A Model for National Electronic Identity Document and Authentication Mechanism Based on Blockchain

Montes D. Juan, Rincón P. Andrés, Páez M. Rafael, Ramírez E. Gustavo, and Pérez C. Manuel

***Abstract*—This paper proposes a security model for a national electronic Identity Document (e-ID) in Colombia, based on blockchain network concept using smart cards and taking advantage of the traditional authentication methods as biometry (citizen authentication) and physical security (document authentication), in order to reduce the security issues of the currently used Identity Document. The proposed model uses smart cards to store information of the citizen, such as the encrypted template of their biometric features in order to perform user authentication, fingerprint and iris recognition technologies. In addition, the well-known benefits of a private blockchain network are exploited to verify the authenticity of the document and validate the legality of the user transactions. The blockchain network architecture are also presented defining the block structure, the type of transactions and the blockchain approach for the e-ID.**

***Index Terms*—Authentication, blockchain, identity, identification document, information privacy.**

I. Introduction

Blockchain is a technology which is based on the idea of a decentralized accounting book that cannot be altered or modified, where consensus is required from all network members and all validated transactions are recorded [1]. This technology is characterized by providing decentralization, integrity, reliability, traceability of information and non-repudiation by users. These features bring benefits in different areas, such as the veracity of transactions, i.e. for a transaction to be valid it must be signed by the user's private key and must be approved by the set of nodes generating the blocks into the blockchain [2]. As a distributed accounting network, if a node is being attacked, the other network members has access rights of a copy of the accounting book avoiding a fraudulent book's modification [3]. In addition of the security features, Blockchain is also claimed as a tracking transaction system providing user's transaction information in short time [4].

Blockchain is a distributed database and a decentralized transaction data technology, applied for the first time in Bitcoin cryptocurrency in 2008 when the idea was coined [5]. Since then, as explained by Bocek *et al.* [4], blockchain technology can be used in applications such as fraud detection, identity management, document verification or governmental services.

In the Colombian society context, the registration process is understood as the right that a citizen has from its birth of being individualized by the state, which upon the constitution gives him or her the possibility of exercising his rights and duties in society. On the other hand, the identification process is understood as the recognition of an element that contains some of the data recorded by each citizen, including biometrics measures which identifies them in an unambiguous way [6].

Fig. 1. Example of colombian ID From [8].

The element that contains the information of a person to be identified, is known as a National Identity Document (ID) Fig. 1, in which is printed the holder photograph, name, date of birth, and other personal details. The card itself works as an official proof for a person to be identified but it does not have a chip inside that allows to perform online transactions in a secure way.

In Colombia, the authorities have registered almost thirty-four thousand misplaced documents that can generate cases of identity theft, in addition there have been cases in which offenders clone documents of people to avoid authorities and commit fraud [9]. There are also cases with lost or stolen identification documents used by criminals to falsify people's identities in order to take out bank loans or sell their properties [10]. Another common problem in Colombia is electoral fraud, where deceased person's ID are used to validate fraudulent votes.

In the current identity document Fig. 1, the document has the fingerprint of the citizen visible on it, which is used to authenticate the identity of the document bearer, however this feature generates a security flaw when sharing sensitive identity information, i.e. any person could take the image of the fingerprint and easily duplicate it for fraudulent purposes [11].

Considering the security flaws that a national ID can have particularly when transactions are made from it. There is a clear gap for introducing new technologies for tracking and validate transactions.

Nevertheless, due to the current technological advances a new concept of an electronic Identity Document (e-ID) has appeared, which consists of generating the same ID document into a smart card where data can be stored digitally (Name, date and place of birth, facial image, and fingerprints), and in addition, it includes more complex security measures

Manuscript received February 15, 2018. This work was supported by the engineering faculty, Pontificia Universidad Javeriana, Colombia.

The authors are with the Pontificia Univerisdad Javeriana, Bogotá-Colombia, Cra 7 no. 40-62, Colombia (e-mail: {juan-montes; arinconp; paez-r; ramirez.g; manuel.perez}@javeriana.edu.co).

DOI: 10.7763/IJMO.2018.V8.642

by encrypting personal data, besides of giving access to novel online services for citizens [7] and using physical security technics to protect the document.

Certainly, blockchain network combined with user's authentication and identification processes can be applied to overcome the aforementioned issues and offering additional services. In the ID context, user's authentication is the process to verify and validate the relationship between the document and its owner, these processes are based on the concept of strong authentication, which consists of the verification of four factors: *something that the person has* (Card), *something that the person knows* (PIN), *something that the person is* (Fingerprint) and *something that the person does* (Signature) [12].

The combination of these factors generate a more secure or strong authentication for the identification of the person. The aim of this paper is to propose a new security model for a national electronic Identity Document (e-ID) in Colombia, based on blockchain network concept by using smart cards to store the information of the person, such as the encrypted template of some biometric features of the person to perform user authentication; also using the benefits of a private blockchain network to verify the authenticity of the document and validate the legality of the transactions that a user would do.

This paper is organized as follows: Section II provides a background of blockchain and biometric user authentication. Section III presents the model proposed, the blockchain architecture, the transaction's blocks and the blockchain e-ID model. Finally, Section IV presents the future works and Section V concludes.

II. Conceptual Framework

A. Blockchain for e-Government

Some governments around the globe are leading the digital transformation through digital identity. The adoption of Blockchain technology for digital identity solutions helps to empower citizens and build a more connected digital society [13].

Although blockchain has only become a trending technology in recent years, Estonia is leading the way in the blockchain revolution. Estonian government has been testing the technology taking the first steps towards becoming an e-state. In 2012, blockchain has been in operational use in Estonia's registries, such as national health, judicial, legislative, security and commercial code systems, with plans to extend its use to other areas such as personal medicine, cyber security and embassy data.

The technology developed by the Estonians is also being used by NATO, U.S. Department of Defense, as well as European Union information systems to provide better levels of cyber security [14].

The One-Stop Services project, in Chancheng District in China, started in 2014 and different local government institutions have deployed it, so that citizens can apply for multiple public services through the same platform, speed up procedures and offering a better service for citizens. According to the Strategic Cooperation Agreement, the application of blockchain technology in Chancheng's e-government focuses on solving the problem of individual credit by building a digital identity system. Chancheng government believes that using blockchain technology to preserve all system records of changes and trading on a cloud system can verify the provenance and authenticity of data during transmission. In this way, it is possible to establish a reliable personal identity system.

The digital identity includes personal identity, authentication and digital signature functions and will provide reliable identification of individuals as a basic part of One-Stop Services [15].

B. Biometric User Authentication

When you submit your final version, after your paper has been accepted, prepare it in two-column format, including figures and tables.

It is different biometric technologies, which permit the acquisition of a person's unique biometric characteristics. Authors in [16], explains how biometrics technologies are used for automatic personal recognition based in two types of biometric features: First, the biological traits like fingerprint, face recognition, palm print, hand geometry or iris recognition and, second, the behavioral characteristics like voice or signature. Even though not all biometric technologies are fully developed or accepted in society, some of them has gained acceptance for user authentication such as fingerprint and iris recognition [17].

Fingerprint recognition is the oldest biometric method and certainly one of the most developed. As explained in [18] there are different fingerprint readers: optical, capacitive, ultrasonic and thermal. A reader acquires not only recognizing similarities of the minutiae of the fingerprint, but identifying other particularities for security purposes, for example, some readers can now differentiate even if the fingerprint read comes from a living person by sensing the blood flow and temperature.

The work in [19] proposed a fingerprint recognition method based on the pattern recognition of a fingertip. These kind of pattern contains information about bifurcations, ridge endings, dots, core points and delta points of the finger. Fingerprint identification system acquire a quantity of minutiae to be compared with the minutiae of a stored template, generating the matching probability between the captured and stored fingerprints. In this way, a range of acceptance is defined and it represents the possibility of both fingerprints come from the same person. The system can be more robust depending on the quantity of acquired minutiae used to compare both fingerprints. The advantages of a fingerprint system are well known [20]: distinctiveness or uniqueness, permanence and performance (accuracy, speed, and robustness) and acceptability. However, it also presents disadvantages such as: universality (people without fingerprints or difficulty to be registered), circumvention and collectability, due to the ease of imitating the footprint by using an artifact or substitute.

Other biometric method is the Iris recognition, which analyze features found in the colored tissue ring. 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, and moreover, it has the potential for higher than

the average matching performance [19]. For this reason, the iris biometrics system is suitable as an identification system [21]. This technology is under development, making it difficult to use and integrate identification systems. In addition, being a technology based on image capture, its main disadvantage is the quality of the image, affected by the luminosity when the image is taken [19] [20].

III. Proposed Model for an Identity Document System

If you are This paper proposes the design of a new model for an Electronic Identification Document (e-ID), which in addition to present visible security elements, has a higher level of security to identify and authenticate the document bearer, as well as authenticate the document itself. It is also proposed to strengthen the validation process of the document and the transactions carried out with it applying blockchain technology but maintaining some current

security measures used in the Colombian Identification Document as physical security (holograms, barcode, 3D image, etc.) and using a new Smart Card with a cryptographic chip to store additional information.

A. Blockchain Architecture

The blockchain technology will be used to record and verify the transactions made by all Colombian citizens registered in the electoral census. Each transaction will be registered and each register will generate a hash (Sha256) building a Merkle tree. The last Hash corresponding to the root of the Merkle tree in which the last transaction made by the citizen is stored safely, subsequently, every transaction could be verified. Likewise, to check the validity of the document, if this Hash is in the blockchain and it is stored inside the document, the document is validated.

Previos Hash	0000000000000000000000000000000000	Header	Block
Timestamp	1508295390		
Nonce	25698765		
Merkle Root	0000000000000000000000000000000000		
Transactions	República de Colombia Registaduria Nacional del Estado Civil Documento de Identidad electrónico Cedula de Ciudadanía		
Height	0		
Header Hash	00000000006387F52D405C9634078168		

Fig. 2. Genesis block.

The following specifications are proposed for the blocks:

The first block or Genesis block Fig. 2, will have a header, which contains the following information: Basic information to start the blockchain, the previous Hash (a zero's string of 256-bit), a timestamp with the time and date in which the block and blockchain was created in the Unix format (epoch), the nonce, a 32-bit number which allows to comply the requirement to obtain a Hash with four zeros on the left of a string of 256-bit in the header Hash field; it is a proof of work, since there is the possibility that some of the nodes are manipulated in order to modify some transaction, despite being in a private network, finally, the root of the Merkle tree, it will also contains a string with zeros (256 bits) because of this block does not register any transaction, only an initial information.

Additionally, the two block identifiers must be calculated: the header Hash and the height of the block. The header Hash is the result of obtaining a double hash of the data in the header of the genesis block, fulfilling the requirement of having four zeros on the left (Hash256 (Hash256 (Block))). The block height will be an integer number, indicating the position of the block into the chain, which for the case of the genesis block will be zero.

The following blocks are the transaction blocks and they are differentiated from the genesis block by having a set of transactions. From the transactions, the hashes are obtained and the Merkle tree is built. Each block will have a size of 128 kilobytes and will have the following characteristics, as shows in Fig. 3:

Previos Hash	00000000006387F52D405C9634078168	Header	Block
Timestamp	1508295390		
Nonce	25698777		
Merkle Root	C9634078166387F52D405C9634078168		
Transactions	…		
Height	1		
Header Hash	00000000006387F52D405C9634077777		

Fig. 3. Transaction block.

The header is composed of the previous Hash (256 bits) corresponding to the hash obtained in the immediately previous block. The Timestamp contains information about the day, time and date of the last transaction, according to the Unix format (epoch). The nonce is a 32-bit number, which allows to comply the requirement to obtain a Hash with four zeros on the left of a string of 256-bit in the header Hash field, the number of zeros varies according to the complexity of the requirement, a time of 2 minutes is proposed with a margin of ± 30 seconds, for the creation of the block.

The Root of the Merkle tree is a 256-bit string corresponding to the hash of the root of the transaction tree. The transactions field, will register transactions made by users and which is not part of the header.

Finally, the block identifiers with the header Hash and the block height exist. The header Hash is the result of obtaining a double hash of the data in the header of the block, fulfilling the requirement of having four zeros on the left (Hash256 (Hash256 (Block))) and adjusting the number of zeros according to the response times. The block height will be an integer number, indicating the position of the block into the chain.

The Fig. 4 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 different types of nodes in the blockchain will be controlled by the Colombian government authority responsible of the issuance of Identity documents (National Registry of Civil Status). The nodes will be geographically dispersed in the main notaries and registration entities of the country, and in special events (i.e. elections) it would be necessary to lease computing capacity due to the number of transactions.

In the system, there are not transactions that constitute some monetary value, because of this, the proposed network must be deployed in a government private network offering services to citizens, where only certified nodes have access to

the blockchain information [22]. That is not to say all nodes are trusted because they are distributed geographically and could be victims of an internal (i.e. an insider) or external attacks. The blockchain network consists of three types of nodes: the first are the registration nodes, in Colombia these kind of nodes 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 Personal Identification Number (PIN).

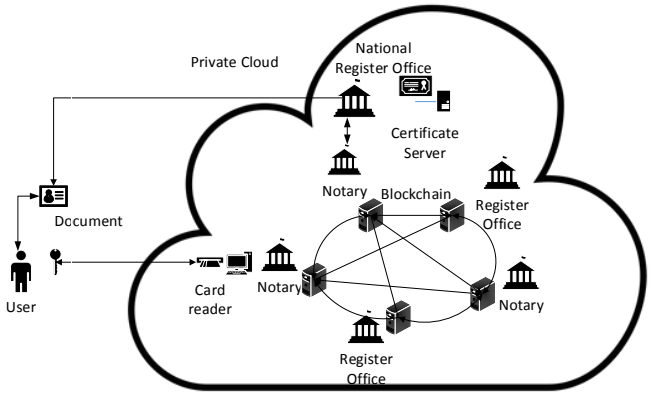

Fig. 4. Blockchain architecture.

With this digital certificate the citizen will be able to sign digital documents (for example, when creating his account) or perform transactions, and authenticate himself with the competent authorities.

The second type of nodes are the notaries, which in the Colombian society are responsible for keeping the record of the people civil status, attesting the correspondence of people identity and their corresponding document, by giving testimony of people authenticity.

And finally, there are the mining nodes that perform the job of finding the hash with the requirements, initially establishing a time of 2 minutes with a margin of ± 30 seconds to generate a hash with a certain number of zeros on the left. In addition of adding new blocks to the database.

The nodes will not only have the database of the stored blockchain, but also a list with the invalidated documents called a revocation list. This mechanism has been thought for rejecting transactions from lost, stolen or invalidated documents, as for example, the ones of dead citizens. It is necessary to generate the revocation list outside of the blockchain network, because without the document or the user's PIN, the last transaction cannot be generated or signed, generating and invalid document report.

B. Blockchain Transactions

Each transaction will be classified in the following 4 established groups: (i) Notary, (ii) Tax, (iii) Government, and (iv) Register. First, there are transactions that take place in a notary office known as notarial transactions which are divided into four types of transactions: change of name, civil status change (married, divorced, etc.), children's registration and death registration. Second, there are 2 types of tax transactions: registration and changes of the RUT (*Single Tax Register*). Third, government transactions which are divided into SISBEN registration (*System of Identification of Beneficiaries of Social Subsidies*) and application for governmental subsidies. Finally, there are the transactions made in the register classified as follows: issuing the identity document for the first time, application to invalidate the document, issue of an ID duplicate and voting.

It is worth to notice voting is an event where the blockchain network would have peak activity. To prevent the network from collapsing by the number of transactions carried out per minute on a day of voting, it is proposed to lease computing capacity when the voting is happening, because in Colombia around 36 million of votes are probably processed [23].

A transaction is composed by a, user identification number, serial number of the document, class and type of transaction, and basic information of the transaction (if necessary). It will be avoided to put the name of the person to preserve the privacy of the citizen. In Fig. 5, an example of a civil status change notarial transaction is shown.

ID Number	101
Serial Number	1
Class	Notary
Type	Civil Status
Information	Married

Fig. 5. Transaction example.

The process begins when the citizen requests his cryptographic document in the registry entity, where its biometric characteristics are taken (fingerprints and / or iris recognition) and stored into the corresponding templates in an encrypted way inside the smart card. The citizen is then asked to type in a PIN (which only he knows), to proceed to the generation of the digital certificate directly on the chip along with his private and public key, in this way the private key will always remain hidden in the chip of the card for security purposes. To be able to use his private key, the user must type his secret PIN, for example, in the case he wants to digitally sign a document.

The creation of the digital certificate is done on the chip, through the *Physically Unclonable/Random Function* (PUF), because it provides strong protection for secret keys and data. A PUF, is a function incorporated in a physical structure, the function is based on the idea of something that is easy to evaluate but hard to predict. The PUF is a function that maps a set of challenges to a set of responses based on an intractably complex physical system. Hence, this static mapping is a random assignment [24]. In other words, the PUF is a hardware analog one-way function that makes the embedded chip easy to make but practically impossible to duplicate, even with identical layout masks [25], due to the variations in the manufacturing process which causes significant differences in the characteristics of the device [24]. Hence, by generating the certificates on the card using the PUF technology, it is possible to ensure no one can clone the digital certificate and the user's private key.

Finally, the registration process ends when the user obtains his electronic ID, which will allow him to carry out the transactions previously specified.

When the user makes a transaction, he must enter his PIN code, in this way he authenticates himself through his digital certificate; later the system verifies if the document is valid

by consulting a list of invalidated documents (Document verification process), if the document is valid, the transaction is registered, and the process is performed to generate the corresponding hash and enter it into the Merkle tree. After 2 minutes ± 30 seconds mining nodes of the blockchain network validate and record the transaction into a block of the blockchain database. When the transaction is validated, the last hash corresponding to the root of the Merkle tree that contains the last transaction, will be stored in a secure area of the chip.

In addition, for the document bearer to be able to carry out a transaction or access to the information contained in the chip, it is necessary a certified reader intended to be in registers and notaries. Additionally, to authenticate the user, the biometric features are used performing a template matching algorithm. Finally, a verification of the document authenticity is performed by comparing the last hash stored in the document chip with one of the hashes stored into blockchain database. In order to generate a valid hash into the chip document, the registration process is considered itself as a first valid transaction, avoiding the fact people will not perform other kind of transactions.

Each time that a citizen makes a categorized transaction Fig. 5, it will be registered using a hash function as a part of the merkle tree, in this way, it is possible to offer privacy because the user chooses a nickname when the document is issued to protect his identification, and generating an associated PIN to perform transactions.

The document consists of two identification numbers: a serial number, unique for each document and an identification number, unique to each user, in the case of taking a duplicate this number does not change, but the serial number will change.

In the case of theft or loss of an e-ID, the person must go to a registry entity, where he will request a duplicate of his document. In this case the registry will generate a report with the serial number of the lost document, and the revocation list will be updated, so no one who keep the document with that serial number will be able to make some transactions. The person who asked for a duplicate will get his new document containing a new serial number, generating a new transaction in the blockchain database with his own identification number in order to make traceability of the transactions with the previous document.

In case of death of a citizen, a death certification is issued and reported to a notary, which generates a report disabling the corresponding document. In other words, the revocation list will be also updated in this scenario, avoiding fraudulent transactions.

IV. Future Work

Based on the proposed document model, it is intended to implement a case study in the Pontificia Universidad Javeriana at Bogotá, Colombia by providing an e-ID which will bring additional user benefits. Among these benefits are the identification of the students that allows them to make use of the services that the university gives, as for instance, the use of lab equipment like personal computers, parking and library access.

The implementation of the case study, pretends to verify some variables in order to adjust them, such as the size of the blocks and the time range, likewise the complexity of the requirement for the header hash, avoiding to delay the identification and authentication process. In addition, it will allow to evaluate the security features of the proposed model, verifying the processes of identification, user and document authentication, and transactions validation. Subsequently, the model and the prototype will be proposed to the National Registry of Civil Status, as responsible government entity for issuance of identity documents for Colombian people.

V. Conclusion

A novel electronic Identity Document model is presented in this work. The model overcome existing security issues of the national identification document in Colombia. The use of a blockchain network combined with biometric authentication technology can potentially solves several security issues in terms of citizen's information protection and fraudulent transactions avoiding identity theft and electoral fraud. It also gives the authorities the possibility of validate the document, recognizing digitally if the document presented is false or disabled.

The proposed model is not only intended to use the blockchain technology for the document authentication process. But it also proposes the use of a PIN and biometric authentication (iris recognition and fingerprints), in order to verify the bearer authenticity by using the concept of strong authentication, where three factors are combined, something that the user has (e-ID), *something the user knows* (PIN), *something the user is* (Biometrics), *generated a secure user authentication.*

References

[1] IBM Offering Information. [Online]. Available: https://www-01.ibm.com/common/ssi/cgibin/ssialias?htmlfid=XI912346USEN

[2] M. E. Peck, "Blockchains: How they work and why they'll change the world," *IEEE Spectrum*, vol. 54, no. 10, pp. 26–35, 2017.

[3] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[4] T. Bocek, B. B. Rodrigues, T. Strasser, and B. Stiller, "Blockchains everywhere - a use-case of blockchains in the pharma supplychain," in *Proc. 2017 IFIP/IEEE Symposium on Integrated Network and Service Management*, 2017, pp. 772–777.

[5] R. Rivera, J. G. Robledo, V. M. Larios, and J. M. Avalos, "How digital identity on blockchain can contribute in a smart city environment," in *Proc. 2017 International Smart Cities Conference (ISC2)*, 2017, pp. 1–4.

[6] Registraduria Civil. Registraduria Nacional del Estado Civil – Identificación. [Online]. Available: http://www.registraduria.gov.co/-Identificacion,3685-.html

[7] A. Poller, U. Waldmann, S. Vowé, and S. Turpe, "Electronic identity cards for user authentication-promise and practice," *IEEE Security and Privacy*, vol. 10, no. 1, pp. 46–54, 2012.

[8] Registraduria Civil. Información para trámites de Cédula de Ciudadanía. [Online]. Available: http://www.registraduria.gov.co/-Cedula-de-Ciudadania,3689-.html

[9] Policia Nacional De Colombia. [Online]. Available: https://www.policia.gov.co/noticia/capturado-un-hombre-quetena-en-su-poder-de-60-cdulas-de-ciudadana

[10] Policía Nacional De Colombia.Cerca de 6 millones de pesos perdió un ciudadano por descuido. [Online]. Available: https://www.policia.gov.co/noticia/cerca-de-6-millones-de-pesosperdi-un-ciudadano-por-descuido

[11] R. Santus. Hackers claim they can copy fingerprints from photos. [Online]. Available: https://mashable.com/2014/12/29/fingerprint-photo-copy/#2dVVvRlksgqq

[12] M. A. Haque, N. Z. Khan, and G. Khatoon, "Authentication through keystrokes: What you type and how you type," in *Proc. 2015 IEEE International Conference on Research in Computational Intelligence and Communication Networks*, 2016, pp. 257–261.
[13] R. Rivera, J. G. Robledo, V. M. Larios, and J. M. Avalos, "How digital identity on blockchain can contribute in a smart city environment," in *Proc. 2017 International Smart Cities Conference (ISC2)*, pp. 1–4,2017.
[14] C. Sullivan and E. Burger, "E-residency and blockchain," *Computer Law and Security Review*, vol. 33, no. 4, pp. 470–481, 2017.
[15] H. Hou, "The Application of Blockchain Technology in E-Government in China," in *Proc. 2017 26th International Conference on Computer Communication and Networks (ICCCN)*, pp. 1–4, 2017.
[16] B. Hoang and A. Caudill, "Biometrics," *Tech. Rep*., 2012.
[17] National Science and Technology Council, "Biometrics in Government POST-9/11," *Tech. Rep*., 2008.
[18] A. Jain, J. Feng, and K. Nandakumar, "Fingerprint matching," *Computer*, vol. 43, no. 2, pp. 36–44, 2010.
[19] S. Liu and M. Silverman, "Practical guide to biometric security technology," *IT Professional*, vol. 3, no. 1, pp. 27–32, 2001.
[20] S. H. Moi, N. B. A. Rahim, P. Saad, P. L. Sim, Z. Zakaria, and S. Ibrahim, "Iris biometric cryptography for identity document," *SoCPaR 2009 - Soft Computing and Pattern Recognition*, 2009, pp. 736–741.
[21] J. Wayman, A. Jain, D. Maltoni, and D. Maio, *Biometric Systems*, 2005.
[22] P. Jayachandran, The difference between public and private blockchain. [Online]. Available: https://www.ibm.com/blogs/blockchain/2017/05/the-differencebetween-public-and-private-blockchain/
[23] Registraduria Civil. Censo Electoral. [Online]. Available: http://www.registraduria.gov.co/-Censo-Electoral,3661-.html
[24] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Proc. 2007 44th ACM/IEEE Design Automation Conference*, 2007, pp. 9–14.
[25] M. D. Yu and S. Devadas, "Secure and robust error correction for physical unclonable functions," *IEEE Design Test of Computers*, vol. 27, no. 1, pp. 48–65, 2010.

Juan C. Montes D. was born in Bogotá, D.C, Colombia, in 1994.

He received his B.E (2017) in electronics engineering from the Pontificia Universidad Javeriana, Bogotá, Colombia.

His main research areas are the telecommunications systems, software defined networking (SDN), internet of things (IoT) and contactless smartcards (RFID, NFC).

Andrés R. Piñeros was born in Bogotá, Colombia on July 15, 1994. He got his bachelor's degree in Emmanuel d´Álzon School in 2012 in Bogotá, Colombia. He finishes the Pontificia Universidad Javeriana, the faculty of engineering and systems engineer department in 2017 in Bogotá Colombia.

He was a teaching assistant in programming class, he solved students' doubts associated with the syntax of the programming language at Pontificia Universidad Javeriana. He is a designer and developer in a Research group at Pontificia Universidad Javeriana, he began works in April of 2017 to the actually in the design of a National Electronic Identity Document (e-ID) for the Colombian context and also develop this solution in smart cards.

Rafael V. Páez is a systems engineer from the Catholic University of Colombia (Bogotá) on 2001, and he carried out graduate studies in security of data processing networks (2002) at the Catholic University of Colombia. He has a PhD in telematics engineering from Technical university of Catalonia (Spain). He is an associate professor at Pontificia Universidad Javeriana and director of research group SiDRe. His main research areas are the security of data processing networks, Information security, Intrusion Detection Systems (IDS), Public Key Infrastructure (PKI), and perimeter security.

Gustavo A. Ramirez E. received the B.S. and M.Sc. degrees in electronic enginieering from the Pontificia Universidad Javeriana of Bogotá, Colombia, in 2010 and 2013, respectively. He is currently a full time professor at the Electronics Department of Pontificia Universidad Javeriana.

His research interests include network security, internet of things; software defined networking, and embedded systems for networking.

Manuel R. Pérez C. was born in Tunja, Boyaca, Colombia, in 1986.

He received his Ph.D (2013) in electronics and communications engineering and his M.Sc (2009) in wireless communications from the Politecnico di Torino, Italy, and his B.E (2010) in electronics engineering from the Pontificia Universidad Javeriana, Bogotá, Colombia, as part of a double degree Program with the Politecnico di Torino.

From 2009 to 2013, he was a research assistant with the iXem Labs (Politecnico di Torino) and the Laboratorio di Antenne e Compatibilita Elettromagnetica (LACE) at the Istituto Superiore Mario Boella (ISMB), Torino, Italy. Since 2013 he has been an Assistant Professor with Electronics Department, Pontificia Universidad Javeriana. He has been also actively collaborated with the *Centro de Excelencia y Apropiación en Internet de las Cosas (CEA- IoT)* as a team director in the areas of Wearables, Smart Cities, and Safety, working in several I+D+i projects. His research interests also include Computational Electromagnetics (CEM), design of antennas, radar, Software Defined Radio (SDR), High Performance Computing (HPC) and Electromagnetic Compatibility.