Digital Academic Certification with Blockchain: A Secure, Privacy-Preserving Prototype Using Hyperledger Fabric

Pablo Blanco
Facultad de Ingeniería, Universidad de la República
Montevideo, Uruguay
pblancouy@gmail.com

Gustavo Betarte
Facultad de Ingeniería, Universidad de la República
Montevideo, Uruguay
gustun@fing.edu.uy

Carlos Luna
Facultad de Ingeniería, Universidad de la República
Montevideo, Uruguay
cluna@fing.edu.uy

María Fernanda Molina
Facultad de Ingeniería, Universidad de la República
Montevideo, Uruguay
mfmolina@fing.edu.uy

ABSTRACT

Academic certificates are essential credentials for students, universities, and third parties seeking to verify academic degrees. Traditional paper-based processes are susceptible to forgery, require manual checks, and cause delays and higher costs. This work introduces a prototype for digital academic certification using blockchain technology, specifically Hyperledger Fabric, emphasizing *security*, *privacy*, *traceability* and, *regulatory compliance*, particularly in relation to data protection laws like GDPR. The system uses private data collections, role-based access controls, and auditable transactions to maintain data minimization and accountability. Verification relies on hash matching, so sensitive data remains off-chain. The architecture clearly defines ecosystem roles—administrators, students, graduates, and verifiers—and considers interoperability with national and regional systems.

Our qualitative assessment indicates that a permissioned blockchain can enhance trust and traceability, although challenges remain in scalability, governance, and adoption. We believe that a privacy-preserving blockchain-based certification system is feasible and could reinforce education infrastructure when integrated with existing digital and data protection policies.

CCS CONCEPTS

• **Security and privacy → Privacy-preserving technology**; *Security and privacy in academia*; • **General and reference → Blockchain**.

KEYWORDS

Academic Certification, Blockchain, Hyperledger Fabric, Privacy, Security, GDPR.

1 INTRODUCTION

The issuance of academic credentials worldwide faces significant challenges related to forgery, complex manual verification processes, and high operational costs. The necessity for a reliable, secure, and verifiable method for managing digital documents has driven the exploration of *blockchain technology* [18]. Blockchain's inherent properties—immutability, auditability, and decentralization—offer a compelling solution to ensure the authenticity, integrity, and security of digital academic certificates, making it a pivotal technology for modernizing public administration and education sectors.

In Uruguay, the University of the Republic (Udelar) seeks to modernize its credentialing system, but faces the critical challenge of adopting new technologies while strictly adhering to local and international personal data protection regulations [12, 20]. Current decentralized solutions often struggle with the "right to be forgotten" and data transparency requirements inherent to public blockchains, making them suboptimal for regulated academic environments. This context motivates the need for a secure, permissioned, and privacy-preserving certification model. Unlike traditional Public Key Infrastructure (PKI) systems, which primarily guarantee data integrity, a permissioned blockchain provides a shared, immutable log of issuance and verification events, crucial for achieving **distributed trust** and consensus on certificate status across different organizations. Specifically, the *Central Informatics Service of Udelar* (SECIU) requires a robust solution to enhance the reliability and security of the digital certificates it issues or verifies. This study, therefore, is justified by the need to design and validate a blockchain-based prototype tailored to the local regulatory landscape, providing both a theoretical, comparative overview of regional initiatives (such as Brazil's *Rede Acadêmica com Blockchain (RAP)* [7, 8]) and a practical, compliant foundation for future national implementation.

The specific objectives of the work are to:

(1) Conduct a comprehensive literature review on blockchain technology and its application in the validation of digital certificates.
(2) Design a digital certification system architecture focused on security, privacy, and traceability. The design is based on a preliminary solution proposed by the authors in [16, 17].
(3) Implement a functional prototype based on *Hyperledger Fabric* [2, 14], that validates the proposed architecture.
(4) Evaluate the prototype's behavior, its advantages, and limitations, and propose a roadmap for future work.

The rest of the paper is organized as follows: Section 2 briefly discusses the current state of the art and key blockchain concepts, while Section 3 describes the design and implementation of the prototype. Section 4 presents the results, analysis, and discussion. Finally, Section 5 summarizes the conclusions and outlines future work.

A more detailed version of this short paper can be found in Report [5].

2 RELATED WORK

The use of blockchain in academic environments has gained notable attention because of its immutability and auditability features, among other qualities. Examples include the MIT Media Lab's *Blockcerts* initiative [21], which sets an open standard for issuing and verifying blockchain-based certificates, and the University of Nicosia, which was among the first to issue degrees that can be verified on the Bitcoin blockchain [19]. These initiatives demonstrate the technical feasibility but often encounter challenges related to privacy and scalability.

Some studies examine the challenges of adhering to personal data protection regulations like GDPR [12, 20] when using blockchain for managing personal data, such as academic certificates. For instance, although Blockcerts offers a decentralized and open approach, it depends on public blockchains like Bitcoin, which can reveal metadata and create challenges for data protection compliance in regulated environments.

Our analysis concentrated on two major regional initiatives that shaped our design, especially regarding data protection: *Rede Acadêmica com Blockchain (RAP)* (Brazilian Academic Blockchain Network) from Brazil [8] and the *Blockchain Federal Argentina (BFA)* from Argentina [3]. RAP is a public, decentralized platform for issuing, safeguarding, and verifying digital certificates [6]. It adopts a hybrid approach that combines blockchain for integrity and a separate database for the long-term storage of sensitive data. Although innovative, its public nature poses potential privacy concerns, as a public blockchain's transactions are transparent and accessible to all network participants, potentially exposing transaction metadata and compromising user anonymity over time. Conversely, BFA functions as a permissioned network for public institutions, with each institution handling its own data and security [4]. The BFA model explicitly recommends cryptographic hashes referencing off-chain data for privacy-sensitive information [10], which directly aligns with our approach.

Considering the characteristics of blockchain, in previous work [16, 17] we have proposed the idea of using blockchain for data access control and auditing, while also leveraging off-chain solutions for safely storing and managing personal data. These off-chain methods permit modifications or deletions of data, which isn't possible directly on the blockchain. Our prototype design draws from best practices of these studies, focusing on a permissioned network for proper data governance and relying on off-chain storage to meet privacy regulations [12, 20]. We chose Hyperledger Fabric because it inherently supports these features, aligning with our requirements.

3 DESIGN AND IMPLEMENTATION OF A PROTOTYPE

The prototype was developed as a proof of concept to validate the research hypotheses. It was designed to meet several key functional requirements: (1) *Issuance of a digital certificate*: an administrator generates a certificate, which includes a cryptographic hash of the student's data; (2) *Secure storage*: sensitive data is stored in a conventional off-chain database, while only its hash is sent to the blockchain; (3) *Controlled access*: the data owner (student) can grant or revoke access to their certificate; and (4) *Verification*: an external verifier can validate the authenticity of a certificate by matching a hash provided by the student against the one on the blockchain.

Additionally, the system was built with several non-functional requirements in mind, crucial for its real-world viability and compliance: (1) *Privacy*: sensitive data (PII) must not be stored on the blockchain ledger, addressing the immutability issue and the "right to be forgotten" defined by the GDPR [11]; (2) *Security*: access control is based on a role-based access model, with cryptographic identities provided by Fabric's Membership Service Provider (MSP) [15]; (3) *Auditability*: all on-chain transactions are cryptographically signed and auditable; and (4) *Integrity*: the use of hashes ensures that any change in the off-chain data is immediately detectable.

The system explicitly models four roles, derived from General Data Protection Regulation (GDPR) concepts [11]:

- **Data Controller (DC)**: The university (e.g., Udelar), which determines the purposes and means of data processing. They are responsible for the overall governance of the network.
- **Data Processor (DP)**: The administrative staff of each faculty, who processes data on behalf of the DC. They are the only actors with permission to issue certificates to the blockchain.
- **Data Owner (DO)**: The student or graduate who owns their personal data. They have the ultimate control over who can access their certificate hash for verification.
- **Receiver (R)**: An external entity (e.g., a company, another university) that needs to verify the authenticity of a certificate.

3.1 Architectural components

The prototype is built on a *Hyperledger Fabric* network composed of two organizations: the *University* and the *Verifier*. The architecture consists of three main components:

(1) **Chaincode (Smart Contract)**: It should be noted that a smart contract is a program that is stored and executed on a blockchain without anyone outside being able to interfere with its operation. The chaincode is the core logic of the system, written in Go [13]. It manages the lifecycle of certificates, from issuance to verification. A key feature is the use of *private data collections* [1], which are crucial for our privacy model. These collections allow sensitive data hashes to be stored only on the peers of the organizations that are explicitly authorized to have them, thus preventing other organizations in the consortium from seeing them.

(2) **Application Gateway**: An intermediary application that allows different actors to interact with the blockchain network. It provides APIs for the Data Processor (to issue certificates), the Data Owner (to grant or revoke access), and the Receiver (to request verification).

(3) **External Database**: A conventional database (e.g., CouchDB) used to store the off-chain sensitive data, such as student

names and academic details. This data is linked to the on-chain hashes, allowing for compliant data deletion and modification.

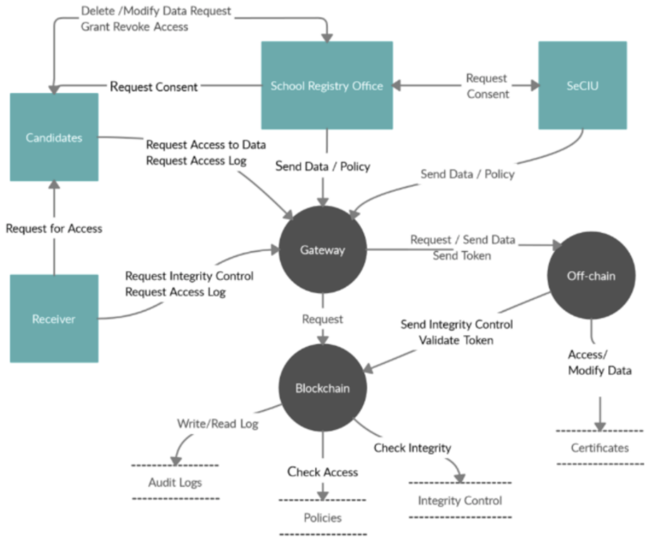

Figure 1: System Architecture.

3.2 Implementation details and logic

The chaincode itself is implemented with specific functions for ‘issueCertificate‘, ‘verifyCertificate‘, ‘updateCertificate‘, ‘grantAccess‘ and ‘removeCertificate‘, among others. The access management logic is handled by the application layer, which manages the student’s private key and controls the submission of verification requests.

The prototype implements the following key use cases, which correspond to the core functionalities of a digital academic certification system:

3.2.1 Certificate Issuance. The **Data Processor** initiates the process by uploading the student’s personal data to the off-chain database. The system then generates a unique cryptographic hash of this data using a secure hashing algorithm (e.g., SHA-256), which is immutably stored on the blockchain ledger. This flow is graphically represented in the Figure 2.

3.2.2 Certificate Verification. The verification process is designed to be privacy-preserving: a verifier submits a certificate hash and ID provided by the Data Owner. The system then queries the blockchain to match this hash against the one on the ledger without exposing any PII. It should be noted that the verification process must be previously authorized by the owner of the information, as it requires access to personal data. This flow is graphically represented in the Figure 3.

3.2.3 Certificate Revocation and Modification. The system provides a mechanism for the **Data Processor** to revoke a previously issued certificate in cases of error or withdrawal. This action involves a new transaction on the blockchain that marks the certificate as invalid.

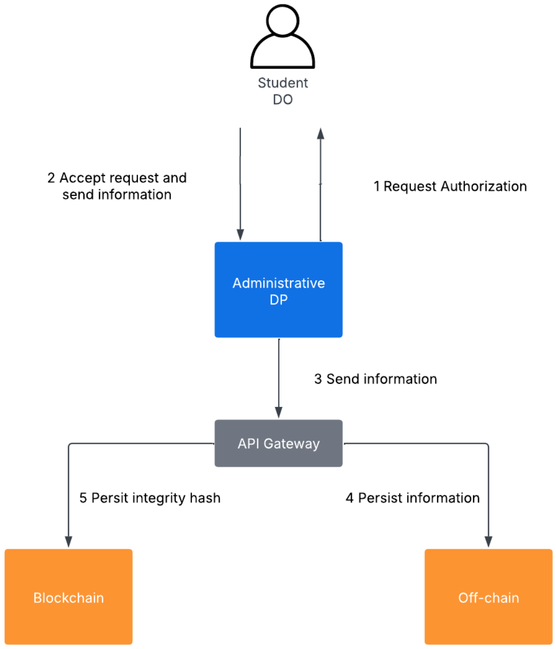

Figure 2: Certificate Issuance Process.

The off-chain data can then be deleted or modified, providing a method to comply with the "right to be forgotten" principle for the underlying data, this flow is represented by the Figure 4.

3.2.4 Access Management. The prototype gives the **Data Owner** (student) control over who can view their certificate hash for verification. This is achieved through a **grant access** function, which allows the student to authorize specific verifiers (Receivers) to query the blockchain ledger for their certificate. This ensures that personal data remains private until the data owner gives explicit consent for its verification, the use case is reflected in the Figure 5.

The design includes detailed diagrams of the architecture and interaction flows, as seen in Figure 1. The use of a permissioned network allows for fine-grained access control to the ledger data, which is a key advantage over public blockchains where all data is transparent. A detailed description of the prototype is available in [5]. The source code is accessible accessible on the GSI’s Gitlab repository [9].

4 EVALUATION AND DISCUSSION

The prototype was evaluated through a series of manual and automated tests performed on a local Hyperledger Fabric network. The methodology focused on validating each of the research objectives, including the proper functioning of issuance, access management, public integrity validation, and data privacy mechanisms. The tests confirmed that the system is fully functional and that each actor can perform their tasks while adhering to the established security and privacy policies. The tests simulated certificate creation, access requests by a data owner, and the subsequent verification by a third

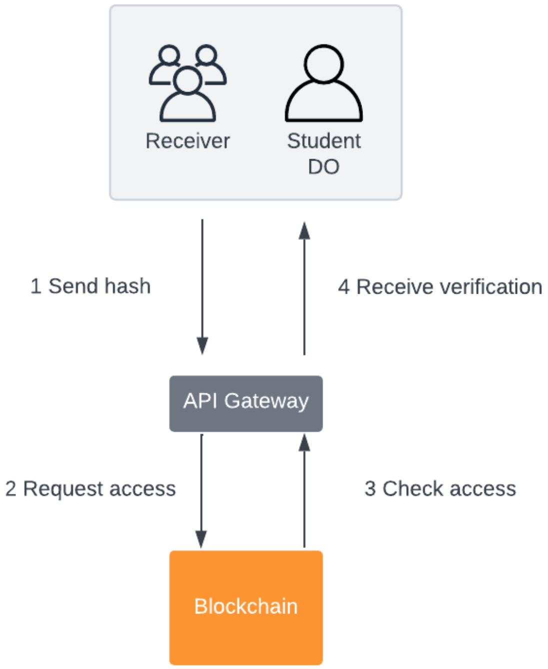

Figure 3: Certificate Verification Process.

party, all of which performed as expected according to the defined rules.

4.1 Threats and Mitigation

The system was designed to mitigate various threats, including:

- **Data tampering**: The immutability of the ledger and the integrity of cryptographic hashes ensure that certificates cannot be altered without being detected. Any attempt to modify a certificate on the off-chain database would result in a hash mismatch during verification, alerting the verifier to a potential fraud attempt.
- **Denial of service (DoS) attacks**: The architecture of private channels in Fabric isolates transactions between groups, which limits the impact of an attack to a single channel. Additionally, the ability to configure 'throttling' (request rate) on the nodes helps control the amount of requests processed at a given time, which is essential for mitigating saturation attempts.
- **Compromise of cryptographic keys**: Fabric allows for integration with *Hardware Security Modules (HSMs)* for secure key storage. Key rotation policies can also be implemented to reduce the risk of long-term compromise.

4.2 Advantages, Limitations, and Challenges

The prototype demonstrated several advantages in the context of academic certification:

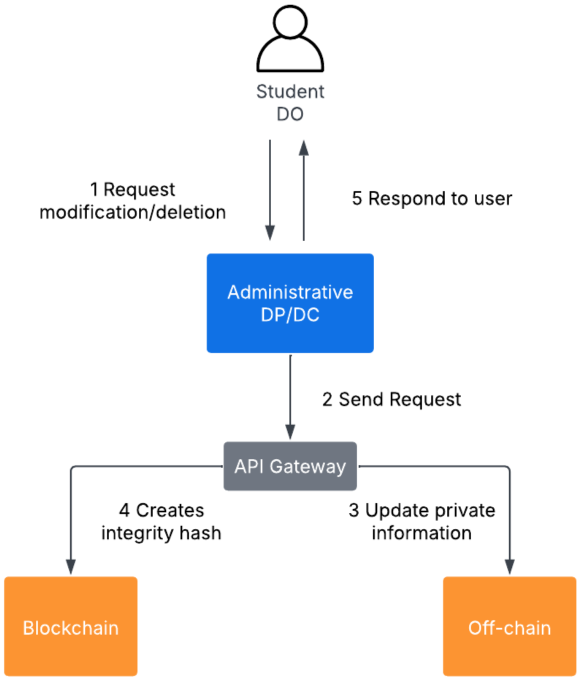

Figure 4: Certificate Removal/Update Process.

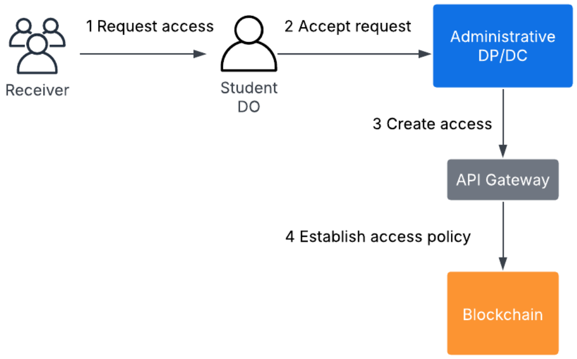

Figure 5: Grant Certificate Access Process.

- **Enhanced security and trust**: The immutability of the blockchain ledger and the cryptographic integrity of transactions make certificates tamper-proof and provide a verifiable audit trail.
- **Improved traceability and auditability**: Blockchain offers by design a reliable log of certificate issuance and verification events, which can be audited by third parties and regulatory bodies.

- **Compliance with data protection regulations**: By storing sensitive data off-chain and only using hashes, the system complies, to our knowledge, with data protection regulations and respects the principle of data minimization, a key concern in an academic context.
- **Reduction of fraud**: The cryptographic integrity of the on-chain record makes it virtually impossible to forge a certificate.

However, the evaluation also highlighted several limitations and challenges:

- **Scalability and performance**: The evaluation is purely functional and qualitative, and thus quantitative metrics (throughput and latency) are missing. While the prototype's performance was adequate for a small-scale network, real-world multi-institutional deployments could face performance bottlenecks. This highlights the necessity of rigorous performance testing (as outlined in future work) to evaluate how the system scales with a larger number of transactions and organizations.
- **Right to be forgotten**: While off-chain data deletion is possible, the immutability of on-chain hashes poses a legal challenge, as the hash could be considered pseudonymized personal data in specific regulatory contexts. To mitigate this issue and achieve better compliance, future work should explore mitigation strategies such as Zero-Knowledge Proofs (ZKPs) to enable privacy-preserving verification without revealing PII.
- **Centralization and governance**: The implementation of a permissioned network requires participating entities to trust a Certificate Authority (CA), which introduces a degree of centralization. Managing a multi-institutional consortium is a complex challenge that requires a clear governance framework to handle access policies and dispute resolution. It should be noted that the work carried out only covers the use case of issuing and validating degrees from a single University.
- **Cost of implementation and maintenance**: The infrastructure and technical support required for a robust Hyperledger Fabric network can be expensive, a factor that could hinder adoption by smaller institutions.

5 FINAL REMARKS

This research successfully proved that a privacy-preserving digital academic certification system can be implemented using Hyperledger Fabric. The prototype confirms that permissioned blockchain technology combined with off-chain data storage offers a secure and compliant way to manage academic credentials.

The findings show that this system provides considerable advantages compared to traditional approaches. Nonetheless, its complete effectiveness depends on overcoming the challenges we've identified. We recommend the following directions for future research:

- *Scalability Analysis*: Perform a more detailed assessment of performance and scalability in real-world conditions, including a greater number of transactions and peers.
- *Advanced Privacy Mechanisms*: Investigate the use of advanced cryptographic techniques such as Zero-Knowledge Proofs (ZKPs) to allow for certificate verification without revealing any details about the certificate or its holder.
- *Integration with National Systems*: Connect the prototype with Uruguay's national identity systems to simplify student onboarding and ensure secure key management.
- *User Interfaces and Interoperability*: Create user-friendly interfaces for different users and explore interoperability standards to enable seamless communication with other national and international certification systems.
- *Credential security*: Consider implementing Hardware Security Modules (HSMs) that adhere to the PKCS11 standard for more secure cryptographic key storage.

This work establishes a strong foundation for the future of digital academic credentials in Uruguay and the surrounding region, supporting the country's broader digitalization initiatives.

REFERENCES

[1] Elli Androulaki, Artem Barger, Vita Bortnikov, Christian Cachin, Angelo De Caro, David Enyeart, Christopher Ferris, Gennady Laventman, Yacov Manevich, et al. 2018. Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. In *Proceedings of the Thirteenth EuroSys Conference*. ACM, 1–15.

[2] Elli Androulaki and et al. 2018. Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. *Proceedings of the Thirteenth EuroSys Conference* (2018), 1–15. https://doi.org/10.1145/3190508.3190538

[3] Blockchain Federal Argentina. 2021. Blockchain Federal Argentina. Available at: https://bfa.ar/.

[4] Blockchain Federal Argentina. 2021. Institutions using Blockchain Federal Argentina (BFA). Available at: https://bfa.ar/instituciones.

[5] Pablo Blanco. 2025. *Digital Academic Certification with Blockchain: A Secure and Privacy-Preserving Prototype Using Hyperledger Fabric*. Master's thesis. https://www.fing.edu.uy/~cluna/PB-thesis.pdf

[6] C Costa, M Pires, E Silva, and R Rodrigues. 2018. RAP: A Private and Secure Digital Diploma Platform Based on Blockchain. In *2018 IEEE 1st International Workshop on Blockchain and Data Management*. IEEE, 1–6.

[7] Banco Nacional de Desenvolvimento Econômico e Social (BNDES). 2021. Rede Blockchain Brasil (RBB): A Hybrid Blockchain Initiative. Available at: https://bndes.gov.br/rbb.

[8] Rede Nacional de Ensino e Pesquisa (RNP). 2021. Diploma Digital: A Blockchain-Based Solution for Digital Certificates. Available at: https://rnp.br/diploma-digital.

[9] Grupo de Seguridad Informática (GSI). 2025. Electronic Titles Repository. https://gitlab.fing.edu.uy/gsi/blockchain/titulos-electronicos/. Prototype source code.

[10] Jacob Eberhardt and Stefan Tai. 2017. On or Off the Blockchain? Insights on Off-Chaining Computation and Data. In *On or Off the Blockchain? Insights on Off-Chaining Computation and Data*. 3–15. https://doi.org/10.1007/978-3-319-67262-5_1

[11] European Parliament and Council. 2016. General Data Protection Regulation (GDPR). Regulation (EU) 2016/679.

[12] European Parliament and of the council. 2016. Regulation (EU) 2016/679. *Official Journal of the European Union* (2016). [Online]. Avalilable: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[13] GO. 2025. GO. Available at: https://go.dev.

[14] Hyperledger. 2021. Hyperledger Fabric. Available at: https://www.hyperledger.org/use/fabric.

[15] Hyperledger. 2023. Hyperledger Fabric Documentation: Access Control. Available at: https://hyperledger-fabric.readthedocs.io/en/release-2.5/access_control.html.

[16] Fernanda Molina. 2021. *Constructing privacy aware blockchain solutions: design guidelines and threat analysis techniques*. Master's thesis. https://hdl.handle.net/20.500.12008/30599

[17] Fernanda Molina, Gustavo Betarte, and Carlos Luna. 2023. A Blockchain based and GDPR-compliant design of a system for digital education certificates. *CLEI Electron. J.* 26, 1 (2023). https://doi.org/10.19153/CLEIEJ.26.1.3

[18] Satoshi Nakamoto. 2009. Bitcoin: A Peer-to-Peer Electronic Cash System. (May 2009). http://www.bitcoin.org/bitcoin.pdf

[19] University of Nicosia. 2017. University of Nicosia Blockchain Initiative. Available at: https://www.unic.ac.cy/blockchain/.

[20] República Oriental del Uruguay. 2008. Ley 18.331: Protección de datos personales y "Habeas Data". Available at: https://www.impo.com.uy/bases/Leyes/18331-2008.

[21] P Shrier and S Shrier. 2019. Blockcerts: The Open Standard for Blockchain Credentials. Available at: https://www.blockcerts.org/.