

Blockchain project for eID

Department of Systems Engineering, Universidad Javeriana

Bogotá

Lucas Bouvarel

Directed by Rafael V. Páez

Contents

[Project Description 2](#_Toc7458880)

[Class Diagram 4](#_Toc7458881)

[Process of a transaction: 6](#_Toc7458882)

[Consensus algorithm 7](#_Toc7458883)

[References 9](#_Toc7458884)

# Project Description

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].

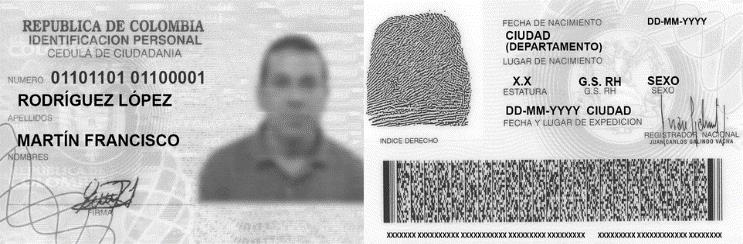


Figure 1 : Colombian ID [7]

The element that contains the information of a person to be identified, is known as a National Identity Document (ID) (Figure 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 [8]. 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 [9]. Another common problem in Colombia is electoral fraud, where deceased person’s ID are used to validate fraudulent votes.

In the current identity document (Figure 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 [10].

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 by encrypting personal data, besides of giving access to novel online services for citizens [11] 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 generates 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.

In this paper we will describe the Blockchain’s code implemented for this new concept of e-ID.

# Class Diagram

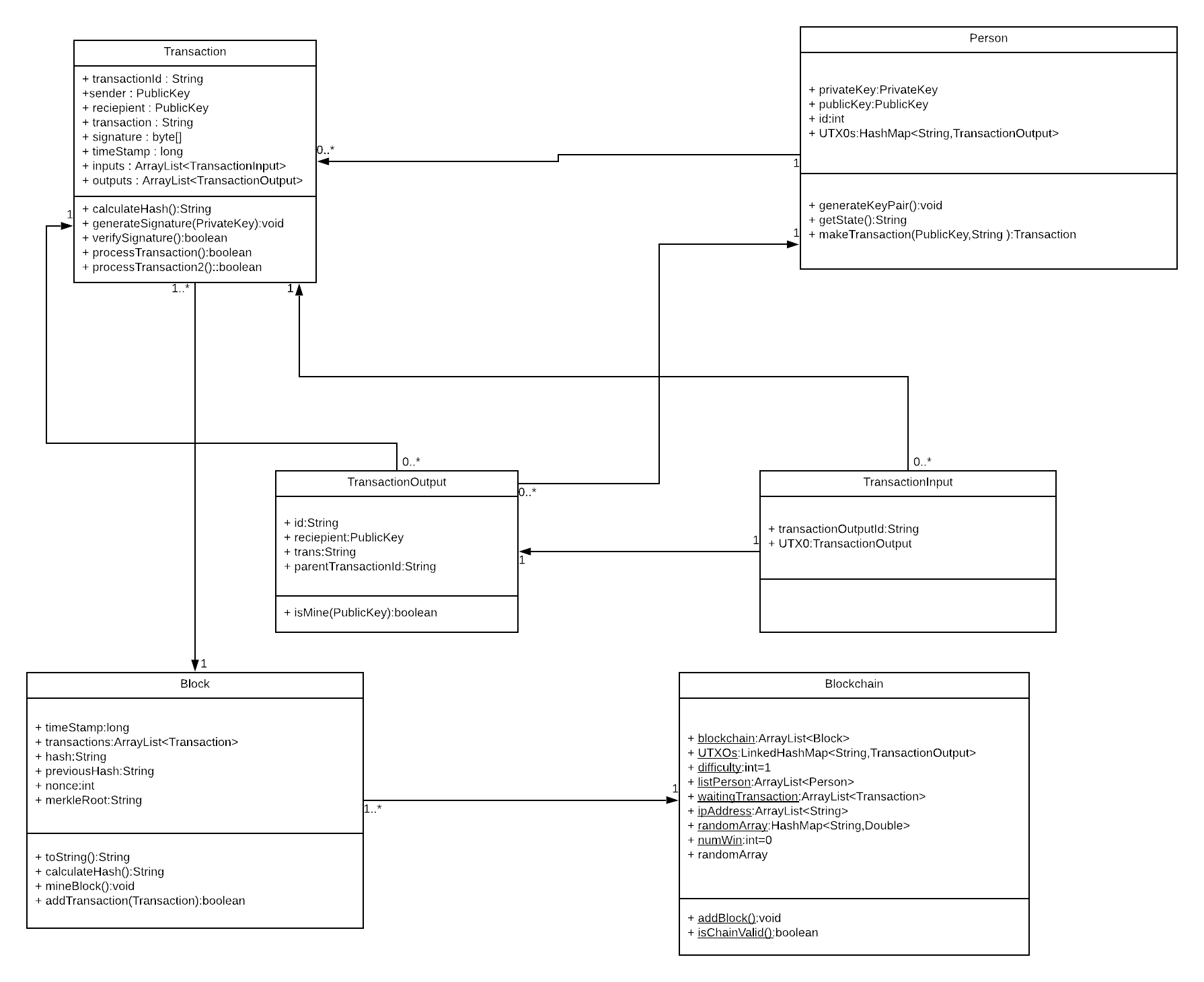


Figure 2: Class diagram



Figure 3: Person.java



Figure 4: Transaction.java



Figure 5: TransactionOutput.java



Figure 6: TransactionInput.java



Figure 7: Block.java

Blockchain.java is the main class that create the Blockchain and the genesis transaction.

It contains every global variable:

* UTXOs : contains every output transaction of every person
* connectedList : contains the nodes that are connected and participate at the blockchain
* ipAddress: contains the ipAddress of all the authorized node that can join the blockchain
* waitingTransaction : the transaction that wait to be added to a block
* randomArray : used for the consensus algorithm

Library used

bouncycastle bcprov-jdk15on-159 <https://www.bouncycastle.org/latest_releases.html>

# Process of a transaction:

1. A person creates a transaction
   * Gather from UTXOs global variable the output that belongs to this person and add them to the personal list UTXO
   * Control if the transaction is possible (If there is a modification of the current state of the person
   * Add the input of the transaction i.e the output’s reference of the UTXO personal list/global variable
   * Create the transaction’s signature with the private and public key
   * Remove every transaction output from the UTXO personal list
   * Add the transaction to the transaction waiting list
2. Broadcast the transaction to every connected node

\*\*\*TORNEO Consensus Algorithm\*\*\*

1. The winner elected by every node add the block to the blockchain:
   * Verify if there are transaction in the waiting list
   * Create a block

For every transaction in the waiting list:

* + Check the signature of the transaction
  + Gather the transaction outputs from the UTXOs global variable thanks to the reference in the input of the transaction
  + Generates the transaction output of the transaction
  + Add these outputs to the UTXOs global variable
  + Remove every transaction’s input to the UTXOs global variable
  + Add the transaction to the block

1. Broadcast the blockchain and the UTXOs global variable to every connected node
2. The nodes which receive the new blockchain check the validity of it

# Consensus algorithm

In this section we present a new consensus algorithm based on the Proof of Luck [10]. It has been modified in order to simplify the implementation and adapt it to be suitable for a private blockchain. Indeed, in Proof of Luck, trusted execution environments are used to be sure that a node is executing the well code and that it is not intending to attack the Blockchain. As we are in an environment where the nodes can be considered as trustful, we do not need theses trusted environments anymore.

When a node wants to join the blockchain he asks the right for by sending a request to every node. If the node is confirmed as authorized, he will receive the blockchain, the right to create transaction and the right to try to add the next blocks. Every 15 seconds (this time can be changed), a request is sent to every connected node to pick randomly a number between 0 and 1. Every node will broadcast this number and wait to receive every random number. When a node has received every random number, he selects the biggest one and sends to the node who had selected this number a “winner vote”. When a node has received as many “winner vote” as the number of connected nodes, it means that he is the winner and he has the right to add the next block. Then the node has to mine the block in the same way as a proof of work consensus algorithm but with a very low difficulty allowing a normal computer to find the nonce value in less than a second. In this way the loss of time and the energy waste are avoided.

A few tests have been made in network between two computers to see the efficiency of this consensus algorithm. In these tests, one transaction is a little character chain. In Figure 8 we can see that the time needed to broadcast x transactions increases linearly as the number of transaction increases too. It takes approximately 1,2 seconds to create and broadcast 1000 transactions.



*Figure 8: Time needed to broadcast x transactions*



*Figure 9: Time needed to mine one block with x transactions and broadcast it*

In Figure 12 we also see that it takes only a few milliseconds to broadcast a block with a lot of transactions.

Future work.

In order to have more significant tests, we should try this consensus algorithm with more than 2 computers to see how the time increased and we should also try to do it through the internet and not only in LAN. Every node writes into a file every block they receive. But, for now, we didn’t implement the code that permits to read this file so in case that every node is disconnected, we will have to implement something that gather the blockchain in this file. Currently, the person database is static and stored in the ram. We will have to create a dynamic database that is stored in hard disk and that is common to every node.

# References

|  |  |
| --- | --- |
| [1] | IBM offering Informations, «Blockchain,» 2017. [En ligne]. Available: https://www- 01.ibm.com/common/ssi/cgibin/ssialias?htmlfid=XI912346U SEN. |
| [2] | M. E. Peck, «Blockchain: How they work and why they'll change the world,» *IEEE Spectrum,* vol. 54, n° %110, pp. 26-35, 2017. |
| [3] | K. C. a. M. Devetsikiotis, «Blockchain and Smart Contracts for the Internet of Things,» *IEEE Access,* vol. 4, pp. 2292-2303, 2016. |
| [4] | B. R. T. S. a. B. S. T. Bocek, «Blockchain everywhere - a use-case of blockchain in the pharma supplychain,» *IFIP/IEEE Symposium on Integrated Network and Service Management (IM),* pp. 772-777, 2017. |
| [5] | J. G. R. V. M. L. a. J. M. A. R. Rivera, «How digital identity on blockchain can contribute in a smart city environment,» *Internation Smart Cities Conference,* pp. 1-4, 2017. |
| [6] | Registraduria Civil, «Registraduria Nacional del Estado Civil - Identificación,» 2017. [En ligne]. Available: http://www.registraduria.gov.co/-Identificacion,3685-.html. |
| [7] | Registraduria Civil, «Información para trámites de Cédula de Ciudadania,» 2017. [En ligne]. Available: http://www.registraduria.gov.co/-Cedula-de- Ciudadania,3689-.html. |
| [8] | POLICIA NACIONAL DE COLOMBIA, «Capturado un hombre que tenía en su poder de 60 cédulas de ciudadanía,» 2015. [En ligne]. Available: https://www.policia.gov.co/noticia/capturado-un-hombre- quetena-en-su-poder-de-60-cdulas-de-ciudadana. |
| [9] | Policia Nacional de Colombia, «Cerca de 6 millones de pesos perdió un ciudadano por descuido,» 2015. [En ligne]. Available: https://www.policia.gov.co/noticia/cerca-de-6-millones-de- pesosperdi-un-ciudadano-por-descuido. |
| [10] | R. Santus, «Hackers claim they can copy fingerprints from photos,» 2014. [En ligne]. Available: https://mashable.com/2014/12/29/fingerprint-photo- copy/#2dVVvRlksgqq. |
| [11] | U. W. S. V. a. S. T. A. Poller, «Electronic identity cards for user authentication-promise and practice,» *IEEE Security and Privacy,* vol. 10, n° %11, pp. 46-54, 2012. |
| [12] | N. Z. K. a. G. K. M. A. Haque, «Authentication through keystrokes: What you type and how you type,» chez *Proceedings of 2015 IEEE International Conference on Research in Computational Intelligence and Communication Networks*, 2015, 2016. |
| [13] | W. H. H. W. a. M. K. M. Milutinovic, «Proof of Luck: an Efficient Blockchain Consensus Protocol,» 2017. [En ligne]. Available: https://arxiv.org/pdf/1703.05435.pdf. |