International Journal of Information Security (2023) 22:869–880
https://doi.org/10.1007/s10207-023-00673-3

REGULAR CONTRIBUTION

Blockchain and smart contract architecture for notaries services under civil law: a Brazilian experience

Leonardo Dias Menezes[1] · Luciano Vieira de Araújo[1] · Marislei Nishijima[2]

Accepted: 14 February 2023 / Published online: 25 February 2023

Abstract
This paper proposes a blockchain solution for some activities currently performed by notary offices under the Civil Law judiciary that is technically viable. The architecture is also planned to accommodate Brazil's legal, political, and economic requirements. Notaries are responsible for providing various intermediation services for civil transactions, where their primary role is to be the trusted party capable of guaranteeing the authenticity of these transactions. This type of intermediation is common and demanded in Latin American countries, such as Brazil, which is regulated by a Civil Law judiciary. The lack of adequate technology to meet such legal demands leads to an excess of bureaucracy, dependence on manual document and signature checks, and centralized and face-to-face actions in the physical dependence of the notary. To deal with this scenario, this work presents a blockchain-based solution to make some of the activities performed by notaries automatic, guaranteeing non-modification and adherence to civil laws. Thus, the suggested framework was evaluated in accordance with Brazilian legislation and provides an economic evaluation of the proposed solution.

Keywords Blockchain · Ethereum · Notary services · Smart contract · Civil law · Brazil

1 Introduction

Brazilian notaries' current performance lags behind the recent technological access to information and automated services available. Individuals' use of information and telecommunication technology (ICT) to access government services is essential to increase transparency and accountability [1]. In this sense, Estonia is a remarkable example of blockchain technology usage in public services, with applications in the national health system, judicial and legislative arenas, security, and commercial systems, among others [2, 3]. The country shares a civil law tradition with Brazil and other Latin American countries.

A Notary under Civil Law has a much broader scope of activities and duties than a Notary under Common Law.[1] Thus, the potential benefits for countries under Civil Law by adopting an ICT solution tend to be larger. In Brazil, as in many Latin American countries, notary services are performed primarily on paper, and the physical presence of an individual to require its services is mandatory. This model is less efficient when compared with the digital solution since it is exclusively based on human procedures, which are subject to human failures. According to the National Council of Justice, the Brazilian Registry Office's revenues were more than US 13 billion dollars in 2017 [4]. These massive resources represent costs for individuals since they pay this value for services. The total cost for individuals also adds the opportunity cost to be physically at notaries to buy services.

Brazil has been a member of the free access to public information (FOI) since 2011—following Law n. 12,527—but

Homepage: marislei.iri.usp.br

✉ Marislei Nishijima
marislei@usp.br

Leonardo Dias Menezes
leonardo.dias.menezes@gmail.com

Luciano Vieira de Araújo
lvaraujo@usp.br

[1] School of Arts, Sciences and Humanities, University of Sao Paulo, Rua Arlindo Bettio, 1000–03828–000 Sao Paulo, SP, Brazil

[2] Institute of International Relations, University of Sao Paulo, Av. Prof. Lucio Martins Rodrigues, S/N – trav. 4-5, São Paulo, SP, Brazil

[1] (https://www.nationalnotary.org/notarybulletin/blog/2011/11/common-civil-lawnotaries).

still faces many challenges in implementing new technologies in the public services, despite the worldwide guidelines on the transparency of public administration [5]. In addition, Brazil has an environment of excessive bureaucracy, legal difficulties in implementing ICT solutions [6], and endemic public corruption [7]. Furthermore, experiences in blockchain are discouraged by incumbents in developing countries due to the difficulty that fraudulent activities have in electronic environments transparent to the public [8, 9].

A systematic review [10] indicates a vast literature, around 443 studies, describing blockchain and its potential uses, where notaries' services are several times mentioned given its very secure nature. Therefore, only some studies still present architectures in blockchain for notary activities, focusing predominantly on technical feasibility [11–15]. Unlike the previous works, the proposed blockchain architecture for some notary services combines existing technical solutions in a simple and innovative decentralized solution that complies with usual regulatory demands. According to the Brazilian Ministry of Management and Innovation in Public Services, historical, disciplinary, and legal principles must be observed. In addition, the architecture innovates by proposing a way to identify the individual who provides the document to receive e notary service, an authentication, for instance, absent in the previous solutions.

Besides this introduction, the paper evaluates blockchain's main characteristics and background in Sect. 2. Then, Sect. 3 presents a blockchain technology application for some of the notary's activities complying with state regulatory demands, while Sect. 4 discusses how the solution overcomes potential barriers and limits. Finally, Sect. 5 summarizes the main conclusions.

2 Background

2.1 Blockchain

Similar to a public record book or a sequence of events, a blockchain is a distributed database. Participants of the system must validate any transaction by consensus, and it is impossible to delete registered information [16]. Bitcoin is considered the first and most important blockchain network. It operates as a financial transaction logbook based on the currency Bitcoin. When a record is created in the Bitcoin blockchain, a user submits a public–private key to the participating network. The participant then announces the transfer amount to another public key by signing the transaction with his private key. To validate a transaction, network participants need to certify that both keys are valid and whether the originator of the transaction has enough balance, measured in Bitcoin currency. As there is no limit superior to the number of keys a user can create on the network, Bitcoin reaches its consensus through proof of work. The processing power of computers connected to the network determines the "majority" to get the consensus. Individuals who dedicate computing power to generate this consensus are called miners. Each block created, or mined, in the Bitcoin network generates a reward in Bitcoin currency [17].

After disseminating the Bitcoin concept, several other blockchain networks were developed based on the same principle to create cryptocurrencies. In 2015, however, Vitalik Buterin developed a protocol in blockchain called Ethereum. In addition to the cryptocurrency values, the new protocol allowed registering computer programs in blockchain and running them using the network's computational power. This function is similar to the previously available and well-developed smart contracts in the field of computer science [18, 19]. These smart contracts programs are developed in Solidity and other GPLs languages and operate similarly to any program developed in Java language. The consumer, however, must have cryptocurrencies (also called Ethereum) to buy Gas to run the program for some time. In doing so, this consumer is rewarding participants in the Ethereum network, which is also public, for his computing power with his cryptocurrency [20].

2.2 Notarization process in Brazil and ICT background

Countries with a tradition of Civil Law use notary services for the official registration of their citizens on paper documents. These services are performed by extrajudicial notaries, where the public authority delegates its record-keeping responsibility to them. We focus on the registry office of notes—but there are seven different registry offices in the country—which performs the following operations of the registry: (i) authentication of copies and signatures; (ii) public bookkeeping of purchase and sale, emancipation, minutes, declarations, union and divorce, and donation; and iii) acts registry certificates [21].

A proposal for an alternative solution using blockchain technology to provide public services to any country requires the identification of the feasibility of ICT use in its environment. By its very definition, the provision of public services must be as inclusive as possible [22]. Thus, a new solution cannot immediately exclude a large part of the population. Considering the degree of Internet access in Brazil, there is no evidence of exclusion. Also, due to the COVID-19 pandemic, several types of information technology usage have been adopted worldwide, and many will be of permanent use. In Brazil, examples of the unprecedented technological change adoptions due to the pandemic are the first remote plenary session of the parliament with votes in March [23] and the generalization of remote medical consultations [24].

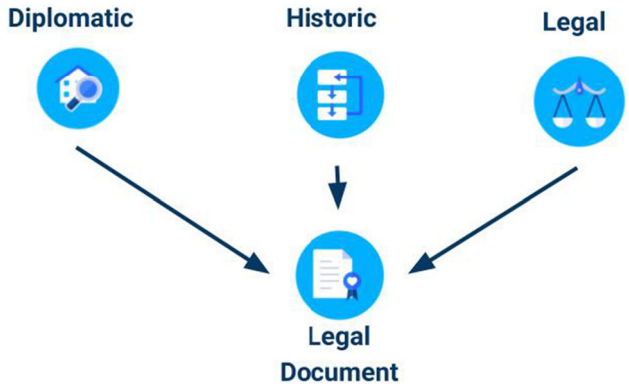


Fig. 1 Legal documents requirements

According to the CETIC (Regional Center for Studies for the Development of the Information Society), in 2018, about 70% of the Brazilian population regularly used the Internet. As for social inclusion, 48% of the Brazilian families from social classes D and E made regular use of the internet in 2018. CETIC data suggest a gap between the supply of services "in the palm of the hand" available to most Brazilians and the use made of this technological capacity. Consumer confidence on the internet is directly related to the perception of website security and the guarantee of privacy of operations [25].

The decentralized, secure, verifiable, and confidence in the immutable structure of documents certified by blockchain structure is supposed to increase the efficiency of notary services and data transparency.

2.3 Brazilian regulatory requirements

The current Brazilian notary model was established by Law 8935 of 1994 and the Constitution of 1988. Digital notaries are not available under federal law, but the National Council of Archives of the Ministry of Justice has already stipulated its guidelines. Resolution 37 of 2012 determines that document authenticity involves legal, diplomatic, and historical aspects.[2] Figure 1 illustrates the resolution structure.

Regarding the legal aspect, a representative public authority must intervene during or after a document production. In the diplomatic aspect, a document must be written at a specific time and place and signed by the responsible persons of the text. Historically authentic are the documents that attest to events that occurred. Provisional Measure 2,200—2 of August 24, 2001, established criteria for adopting a legal electronic signature. To this end, it instituted the Brazilian Public Key Infrastructure (ICP-Brasil) as the managing authority for policies and the entire chain of entities involved

[2] Conarq, Resolução 37, http://www.conarq.gov.br, 2012. (https://www.gov.br/conarq/pt-br).

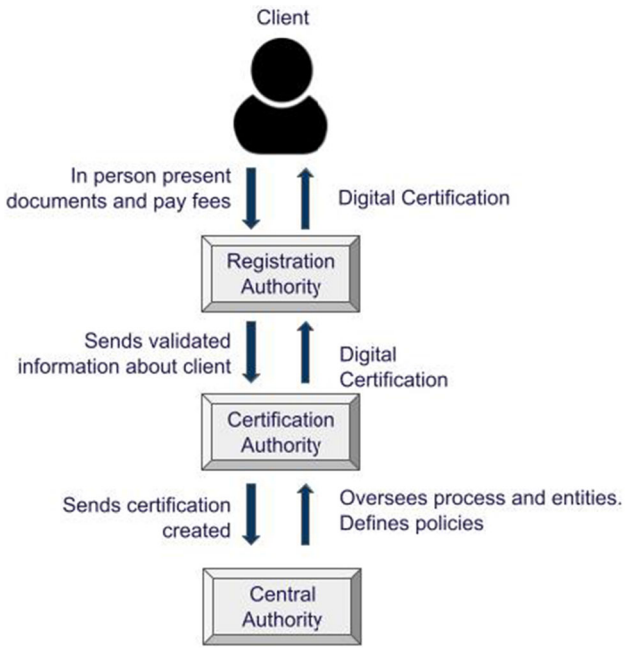


Fig. 2 Digital certification entities

in the digital signature process (Certification and Registration Authorities), see Fig. 2.

The current Registration Authorities request digital signatures in the presence of the future signature holder for the Certification Authorities, which issue and maintain the certificates. Management, policies, and audits of both entities are the competencies of ICP-Brasil as the Root Certification Authority, whose issuance of Digital Signatures is prohibited to end-users. To keep a single base where registries are maintained and ensured as correct, ICP-Brasil centrally held, under public consultation, a Public Key Verifier that allows validating the registration.

3 Proposing an architecture

Would the Registration Authorities' requirements fit an ICT solution under blockchain technology? The approach suggested has the current functionalities covered by legal documents in Brazil to deliver digital documents. Also, the architecture, developed in a pilot platform, complies with the current state regulation. The decentralized, secure, verifiable, and immutable structure of documents certified by blockchain increases the efficiency of notary services and data transparency.

3.1 Regulatory requirements

To comply with Brazilian government regulations, transactions carried out on blockchain must be legitimate in the

diplomatic, historical, and legal aspects, according to the Ministry of Management and Innovation in Public Services. The diplomatic aspect requires documents, assuming the digital nature must be located in time and space. To obey the regulation, the pilot platform of solution saves, for each transaction, the location (municipality) of the author's device and the moment when the transaction occurs using the time stamp of the blockchain itself at the time the transaction is submitted and approved.

The historical aspect determines the document's immutability. Thus, once a document is saved in the blockchain, it is immutable, and any copy obeys the same hash and has the same information. Furthermore, the platform only adds new blocks to the blockchain when it is valid against the generating algorithm. Therefore, the entire historical track of an event can be surveyed and audited, proving its authenticity.

As for the legal aspect, that is, to maintain the digital file's legality without a public authority's physical presence, each event on the blockchain needs to be attested by a Digital Certification provided by a Certification Authority approved, the ICP-Brasil. To technically address this aspect, the pilot platform carries out a verification of each signature made in transactions on the blockchain on the free platform of ICP-Brasil to ensure its legality.

3.2 Functional requirements

The proposed approach keeps all the current functionalities delivering legal documents in Brazil in the digital format. Also, the architecture is under the current legislation to apply immediately to society. From a technical point of view, notaries can be centralized or decentralized in many entities. However, as the first type is frequently under scrutiny due to despotism, the latter is likely to mitigate this weakness as a Byzantine-fault-tolerant algorithm, and multi-signature verifications can be employed for security purposes [26].

In addition, considering Wüst & Gervais's approach [27], for a public notarization solution, storing state is paramount to maintain the point in time and unicity of documents being authenticated. There are multiple writers, presumably any citizen of a country. An Always online Trusted Third Party, however, would retain the current limitations of storing data and infrastructure that nowadays make such a solution not applicable. All writers are known on an ideal notarized system, but they cannot all be trusted since they need their identity validated before issuing documents to the Blockchain. Hence, public variability is required, making the ideal solution a Public Permissioned Blockchain where the ledger and its operations are open and decentralized, but an outside entity is required to validate any writing in the chain. Thus, following the methodological framework proposed by these authors, a decentralized approach for notary activities is the most suitable to our architecture.

The main functionality of the blockchain solution is to legally sign documents in a way that can be verified later, Fig. 3. Also, an original copy could be made while the transaction is made public and transparent. The stages of document signing performed by the proposed architecture are described below.

1. The document generating user performs the upload within the Pilot Platform.
2. The Platform must perform the hashing of the document using the Interplanetary File System (IPFS).
3. The User must sign the document with his Digital Certificate from a Central Certification Authority (CA)
4. The Platform must check with the CA if the Certificate is legitimate.
5. The user must point out other individuals that must sign the document. If so, repeat steps 3 and 4 for each of them.

At the end of this process, the file is permanently saved in the IPSF, and its transactions, with signatures and dates, are permanently stored in the blockchain.

3.3 Architecture

The system's architecture follows the functionalities previously presented with two main components; a web application and a smart contract. Figure 4 shows the interfaces between internal and external components of the system employing the numbers (1, 2, and 3). For a more general view, see Fig. 8 in the appendix.

Interface (1) connects the Web Application and the smart contract and is the most robust linkage since it connects the two layers, the presentation and the operation (backend). The data sent from the Web Application to the smart contract are the user private–public key pair when authenticating, the hash of the document sent to IPFS and the public key for later reference. The data transmitted from the smart contract to the Web Application are: records in blockchain with the public key sent, a hash of documents associated with the queried public key, private key validity for authentication, and signature confirmation approved by ICP-Brasil.

Interface (2) shows the connection between the Presentation Layer and IPFS. This Simple interface sends files from References to the Presentation Layer to IPFS and receives the hashes from these files back. In addition, when selecting a hash from a document searched for in the Presentation Layer, IPFS returns the original file.

Interface (3) brings the connection between the smart contract and the Central Authority. When receiving a new document for signature, the smart contract queries whether

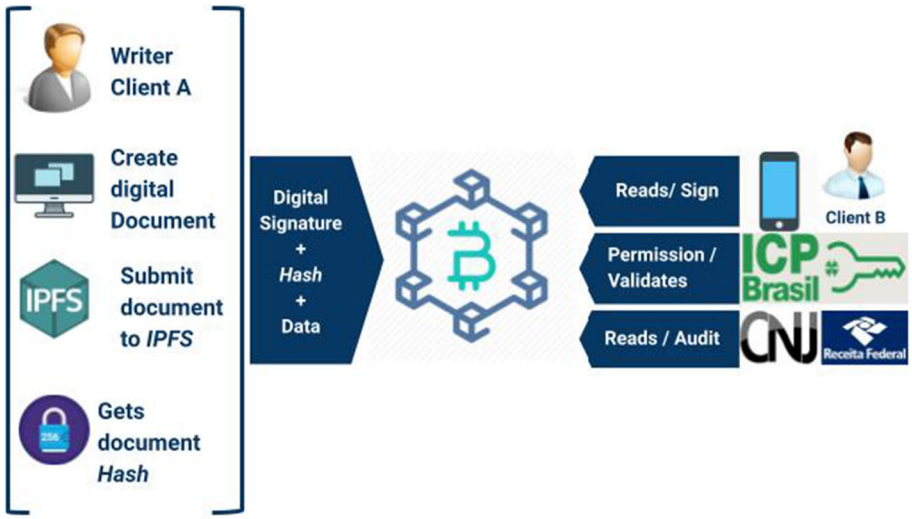


Fig. 3 Functionalities overview

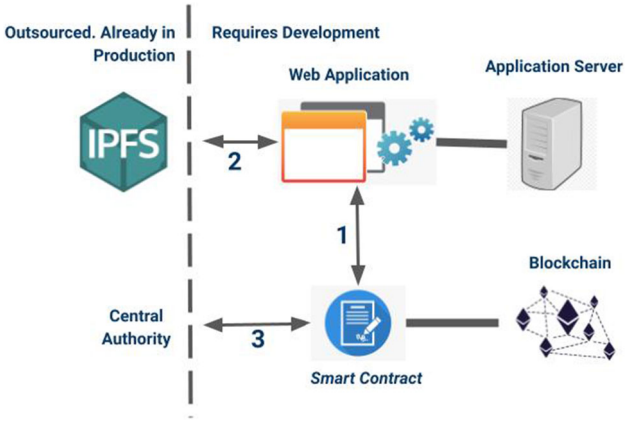


Fig. 4 Architecture view

the signature is valid according to the compliance checker of the CA, which only returns if it is valid or not.

3.4 Existing alternatives

Currently, several online notarization services are available online. An example is Notorize.com, which still has the necessity of human validation and authentication of documents on its backbone. The Open Notary, which is centralized, uses a SQL database to internalize the data. On the contrary, solutions such as Stampd.io provide a web interface for uploading hashes into a public blockchain for a fee but keep the source document private, contrary to another solution, the Blocknotary. On the latest, the documents are uploaded into the IPFS and the hash is stored within the Blockchain with a timestamp. The setback for the Blocknotary is the lack of capability to identify individuals within the solution apart from their blockchain public information. Without a legal validator of the identity of each user in the platform, the authentication loses its legal validity in most countries under Civil Law, including Brazil. Our architecture is similar to the Blocknotary, but it overcomes the problem of individual (user) identification by means of the exchange of data with the ICP-Brasil. This allows the recognition of the individual (authenticity) since the validation of its digital signature is made from inside the smart contract, performing the notary service and avoiding potential fraud.

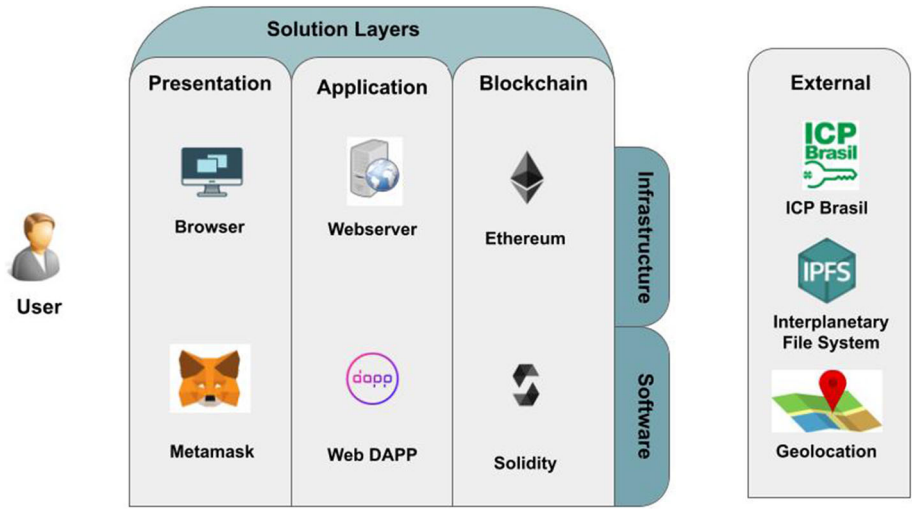
3.5 Solution

Figure 5 shows the current components available to implement a feasible blockchain solution for notaries' activities.

The first requirement in the presentation layer is to show to the final user the availability of a virtual portfolio with the values of cryptocurrencies to allow transactions in a blockchain. Ethereum portfolios are actions that will enable the interaction of accounts in blockchain Ethereum, having a similar effect to a bank app with no need for a bank [28]. The suggested portfolio is the Ethereum Metamask, an extension applicable to the navigator that allows transacting data and identities and accessing the distributed web in blockchain Ethereum [29]. This is necessary since some smart contract functionalities require the users to pay for them. The Metamask extension is very accepted due to having more than one million users.

The application layer uses a Decentralized Application or DApp, which has a presentation that can or cannot be centralized. Still, it must have a distributed structure in its backend, written in any web language [30]. Thus, this layer connects the user's navigator with a blockchain, and it is not exactly a mandatory layer since the user can opt to communicate directly with the blockchain. However, this layer can be essential to facilitate and generalize the application for regular individuals. Finally, in the blockchain layer is the smart contract, which keeps the critical information and operations of the DApp. For the Ethereum web, Solidity is the most used language to develop smart contracts.

Fig. 5 Layers of solution



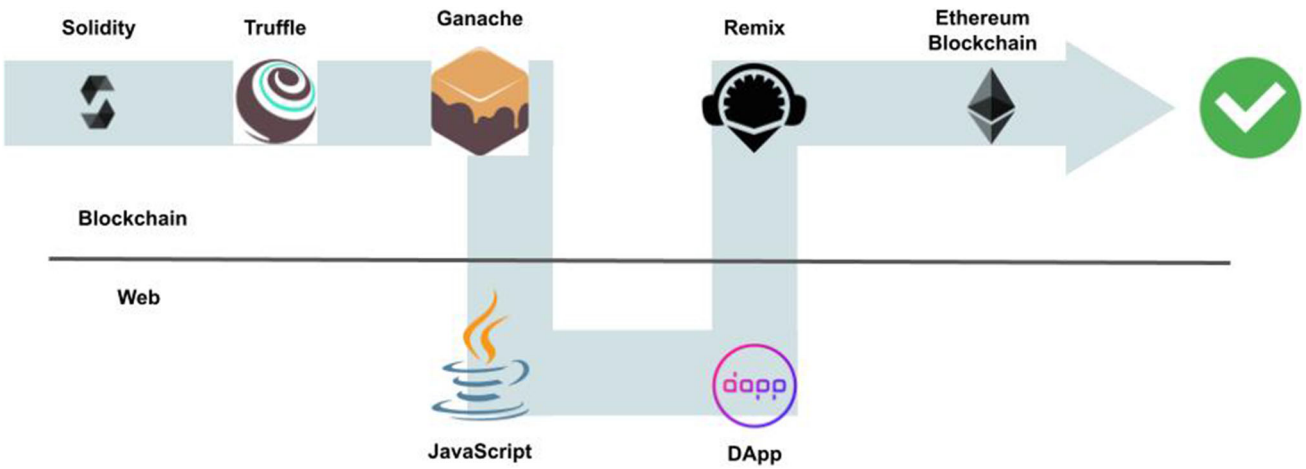


Fig. 6 Stages of development

External to the system's layers, there is the consulting to ICP-Brasil to check digital certification and the Interplanetary File System to keep the documents distributed but out of blockchain to avoid increasing the users' operational costs. In addition, it is essential to use a geolocation service to serve the Diplomatic aspect of the certified documents. This service and the internal clock of the Ethereum Virtual Machine (EVM) guarantee document localization in time and space.

3.5.1 Stages of development

Figure 6 shows the six stages required to develop the platform in blockchain to perform notary services before its tests and implementation.

After describing the code in a language accepted by the EVM, Solidity, in this case, is necessary to compile it. The framework Truffle is a platform that simulates the Ethereum web and allows the code developed in Solidity to work in an EVM [31]. For the smart contract runs in the test, it is important to use an environment of simulation of blockchain Ethereum; this can be done using Ganache, which provides an environment that can monitor the smart contract and create several accounts to interact with it [32].

When the smart contract is finished, it is necessary to develop the front end using JavaScript, for example, to communicate the front end with a blockchain, thus creating DApp. After the initial tests, it is possible to implement the code directly in the blockchain Ethereum using the Remix IDE, a tool for open code writing in Java Script. This tool allows turning the code available directly in the blockchain [33]. At this time, the smart contract is published and available it be accessed from the front-end web developed.

3.5.2 The smart contract

The smart contract operates under some particularities. First, it might have a low cost. Second, considering the documents' size could be significant, the better trade comes from signing them through the IPFS. In this sense, the smart contract only

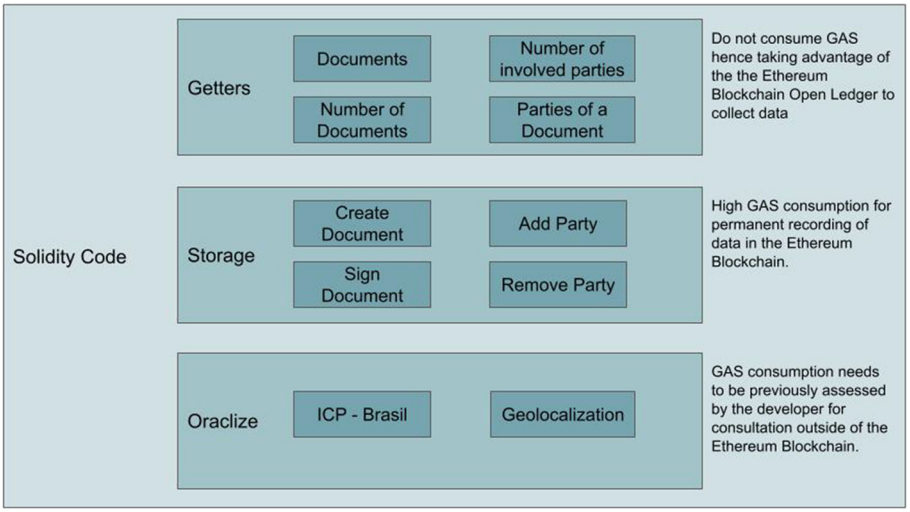


Fig. 7 Functionalities of a smart contract

saves the document's hash, a pattern string of 256 bytes, and not the whole document. In addition, a signature verification must occur when the data is recorded in the blockchain and the same function. This is because encapsulating the record in a different function could lead malicious users to bypass the validation and create illegitimate documents. The same applies to the location and time of a saved signed contract.

To external consults to a blockchain, Solidity allows oracles to external services within its language; a standard method, for example, is called Oraclize. Its function is to rescue available data through an Application Programming Interface (API), perform consults, and save the blockchain [34]. It is important to notice that as the data in a public blockchain is open while compiling a smart contract, functions of the rescue of public data are automatically generated, the Getters. The advantage of these Getters is that their use does not implicate additional cryptocurrency consumption in the Ether case. Thus, a Front End can provide all types of data to its users, turning the documents signed and saved into smart contracts effectively endowed with public faith. Other functionalities are the ones that effectively save the data in the blockchain. Figure 7 shows these functions.

4 Benefits, barriers, and limits of the solution

This section discusses how the proposed solution can overcome technological, economic, and political barriers. It also discusses its potential limits.

4.1 Technical barriers

4.1.1 Security concerns

As the use of the Ethereum infrastructure corresponds to the main function of record keeping, it is important to consider the risks of its exposure to a decentralized network for maintaining files so crucial to civil law. There is an intrinsic risk of network disuse due to potential flaws in the Ethereum network and technological innovation. Creating a centralized database of records governed by states would be necessary to ensure permanent records. This cost, however, is similar to the current cost of keeping the records on paper by the notaries.

A decentralized Database, however, is less open to attacks such as DDOs and human security flaws in regard to privileged accounts being used. Its longevity is ensured by the usage of its solution by the country's individuals and not by a government entity and infrastructure that might fail due to technical or human reasons.

Blockchain technology, however, is not free of risks; access to a user blockchain wallet can be used to impersonate said user within the Blockchain technology (although notarization will still require ICP Brasil valid key). Alternatively, a Long-range Attack may be launched using the Proof of Stake protocol from Ethereum with hijacked Ether values to temporarily control the chain or an Eclipse attack in which an attacker controls a large number of IP addresses in order to include new nodes to the chain.

Aside from the Blockchain, regular centralized flaws can be found on the web application used to connect users to the Blockchain and the ICP Brasil service itself. The first can be replicated and rebuilt as it does not hold a database and its connectors can be made public and the second stands as a legal requirement in order to identify Blockchain writers.

4.1.2 Other technical concerns

Another technical obstacle concerns the process itself of using the smart contract. It would be necessary for each user to have a balance in an Ethereum account to execute the functionalities proposed by the project. However, cryptocurrencies can experience large fluctuations in value, which occurred massively during the short period of their existence,

and the need to acquire them via a private broker, which can involve high arbitrage costs. Alternatively, a user could mine the cryptocurrency using his computational power; however, waiting for the generation of sufficient balance to use the contract directly impacts the proposed efficiency in using technology.

If the government opts for centralized management of blockchain, it could maintain the processing of smart contracts internally by reducing the cost to the taxpayer to zero. The negative impact would be on infrastructure maintenance costs that would return to the State. The loss of decentralization proposed by the public blockchain where record-keeping security and transparency would be at risk as the reported case of blockchain applied in the real state registration in Honduras [8]. Legal Barriers Using certificates approved by ICP-Brasil, it is possible to guarantee the validity of a document in the eyes of Brazilian justice. However, the acquisition and maintenance of such a certificate is financially costly and would alienate a good part of the possible audience of the tool in the use of an automated system. To reduce this risk, the Government could reduce the cost of these certificates, make the rules for certifying certificates more flexible, or even provide them free of charge to every citizen, as is done today with an ID or Birth Certificate. Although the impact on revenues from these certificates is substantial, the costs of maintaining registration records are already borne by the government in several instances (Internal Revenue Service, Social Security, and Electoral Court, to name a few). The efficiency benefits can potentially be very high in the country since the quality of the service improves hugely.

4.2 Economic barriers

An economic efficiency improvement occurs when a service can be produced using fewer resources, lower costs, or better quality and the same costs. Thus, even a profitable activity can be inefficient if it is possible to improve it [35]. This study compares the cost of services online in blockchain with regular notary services. However, it considers only the direct (price) and part of the indirect (opportunity cost of face-to-face needed to obtain the service) costs of regular notaries. Indirect costs like corruption, personal injury due to insecure notarial activity, and other crime costs are not considered, even though they are endemic and very high in Latin America [36].

The notary services prices are regulated by state governments since a notary office is a local monopolist and an essential good. Therefore, its price adjustment requires a Bill of Law (Brazilian Law n. 10,169 of 2000) and varies among regions, e.g., a Firm Recognition in the Acre state costs $ 0.70 and in Rio de Janeiro $ 1.2 in 2018.[3]

The notary services' prices can be split in price and taxes from different levels of government. For example, a signature recognition service from a notary in São Paulo municipality pays taxes for eight governmental institutions, including municipal and state divisions. It corresponded to 41% of the price of a signature recognition in 2020.

As notary services are regulated goods, the government meets difficulties in controlling prices and quality due to the very nature of public goods [35]. Also, considering Brazil's inefficiencies in governance [37] and its high degree of violence, notaries are incentivized to reduce the quality of their services to obtain a larger part of the rent [6]. For instance, the authors report that some notaries prefer to trade using cash to avoid paying fees for credit cards and cards, which increases the risk of consumers' insecurity and the time spent to get some money. Thus, since the proposed architecture homogenizes service quality and increases information for the regulator, both regulators and regulates benefit from higher transparency.

For individuals, however, the cost of these services is not limited to the price notaries charge. The face-to-face needed to obtain the service (time cost) and the maintenance of several paper records (storage cost) are examples of other costs not directly observed. To obtain a notary service, an individual must be in person or send someone to represent him. The opening hours of registry offices, also regulated by state law, generally coincide with other regular working hours (business hours). Thus, to consume these services, an individual must spend time going to the notary office—that, on the contrary, he could use to work and obtain extra income—or pay a legal representative. This cost involves the concept of opportunity cost since an individual could use the time he spent in a notary with different alternative gains [35]. This opportunity cost involves the time of displacement, which can be considerable in some country regions given the high cost of transportation (time and cost to travel) and the time for the service to be performed.

Considering that the notary's operation is still carried out personally and manually, the time of execution of the procedure (search for signature in the file or time to make the seal and stamp on a document) is long. The manual execution may still incur deviations, whether intentional or not, increasing the time of the procedure.

Many consumers face problems with notaries' services due to criminals using their names to get some advantage, and

[3] P. Andrade, Serviço: como se define a tabela de preços dos cartórios, 2018, Accessed on: Apr. 18, 2020, [Online] Available: http://cnj.jus.br/.

notaries offer the services without avoiding fraud.[4] Adoption Barriers to the large-scale implementation of the proposed solution, it is still necessary to mitigate some barriers from the current notarial model.

To determine whether a solution should or not be implemented, it is necessary to also account for the impacts of its development and maintenance of services in the long run—more specifically, the investments through time and the tangible and intangible benefits of using a blockchain tool.

The sunk cost of developing an architecture was already incurred by the authors of the present study that are willing to turn it freely available. As the replication cost of software is almost null, there is no cost to implement the tool on a large scale.

However, there is an infrastructure cost to implement and keep the registers in the Ethereum blockchain and the IPFS. While Ethereum has a positive cost for each use a client makes, there is no cost for using the IFPS, which guarantees the uniqueness of the file that both parties must have locally on their drives. Thus, the cost is to keep the Web server as a component of the interface between users and the Ethereum blockchain.

This server could run on a simple desktop computer, zeroing its cost for pilot purposes. However, large-scale implementation depends exclusively on the volume of transactions executed to maintain good performance. This good performance is restricted because Ethereum today only creates blocks every ten minutes. Thus, investment in infrastructure will be minimal on a large scale since notary activities do not have a massive scale like bank transactions.

Alternatively, considering that in Brazil, most of the use of internet services occurs through cell phones, it is possible only to consider the development of an application, which would impact a longer development time, but, on the other hand, it could remove the need for a Web server, serving the public exclusively via the application. According to the CETIC, 97% of Brazilians used smartphones to access the Internet, and 56%/77% used only smartphones as an exclusive means to access the Internet in urban/rural areas in 2018.

For any transaction within a public blockchain and Ethereum, it is necessary to reward those responsible for processing their machines. The value of using a smart contract, which is paid in "Gas", is measured by the number of functions within it and the number of records that will need to be maintained by the blockchain. A sum operation (ADD), for example, has a cost of 3 Gas in Ethereum; to pull the balance of an account on the Ethereum network, 400 Gas is needed [38].

The cost of each unit of Gas varies according to the volume of available miners and their demand. On April 19, 2020, the average price was 22 Gwei per unit of Gas [28]. A Gwei is a fraction of the cryptocurrency Ethereum and corresponds to 0.000000001 of the value of 1 Ether [16].

Considering the value of each Ether at BRL 958.19 on April 19, 2020 [39], the cost per Gas of BRL is 0.00002108018. During the pilot implementation, it will be possible to check how much Gas the smart contract will consume to run. In this sense, to keep this cost at 1 BRL, the Gas expenditure cannot be bigger than 47,450 [10].

It is also important to note that the platform's users pay the cost of maintaining the Digital Certificate approved by ICP-Brasil. This cost varies according to the Certifying Authority chosen and the duration of the certification contract, for example, an annual value at Serpro for individuals of R$153.00 in 2020.[5]

Comparing the direct cost (price of service) and the opportunity cost of time spent face-to-face needed to get a document legally signed by a regular notary and the same service as the proposed solution of a blockchain notary in prices of 2020, they are similar, but the difference is dependent on Ethereum price, which is very volatile. However, considering the high indirect costs of false identity crimes, corruption in notary activities,[6] and the potential improvement in the sector's regulation activities, a blockchain notary is likely to be more efficient in providing the notary's services.

4.3 Political barriers

It is always important to highlight the impact of political will in implementing a new solution that could directly impact the current billionaire revenues acquired by notaries. In the case of the application of blockchain for real estate registrations in Honduras, it was observed that the lack of political will to

[4] https://www.tudorondonia.com/noticias/titular-decartorio-acusada-de-envolvimento-em-corrupcao-comdeputado-estadual-continuara-afastada,49416.shtml, accessed on June 07, 2020; https://jmonline.com.br/, accessed on June 07, 2020; https://g1.globo.com/rj/rio-dejaneiro/noticia/2020/01/17/prefeito-de-caxiaswashington-reis-vira-reu-por-corrupcao-passiva-emacao-por-fraudes-imobiliarias.ghtml, accessed on June 07, 2020.

[5] SERPRO. Digital Certification. 2020. Accessed on Abril, 19 of 2020. Available at: https://www.serpro.gov.br/clientes/certficacao_digital. Currently available at https://www.serpro.gov.br/links-fixos-superiores/assinador-digital/assinador-serpro

[6] In 2010, for example, the CNJ annulled 5 thousand property registrations in Pará, adding another 410 million hectares in fraudulent registrations (http://g1.globo.com/politica/noticia/2010/08/cnj-anula-5-mil-registros-imobiliarios-supostamente-irregulares-no-para.html 20/05/2019). To cite a more recent case, in 2019, federal agents arrested, in a single operation in Belford Roxo (RJ), 14 individuals, including notaries, clerks, and even a councilor accused of crimes such as embezzlement, falsification of public documents, and passive corruption within notary offices (https://g1.globo.com/rj/rio-de-janeiro/noticia/2019/02/28/forca-tarefa-faz-operacao-para-prender-quadrilha-suspeita-de-praticar-fraudes-em-cartorios-da-baixada-fluminense.ghtml).

change the status quo could be the difference between the success and failure of a project that affects the governors' power [40]. As an incentive for Brazilian policy to adopt a technology that would heavily impact tax revenues, one solution would be to maintain tax collection for various instances via smart contracts. This would have a negative financial impact on consumers who would use the tool. Still, at least it could encourage political will in its application while also bringing transparency in the revenues of the Union, states, and municipalities, which could be audited not only by the National Council of Justice but also by ordinary citizens interested in the responsible spending of public money.

4.4 Limits

Despite the technical contribution of the proposed architecture in identifying individuals (users) who will use notary services, which guarantees security to the solution, at least two limitations connected to economic barriers still remain. First, to consume the notary services in blockchain, an individual must have a digital certification. Second, all individuals using the blockchain notary services need to have a minimum value in Ether in their digital wallet.

5 Final remarks

This work contributes to the literature of notary architecture in blockchain by offering a way to include the identification of individuals using online services with is coherent with demands on notaries in countries under Civil Law.

The architecture proposed is suitable as it connects blockchain resources to regulatory, economic, and political requirements to offer a more efficient provision of notary services. There are several gains to adopting this framework. First, since a secure technological framework can replace the need to ask for services in person at the notaries, it reduces a very high cost, the opportunity cost of using labor hours to get other goods or services. Second, the solution can be implemented based on the current law and under regulatory requirements without needing amendments or similar changes. Third, as the solution reduces production costs and offers a better quality of services, it can offer more efficient services and keep the benefits for providers and the government. Fourth, blockchain supports adopting essential services according to the barriers discussed above. Fifth, the blockchain solution can bring more transparency to production costs, giving the government more information to define the regulated prices. Finally, given that the architecture eliminates the need to be in-person to ask for notary services, it can raise concurrency among notaries since the local monopoly can be overcome by online services, generating a more competitive and, thus, more efficient market.

The results indicate the feasibility of applying a blockchain solution within the services of Notary Publics in Brazil, respecting historical, disciplinary, and legal principles. However, to achieve this objective, individuals must invest in purchasing and maintaining digital certificates approved by a Central Authority, which can be costly given Ethereum's price. However, considering the solution offers many additional benefits, such as reducing false identity and corruption crimes and the potential improvement in the sector's regulation activities, to be investigated in future studies, the solution can improve social welfare. It is important to note that in the solution, the infrastructure used for maintaining records is financed exclusively by the individuals at the time of the execution of the smart contract, based on the use of a public blockchain. But there is room for alternative solutions based on public provision. Since the Latin American countries are under civil law and have very similar institutions to Brazil, there is an opportunity for these countries to also benefit from a digital certification service more accessible. This is because it is a more efficient solution, and there would be no expenditure of public resources to maintain and support an infrastructure installed in the country.

A shared and immutable database would allow the centralization and transparency of all records made by notary offices and thus provide a safer service and be less prone to process deviations, whether intentional or not. As the solution adheres to the current legislation and has economic benefits, it tends to increase its potential for adoption. Also, this online tool can reach a large part of the population of emerging countries as they are widely connected.

Author contributions Leonardo and Marislei wrote the manuscript Leonardo made the calculations and Figures Leonardo and Marislei planned the paper Luciano gave suggestions on preparing the paper All authors reviewed the manuscript

Funding The funding was provided by Coordination for the Improvement of Higher Education Personnel (CAPES) (Scholarship) and National Council for Scientific and Technological Development (CNPq) (Scholarship).

Data availability Data sharing not applicable to this article as no datasets were generated or analysed during the current study. Additional material can be obtained by request with the authors.

Declarations

Conflict of interest The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper (Blockchain and Smart Contract Architecture for Notaries services under civil law: A Brazilian experience).

Appendix

See Fig. 8.

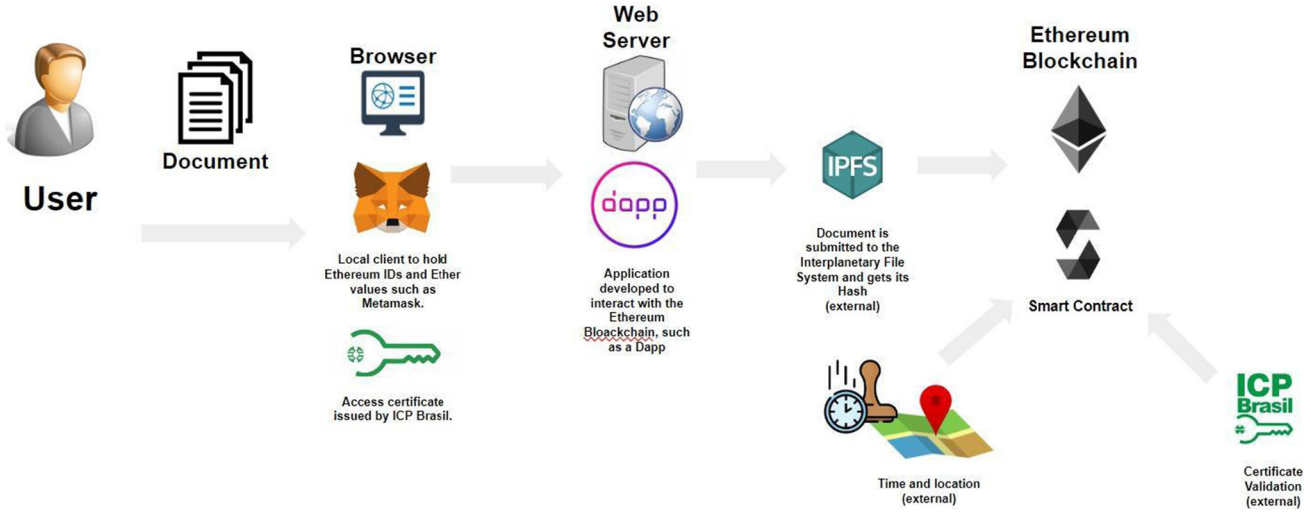


Fig. 8 Proposed architecture general view

References

1. Grimmelikhuijsen, S.G., Welch, E.W.: Developing and testing a theoretical framework for computer-mediated transparency of local governments. Public Adm. Rev. **72**(4), 562–571 (2012). https://doi.org/10.1111/j.1540-6210.2011.02532.x
2. Kotka, T., Vargas, C., Korjus, K.: Estonian e-Residency: Redefining the nation-state in the digital era. University of Oxford Cyber Studies Programme working paper 3 (2015).
3. Lepik, L.M.: e-estonia, www.e-estonia.com. Accessed on August 15 (2019).
4. Montenegro, M.C.: Transparência: CNJ mantém acesso irrestrito a informações sobre receita de cartórios (2019). http://cnj.jus.br/ (2019) Accessed on July 25 2019.
5. Berliner, D.: The political origins of transparency. J. Politics **76**(2), 479–491 (2014). https://doi.org/10.1017/s0022381613001412
6. Varella, M.D., Oliveira, C.G., Moesch, F.: Frog leap: in public policies through digital government: opportunities and challenges. Braz. J. Public Policy **7**, 561 (2017)
7. Carson, L.D., Prado, M.M.: Using institutional multiplicity to address corruption as a collective action problem: lessons from the Brazilian case. Q. Rev. Econ. Finance **62**, 56–65 (2016). https://doi.org/10.1016/j.qref.2016.07.009
8. Harris, C.G.: The risks and dangers of relying on blockchain technology in underdeveloped countries, NOMS 2018–2018 IEEE/IFIP Network Operations and Management Symposium, pp. 1–4. IEEE (2018). https://doi.org/10.1109/NOMS.2018.8406330
9. Feitosa, L.V.S., Costa, C.E.S.: Inovações no setor público: a resistência à mudança e o impacto causado no comportamento do indivíduo. Anais do V SINGE (2016). ISSN: 2317-8302
10. Menezes, L.D.: Blockchain e cartórios: uma solução viável? Dissertação de Mestrado, Escola de Artes, Ciências e Humanidades, Universidade de São Paulo, São Paulo. (2020). https://doi.org/10.11606/D.100.2020.tde-30122020-160504
11. Szalachowski, P.: PADVA: a Blockchain-based TLS notary service. In: IEEE 25th International Conference on Parallel and Distributed Systems (ICPADS), pp. 836–843 (2019). https://doi.org/10.1109/ICPADS47876.2019.00124.
12. Gao, Y., Pan, Q., Liu, Y., Lin, H., Chen, Y., Wen, Q.: The notarial office in E-government: a blockchain-based solution. IEEE Access **9**, 44411–44425 (2021). https://doi.org/10.1109/ACCESS.2021.3066184
13. Sousa, P.S., Nogueira, N.P., Santos, R.C., Maia, P.H.M., Souza, J.T.: Building a prototype based on Microservices and Blockchain technologies for notary's office: an academic experience report. In: IEEE International Conference on Software Architecture Companion (ICSA-C), pp. 122–129 (2020). https://doi.org/10.1109/ICSA-C50368.2020.00031.
14. Páez, R., Pérez, M., Ramírez, G., Montes, J., Bouvarel, L.: An architecture for biometric electronic identification document system based on blockchain. Future Internet **12**(1), 10 (2020). https://doi.org/10.3390/fi12010010
15. Ulloa, R., Gallegos, P.: Design of a Blockchain Architecture and Use of Smart Contracts to Improve Processes in Notary Office. In: Botto-Tobar, M., Montes León, S., Torres-Carrión, P., Zambrano Vizuete, M., Durakovic, B. (eds.) Applied Technologies. ICAT 2021. Communications in Computer and Information Science, vol. 1535. Springer, Cham (2022). https://doi.org/10.1007/978-3-031-03884-6_34
16. Crosby, M., Pattanayak, P., Verma, S., Kalyanaraman, V.: Blockchain technology: beyond bitcoin. Appl. Innov. **2**(6–10), 71 (2016)
17. Nakamoto, S. Bitcoin: a peer-to-peer electronic cash system. Decentr. Bus. Rev. 21260 (2008). https://bitcoin.org/bitcoin.pdf
18. Szabo, N.: Formalizing and securing relationships on public networks. First Monday (1997). https://doi.org/10.5210/fm.v2i9.548
19. Mohanta, B.K., Panda, S.S. & Jena, D.: An overview of smart contract and use cases in Blockchain technology. In: 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2018, pp. 1–4 (2018). https://doi.org/10.1109/ICCCNT.2018.8494045.
20. Buterin, V.: A next-generation smart contract and decentralized application platform. White Paper **3**(37), 2–1 (2014)
21. Lima, LB. Cartório de Notas - O que faz? (2017). Accessed on Mar 27, 2020, [Online]. https://cartorioonlinebrasil24h.com.br/blog/cartorio-denotas-o-que-faz/
22. Gruber, J.: Public Finance and Public Policy. Macmillan, New York (2005)
23. Siqueira, S. *Plenário da Câmara faz primeira sessão virtual de votações nesta noite* (2020). Accessed on May 10, 2020, [Online]. https://www.camara.leg.br/noticias/647856-plenario-da-camara-faz-primeira-sessao-virtual-de-votacoes-nesta-noite/
24. Brasil. PORTARIA No 467, DE 20 DE MARÇO DE 2020 (2020). Accessed on Mar 27, 2020, [Online]. http://www.planalto.gov.br

25. Rohden, S.F., Matos, C.A., Curth, M.: Intenções de recompra e confiança do consumidor on-line. Revista de Ciências da Administração, Universidade Federal de Santa Catarina **18**(45), 9–24 (2016). https://doi.org/10.5007/2175-8077.2016v18n45p9
26. Qin, K., & Gervais, A. (2018). An overview of blockchain scalability, interoperability and sustainability. Hochschule Luzern Imperial College London Liquidity Network.
27. Wüst, K., & Gervais, A. (2018, June). Do you need a blockchain?. In: 2018 Crypto Valley Conference on Blockchain Technology (CVCBT) (pp. 45–54). IEEE.
28. Etherscan. Ethereum Gas Tracker (2020). Accessed on April, 19 of 2020. https://etherscan.io/gastrackeri.
29. Metamask. A crypto wallet gateway to blockchain apps (2020). Accessed on November 17 of 2020. https://metamask.io/index.htmli
30. Raval, S.: Decentralized Applications: Harnessing Bitcoin's Blockchain Technology, vol. 1. O'Reilly Media, Sebastopol (2016)
31. Li, D.H.H.: Edurss: A blockchain-based educational records secure storage and sharing scheme. IEEE Access **7**, 179273–179289 (2019). https://doi.org/10.1109/ACCESS.2019.2956157
32. Group, T.B.: Ganache, one Click Blockchain (2020). Accessed on November 17 of 2020. https://www.truesuite.com/ganachei.
33. Docs, R.: The Remix Ide Documentation (2020). Accessed on November 17 of 2020. https://remix.readthedocs.io/en/latest/i.
34. Docs, R.: The Solidity (2020). Accessed on November 17 of 2020. https://docs.soliditylang.org/en/v0.7.4/i.
35. Jehle, G.A., Reny, P.J.: Advanced Microeconomic Theory, 2nd edn. Addison Wesley, Boston (2000)
36. Nishijima, M., Sarti, F.M., Cati, R.C.: The underlying causes of Brazilian corruption. In: Rotberg, R. (ed.) Corruption in Latin America. Springer, Cham (2019). https://doi.org/10.1007/978-3-319-94057-1_2
37. Oliveira, D.: A cultura dos assuntos públicos: o caso do "custo Brasil." Revista de Sociologia e Política (2000). https://doi.org/10.1590/S0104-44782000000100008
38. Wood, G.: Ethereum: a secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper **151**(2014), 1–32 (2014)
39. COINMARKETCAP. Coin Market Cap. (2020). Accessed on April 19 of 2020. hhttps://coinmarketcap.com/pt-br/i.
40. Benbunan-Fich, R, Castellanos, A.: Digitization of land records: from paper to blockchain (2018).