Prototyping a Smart Contract Based Public Procurement to Fight Corruption

Tim Weingärtner 1, Danielle Batista 2,* Sandro Köchli 1 and Gilles Voutat 1

1 School of Computer Science and Information Technology, Lucerne University of Applied Sciences and Arts, CH-6343 Rotkreuz, Switzerland; tim.weingartner@hslu.ch (T.W.); sandro.koehli.01@stud.hslu.ch (S.K.); gilles.voutat@stud.hslu.ch (G.V.)
2 Faculty of Arts, School of Information, University of British Columbia, Vancouver, BC V6T 1Z1, Canada

* Correspondence: danilusasm@gmail.com

Abstract: Corruption in public procurement is a worldwide appearance that causes immense financial and reputational damages. Especially in developing countries, corruption is a widespread issue due to secrecy and lack of transparency. An important instrument for transparency and accountability assurance is the record which is managed and controlled by recordkeeping systems. Blockchain technology and more precisely blockchain-based smart contracts are emerging technological tools that can be used as recordkeeping systems and a tool to mitigate some of the fraud involving public procurement records. Immutability, transparency, distribution and automation are some of the features of smart contracts already implemented in several applications to avoid malicious human interference. In this paper, we discuss some of the frauds in public procurement, and we propose smart contracts to automatize different stages of the public procurement procedure attempting to fix their biggest current weaknesses. The processes we have focused on include the bidding process, supplier habilitation and delivery verification. In the three subprocesses, common irregularities include human fallibility, improper information disclosure and hidden agreements which concern not only governments but also civil society. To show the feasibility and usability of our proposal, we have implemented a prototype that demonstrates the process using sample data.

Keywords: blockchain; smart contracts; public procurement; records; recordkeeping

1. Introduction

The World Economic Forum recognizes that “public-sector corruption is the single-largest challenge, stifling social, economic and environmental development. Often, corruption centers around a lack of transparency, inadequate record-keeping and low public accountability” [1]. Frauds in public procurements have been an issue for all countries but the social impacts are more visible in the Global South. According to [2], in developing countries “the impacts of corruption severely and disproportionately affect the poorest and most vulnerable in any society, and when it is widespread, corruption deters investment, weakens economic growth and undermines the basis for law and order” (p. 3). Public money diversion through public procurements is a common practice in developing countries and the numbers show that this practice implies the majority of public money diversion in the world [3].

Distributed Ledger Technology (DLT), the more general term for Blockchain, has been showing potential to mitigate some fraudulent practices, especially those involving the recording of financial flows. The features of DLT such as decentralization, distribution, immutability and transparency are mechanisms to mitigate some of the common fraudulent practices involving public procurements and to promote greater transparency and accountability. Several initiatives have been implemented in different countries using DLT and blockchain-based smart contracts to mitigate some of the frauds involving public procurement.
procurement however no one of those initiatives focused on the recordkeeping features of the technology. In this work, we propose a prototype to automatize the recording of some transactions using smart contracts to cover parts of the public procurement procedure aiming to reduce the fraud opportunity. The selection of specific stages was necessary given the complexity of the entire public procurement and the particularities of the different procedures over the world. The three stages covered by our prototype were based on records forgery and undue information disclosure.

2. Public Procurement Process and Current Issues

According to the Organization for Economic Co-Operation and Development (OECD), public procurement “refers to the process of identifying what is needed; determining who the best person or organization is to supply this need; and ensuring what is needed is delivered to the right place, at the right time, for the best price and that all this is done in a fair and open manner” [4] (p. 6). The public procurement procedure varies from country to country, but there are international standards and guidelines to guarantee a fair and transparent process in different jurisdictions such as the OECD Recommendations on Public Procurement and the World Bank procurement Framework. Even though the different jurisdictions and different procedures, there are commonalities among the public procurement practices as the application of basic principles such as transparency, overriding public interest and competitiveness. The basic procedure for public procurements should present, according to the OECD, transparency, integrity, access, balance, participation, efficiency, e-procurement, capacity, evaluation, risk management, accountability and integration.

The public procurement procedure is usually divided into three basic stages, the internal phase, the external phase and the contract management. The internal phase involves the creation of records for the planning of the acquisition of goods and services. Common records produced under this stage are the requests for bids and the terms of reference involving the participation of the public agents in their creation. In this stage, the most important records created present all the terms and conditions for the acquisitions of services and goods and the rules for the bidders to participate in that process.

The external phase implies the publication of the records in order to promote fair competition. Usually, a request for bids is published containing the terms of reference and a draft of the contract for participants to check their admissibility in the process and the terms of the agreement they might become involved with. During the external phase, there is also the judging process to select the bidder presenting the most advantageous proposal. After those two phases, the third stage occurs in which the contract is awarded and managed until its conclusion.

According to the WEF, one of the reasons for high rates of corruption in public procurements is the lack of transparency regarding the internal phase. Records such as the needs assessment and the contract specification are created in ways to benefit specific bidders, a common practice involving vendors and public agents’ informal illegal agreements. It is not just the lack of transparency that can lead to frauds in the public procurement procedure. The undue disclosure of information during confidential stages such as the proposal selection process has the potential to harm the procedure and its competitiveness. Centralization of decision power on the hands of few public agents is also pinned as an opportunity to commit fraud “which leaves the distribution of large sums of money at the discretion of procurement official” [1] (p. 8).

Blockchain has the potential to solve the lack of transparency problem because its “[s]hared storage allows many people to share that security, which means that shared information is kept transparent. Improved transparency can prevent public information disclosure, the intervention of a third party and information monopoly, and it is considered a key factor in the security advantages of blockchain, such as the prevention of hacking” [5] (p. 6). The distributed character of blockchain technology and blockchain-based
smart contracts are also features that diminish the concentration of decision power from the hands of few public officials.

Frauds in public procurement are usually related to the distortion of the necessary competition character of the process, the violation of other principles, such as the overriding public interest and the intention to divert public money [6]. Mondo highlights that to identify frauds in the public procurement procedure “there must be elements indicating the presence of deliberate acts to distort or frustrate the competitive character of the procurement with the goal to obtain undue advantages” [6] (p. 6). As mentioned previously, common frauds regarding public procurement and its records might occur in all three main phases of the procedure. Some of the examples presented on Mondo’s Fraud Framework [6] are aligned with those proposed by the WEF report [1] such as frauds occurring during the formalization of the demand, during the contract planning and the selection of suppliers. There are also common frauds during contract management such as the acceptance of forged or damaged goods as if they were legitimate or perfect, or the approval of the delivery of products different from those specified in the contract.

Our prototype was inspired by the Brazilian Procurement System [7] and based on a general procurement procedure as shown in Figure 1. The prototype focused on three different stages of the procurement process highlighted in Figure 1 such as the bidding process, suppliers’ verification and delivery verification. The decisions on which stages to automate using smart contracts were made considering those stages involving records tampered with or undue information disclosure during the presentation of the proposals. The first two smart contracts imply the external phase and the third one implies the contract management phase.

Figure 1. General Public Procurement procedure (authors’ own).

Other common frauds related to records that might occur during the bidding process are the disclosure of proposal values to specific bidders with the intent to harm the competitiveness of the tender and the forgery, by a public agent, of proposals after their presentation. Both types of fraud benefit a specific supplier and the public agent involved in the proposal judgement stage. The common fraud involving supplier verification, also called habilitation, regards the presentation of forged compliance records such as the taxes regularity certificate and the certificates related to personnel rights compliance. The delivery verification process is commonly affected when a public agent issues an unreliable record certifying that the delivery of goods or services happened when it did not. Another type of fraud involving the delivery check regards the public agent attestation of a
the use of fair, transparent and independently verifiable government tendering scheme without unnecessary hassle” (p. 1). The goal is to provide accountability and allowing citizens to track the activities of their government, openness and accountability. Thus, enabling an independent and automatic auditing process to provide accountability and allowing citizens to track the activities of their government without unnecessary hassle” (p. 1). The goal of the framework is to reach a state of fair, transparent and independently verifiable government tendering scheme through the use of smart contracts. The framework enables an open governance framework.

3. Literature and Related Work

There are several research studies regarding the use of distributed ledger technology, specifically blockchain and blockchain-based smart contracts, as a potential technology to mitigate frauds in public procurement. DLT has a great potential to support public sector activities because of its features such as security, transparency and collaboration [8]. A study regarding the adoption of blockchain technology for administrative reforms and its use by the public administration [5] presents a blockchain administration hierarchy based on an analytic hierarchy process. The findings show that the main factors considered in the use of blockchain for public administration in order of priority are security-related, economic and decentralized. According to the study, the feature of security puts blockchain in a position to improve government trust, by “greatly enhancing the credibility of the government by securing procedural legitimacy through mutually oppressive transparent disclosure of information and rational choice” (p. 13).

A study about the implementation of blockchain-based smart contracts for municipal government processes [9] presented a blockchain-based smart contract prototype for a specific social benefit process from the Syddjurs Municipality government in Denmark. The authors’ findings showed that there are some benefits to adopting that technology for the government processes such as integrity guarantees, verifiability, direct collaboration and payment between the parties. There were also some problems detected such as “the cost of latency, pr. transactions charges, the immutability of errors and a very concerning single point of failure the municipal government: losing blockchain private keys means losing control over municipal government casework, with no recourse” (p. 676).

In South Africa, [10] presents an analysis of blockchain-based platforms as viable solutions to the issue of corruption in public procurement through a high-level overview of legal and practical problems that could impact the adoption of such platforms. The paper highlights the decentralized nature of blockchain-based smart contracts as a potential feature to mitigate fraud and corruption involving government contracts. Nonetheless, the author also emphasizes the legal issues of adopting smart contracts as real contracts, given the lack of remedies such as the possibility of cancelling tender procedures or contracts.

A framework employing the concept of smart contracts to the public procurement process is proposed by [11]. The authors focused specifically on the tender process aiming to consolidate open governance and e-government with the support of blockchain. The authors believe that technologies such as blockchain “have the potential to introduce fairness, openness and accountability. Thus, enabling an independent and automatic auditing process to provide accountability and allowing citizens to track the activities of their government without unnecessary hassle” (p. 1). The goal of the framework is to reach a state of fair, transparent and independently verifiable government tendering scheme through the use of smart contracts. The framework enables an open governance framework.
avoiding citizens’ omission on government transactions and increasing the civil society participation in monitoring those transactions. They used the Ethereum platform to evaluate the performance and financial cost implications and to analyze the security and auditability features.

There are many ongoing projects regarding the use of DLT and public procurements. The World Economic Forum published a report in 2020 about the development of a blockchain-based solution for the public procurement procedure in Colombia, the Transparency Project. According to the aforementioned report “the system was designed for the procurement of the Programa de Alimentación Escolar (PAE), or public-school meal program, a high-priority public program providing meals to the country’s most vulnerable children” [1] (p. 4). Aligned with our idea of using blockchain-based smart contracts on some of the stages of the public procurement procedure, the WEF considered the use of DLT because “[u]sing cryptography and distributed consensus mechanisms, blockchain provides the unique combination of permanent and tamper-evident record-keeping, transaction transparency and auditability, automated functions with “smart contracts” and the reduction of centralized authority and information ownership within processes” (p. 4). The project focused on the vendor bidding and bidding evaluation stages using Ethereum with the goal to evaluate the benefits of using a permissionless blockchain platform for a public procurement use case and to test the fraud reduction in that specific case.

In Mexico, the government promoted the first public procurement using blockchain platforms in 2018 [12]. The Mexican solution adopted a blockchain governance model with the public institutions, universities and civil society organizations as the stakeholders. Using Ethereum, the Mexican Government developed five smart contracts to cover the following phases: public bodies tendering registries, bidder’s registry, bidder’s pre-qualification process, the bidding process and proposal evaluation and selection. In the Seoul district, South Korea, the government developed a smart contract for the proposal evaluation stage to enhance transparency and fairness in the judgement process [13].

4. Research Design

The present work is based on the design science paradigm according to Hevner et al. [14]. The goal of design science is to construct and evaluate artifacts to solve problems. The “design cycle” represents the essence of any design science research project, in which the artifacts are iteratively developed and validated. The environment consisting of people, organizations and technology defines the problem space and provides requirements and business needs. At the same time, a knowledge base adds applicable knowledge during each iteration. In our case, we obtained the requirements from experts in the field of public procurement and our process analysis. We added knowledge on blockchain technology and smart contracts and came up with our concept of a solution to the described problems.

First iterations have been validated against artificial cases and with subject matter experts. In the following stage, we are working towards an applied science research project including government agencies and IT enterprises to validate our concept in a real case environment.

5. Advantages of Blockchain and Smart Contracts

Blockchain developed into a technology broadly applied to several sectors. With the original whitepaper from Satoshi Nakamoto [15] blockchain first became famous for applications in cryptocurrencies. After the creation of Ethereum [16] and its ability to store and execute smart contracts in a virtual machine new areas of application emerged. Yet smart contracts were not new. The concept was primarily proposed by Nick Szabo in 1997 when he explained their use [17]. At that time, a secure technology for a tamper-proof execution was still missing. Today, smart contracts find application in the management of supply chains, securing energy transmission, transferring health records or allowing self-
sovereign identities this being not an exhaustive list. The main advantages of using blockchain-based smart contracts are their immutability, decentralization, transparency, representation of agreements, self-execution and verifiability. We define a smart contract as a pre-written, tamper-proof and unalterable computer program representing an agreement between two or more parties. A Smart Contract is stored, replicated and self-executed on a blockchain or distributed ledger, triggered by digitally verifiable events or conditions and can take custody over and instruct transfer of blockchain-titled assets.

Regarding the decentralization of information, blockchain technology store and manage all information in a decentralized manner resulting in a distribution of information among all users of the network diminishing the power that corporations and the government exercise over information access [5]. The potential of the technology to transform government regimes and their performance is related to the possibility of increasing participation in the decision-making process “as decision making based on blockchain increases and the minority of existing one decision making is converted to a form in which the majority participates, power becomes dispersed, democracy is transformed and direct democracy is more likely to be realized” [5] (p. 7). Nevertheless, the used consensus algorithm and blockchain architecture as well as accessibility plays an important role in the degree of trust placed in the system.

Permissionless, public blockchains generate a high degree of trust if decentralization is high and the participants in the consensus algorithm are independent. In those systems, data privacy is usually a hurdle. To solve this difficulty, confidential data is stored off-chain and referenced by the hash of these data. This makes it impossible to recover the data only from the stored hash. The used consensus algorithm must ensure that the incentive for validating the truth is higher than for cheating. It also requires that the validating party has all information to verify the truth of the information written or at least can verify them in a mathematical way (e.g., zero-knowledge proof). Permissioned (access restricted) blockchains which are sometimes completely private must ensure independence in the way the governance is defined. In addition, the consensus algorithm must ensure neutrality. Since those blockchains often use energy-efficient and faster but less secure consensus algorithm confidence-building is an important aspect. Depending on the structure of the involved parties, the confidentiality of data is also an important aspect that must be considered.

Regarding the procurement process, smart contracts remove the power of single persons during the whole process. During the bidding phase, the hidden entry of a bid is enabled avoiding privileged access to information or its undue disclosure. Concepts for this were derived from blind auctions. This makes it impossible for persons involved to disclose bids to competitors. At the same time, it is guaranteed that bids cannot be changed after submission. Since a smart contract has no vested interests and the code is publicly viewable trust in the process is built. In the phase of supplier verification regulatory requirements such as tax regularity or working conditions compliance must be met. In this sub-process, blockchain-based identities and certificates guarantee the authenticity of the information. If certificates are issued incorrectly, this can be proven afterwards, and an audit trail is always accessible. In addition, process efficiency is increased since no paper certificates must be used and certified by a public officer. Finally, after delivery when the provided goods or services have been verified, documentation on a blockchain guarantees transparency and accountability. Furthermore, the double-check principle for appropriate quality control and approval process can be supported and recorded. In general, it can be stated that transparency, immutability and traceability prevent all major opportunities for fraud.

6. Design of Selected Aspects: Bidding, Supplier Habilitation and Delivery Verification

As described in Sections 3 and 5 we propose the application of blockchain-based smart contracts for three sub-processes: Bidding, supplier habilitation and delivery
verification. In this section, we describe those sub-processes in an in-depth way including implementation aspects.

6.1. Bidding Process

During the bidding process, participating companies submit their offer. For simplicity reasons, we assume that the cheapest offer wins the bidding, and this company is chosen as the preferred supplier. As mentioned above, to avoid disclosure of competing offers the bidding must be conducted with confidentiality. Algorithm 1 shows the pseudo-code of this process. Since we assume the use of a public blockchain, no price information should be transmitted or stored in a smart contract. On the other side, it must be ensured that a company cannot change the price after the offer has been submitted.

To meet both competing requirements we generate a hash (biddingHash) from the price including a nonce or salt value. A so-called salted hash is commonly used in cryptography to prevent the back-calculation of a hash using a brute force or password table approach [18]. Since the price information most commonly is a number in the range of 0.01 to 100,000,000.00 a brute force attempt would be likely successful. Adding a large random alphanumeric value makes this approach impossible. Additionally, a hash of the offer record can be included in the bid to provide further proof (offerHash). Both values, the price and nonce and the electronic version of the document used to calculate the record’s hash (offerHash) must be stored on the side of the vendor. Since we assume a permissionless system, which can be used without access restrictions, a deposit has to be paid to prevent spam offers. This deposit is reimbursed after the final supplier has been determined.

Algorithm 1: Smart Contract Place Bid — places bid and stores the hashes of the bid and offer document in the smart contract

1. **input**: bidding hash, offer hash, tender, sender
2. if status of tender is propose (tender) AND not duplicate bid (sender)
3. store (bidding hash)
4. store (offer hash)
5. lock deposit (sender)
6. register bid (sender)
7. end if

After an offering period of, let us say, 14 days an administrator or the smart contract itself changes the stage of the process in the revealing phase (see Figure 2). If the smart contract should do this independently an external service has to be used to provide the needed event. This service is called an oracle [19] and provides a blockchain-based smart contract with information from outside the blockchain. Due to security and manipulation reasons, this service must be designed and implemented carefully. To keep the decentralized nature of a blockchain and not to introduce a weak point into the process it is advised to use multiple, independent oracle services providing the same information. This allows a majority decision in case of contradictory information.

During the revealing phase, no further bids can be submitted at this stage and all vendors can now reveal their bids (see Algorithm 2). This revealing process is achieved by submitting the values of the price and nonce. The smart contract calculates and verifies the resulting hash with the stored value from the proposal phase (biddingHash). The verification of the offer document must be accomplished by an independent external service (oracle) since this would exceed the calculation power of a smart contract. By knowing the price of all vendors, the smart contract can decide the preliminary winner of the tender. Preliminary since the final supplier can only be determined if the verification of the legal requirements has been accomplished which is explained in the next subsection. In our
prototype, we implemented the selection of the lowest price. Further research will focus on implementing more complex rules.

**Algorithm 2: Smart Contract Reveal Bid**—reveals the bid after the offering period

```plaintext
input: price, nonce, tender, sender

if status of tender is reveal (tender)
    if bidding hash = hash (price, nonce)
        add price (price, sender)
        if all vendors revealed OR revealing period exceeded
            verify and mark preliminary winner
        end if
    else error: price or/and nonce are incorrect
end if
```

![Figure 2. Stages of a tendering process (authors’ own).](image)

6.2. **Supplier Habilitation**

Government must assure that suppliers participating in public procurement are compliant with several legal prerequisites. These can be general aspects, such as the correct payment of taxes or compliance with working conditions. However, these prerequisites can also be tender-specific, such as quality seals or permission to manufacture medical devices. Most of those requirements are not bound to one specific tender but can be reused for multiple calls. We use the concept of self-sovereign identity to solve this aspect [20]. Each vendor can create its own identity. This identity is certified by an official body with proof that is stored on the blockchain. Additional certifications can be bound to this identity by authorized issuers. All certifications are stored on the blockchain. During the verification phase of the procurement, the required certifications are checked without the involvement of the individual issuers. Certifications can have an expiration date or can be revoked. Even the connection to identities on other blockchain systems can be applied.

For the procurement and bidding process, this means that only vendors who can prove all required claims are considered as winning providers (see Algorithm 3). The smart contract can perform this verification without any manual interference and therefore prevent manipulation. The placement of the order can be automated by another smart contract which also holds the agreed payment to ensure the processing of payments after the correct delivery.
Algorithm 3: Smart Contract Supplier Habilitation of the Winner—verifies that the winner of the bidding meets all requirements and places the order

```
input: winner, tender

if status of tender is reveal (tender)
  if all requirements met (winner)
    winner approved (winner)
    place order (winner)
    lock payment (getPrice (winner))
  else
    mark next winner (tender)
    call supplier habilitation of the winner
  end if
end if
```

6.3. Delivery Verification

After the cheapest bid has been selected and the order has been placed the next crucial part is the verification process of the delivered goods or services. Even if the tender process has been fair and accurate the receipt of the delivery contains many possibilities for manipulation. This ranges from the absence of individual goods to non-compliance with quality requirements to the complete lack of delivery. Since a smart contract will never be able to verify the diversity of possible features of physical goods, again an oracle service comes to the application. This time a “human oracle” is used. This means that persons must verify and evaluate the delivered goods or services. To reduce the possibility of corruption the double-check principle is applied. The smart contract chooses randomly two or more auditors from a set of predefined persons. Due to the random selection and the transparent and immutable documentation of these auditors, the chance of intentional misstatements is reduced to a minimum. Only when both auditors have positively assessed the delivery, the payment of the goods is triggered. In the event of a complaint, an external arbitration process is triggered (see Algorithm 4).

The payment is processed by the above-described smart contract that locked the payment at the time of the order. This reduces a further possibility of fraud: the suspension or prevention of payment. Since the buying party must deposit the agreed amount in the smart contract after delivery verification is successful and signed the payment is automatically processed and no interference or delay is possible.
Algorithm 4: Smart Contract Order Verification—verifies the order and releases payment

1. **input**: tender
2. **prerequisite**: only buying party can execute
3. **if** status of tender is evaluate (tender)
4. **repeat**
5.   **select auditor randomly**
6.   **wait for validation of auditor**
7. **until** number of validations reached
8. **if** all validations correct
9.   **release payment**
10. **else**
11.   **start arbitration process**
12. **end if**
13. **end if**

7. Proposed Process and Recordkeeping

Recordkeeping was a term revisited in the 1990s because of the emergence of electronic records. According to [21] "electronic recordkeeping became a widespread term, used to mean the application of recordkeeping strategies to digital records and systems" (p. 321). According to the International Council on Archives (ICA), a record is a document “created, received and maintained as evidence and information by an organization or person, in pursuance of legal obligations or the transaction of business” and a recordkeeping system is defined as “a framework to capture, maintain and provide access to evidence of transactions over time, as required by the jurisdiction in which it is implemented and in accordance with common business practices” [22]. The definition proposed by the ICA is beyond the concept of software or an application and involves the policies and procedures established for records management.

There are some standard principles for recordkeeping practices such as the ISO 15498 [23] and the ARMA Generally Accepted Recordkeeping Principles [24]. The ARMA Principles which are accountability, transparency, integrity, protection, compliance, availability, retention and disposition, must be present on an information governance program. In this paper, we have adapted the principles to analyze blockchain and smart contracts as tools to support adequate records management practices. As shown in Table 1, some of those principles are reinforced by blockchains and blockchain-based smart contracts, such as accountability and transparency but two of them, such as retention and disposition, are not presented in a regular blockchain environment.

Table 1. ARMA Generally Accepted Recordkeeping Principles and Blockchain systems.

| Principle   | Description                                                                 | Blockchain Feature |
|-------------|-----------------------------------------------------------------------------|--------------------|
| Accountability | The attribution of responsibility in a transparent manner.                  | Blockchain systems allow parties to keep track of transactions and transparently audit them among the network participants. |
| Transparency | The business processes and activities shall be documented in an open and verifiable manner, and that documentation shall be available to all personnel and appropriate, interested parties. | The concept of transparency is reinforced by blockchain systems, especially when using smart contracts since the process is automatized, immutable and recorded on the blockchain. |
Integrity
Information assets generated by or managed for the organization shall have a reasonable guarantee of authenticity and reliability. If the requirements are considered during the design phase of the information system, blockchains can support records’ integrity.

Protection
The assurance of the appropriate level of protection to information assets that are private, confidential, privileged, secret, classified, essential to business continuity or that otherwise require protection.

Compliance
Compliance with applicable laws, other binding authorities and the organization’s policies

Availability
Information assets must be kept in a manner that ensures their timely, efficient and accurate retrieval.

Retention
Information assets must be preserved for an appropriate time, considering their legal, regulatory, fiscal, operational and historical requirements.

Disposition
Execute secure and appropriate disposition for information assets no longer required to be maintained, in compliance with applicable laws and the organization’s policies.

Blockchains and smart contracts can provide security from their distributed structure. It is also possible to guarantee the secrecy of some information (e.g., the secrecy of the proposals presented in our prototype). This requires that no confidential information is stored on the blockchain.

Blockchains systems and smart contracts can be compliant if the regulations are considered during the design stage of the system or the contract.

Information can be publicly accessible on blockchain systems.

The preservation of electronic records in blockchain environments is still in its infancy.

Deletion of data on blockchains is still challenging given its immutable character. This requirement has to be considered during the design stage of the system or the contract.

According to [8], one example of the use of blockchain in the public sector is related to records since “storage of static information, i.e., record keeping is a critical action when it comes to the public sector. Timely updation of records, ensuring adequate security, managing the access to these records, immutability, transparency, secure storage and preservation of data are paramount to areas in the public sector where information has to be stored across different systems and database” (p. 52).

From an Archival Science perspective, according to [21], there are three different uses of recordkeeping systems such as a component of information governance (e.g., ARMA Generally Accepted Recordkeeping Principles), an application or software system or as a context to understand the records. In this specific paper, we focus on the first and the second aspect of recordkeeping systems. We already provided the ICA concept of a recordkeeping system as a component of information governance. According to [21] a recordkeeping system as software is defined as “business systems that manage records—that is, systems that capture, maintain and provide access to records over time” (p. 321)

We have already demonstrated in Table 1 that blockchain and smart contracts can serve as tools to support some of the recordkeeping principles in regards to information governance however we cannot consider our solution in the blockchain as an ideal recordkeeping system as software according to [21]’s concept. Our prototype produces some important records related to the public procurement procedure and there are some capture, maintenance and access features present in our solution however it is still challenging to assure the preservation of records for long periods in such novel technology.

The first smart contract in our prototype regards the bidding process, specifically the proposal selection based on the lower value proposal. The smart contract will analyze the
cheapest proposal without disclosing any information to the public agents involved in the process. The proposal selection hash will be recorded on the blockchain as an outcome of the first smart contract execution as a record of that transaction.

The second phase automatized in our project is the habilitation records check. This stage involves the verification of the business qualification records authenticity, such as tax regularity certificates. This is a required transaction to validate the selected business to sign a contract with any public body in the Brazilian context. Our prototype proposes the use of self-sovereign identity to execute the verification process which will also be recorded on the blockchain as an outcome of the second smart contract.

Finally, the third stage implies the attestation of the delivery of goods during the contract management phase of the public procurement procedure. Usually, the delivery is validated on a record containing the information that the delivery was made according to the contract requirements and following the products or services specifications. In the case of our prototype, that record is a hash recorded on the blockchain by the designated public agent certifying that the delivery was properly made. The record can be checked by every node of the network and is recorded right after the certification process.

In all the cases included in our prototype, some of the components of the record are contemplated such as part of the archival bond, the medium, the persons and the acts. We are still working on some of the features of the archival bond and the context of the record. In our current solution, we preserve the relationship between the records and the creator, i.e., the public body responsible for the bidding process and the contract management. The relationship between the records and the specific tender is also preserved by the nonce. We still need to work on the relationship between the records kept on the blockchain platform and the off-chain records, such as the records produced and kept in different information systems regarding the other phases of the procedure (e.g., requisition to procure and the survey of price). The classification scheme is still missing in our process.

Regarding the trustworthiness of the records produced and kept by our solution, we aim to guarantee their reliability in controlling the process of their creation. Using smart contracts, we aim to guarantee that the process to record parts of the procedure is achieved according to the public procurement regulations. In the first smart contract related to the best proposal selection, our prototype selects the lower value proposal and records the result of that transaction on the blockchain according to specific rules. The second smart contract checks the authenticity of the records presented by the winning bidder to execute the habilitation check transaction through an external call to a public agency database (e.g., a call to the revenue agency database to verify the authenticity of a tax regularity certificate). The process implies the verification of the identity of the records and their integrity. This checking process must be registered in the public procurement documentation, and it is not possible to award a contract between the government and the winning business without recording the checking transaction. This phase also implies the reliability of the record produced as an outcome of the habilitation records check smart contract since it follows the regulated procedure to attest to the veracity of the certificates presented by the winning bidder. Finally, the delivery verification process can assure the reliability of the outcome of the third smart contract of our prototype. The delivery is certified by a randomly designated public agent and the recording of that information is also controlled by an automatized process following the specific rules for that stage.

From a usability side, the proposed process should be as similar as possible to today’s process. In addition, the parties involved should not feel that the process is blockchain-based. Nevertheless, some sub-processes must be adapted to meet the requirements from a technological view. For the users this means that digital identities are required, some password-like entries must be made, all documents must be provided in a digital form and deadlines as well as decisions are final and cannot be changed later.
8. Prototype Implementation

To verify the concept and to receive feedback from possible users of a smart contract-based procurement process, we implemented a prototype using the Node-RED framework and the Ethereum blockchain. Node-RED (https://nodered.org/ accessed on 29 June 2021) is an Open-Source flow-based graphical development system that is ideal for prototyping processes. It is commonly used for Internet of Things (IoT) applications since it offers a huge variety of implemented nodes for transaction protocols. In addition, there exists a dashboard node-set that makes it possible to easily build a simple user interface (https://flows.nodered.org/node/node-red-dashboard accessed on 29 June 2021). Figure 3 shows a section of the Node-RED flows and Figure 4 shows the user interface to give a visual impression of how the prototype is displayed to the user. Detailed information and the source code of the prototype can be found on Github (Code of Prototype is available under https://gitlab.enterpriselab.ch/gioutat/procurement but will be moved to https://github.com/timweing after students leave university, accessed on 29 June 2021).

Ethereum (https://ethereum.org/ accessed on 29 June 2021) is a well-known blockchain platform with the feature of deploying and running smart contracts in a special virtual machine (EVM). For the prototype, we used the Ethereum test environment Ganache from the Truffle Suite (https://www.trufflesuite.com/ accessed on 29 June 2021). This is a local runtime environment simulating an Ethereum blockchain. As cryptocurrency we used Ether. The costs for deploying and running smart contracts must be paid as Gas to the miners running the Ethereum nodes. Since we used a local blockchain this was not relevant for the prototype. For productive use on the Ethereum Mainnet, these are costs that should not be underestimated. Furthermore, the application of the Proof of Work consensus algorithm raises severe concerns regarding its energy consumption. It can be considered that on the one side there are changes in the Ethereum blockchain towards a version 2.0 that hopefully will significantly reduce the costs and energy consumption using the Proof of Stake algorithm. On the other side, a productive procurement solution might run on a government-hosted permissioned blockchain that has small to no costs involved. Several architectural designs address the topic of trust in a permissioned environment as public read access, documented and comprehensible audit process, link between a permissionless and permissioned blockchain or distribution over several, independent countries. The continuing research project will address this topic in detail as it will define the requirements of a permissioned blockchain infrastructure to ensure a high level of decentralization and tamper protection. As of today, many industry-related blockchain applications are developed on top of permissioned blockchain infrastructures such as Cardossier (https://cardossier.ch/ accessed on 29 June 2021), TradeLens (https://www.tradelens.com/ accessed on 29 June 2021) or Food Trust (https://www.ibm.com/blockchain/solutions/food-trust accessed on 29 June 2021).
Figure 3. Screenshot from Node-RED Prototype [25].

Figure 4. User Interface of the delivery inspection module (author’s own).

9. Conclusions and Further Work

We presented a new, DLT and smart contract-based approach for the public procurement process. With our interdisciplinary research, we showed how smart contracts can be applied to the discipline of Archival Science and the feasibility of our approach. Using the design science research method [14] we implemented the most crucial steps of the procurement process as a prototype. With this prototype, we have shown that the public procurement process can be applied using a blockchain. Furthermore, the prototype has shown those aspects of the process, that must be improved by further research, such as the selection rules for the winning bid.

From an Archival Science perspective, we can assume blockchain systems could be compared to recordkeeping systems in the sense that they can “capture, maintain and provide access to records over time” as long as the requirements for the creation, maintenance and preservation of those records are considered from the beginning of the information system design. Some of the records’ intellectual components are present in our prototype but there is still some pending process to establish the archival bond and maintain the records’ contexts, especially regarding the link between the on-chain and the off-
chain records produced and kept in different information systems throughout the public procurement procedure. Our research must pursue the requirement for trustworthiness and long-lasting records to establish a recordkeeping system for public procurement records in blockchain environments.

The authors have applied for an interdisciplinary, transnational research grant transferring the results into a productive environment. The goal of this continuation of the research is to verify the usability of such an approach aligned with the archives and records management principles and to prove the concepts outside a laboratory environment.

**Author Contributions:** Conceptualization, T.W. and D.B.; investigation, T.W. and D.B.; methodology, T.W. and D.B.; software, T.W., S.K. and G.V.; supervision, T.W.; validation, T.W., S.K. and G.V.; writing—original draft, T.W. and D.B.; writing—review & editing, T.W. and D.B. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no external funding.

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** Code of Prototype is available under https://gitlab.enterpriselab.ch/gvoutil/procurement but will be moved to https://github.com/timweing after students leave university, accessed on 29 June 2021.

**Conflicts of Interest:** The authors declare no conflict of interest.

**References**

1. World Economic Forum. *Exploring Blockchain Technology for Government Transparency: Blockchain-Based Public Procurement to Reduce Corruption*. World Economic Forum: Geneva, Switzerland, 2020.

2. Gracar, A.; Frenzler, T. *Understanding and Preventing Corruption*; Palgrave Macmillan: London, UK, 2013; doi:10.1057/9781137335098.

3. How Corruption Weakens Democracy. Available online: https://www.transparency.org/news/feature/cpi_2018_global_analysis (accessed on 26 August 2019).

4. Council on Public Procurement. OECD Recommendation of The Council on Public Procurement. OECD, 2019. Available online: https://www.oecd.org/gov/ethics/OECD-Recommendation-on-Public-Procurement.pdf (accessed on 29 June 2021).

5. Myeong, S.; Jung, Y. Administrative Reforms in the Fourth Industrial Revolution: The Case of Blockchain Use. *Sustainability 2019*, 11, 3971.

6. Mondo, B.V. Obra Transparente—Métodos de Detecção de Fraude e Corrupção em Contratações Públicas (Transparent Construction—Public Procurement Fraud and Corruption Detection Methods). Transparência: Brasil, Switzerland. Available online: https://www.transparencia.org.br/downloads/publicacoes/Metodos%20Detec%C3%A7%C3%A3o%20de%20Fraude.pdf (accessed on 30 June 2021).

7. Brasil, Lei de Licitações e Contratos. 1993. Available online: http://www.planalto.gov.br/civil_03/leis/l8666cons.htm (accessed on 29 June 2021).

8. Pramod, D.; Zachariah, B.; Salim, T. Moving Beyond Paperwork: Blockchain in Public Sector. *Telecom Bus. Rev. 2019*, 12, 50–55.

9. Krogsboll, M.; Borre, L.H.; Slaats, T.; Debois, S. Smart Contracts for Government Processes: Case Study and Prototype Implementation. In *Financial Cryptography and Data Security*; Springer: Kota Kinabalu, Malaysia, 2020; pp. 676–684.

10. Williams-Elegebe, S. Public Procurement, Corruption and Blockchain Technology in South Africa: A Preliminary Legal Inquiry. In Regulating Public Procurement in Africa for Development in Uncertain Times. Available online: https://ssrn.com/abstract=3458877 (accessed on 29 June 2021).

11. Hardwick, F.S.; Akram, R.N.; Markantonakis, K. Fair and Transparent Blockchain based Tendering Framework—A Step Towards Open Governance. In Proceedings of the 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), New York, NY, USA, 1–3 August 2018.

12. México: Pionero en Licitar con Blockchain. Bitcoin Mexico. 2018. Available online: https://www.bitcoin.com.mx/primera-licitacion-con-blockchain-en-mexico/ (accessed on 29 June 2021).

13. Ledger Insights. Seoul District Using Blockchain for Public Procurement. Ledger Insights. 2019. Available online: https://www.ledgerinsights.com/seoul-district-using-blockchain-for-public-procurement/ (accessed on 17 April 2021).

14. Hevner, A.R.; March, S.T.; Park, J.; Ram, S. Design Science in Information Systems Research. *MIS Q.* 2004, 28, 75–105.

15. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 04 December 2017).
16. Wood, G. Ethereum: A Secure Decentralized Generalised Transaction Ledger. Yellow Pap. 2014, 151. Available online: https://gavwood.com/paper.pdf (accessed on 29 June 2021).
17. Szabo, N. Formalizing and Securing Relationships on Public Networks. First Monday 1997, 2, doi:10.5210/fm.v2i9.548.
18. Aycock, J.; deGraaf, R.; Jacobson, M. Anti-disassembly using cryptographic hash functions. J. Comput. Virol. Vol. 2006, 2, 79–85, doi:10.1007/s11416-006-0011-3.
19. Caldarelli, G. Understanding the Blockchain Oracle Problem: A Call for Action. Information 2020, 11, 509, doi:10.3390/info11110509.
20. Mühle, A.; Grüner, A.; Gayvoronskaya, T.; Meinel, C. A survey on essential components of a self-sovereign identity. Comput. Sci. Rev. 2018, 30, 80–86, doi:10.1016/j.cosrev.2018.10.002.
21. Duranti, L.; Franks, P.C. Encyclopedia of Archival Science; Rowman & Littlefield: Lanham, MD, USA, 2015.
22. International Council on Archives (ICA). Multilingual Archival Terminology. International Council on Archives. 2021. Available online: http://www.ciscra.org/mat/mat (accessed on 29 June 2021).
23. ISO 15489-1:2015—Information and documentation—Records management—Part 1: Concepts and principles; International Standards Organization: Geneva, Switzerland, 2015.
24. Generally Accepted Recordkeeping Principles. ARMA International. 2009. Available online: http://www.armavi.org/docs/garp.pdf (accessed on 29 June 2021).
25. Köchli, S.; Voutat, G. ProcurementContract—Blockchain für Staatsaufträge; Wirtschaftsprojekt an der Hochschule Luzern-Informatik: Luzern, Switzerland, 2020.