) the hash value, (ii) a public key, (iii) a private key, and (iv) a timestamp that indicate the precise time that the certificate was issued. The document will be wrapped up and signed by the generated hash using the public key and private key, combined with the timestamp, it will create a unique certificate id for the digital certificate. The digital signature now can only be decrypted by the private key, which is held by the university's database.

6) Issuing and Hosting the Digital Certificate – The university has issued a digital certificate to the student. The hash of the digital certificate compromises the unique alphanumeric string that cannot be tampered with its certificate and content. The hash will then be stored in the Ethereum Blockchain (Ganache local blockchain) via the communication with the API Web3.js and smart contracts that consist of the business logic and functionality for Ethereum usage.

B. *Verifying the Digital Academic Certificate*

In the job interview, the student brings along its public key, which is in the form of a unique URL link, the employer can verify the authenticity of the digital certificate through the Blockchain-Based Academic Certificate Credentialing System from the Asia Pacific University.

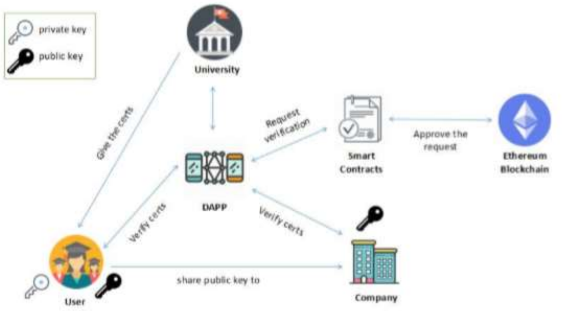


Fig. 7. Flow of the proposed system

VI. Potential Benefits of the Proposed System

A. *Tangible benefits*

- Reduce to almost zero for the production cost of the academic certificates and will be replaced as a digital certificate.
- Increase in time efficiency to issue a digital certificate, as the digital certificate can be issued anytime and anywhere in the world.
- Simple. With a digital certificate, the university can issue, recipients can receive, and relying parties can verify digital records without having to buy tokens, run a node, or become “members” of a network. Reducing the workload of administration staff, instead of preparing the certificate hard copy manually.
- Reduce the workload of administration staff and lecturers. Lecturer no need to manually tracking on who fail to submit their assignment, and they can just download student assignment instead of manually collect from the assignment submission department.

B. *Intangible Benefits*

- A digital certificate is more secure and immutable, the data will be encrypted by the cryptography and stored in a block. After the process of maximum trust verification, the block will be chained onto the blockchain. Where data will not be able to be altered or deleted, recipients can only show the contents of the specific digital academic certificate that the recipient had achieved.
- Traceable digital certificate. The viewer or verifier can search all of the transactions issued by the issuer as blockchain can be traced back.
- Convenient and easily accessible by the recipient. Digital certificates are sent peer-to- peer, directly from the issuing institution to the recipient. The recipient does not have an account to get access or share their records anywhere or anytime instantly.
- Privacy as no personally identifiable information (PII) will be stored in the chain. Instead, only the issuer and the recipient will have the “digital fingerprint” of the record for the specific Blockchain, because the digital certificate is sent directly peer-to-peer from the issuer to the recipient.

VII. Conclusion

In this research, the Blockchain-Based Academic Certificate Credentialing System will be using Blockchain Technology, which allows the university to issue academic certificate and employers or students to verify the given academic certificate through the APU E-Cert web application. Thereby, reducing the incidence of academic certificates forgeries and ensuring that the validity, security and authenticity of an academic certificate would be improved. The advantages of using a digital certification offer a faster, more straightforward and more secure way to issue the academic certificate and aiding the process of validation and verification. Besides that, it is much more portable by using the APU E-Cert web application, the verification and validation process can be done anytime and anywhere. Finally, the digital certificate will last a lifetime without a cost. As for the future enhancement, there are still a lot of functionalities and features that can be implemented such as using it as a document exchange verification, better security and collaborate and open up the system with the universities all over Malaysia. In proposed to fully eliminate and remove counterfeit academic certificate used in the job industry for job interviews.

References

[1] M. M. CHU and Y. YONG, "The Star," The Star, 6 May 2019. [Online]. Available: https://www.thestar.com.my/news/nation/2019/05/06/a-worrying-trend-in-msia/. [Accessed 24 Dec 2020].

[2] M. Sharples and J. Domingue, "The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward," *Institute of Educational Technology*, 2016.

[3] D. Skiba, "The Potential of Blockchain in Education and Health Care," *Nursing Education Perspectives*, vol. 38, no. 4, pp. 220-221 , 2017.

[4] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.

[5] A. Narayanan, J. Bonneau, E. Felten, A. Miller and S. Goldfeder, Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction, New Jersey: Princeton University Press, 2016.

[6] M. Iansiti and K. R. Lakhani, "The Truth about Blockchain," *Havard Business Review* , vol. 1, pp. 118-127, January 2017.

[7] N. Kumavat, S. Mengade, D. Desai and J. Varolia, "Certificate Verification System using Blockchain," *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*, vol. 7, no. 4, pp. 53 - 57, 2019.

[8] T. K. Sharma, "Public vs Private Blockchain: A Comprehensive Comparison," Blockchain Council, 2019. [Online]. Available: https://www.blockchain-council.org/blockchain/public-vs-private-

blockchain-a-comprehensive-comparison/#:~:text=Level%20of%20access%20granted%20to,Examples%20are%20Bitcoin%20and%20Ethereum.. [Accessed 24 December 2020].

[9] V. Lai, "What is Cryptography?," 2018. [Online]. Available: https://crushcrypto.com/cryptography-in-blockchain/. [Accessed 24 December 2020].

[10] A. Kosba, A. Miller, E. Shi, Z. Wen and C. Papamanthou, "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts," *IEEE Xplore*, pp. 839-858, 2016.

[11] H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu and J. Kishigami, "Blockchain contract: Securing a blockchain applied to smart contracts," *IEEE Xplore*, pp. 467-487, 2016.

[12] Schmidt, J. P., 2017. *Credentials, Reputation, and the Blockchain.* [Online] Available at: https://er.educause.edu/articles/2017/4/credentials-reputation-and-the-blockchain [Accessed 24 December 2020].

[13] MIT Media Lab Learning Initiative, 2016. *Blockcerts — An Open Infrastructure for Academic Credentials on the Blockchain.* [Online] Available at: https://medium.com/mit-media-lab/blockcerts-an-open-infrastructure-for- academic-credentials-on-the-blockchain-899a6b880b2f [Accessed 24 December 2020].

[14] Turkanovic, M., Holbl, M., Kosic, K., Hericko, M. and Kamisalic, A., 2018. EduCTX: A Blockchain-Based Higher Education Credit Platform. *IEEE Access*, [online] 6, pp.5112-5127. Available at: <https://ieeexplore.ieee.org/document/8247166> [Accessed 24 December 2020].