scientific reports

Check for updates

OPEN

Blockchain ensuring academic integrity with a degree verification prototype

Mariano Anthony Cardenas-Quispe & Alex Pacheco ✉

Blockchain technology has transformed information management through decentralization, security and immutability. However, a gap persists in its application for the issuance and verification of professional qualifications in education. This study presents a prototype developed in Python and Docker, designed to guarantee the authenticity and traceability of academic credentials through a hybrid blockchain network with six Docker nodes. The prototype includes processes such as initial data registration, node configuration, credential generation with QR codes and associative signature based on Byzantine consensus. During the signing stage, previously stored records are validated and authenticated, ensuring integrity before final credentials are generated. The peer-to-peer network ensures synchronization, decentralized storage and immutability of records. On average, initial title registration on the blockchain took 2.97 s, with block replication taking 0.02 s. Record signing had a latency of 0.96 s, with replication in 0.79 s, and Byzantine consensus took 0.12 s, all with moderate resource consumption. The generated titles, verifiable via QR codes, reinforce trust and reduce academic fraud. This model stands out for its practical and scalable approach, with potential for adaptation to other sectors. Future work should address the scalability and robustness of the system for more complex applications.

Keywords Blockchain, Authentication, Byzantine consensus, P2P network, Signature by association

The integration of technology in our daily lives, especially in the academic and professional environment, has marked a significant transition towards more digitalized approaches[1]. In this context, blockchain technology is characterized by its decentralized structure, where information is distributed among nodes, and its ability to guarantee the immutability of data through advanced cryptography; these characteristics position it as a robust tool to protect the privacy and integrity of information, facing challenges such as counterfeiting and unauthorized access[2–4]. Blockchain's robustness in information security, coupled with its ability to ensure data integrity, makes it a reliable option for managing valuable assets[5,6]. In addition, its decentralized nature makes blockchain a disruptive tool applicable in multiple sectors, including education, underscoring its importance in promoting more transparent and efficient information management[7].

The incorporation of blockchain technology in various sectors has proven to be a technological revolution with applications that transcend the boundaries of finance. In the context of financial and business innovations, blockchain has established itself as a fundamental pillar, driving developments such as tokenization, Initial Coin Offerings (ICOs) and Decentralized Autonomous Organizations (DAOs); these applications have been fundamental in the advancement and growth of various industries, highlighting its versatility and ability to adapt to different contexts[8,9]. Recent research has delved into the use of blockchain technology to optimize the management of academic records and the verification of the authenticity of resumes. These studies highlight blockchain's ability to ensure data security and validation through the use of advanced hashing techniques and decentralized storage, offering a powerful solution against information and document fraud in academic and professional contexts[10–12]. In this study, a prototype is developed, which takes advantage of the benefits offered by blockchain technology, such as immutability, decentralization and the use of advanced cryptographic algorithms. Additionally, complementary tools are integrated, such as the HTTP protocol for communication through REST APIs, and the SMTP interface for the secure sending of confidential emails. In this way, the registration and management of academic credentials is guaranteed on a platform that ensures data integrity, confidentiality and availability.

Cañete L@b Research Center, Professional School of Systems Engineer, Universidad Nacional de Cañete, San Vicente de Cañete, Lima, Perú. ✉email: apacheco@undc.edu.pe

However, there is a notable absence of studies on blockchain systems developed specifically with Python for professional title management and verification. Review of previous research with similar approaches revealed the application of various methodologies, each with specific strengths and limitations. For example:

- Description of platforms and use cases: [13] describe platforms such as Blockcerts and Block.co, along with cases of academic institutions using blockchain. While they provide a broad overview of the blockchain credential ecosystem, they do not delve into methodological analysis or specific technical developments.
- Book review: [14] discusses technological, business and legal aspects of blockchain in his review of the work by Vilarroig Moya and Pastor Sempere (2018), but does not directly address the implementation of blockchain in academia.
- Exploratory research and multi-criteria analysis: [15] combine literature review, interviews with specialists and international experiences on the issuance of degrees and titles supported by blockchain. This method allows the design of a structural model based on multi-criteria analysis, but its scope is focused on conceptualization rather than technical implementation.
- Descriptive literature review: [16], reflects on blockchain and its relationship with technological innovation through a descriptive literature review, using scientific articles from databases such as Web of Science, ProQuest, SciELO and Scopus. This approach organizes findings into relevant topics, although it lacks a direct practical application.

These studies highlight the theoretical and conceptual possibilities of blockchain in academic credentials, but underline the need for research focused on functional prototyping and experimental analysis. This study does not aim to establish that Python is the best language for blockchain, but addresses the challenge of highlighting its applicability in functional development from scratch and evaluating a blockchain prototype in Python, implemented in a distributed environment with Docker, to ensure authenticity and security in professional degrees. In addition, expansion in the industrial and business sectors, increasingly influenced by the formation of trust-based partnerships, faces significant challenges due to increased regulation, cybercrime and fraud, factors that are limiting this growth[17,18].

This work distinguishes itself from previous research focused on conceptualizations or general descriptions by presenting a technical and practical approach. The integration of a custom hybrid blockchain with Python and its deployment in a distributed environment using Docker represent significant advances in terms of scalability and replicability. This work brings a practical and innovative approach to the educational domain by complementing previous theoretical research, such as the study of[19] entitled "Exploring Blockchain Technology and Its Potential Applications for Education". The main contribution lies in the development of a functional scheme that combines traceability and security through the use of QR codes and a Byzantine consensus. Unlike exclusively theoretical approaches, this prototype has been technically validated, offering a concrete solution to real problems of fraud and forgery in academic credentials. Its implementation is positioned as a replicable and adaptable model to diverse needs within the educational sector.

This research is structured as follows: In the methodology, the description is made in high level language about the architecture and design of the software, in the third section the results are shown, which are the simulated nodes with Docker containers in the Docker network, the blockchain, registration blocks and signature of the data, the professional title with QR code for verification in the blockchain, in the fourth section the results are discussed, comparing it with the ideas of other authors, in the fifth section the Limitations and future work are presented, in the sixth section the conclusions are presented.

Method

The selection of tools and technologies to develop a blockchain prototype depends on several factors, such as flexibility, accessibility, learning curve and purpose of the project. While languages such as C + + (Bitcoin), Golang (Go Ethereum) and Rust (Polkadot) are widely used for production blockchain implementations due to their efficiency, performance and low-level control, Python and Docker offer specific advantages in the context of prototyping and initial development, which justify their use in this work.

Python has been chosen as the primary language for this prototype due to its ease of use and accessibility, as it has an intuitive syntax that allows developers to focus on the conceptual and functional aspects of the prototype rather than low-level technical details. In addition, Python offers a wide variety of useful libraries and frameworks for blockchain development, such as web3.py for interfacing with Ethereum, Flask for building API interfaces quickly, and cryptographic tools such as PyCrypto and cryptography, which simplify the implementation of essential functionalities such as hashing, key generation and signature validation. These features make Python an ideal tool for research and prototyping projects, where it is required to test concepts and validate ideas before moving them to a production environment.

On the other hand, Docker is used in this work to create isolated and reproducible environments, which guarantees a consistent execution of the prototype on different platforms. This is especially relevant in the blockchain context, as Docker allows simulating distributed networks by running blockchain nodes in independent containers, effectively replicating a real distributed network in a controlled environment. In addition, Docker facilitates system portability and scalability, which allows testing different network configurations and scales without the need to set up multiple physical or virtual machines, optimizing the development process.

The focus of this work is not to develop a production-ready blockchain system, but to design a working prototype that allows testing, validating and demonstrating fundamental concepts in a controlled environment. Python and Docker efficiently fulfill this purpose, as they simplify the modular development of blockchain components and allow researchers to focus on the underlying algorithms and network dynamics. In future

stages, the results obtained could be migrated to more robust languages and environments such as C++, Golang or Rust, depending on the specific requirements of a system in production.

Regarding the hosting of the prototype source code, the Zenodo platform was used due to its ability to guarantee the immutability of the files through DOI, which can be accessed at the following link https://doi.org/https://doi.org/10.5281/zenodo.14575522.

Zenodo was specifically chosen because its technical features directly align with the research objectives, including data integrity, traceability and accessibility. Developed and maintained by CERN, this platform supports the long-term preservation of academic projects and ensures compliance with international standards for data storage and handling, reinforcing the validity of the study. In addition, Zenodo allows the hosting of different file types and sizes, offering flexibility in data management.

The software is designed to implement a number of critical processes that ensure its efficient operation within the blockchain technology. This design The software is composed six main processes that are fundamental to ensure the integrity, security and efficiency of the system:

- ***Registration on the Blockchain:*** This process records essential data, such as professional title information, issuing authority details and network participants. Smart contracts are executed by custom scripts that verify that the data meets the required conditions before being packaged into blocks. These blocks are distributed and replicated across Docker nodes. To manage this functionality, Flask is used to create REST APIs that facilitate communication between nodes, and the Python hashlib library is used to generate unique hashes that ensure data integrity and authenticity. This process ensures that all recorded information is reliable and cannot be altered without detection.
- ***Network Configuration and Registration:*** This process establishes and synchronizes the nodes of the blockchain network. Using Docker, the system creates five private nodes by default, each running as a separate container. During initial setup, internal IP addresses and communication ports (5000–5004) are assigned to facilitate data exchange. Node authentication is performed using system-generated cryptographic keys, ensuring that only authorized nodes can participate in the network. This initial configuration allows nodes to operate in a distributed and synchronized manner, ensuring a secure and scalable ecosystem for the blockchain. Subsequently, an additional publicly accessible node is deployed, which will serve as an interface for title queries.
- ***Data Registration:*** This process allows different types of information to be registered in the blockchain, such as data on authorities, participants and professional titles. In the specific case of titles, once registered, the system generates a unique hash that identifies the title registration. This hash is sent to the interested party via an email managed with the smtplib and email libraries, providing the user with a means to consult the status of their title and verify the progress of its validation in the blockchain. The recorded data is structured and encrypted using the json and hashlib libraries, ensuring transparency, traceability and security in the management of sensitive information.
- ***Signature by association:*** This process validates and authenticates title records through the participation of authorities in the network. When an authority (node user) decides to sign a record, it uses its private key to generate a cryptographic signature that authenticates both its identity and the validity of the record. This action generates a request that is distributed to the nodes participating in the network. Each node checks the local blockchain to confirm that it is up to date and validates the credential of the signer. If at least 67% of the nodes approve the request, the signature is recorded in a new block within the blockchain. When all the necessary authorities complete the signature process, the professional degree is generated and the system notifies the interested party via email with the PDF attached, informing them that their degree has been fully validated and signed. This approach ensures that all signing actions are verifiable and backed up on the blockchain, reinforcing the integrity and authenticity of the records.
- **Title Generation with QR Code:** In this process, the system extracts the professional title information from the blockchain. A query link is generated based on the unique hash of the title data (different from the hash of the blockchain), which allows access to the specific information of the record. From this link, a QR code is created and incorporated into the title design, along with the relevant data. Finally, the title is exported as a PDF document ready for delivery.
- **Query or Validation of Professional Titles:** The system allows users to query a professional title by entering the unique hash of its data in the blockchain. If the record exists, the title is displayed with all associated data and signatures. Otherwise, no response is generated.

This process ensures that only valid and fully signed records are accessible, reinforcing the trust and transparency of the system. These processes work together in the proposed system to ensure the authenticity, integrity and traceability of academic degrees recorded in the blockchain, as seen in Fig. 1.

The model was developed in Python 3.10, using both Python built-in libraries and third-party packages obtained via pip[20]. It also implements a peer-to-peer (P2P) network that is inspired by the pioneering concept of distributed nodes in a decentralized communication network proposed by[21], which emphasized the importance of each station connecting to all adjacent stations through a continuous connection, in contrast to centralized systems that are limited to connections through a few link points. Following this vision, using Docker containers a P2P network is created that simulates a blockchain with up to five participating nodes, thus establishing a distributed and decentralized environment. Each node in this network plays a fundamental role in the efficient and secure management of the blockchain. In addition, it integrates a public node to facilitate the consultation of academic degrees and access to blockchain information. Communication between the nodes is performed using HTTP protocols and a REST API through port 5000, optimizing data exchange and the management of university degrees in the blockchain (Fig. 2).

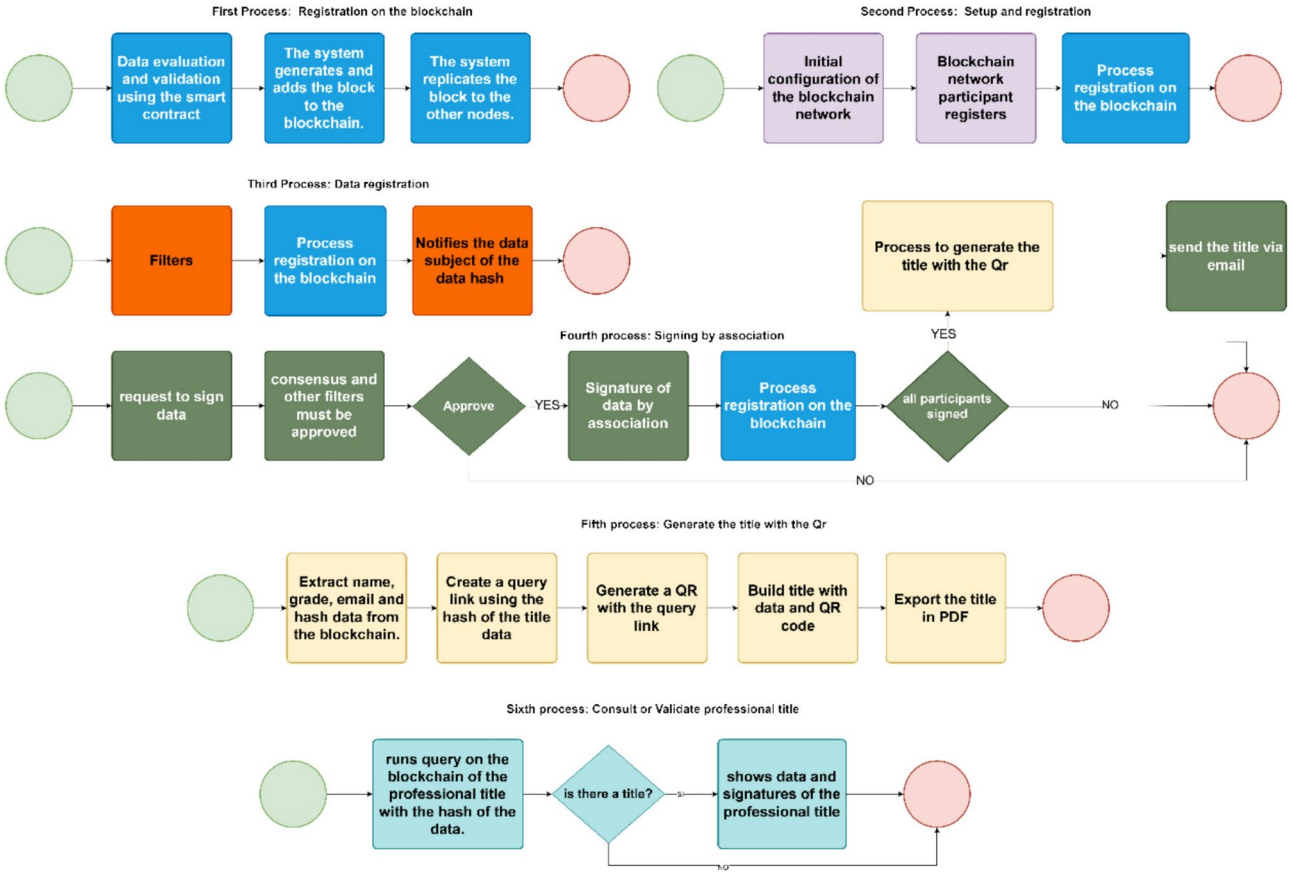

Fig. 1. Relevant system processes.

The system records three groups of information in each block of the chain (Fig. 3). The first group of information is the metadata, which includes details such as the timestamp and other relevant data. The second group of data, called "Contract," records the entity responsible for executing the smart contract and creating the block, ensuring traceability and accountability on the blockchain. The third group, is a specific record intended to store the data that the user wants to record. In addition, each block contains the hash of the previous block, i.e., it is a mathematical function that transforms a block of data of indefinite length into a block of characters of fixed length[22], this is a unique identifier that links each block with its predecessor in the chain to ensure its integrity and immutability[23] (Fig. 4).

The proposed system is configured in such a way that each action, whether it is the registration of information or the digital signature, is stored as an individual block, synchronized in all nodes according to the initial configuration defined by the university. In this process, the institution determines the number of nodes (between 1 and 5) and assigns the two fundamental roles (registering and signing) in a flexible way, being able to assign one or both of them to each node. According to this configuration, the node with the registration role enters the degree information, generating a registration block that is synchronized in the network and sends a preliminary notification to the graduate by means of a hash code. Subsequently, the node or nodes designated with the signing role proceed to digitally sign the transaction, creating new blocks that are synchronized throughout the network and guarantee the integrity and traceability of the process. Finally, once the transaction is completed, the graduate receives a final notification that includes both the hash code and the professional title, which allows him/her to verify the authenticity of his/her certification through the public node, in charge of validating the transaction registered in the private blockchain (Fig. 5).

Results

Blockchain network nodes with docker

The first result demonstrates the initialization of the blockchain system on a VPS (Virtual Private Server), achieved through the activation of containers pretending to be nodes in the network. Each container, acting as an individual node, is an integral part of the blockchain network architecture (as seen in Fig. 2). Figure 6 illustrates the initiation process and details of these containers, highlighting the independent function of each as a node in the network. Communication between the nodes is via port 5000, which is configured in the blockchain system embedded in the custom image named 'node'. Each node has a unique IP address within the internal Docker network, facilitating a coordinated and efficient interaction, as shown in Fig. 7. This interaction is based on the combination of the IP and the port defined in the blockchain system included in the construction of the 'node'

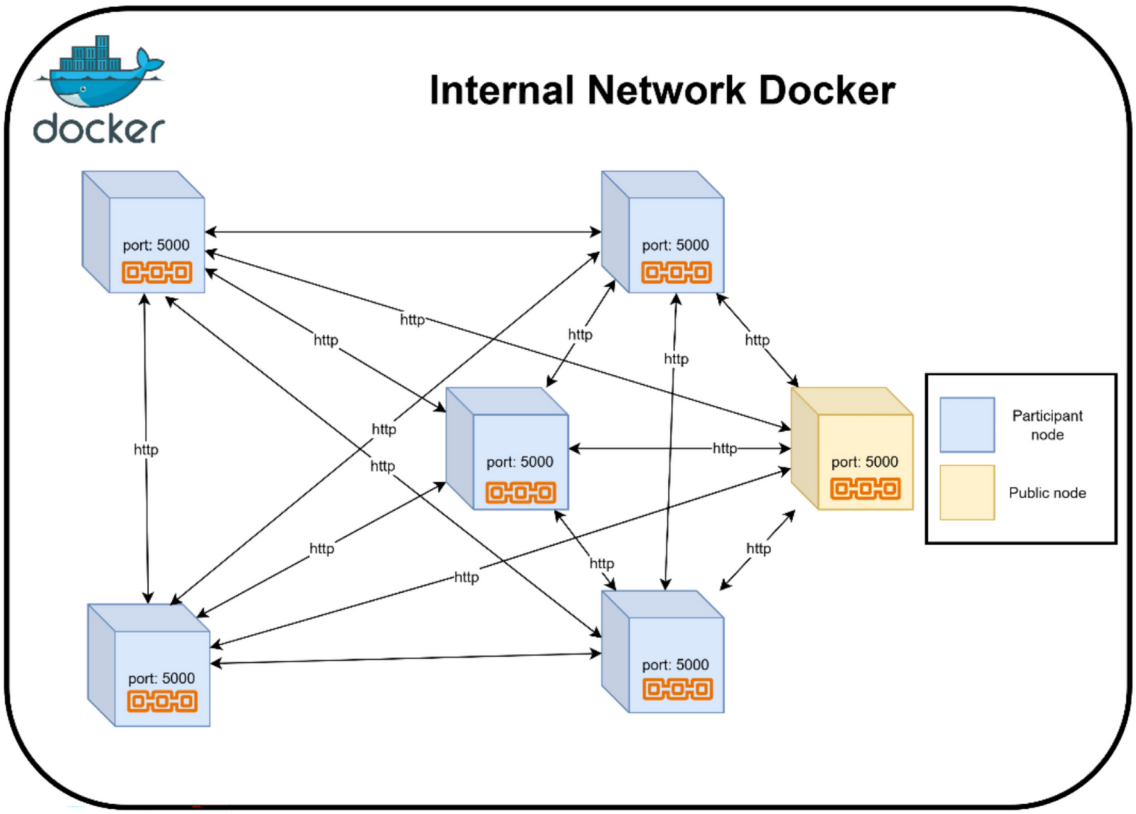

Fig. 2. Representation of communication between nodes (Docker containers) within the private Docker network.

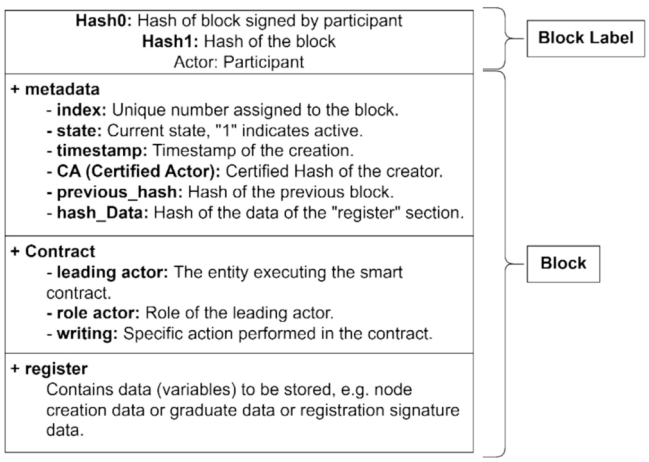

Fig. 3. Block structure.

image. Additionally, to access these nodes from outside the internal network, specific ports have been assigned on the VPS host, ranging from port 5000 to 5004, a detail also seen in Fig. 6. These ports are essential to enable external connectivity to the nodes.

Blockchain transactions view

In this second result, we observe the system's blockchain (Fig. 8), which follows the structure designed in the blockchain structure, as shown in Fig. 3. Each row of the table represents a block in the chain, showing key features such as the block number (index), which serves as a unique identifier for each record; the date and time (timestamp), which provides an unalterable chronological record; the hash of the block, a cryptographic identifier that ensures the integrity of the block data; and the hash of the previous block, which maintains the

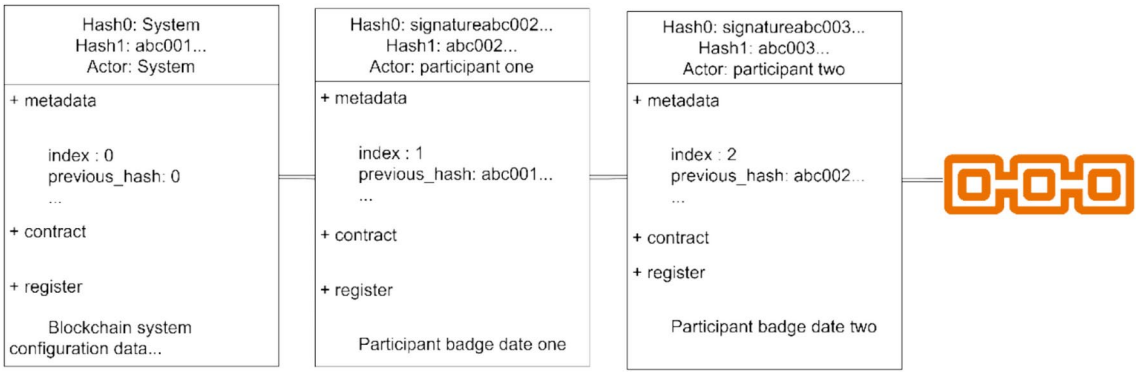

Fig. 4. Blokchain structure.

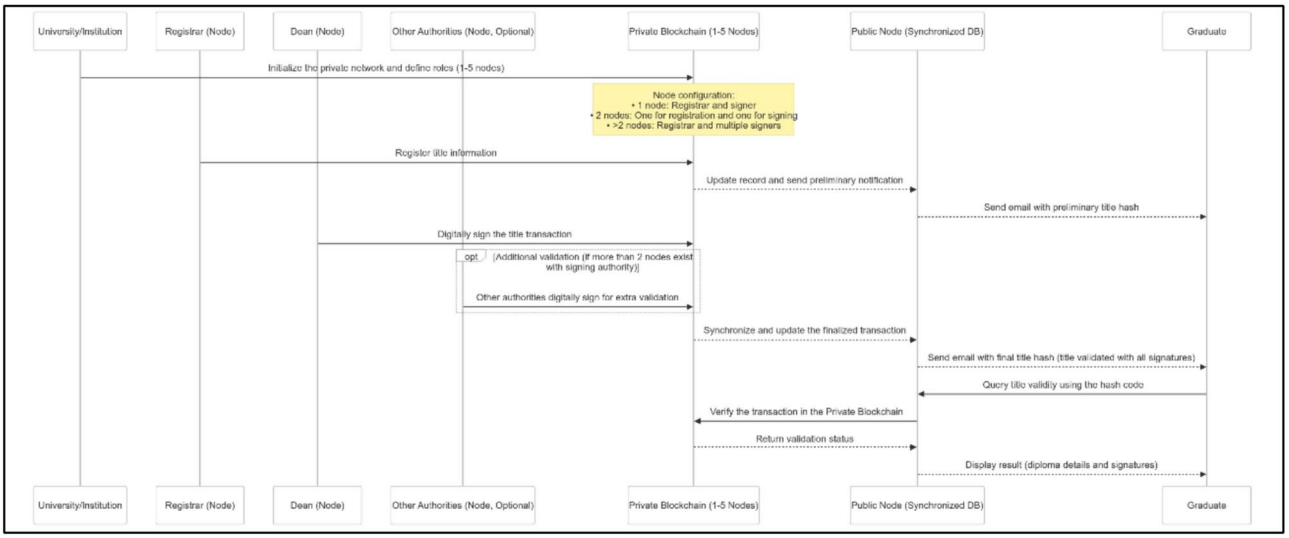

Fig. 5. Business Logic.

continuity and security of the entire blockchain by linking each block to its predecessor in an indissoluble manner.

Chain blocks

Figure 9 presents selected blocks from the blockchain, highlighting their structure and operation. Each block contains two main hashes: the block hash, which summarizes its total content, and the hash_Data, generated from the specific data stored. This design ensures the integrity and authenticity of the records. The genesis block establishes the foundations of the blockchain network, storing key information such as initial nodes and predefined functions, ensuring the initial configuration necessary for the operation of the system. From the genesis block, blocks tailored to different types of information are created, identified by their hash_Data. For example, the participant block records credentials and roles, such as "dean", processing the data to generate a unique hash in hash_Data. Similarly, the university degree record block contains data such as the graduate's name, academic degree and year of issue, generating a unique hash_Data that identifies the record.

The signature block relates existing records by means of the following elements: the professional title hash (card), which corresponds to the hash_Data of the block that stores the professional title; the signer hash (sign), which represents the hash_Data of the block that stores the signer's data; and the relation of both hashes, which links the title to the signer, ensuring its authenticity. In addition, this block includes complementary metadata, such as the signer's role and the date of signature, reinforcing traceability. This design ensures traceability and verifiability of records and signatures in the blockchain. Figure 8 illustrates how these elements interact to maintain system integrity.

Professional degree with integrated blockchain verification

The proposed system generates professional titles by providing them with an additional layer of security and authenticity through blockchain technology. This technology allows the titles to be publicly verifiable through a unique QR code and a query system based on the title hash. Figure 10 shows an example of the notification sent

```
ubuntu@vps-0219b6d7:~/bc/src/participant$ sh start.sh
c1e2f61daec14433cfd534fc3390eb23f195544785b841085d2cc408a01f9d5d
5000
Node 1 private completed...
2ecd6a56062b748538332c8abd216a54f6bcefce6c1cac269f8e568e979245bb
5001
Node 2 private completed...
db44d3863aff862ff17d8a7e9c48f469249e9fc51d78bbb3d64b8a174c511f5c
5002
Node 3 private completed...
96174b23cb1364c1a3f621f1be854074c0831ddb2c75ca7da1f9b3a89dd52efa
5003
Node 4 private completed...
5837e5f8ca9bbc20f88587e765f233568f87e772696c59bdff7422cd3d6442b7
5004
Node 5 private completed...
ubuntu@vps-0219b6d7:~/bc/src/participant$ cd ../public
ubuntu@vps-0219b6d7:~/bc/src/public$ sh start.sh
be6b765877c8aca3c8427eb94f1e48878f2cd20863da71ef836362997607861d
5005
public node realised...
ubuntu@vps-0219b6d7:~/bc/src/public$ docker ps
CONTAINER ID   IMAGE          COMMAND                  CREATED          STATUS          PORTS                                       NAMES
be6b765877c8   public-node    "python3 app/app.py"     3 seconds ago    Up 2 seconds    0.0.0.0:5005->5000/tcp, :::5005->5000/tcp   public
5837e5f8ca9b   private-node   "python3 app/link.py"    18 seconds ago   Up 17 seconds   0.0.0.0:5004->5000/tcp, :::5004->5000/tcp   node5
96174b23cb13   private-node   "python3 app/link.py"    19 seconds ago   Up 18 seconds   0.0.0.0:5003->5000/tcp, :::5003->5000/tcp   node4
db44d3863aff   private-node   "python3 app/link.py"    20 seconds ago   Up 19 seconds   0.0.0.0:5002->5000/tcp, :::5002->5000/tcp   node3
2ecd6a56062b   private-node   "python3 app/link.py"    21 seconds ago   Up 20 seconds   0.0.0.0:5001->5000/tcp, :::5001->5000/tcp   node2
c1e2f61daec1   private-node   "python3 app/link.py"    22 seconds ago   Up 21 seconds   0.0.0.0:5000->5000/tcp, :::5000->5000/tcp   node1
```

Fig. 6. Blockchain nodes with Docker.

```
ubuntu@vps-0219b6d7:~/bc/src/participantes$ docker network inspect bridge | jq '.[0].Containers'
{
  "34d095555c106e2bead86d0cc9b0a340eded2b48e11caf876126fba782b10c9a": {
    "Name": "node1",
    "EndpointID": "c78c069594ab5b5254c68144a6f3316395df5723f0805205b2b4e813a30dd636",
    "MacAddress": "02:42:ac:11:00:02",
    "IPv4Address": "172.17.0.2/16",
    "IPv6Address": ""
  },
  "b2f42a1d730e735a516861a5e540ddec0a964cdc37ac4030c7ba0833e0504115": {
    "Name": "node4",
    "EndpointID": "e4bd9622a75b62532ead685495eecab6369508a746f6c32af4b9947aeb057f57",
    "MacAddress": "02:42:ac:11:00:05",
    "IPv4Address": "172.17.0.5/16",
    "IPv6Address": ""
  },
  "d3b648c147813a7907a26469b2751bca5221e10ba58f679ee1273d38ed1899b1": {
    "Name": "node5",
    "EndpointID": "52ec679e65ad6904e72a07e9bc28803e49e9cade096ea3547f9cfa4ebb912303",
    "MacAddress": "02:42:ac:11:00:06",
    "IPv4Address": "172.17.0.6/16",
    "IPv6Address": ""
  },
  "e0e091887eb4f9eeb123031a2b7cb61836fe9e12fbf0e032c3893d9399d15483": {
    "Name": "node2",
    "EndpointID": "4e33ceb48040f01dea5ae836a848cace13e7a7701752881cf49c942af8bcb764",
    "MacAddress": "02:42:ac:11:00:03",
    "IPv4Address": "172.17.0.3/16",
    "IPv6Address": ""
  },
  "edacc131e8bfe66d166bb632498f39fae42a8d264c56a4c1183c4b04f857b193": {
    "Name": "node3",
    "EndpointID": "7c9f22be2b5b662a08fc97fc6cc4dd3a6a83e958ef7f90c678a03f3e22c45092",
    "MacAddress": "02:42:ac:11:00:04",
    "IPv4Address": "172.17.0.4/16",
    "IPv6Address": ""
  }
}
```

Fig. 7. Blockchain network with Docker.

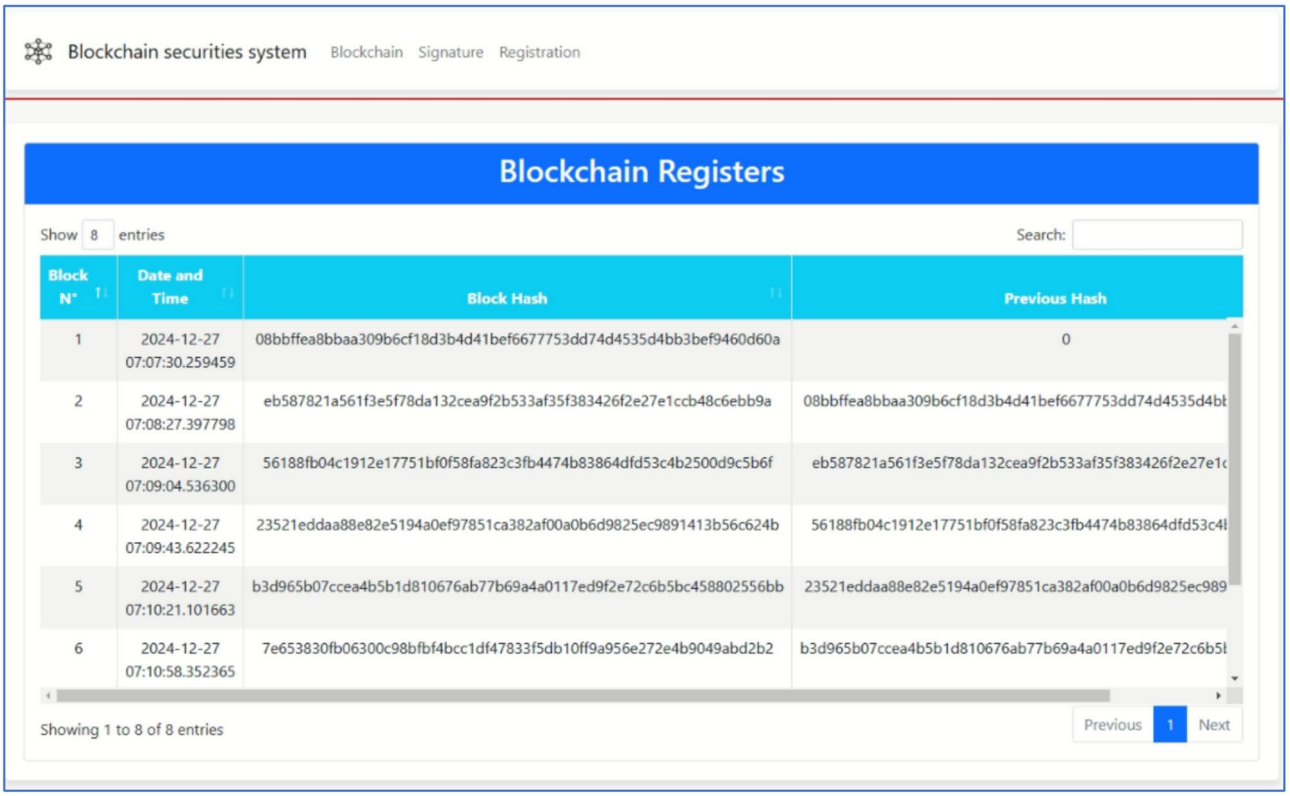

Fig. 8. Blockchain transactions view.

by email, while Fig. 11 exhibits an example of the professional degree issued, which includes the graduate's full name, the academic degree conferred and an embedded QR code. Such QR code is linked to the unique hash of the degree stored in the blockchain, allowing anyone to validate its authenticity by accessing the corresponding record through a link; in this example, the link is composed of the domain localhost (127.0.0.1), the port of the public node (5005) and the path /search, followed by the hash of the degree (e.g., http://127.0.0.1:5005/search/1091985483610fceb1694b107c53e1e0e17291176ca8d014e14f4e139ce6f381), showing the interface where the validated degree is presented (Fig. 12). In addition, Fig. 13 presents the blockchain query system interface, where users can enter the hash of the professional title to locate and verify the associated information, such as the date of issuance, the block in which it is registered and the previous hash of the chain, thus ensuring data traceability and corroborating that the title has not been altered since its issuance.

Performance evaluation

The performance of the developed blockchain system was evaluated by simulating processes in which a node registers 10 credentials and, in addition to registering, signs each of these credentials together with the other four nodes in the network (Table 1).

The performance evaluation, presented in Table 1, includes metrics such as latency, CPU usage and RAM consumption for each operation within the registration and signing processes. Although the average CPU usage appears as 0% for all operations evaluated, this value reflects the fact that the specific tasks of the prototype do not impose a significant load on the system processing resources.

This result can be explained by several factors, including the efficiency of the system design and the low level of computational complexity in the individual operations performed in the current prototype. For example, operations such as the processing of registration and signature interfaces are essentially lightweight transactions, which are not computationally intensive. In contrast, operations such as block replication and Byzantine consensus, which are fundamental to ensuring integrity and security in the blockchain, are optimized to run in a distributed manner, minimizing the impact on each individual node's processor.

In addition, it is important to note that this prototype is designed for testing in a controlled environment, which may differ from a deployment in a production system, where the CPU load could increase due to a higher number of concurrent transactions or a more complex infrastructure. Future iterations of the system will include stress scenarios and production simulations to evaluate how the CPU load evolves under different operating conditions.

Discussion

The first result demonstrates the successful deployment of a hybrid blockchain network composed of multiple dockerized nodes in a VPS environment. Each node operates independently, communicating through port

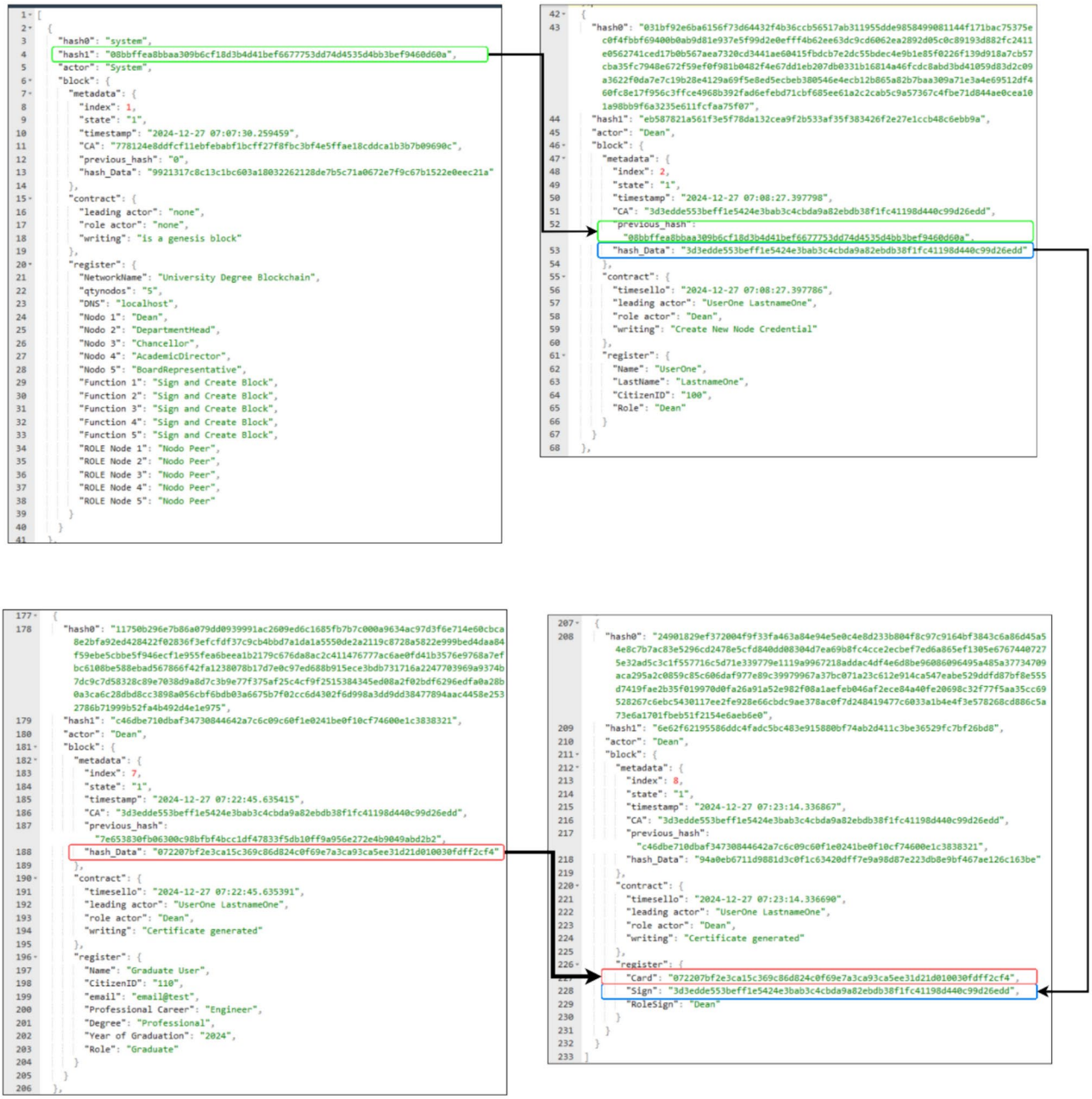

Fig. 9. Blocks of the chain.

5000 configured on the blockchain, achieving a P2P network and a distributed blockchain system[24]. highlighted improvements in scalability, agility and extensibility by developing a cloud network emulation platform with Docker. The use of Docker containers highlights improved performance and efficient approach compared to virtual machines[25]. Besides[26], highlights implementing blockchain in environments that simulate real situations for research, given that real networks are complex. This offers a valuable perspective for our study with blockchain in VPS, emphasizing the need for efficient and flexible tools in virtualized environments. Similarly, by having five restricted nodes for five users or entities and a sixth node dedicated to public queries, a scenario is configured in which, according to[27], private blockchains limit access exclusively to authorized nodes, enabling greater control and efficiency; on the other hand, public blockchains, being freely accessible, guarantee transparency, and consequently a hybrid blockchain is formed that integrates both approaches through a strategic combination of security and visibility.

The second result shows the blockchain successfully implemented, and only the indexes, timestamps, block hash and hash of the previous block are observed, but no further data is shown for each block, this is due to maintain the privacy of the other data, but making public the transactions performed over time. This resembles the information provided by stock exchanges, where details such as the time and volume of individual

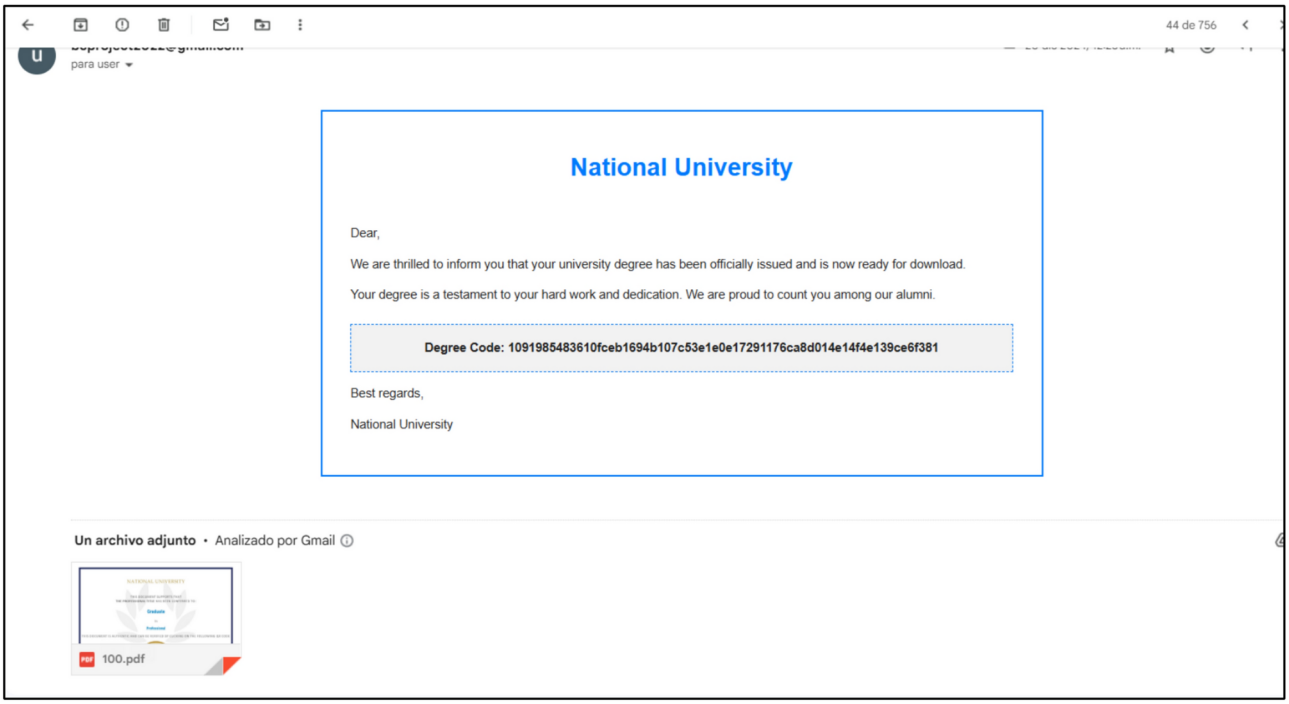

Fig. 10. Title notification via email.

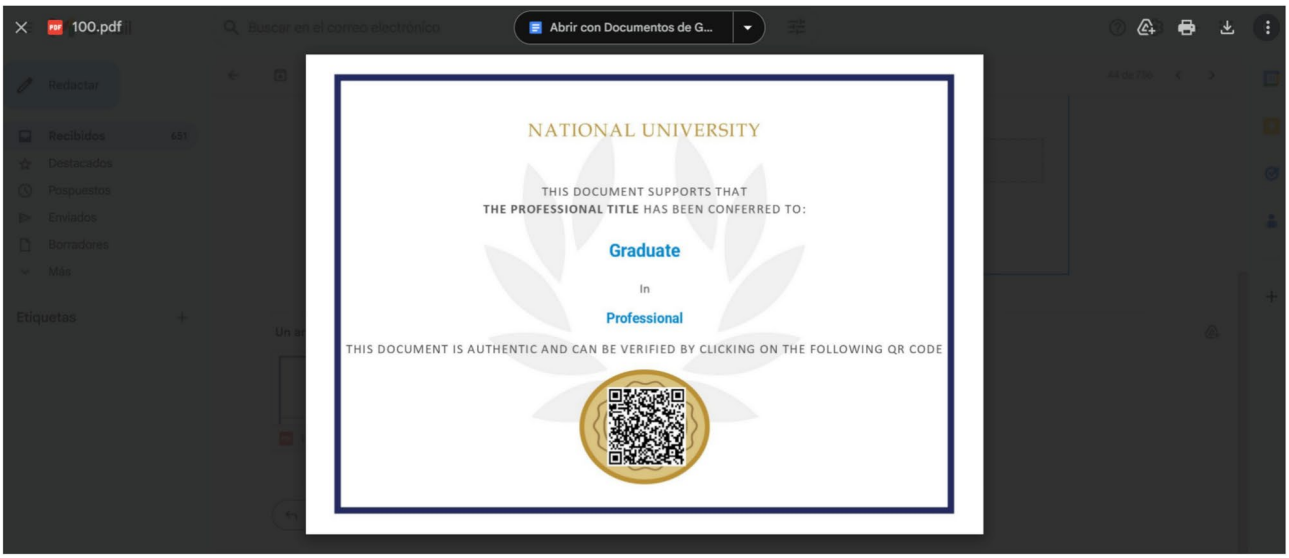

Fig. 11. Professional title with blockchain.

transactions, known as 'the tape', are publicly disclosed, although the identity of the parties involved is not disclosed[28]. In addition, anonymity and privacy on the blockchain is attractive to many IoT applications and services, especially those that need to maintain the confidentiality of identities and privacy[29–31] .

In the third result, specific blocks of a blockchain with a predefined structure are shown (Fig. 2). The initial block, known as the "genesis block," is linked to the next block through the hash of the previous block (Fig. 8). This hash is a unique identifier that is generated from the data of the previous block. The hash of the previous block ensures the integrity of the blockchain. If the content of a block is modified, the hash of the previous block is also modified, making the blockchain inconsistent and invalid[32] . Blocks seven and eight (Fig. 9) illustrate the recording and signing of data. In block seven, the 'record' section contains specific data, such as a college degree. This application underscores the utility of the blockchain as a distributed database, capable of storing information in an orderly and immutable manner[16,33]. On the other hand, the blockchain, noted for its decentralized ledger and robust security, emphasizes non-repudiation as a crucial aspect of its security[34]. In

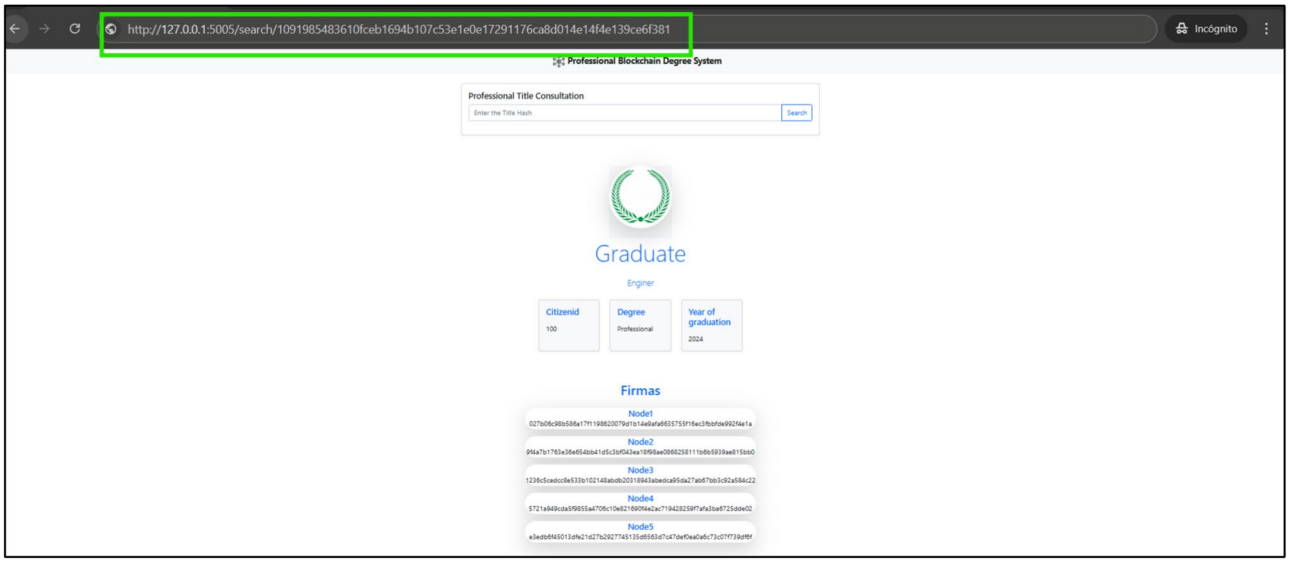

Fig. 12. Title in blockchain.

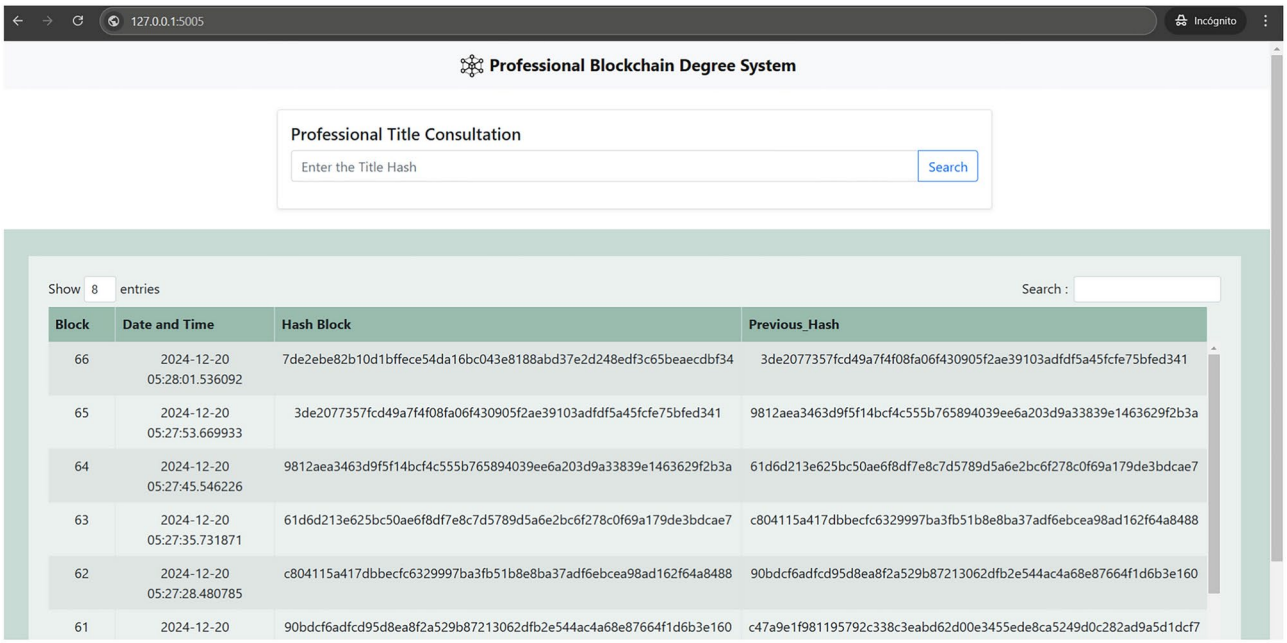

Fig. 13. Public Node.

Process	Operation	Average		
		Latency (Seg)	CPU (%)	RAM (bytes)
Register	Interface Processing Registration	0.00	0	1024.00
	Registration of securities on the blockchain	2.97	0	138,444.80
	Replicate blocks to all nodes	0.02	0	409.60
Firm	Interface Processing Signature	0.00	0	372.36
	Processing of the signature of the professional title registration on the blockchain	0.96	0	166,133.76
	Replicate blocks to all nodes	0.79	0	123,863.04
	Byzantine consensus	0.12	0	10,485.76

Table 1. Performance evaluation.

this context, the methodology implemented in block eight is aligned with the principles mentioned above. It not only allows for establishing a verifiable approval for the records in block seven, but also ensures the precise identification of the participant who makes the signature. Thus, it is guaranteed that the signer is valid and has the required authority, thus strengthening the integrity and trust that are inherent to the blockchain system.

The fourth result demonstrates the scope and effectiveness of a professional title supported by blockchain technology. This title can be verified by scanning an embedded QR code, which adds an additional layer of trust to the information supporting the document. In addition, the added value of this methodology is significant, as it considerably complicates the possibility of falsification of the title, both by internal and external agents to the institution. In addition, trust in professional relationships can be strengthened thanks to the benefits derived from the implementation of blockchain, such as security in data transfer, traceability, standardization of daily procedures, the promotion of a collaborative environment and the reduction of operating costs[35]. According to[36], this technology is key to protecting digital assets, allowing their use without fear of data loss and keeping them up to date at a reduced cost. According to[37], tedious credential verification processes highlight the need for an automated system powered by Blockchain technology, which reduces this time from days to seconds and minimizes the administrative burden.

The performance evaluation reflects significant efficiency in the operation of the blockchain system, with acceptable latency times and moderate resource usage. The results particularly highlight the low latency in block replication (0.02 s) and in the Byzantine consensus process (0.12 s), which is crucial for maintaining synchronization between nodes in distributed environments. The times obtained compare favorably with previous research. For example, a study by 36 reports higher latencies in blockchain systems designed for public networks, where consensus processes such as Proof of Work (PoW) can take several seconds or even minutes due to computational complexity. In contrast, the implementation presented here, based on a simplified consensus for private networks, significantly reduces these times. The use of Byzantine consensus in the developed system has proven to be efficient in validating transactions, achieving a time of 0.12 s per operation. According to[38], Byzantine fault-tolerant consensus algorithms such as Practical Byzantine Fault Tolerance (PBFT) are ideal for private networks, as they balance efficiency and security by avoiding the computational overhead typical of other mechanisms such as PoW. The system's resource consumption is low, allowing its implementation in infrastructures with hardware limitations. Compared to public systems based on Ethereum or Bitcoin, which require high CPU and RAM consumption due to intensive mining, this private system offers a scalable and efficient solution. Also[39] affirms the importance of efficiently managing resources in private blockchain networks. This is consistent with studies by[40], which highlight that efficient replication is a key indicator of reliability in distributed blockchain systems. Furthermore, the system's ability to handle multiple simultaneous transactions and signatures suggests that it is scalable for more complex applications or networks with a larger number of nodes.

Compared with recent schemes, PBAG introduces a privacy-preserving authentication protocol through updated global commitments, achieving efficiency and anonymity in IoV environments[41]. ESP2CS uses Ethereum as a middleware to enable secure communications and payments in IoV, standing out for real-time data editability[42]. Although this work is primarily aimed at title management, there are conceptual similarities with the PBAG and ESP2CS approaches, allowing for points of comparison despite the different application contexts. PBAG, designed for IoV environments, focuses on efficient authentication and privacy preservation in vehicular networks using blockchain. On the other hand, ESP2CS leverages Ethereum as middleware in IoT environments, standing out for enabling secure communications and payments, as well as providing real-time data editability. This paper adapts blockchain capabilities, such as smart contracts and authentication schemes, to the realm of securities management, addressing challenges such as traceability, authenticity and information integrity. Although the direct correlations with PBAG and ESP2CS may seem low, the work demonstrates how these technologies can be extended beyond their original applications, developing innovative solutions in a different domain. This underscores the flexibility and versatility of blockchain as a technological tool to solve speciDic problems in diverse contexts.

Proof-of-Learning, for its part, combines incentives based on game theory to encourage honest behavior and ensure collaborative security in decentralized networks[43]. The proposed model, designed for a private network with a public query node, prioritizes integrity and traceability by employing a mechanism based on the data hash, rather than the block hash. This ensures that data hashes remain confidential, while block hashes remain public to reinforce transparency. Associating an authority's signature with the full data hash eliminates the dependency on indexes or block hashes, allowing secure queries from the public node without compromising privacy or system reliability. This approach stands out as an efficient and robust solution for academic credential management, leveraging the stability of private networks with the accessibility of a public node.

Security analysis

The design of a blockchain system should not only focus on functionality and performance, but also on ensuring an adequate level of security to prevent vulnerabilities and mitigate potential risks. In this work, key security requirements have been integrated into the design of the scheme, with the objective of ensuring both secure operation and reliability of the proposed services. These aspects are detailed below.

To ensure confidentiality, robust cryptographic algorithms such as AES-256 are used to protect sensitive data and private keys used in authentication and transaction signing. This ensures that only authorized parties can access the information. In addition, encrypted transactions add an additional layer of protection, ensuring that data transmitted within the system is safeguarded from unauthorized access.

Data integrity is another key component of the scheme. For this purpose, cryptographic hash functions such as SHA-256 are used, which are collision resistant and allow any modification to the data to be detected. The system design ensures that each block in the chain includes the hash of the previous block, thus guaranteeing the

immutability of the stored information. This mechanism is reinforced by digital signatures that verify that the transactions have not been altered during transmission.

Authentication of network participants is performed by means of a scheme of public and private keys, using technologies such as ECDSA (Elliptic Curve Digital Signature Algorithm). This not only validates the identity of users, but also ensures that only legitimate entities can initiate transactions, minimizing the risk of fraudulent activity in the system.

In terms of availability, the design contemplates measures against denial-of-service (DDoS) attacks. This includes limiting the number of transactions processed per second, as well as implementing prioritization mechanisms based on commission rates. In addition, the system is designed in a distributed manner, replicating nodes to avoid single points of failure that could compromise its operation.

The scheme is also aligned with proactive security best practices. Regular audits and penetration tests are proposed to identify and mitigate vulnerabilities before they can be exploited. Additionally, the system integrates continuous monitoring that detects network anomalies, such as unauthorized transactions or coordinated attack attempts, enabling a rapid response to potential incidents.

Limitations and future work

The model is in the early prototype phase; for this reason, limitations in terms of scalability, robustness, login access to the use of the system are acknowledged. Despite these limitations, looking ahead, it is hoped that this initial work can act as a catalyst for subsequent research into blockchain credential management systems, providing a concrete starting point for the refinement and expansion of the model.

Conclusions

This work sets a precedent for the implementation of blockchain in academic credentials, combining Python and Docker to offer a secure, scalable and accessible system. The proposed block structure proves to be versatile, with potential applicability in a variety of services. On the other hand, the signature-by-association mechanism, or seal of authority, emerges as an effective methodology for the authentication of academic records, with potential extension to other credential systems. Furthermore, the integration of QR codes adds an essential layer of security and accessibility, positioning this solution as a replicable model in various academic institutions.

Data availability

The data will be made available on request to the corresponding author.

Received: 1 July 2024; Accepted: 10 March 2025
Published online: 18 March 2025

References

1. Ramos M, Pacheco A. Towards inventory control excellence: An innovative approach based on a web-based platform [Internet]. [cited 2023 Aug 20]. Available from: https://github.com/mmartinrm97/api-sepulveda/commits/1.0 (2021)
2. Newton, P. J. et al. Magnetisation configuration in arrays of permalloy rectangles and its impact on magnetisation reversal. *Mater. Res. Express* https://doi.org/10.1088/2053-1591/ac2442 (2021).
3. Zheng, K. et al. Blockchain technology for enterprise credit information sharing in supply chain finance. *J. Innov. Knowl.* **7**(4), 100256 (2022).
4. Gad, A. G., Mosa, D. T., Abualigah, L. & Abohany, A. A. Emerging trends in blockchain technology and applications: A review and outlook. *J. King Saud Univ. Comput. Inf. Sci.* **34**(9), 6719–6742 (2022).
5. Arteaga-Mendoza KS, Muñoz-Vera HR, Ortega-Medranda WM, Ballesteros-Navarrete RF. El impacto de la tecnologia blockchain y sus diversas ventajas aplicadas en America Latina. Memorias del V Congreso Internacional de Ciencias Administrativas y Economicas [Internet]. [cited 2023 Mar 21];151–70. Available from: https://munayi.uleam.edu.ec/wp-content/uploads/2019/10/MEMORIAS-DEL-V-CICAE.pdf#page=152 (2020)
6. Uribe-Hernandez, Y., Polo-Nicacio, M., Cardenas-Solis, A. & Pacheco-Pumaleque, A. Internal control automatic physical distance detection system for patient care against a possible COVID-19 infection within a health center. *Int. J. Recent Innov. Tr. Comput. Commun.* https://doi.org/10.17762/ijritcc.v11i4.6377 (2023).
7. Franco-Correa JD. Analisis de la seguridad blockchain en herramientas E-learning para el proceso de educacion continua de la Carrera de Ingenieria en Telematica [Internet]. [Guayaquil]: Tesis de Pregrado, Universidad de Guayaquil; [cited 2023 Mar 23]. Available from: http://repositorio.ug.edu.ec/handle/redug/46723 (2019)
8. Molina-Guzmán, A. Funcionamiento y gobernanza del Sistema Nacional de Salud del Ecuador. *Íconos Revista de Ciencias Sociales* https://doi.org/10.17141/iconos.63.2019.3070 (2019).
9. Pacheco-Jiménez, M. N. De la tecnología blockchain a la economía del token. *Derecho PUCP* https://doi.org/10.18800/derechopucp.201902.003 (2019).
10. Taufiq R, Trisetyarso A, Meyliana, Kosala R, Ranti B, Supangkat S, et al. Robust Crypto-Governance Graduate Document Storage and Fraud Avoidance Certificate in Indonesian Private University. Proceedings of 2019 International Conference on Information Management and Technology, ICIMTech 2019. 1(August):339–44 (2019)
11 Ali, S. I. M. & Sharaf, H. M. Using blockchain in university management systems. *Turk. J. Comput. Math. Educ. (TURCOMAT)* https://doi.org/10.17762/turcomat.v12i2.2389 (2021).
12. Seng VLK, Wan AT, Venkat I, Patchmuthu RK, Ali SHM. Blockchain technology in securing academic credentials: Mobile QR block CV. AIP Conf Proc [Internet]. Nov 20 [cited 2023 Dec 6];2968(1):040004. Available from: /aip/acp/article/2968/1/040004/2922341/Blockchain-technology-in-securing-academic (2023)
13 Mata-Hernández, J. M. & Avendaño-Cruz, S. Blockchain en la educación: su uso en credenciales académicas. *Revista Digital Universitaria* https://doi.org/10.22201/cuaieed.16076079e.2022.23.1.1 (2022).
14 López-Jiménez, D. Blockchain: Aspectos tecnolígicos empresariales y legales. *PAAKAT: Revista de tecnología y sociedad* https://doi.org/10.32870/Pk.a10n18.421 (2020).
15. Aparco-Fernandez RV, Canchaya-Esteban JA, Murillo-Garcia AS, Robles-Luna AJ. Modelo de Implementación del Proceso de Emisión de Grados y Títulos Digitales mediante el uso de la Tecnología Blockchain en Universidades de Lima Metropolitana. Universidad ESAN; (2021)
16 Zevallos-Umpiri, W. Blockchain y la innovación en las tecnologías. *TecnoHumanismo.* **2**(2), 117–125 (2022).

17. Anthony Jahir López Coello AYPCREZMBOB. Blockchain: Medio de seguridad, reducción de costos e identificación de errores para organizaciones ecuatorianas. Revista de Ciencias Sociales (Ve) [Internet]. [cited 2023 Dec 7];27(3). Available from: https://www.redalyc.org/journal/280/28068276019/28068276019.pdf (2021)
18 Fahlevi, M., Saparudin, M., Maemunah, S., Irma, D. & Ekhsan, M. Cybercrime business digital in Indonesia. *E3S Web of Conferences* https://doi.org/10.1051/e3sconf/201912521001 (2019).
19 Chen, G., Xu, B., Lu, M. & Chen, N. S. Exploring blockchain technology and its potential applications for education. *Smart Learn. Environ.* https://doi.org/10.1186/s40561-017-0050-x (2018).
20. Cardenas M. horus100/Llapa-Yachay: Version 1.0.0. Zenodo [Internet]. [cited 2024 Dec 29]; Available from: https://zenodo.org/records/14575523 (2024)
21. Baran, P. On distributed communications networks. *IEEE Trans. Commun. Syst.* **12**(1), 1–9 (1964).
22. Díaz, Y. & Cueva, J. Análisis de la función Hash Criptográfica en cadenas de bloques y su impacto en la seguridad de transacciones de datos. *Redes de Ingeniería* https://doi.org/10.14483/2248762X.14383 (2018).
23. Dolader-Retamal, C., Bel-Roig, J. & Muñoz-Tapia, J. L. La blockchain: Fundamentos, aplicaciones y relación con otras tecnologías disruptivas. *Economía industrial.* **405**, 33–40 (2017).
24 Lai, J., Tian, J., Zhang, K., Yang, Z. & Jiang, D. Network emulation as a service (NEaaS): Towards a cloud-based network emulation platform. *Mobile Netw. Appl.* **26**(2), 766–780. https://doi.org/10.1007/s11036-019-01426-0 (2020).
25 Liu, B. et al. A new container scheduling algorithm based on multi-objective optimization. *Soft comput.* https://doi.org/10.1007/s00500-018-3403-7 (2018).
26. Gill S, Lee B, Qiao Y. Containerchain: A Blockchain System Emulator based on Mininet and Containers. Proceedings - 2021 IEEE International Conference on Blockchain, Blockchain. 2021;484–90 (2021)
27. Paul, P., Aithal, P. S., Saavedra, R. & Ghosh, S. Blockchain technology and Its types—A short review. *Int. J. Appl. Sci. Eng.* **9**(2), 189–200 (2021).
28. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. [cited 2023 Dec 8]; Available from: www.bitcoin.org (2008)
29. Kus Khalilov, M. C. & Levi, A. A survey on anonymity and privacy in bitcoin-like digital cash systems. *IEEE Commun. Surv. Tutorials.* **20**(3), 2543–2585 (2018).
30. Wang, X. et al. Survey on blockchain for Internet of Things. *Comput. Commun.* **1**(136), 10–29 (2019).
31. Zha X, Zheng K, Zhang D. Anti-pollution source location privacy preserving scheme in wireless sensor networks. 13th Annual IEEE International Conference on Sensing, Communication, and Networking, SECON 2016. 2016 Nov 2;(2016)
32. Nguyen LT, Duc Nguyen L, Hoang T, Bandara D, Wang Q, Lu Q, et al. Blockchain-Empowered Trustworthy Data Sharing: Fundamentals, Applications, and Challenges. Mar 12 [cited 2023 Dec 10]; Available from: https://arxiv.org/abs/2303.06546v1 (2023)
33. Dolader, C., Joan, R., Roig, B., Luís, J. & Tapia, M. La blockchain: fundamentos, aplicaciones y relación con otras tecnologías disruptivas. *Economía industrial* **405**, 33–40 (2017).
34 Fang, W. et al. 2020 Digital signature scheme for information non-repudiation in blockchain: A state of the art review. *EURASIP J. Wirel. Commun. Netw.* **1**, 1–15. https://doi.org/10.1186/s13638-020-01665-w (2020).
35 Rodrigues-dos-Santos-Ramos, C. & Queiroz, M. M. Blockchain in education: The influence of trust on adoption and implementation. *RAUSP Manag. J.* **57**(3), 316 (2022).
36. Pathak S, Gupta V, Malsa N, Ghosh A, Shaw RN. 2022 Blockchain-Based Academic Certificate Verification System—A Review. Lecture Notes in Electrical Engineering [Internet]. [cited 2023 Dec 10];914:527–39. Available from: https://doi.org/10.1007/978-981-19-2980-9_42 (2022)
37. Gaikwad H, D'Souza N, Gupta R, Tripathy AK. A Blockchain-Based Verification System for Academic Certificates. 2021 International Conference on System, Computation, Automation and Networking, ICSCAN. 2021 Jul 30 (2021)
38. Cachin C, Vukolić M. Blockchain Consensus Protocols in the Wild. Leibniz International Proceedings in Informatics, LIPIcs [Internet]. Jul 6 [cited 2024 Dec 28];91. Available from: https://arxiv.org/abs/1707.01873v2 (2017)
39. Riahi K, Brahmia MEA, Abouaissa A, Idoumghar L. APBFT: An Adaptive PBFT Consensus for Private Blockchains. Proceedings - IEEE Global Communications Conference, GLOBECOM. 1788–93 (2022)
40. Li, X., Jiang, P., Chen, T., Luo, X. & Wen, Q. A survey on the security of blockchain systems. *Futur. Gener. Comput. Syst.* **1**(107), 841–853 (2020).
41. Feng X, Cui K, Wang L, Liu Z, Ma J. PBAG: A Privacy-Preserving Blockchain-based Authentication Protocol with Global-updated Commitment in IoV. IEEE Transactions on Intelligent Transportation Systems [Internet]. Aug 31 [cited 2024 Dec 29]; Available from: https://arxiv.org/abs/2208.14616v1 (2022)
42. Jabbar R, Kharbeche M. ESP2CS: Securing Internet of Vehicles through Blockchain-enabled Communications and Payments. Dec 5 [cited 2024 Dec 29]; Available from: https://arxiv.org/abs/2312.02589v1 (2023)
43. Zhao Z, Fang Z, Wang X, Chen X, Zhou Y. Proof-of-Learning with Incentive Security. Apr 13 [cited 2024 Dec 29]; Available from: https://arxiv.org/abs/2404.09005v6 (2024)

Acknowledgements

This work was supported by the Vice-Presidency of Research of the Universidad Nacional de Cañete UNDC in the framework of the "II Thesis Project Grant Competition 2022, for Students and Graduates of the Universidad Nacional de Cañete" [contract number 011-2022-UNDC/CO/P/DGA].

Author contributions

A.P. wrote the main manuscript text and M.A.C.Q created the software and collected the data. All authors reviewed the manuscript.

Funding

Universidad Nacional de Cañete, 15478,15478.

Declarations

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to A.P.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Open Access This article is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License, which permits any non-commercial use, sharing, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if you modified the licensed material. You do not have permission under this licence to share adapted material derived from this article or parts of it. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by-nc-nd/4.0/.

© The Author(s) 2025, corrected publication 2025