Triple entry ledgers with blockchain for auditing

Felipe de Oliveira Simoyama*

Universidade Federal de Sao Paulo (UNIFESP),
R. Angélica, 100, Jd. das Flores,
Osasco, SP, 06132-380, Brazil
Email: simoyama@usp.br
*Corresponding author

Ian Grigg

R3CEV,
NYC 1370 Broadway,
Ste 1050 New York, NY 10018, USA
Email: iang@iang.org

Ricardo Luiz Pereira Bueno and
Ludmila Cavarzere de Oliveira

Universidade Federal de Sao Paulo (UNIFESP),
R. Angélica, 100, Jd. das Flores,
Osasco, SP, 06132-380, Brazil
Email: ricardo.bueno@unifesp.br
Email: lu.trt2@gmail.com

Abstract: Legislation generally requires public agencies to account for their activity to the public. Among the many duties imposed by legislatures around the world are requirements for transparency in procurement of services, budgeting and presentation of accounts. However, agencies in countries with high corruption problems have trouble complying with the legislation, especially in smaller agencies. Moreover, it is typically infeasible for national auditors to audit all the accounts rendered, and instead, they select a small sample for audit based on their level of risk. Another problem is that the presentation of accounts occurs once a year for all agencies, leading to a seasonal demand with significant lag time between auditing and accounting period. In this study, we present a non-technical framework based on the emerging technology of blockchain that could be a solution to all these concerns. We apply it within the context of Brazilian legislation and the Federal Court of Accounts of Brazil (TCU), although the proposal is applicable across a wide range of countries facing severe corruption.

Keywords: court of accounts; public accounts; blockchain; corruption.

Reference to this paper should be made as follows: Simoyama, F.d.O., Grigg, I., Bueno, R.L.P. and de Oliveira, L.C. (2017) 'Triple entry ledgers with blockchain for auditing', *Int. J. Auditing Technology*, Vol. 3, No. 3, pp.163–183.

Biographical notes: Felipe de Oliveira Simoyama is a graduate student in Public Administration at Universidade Federal de São Paulo (UNIFESP) and in complex systems modelling at Universidade de São Paulo (USP).

Ian Grigg is a financial cryptographer who has worked on secure protocols, rights, identity, governance, systems audit and startups within the digital cash and digital trading space. He is currently working with R3 on identity and dispute resolution for financial smart contracts and with Solidus on peer-to-peer secure payments for remittance channels.

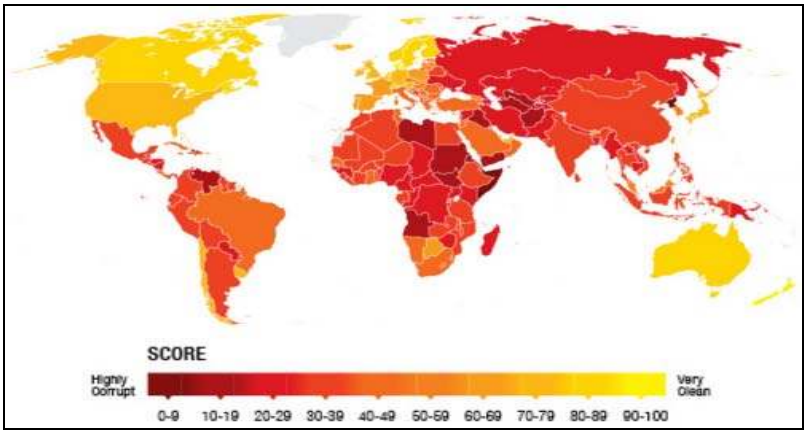
Ricardo Luiz Pereira Bueno is a Business Administration and Strategy Professor at Universidade Federal de São Paulo (UNIFESP). He holds a Master's degree in Public Administration at Fundação Getúlio Vargas (FGV)m and a Doctor's degree in Business Administration at Universidade Federal do Rio Grande do Sul (UFRS).

Ludmila Cavarzere de Oliveira is a Master in Public Policy and Organization Management (2016), specialist in Planning, Implementation and Management of Distance Education (2015), specialist in Public Management (2008) and Bachelor in Translation and Languages – Portuguese, English and Spanish (2003). She is experienced in the area of coaching, instructional design of online courses, translation and proofreading. Currently, she is working for the Labour Court of Law in São Paulo, Brazil.

1 Introduction

Brazil scored 43 points on the corruption perceptions index (CPI) in 2014, which is considered a high-level of corruption (Figure 1), placing it in the 69th position of the CPI ranking. Moreover, recent corruption scandals (Romero, 2012; The Economist, 2015a) show that current preventive controls are not as effective as they should be. In 2013, the Brazilian Chamber of Deputies estimated that corruption leaves out nearly 85 billion of reals per year (Câmara dos Deputados, 2013). In 2007, the Ethos Institute estimated that the cost of corruption in Brazil to be an approximate amount of 180 billion of dollars per year (Penteado, 2007).

Figure 1 CPI infographic of corruption (see online version for colours)



Source: CPI (2014)

One important aspect of corruption is its contagious effect, since the more a society faces corruption, the less their agents will behave honestly. A recent study performed by Villoria et al. (2012) showed that perceptions of corruption are associated with lower levels of institutional trust. Despite Brazilian initiatives towards transparency and participatory culture such as the participatory budget (Walker, 2016), it did not seem to revert the ability of agents to commit frauds.

During recent years, Brazil has evolved in certain respects such as the issuing of the Brazilian Fiscal Responsibility Law (2000), the New Accounting Standards Applied to the Public Sector (2012) and the Brazilian Transparency Law (2011). Even though the supervision of these standards is one of the most important roles of TCU, it does not seem to hinder corruption, since fraudulent agents continue to find different ways to cheat. In fact, Brazil holds a good grade in terms of transparency (scoring 77 in the 2015 open budget index), but the method does not take some issues into consideration, e.g., the tendency of Brazilians not to check public accounts, the level of education required to interpret financial statements and sufficiency of public documents required to detect fraud.

It should be considered that Brazil has institutions to ensure anonymous complaints such as the Public Prosecutor's Office (MPU), the Comptroller General of the Union (CGU) and the TCU. The latter is responsible for external auditing of Brazil's federal agencies and the Union's accounts with the power to impose sanctions and fines, and its annual budget adds up to more than 1.5 billion of reals. One of its main jurisdictions is the *ex post* analysis and issue of opinion on public agencies' yearly accounts, which are mostly comprised by written financial statements and activities reports. However, due to its own size and structure limitations, the TCU cannot carry out an audit on all these accounts, rather it needs to perform audit sampling. Further, not all of these audit samples can be fully analysed. The written reports provide some useful information, but a full audit requires deep investigation, interviews with employees and tests. Queiroz (2004) argues that investigations are more complex, because they require the auditor to use their intelligence with the utmost care (Queiroz, 2004). Although evidence suggests TCU has been efficient in repairing significant values to union's coffers (TCU, 2015), it certainly does not suffice in the fight against corruption.

Technology, however, can shine some light on more efficient auditing procedures, and technology is also an important strategy to enhance public engagement in the participation process. Bryson et al. (2013) argue that technology helps in achieving public participation purposes, since it enables the sharing of information 'typically available only to experts' and also the 'gathering of real-time feedback from participants', while inclusive processes engage diversity. The benefits of electronic participation have been demonstrated by Kim and Lee (2012) by analysing data from the Seoul Metropolitan Government, showing that a reasonable electronic platform can be positively associated with participants' trust in government. During the last decade, the tech-world has been shaken up with bitcoin, the first so-called cryptocurrency, a concept created in 2008 and known as one of the first decentralised virtual currency in the world (Nakamoto, 2008). As well as being a virtual asset, it is also a payment system, as all bitcoin transactions are recorded in a digital distributed public ledger called a blockchain (Luther, 2016). Behind the technology of blockchain, there are complex math calculations, protocols and cryptography to ensure safety of transactions by avoiding fraud, double spending and forging. Evidence of the success of bitcoin can be found in Greece (PR Newswire, 2015)

and Argentina (Benedict, 2015), where recent fiat currency collapses led citizens to invest in bitcoin as an alternate money.

The success of bitcoin begot a great enthusiasm, especially amongst IT and finance experts and economists, and the community of enthusiasts are constantly seeking new applications for the underlying blockchain technology (The Economist, 2015b). Startups such as the Bitnation have actually proposed that the technology can completely replace government services as we know it, for example citizenship identification and public notary services. In effect, the full breadth and depth of applications built on blockchain technology are yet to be appreciated.

For our purposes, the main advantages of blockchain technology include the immutability of the records, the distributed database, the audit trail recording and strong cryptography. We argue that these are important features for audit work, and it is worthwhile to carry out an exploratory research in order to formulate a method to apply such features for auditing. For example, blockchain can be useful to make triple-entry ledgers (Grigg, 2005) achievable, thus allowing cost-effective preventive controls for fraud deterrence.

This article highlights the opportunities made possible by blockchain for auditing and controls over public agencies. However, it is not our purpose to set the technical parameters for its implementation, but rather to present a conceptual framework for the improvement of audit systems. Further, we aim to raise awareness for the possibilities for enhanced risk perception, reduction of costs of control, enhanced transparency and improved auditors' performance by more precisely directed fields of work. Finally, although we present it within the context of Brazil's TCU, this proposal would be equally applicable for any country that employs a national auditor and is concerned with or suffers a corruption deficit to public finances.

2 Methods

Here, we propose a non-technical framework based on the so-called permissioned blockchains technology, also known as private blockchains, combined with the triple-entry ledgers approach by Grigg (2005). This framework is aimed at fighting corruption by increasing transparency, auditing capacity and risk perception. Our proposal was framed as an anti-corruption intervention around the case study of TCU. In order to build this framework, we explored the literature on:

a the factors that determine occurrence of corruption

b strategies recommended by researchers to fight and hinder corruption

c blockchain technology

d the TCU's current framework.

Then, in the last section, we report how the features of our proposed framework are positively aligned with recommendations made by researchers of public administration and political sciences.

3 Effectiveness of control

The TCU requires from Brazilian agencies the implementation of strong internal controls in order to prevent and identify fraud (TCU, 2009), but they also require that the costs of such controls do not exceed the benefits derived there from. However, the future benefits arising from controls cannot be measured *a priori* or even be reasonably estimated. For example, when an agency hires an employee for internal control purposes, it is not possible to measure the economic gains the employee can possibly generate, since the benefits will only be obtained *ex post*. There have been many proposals to improve decision making on internal controls, such as calculation based on opportunity costs, calculation based on gains obtained in the previous period and allocation of investments based on risk level. Although such methods could possibly serve as better predictors than a random walk, there remains a human incapacity to rationally allocate resources for internal control.

The TCU (2015) declares that its benefit-cost ratio is of 3.76, i.e., for each money unit spent by TCU, it returns 3.76 units to the public coffers. This was based on Table 1 plus an amount of 2,079,158,598.89 reals in fines issued in the same period, totalling 6,126,910,800.75 reals. The total cost of TCU amounts to 1,627,537,901.28 reals.

Table 1 TCU monetary results as for 2014

Monetary benefits of TCU	*Amount (in Brazilian reals)*
Irregularity corrections	903,832,291.33
Improvement of government programs efficiency	2,423,996,614.81
Improvement of the efficiency in government agencies administration	235,244,875.56
Reduction in the maximum price of bids	162,695,558.27
Increase in the minimum price of privatisations	321,816,401.89
Other	166,460.00
Total	4,047,752,201.86

Source: TCU (2015)

The most significant values (better efficiency of government and correction of irregularities) are highly subjective. Also, it does not take into account the costs incurred by public agencies in order to comply with TCU requirements. Moreover, it does not consider the opportunity costs of either capital or labour allocation.

However, even if TCU estimates are deemed correct, its net results would amount to 4,499,372,899.47 reals, which is very distant from the estimated 85 billion of reals of annual embezzlement in Brazil, which indicates that current controls are not sufficient in both preventive and corrective approaches, encouraging the development of new methods and systems for auditing.

4 Triple-entry ledgers

Traditional accounting relies on the double-entry bookkeeping system, being at essence a credit-debit mechanism where any entry in an account demands a corresponding entry to a different account. The mechanism of double entry bookkeeping has provided the reliable accounting needed within the enterprise to support the growth of firms since being first documented by Luca Pacioli in 1494. In contrast to the classical double entry framework, Boyle (1997) and Grigg (2005) propose ledgers based on triple entries which provide the same reliable accounting *between* firms that double entry provides *inside* the firm.

Consider a transaction enacted jointly by three parties being a payer, a payee and an issuer, such as is conducted by banks and their customers routinely. The payer sends units of money to the payee (for example, a cheque), and the issuer (a bank) is responsible for verifying and signing the transaction, transferring the money and issuing a receipt for both payer and payee to update their books. Grigg argues that this model, so far a very trivial transaction indeed, gives too much centralised power to the issuer, who would be a powerful candidate for internal fraud.

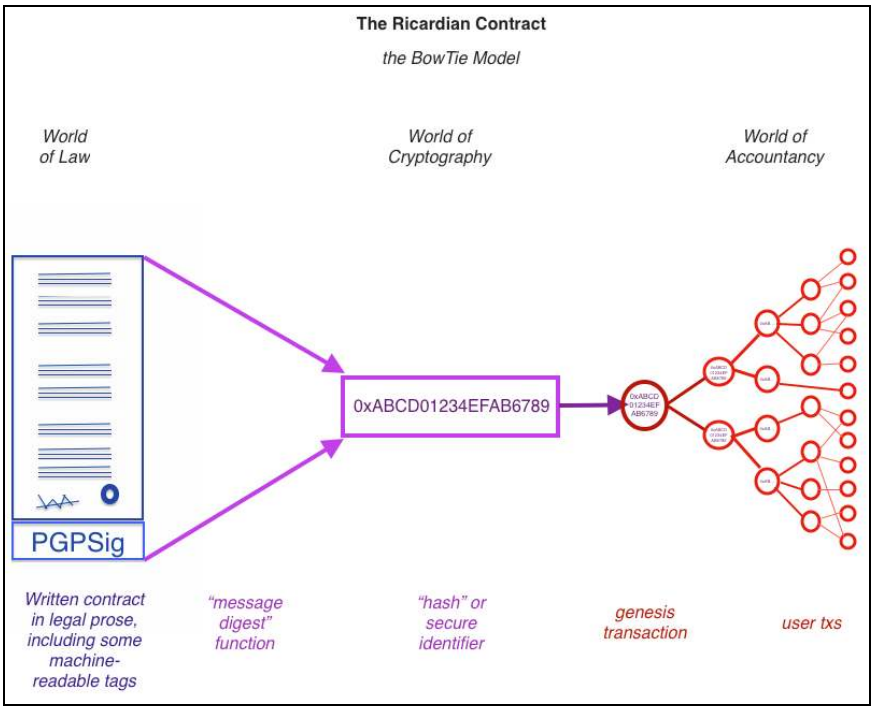
In order to reduce the issuer's capacity to commit fraud, he proposes triple entry accounting with the very advantage that the three parties involved are guaranteed to hold exactly the same information, and no party may introduce unauthorised information. Grigg's proposal for triple entry is a single, cryptographically secured record called 'the receipt'. The full evidentiary force of the receipt is ensured by the digital signatures of both the authorising payer and the accepting issuer, thus ensuring that no party can successfully pass off an unauthorised transaction as valid. To Grigg, this reduces the problem of accounting to that of presence or otherwise of the receipt, which would then be guaranteed by sharing copies of the receipt between all the parties involved. To conceptualise this approach, Grigg says that 'the receipt is the transaction' and the ledger thus becomes the collection of all receipts.

The proposed receipt would contain the original authorisation from the user, the server's response and also a Ricardian contract (see below) containing all the terms and conditions under which the parties are agreed upon to describe the very unit that is being transferred.

5 Ricardian contracts

The Ricardian contract, as defined by Grigg (2004), is a digital contract containing all of the terms and clauses as of a regular written contract, but it is readable both by people and by software. The document is digitally signed, and a unique and secure identifier, a cryptographic message digest or hash, is generated over the contents (see Figure 2). The digital signature affords strong reliability on the contents as being authentically from the named signatory, and the hash provides a strong identifier that can be embedded into all transactions, including the triple entry transactions above, to fix them with a particular contract.

Figure 2 The Ricardian contract (see online version for colours)



Source: GRIGG (2004)

The Ricardian contract was originally proposed as a way to lock down the semantics of an issuance of value from an issuer to holders of that value in a contractually defendable fashion. See Figure 3 for a demonstration issuance of tokens redeemable for refreshments. Odom (2015) extended the use of Ricardian contracts into all forms of parameterisation and also into the payments themselves. Odom further proposed that Ricardian contracts could even include prior contracts, creating a Russian Dolls pattern of advancing trade negotiations, a pattern that has been used successfully by e.g., OpenBazaar to handle eBay-style shopping negotiations.

Despite the high security provided by modern cryptography (e.g., SHA1 message digest algorithm and document signing with RSA or EC), the main advantage of a Ricardian contract is that it allows reliable queries as if it were a database; those contents that are expected to be searched are clearly marked in the text for extraction by code, as shown in Figure 4.

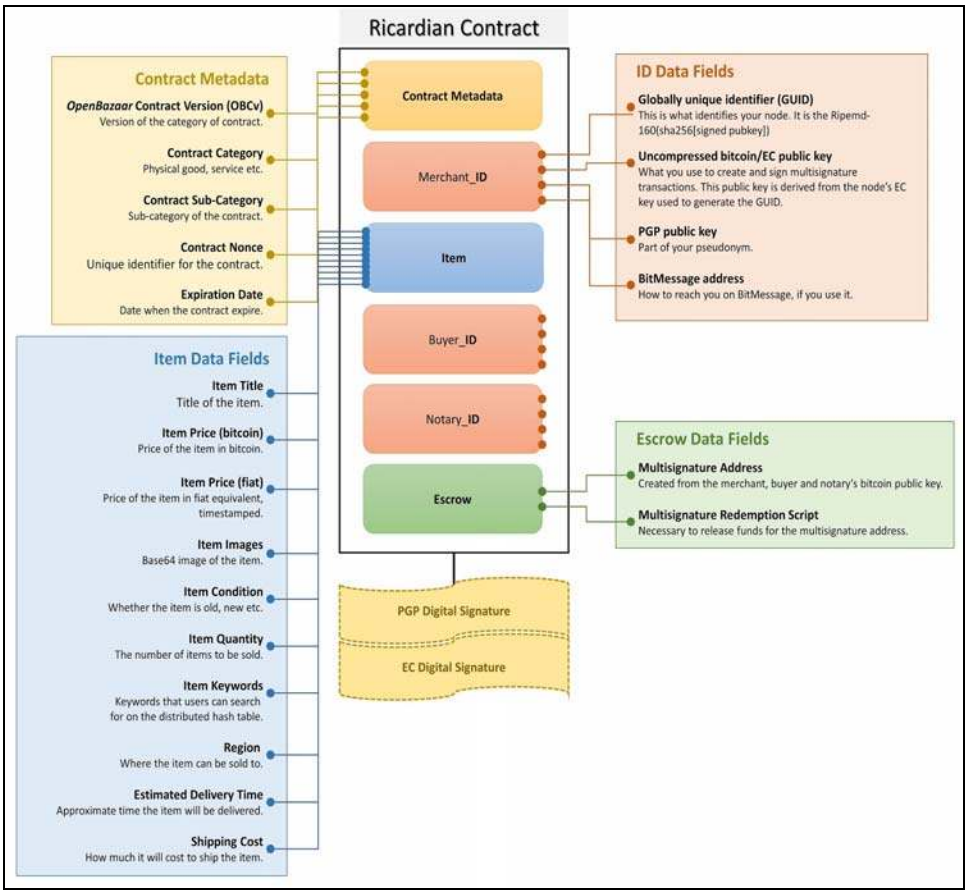
This sort of electronic document can be used for several purposes, for example, replacing bid and auction documents, financial instruments and regular contracts. Hence, if the TCU has access to all the agencies' searchable contracts, it can also analyse and compare these documents for a more preventive and effective approach to fight corruption.

Figure 3 Rachel's beer vouchers (abbreviated)

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

;
;  Rachel's Beer Vouchers
;
;  Issued by Rachel Willmer
;
[entity]
entity_shortname=Rachel
entity_longname=Rachel Willmer
entity_email=rachel@willmer.org

[issue]
;
;  This section identifies the Operator of the issue server,
;  (the "Operator") responsible for the technical hosting/management
;  of system hardware and software.
;
issue_company = Systemics, Inc.
;
;  Systemics, Inc. will initially function as Operator, per
;  Operator Contract posted at
;  http://www.willmer.org/demo/ricardo/contracts/operator/
;  hereafter referred to as the "Contract Publication URL".
;
;  **Notices issued pursuant to this currency contract, such as
;  changes in sub-contractor arrangements, will be published
;  and maintained at the Contract Publication URL**
;
;
issue_email=issue@systemics.com
issue_contract_url= *
{
http://www.willmer.org/demo/ricardo/contracts/issue/
}
issue_type=currency

[currency]
currency_name=pints of beer
currency_tla=BEER
currency_symbol=pt
currency_type=decimal
currency_factor=1
currency_decimal_power=0
;currency_fraction=mg

[conditions]
conditions_backing= *
{
  Rachel's Beer Vouchers are payable to bearer pint for pint in
  fine British beer, on demand, subject to the conditions specified i
  currency contract.

  Rachel will maintain at all times a primary reserve of British
  cash in an amount sufficient to purchase (from a British pub of
  her choosing) pints equivalent to 100% Rachel Beer Vouchers in
  circulation.
}
```

Source: Willmer (2000)

Figure 4 The schema of a typical Ricardian contract (see online version for colours)



Source: Grigg (2004)

Ricardian contracts are a very important addition to our framework since the main sources of corruption are not the transactions per se, but are rather the activities around the payments: negotiations, agreements and deliveries that result in the misuse of public funds. Ricardian contracts afford parties the opportunity to define in full the meaning of their transactions, and to lock in that meaning to the transaction. In some cases, corrupt acts are 'lawful but immoral' which hampers the work of audit for its uncertainty. In this manner, technological enhancements assist the audit process by reducing uncertainty; as triple entry ledgers reduce uncertainty in the quantities and movements of transaction, Ricardian contracts reduce uncertainty as to meaning or semantics of the transactions. Audit is therefore lifted above the accounts and can focus on preventive actions, i.e., blocking the actions that give rise to corruption, overbilling and mismanagement. The task of detecting irregular payments does not suffice alone, firstly, because sometimes the terms on which the conditions were offered are legally approved, and secondly, illegal payments cannot be merely undone and these funds are arduous to recover.

Ricardian contracts and triple entry ledgers provided a great conceptual advance for both financial cryptography in general and a substantial evolution in accounting principles that could increase users' security and reduce costs of transaction. The designs

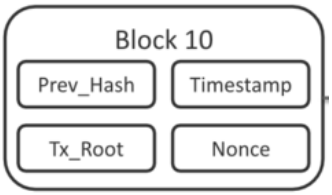
were described more technically by Howland (1996) and also Odom (2015), and code was released and used, but the market conditions that would put these theories into practice and thus present them to the wider audience did not arise until the emergence of bitcoin. The success of bitcoin however has now writ these possibilities large, and has made it possible for us to propose triple entry for wider benefit. It is to that system we now turn.

6 Blockchain and bitcoins

6.1 Bitcoin basics

Bitcoin is a decentralised digital or virtual currency integrated with a payment system, as invented by Nakamoto (2008). All bitcoin transactions are recorded in a publically distributed ledger known as the blockchain. The public ledger is not stored in a central server, rather, it relies on a peer-to-peer network to ensure that all of the full nodes have a copy of the entire ledger in their computers. The ledger is made of blocks with a 1 MB size limit that can contain hundreds, even thousands of transactions in each block. Each block refers to the previous, which refers to the one before, and so on back to the genesis block first created in 2009. A block of new transactions is approved by the consensus algorithm known as mining or Proof of Work, after which a message is broadcast to all nodes in order to update their ledgers with the approved block, and to start working on a newer block.

Figure 5 A sketch of a block in the bitcoin blockchain



A critical feature of bitcoin is the consensus algorithm. In simple terms, the process by which new blocks are approved in the bitcoin blockchain is called *mining*. At its lowest level, a block consists of a cryptographic hash code pointing to the previous block, a set of new transactions; a timestamp and a nonce (see Figure 5). The timestamp will be later analysed in this study, since it will be part of our framework. Mining is a lottery, being the challenge of calculating a costly math problem that reveals a winning number. In the process utilised by bitcoin, miners calculate a cryptographic message digest or *hash* over the entire block such that the hash has many leading zeroes. By varying the nonce, the miner can run through many combinations until a winning number is found. To incentivise, the winning miner is awarded 12.5BTC, and so miners fight for the winning number, ensuring that no one party can gain control. The bitcoin design is a complex but highly tuned interacting composite of parts, and the reader is referred to Nakamoto (2008) and the extensive literature for more details.

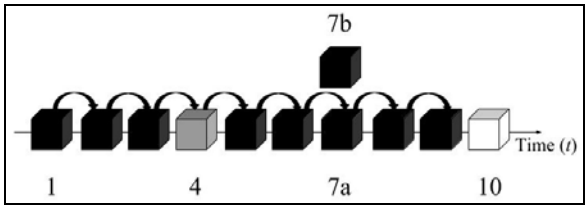
Blockchains can be of two types: permissionless or permissioned. Bitcoin is a permissionlessblockchain, as any user can participate and thus update the blockchain. Permissioned blockchains, however, are only accessible to a predefined list of agents,

such as a community, a bank's clientele, or a country's agencies. In a permissioned system, some features and costs are absent, such as the anonymity of access and the requirement for expensive proof of work. Some prefer the term of 'distributed shared ledgers' for permissioned ledgers, but in this article we use the more popular term of blockchain.

6.2 Blockchain structure

Blockchain can be defined as a growing public database of immutable records. Such records are stored in blocks containing data from the previous block, forming a chain, as shown in Figure 6. The block structure built in a linear, chronological order makes fraud very unlikely. For instance, if a fraudulent agent wants to make alterations in block 4 (grey), he would need to reconstruct all the way from block 4 to 9, while also building the block 10 (white), and all that before the other members of the network finish block 10 themselves. The 7b block is usually called an orphan block, *i.e.*, a valid block that is disconnected from the main (longest) chain. This mostly occurs when two miners build blocks simultaneously, however, only one of them is trusted by the network to have a 'parent'.

Figure 6 A simple form of a blockchain



In this manner, the block structure can be seen as a shared ledger trusted by all the nodes in the network. Each block contains permanent information, not only from the current, but also from the past transactions, creating a permanent link between each block in the chain.

6.3 Timestamping and the double spending problem

Because bitcoin's goals include digital cash, it needs a solution to the double spending problem. I.e., because there is no Central Bank, the system requires another way to establish credibility over monetary balances. The bitcoin design avoids the double spending problem by permitting only valid transactions over unspent balances into each new block, and ensures that no one in the network is able to change the parts of the ledger that are already accepted (*e.g.*, a transaction in a prior block). Therefore, each transaction once accepted within a block inherits the block's timestamp.

6.4 Proof of work and immutability

The proof of work concept is an important feature of bitcoin, since it is what provides for immutability of records and timestamps. In order to create the next block in the chain, some costly and time-consuming work (computing power) is required as described above.

Since each new block refers by hash to its predecessor, if one intends to change an earlier block, the miner would need to recreate all the blocks that follow it as their hash linkages would now be broken. The more blocks that have to be changed, the more difficult is the proof of work calculation needed, and therefore each block rapidly becomes immutable, i.e., unchangeable, as more blocks are added.

7 Enabling triple-entry with blockchain

Before proposing a framework for improving TCU's effectiveness, we should first examine the current procedures they put in place and analyse its strengths and weaknesses.

7.1 The current TCU framework

We can summarise the TCU auditing work as follows.

7.1.1 Annual report of accounts and activities

Every year, all the federal public agencies of Brazil are required to submit the annual report of accounts and activities to the TCU as provided by the Constitution of Brazil (articles 33, 71 and 74) and the internal rules of the TCU. For example, in the year 2014 1,622 accounts were submitted, of which only 350 (21.58%) were judged by the TCU's (Decisão Normativa No. 140, 2014). Most of the report is comprised by standard financial statements, tables and spreadsheets, but it also contains information that cannot be reduced to numbers or templates, such as: performance indicators (that vary according to each agency's nature), explanatory notes and other information free of technical detail (e.g., introduction and conclusion).

Recently, efforts have been made by TCU in order to standardise information provided by agencies through the annual reports (Decision No. 90, 2014), evidencing the difficulty in analysing a large number of reports from different agencies. For example, TCU has invested in a system for submitting the reports divided in sections, however, all these reports are sent in a PDF format and information cannot be extracted to be compared by the TCU, which needs to read and analyse the selected reports individually instead.

7.1.2 Special audits

Special audits are carried out by TCU when there is evidence of fraud or in the case of omission of the annual report by an agency. This type of audit work amounted to 1,903 cases in 2014, i.e., the total number of special audits exceeds five times the number of audits arising from the annual reports. Most of these special audits are required by the agency's own internal control or are originated from complaints.

7.1.3 Continuous monitoring

Continuous monitoring is the process of assessing performance of agencies against legal requirements in financial and accounting terms (Resolution No. 155, 2002). Most of this

work is comprised by assessment of government programs and projects, which is mainly enacted through database queries into the agencies' own management systems and official journals. This type of work allows for a more preventive approach. For example, official journals contain information about future public purchases not in compliance with the law. In 2014, TCU prevented a total of 484,511,960.16 reals from being spent in biddings, 162,695,558.27 of which by reducing the maximum price and 321,816,401.89 by raising the minimum price for privatisations (TCU, 2015).

Our study focus on the improvement of the three types of work above, each with a different approach. In our view, the bitcoin blockchain technology enables triple entry ledgers for auditing with some modifications in its infrastructure as detailed in this article.

7.2 New framework for government accountability

In order to set a triple entry approach for auditing in the TCU, the following premises are required:

1 All the transactions made by federal agencies should be recorded in a blockchain, including: financial transactions, government purchase contracts, call for bids, staff recruitment and others.

2 Every Brazilian federal agency should be required to be a node in the peer-to-peer network, i.e., they should store a copy of the blockchain in a local computer.

3 TCU should be a third party by timestamping every transaction made by federal agencies regardless of what the transaction is. Transactions that are not validated/timestamped by TCU should not have legal value. In this manner, TCU should also be a node in the network, but rather working as a free notary service.

4 There should be transaction database and analytical tools provided by TCU to citizens for transparency purposes.

At present, TCU functions as a central planner for the audit work, where all the agencies are required to submit reports to the TCU annually and wait for judgement. It works like a centralised network, as shown in Figure 7.

Figure 7 The current TCU status: a centralised network (see online version for colours)

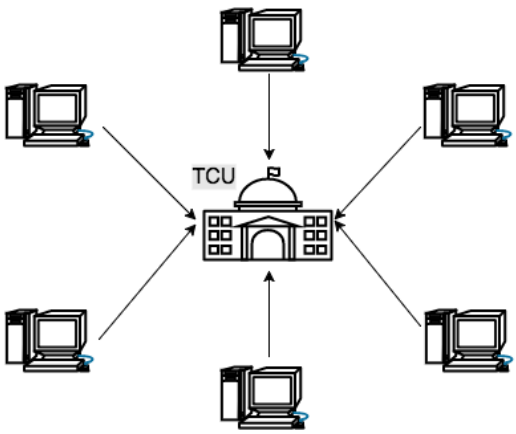
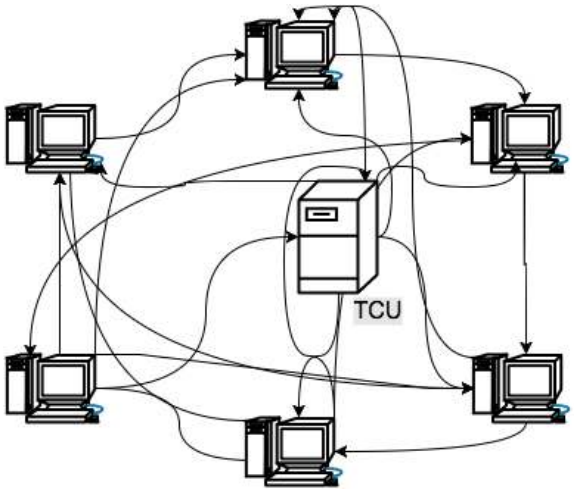
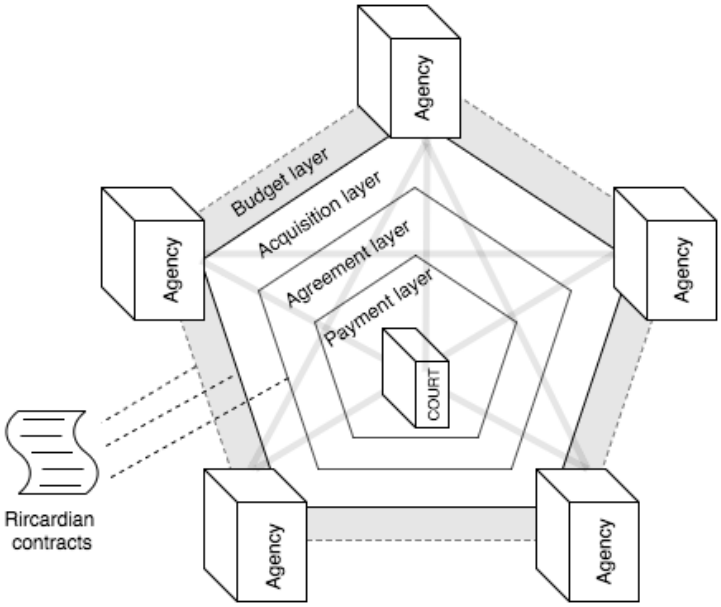


Figure 8 A proposal of a decentralised peer-to-peer network for TCU (see online version for colours)



In our proposal, the work of recording auditable events is required to be decentralised (Figure 8) and with real-time and continuous interaction between all the nodes (agencies). In addition, each node needs to continuously send to and receive information from TCU as it will work as a timestamper for all new transactions. In its turn, TCU carries out audit work by executing database queries in the public ledger, work that could be easily automated with the present technology. For example, TCU could set a warning in the case an agency publishes a call for bid with overpricing for a product (say a computer), and thus allow for close to 100% monitoring.

Figure 9 An overview of overlaying networks with blockchains



As previously stated, a reasonable and new audit framework should not only meet the needs of the current TCU's task, but rather create opportunities for improving it, especially in preventive action. In this manner, we propose an overlay of networks based on blockchain (see Figure 9). Here, we argue that four layers can enhance the TCU's power of auditing and thus curtail corruption. These layers are based on the stages of public procurement and expenditure of Brazil, as described in Table 2.

Table 2 The four-layer blockchain framework for auditing

Layer		*Description*
1	Budget layer (optional)	The first layer is the budget, which occurs on a yearly basis in Brazil. All Brazilian agencies would be required to record their yearly budgets in a standard Ricardian contract. This data of this Ricardian contract is then locked in on the blockchain and the document is timestamped by the TCU, thus receiving a unique and secure identifier.
2	Acquisition layer	In Brazil, bid documents (*editais*) are required to follow mainly the Federal Law number 8.666/93. In this manner, most of the sections of bid documents are mandated by law, such as: summary of items, maximum price per item, deadlines and warranties. All this information can be contained in a Ricardian contract and be easily tracked in real time by the TCU.
3	Agreement layer	The agreement layer is where the contracts between public agencies and private firms are registered. As well as the bid documents, the terms and clauses of contracts issued by public agencies are mostly law enforced, but they vary with the sort of purchase (products, business services, engineering *etc*.). In this way, Ricardian contracts can also be used to record such agreements.
4	Payment layer	The payment is the final stage of public expenditures in Brazil, since it only occurs after proper validation of delivered items. Payments are thus necessarily linked to prior agreements and bid processes. However, payments are merely the transfer of value after all the requirements from previous layers have been accomplished, and as they are made to parties outside the government and outside the blockchain, the payments will be made using the regular fiat currency systems available. Then, in contrast to layers 1, 2 and 3 which record Ricardian contracts as primary documents, the agencies should fully record all the transfers into the fourth layer as shadow transactions or replicas of the regular fiat transfers, instead of using a cryptocurrency (as with bitcoin).

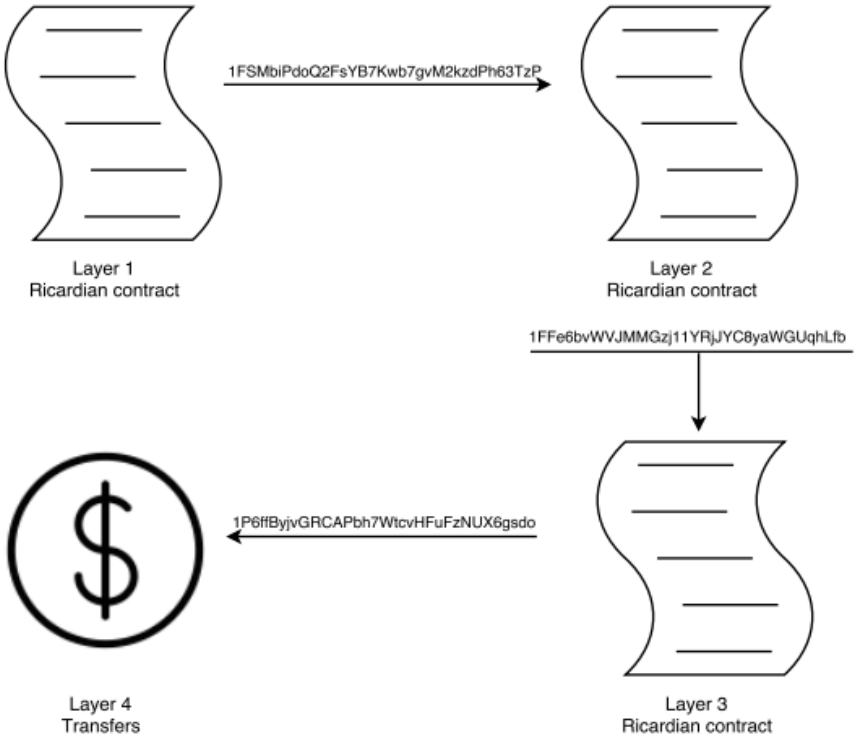
An important question arises about the discretion of the budget layer – why is it optional? It is practically impossible for a central authority to properly estimate a budget for a whole year; therefore changes in the budget are constantly made. If the system is completely locked by an upper layer, it can suffer from systematic malfunction. For example, if an agency needs to purchase an item not previously fixed in the budget, a change is required in the Ricardian contract recorded in layer 1. However, all the transactions made in layer 2, 3 and 4 prior to this change were recorded with a link to the first budget Ricardian contract, and this link cannot be changed, since immutability of records is one of the most important features of the blockchain for our transparent framework. The emergence of a solution for changing and updating the records in the blockchain can eliminate such discretion.

Some could argue that the same problem might occur in the link between layers 2 and 3, and 3 and 4. But we argue that in case the bid documents (layer 2) need to be changed,

the agency can cancel the bid and begin a new process, but it does not require to erase the Ricardian contract, since it rather remains in the blockchain, but further transactions will be recorded in the new contract that is to be made. The same apply to the relationship between layers 3 and 4.

The Ricardian contracts (layers 1, 2 and 3) are timestamped in real time by the TCU, and thus receiving a secure identifier (e.g., a message digest of a certain number of bytes, or hash) over their contract plus timestamp. Each succeeding document will include the secure identifier from its initiating document from the lower layer in order to fully record the contract's life-cycle at each stage, finally ending at and being included in the layer 4 payment transaction. Thus, the TCU, by checking a record from layer 4, can also verify where it is recorded in layers 1 (optional), 2 and 3, as shown in Figure 10.

Figure 10 Linking the documents



Some might argue that having put in place a blockchain for the benefit of all of the agencies, we should take the final step and put the payments themselves onto that blockchain. Whilst initially attractive, it presents challenges: it would represent a significant scaling up of the number of users by including private corporations, and would require a method to convert blockchain money into regular fiat currency. It would significantly complicate the project by bringing in other stakeholders and new risks. Finally, currency systems do not typically spring into life, they generally emerge from factors of demand, and the need to represent substantial fiat currency onto the blockchain would impose a supply-side cost for additional currency both from the government and from the businesses of Brazil. The ideal demand factor would be to accept the blockchain

currency for treasury remittances, but this would further increase the number of stakeholders involved. Therefore, we argue that putting layer 4 payments directly onto the chain be seen as a future, optional goal.

We argue that the working methods of the TCU have been used for years with only slight changes made each year. For example, in 2015 the TCU made changes to the system used to submit the annual activities report (Portaria TCU No. 321, 2015), but the system still works as a mere repository of files, i.e., far from the complexity and the possibilities enabled by the framework hereby presented.

In our view, by using this new framework the TCU will benefit by improving its three types of current audit work, as described in Table 3.

Table 3 Benefits enabled by the new framework

Present audit work	*Benefits of the new framework*
Annual report of accounts	TCU will be able to manage its seasonal demand, since the annual report of accounts would be replaced by real-time auditing. Auditor's work will be enhanced by the use of database queries, report automation, auto-detection of fraud characteristics and other. As previously argued, the use of Ricardian contracts allow for preventive actions instead of corrective ones.
Special audits	With the use of preventive tools, the demand for special audits should increase, so the TCU would need to relocate its resources to more *in loco* investigations. However, special audits will not only rise, but also be more effective, since the TCU will carry out preventive investigations, i.e., before the transfer of values occur.
Continuous monitoring	Ricardian contracts associated with blockchains will expand the possibilities of continuous monitoring by facilitating TCU's current work and allowing for queries and standardisation. For example, TCU can automate its work by setting alerts in the system that warn the auditors in the event of overpricing. This can take place by comparing the Ricardian contracts that contain a certain item (say, a computer) of all agencies, the system will be able to query all the contracts and find those with price well above the average.

Our proposed framework would require new software; however, the need to create, read and store Ricardian contracts and the other aspects of triple entry provides incentives for a single government-sponsored open source project to prepare the code bases. As the code bases will then be available to all agencies, and to all suppliers, the overall cost savings will be significant, and the open source project will represent a form of discipline over agencies. Also, the government could finance a single open source reference library in one language (e.g., Java), and leave it up to the market to provide other languages.

8 Conclusions and discussions

The blockchain and bitcoin provided an evolution arising from financial cryptography. For auditing purposes, the main features of it are the public ledger that allows for a more transparent framework since the records are immutable and decentralised, and the high-level cryptography itself, which guarantees that transactions are authorised by the user involved.

The blockchain timestamping functionality is an essential feature for bitcoin transactions, because it guarantees that the transaction occurred before the date and

timestamped in the block. We argue this is an important feature for our framework, since transparency demands a certain level of assurance that transactions presented to the public are fair and immutable.

In our view, the main benefits of the new framework are:

- The availability of immutable records can reduce the cost of official publications arising from public bids, auctions, contracts and other documents.
- decentralised control can boost the culture of active citizenship and transparency.
- the peer-to-peer network and timestamping provided by the national auditor can raise the risk perception of the agencies as being continuously audited, thus leading to lower levels of corruption (Berninghaus et al., 2013).
- by having all the information on a public ledger, the auditor's work would be simplified and improved through the use of database queries, and allow for comparison across the expenditures of all agencies. Also, this sort of automation can save time used in repetitive tasks and allow auditors to work in riskier areas. This has been recently examined by Lombardi et al. (2015): "automation will be used for more repetitive, transactional tasks, allowing auditors more time to apply their expert judgments to riskier, more pressing areas".
- Big data can serve as complementary evidence for auditors (Yoon et al., 2015).
- Politicians' perception of risk should increase, as "the more information the budget discloses, the less the politicians can use fiscal deficits to achieve opportunistic goals" (Benito and Bastida, 2009).
- Greater transparency can also help resource allocation efficiency. Even though Francis et al. (2009) research was applied to firms, it follows that, in the public sector, it should help prevent erroneous behaviour and also compel public officials to disclose information that we would not even keep if not required by law.
- Auditors can monitor and check the accounts in real time, instead of having to wait for the annual submission of reports, leading to reduced seasonality and continuous control monitoring (Lombardi et al., 2014).
- Standardised information from transactions and Ricardian contracts reduce or eliminate the need for auditor's rework, including e.g., the need for auditors to create custom agency-specific spreadsheets to execute part of their work.
- Reducing costs of transactions which are very high in public biddings, as shown by Silveira and Ducati (2014), by analysing data from a Brazilian government-controlled company.
- For querying purposes, the costs of permissioned blockchains are distributed, e.g., incurred by the agent interested in the data, whereas a centralised database would incur costs to the entities in charge of the data (higher costs).

Again, it is not our purpose to describe the technical requirements for the implementation of our framework. Currently, there are many startups working with diverse applications with different types of blockchains, and the presented framework is within the capabilities evidenced by startups we have seen so far. However, our blockchain proposal

differs from the bitcoin traditional blockchain. For example, the Proof of Work consensus algorithm from bitcoin is not a requirement, because we propose a permissioned blockchain, in which all of the nodes of the network are known (not anonymous), and consensus can be provided cheaply by a quorum of TCU-controlled nodes; hence our framework should consume much less energy than bitcoin. Also, for similar reasons, the limits of 1 MB per block and ten minutes block time imposed by bitcoin would be inapplicable, and our transactions should therefore be a lot faster.

The most important features of blockchain for our framework are the decentralised public ledger that allows for shared viewing of key records; the strong cryptography that ensures the documents are signed by authorities; and the timestamping that ensures transactions and documents occurred before a certain date and time. Together, these create a long-lasting, immutable and transparent record of activity by agencies, leading to more efficacious and cheaper audit.

The opportunities for further studies include the analysis of technical implementation of overlaying blockchains and the use of such tools for other purposes, such as: internal control of public and private organisations, combining matching game theory techniques for fraud prevention and detection, the use of the timestamping feature for government authorities to serve as real-time public notaries, internal payments among agencies, and eventually the participation of the public in the blockchain. Also, policymakers should consider the political challenge in enhancing transparency (Perreaud, 2015). Fung (2015) argues that political leaders who have the resources and authority to change the status quo fail to do so due to the lack of motivation. Finally, it is important to allow the participation of civil societies on the demand side, since they will be responsible for creating the demand for this e-government service (Richards, 2012).

References

Benedict, M. (2015) 'Argentine small businesses turning to bitcoin', *Financial Times*, 19 July, p.4, Academic OneFile Web [online] https://www.ft.com/content/b2a8cca4-2c11-11e5-8613-e7aedbb7bdb7 (accessed 13 January 2017).

Benito, B. and Bastida, F. (2009) 'Budget transparency, fiscal performance, and political turnout: an international approach', *Public Administration Review*, Vol. 69, No. 3, pp.403–417.

Berninghaus, S.K., Haller, S., Krüger, T., Neumann, T., Schosser, S. and Vogt, B. (2013) 'Risk attitude, beliefs, and information in a corruption game – an experimental analysis', *Journal of Economic Psychology*, Vol. 34, pp.46–60 [online] http://www.sciencedirect.com/science/journal/01674870/40.

Boyle, T. (1997) *Shared Transaction Ledger* [online] ledgerism.net/STR.htm (accessed 7 May 2016).

Brazilian Fiscal Responsibility Law (2000) *Lei Complementar No. 101*, Brasília, Brazil.

Brazilian Transparency Law (2011) *Lei Federal No. 12.527*, Brasília, Brazil.

Bryson, J.M., Quick, K.S., Slotterback, C.S. and Crosby, B.C. (2013) 'Designing public participation processes', *Public Administration Review*, Vol. 73, No. 1, pp.23–34.

Câmara dos Deputados (2013) *Custo da Corrupção no Brasilchega a R$ 85 bilhõesporano*, 18 de junho de [online] http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-permanentes/credn/noticias/custo-da-corrupcao-no-brasil-chega-a-r-85-bilhoes-por-ano (accessed 23 December 2015).

CPI (2014) *Corruption Perceptions Index* [online] http://www.transparency.org/cpi2014 (accessed 5 May 2016).

Decisão Normativa No. 140 (2014) Tribunal de Contas da União.

Decision No. 90 (2014) Tribunal de Contas da União.

Francis, J.R., Huang, S., Khurana, I.K. and Pereira, R. (2009) 'Does corporate transparency contribute to efficient resource allocation?', *Journal of Accounting Research*, Vol. 47, No. 4, pp.943–989, Blackwell Publishing Inc.

Fung, A. (2015) 'Putting the public back into governance: the challenges of citizen participation and its future', *Public Administration Review*, Vol. 75, No. 4, pp.513–522.

Grigg, I. (2004) 'The Ricardian contract', Presented at *Proceedings of IEEE Workshop on Electronic Contracting* IEEE Computer Society Press, Los Alamitos, 6 July, pp.25–31.

Grigg, I. (2005) *Triple Entry Accounting* [online] http://iang.org/papers/triple_entry.html (accessed 18 December 2015).

Howland, G. (1996) *The Development of an Open and Flexible Payment System*, Systemics Inc. [online] http://www.systemics.com/docs/sox/overview.html (accessed 5 January 2016).

Kim, S. and Lee, J. (2012) 'E-participation, transparency, and trust in local government', *Public Administration Review*, Vol. 72, No. 6, pp.819–828, Wiley Subscription Services, Inc.

Lombardi, D.R., Bloch, R. and Vasarhelyi, M.A. (2015) 'The current state and future of the audit profession', *Current Issues in Auditing*, Vol. 9, No. 1, pp.10–16.

Lombardi, D.R., Vasarhelyi, M.A. and Verver, J. (2014) 'Continuous controls monitoring: a case study', *Journal of Emerging Technologies in Accounting*, Vol. 11, No. 1, pp.83–98.

Luther, W.J. (2016) 'Cryptocurrencies, network effects, and switching costs', *Contemporary Economic Policy*, Vol. 34, No. 3, pp.553–557.

Nakamoto, S. (2008) *Bitcoin: A Peer-To-Peer Electronic Cash System* [online] http://www.bitcoin.org (accessed 6 January 2016).

New Accounting Standards Applied to the Public Sector (2012) *Normasbrasileiras de contabilidade: contabilidadeaplicadaaosetorpúblico: NBCs T 16.1 a 16.11*, Conselho Federal de Contabilidade [online] http://portalcfc.org.br/ (accessed 8 April 2016).

Odom, C. (2015) *Open-Transactions: Secure Contracts between Untrusted Parties* [online] http://www.opentransactions.org/open-transactions.pdf (accessed 23 January 2016).

Penteado, C. (2007) 'Global highlight: Brazil's Ethos Institute's 'Corruption Inc.', *Advertising Age*, Vol. 6 [online] http://adage.com/article/print-edition/global-highlight-brazil-s-ethos-institute-s-corruption/114731/ (accessed 7 May 2016).

Perreaud, C.G. (2015) 'Widening the lens to assess citizen participation', *Public Administration Review*, Vol. 75, No. 6, pp.889–890, Wiley Subscription Services, Inc.

Portaria TCU No. 321 (2015) Tribunal de Contas da União.

PR Newswire (2015) *Coinstructors Proposes Disruptive 'Blockchain Solution for Greece' Amid Eurozone Crisis is Bitcoin 2.0 The Answer* [online] http://www.prnewswire.com/ (accessed 23 February 2015).

Queiroz, J. (2004) *Auditorship of Frauds: Detention and Verification of Frauds in the Federal Accords. f 145. Work of Course Conclusion, Specialization, External Control*, Institute Serzedello Corrêa, Brasilia.

Resolution No. 155 (2002) Tribunal de Contas da União.

Richards, R.C. (2012) 'Complementarity, integration, and responsiveness: making e-government work in developing nations', *Public Administration Review*, Vol. 72, No. 1, pp.160–162, Blackwell Publishing Ltd.

Romero, S. (2012) 'Brazil faces a new corruption scandal', *New York Times*, 30 November, NA(L), Academic OneFile [online] http://www.nytimes.com/2012/11/30/world/americas/brazil-faces-a-new-corruption-scandal.html?_r=0 (accessed 23 January 2016).

Silveira, N.G. and Ducati, E. (2014) 'O Custo do PregãoEletrônico e a Aplicação do Princípio da Economicidade – CasoEletrosul', Presented in *5. Congresso UFSC de Controladoria e Finanças & Iniciação Científicaem Contabilidade*.

The Economist (2015a) 'Dilma's disasters; Brazil's president', *The Economist*, 5 December, Vol. 36, US, Academic OneFile [online] http://www.economist.com/news/americas/21679516-impeachment-proceedings-against-dilma-rousseff-are-bad-brazil-they-make-it-more (accessed 24 December 2015).

The Economist (2015b) The trust machine: the promise of the blockchain', *The Economist*, 31 October, Vol. 2, p.13, US, Academic OneFile [online] http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine (accessed 24 December 2015).

Tribunal de Contas da União (TCU) (2009) *Critérios Gerais de Controle Internona Administração Pública Um Estudo dos Modelos e Das Norm as disciplinadora sem diversos países*, Brasília, Brazil.

Tribunal de Contas da União (TCU) (2015) *Relatório de atividades: 2014*, Brasília, Brazil.

Villoria, M., van Ryzin, G. and Lavena, C. (2012) 'Social and political consequences of administrative corruption: a study of public perceptions in Spain', *Public Administration Review*, Vol. 73, No. 1, pp.85–94.

Walker, A.P.P. (2016) 'Self-help or public housing? Lessons from co-managed slum upgrading via participatory budget', *Habitat International*, July, Vol. 55, pp.58–66.

Willmer, R. (2000) *Rachel's Beer Vouchers*, WebFunds Contract [online] http://www.webfunds.org/ricardo/contracts/webfunds/BeerVouchers.html (accessed 22 February 2016).

Yoon, K., Hoogduin, L. and Zhang, L. (2015) 'Big data as complementary audit evidence', *Accounting Horizons*, Vol. 29, No. 2, pp.431–438.