

A Blockchain-based Educational Record Repository

ILLUSTRATED TECHNICAL PAPER

Emanuel E. Bessa
Salvador University - UNIFACS, Brazil

Joberto S. B. Martins
Salvador University - UNIFACS

Abstract

This "**ILLUSTRATED TECHNICAL PAPER**" presents the slides describing the contents of the paper "A Blockchain-based Educational Record Repository".

The talk was presented at **7th International Workshop on ADVANCEs in ICT Infrastructures and Services - ADVANCE 2019**, 21 - 22 January 2019 at Praia, Cape Vert.

The "illustrated technical paper format" is intended to complement, enrich and subsidize the technical paper content and contains slides, complementary text and additional and/or focused bibliographic references.

Index Terms

Blockchain, Educational Records, Educational Repository, e-Diploma, e-Certificate, BcER².




1 PAPER ABSTRACT

The Blockchain technology was initially adopted to implement various cryptocurrencies. Currently, Blockchain is foreseen as a general purpose technology with a huge potential in many areas. Blockchain-based applications have inherent characteristics like authenticity, immutability and consensus. Beyond that, records stored on Blockchain ledger can be accessed any time and from any location. Blockchain has a great potential for managing and maintaining educational records. This paper presents a Blockchain-based Educational Record Repository (BcER²) that manages and distributes educational assets for academic and industry professionals. The BcER² system allows educational records like e-diplomas and e-certificates to be securely and seamlessly transferred, shared and distributed by parties.

-
- Emanuel E. Bessa is with Salvador University - UNIFACS, Brazil. E-mail: emanuel.bessa@hotmail.com
 - Prof. Dr. Joberto Martins is with Salvador University - UNIFACS, Brazil. E-mail: joberto.martins@gmail.com

2 PAPER SLIDES

ADVANCE' 2019

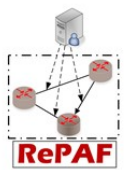

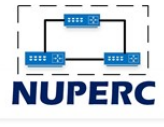


Praia, Cape Verde
 January 21th – 22th 2019

A Blockchain-based Educational Record Repository

Emanuel E. Bessa

Prof. Joberto S. B. Martins

01/06/2019
7th International Workshop on ADVANCES in ICT Infrastructure and Services
1

Fig. 1.

-- > **PAPER TEXT EXTRACT:**

This article presents **BcER²**, a blockchain-based Educational Record Repository that manages and distributes educational assets for academic and industry professionals [1].

Authors argue that "the BcER² system allows educational records like e-diplomas and e-certificates to be securely and seamless transferred, shared and distributed by parties."

-- > **Paper to read:**

- The full paper text describing BcER² system is "**A Blockchain-based Educational Record Repository**" and is available at:
 - * ZENODO: <https://zenodo.org/record/2567524>
 - * Research Gate: https://www.researchgate.net/publication/331162617_A_Blockchain-based_Educational_Record_Repository

-- > **Complementary papers on BAM configuration, operation and management:**

- Blockchain main characteristics are described in [2] [3] [4] [5] [6] [7] [8]



Agenda

- Blockchain Technology in Education & Motivation
- Blockchain-based Educational Records Repository (**BcER²**)
Architecture and Components
- Final Considerations

01/06/2019

7th International Workshop on ADVANCES in ICT Infrastructure and Services

2

Fig. 2.

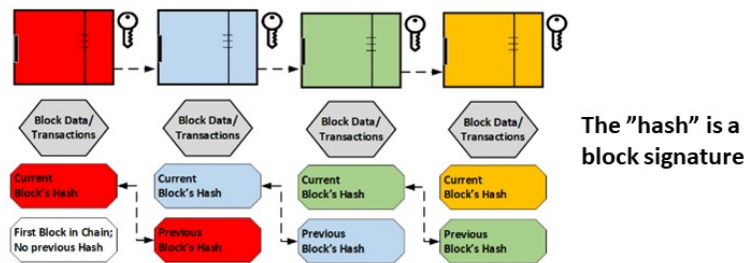
-- > **PAPER TEXT EXTRACT:**

"The paper [1] is organized as follows. Section 2 summarizes the fundamental aspects of Blockchain technology. Section 3 indicates the relevant work being done related to Blockchain and BcER² system. Section 4 describes the architecture, entities, components and implementation of the BcER² system. Section 5 presents a proof-of-concept of the BcER² implementation. Finally, section 6 presents the final considerations and future work."



Blockchain & Education:

- Blockchain
 - Technology behind cryptocurrencies and smart contracts (various areas)
 - Blockchains is a digital distributed ledger implementation
 - Blockchains can be also described as a register on which everyone can write, but cannot erase and/or destroy
 - Blockchains are decentralized and distributed



- May potentially support application development in many distinct areas

01/06/2019

7th International Workshop on ADVANCES in ICT Infrastructure and Services

3

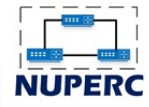
Fig. 3.

— > PAPER TEXT EXTRACT:

"A blockchain is essentially a distributed database of records that keeps potentially all kind of data, like transactions, contracts and events. All information handling takes place across a peer-to-peer network and is maintained chronologically in digital blocks. These basic features and capabilities make Blockchain transparent, secure, decentralized and with almost unlimited storage capacity [6]."

"Blockchain uses the concept of hashing. The "hash" is a block signature and considers all data and transactions involved. In summary, a cryptography hash function takes a input string and turns it into a unique n-digit string [8]. Figure 3 illustrates how blocks are chained in Blockchain."

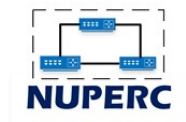
"With traditional methods for recording transactions and tracking assets, participants on a network keep their own ledgers and other records. This traditional method can be expensive, partially because it involves intermediaries that charge fees for their services. It's clearly inefficient due to delays in executing agreements and the duplication of effort required to maintain numerous ledgers. It's also vulnerable because if a central system (for example, a bank) is compromised due to fraud, cyberattack, or a simple mistake, the entire business network is affected. To solve or improve traditional method Blockchain has a set of key characteristics: consensus, provenance, immutability and finality [8] [4]."





Motivation:

- Educational records are used worldwide and, from the student or professional point of view, is an important asset for individuals pledging for scholarships, jobs and professional and academic visibility
- Education has global impact and coverage and information concerning everyone's education should flow as easily as possible
- Secure, immutable and trustable **educational records** are necessary on a global basis
- Generalized access is potentially important (web access)



01/06/2019

7th International Workshop on ADVANCES in ICT Infrastructure and Services

4

Fig. 4.

-- > PAPER TEXT EXTRACT:

"An "education record" in the context of this paper is a record containing files, documents, and other materials which [8]: i) Contains information directly related to the academic historical of a student or a professional; and ii) From a local perspective are typically maintained by an educational institution or by other entity acting for such institution."

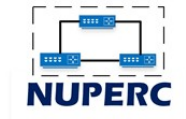
"There are significant advantages and benefits in using a Blockchain-based educational repository [5] [9]: i) Educational records (e-diplomas, e-certificates, other) uploaded and managed on the Blockchain ledger are more secure and resistant to "physical wear and tear" than paper documents [5]; ii) Educational records are seamless and efficiently transferred and shared among parties (universities, schools and employers) fostering worldwide visibility; and iii) Educational records stored on the blockchain can be accessed any time, from any location."

"In summary, educational records managed by Blockchain technology stimulate the knowledge/reward principle, makes credentials more trustworthy and keeps educational records safe and easy to access [5]."



Blockchain Characteristics & BcER² Education Application

- Distributed & decentralized
- Authentic
- Immutable
- Eliminates intermediaries
- Easy access



6/1/2019

7th International Workshop on ADVANCES in ICT Infrastructure and Services

5

Fig. 5.

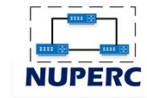
- **PAPER TEXT EXTRACT:**

"All relevant participants make decisions by consensus, in this process most participants must agree that a transaction is valid. This goal is achieved through the implementation of consensus algorithms. Each network enforces the conditions under which transactions are performed or the exchange of assets may occur. Provenance guarantees that participants know where the asset came from and how its ownership has changed over time. With immutability, no participant can tamper with a transaction after it has been recorded to the ledger. If a transaction is in error, a new transaction must be used to reverse the error, and both transactions are then visible. With finality, a single shared ledger provides one place to go to determine the ownership of an asset or the completion of a transaction."



Educational Record (asset)

- Information directly related to the academic historical of a student or a professional
- From a local or institutional perspective are typically maintained by an educational institution or by other entity acting for such institution
- Prototype implementation: course certificate and diplomas (e-diploma and e-certificates)



6/1/2019

7th International Workshop on ADVANCEs in ICT Infrastructure and Services

6

Fig. 6.

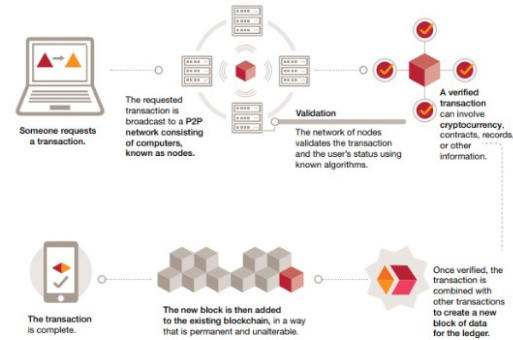
— > **PAPER TEXT EXTRACT:**

"An "asset" can be anything of value that will be kept securely by the educational repository. Educational records like certificates, diplomas, educational records and similar documents are BcER² assets."



Blockchain-based Educational Records Repository – Operation Flow

- Consortium blockchain structure
- Only authorized persons are able to create certificated records
- Anyone can verify/ access



6/1/2019

7th International Workshop on ADVANCES in ICT Infrastructure and Services

7

Fig. 7.

-- > PAPER TEXT EXTRACT:

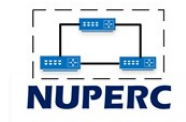
"In order to meet the different alternatives of use, blockchain-based applications can be implemented using 3 types of general structures as follows [4]: i) Public Blockchain; ii) Private Blockchain; and iii) Consortium Blockchain."

"The type of Blockchain structure to be used strongly depends on the application. The BcER² repository adopted the consortium system since only authorized persons are able to create certificates records on the network. On the other hand, anyone can verify their authenticity. Thus, when registering an educational record, for example, the responsible for creating the record writes in the registry or in the database using its own private key. Users who want to check the veracity of the record must have a corresponding identifier number to be inserted into the system."



Blockchain-based Educational Records Repository – Entities

- Assets
- Registers
- Transactions
- Participants



01/06/2019

7th International Workshop on ADVANCES in ICT Infrastructure and Services

8

Fig. 8.

— > PAPER TEXT EXTRACT:

"The entities belonging to the BcER² educational repository are the following: i) Assets; ii) Registers; iii) Transactions; and iv) Participants."

"An "asset" can be anything of value that will be kept securely by the educational repository. Educational records like certificates, diplomas, educational records and similar documents are BcER² assets."

"Participants are the educational organization representatives, students and people in general that are somehow interested in either distributing or accessing educational records. Participants are defined in the "business network model" adopted by the blockchain application process. For BcER², coordinators, students, and anyone else interested in having access to the educational records are the participants belonging to the network. Each one has their specifically assigned functions, responsibilities and access restrictions."

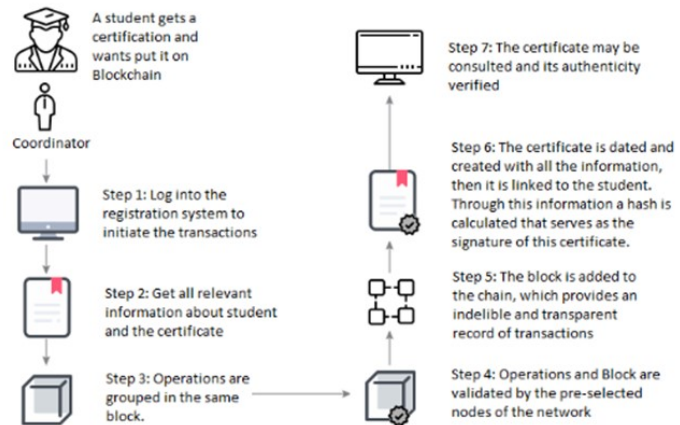
"Transactions are submitted by participants to create or access the assets held in the blockchain-based asset registries on the blockchain ledger. Transactions, in general, do belong to a business network and, as such, do require a "business network model". The business network model, from the blockchain system perspective, defines the operation involved with the assets."

"Registers can be defined as the set of data that involve the assets, transactions and the participants. This set is what will be included in the block after the validation. Registers are new information that is added to the blockchain ledger."



Blockchain-based Educational Records Repository

• Operation flow



01/06/2019

7th International Workshop on ADVANCES in ICT Infrastructure and Services

9

Fig. 9.

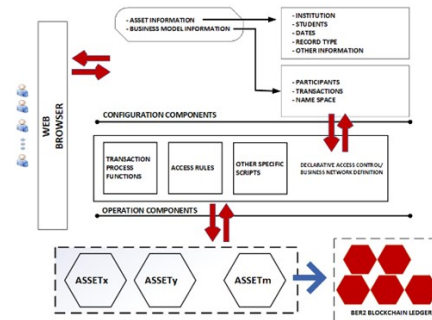
-- > PAPER TEXT EXTRACT:

"The BcER² effective structure uses the basic steps and operation flow of a blockchain-based application as illustrated in Figure 9: i) A transaction is requested by someone who has prior authorization and needs to create an educational record; ii) The request record transaction is sent to the nodes belonging to the BcER² system; iii) The educational record transaction is verified by the ledger; and iv) A new block of data corresponding to the educational record transaction is accessed or created and annexed to the ledger becoming permanent and immutable completing the transaction."



Blockchain-based Educational Records Repository - Components

- Based on “Hyperledger Composer” (implementation)
- Application model:
 - Asset information
 - Business Model Information (participants, name space and transactions involved)
 - Transaction Process Function
 - Access rules



6/1/2019

7th International Workshop on ADVANCES in ICT Infrastructure and Services

10

Fig. 10.

— > PAPER TEXT EXTRACT:

"The basic components belonging to the the BcER² educational records repository are illustrated in Figure 10 and basically reflect the business network adopted which is suitable for an educational records repository that registers, manages and provide access to them."

"The "asset information" component contains information related to the educational record being managed by BcER². This component is responsible for asset's definition and consistency."

"The "Business Model Information" component contains information related to the process involved in the asset management. It defines basically the participants, name space and transactions involved in the process."

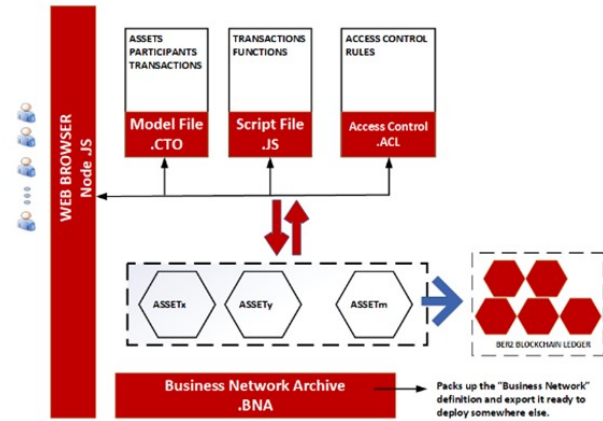
"The "Transaction Process Function" component contains the information concerning the specif functions invoke in the business model to manage the asset."

"The "Access Rules" component contains, as the name suggests, the access rules including all priorities among participants involved in the business model adopted."



Blockchain-based Educational Records Repository - Implementation

- “Hyperledger Composer”
Prototype implementation
(java)



6/1/2019

7th International Workshop on ADVANCES in ICT Infrastructure and Services

11

Fig. 11.

— > PAPER TEXT EXTRACT:

"The Hyperledger Composer [7] was used to implement the BcER² educational repository (Figure 11). Hyperledger Composer is an open source development tool set and framework aiming to support the development of blockchain applications. It allows the modeling of the business network and integrates existing systems components and data deploying as such the blockchain application."

"BcER² is composed of assets, participants and transactions, with each of these entities being represented within Hyperledger framework as configuration files (Figure 11)."

"The .CTO hyperledger component is responsible for implementing the assets, participants, and transactions, including all relevant information. A Hyperledger Composer CTO file is composed of the following elements: i) A name-space with resources declaration; ii) Resources definition including assets, transactions, participants and events; and iii) Optional resource import declarations from other name-spaces."

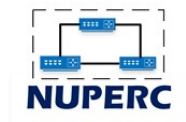
"The .ACL hyperledger component provides declarative access control for the elements in the domain model. By defining access and control (ACL) rules you can determine which users/roles are permitted to create, read, update or delete elements in a business network's domain model."

"The 'Business Network' definition, from the Hyperledger Composer perspective, is composed by a set of model files defining assets, participants and transactions (Figure 11). The ".JS" script file is responsible for maintain a set of scripts. The scripts contain transaction process functions that implement the transactions defined in the 'Business Model'. Transaction processing functions are automatically invoked at run-time when transactions are submitted and their structure are composed by a JavaScript function."



Proof-of-Concept

- Salvador University complementary course certificates (prototype implementation)
- Creating Assets
- Accessing them and verifying the effectiveness of credentials and other distribution and immutability aspects



01/06/2019

7th International Workshop on ADVANCES in ICT Infrastructure and Services

12

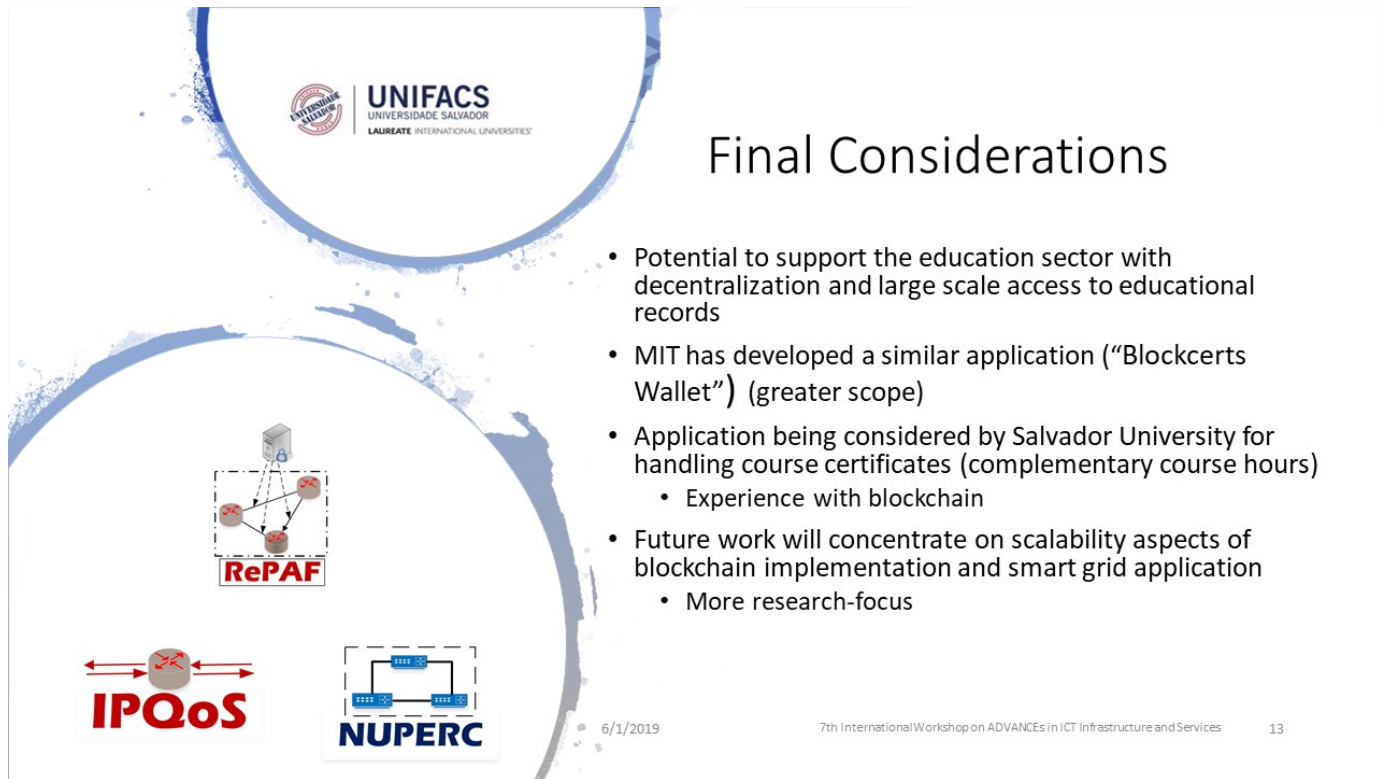
Fig. 12.

— > PAPER TEXT EXTRACT:

"The main objective of the BcER² repository proof-of-concept is to validate the deployment of the business network and verify the operation steps of the repository by: i) Creating assets; and ii) Accessing them and verifying the effectiveness of credentials and other distribution and security aspects."

"The proof-of-concept of the BcER² repository operation was implemented by emulating participants as follows: i) 'Users' are the general public accessing educational records; and ii) The 'Coordinator' (Register Authority) is a UNIFACS authority creating educational record entries."

"The proof-of-concept method and parameters used to validate the operation of BcER² was the creation of a set of educational records followed by authenticity verification and access by the system administrator and distributed users. The experimental setup included the creation of 10 different educational records with course certificates and various nodes (N>10) simulating different users acting on the validation process (transactions) and verifying their authenticity. The results allowed the distributed access to educational records enabling verification through blockchain technology. Security access was also validated by trying to access educational records without the adequate credential. The scalability of the solution was not evaluated and will be addressed by future work."



Final Considerations

- Potential to support the education sector with decentralization and large scale access to educational records
- MIT has developed a similar application ("Blockcerts Wallet") (greater scope)
- Application being considered by Salvador University for handling course certificates (complementary course hours)
 - Experience with blockchain
- Future work will concentrate on scalability aspects of blockchain implementation and smart grid application
 - More research-focus

6/1/2019

7th International Workshop on ADVANCES in ICT Infrastructure and Services

Fig. 13.

-- > **PAPER TEXT EXTRACT:**

"In the current scenario, the proposed application covers only the UNIFACS network for the purpose of managing diplomas and certificates issued by the university. The BcER² application has the potential to cover additional areas in which digital certificates provide interesting opportunities such as [10]: i) Corporate Training - Many large companies offer a multitude of training opportunities to their employees, but lack the systems to track and store results reliably. Current human resources systems often do not interact with corporate databases and there are no consistent standards for comparing skills and accomplishments; and ii) Workforce Development - There are millions of records and learning certificates, but there are no systems to manage them. This is especially a problem for people with low qualifications, who often do not have recognized diplomas or degrees."

"In terms of future work, it is intended to evaluate the scalability issues and impacts associated with the deployment of a huge repository. Another aspect to be considered is to bring together stakeholders such as employers, students, teachers and contractors in a way that they interact with each other enabling wide-spread use of trustable e-certificates. A final target will be to adopt a fully standardized asset representation as an additional step towards a secure and decentralized way of conferring a wide-spread use of the system."



Obrigado

Discussion and Questions

Contacts:

Prof. Dr. Joberto S. B. Martins - joberto.martins@gmail.com

Slides available at:

--- Research Gate (Joberto Martins): https://www.researchgate.net/profile/Joberto_Martins

--- Academia (Joberto Martins): <https://unifacs.academia.edu/JobertoMartins>



Fig. 14.

— > **PAPER TEXT EXTRACT:**

"Authors thanks FAPESB (Fundação de Apoio à Pesquisa do Estado da Bahia) by the scientific initiation (IC) scholarship support."

Prof. Dr. Joberto S. B. Martins

PPGCOMP

- ◆ Current position: Full Professor at Salvador University - UNIFACS and visiting professor at Hochschule Für Technik und Wirtschaft Des Saarlandes - HTW – Saarbrücken, in Germany.
- ◆ PhD in Computer Science, UPMC, Paris – France, 1986; M.Sc. in Electronic Engineering, PII, Eindhoven – Netherlands, 1979
- ◆ Worked as visiting scientist at ICSI – California University at Berkeley (USA) in 1995; PosDoc at Paris Saclay - Évy University – Paris – 2016
- ◆ Member of IEEE Research Committee on Smart Grid and IEEE Technical Activities Committee on Smart Cities
- ◆ Additional information: see “Joberto Martins” on Google



Fig. 15.

REFERENCES

- [1] Emanuel E. Bessa and Joberto S. B. Martins. A Blockchain-based Educational Record Repository. In *ADVANCE 2019 - International Workshop on ADVANCEs in ICT Infrastructures and Services*, pages 1–8, Cape Vert, January 2019. Université Paris-Saclay Évry.
- [2] Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. page 9, 2008.
- [3] Habib Azam. What are the different generations of blockchains?, January 2018.
- [4] Sanjaya Baru. Blockchain: The next innovation to make our cities smarter. page 48, January 2018.
- [5] Institute of BlockchainTM. Blockchain and Education, June 2018.
- [6] Michael Crosby. BlockChain Technology: Beyond Bitcoin. (2):16, 2016.
- [7] Linux Foundation. Introduction | Hyperledger Composer.
- [8] Alexander Grech and Antony F. Camilleri. Blockchain in Education. Technical Report EUR 28778 EN, European Union, Luxembourg, 2017.
- [9] Raza Sheeraz. Blockchain Can Help People Keep Their Educational Records Intact, May 2018.
- [10] MIT Media Lab. Certificates, Reputation, and the Blockchain, October 2015.



Emanuel Estrela Bessa - Computer science student at Salvador University (UNIFACS). Research interest include Blockchain technology and Smart Cities. Emanuel is a member of IPQoS Research Group and RePAF Project (Resource Allocation Framework for MPLS, Elastic Optical Networks (EON), Network Function Virtualization (NFV) and IoT) at UNIFACS.



Prof. Dr. Joberto S. B. Martins - Professor at Salvador University (UNIFACS) and PhD in Computer Science at Université Pierre et Marie Curie - UPMC, Paris (1986). Invited Professor at HTW - Hochschule für Technik und Wirtschaft des Saarlandes (Germany) since 2003, Senior Research Period at Université of Paris-Saclay in 2016, Salvador University head and researcher at NUPERC and IPQoS research groups on Resource Allocation Models, Software Defined Networking - OpenFlow, Smart Cities, Smart Grid, Cognitive Management and AI application. Previously worked as Invited Professor at Université Paris VI and Institut National des Télécommunications (INT) in France and as key speaker, teacher and invited lecturer in various international congresses and companies in Brazil, US and Europe.