Blockchain-Based Academic Record System

Lucas M. Palma[1], **Martín A. G. Vigil**[1], **Jean E. Martina**[1]

[1]Universidade Federal de Santa Catarina

lucas.palma@posgrad.ufsc.br, {martin.vigil, jean.martina}@ufsc.br

Abstract. *Blockchain offers some valuable properties, such as decentralization, transparency, pseudo anonymization, and data integrity. Combined with Smart Contracts, they enable decentralized applications and agreements without the need for a trusted third party. They can also work as tools to improve governance processes. Noteworthy are works that use blockchain in the automation and enhancement of degree certificates issuance. These works range from a simple proof of existence of degree certificates to more sophisticated proposals, which include the record of credits taken in a higher education system. Here, we propose an automated, transparent, auditable, and secure model to record credits and issue degree certificates using blockchain. We aim to minimize the bureaucracy of the processes involved, facilitate auditing, and reduce the falsification of degree certificates. The proposed model considers the existence of a public higher education regulatory agency and independent educational institutions. Unlike related works, this proposal encompasses undergraduate students' entire trajectory, from registration to the issuance of his or her degree certificate. Hence, we present a prototype and a cost analysis considering official data from the Brazilian higher education system and the Ethereum blockchain platform.*

Resumo. *Blockchains oferecem propriedades como descentralização, transparência, pseudo-anonimização e integridade de dados. Combinadas com contratos inteligentes, elas permitem o desenvolvimento de aplicativos e acordos descentralizados sem a necessidade de terceiros confiáveis. Elas também podem funcionar como ferramentas para a melhoria de processos de governança. Destacam-se os trabalhos que utilizam blockchain na automação e aprimoramento da emissão de certificados de graduação. Esses trabalhos variam de uma simples prova de existência de certificados de graduação até propostas mais sofisticadas, que incluem o registro de créditos obtidos em um sistema de ensino superior. Neste trabalho, propõe-se um modelo automatizado, transparente, auditável e seguro para registrar créditos e emitir certificados de graduação utilizando blockchain. Os principais objetivos são minimizar a burocracia dos processos envolvidos, facilitar a auditoria e reduzir a falsificação de certificados de graduação. O modelo proposto considera a existência de uma agência reguladora pública de ensino superior e instituições educacionais independentes. Diferentemente de trabalhos relacionados, esta proposta abrange toda a trajetória dos estudantes de graduação, desde o registro até a emissão do seu certificado de graduação. Apresenta-se um protótipo e uma análise de custos considerando dados oficiais do sistema de ensino superior brasileiro e a plataforma de blockchain do Ethereum.*

1. Introduction

In 2008, anonymous researchers proposed a decentralized peer-to-peer network, where participants can engage in monetary transactions (i.e., Bitcoin [Nakamoto 2008] transactions) without the intervention of a trusted third party (TTP). Two devices guarantee the correctness and integrity of transactions. The first one is the blockchain, a chained list of blocks, where blocks are composed of a pointer to the previous one and a collection of transactions. Every participant of the network maintains a local copy of the entire blockchain. When creating a new block, it is necessary a consensus so that the copies of the chain remain cohesive. That is done by the execution of a cryptographic puzzle called Proof of Work (PoW). The second device is the monetary incentive. Every time a participant successfully proposes a block, it receives a reward as encouragement for adequately executing the protocol. Following the success of Bitcoin, new blockchain platforms arrived. For instance, we cite Ethereum [Wood et al. 2014]. This platform combines the decentralized nature of blockchain with smart contracts (pieces of software executed in the blockchain). In this way, one can run decentralized applications with properties such as transparency, integrity, and pseudo-anonymity.

In this context, we believe that blockchains can build infrastructures to help with Higher Education challenges such as the fraud of degree certificates. Higher education has expanded significantly around the world in the past century [Schofer and Meyer 2005]. Now, not only the wealthy but also the lower classes have had better chances to pursue a degree in Higher Education Intuitions (HEIs). In Brazil, one of the reasons for people to seek higher education is that it usually allows one to get jobs that pay higher salaries, and therefore, enjoy a higher standard of living. Specifically, research has shown that Brazilians who owned a higher education degree earned around 269% more than those that do not [Instituto Brasileiro de Geografia e Estatística 2011]. It is, therefore, no surprise that some Brazilians may be tempted to acquire forged degree certificates to be eligible for well-paid jobs.

Another important problem that is relevant to our proposed solution is the curation and management of academic records. Despite the usual problems on curating academic records for long periods, such as, natural events like flooding or fire which could render the records unavailable, we have the risk of academic institutions disappearing together with their records.

Regardless of economic and social reasons why such problems happen in Brazil, the way degree certificates are issued has no transparency and redundancy and can be exploited by fraudsters. The issuance of degree certificates should follow Ordinance 33/1978 from the Ministry of Education [Ministério da Educação do Brasil 1978]. It turns out to be a bureaucratic, paper-based, and error-prone process. More precisely, the procedure consists of several steps that involve HEI staff. The use of paper documents from the moment a student completes all requirements for a degree to the moment his or her certificate is issued is another problem. Finally, the university president signs a stack of certificates every term. In this stack, he or she may sign without intention a certificate forged by a dishonest employee. This calls for a more efficient and secure solution.

Our contribution [Palma et al. 2019] is to execute the issuance of degree certificates in a blockchain-based system. Every time a student completes the required number of credits (courses completed with success), smart contracts log this achievement as a

record in the blockchain. The goal is to tackle bureaucracy, human interference, and fraud. To the best of our knowledge, we are the first to automate degree certificates issuance with the help of smart contracts and to take into account the complete undergraduate student journey, since his or her registration in the HEI until the issuance of his or her degree certificate. As a proof of concept, we develop a prototype to be run on Ethereum blockchain. Smart contracts are written using Solidity language and executed in one of the Ethereum networks for testing.

2. Proposal

In this section, we propose an automated, transparent, and secure blockchain-based academic record system. There are four types of participants in our proposal. The first type is the Regulatory Agency (RA), which is responsible for regulating the national higher education system. More specifically, RA authorizes institutions to issue nation-wide valid degree certificates, evaluates and approves the courses' curriculum, and oversees the degree certificate issuance. RA is a node in the blockchain network responsible for deploying the smart contracts that work as an interface between the participants and the blockchain. In the Brazilian scenario, the Ministry of Education (MEC) could represent this participant. It is important to highlight that RA does not act as a reliable third party in every step of the proposal. It simply ensures that only recognized institutions can participate. Therefore, we suggest the adoption of a Public-Key Infrastructure (PKI) to authenticate participants' identities. Since we are using the Brazilian higher education as our application scenario, we recommend the official Brazilian PKI, ICP-Brasil. In this way, RA can take advantage of national and well-established identity infrastructure.

The second type is the Higher Education Institution (HEI). HEIs offer undergraduate courses, register students, and issue degree certificates. By this means, Students (the third type of participant) attend classes and score credits to complete courses. Upon a Student complete a course, HEIs record his or her progress in the blockchain.

The fourth and last participant is called Verifier, which may be any individual reading information in the blockchain. For instance, a job recruiter interested in verifying the validity of a particular degree certificate.

To begin with, RA needs to deploy an identity management smart contract called *Authority*. This contract receives as entries, digital certificate information, and HEIs' Ethereum account addresses. In this way, it is possible to associate an address to a specific digital certificate. Also, *Authority* provides functions to manage these certificates, such as revoking them. It works like a simplified reproduction of a PKI in the blockchain. Only RA should be able to execute such functions since it is responsible for regulating which HEIs may integrate the system. This smart contract is required as we rely on the Ethereum Blockchain Platform, which is a public permissionless blockchain. In contrast, we could choose to deploy our proposal in a permissioned platform, for example, the Hyperledger, where the blockchain protocol manages the certification and authorization.

In a third step, RA creates multiple instances of the smart contract *Curriculum*. Each of them represents an undergraduate course curriculum, and it is associated with a specific HEI. This step is equivalent to real-world curriculum approval. Furthermore, this smart contract is the HEI's interface with the blockchain. Therefore it has functions to register students and courses, as well as functions to update students' progress. Similarly

to *Authority*, after the deploy, only the specified HEI can operate it. Nonetheless, for every execution of *Curriculum*, it is necessary a credential check through *Authority*. If, for example, HEI's certificate representation in the blockchain was revoked by RA, no state changes will be permitted in that particular *Curriculum* instance. Otherwise, the HEI may subsequently record the courses students must attend to receive his or her degree certificate.

Next, for each degree an HEI offers, it provides the identification of the enrolled students to the corresponding instance of *Curriculum*. Over time, HEIs use functions provided by the *Curriculum* to update students' status. When *Curriculum* identifies that a student completed a degree, it creates a new instance of a smart contract *Diploma*, which registers an event saying that the student finished his or her degree and is granted a degree certificate in the blockchain.

Our proposal combines the following important properties: 1) *data integrity*: It prevents students' credit records from being tampered or lost as they are registered as transactions in the blockchain; 2) *authentication and non-repudiation*: Only institutions certified by ICP-Brasil are allowed to issue degree certificates; 3) *transparency*: Institutions and citizens are allowed to audit and question the processes as well as verify the validity of degree certificates, and; 4) *automation*: The procedures are heavily automated by smart contracts, reducing the human interactions and paper-based processes.

Alternatively, we could deploy our proposal using different blockchain architectures. For instance, instead of a public blockchain, we could use a private one. In this way, the smart contract *Authority* would not be necessary since the participants are known, and the blockchain consensus protocol could conduct authentications and authorizations. Moreover, in this case, we do not need cryptocurrencies, which makes it possible to use a lightweight consensus protocol in the place of Proof of Work (e.g., a consensus algorithm that does not consider computational power but reputation). These modifications significantly impact the execution costs, as the network would not charge blockchain transactions. Moreover, private blockchains can reduce possible privacy issues. Although in our solution, the students are pseudo-anonymized, that is, they are identified only by the addresses of their wallets. With the help of other databases, it is possible to re-identify individuals through their behavior, in this case, the courses taken by an address in a specific sequence. This problem would be mitigated, as only a known set of participants would have access to the data. However, in this private version, the anchor of confidence would be displaced closer to the regulatory agency and HEIs. In other words, the system would not be necessarily open to the scrutiny of citizens, creating a possible absence of transparency.

Another approach is to use hybrid architecture, with two blockchains, public and private, similar to the related work [Kuvshinov et al. 2017]. On such a solution, we could still have the automation of smart contracts and the audit of data between HEIs in a private chain. In the public blockchain, we could register the metadata of processes, in a way the citizens could only verify the authenticity of a *Diploma*. Still, they would not have access to identifiers and credits. The problem of this alternative is how to establish the link between the two blockchains. One could create the role of a special participant that supervises the correctness of data published in a public chain, but this would affect the decentralization of the system.

Lastly, we have public permissioned blockchains, which is the natural extension for this work. In this environment, we can establish a set of participants with writing permissions and others that can only read data. Platforms such as Hyperledger reduce the execution costs by not using cryptocurrencies. However, it would still be a trade between process transparency and data privacy.

In the present proposed model, we disclose no students' grades in the blockchain, which have already been deemed private data by the Office of the Comptroller General based on Art. 31 of Federal Law 12.527 [Governo Federal 2011]. Rather, our solution publishes the courses students have completed and the degrees students have pursued and been occasionally granted in the blockchain. The question of whether privacy is violated should be carefully analyzed anyway. According to the above federal law, entities supported by taxpayers' money and non-profit-making entities should guarantee public access to their data other than individuals' private data. As such, our solution does not violate privacy concerning students who attend public HEIs in Brazil. Universities such as the Federal University of Santa Catarina publicly list the individuals it has granted academic degree [Universidade Federal de Santa Catarina 2018]. Additionally, this university also identifies which degrees students have been granted and dates the students started and finished their degrees.

As to security, one must analyze how malicious students, HEIs, and RA could harm the system. No students can access a smart contract since only HEIs can do so. Therefore, a malicious student cannot interfere with the system. One HEI cannot access a smart contract owned by another HEI. However, the staff of an HEI can provide bogus data as input to the system by accessing its smart contracts. For example, an administrative employee can add fake students to a smart contract. Also, a tutor or professor can allegedly endorse that a student completed a course. Such misuses can be identified by auditing the transactions an HEI malicious employee has addressed to the smart contracts.

Moreover, the blockchain holds HEIs accountable for their transactions, thereby discouraging abuses. Moreover, by disabling smart contracts, an HEI removes a wrongly issued degree.

In contrast to HEIs, RA is trusted to not abuse the system. Note that the trust in RA is established by law. However, RA's credentials in the blockchain might be compromised. In this case, RA would need to identify when its credentials were compromised and denounce all smart contracts created since then.

3. Cost Evaluation

Here, we estimate the costs charged by the Ethereum network to run our prototype. The source code is available at `https://pastebin.com/DSVccxJr`. We approximate the gas costs (the Ethereum's unit that measures the cost of executing smart contracts instructions) required to deploy and execute our proposal. At the end of this section, we present the total network costs for issuing a degree certificate.

Table 1 summarizes the gas cost for every transaction executed in our experiments. Constructors are the most expensive functions. The reason is that the input for these constructors is larger than the input for the other functions. Moreover, our constructors initiate internal variables in non-volatile memory, which re-

lies on expensive Ethereum Virtual Machine instructions. Nonetheless, constructors are executed only once when a smart contract is deployed. Therefore, their fees are to be paid only on this occasion. Our estimation requires approximations, which are presented in Table 2. According to the survey on Brazilian higher education [Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira 2019], there are 299 active public HEIs. These institutions offer, on average, 35 degrees. In 2018, 2,077,481 new students enrolled in these HEIs.

Furthermore, we approximate how many courses students need to complete and how long they take. Note that this highly depends on the degree students pursue. According to the Ministry of Education [Conselho Nacional de Educacão 2007], Brazilian undergraduate students need to attend, on average, 3,000 hours on courses. Moreover, a student should attend these hours in four years or more. To come close to a reasonable number of courses students should attend while they pursue their degree, we analyzed the number of hours of each course taught at the Federal University of Santa Catarina. Since there are discrepant values (e.g., 0 and 720 hours), we calculated and chose the median of 72 hours. Therefore, taking into account a degree requires at least 3,000 hours, and each course is 72 hours long, we computed the number of courses to be attended. We rounded this number to 40 so that they can be distributed evenly along the four years students go to HEIs.

Authority		*Curriculum*		*Diploma*	
Function	gas	**Function**	gas	**Function**	gas
constructor	596,402	*constructor*	1,374,998	*constructor*	448,196
addCert	154,558	*registerDiscipline*	121,236		
check	27,598	*registerStudent*	131,460		
		updateDiscipline	132,586		
		issueDiploma	580,782		

Table 1. Prototype's gas cost.

Description	**Approximate Value**
Active Brazilian public HEIs	299
Average degrees offered by a HEI	35
Average courses required for a degree	40
Students entering HEIs per year	2,077,481
Average courses to be attended per year	10
Average degree duration in years	4

Table 2. Brazilian higher education parameters.

We now turn to estimate how much gas is needed to use our prototype for the

public higher education system in Brazil. We assume a gradual adoption starting with only newly enrolled students. In the first year, smart contracts are instantiated by evaluating their constructor, and initial data is added to them by executing the appropriate functions as follows. An instance of the smart contract Authority is deployed. One instance of Curriculum is created for each of the 35 degrees each of the 299 HEIs offers. Next, the certificate of each HEI is added to *Authority* by evaluating function *addCertificate*. Also, every student enrolling with an HEI attends ten courses a year. At the end of the first year, function *updateDiscipline* is executed for each course a student attended in order to register his or her achievements.

In the second and third years, new students enroll with HEIs. Similar to the first year, newcomers are registered in instances of *Curriculum*. All current students are enrolled in ten courses a year, and the achievements of all registered students are stored. In the fourth and following years, not only new students enroll with HEIs but also some students graduate and leave HEIs. Therefore, in addition to registering students and their achievements, at the end of the year, an instance of *Diploma* is created for one-fourth of the registered students by evaluating function *issueDiploma*. Executing functions that handle students' data (viz., *registerStudent*, *updateDiscipline*, and *issueDiploma*) dominates the total costs. The reason is that, although the input of such functions is minimal, and they do not require the most gas, they are evaluated numerous times during the time a student is enrolled in a *Curriculum*.

To estimate the cost of a single *Diploma*, we sum all the gas needed to register a student and his or her achievements while he or she attends 40 courses. Additionally, we add to these costs the gas used to create an instance of *Diploma*. We rule out the costs of initially deploying smart contracts *Authority* and *Curriculum*, which tend to zero as these costs are shared by all students entering and leaving HEIs in the long run. Thus, the cost per student is 5,883,096 gas. In the moment of writing this document, these amounts of gas is equivalent to US$1.39. However, this price may change depending on the Ethereum network.

4. Conclusion

Higher education can pave the way for better jobs and higher standards of living. This is why many in Brazil pursue an undergraduate degree certificate. Higher education institutions implement bureaucratic, error-prone, paper-based procedures to issue degree certificates. Fraudsters have explored these procedures to forge degree certificates and its related data were also already lost forever due to unforeseen circumstances. We propose a state-of-the-art solution to mitigate such issues. The proposal consists of not only registering the academic history of undergraduate students in the blockchain but also deploying autonomous applications, namely smart contracts, to issue degree certificates with minimal interference of higher education institutions. As a proof of concept, we describe a prototype consisting of a set of smart contracts written in Solidity language. The prototype is to be run in Ethereum public blockchain.

Regarding future work, we believe that there are at least two significant contributions that can improve the proposal presented in this work. The first is related to privacy, we believe that a relevant contribution would be the proposal of a mechanism that reduces the possibility of re-identifying students while maintaining the automation offered

by smart contracts. Secondly, future work should consider the problem of blockchain growth over the years.

References

Conselho Nacional de Educacão (2007). ResoluÇÃo n 2, de 18 de junho de 2007. Technical report, Ministério da Educação do Brasil. http://portal.mec.gov.br/cne/arquivos/pdf/2007/rces002_07.pdf. Accessed September 25, 2018.

Governo Federal (2011). Lei n 12.527, de 18 de novembro de 2011. *Lei de Acesso a Informação*. http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Accessed August 04, 2018.

Instituto Brasileiro de Geografia e Estatística (2011). De cada 10 novos assalariados, seis são de empresas de alto crescimento. https://agenciadenoticias.ibge.gov.br/2013-agencia-de-noticias/releases/14460-asi-de-cada-10-novos-\\assalariados-seis-sao-de-empresas-de-alto-crescimento.html. Accessed June 8, 2018.

Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (2019). Sinopse estatística da educação superior 2018. https://portal.inep.gov.br/basica-censo-escolar-sinopse-sinopse. Accessed Jan 20, 2019.

Kuvshinov, K., Mostovoy, J., and Nikiforov, I. (2017). Disciplina: a blockchain for education. https://disciplina.io/yellowpaper.pdf. Accessed March 03, 2018.

Ministério da Educação do Brasil (1978). Portaria mec/dau n 33 de 2 de agosto de 1978. *Estabelece a sistemática para o registro de diplomas de curso superior.*

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Technical report, Manubot.

Palma, L. M., Vigil, M. A. G., Pereira, F. L., and Martina, J. E. (2019). Blockchain and smart contracts for higher education registry in brazil. *International Journal of Network Management*, 29(3):e2061.

Schofer, E. and Meyer, J. W. (2005). The worldwide expansion of higher education in the twentieth century. *American Sociological Review*, 70(6):898–920.

Universidade Federal de Santa Catarina (2018). Egressos da UFSC. https://egressos.sistemas.ufsc.br/listaEgressos.xhtml. Accessed August 04, 2018.

Wood, G. et al. (2014). Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, 151(2014):1–32.