THE JBBA

PEER REVIEWED RESEARCH

OPEN ACCESS
ISSN Online: 2516-3957
ISSN Print: 2516-3949
https://doi.org/10.31585/jbba-3-2-(7)2020

Academic Certification using Blockchain: Permissioned versus Permissionless Solutions

Carlos Castro-Iragorri[1] and Olga Giraldo[2]
[1]Universidad del Rosario, Colombia
[2]Vrije Universiteit Amsterdam, The Netherlands

Correspondence: carlos.castro@urosario.edu.co
Received: 03 June 2020 **Accepted**: 15 June 2020 **Published**: 02 July 2020

Abstract
Understanding the challenges of implementing blockchain solutions is an important step towards scaling and adopting the technology. This paper analyses the adoption of blockchain technology in the management of academic certificates. In this use case, we identify certification providers that have adopted a permissionless approach and consortiums of academic institutions that are in the process of building permissioned networks. We explore the challenges faced by both approaches, and obtain information from competing projects to provide a preliminary approach for cost-benefit analysis that could potentially be applied for similar blockchain projects. For the management of academic certificates, we find that beyond the cost of implementing the technology there are additional elements of critical importance for adoption. For example, if blockchain-enabled certificates will replace notarised documents, how does the technology complement other forms of digital credentials, the ease of integration to existing administrative records within institutions and whether they are a viable first step towards a comprehensive, efficient and reliable system to share information among institutions.

Keywords: *permissioned, permissionless, digital credentials, cost-benefit analysis*

JEL Classifications: *M210, O300.*

1. Introduction

Although distributed ledger technology (DLT), in particular blockchain, has captured an important amount of attention in the last decade, it is challenging to identify the added value of the technology to some of the solutions proposed. Expectations and investment are still high in firms and governments [1]. However, there is not enough information regarding investments and outcomes on existing projects. Also, IT projects are risky endeavours with overrun cost [2].

Within the context of DLT, decentralisation provides high censorship and tamper resistance, but these features come at higher costs in terms of the use of resources, processing time and coordination efforts compared to a fully centralised system [3]. Some analyst indicates, that the high cost of managing the information contained in a public permissionless blockchain, such as Bitcoin or Ethereum, compared to hosting the same information on a centralised database, is only economically rational if users have strong preferences towards censorship resistances, and are willing to pay the premium [4].

More recently, permissioned blockchains have attracted the attention of traditional firms looking to incorporate the benefits of DLT and customise these solutions to the need of their industries [1]. As there is a more general understanding of the benefits of the technology in each industry, firms are interested in solving the permissioned versus permissionless dilemma. One simple way to understand the dilemma is to think of permissionless blockchain as an existing infrastructure of highways that a firm uses to provide goods and services. Therefore, a firm that wants to jump into this ecosystem must invest in connecting to the highway and pay the toll required to use and maintain the existing infrastructure. It must also, abide by the rules (speed limits) and possible externalities (congestion) of using the infrastructure. On the other hand, for a permissioned solution, there is no existing infrastructure; therefore, the interested firms must incur the fixed cost of building the roads that will allow them to provide their goods and services. To reduce the individual contributions and diversify the risk, firms form a consortium and create a governance structure in charge of initially building the infrastructure, and later on, managing and settling disputes. This consortium agglomerates firms with similar interest, therefore, it is possible to have a more efficient and customised infrastructure that will meet the needs of the firms to deploy their solutions.

There are important efforts in terms of interoperability and integration between permissioned and permissionless blockchain [5]. Therefore, shortly, as was the case of the internet, the public highways and the private roads will be connected and firms will be able to deploy business

applications that can operate across various types of distributed ledgers.

The objective of this article is to analyse the use case for the management of academic certificates using blockchain technology. We address the added value of using blockchain technology and ascertain the similarities and challenges between providing such services using a permissioned and a permissionless approach. In addition, we provide an example of cost-benefit analysis.

The document is organised as follows: section 2 introduces the use case in the context of the education sector; section 3 explains the role of blockchain technologies in the certificate management operating processes; section 4 provides a cost-benefit analysis applied to the case and section 5 concludes.

2. Managing Academic Certificates

Certificates are a social convention that provides a medium to convey new information regarding an individual or an organisation. In education, the most common form of certificates is that which provides new information regarding accomplishments and skills. The information regarding skills is relevant for employers and to continue the acquisition of knowledge.

According to research by the European Union [6] academic certificates are one of the areas in education where we could see the implementation of blockchain technologies in the short term. Further down the road this would also include transfer credit systems and lifelong learning records [7].

As considered in [6] the ontology of a certificate can be broken down into its components and its related processes. The components are as follows: a claim, the evidence, a signature, a document, an issuer and a recipient. The processes are as follows: design, issuing, verification and sharing or socialising.

So far the traditional method to provide a certificate has been paper. Paper certificates have the following characteristics: they include physical security measures (watermarks, seals) to avoid forgery; the issuer and recipient guard independent copies; they cannot be revoked and they require a manual verification. More recently, institutions have introduced different standards for digital certificates with some form of delegated signature verification. The claim and evidence information are kept in centralised databases hosted by the institution. Since the certificates are controlled by the issuer institution they can be revoked.

What is the added value of blockchain technology? According to [6], the traceability of the issuing process and the multiple copies provide stronger security features. The verification process is independent from the issuer; therefore, the service can be performed by any institution with access to a persistent registry, allowing for vendor independence. Both the issuer and the recipient obtain different levels of control over the certificate. The issuer may revoke the claim without incurring in additional cost, for example, obsolete skills or technologies. The recipient will control, collect and socialise its verifiable skills in a more efficient manner. Avoiding the need to solicit his learning record and possibly pay additional fees to update his resume.

The benefits for the recipient are complemented by self-sovereign identity. With self-sovereign identity individuals own and control their digital identity without the intervention of third parties In this context, an academic certificate or any other type of certificate is considered as a claim, associated and owned by an individual or organisation, that represents sets of information that are relevant to establish business or personal relationships.

Today, educational attainment is largely a decentralised activity because; students and professionals obtain a wide range of skills in different periods of their working life and at different types of institutions (universities, employers, online learning platforms, among others). However, the current challenge is that each institution is an independent silo of the academic accomplishments of a student. Hence the transit of one institution to another, or between employers requires a student to provide verifiable copies of their academic achievements and new skills. These pain points and inefficiencies justify improving the existing process.

To avoid the current equilibrium of independent silos, blockchain technology provides the decentralised infrastructure to safely share abstractions of the information related to the educational accomplishments of a student. Most of the current implementations, register onto a blockchain hash obtained from the information contained in the certificate; this is what we denote as an abstraction. Blockcerts extends existing digital standards in education, in particular Open Badges, to incorporate a blockchain-based verification process[1].

Currently, projects that have implemented a solution or advanced proof of concepts for academic certificate management can be categorised into certification vendors and university consortiums. Certification vendors are firms or start-ups that have seen the potential of blockchain technology for data management, self-sovereign identity or know your customer (KYC), creating a business model around it. Other firms have included blockchain technology as part of their existing portfolio of services. In the former, the firms act as a notary (a third party between the issuer and the recipient or a recipient and employer). Some of these vendors are Accredible[2], Xertify[3] and Gradbase[4].

Universities have not lagged; the Blockcerts standard was initially developed by the MIT Media Lab and Learning

[1] https://www.blockcerts.org/.
[2] https://www.accredible.com/.
[3] https://xertify.co/.
[4] https://gradba.se/en/.

Machine[5]. As of 2018, the Digital Credential Consortium is a university lead effort to design and build an infrastructure for digital credentials of academic achievement. The consortium founders are universities in Europe, North America and Latin America. Similar consortiums have been created in Singapore[6] and Spain,[7] with an increasing number of universities joining the effort. In addition, individual universities like the Open University UK and the University of Nicosia [6] were early adopters of the technology, using permissioned blockchains and the Blockcerts standard or similar types of digital badges standards.

Universities, as the main issuer of these types of certificates, have computer science departments, in-house IT personnel and the possibility to establish partnerships or fund start-ups to develop the technology. Besides, they might be reluctant to share academic information with external vendors unless they are unable to provide the service or incorporate blockchain technologies. For this reason, the most important clients of certification vendors are online education, professional associations and companies. This attitude will be a challenge going forward: to overcome the shortcomings of the current system of academic credentials, it would be desirable to allow the integration of solutions and achieve lifelong learning records. Otherwise, we might end up with the latest technology, but we will not be able to overcome the current independent silos equilibrium.

3. Blockchain Infrastructure for Managing Academic Certificates

A system for managing academic certificates can be broken down to the processes mentioned previously: design, issuing, verification and sharing or socialising. We need to understand how these operating processes are related to the services that will be impacted by the introduction of blockchain technology.

Figure 1, represents the operating processes in stages, and identifies the processes transformed by blockchain technologies.

The academic certificates (claim and evidence) are part of the administrative records stored in databases on-premise or in the cloud by issuer institutions. With or without blockchain this information is held within the institution. Data protection requirements such as General Data Protection Regulation (GDPR) require education providers to be accountable for the information of students.

The first stage of figure 1, represents the design and storage of the information contained in the certificate. In the traditional approach, the university or education provider will also be in charge of providing a system to share and verify the information contained on the paper or digital certificate. In other words, the process is entirely integrated and managed by the issuer institution.

The second and third stages of figure 1 represent the process affected by blockchain technologies, in particular, how information is shared and verified.

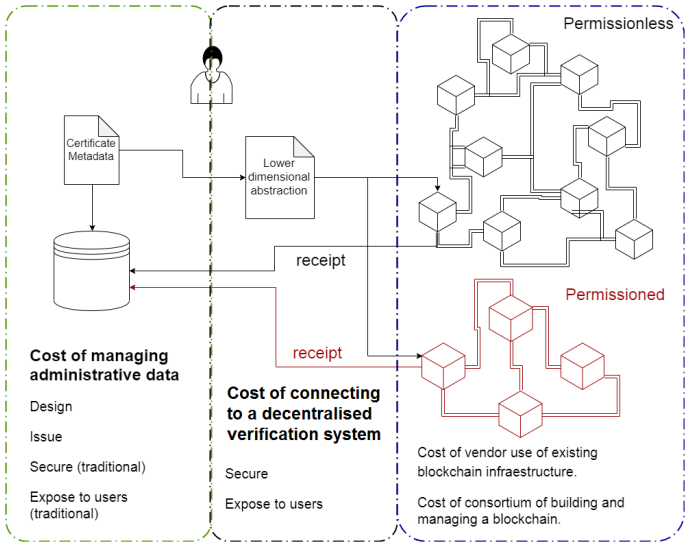

Figure 1: Management of academic certificates using Blockchain technologies.

The system storing the information on the accomplishments of the students needs to be able to interact with a blockchain for issuance and verification. As we mentioned before, the added value of blockchain technologies for this use case is primarily concerned with the introduction of a decentralised verification system for the academic certificates. This system must also provide enough trust to avoid any further use of notary service.

When a student satisfies the requirements regarding a skill or a degree, a certificate is issued and the abstraction of the metadata contained in the certificate is registered on the blockchain. The recipient can share any digital form of the certificate and the certification vendor or the university consortium will provide a universal verifier that will be capable of declaring the veracity of the information contained in the certificate. In both cases, issuance and verification against the blockchain are performed using applications that interact with some distributed ledger.

In the third stage of figure 1, we see that the ledger can exist in a public, permissionless blockchain or a permissioned blockchain exclusively built by the consortium. To register the information contained in the certificate using a permissionless blockchain, the certification vendor is subject to the cost and rules of using this public infrastructure. For example, the use of a cryptocurrency that is a fundamental element in the incentive system that guarantees the verification and creation of new blocks. On the other hand, the consortium must build

[5] https://www.learningmachine.com/badges-and-blockcerts/.
[6] https://opencerts.io/.
[7] https://www.chaintalent.io/; http://tic.crue.org/blue/.

and operate the first nodes in the network, provide assistance and training for the introduction of new nodes, set up a governance structure and maintain and update the scaling infrastructure.

The cost comparisons between the permissionless and the permissioned solution are based on the high variable cost/low fixed cost of the former and high fixed cost/low variable cost of the latter. Estimates from [8] indicate that permissioned blockchain projects have fixed costs that are ten times higher than their permissionless counterparts. However, they also show that, with the current consensus mechanisms of permissionless blockchain, the average variable cost per transaction is five times higher than for permissioned blockchain. In other words, the current consensus mechanism for permissionless blockchain is well suited for a small or moderate number of transactions (less than 500k per year), but for a high transaction volume, a private blockchain is the better solution.

4. Cost-benefits Analysis for Managing Academic Certificates

Blockchain technologies provide opportunities for new business and service models or improve an existing processes. We focus on the latter and provide a first approach to cost-benefit analysis for managing academic certificates at universities. There are few documented cases of cost-benefit analysis applied to blockchain technologies, some of these look at permissionless blockchain [4], permissioned blockchain [9], compare both approaches [8] or look at specific use cases like supply-chain finance [10].

To estimate the certification needs of an institution, we use data on issued certificates and graduating student population over a school year. Universidad del Rosario is a private university in Colombia with 12,100 students. That is considered a medium-size university according to US standards[8]. Extension schools and continuing education are also important in most universities; at Universidad del Rosario this adds 15,130 participants in programmes that also receive certificates. During the school year, 3,893 students graduated from the different degree-granting programmes. Also the universities' registrar's office issued a total of 3,383 certificates of different types. This gives a rough estimate of at least 22,406 certificates issued during the school year, including graduating students, participation certificates for continuing education and various additional types of certificates.

Universities looking into blockchain technologies are mainly interested in providing a better and more secure information services regarding the skills and accomplishment of their alumni and student population. In addition, they are interested in improving the existing process and any possible cost avoidance and savings. Most universities already offer e-transcripts and digital certificates to students and alumni; the cost varies since it can be a free service or have a fee from 3 to 10 USD. Since this is a digital timestamped object, the recipient can use it as proof of his accomplishments to as many solicitors (e.g. prospective employers) as required, so there is no scaling cost. The prices of a paper certificate is usually twice that of digital certificates (15 – 25 USD), and if they are notarised documents, the price will go up to 50 USD. These costs are obtained from Stanford University[9], MIT[10] and Universidad del Rosario, Colombia[11]. Paper documents do not scale, so the cost to the recipient would increase depending on the number of solicitors.

Blockchain-enabled certificates are digital objects that provide decentralised verification, and the benefits for the recipient are that they are readily available and with the additional security measures they could be legally considered as notarised documents. They would be readily available because the information they provide would be submitted to the network at the moment of initial issuance and the recipient or solicitor could obtain that information directly at no additional effort or cost. Ideally, there would be no need to incur the cost of re-issuance or notary services.

For universities, the direct benefits are efficiency gains due to streamlined documentation and labour cost reduction for issuance, resolution of conflicting records and verification. An indirect benefit is the reduced exposure to fraud; however, it is difficult to quantify this benefit. To quantify the direct benefits, we obtain information from the registrar's office regarding expenses related to the management of academic certificates: physical and digital cost of issuance, labour cost associated with document processing, resolution of conflicting records and/or manual verification.

Concerning cost, we will only consider the adoption of blockchain technologies for the decentralised verification process. As we mentioned in the previous section, individual institutions are required to maintain governance and oversight on the administrative records of their students and alumni. Our main assumption is that universities may choose to adopt a system of decentralised verification using a certification provider that uses a permissionless/public blockchain infrastructure, or by joining a consortium of institutions that are using a permissioned/private blockchain.

The current business model of certification providers is to charge the issuers for the service.[12] Certification vendors offer

[8] According to [11] in the US small universities have an enrolment of less than 5,000 students, medium size can go up to 15,000 students and larger institutions have more than 15,000. The largest institutions have 30,000 – 70,000 students.

[9] https://registrar.stanford.edu/students/certifications-and-verifications/notarized-documents

[10] https://registrar.mit.edu/transcripts-records/replacement-diplomas

[11] https://www.urosario.edu.co/registro-y-control/solicitud-de-certificados/

[12] Some vendors are transitioning to charging the recipient to manage all types of certificates, not only academic. Discussions

different packages for universities depending on the number of certificates or unique recipients per year. Naturally, the cost to issuers will decrease with the number of certificates. In table 1, we provide an estimate of the yearly cost of using a certification vendor based on a demand of 22,000 certificates per year.

Table 1: Cost per year for issuing organizations of using certification providers.

	Accredible	Xertify
# certificates / recipients		
basic	<10,000	<10,000
advanced	>10,000	unlimited
Price USD		
basic	$ 1.04	$ 0.90
advanced	$ 0.96	15% commission
Yearly cost USD	$ 21,120	$ 19,800

It is important to note that for some of these providers blockchain technologies are only part of their portfolio of services, so it is difficult to make an exact comparison of the service provided; however, they do provide a measure of the cost faced by institutions (issuers).

Certification vendors are using the Bitcoin or the Ethereum public network as a method to notarise the certificates, so it is interesting to determine the cost of using this infrastructure. Blockcerts provide a set of applications and the documentation to implement the verification of digital certificates using permissionless blockchains. To make an efficient use of the network, it is recommended to batch many certificates onto one transaction on the blockchain registry. Certification providers follow and convey this recommendation to their clients to reduce the cost of using the network.

In the Ethereum network, the transaction fee in Ether is composed of two elements – the gas limit and the gas price. The gas limit guarantees that there are sufficient resources to process the transaction in the registry by the network and the amount necessary depends on the complexity with a recommended floor of 21,000. Gas price represents the reward for processing the transactions; therefore, lower values will require more time to get the transaction processed. Both values are affected by the network activity, meaning that when there is congestion on this public infrastructure (e.g. when there is an attractive initial coin offering, ICO) both the gas limit and price will need to increase.

Using the reference gas limit and price mentioned for the implementation of Blockcerts, we find that the yearly cost of issuing 22,000 certificates in batches of 200 certificates (that is 110 transactions per year) is around $25 USD (Table 2).[13] On the other hand, if it takes one transaction to issue each certificate the total cost of issuing the 22,000 certificates would be $5,011 USD. The price considers the average price of Ether during 2018 when the cryptocurrency was quite volatile; using data for 2019 the price is approximately $10 USD for batched certificates and $1,965 USD for the individual certificate issuance.

Table 2: Cost of using the Ethereum network for registering 22,000 academic certificates per year.

Gas Limit	25,000
Gas price in GWei	20
Transaction Fee (ETH)	0.0005
ETH-USD (avg) 2018	$ 456
ETH-USD (avg) 2019	$ 179
Transaction Fee (USD) 2018	$ 0.23
Transaction Fee (USD) 2019	$ 0.09
# transactions for 200 certificates	110
Price for batched certificates	$ 25
Price for individual certificates	$ 5,011

The estimated cost of using the Ethereum network to register groups of certificates is very small compared to the cost submitting transactions for individual certificates. The verification process is not affected by grouping the certificates and hence provides an efficient use of the network at minimal cost. Using a Merkle tree of certificate hashes provides a tractable and reliable approach to batch certificates and reduces cost. Overall, the cost associated with using the permissionless blockchain infrastructure does not seem to represent a significant factor that will affect adoption because the transactions are simple and hence the computational burden on the network is small.

For the decentralised issuance and verification of certificates, vendors must develop applications that can interact with the existing information systems within the institutions to register the abstraction of the certificate onto the blockchain and to query the metadata needed to reproduce and verify the contents of an existing certificate. Information for budgeting blockchain projects is rare; several web pages give rough estimates of blockchain development cost including the developers and infrastructure.[14] The estimates depend on the

on standards (like Verifiable Credentials and Blockcerts) are currently exploring the benefits of decentralised identifiers for the issuer and the recipient. Recipients would hold their certificates in some form of wallet and provide them to any number of solicitors. The certification providers, for a fee, would use blockchain to guarantee the validity of the information regardless of the issuer. This is similar to what a credit bureau currently does; for a monthly fee (5 – 20 USD), they collect information regarding an individual creditworthiness and provide a credit score for solicitors.

[13] https://github.com/blockchain-certificates/cert-issuer

[14] https://www.codementor.io/freelance-rates/blockchain-developers

complexity of the project and are in the range of 15k – 200k USD. In the interviews conducted with the certification vendors with less than 5 years with a product in the market, the project had an overall investment of 60k, a team of two developers with an additional staff of three persons in charge of the commercial strategy and were using cloud infrastructure. Some of these providers were start-ups with several modifications on the product they offer or their commercial strategy and some are still determining whether they will focus exclusively on blockchain technologies or just have it as part of their portfolio for digital certificates.

Consortium-led projects have been created mainly by universities with the collaboration of IT companies. This is the case of Fundación Universitaria San Pablo CEU and Ibermatica in Spain. They started building a permissioned blockchain for the management of academic certificates using Hyperledger Fabric. Since it is a permissioned network, there is no existing infrastructure, so members need to assume the fixed cost to build the network, the applications, and deploy the first nodes in the network. Currently, they are working on two permissioned networks ChainTalent and Red BLUE for Spanish universities. The costs are assumed by the initial members of the consortium and a fee is charged on incoming members. ChainTalent is the more mature of the projects since it has been in development since 2018 and currently has four nodes operating in the network. The main components of the application were developed over a period of four months with a team of two developers and a project lead. The overall investment in the project up to the end of 2019 has been approximately 80k USD. The consortium has established a yearly membership fee of 5,000 EUR (5,600 USD) which provides an unlimited number of certifications to be issued by universities, their main clients. There are additional fees regarding installation of the node, integration to the institution's information systems and maintenance. An exact value for the additional fees depends on the client, but overall the additional fees do not exceed the yearly membership fee.

Similar to the services provided by the certification vendors, consortiums provide applications such as a universal verifier and the possibility for students and alumni to share the certificate information with solicitors using social media.

Using the information regarding cost avoidance and efficiency gains at Universidad del Rosario, we quantify the benefits of adopting a decentralised verification process based on blockchain and compare the cost of adopting the technology using a certification provider or joining a university consortium.

Table 3: Cost-benefit analysis for universities adopting a decentralised verification system based on blockchain technologies.

	USD
Number of Records	22.000
Cost of Record Procesing	$ 35.000
Reduction in Cost per Record	25%
Savings Record Processing	$ 8.750
Conflicting records	5%
Cost of resolution of conflicting records	$ 2.200
Annual Efficiency Benefits	**$ 10.950**
Cost of integration of the technology	$ 1.980
Annual Cost of Decentralized Verification	$ 19.800
Cost of Adoption Through Vendor	**$ 21.780**
Benefit Cost Ratio	0,50
Cost of integration of the technology	$ 1.680
Annual Cost of Decentralized Verification	$ 5.600
Cost of Adoption Through Consortium	**$ 7.280**
Benefit Cost Ratio	1,50

Table 3 summarizes the results of the cost-benefit analysis. In the top part, we estimate the cost of processing the certificates during a year. This cost includes both labour cost and any additional cost for physical or digital certificates. On average, the cost of producing a certificate is $1.6, but this can vary for more complex degree certificates ($5.4) to simpler certificates of continuing education ($0.1). We use very conservative estimates in terms of the reduction of cost (25%) given that the largest savings were already obtained from digitisation. This is important because the immediate benefits of blockchain projects for document processing are sometimes related to the redesign of the process and the digitisation; hence, a common criticism is that these benefits are not related to the use of decentralised verification services [9]. Also, we include the cost avoidance of dealing with conflicting records and any non-automated process related to verification. We estimate the annual benefit regarding conflicting records and automated decentralised verification of around $2,200.

Regarding the cost of using a decentralised verification system, we use the estimated cost from choosing a certification vendor or participating in a university consortium. Also, we estimate the cost of integrating blockchain issuance and verification to the existing technologies. These costs represent anywhere from 10 to 30% of the cost of using the service.

We find that the benefit-cost ratio is 0.48 in terms of adopting the technology using the current price structure offered by certification vendors. On the other hand, the benefit-cost ratio is 1.5 of using the technology by joining a university-sponsored consortium. These estimates are based on the interviews conducted and public information obtained on the different projects. In particular, it is fair to say that

certification vendors have already gone through various iterations of the service, whereas university consortiums are in the process of developing and delivering the technology so their cost could be underestimated. Our results are meant to illustrate the dilemmas in implementing blockchain technologies and a careful comparison of the portfolio of services provided by certification vendors should be taken into consideration.

5. Conclusion

Blockchain technologies have already begun to change how we share important information, in this case, the acquisition of skills and knowledge. Although, we expect a full transformation of the knowledge management system, for the moment, the most immediate impact is to provide direct access to the certificates without the need of re-issuance and a decentralised verification system. Since digital certificates and e-transcripts are a reality at most institutions, the added security features from blockchain technology and reduced cost are especially important, if at some point they are legally accepted as notarised documents with a general acceptance across national borders.

Implementing blockchain projects has similar fixed costs for providers and challenges related to the issuance and verifications systems; this is independent from choosing a permissioned or a permissionless network. We do not find that the fees associated with using existing permissionless networks are important, nor are marginal costs for that matter. The reason is that the transactions that are registered onto the blockchain are not complex operations or time-critical and there are well-known approaches to reduce the cost substantially. So price differentials among certificate vendors are related to the quality of applications that provide a seamless interaction with the information systems of the issuer institutions and additional technologies that are part of their portfolio.

For consortium and permissioned blockchain initiatives, we do not find that the fixed cost of starting the network overwhelmingly increase the fees for newcomers. IT companies that are helping universities implement the technology are paying for some of the fixed cost and investing on building the infrastructure. The current prices for joining a permissioned network and issuing certificate are lower than using certificate vendors, but at the same time, this might also indicate that the former provides a richer portfolio of services for certificates, while consortiums are specializing in blockchain technologies.

The benefits for consortiums of tertiary education institutions are beyond the benefits of just a system for issuing and verifying academic certificates, and this is probably the first step towards systems for sharing information and knowledge management that can be built around the initial nodes that are being developed for certificate management. A similar system but using centralized databases is already a reality for most high schools, colleges and universities in the United States: The National Student Clearinghouse. The National Student Clearinghouse is a non-profit organization that exists since 1993 providing a unique database for enrolments and educational accomplishments for 97% of post-secondary students in the US. Since 2000, they provide digital verification services for degrees using DegreeVerify℠, which also provides readily available e-transcripts for students. This is a good example for a consortium-led effort between universities to share academic information. More importantly, this consortium already provides some estimates on the benefits of sharing information among institutions: first, there are costs saving in sharing academic information ($750 million USD in annual savings), and second, it provides a data-rich environment to analyse the trends in the industry.

Competing Interests:
Universidad del Rosario is one of the participating universities in Red Blue, one of the blockchain projects mentioned.

Ethical Approval:
Not applicable.

Author's Contribution:
CC-I designed and coordinated this research and prepared the manuscript in entirety. O-G has collaborated on different projects on the application of blockchain technology for academia.

Funding:
None declared.

Acknowledgements:
This paper benefited from comments received from the anonymous referees, Federico Lopez, Mauricio Tovar, Ana Maria Moreno, and seminar participants at the Hyperledger Global Forum 2018, Universidad Nacional de Colombia, Red Arca and Universidad Jorge Tadeo Lozano. CC-I would like to thank Francisco Garcia Camargo, director of de registrar's office at Universidad del Rosario, Pablo Carretero Sanchez, Blockchain lead at Ibermatica, Danny Suarez and Sebastian Farfan, co-founders of Xertify.

References:

[1] Deloitte, "Deloitte's 2019 Global Blockchain Survey," 2019. [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/se/Documents/risk/DI_2019-global-blockchain-survey.pdf.

[2] B. Flyvbjerg and A. Budzier, "Why your IT project may be riskier than you think," *Harvard Business Review,* pp. 2-4, September 2011.

[3] M. Rauchs, A. Glidden, B. Gordon, G. Pieters, M. Recanatini, F. Rostand, K. Vagneur and B. Zhang, "Distributed Ledger Technology Systems: A Conceptual Framework," 2018. [Online]. Available: https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2018-10-26-conceptualising-dlt-systems.pdf.

[4] C. Platt, "Medium," 14 May 2018. [Online]. Available: https://medium.com/@colin_/analysing-costs-benefits-of-public-blockchains-with-data-104ec5f7d7e0.

[5] Hyperledger, «www.hyperledger.org,» 11 September 2019. [En línea]. Available: https://www.hyperledger.org/announcements/2019/09/11/consensys-joins-hyperledger-as-a-premier-member.

[6] A. Grech and A. F. Camilleri, "Blockchain in Education," 2017. [Online]. Available: https://publications.jrc.ec.europa.eu/repository/bitstream/JRC108255/jrc108255_blockchain_in_education(1).pdf.

[7] P. Ocheja, B. Flanagan, H. Ueda and H. Ogata, "Managing lifelong learning records through blockchain," *Research and practice in technology enhanced learning,* vol. 14, no. 4, pp. 2-19, 2019.

[8] Ernst & Young LLP., «Total cost of ownership for blockchain solutions,» 2019. [En línea]. Available: https://www.ey.com/Publication/vwLUAssets/ey-total-cost-of-ownership-for-blockchain-solutions/$File/ey-total-cost-of-ownership-for-blockchain-solutions.pdf.

[9] Forrester Research, «Emerging technology projection: The total economic impact of IBM blockchain,» 2018. [En línea]. Available: https://www.ibm.com/downloads/cas/QJ4XA0MD.

[10] P. Panuparb, "Cost-benefit analysis of a blockchain based supply chain finance solution," May 2019. [Online]. Available: https://ctl.mit.edu/pub/thesis/cost-benefit-analysis-blockchain-based-supply-chain-finance-solution. [Accessed 24 February 2020].

[11] «CollegeData,» [En línea]. Available: https://www.collegedata.com/en/explore-colleges/the-facts-on-fit/features-that-set-colleges-apart/college-size-small-medium-or-large/. [Último acceso: 11 06 2020].

