Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 07, July-2020

Education Degree Fraud Detection and Student Certificate Verification using Blockchain

Jayesh G. Dongre
Smt. Indira Gandhi College of Engineering
Navi Mumbai, India

Dr.Kishore.T.Patil
Smt. Indira Gandhi College of Engineering
Navi Mumbai, India

Sonali M. Tikam
Smt. Indira Gandhi College of Engineering
Navi Mumbai, India

Vasudha B. Gharat
Smt. Indira Gandhi College of Engineering
Navi Mumbai, India

***Abstract*— To verify the authenticity of an academic degree and certificates we propose a system which employs a digital signature scheme and timestamps using blockchain technology. As the number of universities and tertiary education students, the number of graduates is constantly increasing. Due to this verification process of these degree certificates generates a lot of new job opportunities. The sudden changes in the technology and development of new technologies like blockchain is booming, the implementation of blockchain using blockcerts software provides us a solution of plausible business models. In this paper we showcase two financial models balancing where the service rates is been balanced between graduates and employer as to main stakeholders of that service. A proof check of certificates for students is done at low cost and an easy check of the authenticity of the certificate is done from and trustable source while recruiting by the employer**.

Keywords*— *Blockcerts, Stakeholders, Tertiary, Recruiting

I. INTRODUCTION

Proving unambiguously that you have an academic certificate (university degree, doctorate, or any certification of studies) is a process that changes in each country or institution of education.

Some academic centres allow a quick and simple online query to verify the authenticity of their certificates, without even asking who requires that information. Some assign the role to third parties (whether by default or as required by regulations) or market the service. Finally, there are times when there is no alternative but to contact the office of the academic secretary at the educational institution directly, so that we can confirm if a diploma or qualification is valid or not. While, academic credential fraud is a fact and comes through counterfeiting, as well as through the involvement of the authorities and employees of the institution. The frequency of these events is also adequate to detect the emergence of dedicated companies.

- ***Internal Fraud:***

The fraud consists of applying to an educational institution 's academic records individuals who did not actually successfully graduate or credential. Sometimes with the participation of someone who's part of the academic institution, but not necessarily so. If the fraud occurs on the same date as the alleged graduation or qualification, technology does not offer a straightforward solution unless the individual involved is in possession of the private keys needed by a digital signature scheme. So if anyone wants to prove who is not a graduate in the past, a remedy is to use a time mark next to each diploma's digital signature. Therefore, if a person claims to have received a university degree a decade ago, then the digital signature with its timestamp must show that it was indeed ten years ago. In this way, modifying university records or databases avoids the creation of fake degrees in the future. Besides its cost, the issue with conventional timestamp technology is that it needs availability and faith in third parties (Time Stamping Authority) who validate the date. Then its legal use is not universal but up to every jurisdiction, and the possibility of bankruptcy, closure or negligence of who is certifying. On the other hand, chaining timestamps can reduce the risk of bankruptcy, closure or failure, but this additional complexity not only doesn't solve the problem at all (confidence is still required), but also requires perpetual maintenance to maintain the validity of the certified timestamp. The use of decentralized blockchain is a simpler, economical, and straightforward solution to correct the aforementioned drawbacks. Although the time accuracy in many of today's blockchains is far from ideal, it's more than enough where a date is needed (not the exact minute or second the certification was signed into). In this way there is no need for confidence or ongoing maintenance / payments to provide a clear timestamp. The method which uses a blockchain is the one already described. A cryptographic hash function is applied to the diploma and recorded in the public blockchain with a transaction which the academic institution digitally signs. Given the decentralized nature of a blockchain, the date on which the information was recorded can not be changed and is publicly verifiable without our trust being required by intermediaries.

Today's blockchain technology provides doors for implementing new business models on relatively concentrated markets. The use of blockchain in the education sector is one of the most challenging areas where mid- and long-term results can be achieved. One of the areas where blockchain can provide a timely and solid solution thanks to the use of widespread cryptocurrencies is the easy, trustable

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 07, July-2020

and cheap verification of official documents, such as university degrees. Here the selection of a suitable public blockchain in terms of availability, versatility and cost is crucial to the creation of a top-up sustainable business model. Within this paper we discuss the question of finding an economically viable solution to test university degrees automatically.

- ***Blockchain Technology:***

Blockchain is a ground breaking technology that enables new types of distributed software architectures, where components can find agreements on their shared states for decentralized and transactional data sharing through a broad network of untrusted users, without relying on a central point of integration that should be trusted by any component within the framework. The data structure blockchain is a time-stamped block list, which tracks and aggregates data about transactions that have ever happened within the blockchain network. Thus, the blockchain provides an unchangeable storage of data that only allows transactions to be inserted without updating or deleting any existing transaction on the blockchain to prevent tampering and revision. Blockchain's most famous application are cryptocurrencies, which during the last year was a huge phenomenon due to their promising use of the technology. The largest and most popular of them is Bitcoin [6], and along with newer ones like Ethereum, they are leading the cryptocurrency market at the 4-moment with more than 1,600 different currencies, with a market cap that last year was close to a trillion dollars, now over 300 billion dollars. Satoshi Nakamoto comments, as stated in the original Bitcoin paper [6]: A purely peer-to - peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures offer part of the solution, but if a trustworthy third party is still needed to avoid double-spending, the key benefits are lost. Using a peer-to - peer network we offer a solution to the double-spending problem. The network timestamps transactions by hashing them into an ongoing proof-of - work hash-based chain, forming a record that cannot be changed without redoing the proof-of-work, creating a record which cannot be updated without proof-of - work redoing. The longest chain serves not only as evidence of the sequence of observed occurrences, but also as evidence that it originated from the largest pool of Computing power. So long so nodes that do not collaborate to attack the network control a majority of CPU power, they can produce the longest chain and outpace attackers. This requires minimal structure for the network itself. Messages are distributed on the best possible basis of effort, and nodes can leave and re-joins the network at will, embracing the longest proof-of - work chain as evidence of what happened when they left. Bitcoin incorporates and uses the Blockchain principle to allow transactions to be validated by the majority of computing power in a network, ensuring that each transaction is checked and validated by the majority of nodes that actively compute network transactions. Then, the verified transactions are stacked in an unchangeable sequence. All computers which used computational resources to verify a block of data receive some cryptocurrency as a reward. In this way, a large number of computers verify all transactions, and it is virtually impossible to manipulate the verification of a transaction, because it would require an unreasonable amount of computing power in order to achieve the majority of the verification phase of the network.

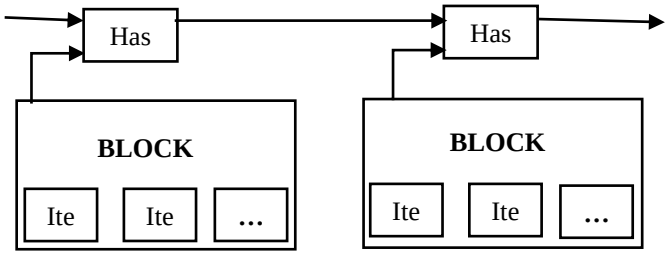

Fig 1: Basic Blockchain Knowledge

II. ANALYSIS

The goal of this project is to solve the problems of the current system of certificate verification and to stop user fraud and offer transparency in the education system by using blockchain technology. This project is designed to evaluate the application of blockchain to implement distributed system as a service.

The digital certificate, which adopts digital signature technology, provides the administrator with the authority to confirm the administrator in the digital fields used to validate the identity of a user and the authorisation to access the network resources

(A) Objectives:

1. Digital certificate that adopts digital signature technology provides the authority to validate the user himself in the digital fields used to validate the identity of a user and the authorisation to access the network resources.
2. This provides employers with clarity to check workers' educational credentials during the recruiting process and saves time for the review of educational documents

(B) Scope:

1. Blockchain technology is a growing field of interest for many European and other industries and universities. As a fairly recent breakthrough in the field of computer science, blockchain is a modern, cross-industry and disruptive technology that is expected to drive global economic growth over the next few decades
2. According to numerous researches around one million students passing out each year, the issuing authorities of the certificate tend to be compromised for the student data protection credentials. Events which cause the graduation certificate to be forged are often seen due to the lack of an effective anti-forge mechanism. These systems are implemented to solve this problem while security problems still exist. Blockchain is one of the latest Data Security technology that can be adopted. The unalterable property of the block chain helps to solve the problem of forgery of certificates.

III. LITERATURE SURVEY

1. **Eductx: A Blockchain-Based Higher Education Credit Platform By (Muhamed Turkanović , Marko Hölbl , Kristjan Košič, Marjan Heričko, Aida Kamišalić.)** :

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 07, July-2020

Blockchain technology enables the creation of a decentralized environment, where transactions and data are not under the control of any third party organization. Any transaction ever completed is recorded in a public ledger in a verifiable and permanent way. Based on the blockchain technology, we propose a global higher education credit platform, named eductx. This platform is based on the concept of the European Credit Transfer and Accumulation System (ECTS). It constitutes a globally trusted, decentralized higher education credit, and grading system that can offer a globally unified viewpoint for students and higher education institutions (heis), as well as for other potential stakeholders, such as companies, institutions, and organizations. As a proof of concept, we present a prototype implementation of the environment, based on the open-source Ark Blockchain Platform. Based on a globally distributed peer-to-peer network, eductx will process, manage, and control ECTX tokens, which represent credits that students gain for completed courses, such as ECTS. Heis are the peers of the blockchain network. The platform is a first step toward a more transparent and technologically advanced form of higher education systems. The eductx platform represents the basis of the eductx initiative, which anticipates that various heis would join forces in order to create a globally efficient, simplified, and ubiquitous environment in order to avoid language and administrative barriers. Therefore, we invite and encourage heis to join the eductx initiative and the eductx blockchain network. INDEX TERMS Blockchain, higher education, ECTS, tokens.

2. **Blockchain, academic verification use case by (Federico Bond, Franco Amati, Gonzalo Blousson):**
To verify the authenticity of academic certificates we propose employing a digital signature scheme and timestamps using blockchain technology, because of its greater transparency, less maintenance and lower cost than traditional alternatives. Based on conversations held on July 31, 2015 on the stage of the first Bitcoin forum organized by the government of Ciudad de Buenos Aires.

3. **Using blockchain as a tool for tracking and verification of official degrees by (Miquel Oliver, Joan Moreno, Gerson Prieto, David Benítez):** While the number of universities, tertiary education students and number of graduates per year constantly increase, the need to easily verify degree certificates generates new business opportunities. The irruption of blockchain, and its implementation based in the blockcerts software, provides a straightforward solution that demands to explore plausible business models. In this paper we project two financial models balancing where the price for the service is balanced between the graduate and the employer as the main stakeholders of that service. Students demand a proof-of-certification at low cost and easy to check, employers also demand quick and trustable verification of degrees when recruiting. Both models are projected for several geographic markets and shares to explore plausible ways to develop that business in the European Union

IV. DESIGN

The design contains 3 Main components/ Model. They are to authentic details, Apply for new one, Check for authenticity. Here is the entire flow of the project in the form of flowchart.

Below are the mentioned tasks which is available in the system:
The system is such design as soon you open there is a login/Registration option. Student / Employer can use this software/portal to authenticate their certificates, apply for new certificates and for uploading new issued certificates if the university or the institution is new and not listed. As you upload the certificates it creates a database for the respective new institution.
The Employer can use it for checking the authenticity of the certificate as a part of recruiting process and file action against the fake one.

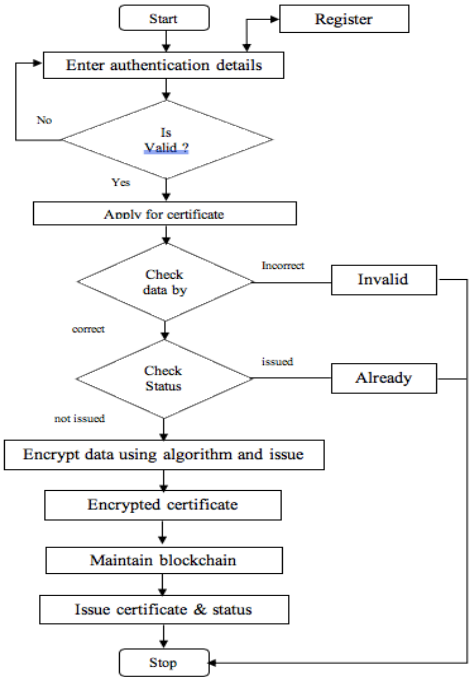

Figure 2: System architecture

V. FUTURE MODIFICATIONS

In the future, we plan to test the prototype in a real-life environment, which would include HEIs, students and companies. In this way the presented concept could be further validated. Additionally, we plan to adapt this system blockchain so that each course would be assigned with a unique blockchain address and a pool of tokens. After completing the course obligations, students would get tokens from the course address and not directly from the institution. The course address would be a multi signature address between an institution and a professor

VI. CONCLUSIONS

The proposed platform takes the advantage of the blockchain in order to create a globally trusted higher education credit and grading system. As a proof of concept, we presented a prototype implementation of the system platform which is

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 07, July-2020

based on the open-source Ark blockchain platform. The proposed system platform addresses a globally unified viewpoint for students and organizations. Students benefit from a single and transparent view of their completed courses, while have access to up to date data regardless of a student's educational origins. Other beneficiaries of the proposed system are potential employers, who can directly validate the information provided by students. The proposed solution is based on the distributed P2P network system. It transfers the higher education grading system from the current real-world physical records or traditional digital ones (e.g. databases) to an efficient, simplified, ubiquitous version, based on blockchain technology. It is anticipated that such a system could potentially evolve into a unified, simplified and globally ubiquitous higher education credit and grading system.

REFERENCES

[1] C. K. Wong and S, S. Lam "Digital signatures for flows and multicasts", WEEE/ACM Transactions on Networking, 7(4): 502- 513, 1999.
[2] A. M. Antonopoulos, Mastering Bitcoin: Unlocking Digital. Sebastopol, CA, USA: O'Reilly Media, 2015.
[3] Benyuan He, "An Empirical Study of Online Shopping Using Blockchain Technology", Department of Distribution Management, Takming University of Science and Technology, Taiwan, R.O.C., 2017.
[4] Chris Dannen, Introducing Ethereum and Solidity, https://www.apress.com/br/book/9781484225349
[5] J. Clark and P. C. van Oorschot, "SoK: SSL and HTTPS: Revisiting past challenges and evaluating certificate trust model enhancements," in proc. IEEE S&P'13, May 2013, pp. 511–525.
[6] L. Zhang, D. Choffnes, D. Levin,et al., "Analysis of SSL certificate reissues and revocations in the wake of Heartbleed," in proc. ACMIMC'14, Nov 2014, pp. 489– 502.
[7] M. Carvalho and R. Ford, "Moving-target defenses for computer networks,"IEEE Security & Privacy, vol. 12, no. 2, pp. 73–76, Mar.-Apr.2014.
[8] Papazoglou, M., Service-Orientated Computing: Concepts, Characteristics and Directions, in International Conference on Web Information Systems Engineering. 2003, IEEE: Rome.
[9] D. Ferraiolo, R. Kuhn, and R. Sandhu, "Rbac standard rationale: Comments on "a critique of the ansi standard on role-based access control", "IEEE Security Privacy, vol. 5, no. 6, pp. 51–53, Nov 2007.
[10] A. Ouaddah, A. A. Elkalam, and A. A. Ouahman, "Towards a novel privacy-preserving access control model based on blockchain technology in iot," in Europe and MENA Cooperation Advances in Information and Communication Technologies. Springer, 2017, pp. 523– 533.
[11] L. Y. Chen and H. P. Reiser, "Distributed applications and interoperable systems, 17th ifip wg 6.1 international conference, dais 2017, held as part of the 12th international federated conference on distributed computing techniques, discotec 2017, neuchtel, switzerland, june 1922, 2017." Springer, 2017.
[12] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "Medshare: Trust-less medical data sharing among cloud service providers via blockchain," IEEE Access, vol. 5, pp. 14 757–14 767, 2017.
[13] M. Warasart and P. Kuacharoen, "Paper-based Document Authentication using Digital Signature and QR Code," no. Iccet, 2012.
[14] J. van Beusekom, F. Shafait, and T. M. Breuel,"Text-line examination for document forgery detection," Int. J. Doc. Anal. Recognit., vol. 16, no. 2, pp. 189–207, 2013.
[15] Mahamat, M. B. (2016), A Web Service Based Database Access for Nigerian Universities' Certificate Verification System.
[16] Osman Ghazali, Omar S. Saleh, "Cloud Based Graduation Certificate Verification Model".
[17] Lisha Chen-Wilson, Dr David Argles,"Towards a framework of A Secure E-Qualification Certificate System.
[18] Jiin-Chiou Cheng, Narn-Yih Lee, Chien Chi, and Yi-Hua Chen," Blockchain and Smart Contract for Digital Certificate".