Improving the Process of Lending, Monitoring and Evaluating through Blockchain Technologies

An Application of Blockchain in the Brazilian Development Bank (BNDES)

Gladstone Moises Arantes Junior, José Nogueira D'Almeida Jr., Marcio Teruo Onodera,
Suzana Mesquita de Borba Maranhão Moreno, Vanessa da Rocha Santos Almeida
BNDES – Brazilian Development Bank
Rio de Janeiro, Brazil
{glads, josej, marcio.onodera, suzana, vanessa}@bndes.gov.br

***Abstract*— This paper describes a proposal for a process of lending, monitoring and evaluating development projects in the Brazilian Development Bank using blockchain technology. After highlighting the difficulties to implement this proposal, this paper also discusses what can be done as a transition process and outlines what have already been done. The proposals increase transparency of public money allocation, simplify manual activities, reduce operational costs and produce data to support aggregate analysis of the benefits arising from the bank's loans.**

Keywords—blockchain; transparency; development bank; public sector;

I. INTRODUCTION

Trust is in crisis at several spots worldwide [1]. As the Internet and social networks promote information disclosure, broadening the scope of personal opinions, institutions and media vehicles deal with the population's discredit. Due to distrust and facilities created by information technology, society demands a more transparent and agile government. Digital government, also called e-Government, can be defined as the use of information technology to render services and engage citizens [2].

Several technologies may be employed in e-governments, and blockchain is one of them. Blockchain technology [3] is a new way to make value transactions feasible and store the data generated in a distributed way, being an alternative to traditional centralized systems, without the need for a reliable intermediary to manage the information. The information is stored in a peer-to-peer network after consensus between nodes. In such infrastructures it is not possible to change data previously stored. When in public networks, such as Bitcoin [4] and Ethereum [5], completely anonymous parties that do not trust each other can build up a network that stores reliable information [6].

Tapscott [7] states that blockchain technology can be used to improve service rendering while ensuring information integrity and transparency. Examples of use of this technology in government services include: public records anti-fraud storage, such as private property and criminal records; individual or legal person digital identification, and national currency digitalization. Several banks all over the world are exploring Blockchain technology for finance services too [8].

This paper describes an improved process of lending, monitoring and evaluating development projects counting on BNDES public financing. The key component to enable the process improvement is a proposed mechanism to track funding, called BNDESToken. This paper also explains how BNDES is implementing a transition solution, which is going to be used during proofs of concept in some financing projects.

The remainder of this paper is divided as follows: Section II presents an overview of the current business scenario and highlights relevant activities. Section III discusses the proposed process and what the main difficulties are to implement it. Section IV describes a transition solution taking into account the difficulties mentioned in Section III. Section V delineates what has already been implemented, also stating relevant technical aspects. Section VI details the main related works and how they can be compared with the proposal of this paper. Lastly, Section VII presents our conclusions and next steps.

II. OVERVIEW OF THE BUSINESS SCENARIO

The Brazilian Development Bank (BNDES) [9] is the main financing agent for development in Brazil. Since its foundation, in 1952, BNDES has played a fundamental role in stimulating the expansion of industry and infrastructure in the country. The Bank offers several financial support mechanisms to Brazilian companies of all sizes as well as public administration entities, enabling investments in all economic sectors.

BNDES has several tools to finance the investment needs of its clients on a long-term basis. Support mechanisms are divided into financing, non-reimbursable resources and subscription of securities. The focus of this paper is the mechanism of financing, but the overall idea can be easily adapted to non-reimbursable resources.

BNDES Financing is earmarked for investment projects, isolated acquisition of new machinery and equipment, exports of machinery, Brazilian equipment and services and the acquisition of goods and production inputs. BNDES has several funding resources to finance long term investments in Brazil. In 2017, 80% of these resources came from the Brazilian government.

Fig. 1 illustrates the activities relevant to the context of this paper.[1] Some activities must occur before Fig. 1 first step. In short, they are: (i) The development bank must approve a development project to a client. A legal contract must state the conditions of each disbursement; (ii) a client asks for a disbursement to the development bank; (iii) The development bank approves the disbursement.

In step 1, the development bank makes a fiat money transfer to a client using a service of commercial banks.[2] In step 2, the client pays some contractors using a service of commercial banks. In general, a client can pay many contractors using the money of the same disbursement.

Step 3 shows that the client proves his money spending to the development bank. The proof must include contractor's payment receipt to prove that the client paid contractors and what products or services type were commercialized.

In step 4, the development bank approves client's proof. The goal of this activity is to guarantee that the money was used as planned. It can involve a significant amount of manual work. The development bank publishes lending information in step 5. The society can now see how the money was used.

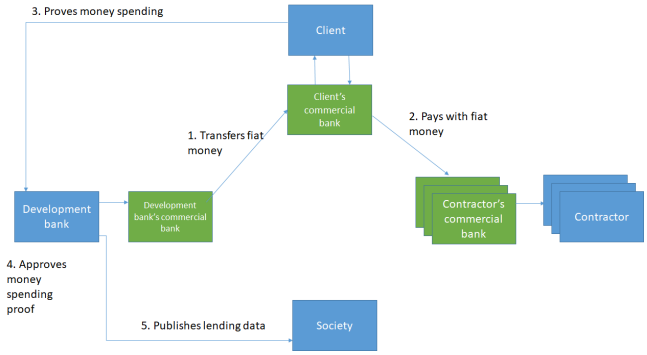

Fig. 1. Relevant activities – business scenario.

It is possible to spotlight three main points in this scenario. The first one is that the process information is fragmented between the development bank, client and contractors. Integrating data would improve the process efficiency, while minimizing cost. Also, in order to improve transparency, it is important that society can access information without intermediation. Secondly, technology can be used to segregate disbursement approval and money transfer to client. Since these two concepts are tied together, in order to minimize paperwork, the development bank has to disburse large amounts of money to its clients. Clients take some time to spend all the money so they have to invest the funds. If the value of investment interest rate is greater than the value of the lending interest rate, clients may opt to postpone the project schedule. It is possible to improve both the process efficiency and fiat money allocation if the disbursement date becomes closer to when the client pays its contractors. Finally, maximizing process automation would increase efficiency of processes, while reducing verification and audit costs, especially in steps 3, 4 and 5.

III. PROPOSAL DEFINITION – FUTURE VISION

The proposed solution is a payment system that is illustrated in Fig. 2.

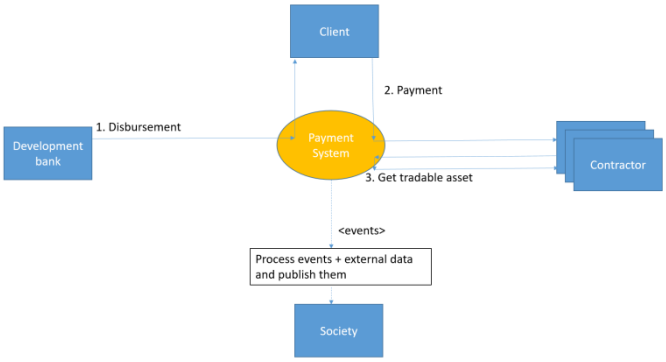

Fig. 2. Relevant activities – future vision.

First, in order to be a user of the payment system, the development bank, clients and contractors need to register themselves.

In step 1, the development bank requests the payment system to make a disbursement. The system checks if the development bank is authorized and the client is enabled to receive the disbursement. If true, the system transfers a representation of money from the development bank to the client. The system emits a <disbursement event>.

The client requests the system to make a payment to a contractor in step 2. The system checks if the client is authorized and has enough balance and if the contractor is enabled to receive the payment. If true, the system transfers a representation of money from the client to the contractor. This transfer demonstrates what products or services are commercialized. In addition, it has legal value to be used as money spending proof of the client. The system emits a <payment event>.

In step 3, a contractor requests the redeeming of its representation of money. The payment system checks if the contractor is authorized and has enough balance and if the payment system has enough tradable assets – defined as an asset that can be traded outside this system, for example a liquid digital token that can be traded for fiat money. The system emits a <redemption event>.

When a trigger event of the payment system is observed, the publishing software updates the lending information.

[1] In reality, it is a very simplified explanation. There are some differences between BNDES products and programs regarding these activities.

[2] In reality, BNDES can make transfers as a commercial bank. However, in order to segregate responsibilities, this text describes as if a commercial bank was needed to initiate a bank transfer.

Some technological solutions could have been chosen to represent the payment system. A first solution is to create a system with a traditional database, an API and a WEB layer to provide account creation, value transfer and an information presentation dashboard.

The inviolability of information could be guaranteed by procedures and audits. The first disadvantage of this solution is the centralized data management. From an external observer's point of view, the information could be manipulated by the responsible institution with consent from the auditors. Moreover, audits are performed afterwards while the ideal solution should guarantee real-time inviolability. A third disadvantage is the high cost and effort to maintain the mentioned procedures and audits.

In addition, there are other requirements for the payment system. As previously described, the centralized system should be able to demonstrate what products or services are commercialized with legal value and to transfer tradable assets.

The use of blockchain technology in the payment system allows society to rely on the irrevocable inviolability of information without the need for a trust relationship with the centralizing entity. The inviolability of information together with smart contract capabilities allow transactions to achieve legal value in the future [10] [11]. Finally, it is a natural choice to transfer digital tokens.

The key of the proposed blockchain solution is a smart contract with a proprietary token to track funding, called BNDESToken. BNDESToken [13] is defined as a mechanism to track public funding route in projects counting on BNDES financing, providing society with information on how they are promoting the country's development.

Each unit of BNDESToken is equivalent to one Brazilian fiat currency, the real (1:1). Fixed quote is a simple way to create a mark in national fiat currency. BNDESToken is distributed at the moment of financing disbursement and the token is always owned by the person/institution that owns the Real. By adopting a technology that allows verifying who is in possession of the token, a mechanism is obtained to trace the funds desired in real time. Therefore, in practice, BNDESToken is only a digital representation of the Real, analogous to a voucher for future funding redemption.

IV. PROPOSAL DEFINITION – TRANSITION VISION

The future vision of the proposed definition assumes it is possible to have blockchain transaction linked to products or services with legal value. This section is a transition proposal aiming to drive proof of concepts projects.

Six assumptions are selected so as to simplify the proposal adoption by simplifying coordinating efforts with other institutions and technical implementation [12]. The first is that the token issuance does not increase the economic monetary base, since BNDES ceases to disburse the Real, but maintains it as guarantee. The second assumption refers to the fact that BNDESToken cannot be passed on indefinitely. BNDES issues the token during the funding provision, which can be passed on a few times in the chain and then must be redeemed with the BNDES System. This assumption avoids the creation of secondary capital market to the proposed token. The third is that the total amount of BNDESToken of an account does not change over time. That is, there is no inflation correction on token balance of an account. The fourth assumption is that only legal entities with e-CNPJ (see definition later) are eligible to receive BNDESToken. Individuals may be considered at a later time, depending on a more in-depth analysis. The fifth assumption is that tokens are fungible. There is not a unique identifier for each BNDESToken. When tracing some funding separately is needed, one should review this simplification. The last assumption is that transfer events are not automatically linked to milestones of the client project.

The first decision to the transition proposal was the use of either a permissioned or a permissionless blockchain network, and the option was for a permissionless network because of four main reasons, as follows: (i) the greater the number of nodes involved in consensus algorithm decision the more difficult it is to defraud the data. There are public blockchains with thousands of nodes. To obtain a permissioned blockchain with the same computational capacity, BNDES would need to partner with many institutions interested in participating as a node. This activity would take a long time, preventing BNDES from starting a proof of concept project. Regarding the permissioned network with few nodes, an external observer could understand that there is a possibility of agreement between the nodes of the network at the moment of the execution of the consensus algorithm; (ii) the transparency itself, which is somehow complementary to the previous one. Permissionless blockchains allow data monitoring to be performed even without the use of tools provided by BNDES. Anyone can connect their monitoring software to the permissionless blockchain and follow the events in real time; (iii) it is more likely that a solution that makes a blockchain transaction linked to products or services with legal value will be available in a network with a large number of participants and where open innovation is possible, i.e, in a permissionless blockchain; (iv) BNDES is already carrying out a proof of concept with a permissioned blockchain, as discussed in Section VI.

The criteria for choosing what permissionless blockchain should be adopted were platform maturity and program execution capability to express business domain rules. The decision for the use of the Ethereum blockchain network was due to the fact that, along with Bitcoin, it shows greater maturity than the other options [1]. Furthermore, Ethereum still allows the creation of very powerful smart contracts (Turing complete), able to guarantee the necessary business rules. This ability to produce complex smart contracts is different from Bitcoin blockchain, which supports relatively simple scripts.

On the Ethereum platform, the token concept represents a digital asset whose value may or may not correspond to a real asset. Tokens are themselves implemented as smart contracts that maintain the balances of each address and can be

programmed according to predefined patterns. The proposed solution uses the well-known ERC-20 standard as a foundation and complements it with the necessary business rules. The ERC-20 is the de facto standard of the Ethereum platform, with more than 500 tokens created, which together manage more than $ 25,000,000,000.00 [15].

Using the standard brings a number of advantages. First of all, people who know the Ethereum platform understand the contract much more easily, since most of its methods are inherited from the standard token. Second, some blockchain explorers such as EtherScan (https://etherscan.io/) already have specific functionalities to present ERC-20 contract information. Finally, it is possible that Ethereum platform programs capable of executing contract methods – such as MyEtherWallet (https://www.myetherwallet.com/) – evolve to be able to negotiate any tokens, as well as other services that, over time, may be implemented on ERC-20.

The core of the solution is to use an ERC-20 contract to represent BNDESToken. The contract contains the balances of all entities that have BNDESToken and provides methods such as asset transfer, issuance and destruction of tokens, besides balance view.

Fig. 3 illustrates the transition vision of the proposed solution.

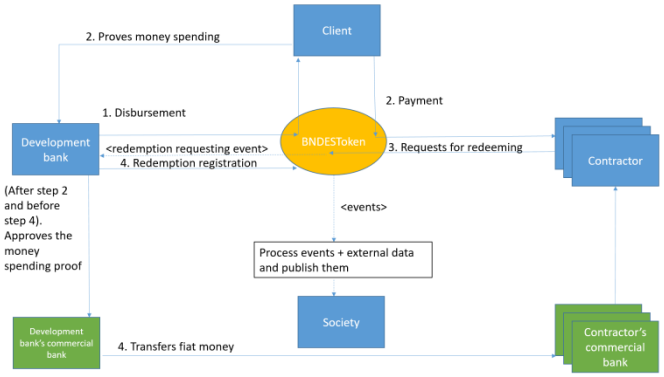

Fig. 3. Relevant activities – transition vision.

As in the future vision, in order to be a user of BNDESToken, the development bank, clients and contractors need to register themselves.

In step 1, the development bank requests BNDESToken to make a disbursement. The smart contract checks if the development bank is authorized and the client is enabled to receive the disbursement. If true, the smart contract mint new tokens and transfers them from the development bank to the client. The smart contract emits a <disbursement event>.

The client request for payment in step 2. The smart contract checks if the client is authorized and has enough balance and the contractor is enabled to receive the payment. If true, the smart contract transfers tokens to the contractor. This transfer does not demonstrate what products or services are commercialized. Then, although the transfer contains token values, it cannot be used as a complete money spending proof. Also in step 2, the client proves his money spending to the development bank. The smart contract emits a <payment event>.

In step 3, a contractor requests the redeeming of its tokens. DLT checks if the contractor is authorized and has enough balance. If true, DLT burns the received BNDESTokens and emits a <redemption request event>. In step 4, The development bank observe that a redemption request event has occurred and pays the contractor using a service of commercial banks. It also registers the redemption using the smart contract.

At some time after step 2 and before step 4, the development bank approves the money spending proof. When a trigger event of DLT is observed, the publishing software updates the lending information.

The following subsections detail the functioning of business identification, token transfers, client operations tracking, and solution transparency.

A. Identification of legal persons

To receive BNDESToken, legal persons must have been previously identified; therefore there must be a mapping of the legal person's identity in the real world, which is performed through its Ethereum account, in order to assure that identification. This mapping must be verified in a reliable way into BNDESToken smart contract, be valid for a given predetermined time space, and periodically revalidated.

Ideally, the government could render service similar to that which is performed for individuals in Estonia, through the e-Residency program [16]. If any official government service recorded this mapping on the blockchain or provided a digitally signed service with the mapping, there would be no issue to be resolved.

Although this alternative does not exist, the Brazilian government maintains the National Institute of Technology (http://www.iti.gov.br/), which coordinates the operation of the ICP-Brasil (Brazilian Public Keys Infrastructure). ICP-Brasil (http://www.iti.gov.br/icp-brasil) and is a reliable hierarchical chain that enables digital certificates issuance for virtual identification of individuals and legal entities. In Brazil, each legal entity has a unique identification that is called a CNPJ number (National Database of Legal Entities). All legal entities represented by a CNPJ number can issue an e-CNPJ. The e-CNPJ Digital Certificate is one of the digital certificates issued by the body, and it is an electronic identity document that guarantees the authenticity of issuers and recipients of documents and data that travel on the Internet, as well as ensuring their privacy and inviolability.

The e-CNPJ is used to send labor, social security and tax information to the government. According to the Internal Revenue Service [17] [18], since the beginning of 2017, the use of e-CNPJ is mandatory for all legal entities except companies opting for the Simples Nacional (taxation system) with up to three employees. Even legal entities that do not have the certificate may come to contract it. Therefore, this paper

assumes as a premise that the legal entities that negotiate BNDESToken have the e-CNPJ.

The identity mapping proposal of this article consists of registering a relationship between the e-CNPJ and an Ethereum wallet address belonging to the legal entity. The legal entity can be either the BNDES client or a client's contractor (or, in some cases, a financing support entity, as is the case of the transfer entity for some donation projects). If it is the client, the credit disbursement is divided into sub-credits depending on the particularities of the project being developed by the client. There should be an identity mapping for each client's sub-credit.

The mapping should be maintained in a decentralized manner. The proposal is for the user together with the e-CNPJ, to sign a document that explicitly associates the CNPJ number with the blockchain address. This same user uses the same address to send the signed document to the blockchain. The smart contract that receives this information performs document signature validation through a code recorded on the blockchain. If the signature is validated, as the contract is sure that the owner of the address is the one who executed the transaction, it is explicit and guaranteed that the association is valid.

From there, any case of use can only verify that the association exists, and can focus its work on its own business functionalities. The identification use case of this article can carry out the necessary verifications for the BNDES register (for example, legal impediments of a company, certificates, etc.) before enabling the legal person to negotiate BNDESTokens.

The mapping should be public. With the open information, external observers may audit and find possible issues on the database.

B. Transferences

New BNDESTokens are issued when BNDES disburses funds to a client's authorized account as discussed in the previous subsection. This transfer increases the client balance and the total balance of tokens issued. In general, a financing operation can be carried out in one or more disbursements. Each disbursement happens on a schedule agreed with the client, which may depend on delivery milestones in a project, for instance.

The client can issue registry payment orders to authorized contractors as long as they have sufficient balance and the transaction complies with the transfer rules. In some scenarios analyzed, such as payment of taxes, the client may need to redeem part of the amount received.

At some point, a legal entity "PJ" requests the exchange of BNDESTokens for fiat currency. The proposal is that this should occur as follows:

(1) the legal entity "PJ" requests the exchange of x number of BNDESTokens from an address of its property, called "CNT";

(2) the smart contract verifies whether the redemption request rules have been met, as, for example, if the token has already passed on to the minimum number of legal entities required, and the request is timely;

(3) a transfer is triggered on the "CNT" smart contract to a known redemption address in BNDES' possession;

(4) the smart contract destroys x number of tokens and triggers an exchange request event;

(5) a BNDES' system receives the redemption request event, verifies business rules to ensure the validity and security of the transaction and, if necessary, makes financial reallocations to enable the transfer of x reais – considering the already mentioned quotation of R$ 1 (1 real);

(6) BNDES carries out a bank transaction of x reais to the bank account of the legal entity "PJ" informed at the time of its registration and publishes a bank transfer evidence;

(7) BNDES records that bank transfer was realized and the smart contract records the completion of the bank transfer along with some evidence data (e.g. the hash of the published document in step 6);

(8) The smart contract triggers an event to indicate that it has made the requested redemption;

(9) An interested system of "PJ" can watch the event and perform some action according to its business processes.

Another option evaluated for steps 6 and 7 above was to send an amount equivalent to "x" in digital currency (Ether) to the address of "PJ". The advantage of this option is that the whole financial transaction would be carried out in the blockchain itself, without involving the banking system. In fact, it is the option described in Section III (Future Vision). However, this option was not adopted in the transition proposal for three reasons. The first is the high exchange rate risk associated with changes in the value of Ether in relation to fiat currencies. The second is the costs associated with using a third-party to exchange the digital currency for fiat currency if the redemption requestor wants to use fiat money. Finally, this option introduces regulatory risks and greater cultural change to "PJ". All these disadvantages can change in the future.

C. Impacts on operations monitoring

After the operation is contracted, the client has to account for the funding allocation performed. It is the financial and physical monitoring (money spending proof).

To perform the financial monitoring, nowadays the client has to send bank receipts periodically or after some milestone. With BNDESTokens, all transactions are automatically visible, bringing submission time and operation confirmation to the network, mitigating human activities and increasing information reliability.

To perform physical monitoring, the client has to send a document proving incurrence of each expense (invoice of a product acquired, for instance). The proposal foresees the

development of an off-chain functionality, in which the client is able to describe each expense and upload documents. It is interesting to observe that this change stimulates the verification to be performed at the moment of transfer of funding to the contractor, and not posteriorly as is normally verified at present.

D. Transparency

Any external observer can visualize the information adhering to the ERC-20 standard through a browser for the blockchain used. For Ethereum, there is the previously mentioned EtherScan. For example, the browser presents the total BNDESToken balance, token addresses and details of the transfers made.

To visualize BNDESToken domain specific information, an observer can develop his/her own application to read blockchain data, register to receive events issued by the smart contract, and access public service data that he/she deems reliable.

This work foresees the development of an online responsive dashboard, aiming only to facilitate the transactions monitoring, since such monitoring does not depend on a tool built by BNDES. In this application, the blockchain data can be related to off-chain data to facilitate user interpretation. For example, the dashboard may present legal names instead of the Ethereum address and brings the information in graphs in granular or aggregate form. In addition to providing details to track transfers, the proposal foresees the dashboard should have additional links to EtherScan for client accountability, for data collected from online services, such as the size and location of legal entities, and for data managed by BNDES, such as detailing of financing projects.

V. Present Phase of Implementation

BNDES is working to achieve a proof of concept of the proposal described in Section IV as reported in [19]. The project was prioritized to be carried out after winning an internal innovation contest with participation of more than three hundred competitors. The contest, called ideaLab, established that the winning proposals would have six months to generate an initial result for the bank, when there would be reassessment of priorities. At the present time, BNDESToken has just a little more than four months of project and a team of five people.

So far, the development includes an initial version of BNDESToken smart contract, a Web application to facilitate user interaction, and an online dashboard. The development initial focus was token transfer functionalities, client tracking and online dashboard. The current development presupposes the existence of clients and contractors, and the token is always disbursed by BNDES to a client, who transfers it to one or more contractors. These contractors cannot transfer the token again, needing to request the redemption from BNDES. This is in accord with the second assumption described in Section IV.

The corporate identity module is still being discussed by the team and will probably be implemented as an independent smart contract to create a generic solution to be reused by other applications in the future. The project aims to leave this legacy to the country and has been searching for partnerships, including the National Institute of Technology, in order to work towards this direction. Currently, BNDESToken smart contract contains a mapping for legal entities in order to enable the use of other functionalities of the application.

The token smart contract is written in Solidity and deployed on Rinkeby network, one of the Ethereum test networks. To sign transactions, the user needs to use a browser extension, such as Metamask [20], whose implementation still only supports a few browsers. The application uses JavaScript language, with Angular and Typescript on the presentation layer, and NodeJS on the server. MongoDB database is used to store information that does not go to the blockchain. Integrations with the bank's internal systems have not been developed.

E. Data Structures

The relevant data structures of the BNDESToken smart contract are illustrated in Fig. 4. As mentioned in Section IV, BNDESToken follows the ERC-20 standard and therefore maintains the balance of each address that registers to use the token (see line 1 of Fig. 4). In addition, the smart contract also contains the CNPJ number of each Ethereum address and, in the case of a client, the information of which sub-credit identification of the financing project it is associated with (see lines 2-6 of Fig. 4).

```
1. mapping (address => uint256) public balanceOf;
2. struct PJInfo {
3.    uint cnpj;
4.    uint idSubcredito;
5. }
6. mapping (address => PJInfo) public pjsInfo;
```

Fig. 4. Relevant data structures of BNDESToken smart contract.

The WEB application currently stores information in the MongoDB database registration information associated with each CNPJ number – such as e-mail, telephone, location, company name, sector and bank details. Some of this information will no longer be stored locally when integrations are developed to fetch data associated with a CNPJ number.

For each payment order, the following information is stored in the database: source and target ID data, description and attached documents, hash of blockchain transaction, and date and time the transaction was requested by the client. This data is used to compose the operations tracking functionality described in Subsection IV.C and the dashboard panel.

For each redemption, the following information is stored in the database: requesting contractor ID, bank details of the contractor at the time of the redemption request, whether the redemption is settled or not, hash of the redemption request and of the redemption blockchain transactions and date and time the transaction was requested by the contractor. This data is used to compose the redemption functionality described in step 7 of Subsection IV.B and the dashboard panel.

BNDES plans to perform proofs of concept with clients of Brazilian public administration later this semester. On these

loans, there are no questions regarding business secrecy, so they are a good start point to analyze the usage of this solution.

VI. Related work

A Canadian government's research and development body, the National Research Council, has recently announced a prototype system to publish how managed funds are being allocated to projects [21]. The system stores project information on Ethereum public blockchain. However, only the initial disbursement is discussed, and there is no trace of what happened to the funds after the first action.

KfW (https://www.kfw.de/), the German development bank, has developed a system called TruBudget, to track funding routes by recording each step of the workflows and approvals, carried out by different partner institutions which work together to finance and implement projects, minimizing the risk of misuse of funds [22]. By allowing the definition of workflows in a flexible way, the system can be used as a monitoring and recording instrument in different scenarios of use of a project or process.

TruBudget was developed using MultiChain [23]. Because it is a permissioned blockchain, the transactions performed are taxation-free, since it is not necessary to remunerate the network transactions validator. In addition, it is possible to have autonomy to define which nodes participate in the network and who visualizes the information stored. In this way, network participants may agree on whether the access to information on the platform can be disclosed to other interested parties or be open to the public as, depending on the case of use, some information may be subject to legal restrictions. It is important to note that TruBudget does not represent a payment token, which implies no regulatory issues and minimizes the implementation effort on the clients, including impact on business processes. On the other hand, the use of the token proposed by this article makes the solution more trustworthy since funding transfer is inseparable from the registration of each workflow step of the funding route.

TruBudget is currently being deployed at BNDES to track funding donations to the Amazon Fund, whose resources come mostly from Norway and Germany through KfW [24]. BNDES plans to perform proofs of concept with beneficiaries of the Amazon Fund later this semester.

In addition to governments, it is possible to find information tracking solutions using blockchain in other domains. For example, Everledger has a diamond supply chain tracking system to ensure origin, minimizing falsification and maximizing the use of an adequate extraction process [25]. Fundraising entities for charity are also using blockchain to enable "ultra-transparent" donations. Solutions like GiveTrack [26], which initially used only the potential of cryptocurrency to facilitate the delivery of resources, has been developed to give more transparency to the donor, who is interested in knowing whether their funding has come to the project, whether it has already been used, and how. Finally, NU's WFP (World Food Program), body of food distribution, has been using a solution to distribute tokens that can be exchanged for food in humanitarian aid regions, such as Syrian refugee camps [1]. The project, called Building Blocks, which also contains a personal identification solution for biometric analysis, aims at having more efficient and inexpensive means for distributing aid, including seeking integration with information from education and health agencies.

VII. Conclusions and next steps

Blockchain has shown to be a very promising technology for BNDES to present how funds move through the economy after disbursement, serving as input for monitoring public money allocation and for research on the effectiveness with respect to contributing to the country's development. The proposal described in this paper can be used by other development banks, government agencies or other entities that wish to track their funds disbursed and analyze how they were used.

The in-depth understanding of technology has also made the authors of the paper aware of additional advantages, such as simplification of monitoring process for the client, possible creation of new financial products, and the possibility of measuring the real effects of development policies. The authors also understand that with the increasing adoption of blockchain technology, the world will increasingly reuse existing smart contracts for different purposes, decreasing the costs of transactions of value exchanges.

A relevant issue arising from the change in the business model by the introduction of the BNDESToken is the possible impact on how credit relationship is established. Currently, funding transfer of the contract in fiduciary currency begins at the moment of credit disbursement to the client. With the use of this new technology, the moment of transfer of fiat currency is postponed until a later moment, when BNDESToken redemption takes place.

A number of questions arise: what exactly can this change of credit relationship entail contractually? When does interest on the loan start to be applied? How can BNDES invest the fiat currency that has not yet left the cash? Is there any regulatory impact? What kind of financial instrument is BNDESToken in the event of a legal dispute? How to deal with business and/or bank secrecy when operations involve companies? How does tax collection work when a transaction is paid with BNDESTokens and not with fiat currency? What procedures and verifications are required to enable a contractor? These are important issues that the authors still have to address.

There are several next steps for the project. A first point is an in-depth study of the solution for identification of legal entities. In the current proposal, those employees who have access to the digital certificate have the full power over BNDESToken. It is necessary to consider how to increase the flexibility of the solution in order to improve governance and accountability of legal entities' employees.

A second point is how to make user's experience simpler. The concepts and tools of use have not been popularized in

society. In the case studied, for example, users who send transactions to the Ethereum network need to install Metamask and have Ether to pay the blockchain tax fee. Society in general needs to pass through maturation regarding the concepts to understand why the use of technology increases the reliability of the information presented.

A third point is that currently all data recorded on the blockchain are public, but it is possible that business secrecy (such as dates, prices and quantity of purchased items, for example) makes it necessary to give privacy to some information. This requirement has not been considered in the proposal so far.

Another point is to re-evaluate whether Ethereum is actually the most appropriate blockchain platform for the solution. It is necessary to follow the dynamic development and maturity of the blockchain market taking into account the requirements of the solution, especially data privacy.

The authors also foresee the construction of new cases of use around BNDESTokens. Some of them linked with future vision as, for instance, automatic tax collection, token transfer associated with electronic invoice. Other ones linked with new requirements arising during discussion with stakeholders, like the control of the geographical region in which the BNDESToken can be used, preventing it from being used outside a given city, or sent abroad.

Finally, the development of proof of concept should be improved and tested in real scenarios in order to obtain an overview of the main problems to be solved, and the priority of each one of them.

REFERENCES

[1] R. Edelman, "2018 Edelman Trust Barometer", 2018. [Online]. Available at: https://www.edelman.com/trust-barometer. [Accessed: Apr. 15, 2018].

[2] Center for Technology in Government, "A working definition of e-government", University at Albany. [Online]. Available at: https://www.ctg.albany.edu/publications/reports/future_of_egov?chapter=2. [Accessed: Apr. 15, 2018].

[3] G. Y. Allayannis and A. Fernstrom, "An Introduction to Blockchain", Darden Case No. UVA-F-1810, 2017. [Online]. Available at SSRN: https://ssrn.com/abstract=3050049. [Accessed: Apr. 15, 2018].

[4] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008. Available at: https://bitcoin.org/bitcoin.pdf. [Accessed: Apr. 15, 2018].

[5] G. Wood, "Ethereum: A secure decentralized generalized transaction ledger", 2014. Available at: https://ethereum.github.io/yellowpaper/paper.pdf. [Accessed: Apr. 15, 2018].

[6] M. E. Peck, "Do You Need a Blockchain?", 2017. Available at: https://spectrum.ieee.org/computing/networks/do-you-need-a-blockchain, IEEE Spectrum. [Accessed: Apr. 15, 2018].

[7] D. Tapscott and A. Tapscott, "Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World", 2016.

[8] L. M. Applegate, R. Beck, and C. M.-Bloch. "Deutsche Bank: Pursuing Blockchain Opportunities (A)." in Harvard Business School Case 817-100, Apr. 2017.

[9] BNDES, "The Brazilian Development Bank", 2018. [Online]. Available at: https://www.bndes.gov.br/SiteBNDES/bndes/bndes_en. [Accessed: Apr. 15, 2018].

[10] R. T. Ainsworth and A. B. Shact, "Blockchain (Distributed Ledger Technology) Solves VAT Fraud", Boston Univ. School of Law, Law and Economics Research Paper No. 16-41. Oct. 17, 2016. [Online] Available at SSRN: https://ssrn.com/abstract=2853428 or http://dx.doi.org/10.2139/ssrn.2853428. [Accessed: Apr. 15, 2018].

[11] K. Hegadekatti and Yatish S G, "The Programmable Economy: Envisaging an Entire Planned Economic System as a Single Computer Through Blockchain Networks", Mar. 30, 2017. [Online]. Available at SSRN: https://ssrn.com/abstract=2943227.

[12] M. Iansiti and K. R. Lakhani, The Truth about blockchain, in Harvard Business Review, January-February 2017.

[13] G. M. Arantes Jr., J. N. D Almeida Jr., M. T. Onodera, S. M. B. M. Moreno and V. R. S. Almeida. "BNDESToken: A Proposal to track BNDES' Funding Route", "BNDESToken: Uma Proposta para Rastrear o Caminho de Recursos do BNDES" (original in Portuguese), in WBlockchain, SBRC, 2018, in press.

[14] M. Bartoletti and L. Pompianu, "An empirical analysis of smart contracts: platforms, applications, and design patterns", in Financial Cryptography and Data Security, Springer, 2017, pp. 494-509.

[15] Asseth Stream1. "Jodi Baylina & Jacques Dafflon - ERC 777 Q&R", Ethereum Community Conference, France, YouTube, Mar. 9, 2018 [Video file]. Available at: https://www.youtube.com/watch?v=qcqhryzGTy0. [Accessed: Apr. 15, 2018].

[16] "e-identity". [Online]. Available at: https://e-estonia.com/solutions/e-identity/e-residency/. [Accessed: Apr. 15, 2018].

[17] Receita Federal do Brasil, "Information about the Requirement to Use Digital Certificates", "Informações sobre a Obrigatoriedade de Utilização de Certificado Digital" (original in Portuguese), 2015. [Online]. Available at: http://idg.receita.fazenda.gov.br/orientacao/tributaria/senhas-e-procuracoes/senhas/certificados-digitais/informacoes-sobre-a-obrigatoriedade-de-utilizacao-de-certificado-digital-com-atualizacoes-da-in-rfb-no-1-036-2010. [Accessed: Apr. 15, 2018].

[18] Receita Federal do Brasil, "Nº 125 Resolution", "Resolução nº 125" (original in Portuguese), 2015. [Online]. Available at: http://www8.receita.fazenda.gov.br/simplesnacional/noticias/NoticiaCompleta.aspx?id=8bb40fb6-5eff-418d-b38b-987f8b90e762. [Accessed: Apr. 15, 2018].

[19] Trustnodes, "Brazilian State Bank to Tokenize Brazilian Real on Ethereum's Public Blockchain", Mar. 6, 2018. Available at: https://www.trustnodes.com/2018/03/06/brazilian-state-bank-tokenize-brazilian-real-ethereums-public-blockchain. [Accessed: Apr. 15, 2018].

[20] "Metamask - Bring Ethereum to your browser", 2018. [Online]. Available at: https://metamask.io/. [Accessed: Apr. 15, 2018].

[21] National Research Council of Canada, "Blockchain Publishing Prototype", 2018. [Online]. Available at: https://nrc-cnrc.explorecatena.com/en/. [Accessed: Apr. 15, 2018].

[22] KfW, "Blockchain boosts effectiveness of development cooperation", 2017. [Online]. Available at: https://www.kfw.de/KfW-Group/Newsroom/Latest-News/Press-Releases/Pressemitteilungen-Details_426112.html. [Accessed: Apr. 15, 2018].

[23] MultiChain, "MultiChain – Open Platform for Building Blockchains", 2018. [Online]. Available at: https://www.multichain.com/. [Accessed: Apr. 15, 2018].

[24] A. Mari, "Brazilian and German development banks agree blockchain partnership", 2018. [Online]. Available at: http://www.zdnet.com/article/brazilian-and-german-development-banks-agree-blockchain-partnership/. [Accessed: Apr. 15, 2018].

[25] Everledger, "Diamond Time-Lapse Protocol", 2018. [Online]. Available at: https://www.everledger.io/. [Accessed: Apr. 15, 2018].

[26] BitGive, "GiveTrack: Donation Tracking", 2018. [Online]. Available at: https://www.bitgivefoundation.org/givetrack-static/. [Accessed: Apr. 15, 2018].

[1] World Food Program, "Building Blocks", 2018. [Online]. Available at: http://innovation.wfp.org/project/building-blocks. [Accessed: Apr. 15, 2018].