POLITECNICO DI TORINO
Repository ISTITUZIONALE

An Architecture for Biometric Electronic Identification Document System Based on Blockchain †

Original
An Architecture for Biometric Electronic Identification Document System Based on Blockchain † / Páez, Rafael; Pérez, Manuel; Ramírez, Gustavo; Montes, Juan; Bouvarel, Lucas. - In: FUTURE INTERNET. - ISSN 1999-5903. - ELETTRONICO. - 12:1(2020), p. 10. [10.3390/fi12010010]

Availability:
This version is available at: 11583/2788889 since: 2020-02-03T21:11:44Z

Publisher:
MDPI

Published
DOI:10.3390/fi12010010

Terms of use:
openAccess

This article is made available under terms and conditions as specified in the corresponding bibliographic description in the repository

Publisher copyright

(Article begins on next page)

16 October 2021

future internet

MDPI

Article

An Architecture for Biometric Electronic Identification Document System Based on Blockchain †

Rafael Páez [1,‡], Manuel Pérez [2,*,‡], Gustavo Ramírez [2,‡], Juan Montes [2] and Lucas Bouvarel [1]

[1] Department of Computer Science Engineering, Pontificia Universidad Javeriana, Bogotá D.C. 110231, Colombia; paez-r@javeriana.edu.co (R.P.); lucas.bouvarel@gmail.com (L.B.)

[2] Department of Electronics Engineering, Pontificia Universidad Javeriana, Bogotá D.C. 110231, Colombia; ramirez.g@javeriana.edu.co (G.R.); juan-montes@javeriana.edu.co (J.M.)

* Correspondence: manuel.perez@javeriana.edu.co; Tel.: +57-1-3208320 (ext. 5344)

† This paper is an extended version of the paper entitled "Consensus Algorithm for a Private Blockchain", presented at 2019 IEEE 9th International Conference on Electronics Information and Emergency Communication (ICEIEC), Beijing, China, 12–14 July 2019.

‡ These authors contributed equally to this work.

Received: 19 December 2019; Accepted: 9 January 2020; Published: 11 January 2020

Abstract: This paper proposes an architecture for biometric electronic identification document (e-ID) system based on Blockchain for citizens identity verification in transactions corresponding to the notary, registration, tax declaration and payment, basic health services and registration of economic activities, among others. To validate the user authentication, a biometric e-ID system is used to avoid spoofing and related attacks. Also, to validate the document a digital certificate is used with the corresponding public and private key for each citizen by using a user's PIN. The proposed transaction validation process was implemented on a Blockchain system in order to record and verify the transactions made by all citizens registered in the electoral census, which guarantees security, integrity, scalability, traceability, and no-ambiguity. Additionally, a Blockchain network architecture is presented in a distributed and decentralized way including all the nodes of the network, database and government entities such as national register and notary offices. The results of the application of a new consensus algorithm to our Blockchain network are also presented showing mining time, memory and CPU usage when the number of transactions scales up.

Keywords: biometric systems; identification technologies; authentication; smart government; electronic identity document (e-ID); Blockchain technology (BCT)

1. Introduction

Nowadays the high penetration of information and communication technologies (ICT) in our daily lives has led to a new paradigm of how people should live in modern societies. In addition, with the growing attention about technology application on governmental processes, governments have focused their politics on the implementation of a novel concept known as electronic Government. Different works have defined the e-Government as an ICT application strategy oriented to improve public services with the goal of increasing the government's interaction with its citizens, employees or any internal entity to ensure efficiency and effectiveness within the government or with other governments [1].

The definition of e-Government includes four main aspects: (i) Government to Citizen (G2C), (ii) Government to Company (G2B), (iii) Government to Employee (G2E) and (iv) Government to Government (G2G) [1]. One of the features of e-Government is, in particular, the ability to use ICT for registration and identification of its citizens. It is worth to clarify that the concept of identification

in our work is to recognize if a person or thing is the same that is supposed or sought. In Latin American countries, for example, it is necessary to conduct a registration process, which at the same time represents the constitutional right that a citizen has of being individualized by the state from the moment of its birth [2]. The official registration process ends with the delivery of the identity document (ID) that uniquely identifies a citizen in the database of the government registry office [3]. The data stored in the ID are normally the photo of the carrier, the name, date of birth, and other personal information. This identification itself works as a verification test of personal identity. However, due to the current advance of technology, a novel concept of Electronic Identity Document (e-ID) has appeared, which mainly consists in generating the same ID in a smart card where the data of the carrier can be stored digitally including new features such as facial and fingerprint information for recognition, in addition, it includes more complex security measures by means of encryption of personal information giving access to online services for citizens [4]. Additionally, we argue that blockchain technology (BCT) currently represents a great opportunity to provide solutions to several public problems, in particular, those related to corruption. That is to say, BCT application in government will have a remarkable impact in scenarios where government transparency is requested by its citizens such is the case of public data management, electronic voting, taxing, among others. Nowadays, the national ID used in many countries presents security problems where the authorities have registered thousands of lost documents that can generate cases of identity theft. In other situations, there have been cases in which criminals clone documents of people to avoid authorities and commit fraud and also cases of lost or stolen identification used by criminals to falsify the identities of people in order to obtain bank loans or sell their properties [5]. Considering the vulnerabilities and security threats that national ID systems have particularly when making transactions, there is a clear gap for the implementation of ICT technologies to track and validate transactions. Certainly, the blockchain network combined with the authentication and user identification processes could be applied to overcome the aforementioned problems. In the context of the ID, user authentication is the process to verify and validate the relationship between the document and its owner. This process is based on the concept of strong authentication defined on three factors: something the person has (a card), something the person knows (a PIN) and something the person is or does (its fingerprint or signature) [6]. The combination of those factors generates a more secure or strong authentication for the identification of the person itself.

The goal of this paper is to propose an architecture to manage transactions using biometry in a national electronic identity document (e-ID) system. The proposed architecture is based on Blockchain for transaction validation, smart cards, and biometric user authentication. Our hypothesis is to validate BCT functionalities into common government transactions, improving security measures for user authentication by including fingerprint and iris recognition information into a smart card. Therefore, the contributions of this paper are listed as follows:

- A Blockchain network architecture proposal for a national e-ID system with iris and fingerprint recognition features.
- A fingerprint and iris recognition set up for the proposed e-ID system.
- The design, implementation, and validation of a Blockchain network for the proposed e-ID system through a new consensus method called tournament consensus algorithm (TCA).

This paper is organized as follows. Section 2 presents definitions and related work about Blockchain generalities including security problems, architectures, and applications. Section 3, gives some definitions about current document and user authentication methods. Section 4, presents the proposed e-ID system including the Blockchain architecture using biometric user information. Section 5, presents a brief review of consensus algorithms for Blockchain network evaluation. Section 6, presents the performance results of the implemented system. Finally, Section 7, presents the conclusions, remarks and future work.

2. Related Work

BCT is based on the idea of a decentralized ledger that cannot be altered or modified, where consensus is required from all members of the network and all validated transactions are recorded. This technology is characterized by providing decentralization, integrity, reliability, traceability of information and non-repudiation by users. These functions provide benefits in different areas, such as the veracity of the transactions [7]. All the participant nodes in a Blockchain have access to the information registered at any time, in this way, if a node is being attacked, the other members of the network could detect it and reject the fake block avoiding fraudulent transactions [8,9].

Although BCT has been presented as a promising technology for safe transactions, several security problems on BCT have been analyzed, as for example [10,11]:

- *Selfish Mining Attack*, in order to obtain undue rewards or wasting power from honest miners [12,13].
- Decentralized autonomous organization (DAO) attack [14]: it is deployed on a smart contract platform, using it as malicious smart contract.
- Border gateway protocol (BGP) hijacking attack [15]: the purpose is to rerouting traffic to a mining pool controlled by the attacker and subsequently steal cryptocurrencies.
- Eclipse attack [16,17]: this attack permits to control all the victim's connections isolating him from the other peers. Moreover, this attack works as a base for other attacks.
- Liveness attack [18]: it permits to delay the confirmation time of a determined transaction and in some BCT the transaction will be regarded valid. Then, the attacker could continue building a private blockchain to incorporate the blocks in the public blockchain.
- Balance attack [19]: this attack works to BCT using the proof of work (PoW) consensus algorithm and allows double-spending.

Other security problems but focused on the internet of entities (IoE) are analyzed in [20] where mobile networks and internet of things are integrated to offer services and they propose a Blockchain paradigm to secure this environment. Likewise, Huang et al. [21] propose a decentralized solution based on blockchain for IoT in order to data exchange in a trusted way, providing an architecture using Ethereum and smart contracts.

Although Blockchain-based applications are springing up, covering numerous fields including financial services, reputation system and more recently Internet of Things (IoT), currently, few works have been carried on Blockchain architectures for government issues and to the best of the authors knowledge, there have not been architecture proposals to manage citizens authentication with the combined use of smart cards and biometry technology. Considering the aforementioned, Estonia leads the Blockchain adoption, deploying systems for an e-Government. Since 2012, the Blockchain has been operational in health, judicial, legislative, security and commercial codes systems, with plans to extend its use to other areas, such as medicine, cybersecurity, and embassy data. Moreover, since 2014 Estonia launched the e-residency program which allows non-Estonian access to services like the previously mentioned [22].

In [20], biometry is proposed to secure digital identity models and to be used in smart devices. In these devices is important to identify in a unique way to the user in order to provide the corresponding service and the biometry is a suitable technology to do it and we combine BCT to secure biometry features keeping them in the blockchain to avoid spoofing or other related attacks. In [23] the author states that BCT will bring several benefits to the users and developers of biometric systems to achieve better security, scalability, and privacy, so both technologies complement each other in terms of security.

3. Authentication Methods

3.1. Document Authentication

These methods verify and validate the authenticity of the document. In this paper, the five most used types of document authentication methods are briefly reviewed: changeable laser image, holograms, watermarking, one-way functions and protocols.

3.1.1. A Changeable Laser Image (CLI)

CLI is a mechanical and visual method that consists of a laser drilling from different angles making an image that changes depending on the viewing angle. The main advantages of laser marking are its long-lasting feature and tamper-proof. For example, the national identity document in Spain use CLI with the photo and the expedition date to authenticate the document [24].

3.1.2. Holograms

Other mechanical and visual methods for document authentication are based on *holography* where mainly optical variable ink (OVI), orlas, guilloch 3D, microtext, kinegram, reliefs, tactile letters, ultraviolet and infrared Inks, and OCR-B (OCR-B is a monospace font developed in 1968 which includes ASCII symbols, and other symbols needed in the bank environment. It is widely used for the human readable digits in Universal Product Code (UPC) barcodes) characters are used. Authors in [25] defines a hologram as a three-dimensional image reproduced from an interference pattern recorded by coherent light beams, this image reproduce different figures by means of movement or the simple reflection of light. Recently the work in [26], has extended the concept of holograms by proposing a digital holography (DH) system for authentication using a charged-coupled device (CCD) camera and a numerical 3D image reconstruction.

3.1.3. Watermarking Methods

Methods which consist of hidden information embedded in watermarks, this method involves inserting a message, hidden or not, inside a digital object (images, audio, video, text, software) to verify the legitimacy of the document. These marks can be classified as (i) visual, hidden marks only visible to the human eye with light reflection. (ii) Static software watermarking (data and code), (iii) dynamic software watermarking (data structures and execution trace) [27].

3.1.4. One-Way Functions

Functions which refer to software methods, they are a type of functions which are easy to obtain but hard to invert, which from a data (or file) with an arbitrary length, generate a fixed-length string. If a single character or bit (or file property) is modified, the string changes significantly. In this way, it is possible to provide information integrity. Some examples of those methods are hash algorithms (SHA-1, SHA-2, and SHA-3) or the cryptographic hash functions (MAC).

3.1.5. Document Authentication Protocols

These are methods used to address security issues within open networks, where it is intended to verify the authenticity of the connection nodes, as the first and most important line of defense in a system of trusted and open networks [28]. The most used protocols are secure sockets layer (TLS/SSL), the IP authentication header (IP SEC), secure shell (SSH) and Kerberos.

In summary, for national identification document systems, mechanical and visual methods are the most used for document authentication, more specifically the use of CLI in conjunction with different types of holograms is incorporated. Nevertheless, as is explained in [29], these types of methods are static and predefined, making them vulnerable to duplicity or counterfeits threats. This is to say, for national identification document systems, there still are challenges in terms of security, particularly

from the implementation point of view when combined with different document, user and transaction authentication methods.

3.2. User Authentication

These methods consist of the verification and validation of the relationship between the document and the owner. As defined in [6], we consider in this paper, three common factors used for authentication: (i) something that the user is or does, as for example biometric characteristics and behavioral characteristics, (ii) something that user knows, such as PIN, passwords, one-time password (OTP) and (iii) something that the user has, like for example public-key cryptography (PKC) technologies.

Authentication based on *something that the user is or does* factor represents mainly all kinds of biometric technologies. These are all sensors and technologies that allow the acquisition of unique biometric characteristics of the people. Authors in [30] explains how biometrics technologies are used for automatic personal recognition based on two types of biometric characteristics: First, the biological traits like fingerprint, face recognition, palm print, hand geometry or eye iris. Secondly, the behavioral characteristics like gait, signature, voice or typing pattern.

The work in [31] shows how a biometric system works. Even though nowadays there are several biometric technologies, not all of them are fully developed, for this reason in this paper, the most used ones are described [32].

3.2.1. Fingerprint Recognition System

Biometric fingerprint-based recognition is the oldest method and one of the most developed. As presented in [33], there are different types of readers, such as optical, capacitive, ultrasonic and thermal for the digitization of the fingerprint characteristics. In general, a reader acquires and recognizes the fingerprint pattern, called minutiae, and additional features like for example body temperature. As explains in [31], a minutiae contains the information about bifurcations, ridge endings, dots, core and delta points of the fingerprint. A fingerprint reader acquires a numerous quantity of minutiae to be compared with the minutiae stored, generating a numerical result that represents the probability of a match between the captured and the stored fingerprint. The system can be more robust depending on the number of minutiae acquired. The advantages of the fingerprint systems among others are distinctiveness or uniqueness, permanence and performance in terms of accuracy, speed, and robustness [34]. However it has also some disadvantages like lack of universality when people do not have a fingerprint because of some accident, acceptability and circumvention because of easily imitation using an artifact or a substitute.

3.2.2. Face Recognition System

Biometric face-based recognition systems seek for facial features and require a digital camera to digitize the user's facial image for authentication [31]. The face recognition method is usually passive, since it does not require people cooperation to look into a scanner. This system is capable of capturing face images from a distance using a video camera, and through a face recognition algorithm, process the captured data for detecting, tracking and finally recognizing people. Face recognition involves computer recognition of personal identity based on geometric or statistical features derived from face images [35].

3.2.3. Iris Recognition System

Biometric iris-based recognition systems involve analyzing features found in the colored tissue ring of the iris [31]. The iris scanning undoubtedly is the less invasive of the eye biometrics technologies, it uses a conventional camera element and requires no close contact between the user and the scanner. In addition, it has the potential for higher than average matching performance. For this reason, iris biometrics work well in identification mode [35].

Authentication based on *something that the user knows* factor is mainly related to passwords or PINs known by people.

3.2.4. The Password

A password consists of a word or string of characters that are used for a user to prove its identity and must be kept in secret. There are common methods used by attackers to obtain a password, named as follows: guessing, dictionary, brute force and rainbow tables [36].

3.2.5. A Personal Identification Number (PIN)

A PIN is a numeric password used to authenticate a user into a system. The PIN is not printed or embedded on the card but is manually entered by the user [37].

3.2.6. One-Time Password (OTP)

OTP is an evolution of the password authentication which minimize replay and brute force attacks. It provides a one-time valid password to authenticate in a computing system, next access will require the generation of another OTP. In this way, a man in the middle (MitM) attack will have few possibilities of success.

3.2.7. Zero-Knowledge Proofs (ZKP)

Another alternative of authentication solution based on this kind of method is the ZPK, which allows a user to prove against a verifier that a statement is true, without revealing any information (Secret, procedure, etc). Financial entities use this method, asking in a random way, to their customers about different personal questions that were previously set by them [38].

The last authentication methods are based on *something that the user has* factor, which is mainly related to Public Key Infrastructure (PKI) which involves three entities: a client, a server and a certification authority. The certification authority is a trusted source that ensures the identity of the parts that are communicating, in addition, it also manages these certificates to ensure that they are all valid. The public key cryptography (PKC) generates two keys [39]. One key is known as the private key and is kept as securely as possible. The other key is known as the public key. The data encrypted with the private key can only be decrypted with the public key and vice versa, these guarantee the non-repudiation [40]. PKC is widely used for broadcast authentication [41] where different technologies are involved for writing or reading information. These technologies are described as follows:

3.2.8. Smart Card

A smart card is composed of an embedded microprocessor and a memory, it has various types of applications such as identification, data access, authentication, security key storage, and financial transactions [42]. When a smart card is inserted into a card acceptance device (CAD), the metallic pads come into contact with the CADs corresponding metallic pins, thus allowing the card and CAD to communicate. Smart cards are always reset when they are inserted into a CAD. This action causes the smart card to respond by sending an "answer-to-reset" (ATR) message, which informs the five shapes CAD, what rules govern communication with the card and the processing of a transaction.

3.2.9. Barcode

A barcode allows a faster capture of data, the immediate integration of the decoded data in the system and low-cost printing. There are two main different kind of barcodes: one dimensional (Figure 1a) and two dimensional ones (Figure 1b,c). One dimensional barcode allows us to store a limited amount of information and it consists of a group of bars and spaces that are designed to be scanned and read on a computer. However, the main problem is that it has a small storage capacity that ranges between 20 and 30 digits. Among them can be mentioned Ean 13, Ean 8, Code 128, Dun 14,

Upc 39. On the other hand, barcode labels have a control digit that prevents the scanning tool from losing data and data that does not pass the setpoint digit test will not be entered into the system [43]. Two-dimensional barcodes allow to store more information than one-dimensional barcode, for example, the PDF-417 can store a maximum of 1800 alphanumeric characters (ASCII) or 1100 binary codes for each symbol (each rectangle in the form of a "point cloud"). Another two-dimensional barcode is the quick response (QR) code, approved as ISO international standard (ISO/IEC18004) and It uses four standardized encoding modes: numeric with a data capacity of 7089 characters, alphanumeric with 4296 characters, byte/binary with 2953 bytes and kanji (Japanese writing) with 1817 characters [44]. In security terms, a QR Code could be manipulated to change the encoded information and it is possible to carry out SQL injection, command injection phishing and pharming attacks, reader software and social engineering attacks [45].

(**a**) (**b**) (**c**)

Figure 1. Barcode technology evolution: (**a**) code 128, (**b**) code PDF417 and (**c**) quick response (QR) code.

3.2.10. Radio Frequency Identification (RFID)

Radio frequency identification (RFID) is an electromagnetic proximity identification and data transaction technology which has an effective range from 10 cm to a few dozens of meters depending on tag class. This technology is used for automated identification of objects and people and brings an important development in ubiquitous or pervasive computing [46]. An RFID system has three main components: a tag or transponder that is located on the object to be identified and usually is the RFID device. The tag reader or transceiver is composed of an antenna and its main characteristic is the ability to read and write data over RFID tag. Finally, the data processing subsystem which uses the data obtained from the tag reader usually is a host system or connection to an Enterprise system [47]. Its capacity to store data is limited, usually 1 kilobyte (Mifare card) and until 8 kilobytes [48].

3.2.11. Near Field Communication (NFC)

It is a particular application of RFID, which provides wireless communication and data exchange by the proximity between devices over a distance up to 10 cm. The main advantage is simplicity: a transaction starts automatically just by the touch of a reader, another near field communication (NFC) device or an NFC compliant transponder. An NFC device has three operating modes: peer-to-peer mode, reader/writer mode, and card emulation mode. In peer-to-peer mode, communication is established between two NFC devices and they can exchange data. The reader/writer mode device can read or write information like URLs, SMSs, and phone numbers and it can contain until 32 KB (Type 4) [49]. Finally, the card emulation mode allows the NFC device to emulate a contactless smartcard [46].

By using previous technologies, it is possible to authenticate a person or document. Despite governments combine several methods to identify citizens in order to avoid identity theft, there is a long way to authenticate transactions.

4. Proposed Architecture for Biometric E-ID System with Blockchain

The proposed system has a higher level of security to identify and authenticate the document bearer and the document itself as well. Additionally, in order to strengthen the validation process of the document and the transactions carried out, blockchain technology is applied maintaining some current security measures used in a current identification document as for example holograms, barcodes, 3D images, among others by the use of the smart card technology with a cryptographic chip to store all the bearer information. The blockchain technology will be used to record and verify the transactions

made by all citizens registered in the electoral census. The transactions and block information of the blockchain systems are explained in more detail in [50].

4.1. Blockchain Architecture

Figure 2 shows the network architecture in a distributed and decentralized way including all the nodes of the network, the database that forms the blockchain and government entities. The network is intended as a private cloud, where only the nodes located in the notarial and registry entities can be part of it. The network consists of three types of nodes: the first are located in the register offices, which are in charge of issuing a new or a duplicate identity document when the citizen personally makes the request. In addition, they are the only certified entities able to generate the digital certificate with the corresponding public and private keys for each citizen by using a user's PIN. With this digital certificate, the citizen will be able to sign digital documents (for example, when creating its account) or perform transactions, and authenticate itself with the competent authorities. The second type of nodes are located in notary offices, which are responsible for keeping the record of the people's civil status, attesting the correspondence of people's identity and their corresponding document, by giving testimony of people's authenticity.

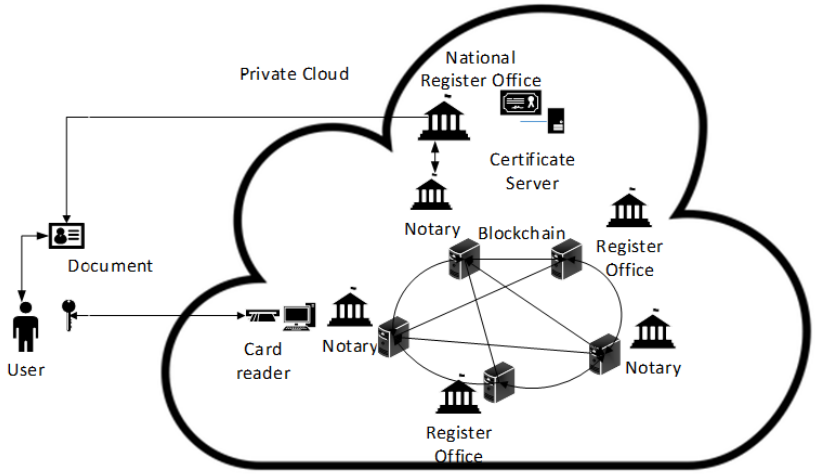

Figure 2. Proposed Blockchain architecture for the e-ID system [50].

4.2. Blockchain Node Architecture

The block diagram of a node in the proposed network architecture is shown in Figure 3. The citizen which owns its own electronic ID , where fingerprint and iris template are stored, generates a security certificate through a match on card (MoC) system. MoC system allows local verification of the templates stored on the card, these are read by a standard 32K Near Field Communication (NFC) storage chip and governed by the common criteria Evaluation Assurance Level (EAL) 5, allowing the authentication of the user against the national government through generic software. During the operation, the transaction is protected by the media on the card and by the encryption offered by the Blockchain. All nodes are aware of the existence of the transaction but only the receiver knows the content.

Usually, software used to validate the user identity leaves gaps in security such as possible phishing of identity through NFC failures and the possible acceptance of a fingerprint that does not coincide. In order to tackle the user's impersonation threat, our proposal considers a double biometric user validation together with public and private keys encrypted in the security certificate through NFC. Additionally, extra security is guaranteed when transactions are stored by means of the Blockchain technology in a distributed system that ensures traceability, security, and scalability.

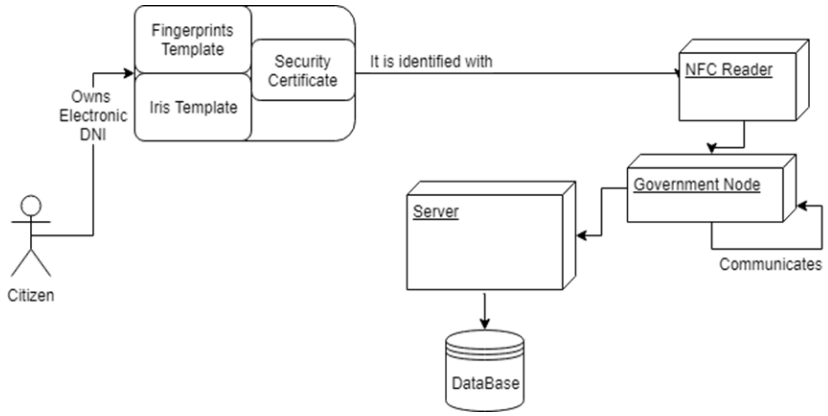

Figure 3. Block diagram of a node in the proposed network architecture.

The proposed solution is based on a private model since all the nodes belong to a single organization (national government), so that the system will be restricted, highly efficient and able to maintain centralized information. The combination of this system with the document makes it unlikely that the information will be compromised or that it will be impersonated.

4.3. Deployment Model

In order to depict physical relationships among hardware and software components, the software deployment diagram is shown in Figure 4. The transaction process perform by a citizen is explained as follows:

(i) A citizen arrives at a governmental office (National Register office, local register office, notary's office), and accesses to an authorized computer named Webserver identification, which is equipped with a card reader and a biometric reader.
(ii) The citizen uses his/her card and biometric feature (iris) to authenticate himself.
(iii) If the identification citizen is correct, automatically is shown the citizen's information on a form and subsequently, the citizen could perform a transaction using a drop-down list.
(iv) The identification webserver is connected to a database that will store the data of citizens along with their digital signatures, fingerprint templates, and iris. In this way, it is possible to verify the citizen authenticity.
(v) Finally, the identification webserver will deploy a message on the screen indicating the correct user validation.

4.4. Transactions

When the system validates and authenticates a citizen, and he/she wants to make a transaction, chooses one of the predefined transactions from drop-down list. A citizen could perform different transactions related to his personal information as the change of its civil status, register a son, request a document duplicate, among others, as shown in Figure 5.

4.5. System Implementation

Each time that a user performs a transaction, it will be validated, that is, it is verified that it is a well-formed transaction if so, it is signed using the user's digital certificate; then each transaction is recorded along with its associated information (Transaction ID, Issuer, etc.). Every transaction is kept waiting until one thousand (1000) transactions are completed and a new block is created. The number of transactions can be set according to performance measures. When a new block is created begins the process to assign which node will be in charge of mining it, according to the consensus algorithm proposed in Section 5.5. Finally, when a new block is mined, it is incorporated into the Blockchain.

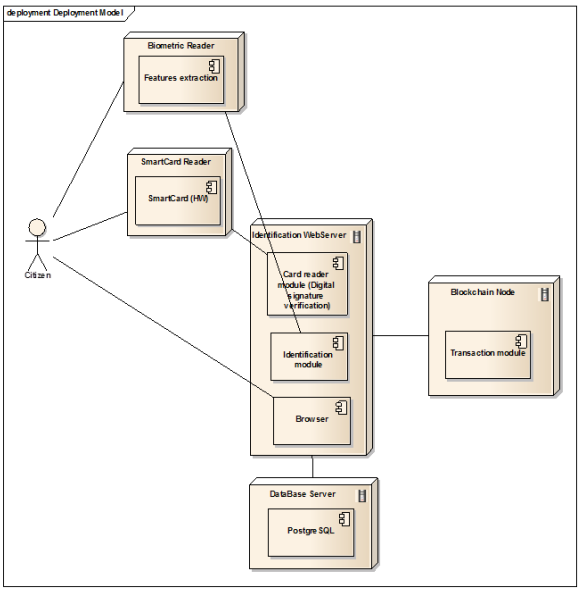

Figure 4. Deployment model.

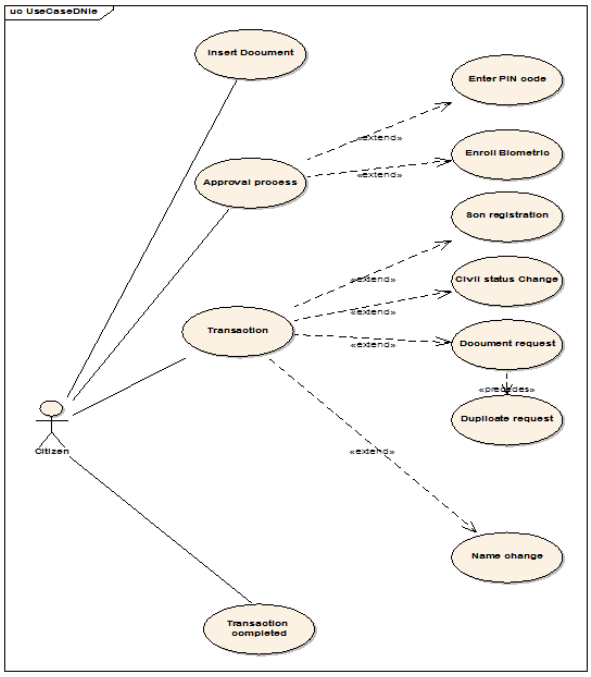

Figure 5. Use case diagram.

5. Consensus Algorithms

These algorithms are essential because their mechanisms are used to add a new block in the chain and also, to have control on the Blockchain. Nodes belonging to the Blockchain network are in charge satisfying requirements imposed by the system, which means accomplishing the hash function result at first, with a determined quantity of zeros. Depending on the way of performing the consensus, it could waste a lot of power, as for example, proof of work algorithm, and it is not a good choice in a private Blockchain. Another option is to use the proof of stake algorithm or design a new algorithm according to the Blockchain environment and needs.

5.1. Proof of Work (PoW) Algorithm

The proof of work algorithm was the first algorithm created for Blockchain. Indeed, the first one was created with the Bitcoins in 2009. That is why this consensus algorithm is the most known and it consists of finding a 'magical number' named as nonce to gain the right to append a new block in the chain and collect a reward. This nonce number goes changing from zero to a number which permits to obtain the number of zeros at first of the hash function result, as requested by the system, performing the same operation many times, that is calculating the hash function SHA256 and verifying if the condition is met. In other words, mining is the process of hashing the block header repeatedly, changing one parameter, until the resulting hash matches a specific target. There is no other way to find a specific solution for the problem than to try many times, as happen in a brute force attack.

Every node tries to find a solution and when it happened, the winner will be rewarded. Indeed, everyone tries but when one node finds a solution, every other node stops its search and verifies this proposed solution. The solution is accepted if there is 51% (or mare) of nodes approving it. This process is called mining and those who are resolving the math operation are called miners. Mining serves to secure the Blockchain system without a central authority because it avoids the fact that everyone can create a block every time they want to and also to generate new money in the system through the rewards collected by miners. The creation of cryptocurrency is an incentive system that helps to secure the decentralized ledger.

The difficulty target in Bitcoin Blockchain is adjusted every 2016 blocks so that the average time stays at 10 min. This difficulty is calculated according to the computing power of every node. However, it represents big environmental problems because today the value of bitcoins is very expensive and a lot of people try to mine to get the reward. So, the difficulty of the target is very high and it requires a very high power consumption to solve it.

When someone finds a solution, he broadcasts it to every node of the chain in order to add the block into the public ledger. Even if it is really hard to find proof of this work, it may happen that before everyone receives the validated block, another node finds a solution and starts broadcasting it. The other miners receive the first block sent and ignore the other one. That is to say, not all nodes have the same ledger as they should. This is called the forking problem. There are different versions of the ledger with different chains of block. To solve this problem, every node continues with the block they received first. After a certain time, a chain will be longer than the others because there can be more nodes to mine for example, and so they will have more chances of extending the chain. In this case, the rule is simple, the longest chain wins. So, when a fork problem occurs, the process continues and later, the longest chain is accepted by every node. Therefore, the youngest block in a chain can be subject to variation but thanks to the difficulty of adding a block, the stabilization of the Blockchain is sure.

5.1.1. Security Problems in PoW

Blockchain is today considered as a technology really secure because of the difficulty to falsify a block or to change the ledger. However, there are some security issues that have been found and this resulted in the development of various proof-based algorithms.

Imagine for example that we change the contents of an older block. The hash of this block becomes no longer valid because the Nonce value found for the block was appropriate for the older transactions. But like we have seen, if we change a little thing in the input of a hash function, everything changed in the output. Consequently, every other block that follows this invalid block is also invalid. In fact, every block is linked to each other like a chain, thanks to the previous hash block field in the header. The header is used as the input of the hash function so for all the following blocks, the Nonce value is no longer good. That is to say, thanks to this hash function, changing a little part of the Blockchain, makes everything that follows false and you need to find again all the Nonce values of the following blocks. Because of the difficulty of the puzzle and the rule that the longest chain wins, it seems impossible to falsify the Blockchain. But imagine that this person has a really huge resource of modern

hardware that allows him to have more computing power than all the network's nodes. In this case, he will be able to falsify all the Blockchain. A famous attack consists of starting mining a fraudulent branch at the end of the Blockchain and trying the best to be longer than the honest fork. This attack is called the Double spending attack or the 51% attack in reference to the minimum computing power of the network required in order to do this work [51].

Today, it is impossible for a single node to do this but thanks to mining pools, this kind of attack could be possible. To avoid this problem a lot of research has been done [52]. In a mining pool, the reward would be shared by everyone in equal parts. To disturb pool mining, Miller et al. [53] proposed an evolution of the PoW algorithm. They called it the non-out-sourceable puzzles. This consensus algorithm was developed to discourage the mining pool and to do that, they created a mechanism that gives chances to a miner inside a pool to win all the rewards without making any effort.

Another technique is used in the Ethereum cryptocurrency, it is called greedy heaviest observed subtree (GHOST). This consensus algorithm requires the mining nodes to include, in the header of the block they want to validate, the headers of the recently orphaned blocks known as uncles. Orphaned blocks are blocks that have been added on parallel branches of the main Blockchain. For Bitcoins, an uncle is, therefore, a block that would be considered as an orphan because it is not located on the longest chain. In GHOST strategy the longest chain is not chosen, it is the one with the most PoW contributions that will be selected as the valid chain. Ethereum encourages miners to include a list of uncles when they validate a new block. This technique has two main effects:

- It reduces the incentive of centralization by always rewarding (minimally) miners who produce obsolete or orphaned blocks because they are not part of a large group and get noticed about other blocks later (due to propagation delays of the network).
- It increases the safety of the chain by increasing the amount of work on the main chain. As a result, less work is wasted on alternative branches in favor of the main branch.

5.2. Proof of Stake (PoS) Algorithm

In this system, each node of the network has to prove that it has a certain part of the circulating token if it wishes to take part in the process of block validation. The consensus algorithm will then choose to delegate the validation of a new block to one of the nodes that own the largest share. In a simplistic way, in the context of a proof of stake (PoS), the probability for a node to be chosen to validate a new block corresponds to its holding percentage, its stake of the circulating token (currency or share). If a node owns x quantity and if there is a total of y coins, its chance to append the next block is x/y. This selection is done in a pseudorandom way to prevent a node from knowing in advance when it will be its turn to validate the next block. Nevertheless, taking into account certain additional parameters, such as the possession time of the token, allowing the "richest" nodes to be almost always selected. Finally, the validation of a block does not strictly give rise to remuneration, it is rather the holding of a certain amount of cryptocurrency that pays a remuneration, similar to interests.

Compared to the PoW method, PoS has two main advantages:

- Saving power: the PoS is a mechanism that consumes much less energy than PoW (which, in turn, requires a large number of cryptographic calculations to find the proof of work required for the validation of each block).
- The 51% attack is more difficult: in a PoS-type system, the 51% attack requires controlling more than half of the circulating token, which is usually much more expensive than controlling 51% of computing power in the PoW system.

Security Problem in PoS

PoS algorithms have some disadvantages and security problems too. One famous problem is called nothing-at-stake. In pure PoS algorithms, nodes are not encouraged to vote for the chain that would be the most likely to be legitimate (i.e., the longest for the Bitcoin platform). In the

presence of several potential chains (in case of forks), and in order to maximize their probability of obtaining the reward, the nodes will, therefore, allocate their "stake" uniformly and thus vote in parallel for the last blocks composing the potential chains. Unlike PoW where mining on multiple chains simultaneously costs energy and so money to the miner, mining on multiple chains costs nothing in a PoS system. Consequently, by satisfying their personal interests, miners could facilitate the realization of double-spending types of attack. An attacker may be able to send a transaction in exchange for some digital good (usually another cryptocurrency), and start a fork from one block behind the transaction and send the money to themselves instead, and even with 1% of the total stake the attacker's fork would win because everyone else is mining on both.

In pure PoS, the miner is selected on the pure stake he owns: more stake a miner has, the more chance he will get to become the block appender. Unfortunately, pure PoS would lead to an (undesirable) consequence of centralization: the richest member would always have an advantage. To avoid this, several alternative methods have been proposed [54,55].

5.3. Satoshi Consensus Algorithm

In the Satoshi consensus algorithm [56], the miner is chosen based on the state of the block. A Satoshi is the smallest currency unit of a bitcoin. To decide who is going to append the next block, a random index number is chosen between 0 and the total number of satoshis. Then, every transaction which used this satoshi is found out and the current owner of this satoshi will become the one appending the next block.

5.4. Proof of Luck (PoL) Algorithm

In the proof of luck algorithm, every participant node receives transactions and commits them building a new block. This algorithm uses trusted execution environments (TEE), which is a trusted hardware environment such as Intel Software Guard Extensions (SGX)-enabled CPUs. The algorithm receives a proof of luck generated from inside a TEE and the participant node extends its chain and then broadcasts it. The new Block consists of a hash parent of the previous block, data (new transactions), and a proof of luck. That proof of luck consists of computing a numeric score (luck) of a given blockchain by summing a determined quantity of values of each block. The chain with the highest luck will be chosen [57].

5.5. Consensus Algorithm for Private Blockchain

In the proof of luck (PoL) algorithm, TEE are used to be sure that a node is executing the desired code and does not intend to attack Blockchain. Having in mind that our private Blockchain is a trusted environment where nodes can be considered also trusted, we no longer need TEE avoiding additional hardware requirements. Next we propose a new consensus algorithm named tournament consensus algorithm.

Tournament Consensus Algorithm (TCA)

When a node wants to join the blockchain it asks the right for this by sending a request to every node. If the node is confirmed as authorized, it will receive the blockchain, the right to create a transaction and the right to try to add the next blocks. Every random time (an interval could be defined), a request is sent to every connected node to choose randomly a number between 0 and 1 (PoL algorithm authors propose 15 s comparing it with Ethereum). Every node will broadcast this number and wait to receive every random number from others. When a node has received every random number, it selects the biggest one and sends it to the node which had selected this number a "winner vote". When a node has received as many "winner votes" as the number of connected nodes, it means that it is the winner and it has the right to add the next block. Then the node has to mine the block using a challenge much more easily than proof of work consensus algorithm, allowing any normal computer to find the solution quickly. In this way, the loss of time and energy waste is avoided.

With the TCA, we introduce a simple mechanism to decide which node will be the miner and taking advantage of the PoL algorithm characteristics, we obtain better response time as is shown in Figure 6 and the high-cost attacks on individual TEE are avoided. Likewise, we can set the values to begin the process of sending random numbers and perform the consensus algorithm.

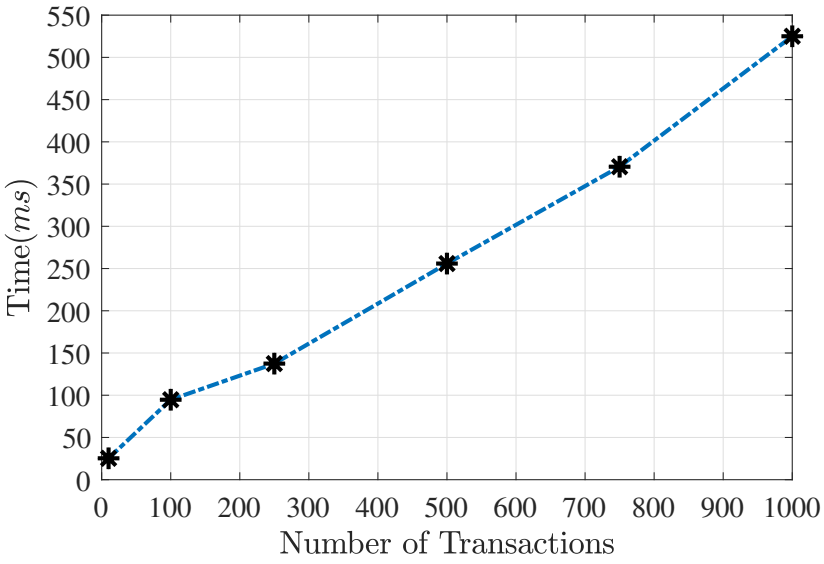

Figure 6. Time for mining and broadcasting one block versus the number of transactions.

6. System Performance Results

Some tests have been made in network to verify the efficiency of the consensus algorithm proposed (tournament consensus algorithm) measuring the time for mining and broadcasting it, cache memory usage, CPU percentage. In these tests, a transaction has described in Table 1.

Table 1. Transaction example.

ID Number	101
Serial number	1
Class	Notary
Type	Civil status
Information	Married

The common characteristics of the lab computers used to perform several tests are as follows:

- Processor: Intel Core i5 750, 2.66 GHz of 4 Cores.
- RAM Memory: 4 GB.
- HDD: 512 GB.
- Network Card: Intel 82574L Gigabit Ethernet NIC.
- OS: Linux Ubuntu 18.04.

Figure 6 shows the calculated time for the mining process of one block and the posterior broadcasting process of this block to every node in the Blockchain system. In this test was used a lab computer, varying the number of transactions, in order to obtain an estimated time. According to the figure, for mining one block containing one thousand (1000) transactions, the spent time was approximately five hundred and thirty (530) milliseconds.

In order to estimate the cache memory needed when several transactions must be kept in memory until the corresponding block is closed, a test was made and with one thousand (1000) transactions the RAM used is six hundred (600) megabytes approximately (Figure 7).

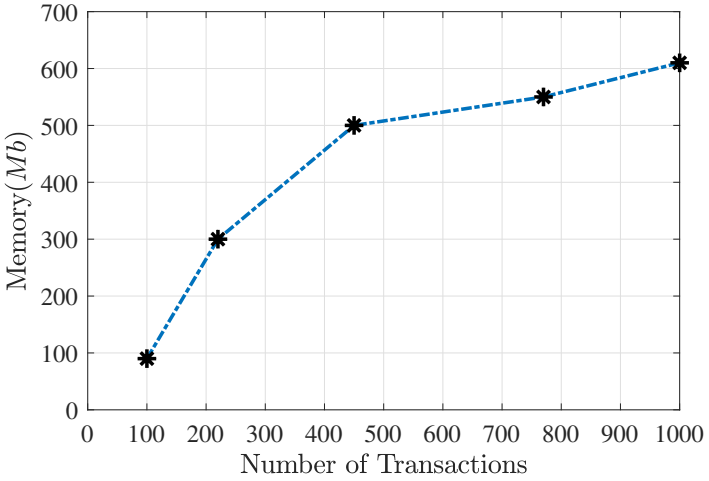

Figure 7. Used memory for broadcasting a number of transactions.

Figure 8 shows the CPU usage by a miner computer in the broadcasting process. At first, between one hundred and two hundred (100–200) transactions, the memory consumes rise quickly but after two hundred ten transactions, it continues to rise but to a lesser extent. In this way, for broadcasting one thousand (1000) transactions, the CPU usage amounts to approximately 43%.

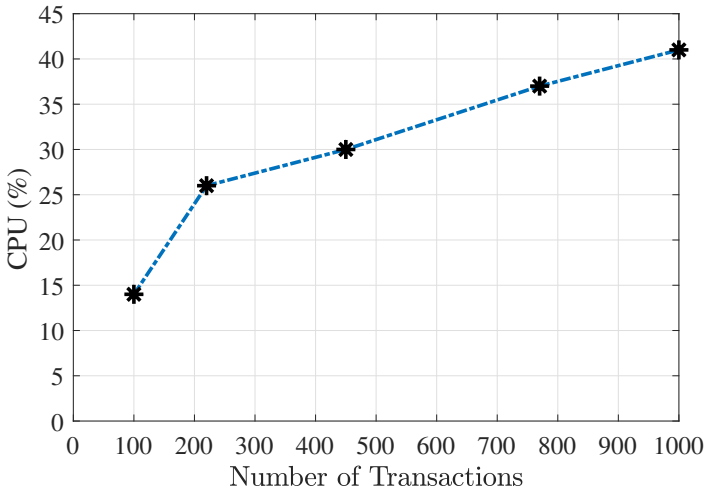

Figure 8. CPU usage for creating and broadcasting a number of transactions.

Although the CPU usage percentage is considerable, could be applied to different strategies, for example,

- If the number of users is not so high, adjusting the number of transactions setting a limit of CPU usage. For example with 30%, and according to Figure 8, could be managed four hundred fifty (450) transactions.
- In special dates, where thousands of transactions could be made, (for example popular elections) it could be possible to maintain the number of transactions (1000 transactions), but dedicating some special machines with better characteristics for creating and broadcasting transactions when a block is mined.

7. Conclusions and Future Work

We presented an analysis of private BCT architecture to achieve power and transaction efficiency in most general government services, where the security cannot be compromised. Therefore, TCA fulfilled the previous requirements under a private Blockchain deployment. Afterward, the TCA is

evaluated under a controlled scenario, where we showed its performance for different volumes of transactions. The results show that TCA requires an adequate amount of computing resources without compromise security risk in the integrity of the chain, unlike the analysis made to PoW and PoS algorithms, which present more power consumption and security issues into private blockchains.

According to the architecture proposed, the smartcards are the key to get the right to make a blockchain transaction. We proposed a robust authentication mechanism that combines the three user authentication factors according to the MoC mechanism present on current smartcards and biometric systems. As a result, our mechanism avoids the identity theft for document owner and control that only the owner can access to e-government services.

In order to have more significant tests, we should evaluate the proposed consensus algorithm with additional computers in the network to measure the time scaling and not only working on a local network but directly on Internet, which will be a network where the proposed system will work. Additionally, in terms of implementation, the proposed blockchain system considers that all nodes register every received block in a local file that needs to be gathered among the different nodes prior to the initiation of the system.

Author Contributions: Conceptualization, G.R.; Data curation, G.R.; Formal analysis, M.P.; Funding acquisition, R.P.; Investigation, M.P., R.P. and G.R.; Methodology, M.P.; Project administration, R.P.; Software, J.M. and L.B.; Validation, J.M. and L.B.; Writing–original draft, R.P.; Writing–review and editing, M.P. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Pontificia Universidad Javeriana.

Acknowledgments: The authors would like to thank the Pontificia Universidad Javeriana for funding the project of this proposal.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

MDPI	Multidisciplinary Digital Publishing Institute
ICT	Information and communication technologies
e-ID	Electronic identity document
BCT	Blockchain technology
CLI	Changeable laser image
PKC	Public key cryptography
PIN	Personal identification number
OTP	One-time password
ZKP	Zero-knowledge proofs
RFID	Radio frequency identification
NFC	Near field communication
PoW	Proof of work
PoS	Proof of stake
PoL	Proof of luck
TEE	Trusted execution environments
TCA	Tournament consensus algorithm

References

1. Supriyanto, A.; Mustofa, K. E-gov readiness assessment to determine E-government maturity phase. In Proceedings of the 2016 2nd International Conference on Science in Information Technology, ICSITech 2016: Information Science for Green Society and Environment, Balikpapan, Indonesia, 26–27 October 2016; pp. 270–275.
2. Registraduria Nacional del Estado Civil. Available online: https://www.registraduria.gov.co/ (accessed on 18 September 2019).

3. Ansari, A.Q. E-Document retrieval using rough-set theory. In Proceedings of the ICIIP 2011 International Conference on Image Information Processing, Shimla, India, 3–5 November 2011.
4. Waldmann, U.; Vow, S.; Sven, T.; Poller, A. Electronic Identity Cards for User Authentication—Promise and Practice. *IEEE Secur. Priv.* **2012**, *10*, 46–54.
5. Policia Nacional de Colombia. Available online: https://www.policia.gov.co/ (accessed on 18 September 2019).
6. Haque, M.A.; Khan, N.Z.; Khatoon, G. Authentication through keystrokes: What you type and how you type. In Proceedings of the 2015 IEEE International Conference on Research in Computational Intelligence and Communication Networks, ICRCICN, Kolkata, India, 20–22 November 2015; pp. 257–261.
7. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 10 January 2020).
8. Christidis, K.; Devetsikiotis, M. Blockchains and Smart Contracts for the Internet of Things. *IEEE Access* **2016**, *4*, 2292–2303. [CrossRef]
9. Bocek, T.; Rodrigues, B.B.; Strasser, T.; Stiller, B. Blockchains everywhere—A use-case of blockchains in the pharma supply-chain. In Proceedings of the IM 2017—2017 IFIP/IEEE International Symposium on Integrated Network and Service Management, Lisbon, Portugal, 8–12 May 2017; pp. 772–777.
10. Li, X.; Jiang, P.; Chen, T.; Luo, X.; Wen, Q. A survey on the security of blockchain systems. *Future Gener. Comput. Syst.* **2017**. [CrossRef]
11. Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In Proceedings of the 2017 IEEE 6th International Congress on Big Data, (BigData Congress), Honolulu, HI, USA, 25–30 June 2017; pp. 557–564. [CrossRef]
12. Solat, S.; Potop-butucaru, M. ZeroBlock: Preventing Selfish Mining in Bitcoin. Ph.D. Thesis, Sorbonne Universites, Paris, France, 2016.
13. Eyal, I.; Sirer, E.G. Majority is not Enough: Bitcoin Mining is Vulnerable. In Proceedings of the 18th International Conference on Financial Cryptography and Data Security, Barbados, Federation of the West Indies, 3–7 March 2014; Volume 8437, pp. 436–454. [CrossRef]
14. Zhao, X.; Chen, Z.; Chen, X.; Wang, Y.; Tang, C. The DAO attack paradoxes in propositional logic. In Proceedings of the 4th International Conference on Systems and Informatics, ICSAI 2017, Hangzhou, China, 11–13 November 2017; pp. 1743–1746. [CrossRef]
15. Apostolaki, M.; Zohar, A.; Vanbever, L. Hijacking Bitcoin: Routing Attacks on Cryptocurrencies. In Proceedings of the IEEE Symposium on Security and Privacy, San Jose, CA, USA, 22–26 May 2017; pp. 375–392. [CrossRef]
16. Singh, A.; Ngan, T.W.; Druschel, P.; Wallach, D.S. Eclipse attacks on overlay networks: Threats and defenses. In Proceedings of the IEEE INFOCOM, Barcelona, Spain, 23–29 April 2006; pp. 1–12. [CrossRef]
17. Heilman, E.; Kendler, A.; Zohar, A.; Goldberg, S. Eclipse Attacks on Bitcoin's Peer-to-Peer Network. In Proceedings of the USENIX Security Symposium, Washington, DC, USA, 12–14 August 2015; pp. 129–144.
18. Aggelos Kiayias, G.P. On Trees, Chains and Fast Transactions in the Blockchain. In Proceedings of the International Conference on Cryptology and Information Security in Latin America, Havana, Cuba, 20–22 September 2017. [CrossRef]
19. Natoli, C.; Gramoli, V. The Balance Attack or Why Forkable Blockchains are Ill-Suited for Consortium. In Proceedings of the 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2017, Denver, CO, USA, 26–29 June 2017; pp. 579–590. [CrossRef]
20. Saia, R. Internet of Entities (IoE): A Blockchain-based Distributed Paradigm to Security. *arXiv* **2018**, arXiv:1808.08809.
21. Delgado-Mohatar, O.; Fierrez, J.; Tolosana, R.; Vera-Rodriguez, R. Blockchain and biometrics: A first look into opportunities and challenges. *Adv. Intell. Syst. Comput.* **2019**, *1010*, 169–177._21. [CrossRef]
22. Prause, G. E-Residency: A business platform for Industry 4.0? *Entrep. Sustain. Issues* **2016**, *3*, 216–227. [CrossRef]
23. Garcia, P. Biometrics on the blockchain. *Biom. Technol. Today* **2018**, *2018*, 5–7. [CrossRef]
24. Ministerio del Interior España. Guía De Refernecia Del DNIE Con NFC. Available online: https://www.dnielectronico.es/PDFs/Guia_de_Referencia_DNIe_con_NFC.pdf (accessed on 10 January 2020).
25. Andrulevičius, M. Methods and applications of optical holography. *Mater. Sci.* **2011**, *17*, 371–377. [CrossRef]
26. Chan, H.T.; Hwang, W.J.; Cheng, C.J. Digital hologram authentication using a hadamard-based reversible fragile watermarking algorithm. *IEEE/OSA J. Disp. Technol.* **2015**, *11*, 193–203. [CrossRef]

27. Hanchez, D. A Comparative Study of Software Protection Tools Suited for E-Commerce with Contributions to Software Watermarking and Smart Cards. Ph.D. Thesis, Univesité Chatolique de Louvain, Ottignies-Louvain-la-Neuve, Belgium, 2003.
28. Duncan, R. An Overview of Different Authentication Methods. Available online: https://www.sans.org/reading-room/whitepapers/authentication/overview-authentication-methods-protocols-118 (accessed on 10 January 2020).
29. Nagel, R.H. System and Method for Production and Authentication of Original Documents. U.S. Patent 7080041, 18 July 2006.
30. Hoang, B.; Caudill, A. *Biometrics*; Technical Report; IEEE: Piscataway, NJ, USA, 2012.
31. Liu, S.; Silverman, M. Practical guide to biometric security technology. *IT Prof.* **2001**, *3*, 27–32. [CrossRef]
32. National Science and Technology Council. Biometrics in Goverment POST-9/11—Advancing Science, Enhancing Operations. Available online: https://fas.org/irp/eprint/biometrics.pdf (accessed on 10 January 2020).
33. Jain, A.; Feng, J.; Nandakumar, K. Fingerprint matching. *Computer* **2010**, *43*, 36–44. [CrossRef]
34. Moi, S.H.; Rahim, N.B.A.; Saad, P.; Sim, P.L.; Zakaria, Z.; Ibrahim, S. Iris biometric cryptography for identity document. In Proceedings of the SoCPaR 2009—Soft Computing and Pattern Recognition, Malacca, Malaysia, 4–7 December 2009; pp. 736–741.
35. Wayman, J.; Jain, A.; Maltoni, D.; Maio, D. *Biometric Systems—Technology, Design and Performance Evaluation*; Springer: London, UK, 2005; pp. 1–369.
36. Thing, V.L.L.; Ying, H.M. Rainbow Table Optimization for Password Recovery. *Int. J. Adv. Softw.* **2011**, *4*, 479–488.
37. Vaidya, S.A.; Bhosale, V. Invisible touch screen based PIN authentication to prevent shoulder surfing. In Proceedings of the 2016 International Conference on Inventive Computation Technologies (ICICT), Coimbatore, India, 26–27 August 2016; pp. 1–4.
38. Martín-Fernández, F.; Caballero-Gil, P.; Caballero-Gil, C. Authentication Based on Non-Interactive Zero-Knowledge Proofs for the Internet of Things. *Sensors* **2016**, *16*, 75. [CrossRef] [PubMed]
39. Fisher, R.; Lyu, M.; Cheng, B.; Hancke, G. Public key cryptography: Feasible for security in modern personal area sensor networks? In Proceedings of the IEEE International Conference on Industrial Technology Taipei, Taiwan, 14–17 March 2016; pp. 2020–2025.
40. Murrell, S.; Einspruch, N.G. Electronic identification, personal privacy and security in the services sector. In Proceedings of the 5th International Conference Service Systems and Service Management—Exploring Service Dynamics with Science and Innovative Technology, ICSSSM'08, Melbourne, VIC, Australia, 30 June–2 July 2008.
41. Liu, Y.; Li, J.; Guizani, M. PKC based broadcast authentication using signature amortization for WSNs. *IEEE Trans. Wirel. Commun.* **2012**, *11*, 2106–2115.
42. Yaakob, W.F.H.; Manab, H.H.; Adzmi, S.N.M. Smart card chip design implementation on ARM processor-based FPGA. In Proceedings of the 2014 IEEE 3rd Global Conference on Consumer Electronics, GCCE, Tokyo, Japan, 7–10 October 2014; pp. 294–297.
43. Sigar, K.O.; Jared, O.K. A Critical Look of USSD Technology Adoption and Benefits. *Int. J. Adv. Res. Comput. Sci.* **2014**, *5*, 27–29.
44. Siyang, Z. Deformed Two-Dimension Code Quick Recognition Algorithm Design and Implementation in Uncertain Environment. In Proceedings of the 2015 7th International Conference on Measuring Technology and Mechatronics Automation, ICMTMA 2015, Nanchang, China, 13–14 June 2015; pp. 322–325.
45. Leithner, M.; Kieseberg, P.; Schrittwieser, S.; Munroe, L.; Mulazzani, M.; Sinha, M.; Weippl, E. QR code security. In Proceedings of the MoMM'2010—The Eighth International Conference on Advances in Mobile Computing and Multimedia, Paris, France, 8–10 November 2010; p. 430.
46. Roberts, C.M. Radio frequency identification (RFID). *Comput. Secur.* **2006**, *25*, 18–26. [CrossRef]
47. Sarma, S.E.; Weis, S.A.; Engels, D.W. RFID Systems and Security and Privacy Implications. In Proceedings of the Cryptographic Hardware and Embedded Systems, Redwood Shores, CA, USA, 13–15 August 2002; pp. 454–469.
48. Jara, A.J.; Alcolea, A.F.; Zamora, M.A.; Skarmeta, A.F. Analysis of different techniques to define metadata structure in NFC/RFID cards to reduce access latency, optimize capacity, and guarantee integrity. *IFAC Proc. Vol.* **2010**, *10*, 192–197. [CrossRef]

49. Shobha, N.S.S.; Aruna, K.S.P.; Bhagyashree, M.D.P.; Sarita, K.S.J. NFC and NFC payments: A review. In Proceedings of the 2016 International Conference on ICT in Business, Industry, and Government, ICTBIG, Indore, India, 18–19 November 2016; pp. 1–7.
50. Juan, M.D.; Andrés, R.P.; Rafael, P.M.; Gustavo, R.E.; Manuel, P.C. A Model for National Electronic Identity Document and Authentication Mechanism Based on Blockchain. *Int. J. Model. Optim.* **2018**, *8*, 160–165. [CrossRef]
51. Giang Truong, N.; Kyungbaek, K. A survey about consensus algorithms used in Blockchain. *J. Inf. Process. Syst.* **2018**, *14*, 101–128.
52. Ittay Eyal, E.G.S. How to Disincentivize Large Bitcoin Mining Pools. Available online: http://hackingdistributed.com/2014/06/18/how-to-disincentivize-large-bitcoin-mining-pools/ (accessed on 18 September 2019) .
53. Miller, A.; Kosba, A.; Katz, J.; Shi, E. Nonoutsourceable scratch-off puzzles to discourage bitcoin mining coalitions. In Proceedings of the ACM Conference on Computer and Communications Security, Denver, CO, USA, 12–16 October 2015; pp. 680–691.
54. King, S.; Nadal, S. PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake. Available online: https://bitcoin.peryaudo.org/vendor/peercoin-paper.pdf (accessed on 10 January 2020).
55. Vasin, P. BlackCoin's Proof-of-Stake Protocol v2 Pavel. Available online: https://blackcoin.org/blackcoin-pos-protocol-v2-whitepaper.pdf (accessed on 10 January 2020).
56. Bentov, I.; Gabizon, A.; Mizrahi, A. Cryptocurrencies without proof of work. In Proceedings of the International Conference on Financial Cryptography and Data Security, Barbados, Federation of the West Indies, 22–26 February 2016.
57. Milutinovic, M.; He, W.; Wu, H.; Kanwal, M. Proof of Luck: An efficient blockchain consensus protocol. In Proceedings of the SysTEX 2016—1st Workshop on System Software for Trusted Execution, Colocated with ACM/IFIP/USENIX Middleware 2016, Trento, Italy, 12–16 December 2016; pp. 2–7.

© 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).