DOI: 10.15514/ISPRAS-2023-35(1)-8

Blockchain and Satisfiability Modulo Theories for Tender Systems

R. Dávila, ORCID: 0000-0002-3174-5748 <photographic_ren@comunidad.unam.mx>
R. Aldeco-Pérez, ORCID: 0000-0002-7003-2724 <raldeco@unam.mx>
E. Bárcenas, ORCID: 0000-0002-1523-1579 <ebarcenas@unam.mx>
Universidad Nacional Autónoma de México
Ciudad Universitaria, Coyoacán, 04510 Mexico City, Mexico

Abstract. A tender process consists in competing offers from different candidate suppliers or contractors. The tender winner is supposed to supply or provide a service in better conditions than competitors. Tenders are developed using centralized unverified systems, which reduce transparency, fairness and trust on the process, it also reduces the ability to detect malicious attempts to manipulate the process. Systems that provide formal verification, decentralization, authentication, trust and transparency can mitigate these risks. Satisfiability Modulo Theories provides a formal analysis to prove correctness of tender offers properties, verified properties ensures system reliability. In addition, one technology that claims to provide decentralization is Blockchain, a chain of distributed and decentralized records linked in a way such that integrity is ensured. This paper presents a formal verified and decentralized proposal system, based on Satisfiability Modulo Theories and Blockchain technology, to make electronic procurement tenders more reliable, transparent and fair.

Keywords: Satisfiability Modulo Theories; Tender verification; Blockchain; e-Procurement

For citation: Dávila R., Aldeco-Pérez R., Bárcenas E. Blockchain and Satisfiability Modulo Theories for Tender Systems. Trudy ISP RAN/Proc. ISP RAS, vol. 35, issue 1, 2023. pp. 113-122. DOI: 10.15514/ISPRAS-2023-35(1)-8

Acknowledgments. This research was supported by the Mexican Council CONACYT (1006953) in collaboration with Instituto de Investigaciones en Matemáticas Aplicadas y en Sistemas: Posgrado de Ciencia e Ingeniería de la Computación of the Universidad Nacional Autónoma de México. The work was also supported by UNAM-PAPIIT(IA104122) and UNAM-PAPIIT(TA101021).

Блокчейн и задача выполнимости формул в теориях для тендерных систем

Р. Давила, ORCID: 0000-0002-3174-5748 <photographic_ren@comunidad.unam.mx>
Р. Альдеко-Перес, ORCID: 0000-0002-7003-2724 <raldeco@unam.mx>
Э. Барсенас, ORCID: 0000-0002-1523-1579 <ebarcenas@unam.mx>

Национальный автономный университет Мексики
Мексика, 04510 Мехико, Койоакан, Университетский городок

Аннотация. В тендерном процессе участвуют конкурирующие предложения от разных кандидатов – поставщиков или их контрагентов. Победитель тендера должен поставить или оказать услугу на лучших условиях, чем конкуренты. Тендеры разрабатываются с использованием централизованных непроверенных систем, что снижает прозрачность, справедливость и доверие к процессу, а также снижает возможность обнаружения злонамеренных попыток манипулирования процессом. Системы, которые обеспечивают формальную проверку, децентрализацию, аутентификацию, доверие и прозрачность, могут снизить эти риски. Задача выполнимости формул в теориях обеспечивает формальный анализ для доказательства правильности свойств тендерных предложений, проверенные свойства обеспечивают надежность системы. Кроме того, одной из технологий, обеспечивающих децентрализацию, является блокчейн, цепочка распределенных и децентрализованных записей, связанных таким образом, что обеспечивается целостность. В нашей статье представлена формальная проверенная и децентрализованная система управления тендерными предложениями, основанная на задаче выполнимости формул в теориях и технологии блокчейн и направленная на то, чтобы сделать электронные тендеры на закупки более надежными, прозрачными и справедливыми.

Ключевые слова: задача выполнимости формул в теориях; проверка тендеров; блокчейн; электронные закупки

Для цитирования: Давила Р., Альдеко-Перес Р., Барсенас Э. Блокчейн и задача выполнимости формул в теориях для тендерных систем. Труды ИСП РАН, том 35, вып. 1, 2023 г., стр. 113-122. DOI: 10.15514/ISPRAS–2023–35(1)–8

Благодарности. Исследование поддерживалось Национальным советом по науке и технологии CONACYT (1006953) при сотрудничестве с Научно-исследовательским институтом прикладной математики и систем. Работа также поддерживалась грантами IA104122 и TA101021 Программы поддержки научно-исследовательских и технологических инновационных проектов (UNAM-PAPIIT).

1. Introduction

Public tenders are sensitive to fraud and corruption; therefore, the laws of most countries regulate government procurement. One example is the European scheme for public tenders, which is one of the most organized and documented [1]. In this scheme, contracts typically go through competitive processes, following common and local legal guidelines of each member country of the European Union. The purpose of this scheme is to offer a fair process for the participants, including a fair price for the taxpayers of the country issuing the tender. Currently, this scheme handles various types of procedures for tendering, such as open or restricted. These procedures have in common a negotiation about what the participants will supply, but with different rules between each type of procedure.

Although governments have robust legal rules for bidding procedures, these procedures are carried out centrally, where a collective or an individual entity reviews each bid based on the rules established by the corresponding tender. So later, the supplier with the proposal offering the best cost/quality ratio is selected.

This centralization creates different risks for the tendering procedures. Centralized entities might give preferential treatment to some of the participants, thereby, undermining the fairness of the process. There is also the possibility that bids are manipulated to favor a specific participant. In addition, the transparency of the procedures can be compromised, as the results of the tendering process presented to the public are not reliable [2] as malicious manipulations are not published.

This problem has been already identified by some governments that have proposed initiatives for electronic tendering schemes. Some of these schemes are implemented using information systems that carry out bidding procedures through the Internet. One example of these kind of government is presented in [3], where a large-scale implementation was developed.

Despite the advantages offered by these systems, they are still centralized, therefore, managed by selected entities who must comply with the applicable rules. Centralization might hide malicious manipulation.

In addition, it is also not possible to automatically verify if the tender rules are meet by the participants. By doing this, human errors and data manipulation can be reduced. Therefore, systems that provide automated verification, decentralization and transparency can mitigate these risks.

Therefore, by modelling and implementing a system based on Satisfiability Modulo Theories and Permissioned Blockchain, to validate, automate, offer immutable transparency, and ensure fairness in tendering procedures is possible.

Satisfiability Modulo Theories (SMT) [4] is a verification technique to prove correctness of system's properties. Properties are expressed in a formal language and when all given properties are satisfied, it is said that the system is valid. This technique can be used to implement automatic verification of rules on a system.

Permissioned Blockchain [2] is a type of restricted Blockchain, where access to participants is controlled by having full identification of them. These participants are impartial entities that attest to the records that are generated in the Blockchain. This type of blockchain by having access control, greatly reduces the energy consumption required by public blockchains. In the latter, anonymity requires high resources in terms of hardware and energy, so a permissioned blockchain is more convenient for governments or public institutions.

Considering this, we propose a tendering system based on Satisfiability Modulo Theories and Permissioned Blockchain that supports biding processes.

By using this system, participants' bids will be automatically validated to later be registered in a blockchain, that through consensus of several peers supports decentralization. Therefore, reducing the reliance on a single entity. As consequence, reliability, fairness, integrity, and transparency of a tendering process can be guaranteed.

This paper presents the following contributions:

- Presents a system design for the public tendering procedure, as a reference for investigations of a similar nature;
- Shows the operation of the system model with facilities for its optimization and improvement;
- Validates inputs to the system through the use of a formal verifier;
- Securely and robustly registers the operations carried out in the tender process in a permissioned Blockchain system;
- Offers a proof of concept to set a precedent that implementation is possible.

1.1 Related work

First, work related to verification is shown, from which reference was taken to support the formality of our proposal.

Y. Limón et.al. present a “Mu-Calculus Satisfiability with Arithmetic Constraints” [5]. They study an extension of modal mu logic and Presburger arithmetic constraints, over tree models. They describe a satisfiability algorithm similar to our model.

D. Medina-Martínez et.al. present a “Database Management System Verification with Separation Logics” [6]. They propose to use Separation Logics to verify a database management system, focused on the verification of libraries containing heap data structure manipulation. Inside of the verification they use classical First Order Logic (FOL) reasoners to strength the verification process, in a similar way to our proposal.

In the following sections, we present results in the design, formalization and modeling of such a proposal.

2. Background

In this section, the concepts of Satisfiability Modulo Theories, Blockchain and Smart Contracts are presented.

2.1 Satisfiability Modulo Theories

The Satisfiability Modulo Theories (SMT) problem is a decision problem for logical formulas with respect to combinations of background theories expressed in classical First Order Logic with equality [4].

A decision problem is a problem that can be abstracted as a yes or no question of the input values, while a formal theory is a set of sentences that can be used to restrict the models we wish to consider.

An approach to solve SMT formulae is based on the observation that an SMT can be reduced to a Propositional Satisfiability Problem (SAT) formulae. Reductions can be solved atomically, to finally combine the results, to prove if the input formula is valid. This approach will be useful to validate the inputs during the operation of our proposed model protocol.

2.2 Blockchain

At the end of 2008 [7], along with the invention of cryptocurrencies, decentralized and transparent databases became popular. This is now known as Blockchain. According to NIST "Blockchains are distributed ledgers of cryptographically signed transactions that are grouped into blocks. Each block is cryptographically linked to the previous one (making it tamper evident) after validation and undergoing a consensus decision. As new blocks are added, older blocks become more difficult to modify (creating tamper resistance and strength integrity). New blocks are replicated across copies of the ledger within the network, and any conflicts are solved automatically using established rules [8]".

There exist two types of Blockchain: Permissionless and Permissioned. The former, called Public or Permissionless, it is open to all participants preserving their anonymity and offering full ledger transparency. Everyone in the network can validate transactions and can partake in the process of consensus. However, this type has a high energy consumption and uses consensus algorithms that take considerable time to reach an outcome [2]. An example of an application of this type of Blockchain is the Ethereum platform [9].

The latter, called Private or Permissioned, it is not open to all nodes. The participation of nodes is managed by third parties, usually impartial entities, i.e., they do not belong to the same organization and do not share interests. In this type of Blockchain, not all the nodes in the network can participate in the verification of the transactions. Instead, a selected group of nodes perform such verification, therefore, improving its efficiency. At difference of public blockchains, private blockchains do not provide decentralized security due to restricted access [2]. However, since in a private blockchain a third party assigns the access rights to each participant, the privacy level is increased making this type of blockchain suitable for government sectors. Moreover, their energy consumption is lower as consequence of the used consensus algorithms [2]. An example of this type of Blockchain is the Hyperledger Fabric platform [10].

Blockchain types use consensus protocols. A consensus protocol provides a technique for users or machines to coordinate in a distributed and decentralized setting. It ensures all participants agree on a unified transaction ledger without the help of a central authority. In the case of public blockchains, the consensus is achieved by the validations of the participants in the network, and in the case of private blockchains, the consensus is achieved by the selected entities accepted in the network [9].

3. System model

In this section, we present the high-level design of our system including the actors and its functionality. This functionality is later described through a set of sequence diagrams, as well as the description of the operation of the system's Blockchain network.

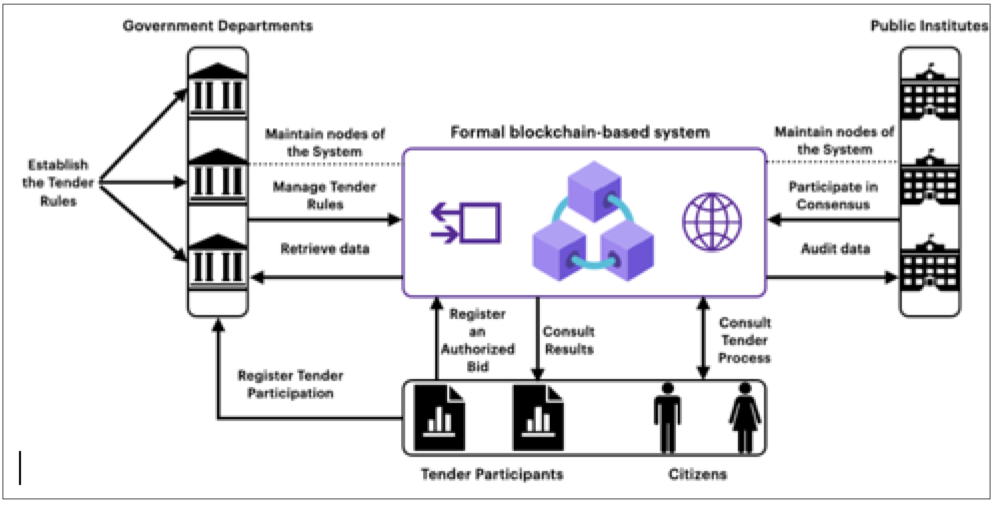

Fig. 1. Architecture of the model

3.1 System overview

The Fig.1 illustrates the architecture of the model. In this, there are 5 blocks that groups the main actors of the system. These blocks are defined as follows.

Formal blockchain-based system. This is the main block of the model that is depicted in purple on Fig.1. Here, the tender rules are established, operations in the Blockchain are registered and the winning offer is determined, all in an automated way. It also offers access to the information registered in the Blockchain to participants and citizens interested in reviewing the procedures carried out within the tender system.

Government Departments. This block represents the public government institutions that issue the calls for bids, establish the tender rules, control access to participants and are constantly managing the operations that occur in the Blockchain.

Public Institutes. This block represents the public institutions that participate in the bidding process as members of the consensus for registering transactions in the Blockchain. They audit the information that is recorded in the system, and also handle the operations that occur within the Blockchain. The participation of these institutions is considered impartial, to strengthen the fairness of the tender process.

Tender participants. This part of the block represents the companies or organizations interested in participating in the tender process. They are obliged to register their participation so that they have control over their access. Once registered, they can send their offers to the system, consult the results of the valid rules that they comply with, or consult the transactions with information on the procedures that were carried out in the tender process in a transparent manner.

Citizens. This part of the block represents citizens interested in reviewing a tender process, to check the procedure was fair and that the use of their taxes will be made according to the legislation.

Once the blocks that represent the actors in the model have been described, the proposed functionality of the system is presented below.

4. Formal model analysis

In this section, we present the results of the formalization of the tender rules and the offers of the participants, that occur in the Formal blockchain-based system (Fig. 1 in Section III).

Following tender rules specified in [1], we have identified the next four types of general rules in a tender process.

Specifications associated to a particular tender entity (several tender entities may form part of the tender), such as antitrust regulations or import or export taxes; Specifications associated to bidders, such as your legal identification or certifications; General specifications, such as a tender registration; and Numerical constraints, such as the price limit of the tender or budget of some offer proposal.

To explain how these rules are used in the tender we present the following set of definitions.

To formalize the tender rules, we propose a hybrid specification based on a rule-based expert system which are non-numerical specifications [11] and a numerical constraint system [12]. The rule-based expert system formalizes the knowledge required to express the type of rules not involving numerical constraints, that is, specifications associated to tender entities and bidders, and general specifications. Numerical constraints are formalized by the corresponding system.

Definition 1 (Non-numerical specifications). Non-numerical specifications are expressed by a set of rules of the following form:

$$\text{IF } antecedent \text{ THEN } consequent$$

where antecedent and consequent may represent a Boolean combination of statements.

Definition 2 (Numerical specifications). Numerical constraints are expressed by an equation system:

$$\begin{aligned} &a_{1,1}x_1 + a_{1,2}x_2 + \cdots + a_{1,n}x_n \leq t_1 \\ &a_{2,1}x_1 + a_{2,2}x_2 + \cdots + a_{2,n}x_n = t_2 \\ &\vdots \\ &a_{m,1}x_1 + a_{m,2}x_2 + \cdots + a_{m,n}x_n \geq t_m \end{aligned}$$

for any positive integers n and m. Notice other relations, such as >, <, ≤, ≥, may also be expressed, for instance $x \leq k$ holds if and only if $x + y = k$ for some positive integer y.

Now, we are going to define a bidder.

Definition 3 (Bidder Offer). A bidder offer is defined by the tuple ($Statements$, $NumericalEqualities$), where $Statements$ is a set of fulfilled properties, defined by the tender rules, and $NumericalEqualities$ is a set of equalities between variables and positive real numbers, associated to costs.

We are now ready to define when a bidder satisfies the tender rules.

Definition 4 (Bidder offer fulfillment). Given a set of tender rules, expressed in terms of a rule-based expert system (Definition 1) and a numerical constraints system (Definition 2), we say a bidder offer fulfills the rules, if and only if, the statements and numerical equalities (Definition 3) fulfill all numerical and non-numerical specifications.

Definition 5 (Tender Rules Formalization). Given a set of tender rules, expressed in terms of a rule-based expert system (Definition 1) and a numerical constraints system (Definition 2), and a bidder b, we define the FOL formula $TR(b)$ (b occurs in TR) as follows:

$$TR(b) \coloneqq ES(b) \land NS$$

where n rules of the expert system are defined by the formula

$$ES(b) \coloneqq \bigwedge_{i=1}^{n} (Antecedent(b)_i \to Consequent(b)_i)$$

and m numerical constraints are defined by the formula

$$NS \coloneqq \bigwedge_{j=1}^{m} \sum_{k=1}^{l} a_{j,k} x_l = c_j$$

where c is a value given by the bidder b. Other relations, such as >, <, ≤, ≥, may also be expressed.

Definition 6 (Bidder Offer Formalization). Given a bidder b, expressed in terms of statements and numerical equalities (Definition 3), and his offer, we define the FOL formula $BO(b)$ (b occurs in BO) as follows:

$$BO(b) \coloneqq ST(b) \wedge NE$$

where n statements of the offer are defined by the formula

$$ST(b) \coloneqq \bigwedge_{i=1}^{n} (Statements(b)_i)$$

and m numerical equalities of the offer are defined by the formula

$$NE \coloneqq \bigwedge_{j=1}^{m} (a_j x_j = c_j)$$

where c is a value given by the bidder b.

Based on these definitions, the following theorem is constructed and proved.

Theorem 1 (Bidder offer verification). Given a set of tender rules and a bidder offer b, the FOL formula $TR(b) \wedge BO(b)$ is satisfiable if and only if the bidder offer fulfills the tender rules.

Proof: $[\![TR(b) \wedge BO(b)]\!]_V^S = 1 \Longrightarrow b$ fulfills tender rules.

Induction over the size of $TR(b) \wedge BO(b)$.

Base case:

There is only one rule for $BO(b)$ then there is only one $TR(b)$ rule to be satisfied,

$$ES(b) \wedge NS \wedge ST(b) \wedge NE$$

where

$$ES \coloneqq (Antecedent(b)_1 \rightarrow Consequent(b)_1)$$
$$NS \coloneqq a_{1,1}x_1 = c_1$$
$$ST \coloneqq Statement(b)_1$$
$$NE \coloneqq a_1 x_1 = c_1$$

Assume $BO(b)$ rule satisfies $TR(b)$ rule.

Therefore $\big(TR(b) \wedge BO(b)\big) = 1$ and by Definition 4 in this Section then b fulfills the tender rules.

Induction hypothesis: if there are n rules for $BO(b)$ then there are n $TR(b)$ rules to be satisfied.

Inductive step: proof for $n+1$ rules for $BO(b)$ over $n+1$ $TR(b)$ rules.

Case 1:

There is one $ES(b)$ rule and $n+1$ NS rules

where

$$ES \coloneqq (Antecedent(b)_1 \rightarrow Consequent(b)_1)$$
$$NS \coloneqq \bigwedge_{i=1}^{n+1} \sum_{j=1}^{m+1} a_{i,j} x_m$$
$$ST \coloneqq Statement(b)_1$$
$$NE \coloneqq \bigwedge_{i=1}^{n+1} a_i x_i = c_i$$

Assume $BO(b)$ rules satisfy $TR(b)$ rules.

Therefore $\big(TR(b) \wedge BO(b)\big) = 1$ and by Definition 4 in this Section then b fulfills the tender rules.

Case 2:

There are $n+1$ $ES(b)$ rules and one NS rule where

$$ES(b) \coloneqq \bigwedge_{i=1}^{n+1} (Antecedent(b)_i \rightarrow Consequent(b)_i)$$
$$NE \coloneqq a_{1,1}x_1 = c_1$$
$$ST(b) \coloneqq \bigwedge_{i=1}^{n+1} (Statements(b)_i)$$
$$NE \coloneqq a_1 x_1 = c_1$$

Assume $BO(b)$ rules satisfy $TR(b)$ rules.

Therefore $\big(TR(b) \wedge BO(b)\big) = 1$ and by Definition 4 in this Section then b fulfills the tender rules.

Case 3:

There are $n + 1$ $ES(b)$ rules and $n + 1$ NS rules

where

$$ES(b) \coloneqq \bigwedge_{i=1}^{n+1} (Antecedent(b)_i \rightarrow Consequent(b)_i)$$
$$NS \coloneqq \bigwedge_{i=1}^{n+1} \sum_{j=1}^{m+1} a_{i,j} x_m$$
$$ST(b) \coloneqq \bigwedge_{i=1}^{n+1} (Statements(b)_i)$$
$$NE \coloneqq \bigwedge_{i=1}^{n+1} a_i x_i = c_i$$

Assume $BO(b)$ rules satisfy $TR(b)$ rules.

Therefore $\big(TR(b) \wedge BO(b)\big) = 1$ and by Definition 4 in this Section then b fulfills the tender rules.

The other implication direction is proved in an analogous manner. ■

The demonstration presented gives us the certainty that the rules of a tender process could be formalized correctly. This increases confidence for the participants in the tender, for the governments and for the citizens.

With the tender rules and participant bids formalized, we give the proposal model more confidence, and allows us to understand what the verifier block does precisely.

5. Discussion, Future work & Conclusions

In conclusion, we presented a formal model for verification to provide a more robust solution to a complex problem such as a tender process. Using that model, we created a system that along with a Blockchain network can offer greater confidence in a tender process.

To reach that goal, we also define logical formulas that are the basis for the formalization of offers in a bidding process. Later, we demonstrate the correct operation of the logical formulas, and thus have the confidence that the verification works correctly.

As future work, our prototype can be implemented with an attractive and user-friendly interface (system view) for potential final users. To have a fully automated system, the inputs for the automatic solver can be formatted on a logic-based notation. For that purpose, a procedure with this purpose should be constructed and integrated to our system.

Finally, this is an extension of [13] and short varsion of [14].

References / Список литературы

[1] Public tendering rules in the EU. Available at: https://europa.eu/youreurope/business/selling-in-eu/public-contracts/public-tendering-rules/index_en.htm.

[2] Huynh T.T., Nguyen T.D., Tan H. A survey on security and privacy issues of blockchain technology. In Proc. of the International Conference on System Science and Engineering (ICSSE), 2019, pp. 362-367,.

[3] Road data exchange layer. Available at: https://x-road.global/.

[4] Barrett C., Sebastiani R. et al. Satisfiability Modulo Theories. In Handbook of Satisfiability. IOS Press, 2009, pp. 825-885.

[5] Limón Y., Bárcenas E., et al. Mu-calculus satisfiability with arithmetic constraints. Programming and Computer Soft-ware, vol. 46, no. 8, 2020, pp. 503-510 / Лимон Й., Барсенас Э. и др.. Выполнимость мю-исчисления с арифметическими ограничениями. Труды ИСП РАН, том 33, вып. 2, 2021 г., стр. 191-200. DOI: 10.15514/ISPRAS–2021–33(2)–12.

[6] Medina-Martínez D., Bárcenas E. et al. Database management system verification with separation logics. Programming and Computer Software, vol. 47, no. 8, 2021, pp. 654–672.

[7] Nakamoto S. Bitcoin - A Peer-to-Peer Electronic Cash System. Appendix A. The bitcoin whitepaper by Satoshi Nakamoto. In Antonopoulos A. Mastering Bitcoin: Programming the Open Blockchain, 2nd ed. O'Reilly Media, 2017, pp. 323-334

[8] Yaga D., Mell P. et al. Blockchain technology overview. arXiv:1906.11078, 2019, 68 p,

[9] Ismail L., Materwala H. A review of blockchain archi-tecture and consensus protocols: Use cases, challenges, and solutions, Symmetry, vol. 11, issue 10, 2019, article no. 1198, 44 p.

[10] Hyperledger fabric. Available at: https://hyperledger-fabric.readthedocs.io/en/latest/index.html.

[11] Grosan C., Abraham A. Rule-Based Expert Systems. Intelligent Systems Reference Library, vol. 17, 2011, pp. 149–185.

[12] Bockmayr A., Weispfenning V., Maher M. Solving numerical constraints, In Handbook of Automated Reasoning. Robinson A., Voronkov A. eds. MIT Press, 2001, pp. 751–842.

[13] Dávila R., Aldeco-Pérez R., Bárcenas E. Tender system verification with satisfiability modulo theories.Iin Proc. of the 9th International Conference in Software Engineering Research and Innovation (CONISOFT), 2021, pp. 69–78.

[14] Dávila R., Aldeco-Pérez R., Bárcenas E. Formal Verification of Blockchain Based Tender Systems. Programming and Computer Software, vol. 48, issue 8, 2022, pp. 566-582.

Information about authors / Информация об авторах

René DÁVILA, Master degree in Computer Science and Engineering, PhD Student at Research Institute in Applied Mathematics and Systems (UNAM). Research interests: Decentralised and Distributed Authentication Protocols, Applications of Blockchain to improve services and Privacy of information, Security, Computer Logic, Distributed Systems, Algorithms Analysis.

Рене ДАВИЛА, магистр компьютерных наук и инженерии, аспирант Научно-исследовательского института прикладной математики и систем (UNAM), Научные интересы: протоколы децентрализованной и распределенной аутентификации, применение блокчейна для улучшения услуг и конфиденциальности информации, безопасность, компьютерная логика, распределенные системы, анализ алгоритмов

Rocío ALDECO-PÉREZ, Doctor on Computer Science, Research Associate. Research interests: Privacy of information, Decentralised and Distributed Authentication Protocols, Applications of Blockchain.

Росио АЛЬДЕКО-ПЕРЕС – кандидат компьютерных наук, доцент. Область научных интересов: конфиденциальность информации, децентрализованные и распределенные протоколы аутентификации, применение блокчейна.

Everardo BARCENAS, Ph.D., Assistant Professor. Research interests: modal logics, proof theory, automated reasoning, description logics, model checking, knowledge representation, planning, computer vision.

Эверардо БАРСЕНАС, кандидат наук, доцент. Научные интересы: модальная логика, теория доказательств, автоматические рассуждения, логика описания, проверка моделей, представление знаний, планирование, компьютерное зрение.