IDB

WORLD ECONOMIC FORUM

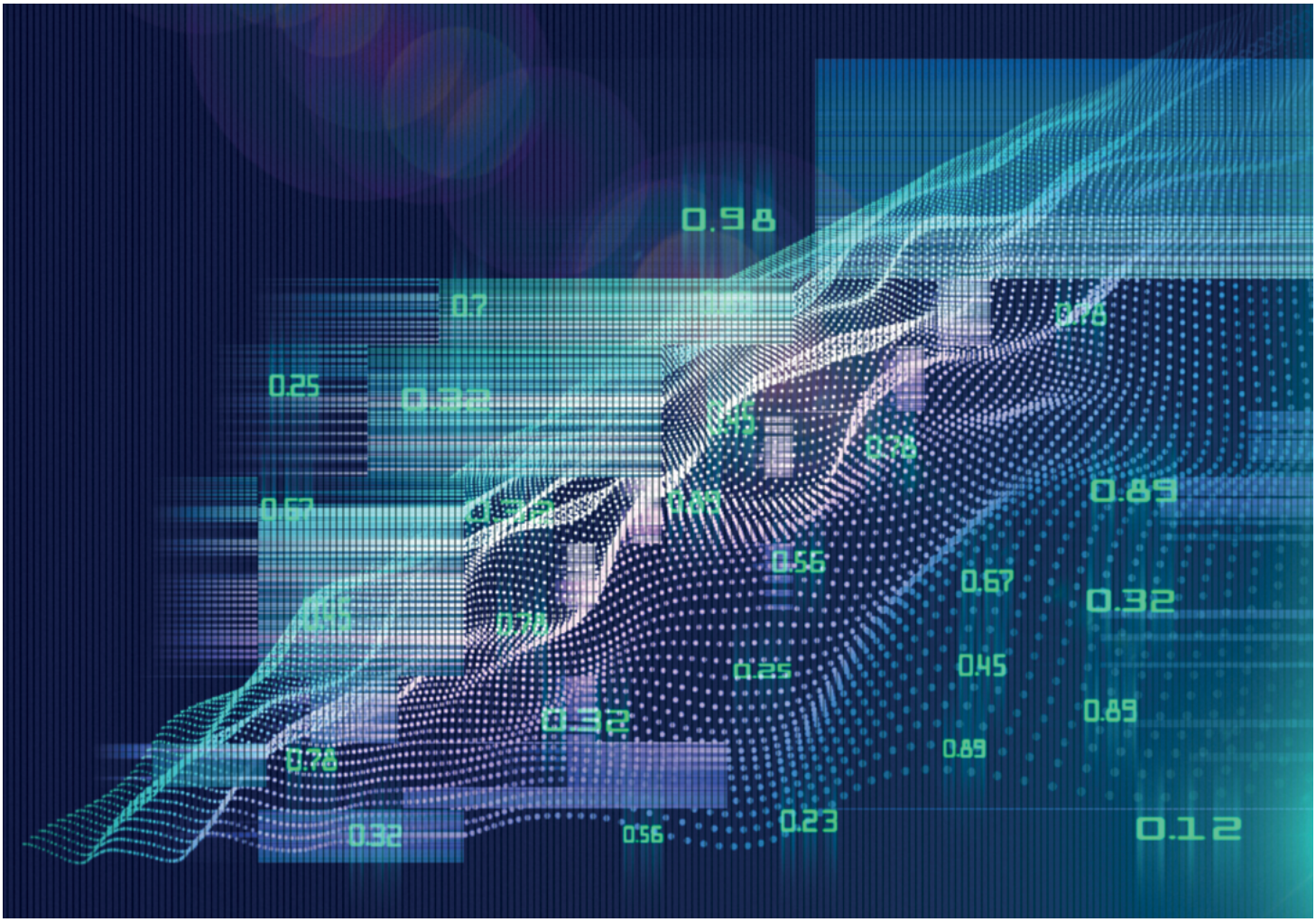
COMMITTED TO IMPROVING THE STATE OF THE WORLD

Insight Report

Exploring Blockchain Technology for Government Transparency:

Blockchain-Based Public Procurement to Reduce Corruption

June 2020



World Economic Forum
91-93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland
Tel.: +41 (0)22 869 1212
Fax: +41 (0)22 786 2744
Email: contact@weforum.org
www.weforum.org

Contents

Introduction

The costs to society of public-sector corruption and weak accountability are staggering. In many parts of the world, public-sector corruption is the single-largest challenge, stifling social, economic and environmental development. Often, corruption centres around a lack of transparency, inadequate record-keeping and low public accountability. Blockchain and distributed ledger technologies, when applied thoughtfully to certain corruption-prone government processes, can potentially increase transparency and accountability in these systems, reducing the risk or prevalence of corrupt activity.

In partnership with the Inter-American Development Bank (IDB) and the Office of the Inspector General of Colombia (*Procuraduría General de Colombia)*, the Forum has led a multistakeholder team to investigate, design and trial the use of blockchain technology for corruption-prone government processes, anchored in the use case of public procurement. The project, led by the Blockchain and Digital Currency team housed within the World Economic Forum Centre for the Fourth Industrial Revolution, is called *Unlocking Government Transparency with Blockchain Technology* (hereafter, the *Transparency Project*).

The project developed a blockchain-based software proof-of-concept (PoC) for public procurement that intends to be tested in a live procurement auction in Colombia in 2020. The system was designed for the procurement of the *Programa de Alimentación Escolar* (PAE), or public-school meal programme, a high-priority public programme providing meals to the country's most vulnerable children. This programme has been a historic site of procurement corruption in the country.[1]

Using 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. These properties make blockchain a high-potential emerging technology to address corruption. The project chose to focus on the public procurement process because it constitutes one of the largest sites of corruption globally, stands to benefit from these technology properties and plays a significant role in serving public interest.

Following the methodology of the World Economic Forum Centre for the Fourth Industrial Revolution, the *Transparency Project* draws input from a multistakeholder community of global experts. Input was gathered at dedicated workshops and meetings in Bogotá and Medellín, Colombia, at the World Economic Forum Sustainable Development Impact Summit 2019, at the Partnering Against Corruption Initiative (PACI) Biannual Community meeting, at the World Economic Forum Annual Meeting in Davos-Klosters, and at other venues.

The project is rooted in a software PoC for the fully public and "permissionless" Ethereum blockchain network in order to uncover the salient technology trade-offs and limitations with blockchain for public procurement generally and with a fully open and decentralized blockchain configuration specifically. The project further includes globally relevant and complementary policy proposals to strengthen public procurement, as well as governance guidelines for the effective deployment of a blockchain-based system. Importantly, it also discusses civic engagement strategies to strengthen system participation and success through public monitoring. Of course, technology and policy can only mitigate corruption to a limited degree; cultural and social change are required to truly address deep-rooted corruption practices. Put another way, technology cannot fully solve what is at the heart of human behaviour problems.

Collectively, the project is the first to take a multidimensional approach to blockchain experimentation for anti-corruption, considering numerous policy, governance and civic engagement elements alongside detailed technical design. This report aims to communicate project findings and contribute to the global understanding of blockchain technology for public-sector transparency and corruption reduction. Policy-makers may wish to study its findings to inform their understanding of blockchain technology's potential to improve transparency and accountability in their own systems. The report can also serve as a case study highlighting the trade-offs, limitations and policy considerations related to public-sector blockchain technology development.

Executive summary

Summary of findings

The project takes a three-pronged approach to blockchain experimentation in the anti-corruption context, focusing specifically on public procurement. It includes: 1) a software proof-of-concept (PoC); 2) the enumeration of complementary policy proposals to strengthen procurement integrity; and 3) a civic engagement strategy focused on encouraging and empowering citizen monitors to flag risky behaviour in the system. This report aims to communicate the findings of this novel and multifaceted project with the goal of identifying the value of blockchain technology for public procurement and laying the foundation for similar experimentation, innovation and adoption worldwide.

The project is anchored in a software PoC to uncover, using a bottom-up approach, key capabilities and limitations associated with blockchain for public procurement, as well as critical related policy considerations. The PoC is focused on the vendor bidding and bid evaluation phases of procurement. It is designed for a public, permissionless blockchain network (Ethereum) in order to also study the benefits of a permissionless blockchain for public procurement and anti-corruption use cases. Permissionless blockchains maximize decentralization and provide unparalleled security with respect to data permanence and process integrity – qualities that are particularly beneficial in the anti-corruption context.

The project's findings reveal multiple challenges and unanticipated vulnerabilities with fully permissionless blockchain networks, despite their benefits. The most notable challenges relate to scalability and vendor anonymity (or more generally, privacy). However, future technological developments or alternative configurations may remedy these issues.

For example, permissioned or "hybrid" blockchain networks (which employ both a permissioned and a permissionless base-layer blockchain protocol) offer a potential solution. This report presents the trade-offs of each configuration for public procurement. The results suggest that a hybrid blockchain may be most attractive, as these mixed systems strike an ideal balance, given present technological limitations, between transparency, procedural integrity, scalability and security. They also highlight the importance of tracking innovations in cryptography and protocol scalability that may be able to address present technology challenges.

Furthermore, whether permissioned or permissionless, blockchain is not a panacea. This report highlights the importance of a multifaceted approach to blockchain implementation, complemented by policy reforms that can help realize the technology's transparency- and accountability-enhancing capacities. In particular, multistakeholder and civic engagement in the development, deployment and monitoring of blockchain-based procurement systems are crucial to achieving impact. It is also important to note blockchain technology's inability to reduce corruption risk in certain human activities that can occur outside any electronic procurement (e-procurement) system,[2] most notably bribery or collusion among vendors or between vendors and tenderers.

Ultimately, blockchain technology provides several unparalleled qualities and capabilities towards combating procurement corruption. However, with today's technology challenges and limitations, the argument for implementing a blockchain-based solution is equivocal. Policy-makers should ultimately identify their priorities and requirements given their specific social, political and economic conditions and the trade-offs associated with various blockchain technologies.

Report structure

The report begins with a discussion of the prevalence and diverse harms of public-procurement corruption globally and in Colombia specifically. It also maps the vulnerabilities within vendor bidding and bid evaluation that help facilitate the high incidence of corruption worldwide. It then describes the *Transparency Project* and its scope, highlighting blockchain technology's hypothesized contributions.

Next, the report includes a technical summary of a blockchain-based e-procurement system that served as the model for the PoC. It then provides a downloadable model Request for Proposal (RFP), including sample functional specifications, which institutions can reference if they choose to develop blockchain-based systems of their own. Further, the report enumerates complementary policies for strengthening procurement integrity, as well as guidelines for deployment and successful civic engagement. It also describes roadblocks and challenges from the Colombian context that impacted the PoC's outcomes.

The report then describes key technical findings and conclusions related to the PoC and to trade-offs between various blockchain permissioning configurations for public procurement. It subsequently lists suggestions for further experimentation and development. The report concludes with a link to the addendum, called the *Supplementary Research Report*. This downloadable document provides a framework for establishing success metrics for a new blockchain-based e-procurement system; background information on the Colombian public-school meal programme; a snapshot of the Colombian regulatory framework for blockchain and cryptocurrency; a discussion of existing efforts to curb procurement corruption; an exploration of additional use cases for blockchain in government transparency and accountability; and a "Further reading" section for additional coverage of the subject.

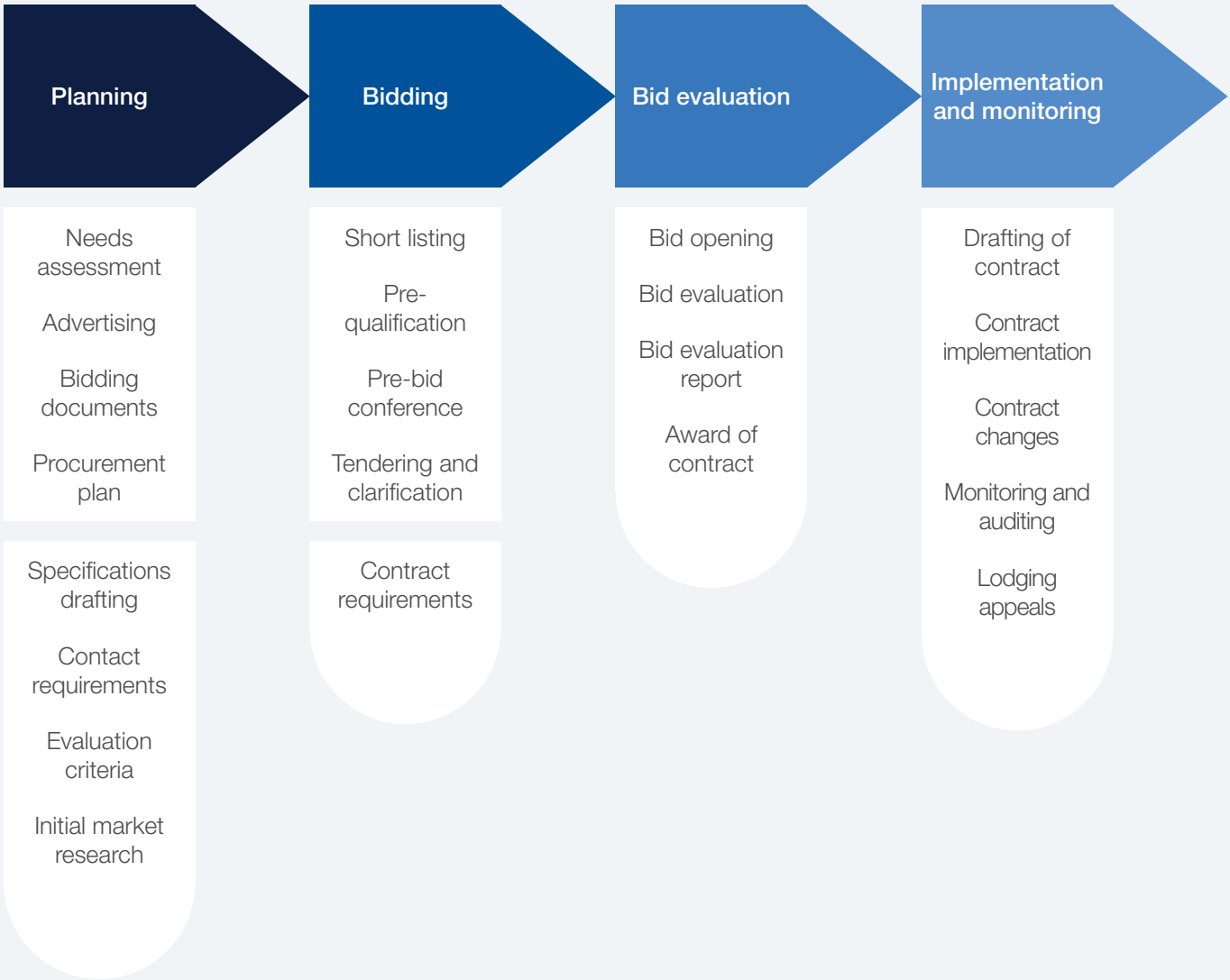
The problem: Corruption in public procurement

According to leading international organizations such as the Organisation for Economic Co-operation and Development (OECD) and Transparency International, public procurement, also referred to as government contracting or tendering, is one of the public-sector activities most vulnerable to corruption. Through public procurement, governments at the local, regional or national level purchase goods, services and other works – from the building of bridges and airports to the supplying of schools and hospitals.[3]

Governments collectively spend approximately $9.5 trillion on procurement contracts worldwide through processes often marked by complexity, opacity and a high degree of human discretion.[4] These factors result in a substantial risk for corruption. Across the world, the OECD and United Nations Office on Drugs and Crime estimate that 10-30% of a public contract's overall value is commonly lost to corruption, diverted to the pockets of corrupt government officials and other participants.

In the case of large government contracts, public procurement usually consists of four phases: planning, bidding, bid evaluation, and implementation and monitoring (Figure 1). Smaller or highly complex contracts may be awarded via a direct or negotiated purchasing agreement.[5] Each phase of each kind of public procurement process presents its own challenges and opportunities for corruption, including bribery, undue influence on government assessments, private-sector collusion, bid rigging, coercion, extortion, and fraudulent submissions and bid evaluations.[6]

FIGURE 1: **The four key stages of the public procurement process**



Source: Transparency International, 2014

Public procurement is a hotbed of corruption for multiple reasons:

1. Vast sums of money are up for grabs: Every year, governments spend between 10% and 30% of national GDP on procurement.[7]

2. Public procurement involves close and repeated interaction between government officials and the private sector. The blending of public-sector activity with private-sector profit motivations is a high-risk combination.[8]

3. The procurement process is often complex and bureaucratic, increasing the opportunities and motivations for shortcuts and "wheel-greasing".[9]

4. Low transparency in the needs assessment, contract specification and vendor selection processes is common, which leaves the distribution of large sums of money at the discretion of procurement officials.[10]

5. People rarely report corrupt activity in the public procurement process even when they become aware of it. This is often attributed to a sense of distance from, or indifference towards, government financial loss, the absence of effective reporting and whistle-blower channels, or concerns that complaints would be futile or result in reprisal.[11]

Certain auctioning processes and industries are particularly opaque and thus especially vulnerable to corrupt practices. For example, direct purchasing agreements and negotiated contracts are generally not awarded based on a set of predetermined, objective criteria, which makes these award processes far more difficult to monitor or audit as compared with open bidding.[12] Similarly, the lack of easily obtainable market guideposts and the unpredictability of many major construction projects leave needs assessments and post-award adjustments largely to the discretion of government officials and their chosen private-sector counterparts.[13]

The harm: Crippling public services, economic development and democracy

Corruption in public procurement erodes trust in government institutions, promotes unfair business practices, results in market distortions, weakens foreign investor appetite, and decreases access to and quality of much-needed public goods and services.[14] As Transparency International writes, "taxpayers' money to pay for hospital equipment, books for schools or safer roads, for example, ends up sitting in the pockets of the corrupt".[15] The consequences of systemic corruption are pervasive, ultimately stunting progress in public health, sustainable development, quality of life and trust in public officials.

Even when procurement corruption is caught, the effects send shock waves through countries. For instance, Latin America's largest construction conglomerate, Odebrecht, declared bankruptcy after a 2014 investigation led by Brazilian, US and Swiss officials found the company had paid roughly $800 million in bribes to multiple governments.[16] This high-profile investigation and the subsequent annulment, or potential annulment, of corrupt contracts paralysed related industries across the region, interrupting payment chains, causing the bankruptcy of suppliers and resulting in the dismissal of thousands of workers.[17] Furthermore, Brazilian state-owned banks held the majority of Odebrecht's $25.3 billion debt, a financial blow that ultimately may fall on the shoulders of Brazilian taxpayers.[18]

As a deterrent backed by legal force, steep financial consequences and possible incarceration, the criminalization and prosecution of procurement corruption are essential components of any country's anti-corruption framework. However, proactively limiting opportunities for corruption in the first place may more efficiently minimize the various financial, societal and political harms that emanate from this widespread phenomenon.[19] To this end, the leading institutions tasked with anti-corruption oversight universally advocate increased transparency and accountability throughout the procurement process.[20]

CASE STUDY: **Procurement corruption in Colombia**

Colombia is no exception when it comes to procurement corruption. A recent study by the country's Corruption Ombudsman in partnership with Transparency for Colombia and the Charles Leopold Mayer Foundation found that approximately $6 billion were compromised by procurement corruption in Colombia between 2016 and 2018. The sectors most affected by corruption included education, infrastructure and transportation, health and civil services.[21] Notably, Colombia's experience with corruption is roughly average, ranking 96th among the 180 countries catalogued in Transparency International's 2019 Corruption Perceptions Index. On an absolute level, Colombia received a score of 37/100 where a score of 0 indicates a perceived very high level of public-sector corruption and 100 indicates a perceived very low or clean level of corruption.[22]

In addition to involvement in international bribery schemes like the one exposed within Odebrecht, more localized procurement corruption in Colombia erodes public services and economic development. For example, in a 2017 investigation of the public-school meal programme (*Programa de Alimentación Escolar*, or PAE), which provides breakfast and lunch in Colombia for the most in-need children, the country's Comptroller General revealed disturbing irregularities in the pricing and delivery of food, with contractors purchasing chicken breasts at four times the market price and 32 million meals going undelivered in 2016.[23]

The Colombian government recognizes that public procurement is one of the weakest links in the country's anti-corruption efforts at the national, regional and local levels. However, recent attempts at reform, including the 2011 Anti-Corruption Act and the new federal Anti-Corruption Office, have done little to reduce instances of corruption.[24] In fact, in 2017, the US Department of Justice indicted and ultimately extradited Colombia's National Director of Anti-Corruption on bribery and money laundering charges.[25] For these reasons, the Colombian public sector has decided to embrace innovative approaches to anti-corruption, which, among other initiatives, include a joint project between the Colombian Inspector General's Office, IDB and the World Economic Forum to develop a blockchain-based response to procurement corruption.

Table 1 summarizes where corruption commonly occurs in the vendor bidding and bid evaluation phases of public procurement processes globally, including in the PAE public-school meal programme in Colombia, which is the focus of the *Technology Project*.

TABLE 1: **Corruption in public procurement: Bidding and bid evaluation phases**

- **Undue direct contracting** – Bypassing a competitive bidding process and awarding the contract to a predetermined entity because of specious claims related to "extreme urgency" or other circumstances
- **Lack of competition in the bidding process** – From absence of public notice for the invitation to bid, low access to pre-tendering phase, or low confidence in the procurement process
- **Evaluation and award criteria not objective, complete or announced in advanced** – Government officials who fail to clearly announce tender offers, fail to share key bidding information with all bidders, or fail to create tender offers with objective and clear evaluation and award criteria
- **Bid tailoring** – Contract details and evaluation criteria tailored to favour a specific vendor
  - **Low contract standardization** – Narrow contract evaluation criteria and requirements that disqualify some vendors from participation
- **Vendor track-record fraud** – Deliberate misrepresentation of vendors' track record, capacities and qualifications
- **Vendor eligibility exceptions** – Exceptions enabling vendors with poor track records or qualifications to compete
- **Low tracking of vendor history and past performance** – Low vendor performance tracking that enables repeat participation by corrupt or low-performance vendors
- **Bid price collusion** among vendors – From weak confidentiality in the bidding process
- **Conflicts of interest** – Public officials who select vendors and receive campaign financing or other benefits from them; frequent close relationships between regional vendors and political leaders such as a mayor or senator
- **Subcontractors or partners chosen in a non-transparent way** – Without accountability of performance from those selected
- **Unclear payment flows with subcontractors**, allowing for bribes – Frequent bribes paid by the subcontractors and small and medium-sized enterprises (SMEs) involved in a contract rather than the tender-contract winner itself
- **Vendor failure to disclose accurate cost or pricing data** – Inaccuracies resulting in invoice markups or "channel stuffing" after vendor selection
- **Poor contract price "benchmarking" practices** – Government agency use of an unreliable service reference-price benchmark, sometimes referring to the same one or two pricing benchmarks that do not accurately reflect the service price
  - **Low transparency** in price benchmarking sources
  - **Too few or no price benchmarks** listed or employed
  - **Contract price overestimation** with exorbitantly high price benchmarks that enable the tenderer to accept exorbitantly priced contracts
  - **Abnormally low bid offers** from vendors to win bids, followed by incomplete contract fulfilment, default from contract or vendor failure to fully pay subcontractors
- **Decisions made and reviewed by only one person** – Failure to uphold the "four eyes principle"
- **Inadequate records** – Delayed, incomplete or inaccessible records of vendor selection and procurement process
- **State-level or national auctions** that require very high operational and financial capacities – Favouring established, large-scale producers and hurting competition
- **Low investigatory capacity** – Of national monitoring and oversight institutions
- **Manipulation of records** – In paper-based, non-digitized procurement systems

Sources: OECD, 2016; Transparency International, 2014; interviews in Colombia

Project use case and experiment

Project overview and scope

The *Transparency Project* is rooted in the development of a software proof-of-concept (PoC) for the procurement of the Colombian PAE public-school meal programme. Background information on the PAE is provided in the *Supplementary Research Report*. By being rooted in a software PoC, the project takes a bottom-up approach to investigating and uncovering the technology and governance trade-offs, possibilities and constraints involved with a blockchain-based public procurement system whose primary goals are to increase transparency and accountability and, thus, to reduce instances of corruption.

The project takes a three-pronged approach, as shown in Figure 2.

The software PoC was developed during the second half of 2019 by a team of blockchain engineers within the National University of Colombia's InTIColombia Research Group.[26] It was developed to reflect technical, policy and civic engagement specifications and guidelines that were carefully co-designed by the project's diverse multistakeholder community of global experts. At the same time, the PoC's technical development itself triggered various questions regarding policy and community engagement. Thus, while each of the three elements in the project approach is a distinct aspect, all three critically informed one another.

Vulnerabilities in public procurement to address

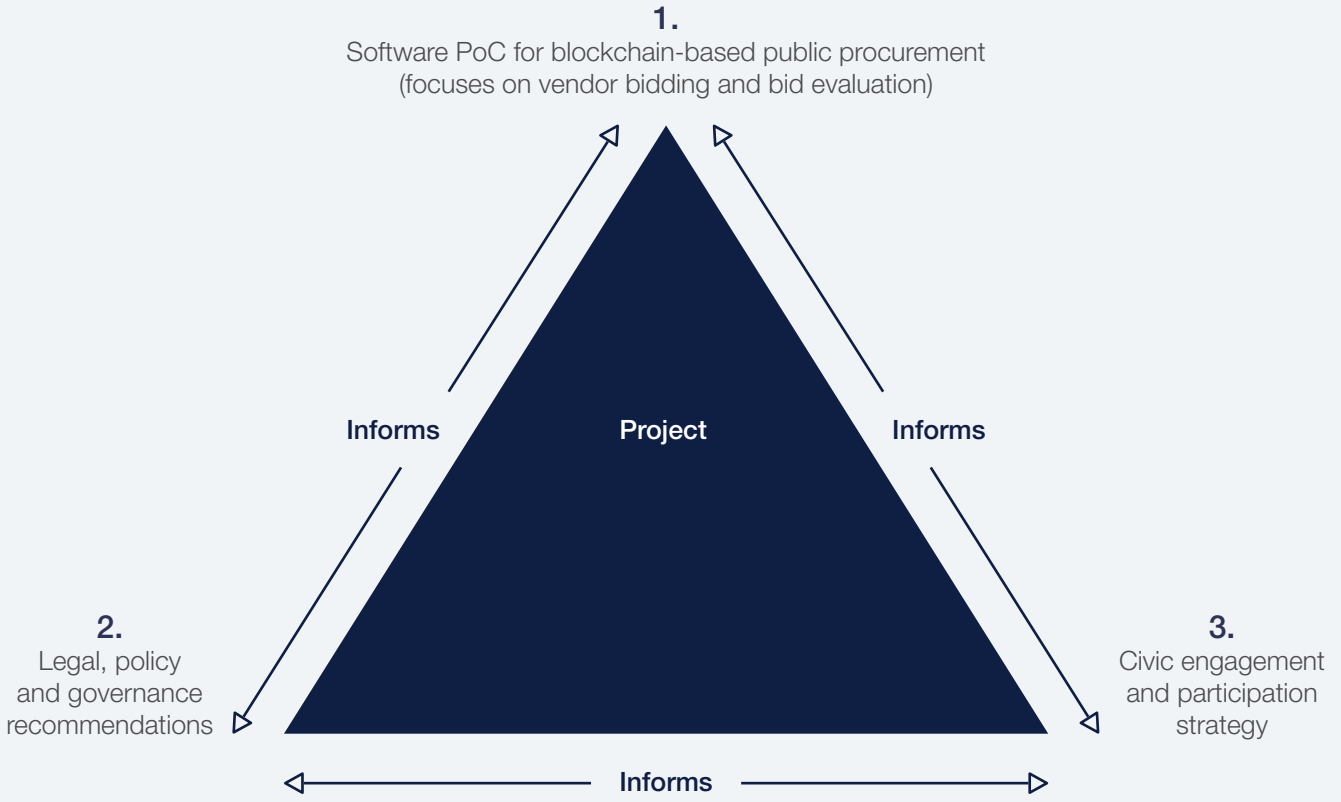
The project's software PoC seeks to improve the vendor bidding and selection phase of public procurement through specific channels:

1. Permanent and tamper-evident record-keeping
2. Real-time procedural transparency and auditability
3. Automated functionalities with "smart contracts"
4. Reduced reliance on the discretionary decision-making of centralized parties and authorities
5. Enhanced citizen engagement

The project hypothesizes that by combining these five capabilities in a software solution and pairing them with complementary policies and governance systems, governments can deploy a more transparent and accountable e-procurement system that helps to stunt the widespread instances of corruption.

A summary of the challenges with respect to accountability and transparency in public procurement is given in Table 2, abbreviated from Table 1. The *Transparency Project* seeks to address the highlighted items, either through the software solution; legal, policy or governance recommendations; or civic engagement and participation. In many cases, issues are addressed by a combination of these elements.

FIGURE 2: **Project approach**



Source: World Economic Forum

TABLE 2: **Summary of accountability and transparency challenges in public procurement**

Transparency and access	Competitiveness and integrity
– **Delayed or incomplete publication of records** – **Low procurement process and record access and visibility** – Low transparency in payments	– **Direct contracting** – **Bid tailoring** – Conflicts of interest and bribery – **Prevalence of auctions that favour established and large vendors**
Contract pricing	**Institutional challenges**
– Price collusion among vendors – **Poorly conducted price "benchmarking"** – **Vendor underestimation of contract price to win bid**	– **Low investigatory capacity at national monitoring, oversight and "watchdog" institutions**

Proof-of-concept technical guidelines

This section summarizes the co-designed technical design guidelines and recommendations that informed the PoC for the *Transparency Project*. Additional guidelines and functional specifications developed for the project's software solution can be found in the annex of the Model Request for Proposal (RFP) document. It is important to note that this information heavily informed the project PoC but, in some cases, the PoC end-product diverges from this guidance, as described in this document.

Figure 3 shows the public procurement process that is the basis of the software solution. It is based on Colombian legal requirements.[27]

Table 3 lists the key steps and features of the intended software solution, which are specifically designed to address sources of vulnerability and corruption. It is important to reiterate that any technology solution, including the one described here, has limitations and fails to stop certain corrupt activities, such as vendor collusion or bribing activity conducted outside the e-procurement system. It is also difficult to reduce corruption risk in certain activities, such as vendor registration, which typically depend on authorization by a centralized public-sector entity.

FIGURE 3: **Vendor selection process within Colombian public procurement law**

Source: World Economic Forum

TABLE 3: **Intended software solution to address sources of vulnerability and corruption**

1. Vendors register to participate in the new system to compete for tenders.

– The vendor registers through a state bidding agency or tenderer so neither alone can block registration. Vendors who are qualified in the national vendor database may register to participate in the system.

– Once approved, the vendor generates a unique blockchain-based address, which is used as an identity for the bidding process (denoted as the "vendor ID").

– To submit bids anonymously during the bidding period, the vendor uses the private key of the "vendor ID", along with a unique identifier from the specific tender process, to generate a pseudonymous one-time address from which the vendor will submit their bid to the specific tender auction (denoted as the "hidden ID"). The vendor establishes a secret link or cryptographic commitment from the "vendor ID" to the "hidden ID" that will be revealed upon the bid evaluation to indicate the vendor's identity. A 12-keyword mnemonic feature allows vendors to recover their "vendor ID" and "hidden ID" account information if they are lost.

2. The initial tender offer is published as a smart contract using blockchain technology.

– The tenderer initiates the procurement process by publishing its draft tender offer to the public. A new smart contract for the draft tender offer is created; it holds a link to the tender offer document, which is stored in a distributed file storage system compatible with the blockchain network (e.g. InterPlanetary File System (IPFS) for Ethereum).[28] A hash of the file is also taken and published onto the smart contract.[29]

– Each tender includes the full terms and conditions of the tender, as well as the evaluation criteria with clearly defined weights (e.g. 30% price, 20% experience, etc.) that the tenderer will use to select the winning bid.

– The required "price benchmark" field forces the tenderer to list price benchmark sources, providing transparency. Sources and benchmarks may need to be kept private until after the bidding period closes in order to not compromise competitive bidding.

3. A public comment period for the tender offer is established.

– The smart contract imposes a minimum public comment period (according to law) when the public and prospective vendors can review, ask questions and raise concerns about the tender offer. Public comments can be submitted to a hash function with output recorded on the smart contract or elsewhere.

– The tenderer incorporates relevant feedback and makes necessary modifications, including to evaluation criteria and weights.

– If contract modifications are made towards the end of the comment period, an automatic red flag warns of potentially suspicious activity (e.g. the tenderer hiding adjustments through last-minute changes).

4. The final tender offer is published as a new smart contract on blockchain.

– A second, new tender offer smart contract is created; it holds a link to the final published tender offer, which is stored in the distributed file storage system (e.g. IPFS). A hash of the document is also taken and published onto the smart contract. The hash provides a timestamped record that can serve as a reference if the tenderer is suspected of modifying the tender offer later in the process.

– The tender offer cannot be modified after publication.

5. The provision for tender withdrawal, cancellation, restart is stipulated.

– The system allows the tenderer to withdraw the tender offer and restart the process, withdraw the tender and conduct a direct contract, or cancel the auction completely. All cases require the tenderer to put the rationale in writing in the system for permanent record-keeping.

6. The bidding period opens.

– The bidding period automatically opens according to a schedule programmed in the final tender offer smart contract. During the bidding period, the software allows vendors to submit their encrypted bid offers for the required minimum bidding period.

– Vendors submit encrypted bid offers (within unique bid offer smart contracts) with anonymous one-time accounts (“hidden IDs”) associated with their primary vendor account (“vendor ID”). Bids are encrypted under vendors’ “hidden ID” private keys so no parties other than the vendor can see bid information at this point.

– Encrypted bid documents are stored in the decentralized file storage system (e.g. IPFS). A hash of each bid offer document is also stored within its corresponding bid offer smart contract. This hash output can be used to verify against potential bid manipulation or the tenderer claiming the bid was not submitted.

7. The bidding period closes.

– The bidding period is automatically closed according to the schedule programmed in the final tender offer smart contract. No bids are accepted after the close.

8. The tenderer downloads and opens the eligible bids.

– The tenderer downloads all the submitted bids from registered bidders.

– The tenderer automatically asks vendors to reveal their bid offers by requesting them to publish their “hidden ID” private keys, which can be used to decrypt their bid offers.

– During the decryption process, the software validates the cryptographic connection between the “vendor ID” and “hidden ID”. Only bid offers from vendors whose connection is proven between their “hidden ID” and “vendor ID” are automatically decrypted and published. These bid offers proceed to the evaluation phase.

9. The tenderer conducts the phase 1 evaluation of bids.

– The software automatically evaluates bid offers to meet minimal evaluation criteria (phase 1 evaluation). Qualifying bids that will proceed to the phase 2 evaluation are recorded in the tender offer smart contract.

– Bid offer evaluation results are automatically published for scrutiny.

10. A public comment period for phase 1 is established.

– An automatic minimum public comment period (as required by law) with the publication of comments is imposed.

– Public comments can be submitted to a hash function with output recorded on the smart contract or elsewhere.

– If relevant, bids and tender offer can be evaluated against the hash of each respective record posted on the blockchain to verify against changes after bid submission or tender offer publication.

11. The tenderer conducts the phase 2 evaluation of bids.

– The tenderer proceeds to evaluate all qualifying bids from phase 1 and assigns scores to relevant sections in each bid. Scoring may be performed manually or automatically.

– Scores are automatically summed; the system produces the recommended winner. If the winner is different than the recommended winner (by score count), the system generates an automatic red flag.

– The tender evaluation, scoring and decision are published for scrutiny.

12. A public comment period for phase 2 is established.

– An automatic minimum public comment period (as required by law) with the permanent publication of comments is imposed.

– Comments can be submitted to a hash function with output recorded on the smart contract or elsewhere.

– The tenderer integrates any changes after the public comment period and publishes final phase 2 scoring, decisions and winner results.

13. The final winner decision is published.

– All process records remain permanent and tamper-proof for public scrutiny via blockchain-based record-keeping; records are also backed up in the centralized database.

Technology design guidelines

This section briefly describes the high-level technical design guidance used for the *Transparency Project* PoC. The project's PoC experiments with a fully permissionless configuration to investigate the associated capabilities and limitations for the public procurement use case and for public-sector transparency in general. It specifically employs the public Ethereum blockchain "mainnet", or main network. A fully permissionless blockchain network maximizes system decentralization and security (in terms of data permanence and censorship resistance) and is thus highly relevant to the anti-corruption context. It is also the foundational blockchain technology; close study of its capabilities and limitations can uncover relevant trade-offs for policy-makers seeking to understand which blockchain configurations are most appropriate for their needs. Alternative configurations and blockchain protocols, discussed later in this section and report, can and should also be considered for follow-on projects.

Blockchain network permissioning configuration
Blockchain networks can have permissioned or permissionless configurations along three levels, listed below. Permissioned configurations indicate invite-only or private and constrained access. Permissionless configurations are fully open with public access.

- Read access (ability to view transactions and information)
- Write access (ability to submit transactions and information), or
- Consensus-participation access (ability to serve as a transaction-validator node).

The use of a fully permissionless configuration provides many benefits to a blockchain-based public-procurement system. It also has downsides. Table 4 lists the advantages and disadvantages:

TABLE 4: **Permissionless blockchain network configuration advantages and disadvantages**

Advantages to a fully permissionless blockchain configuration in public procurement:

Read access: Permissionless (with bid confidentiality schemes where appropriate)

- All transaction and bidding information is public, enabling permanent public records and real-time scrutiny. Public readability is critical for citizen engagement with the platform.
- All tender offers are publicly viewable from the announcement of the auction onwards. They are never encrypted and should be made available for immediate public access.
- All vendor bids are public yet encrypted to all parties from the time submitted until after the close of the bidding period when they can be decrypted. After the tenderer concludes each round of bid evaluation, it publishes for the public record all bid information revealed to it during that evaluation round.
- Bid decisions and evaluations by the tenderer are always publicly viewable and remain permanent records as soon as decisions are concluded. The public can comment on decisions and evaluations during pre-specified periods in the procurement process.

Write access: Permissionless (except for permissioned vendor participation)

- Public write access enables citizens, journalists and other parties who are monitoring the process to comment within the system and raise alerts regarding suspicious and potentially corrupt behaviour by the tenderer or bidding parties. The public can make comments and complaints within the system during pre-specified periods for public comment. Anyone can make comments, and they interface with a user-friendly website or mobile phone application.
- Note: Vendor bid submission is partially "permissioned" in the solution. Anyone can submit bids, but only bids from officially preregistered accounts – which receive a secret passphrase upon registration – are reviewed. All such bids are documented, and the tenderer is unable to delete or "censor" them.
- Note: A government's ability to conduct a tender offer within the blockchain solution is also "permissioned": tenderers who launch and conduct auctions in the system must be pre-approved by the bidding agency.

Consensus-participation access (participation in transaction verification): Permissionless

- Permissionless consensus provides a high degree of network security, as measured in terms of the network hash-rate for proof-of-work networks like Ethereum. Across various types of decentralized consensus algorithms beyond proof-of-work, network security is generally higher in permissionless systems as they allow for more node participants, which in turn raises the costs and difficulty for a "double-spend" attack, where malicious or corrupt actor(s) dominate(s) the network's computational or voting power, either by bribing or colluding with other nodes or by other means, in order to compromise transactions and records.[30]

- In general, the higher network security afforded from maximized decentralization of the consensus process is achievable only in permissionless-consensus blockchain networks. It is particularly valuable for anti-corruption use cases as it raises the cost and increases the difficulty of corrupt actors to unduly affect transactions and records in the system.

- For institutions organizing a new decentralized application or service, permissionless-consensus participation generally has lower set-up and maintenance costs as there is no need for certain participants to set up nodes to operate the network. By contrast, in a permissioned-consensus network, predesignated nodes, or other parties on their behalf, would need to bear software set-up and ongoing maintenance, security and upgrade costs. It may also be challenging to identify suitable and trustworthy entities to operate nodes.

Disadvantages to a fully permissionless blockchain configuration:

- **Transaction throughput and scalability**: All else being equal, blockchain networks with permissionless-consensus participation have lower transaction scalability and throughput as their consensus algorithms have higher transaction approval requirements. Most major permissionless blockchain networks have constrained transaction throughput today. Today's Ethereum mainnet can process roughly 15 transactions per second for all global participants, and thus is not currently suitable for a large-scale deployment. With network congestion, including that which could be caused by the procurement application itself, the solution's transaction speeds could slow down.

- **Transaction fees**: Permissionless-consensus blockchain networks require transaction fees to compensate nodes, or miners, for performing transaction verification. Transaction fees are typically sent alongside transactions in the system.[31] The use of transaction fees raises several issues:

  - While transaction fees are generally very low in blockchain networks, they are variable and can increase rapidly in times of network congestion or stress.

  - The use of cryptocurrency for transaction fees may be problematic in jurisdictions where their use is illegal or not explicitly permitted.

  - Transaction fees may compromise vendor anonymity during the bidding period as vendors may need to pay a traceable transaction fee when submitting their bid. Special consideration and steps must be taken to disassociate this transaction fee from the vendor's identity during the bidding period.

  - It may not be legal for vendors to pay extra costs (i.e. transaction fees) to use an e-procurement system.

- **Energy consumption**: A proof-of-work blockchain-based system, such as Ethereum today, requires substantial electricity consumption and cost. Alternative consensus algorithms such as proof-of-stake consume significantly less electricity.

Selecting a blockchain network: Once the read, write and consensus-participation access is determined, the blockchain protocol supporting the new public procurement solution can be selected. It is important to select a protocol with very high network security. The network should also have a technical development and support ecosystem. It is also beneficial if contributors are continually working towards improving the network – from fixing software problems to implementing upgrades and improving scalability. The Ethereum blockchain network currently has the largest network hash-rate, a key security parameter, and the largest ecosystem of validating nodes and technical contributors of any smart-contract-capable blockchain network; notwithstanding, alternative networks with high security and robust technical ecosystems may also be suitable.

The mainnet of a network is also strongly preferred, all else equal, because of its greater network security relative to a test network, or "testnet" environments, which typically have fewer validator nodes and are thus more vulnerable to adversarial attacks that can compromise records and transactions in the network. Testnets can also be closed or reset, jeopardizing an application and its records.

Blockchain scalability: In the future, if the software solution seeks to scale to multiple jurisdictions with greater transaction volumes, network throughput on a public, permissionless blockchain network such as Ethereum could be prohibitive. To resolve scalability challenges, the solution may need to shift to employ one of the following architectures:

- A permissioned blockchain implementation
- A "hybrid" implementation with two protocol-level blockchain networks: a permissioned blockchain network can allow for higher transaction throughput while a permissionless protocol is employed for tamper-evident record-keeping
- A new, next-generation protocol-level implementation with advanced throughput (e.g. Ethereum 2.0 for the Ethereum permissionless network), or
- A "layer 2" scalability solution on top of a permissionless blockchain protocol, such as "state channels" for Ethereum.

Research for most next-generation protocol-level implementations and "layer 2" networks is still under way and not ready for production-level deployments.

File and document storage: Data storage on public, permissionless blockchain networks such as Ethereum is inherently expensive, as data is permanently stored and replicated on the thousands of nodes in the network.

To address data storage challenges, data files can be stored in a specialized decentralized file storage system connected with the blockchain network. An example is the IPFS, a leading distributed file storage system compatible with the Ethereum blockchain network. The *Transparency Project* software solution employs IPFS to store, in a decentralized manner, the tender information submitted from the tenderer, an encrypted copy of each bid offer submitted from vendors, and a decrypted copy of each qualifying bid offer after the bidding period closes.

It is advisable to also store "backup" data files within a centralized system. If feasible, this system should have tamper-resistance or tamper-proofing elements. Storing backup files reduces risks associated with blockchain networks that could occur in the future. For instance, it is possible that network participation could decline dramatically over time and reduce record-security in that system. In this case, it could be feasible for past records to be affected. When necessary (i.e. during the bid evaluation phase), documents such as bid offers should be stored in an encrypted state.

Open data contracting standard: The use of the Open Contracting Data Standard (OCDS), a framework defining a common data model for the disclosure of data and documents in government contracting processes, including those for public procurement, should be considered. The OCDS has been used in modern digital procurement services and can inform data format and disclosure to increase public transparency and access.[32] The World Trade Organization (WTO) also developed the Agreement on Government Procurement (GPA), prescribing best-practices-based methodology for publishing OCDS data.

Model Request for Proposal: “Blueprints” for a blockchain-based procurement system

Governments or institutions seeking to hire a software development team to build a blockchain-based e-procurement system can refer to this report’s model Request for Proposal (RFP) as a starting point or guide for their own RFPs, requests for information or terms of reference. The model RFP may also serve as a research resource for institutions or technology researchers interested in blockchain for public procurement and government transparency.

The model RFP document was co-designed within the project’s expert community. By providing a sample RFP that includes technical design and specification guidelines, the Forum, IDB and Colombian Inspector General’s Office hope to support governments and institutions in their research, experimentation and understanding of a blockchain-based public procurement system.

– A downloadable Model RFP document is available for reference in PDF format.

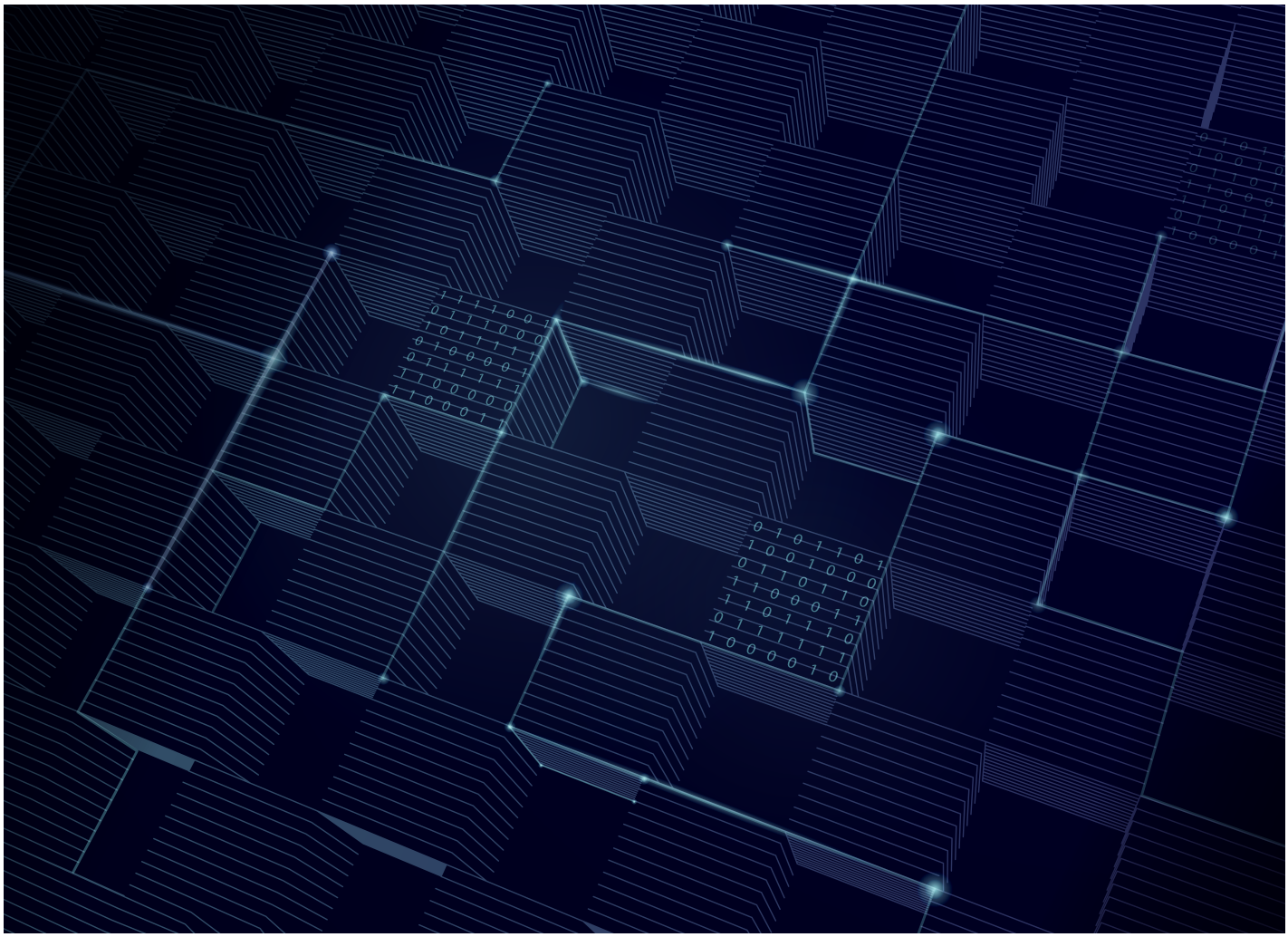
– A downloadable and editable Model RFP document is available for reference in Word document format.

Notably, the annex sections provide additional technical solution guidance and “blueprints” for software development teams, complementing the information provided in the previous section. The annex consists of the following elements:

1. Process flow chart

2. Solution requirements

3. Software functionality specifications and guidelines



Policy and governance considerations and guidance

Policy and governance components must accompany the implementation of blockchain technology to maximize its potential to improve transparency and accountability within public procurement processes. This section provides a menu of complementary policy proposals governments should strongly consider to strengthen integrity in e-procurement. It then enumerates software development and deployment strategies for blockchain-based e-procurement, informed by the project's PoC. Further, it discusses the civic engagement approach adopted over the course of the project PoC. Finally, it highlights a few significant legal and policy issues from the Colombian context that may resonate with policy-makers or technologists developing similar projects elsewhere.

Of note, while many elements described in this report are broadly relevant, policy-makers must consider specific national or regional contexts and conditions to determine the most feasible and appropriate regulations and civic engagement strategies to accompany a blockchain-based e-procurement solution, or any e-procurement solution more generally.

Legal and policy recommendations: Complementary policy proposals

The full anti-corruption potential of any new e-procurement platform cannot be realized in the absence of a clear legal framework based on international best practices and effective stakeholder engagement and oversight. While the particularities of each country and industry context make detailed policy proposals impossible, this section highlights policy solutions that can complement and magnify the anti-corruption capacity of an e-procurement system, whether blockchain-based or not.

These policy proposals reflect best practices advocated by the Open Contracting Partnership (OCP), the Open Data Charter, the OECD, the United Nations and the WTO. They are meant to flag a few concrete ideas and initiatives that would capitalize on the information dissemination capacity of blockchain-based procurement to increase accountability, transparency, corruption prevention and fairness throughout the procurement process.

Build a comprehensive e-procurement hub

i. **Remove legal barriers:** Governments should revise laws that effectively limit the use of e-procurement platforms, such as those that require in-person interactions between tenderer and vendor or mandate paper bid submissions.

ii. **Mandate the use of the designated hub:** Governments should mandate the use of a new e-procurement platform, if feasible, to compel behavioural change away from in-person procurement processes and to consolidate all transactions on a single database or record system.[33]

iii. **Make the hub comprehensive:** Either the e-procurement system itself or an affiliated website should contain all relevant information about the procurement process, including procurement policies, procurement officer codes of conduct and special interest disclosure requirements, notices about upcoming auctions, tender documents, vendor bids, award and rejection criteria, award notices, contract details, and vendor "blacklists" and "whitelists".[34][35]

    In addition to the initial procurement auction, all post-award contract renegotiations should be documented on the blockchain platform. As a hotspot for secretive self-dealing, contract renegotiation should be kept to an absolute minimum. When necessary, requiring the renegotiation process to occur publicly on the e-procurement platform sheds light on adjustments to the initial agreement and eliminates incentive to renegotiate for corrupt purposes.[36]

iv. **Make information accessible:** All this information must be free and accessible to the public – structurally and cognitively. Exclusionary access fees or registration walls should not exist, and the site content should be both searchable and downloadable.[37] Existing e-procurement websites like Open Public Contracts in Slovakia and Tender Monitor in Georgia provide blueprints for such a platform.[38] Both websites, developed by the national chapters of Transparency International, exemplify the power of concentrated and publicly available procurement data by enabling users to search for key signs of corruption, such as repeat bid winners, auctions with only one bidder and procurement contract details.[39] While the general public may not regularly log on to such a resource, the accessibility of high-quality reporting data propels citizen monitoring activities.[40]

Governments may also derive other benefits from increasing the accessibility of procurement information. Experience shows that easily accessible procurement information allows for greater competition among a wider variety of entities. Meanwhile, short-term auction notice and opaque processes cater to the interests of large, well-connected companies and repeat players.[41] Furthermore, this increase in competition overwhelmingly translates into significant cost savings and improved deliverables.[42]

A. Establish competitive auctions as the default procurement process

E-procurement platforms of various kinds can facilitate vendor participation by lowering the costs and physical barriers to entry.[43] While the extent of internet proliferation may pose a challenge in some areas, electronic bid submission allows for greater participation among SMEs and non-urban entities that no longer must bear the costs of paper applications and in-person meetings.[44] States should reinforce and promote these competition-promoting qualities by institutionalizing open and competitive auctions as the clear default procurement process.

i. **Remove arbitrary restrictions on contract eligibility:** As a base consideration, governments should minimize arbitrary or unnecessary restrictions on contract eligibility. This includes general prohibitions against foreign or out-of-state companies and overly restrictive contract specifications that frequently foreclose participation to all but a single vendor.[45]

ii. **Enact "whitelisting":** The construction of whitelists – electronic databases containing the names of companies with a record of completing contracts honestly and efficiently – can provide added incentive for clean contracting and help promote the participation of otherwise disadvantaged vendors.[46] Attention should be paid to any whitelists so they do not perpetuate anti-competitive behaviour by unfairly favouring or disfavouring certain vendors.

iii. **Localize procurement and support small and medium-sized providers:** Where possible, auction conditions should not favour the largest-scale producers and vendors. Conducting auctions at the city or district level rather than the country or state level, for instance, can improve the ability of smaller vendors to meet the minimal capacity requirements in tender offers. It may also be possible to support smaller vendors through efforts such as auction pre-qualification or exemption from certain document requirements. However, processes that grant certain vendors favoured status should be carefully monitored as they may become a source of corruption. Jurisdictions can also require a certain percentage of very large contracts to be awarded to small or medium-sized providers. A new blockchain-based e-procurement system may need to be designed to flexibly enable such policies.

iv. **Limit direct contracts and restricted auctions:** Direct contracts or restricted procurement auctions are a common site of corruption due to the heightened opacity and absence of competition. Various circumstances may necessitate the use of these otherwise less-favourable methods, such as a very limited pool of qualified bidders or a contract for highly complex goods or services. States should exhaustively enumerate the possible methods for procurement and clearly describe factors that would necessitate direct contracts or restricted auctions.[47]

    In particular, where the contract amount is the determining factor, states may want to make clear, in absolute terms, the ceiling price for limited bidding or direct contracting.[48] Governments should automatically investigate contract values that exceed this ceiling yet were not awarded via an open auction. Governments may also want to question or disqualify bids below a certain percentage of the average bid offer value to reduce the risks associated with abnormally low bid offers.

The universe of possible procurement methods could generally follow the following categorizations:

1. **Open auction**: A publicly advertised auction among a wide variety of qualified vendors; use as the default process

2. **Restricted auction**: An auction that allows only the participation of preselected vendors – a process that should be publicly advertised and transparent; use when necessary, as determined by pre-established objective criteria

3. **Negotiated contract**: A contract whose terms are negotiated between the tenderer and vendor; use when technical specification is impossible without vendor participation, when the initial tendering process failed to produce a winning vendor, or in response to an emergency or catastrophic event

4. **Direct or single-sourced contract**: A contract that is directly awarded to a single bidder through a non-competitive process; use in exceptional circumstances – where a contract value is very low, in response to an emergency or catastrophic event, in a monopolized industry where competitors are not yet available, or in a project with national security concerns[49]

Regardless of the selected method, procurement processes and outcomes should always be published on the blockchain platform or affiliated e-procurement hub to maximize transparency and reduce discretionary decision-making.

The 2020 COVID-19 pandemic is an example of a public emergency that may necessitate direct contracting to procure necessary goods and services quickly. The OCP has recently published recommendations for emergency procurement for COVID-19.[50] Countries including Colombia have published public dashboards in line with these recommendations.[51] Additionally, Transparency International published guidance from 13 Latin American chapters outlining minimum elements governments must consider to support integrity in public contracting during emergencies such as the COVID-19 pandemic.[52] The chapters further urge the following verbatim best practices for public procurement, particularly in times of a health emergency:[53]

- Activate national anti-monopoly agencies to avoid collusion between economic actors or practices that result in price speculation
- Activate real-time audits for public procurement processes, precisely because of the exceptional nature of the situation and the magnitude of the emergency
- Provide all relevant government procurement information on a single platform or identify a platform on which this information can be stored
- Ensure proper accountability during the emergency response.

B. Standardize notices, tenders, bids and contracts

Non-standard bidding documents reduce transparency and increase discretion at various stages in the procurement process.[54] From the initial auction notice to the final contract award, governments should specify the minimum information to be included in each document and notification. For example, tender documents could be required to include the bidding time frame, the nature and frequency of communication during the procurement process, qualification requirements, objective award and rejection criteria, and any relevant legal terms and conditions.[55] Best practices advocate the use of standardized language in tender offers, where possible, to ensure uniformity, fairness and transparency among procurement participants and across procurement auctions.[56] In addition to reducing the opportunities for corruption, such measures will assist with monitoring and accountability through increased comparability. They will also likely increase procurement efficiency.

C. Mandate transparent price benchmarking

Opaque or untethered price specifications within a procurement contract present significant opportunity for corruption. Tenderers and vendors alike should be required to provide multiple market-based price benchmarks to reduce the opportunity for self-interestedly inflated cost estimations. Requiring this type of market information is most challenging in the context of unique projects or in monopolized industries, where comparable products or services may be more difficult to encounter. Nonetheless, requiring that all tenders and bids contain, for example, three points of reliable market-based data to back each price estimation is achievable in most contexts and could reduce discrepancies within contract pricing and lower overall prices. In a blockchain-based e-procurement system, “oracles” could connect with external price benchmark sources in order to pull them directly into the tender offer, if relevant.[57]

D. Facilitate citizen audits

Over the past 20 years, organizations like Transparency International and the Partnership for Transparency Fund have developed citizen-fuelled auditing frameworks to complement government efforts, fill existing blind spots and engage the broader public with the issue of official corruption.[58] Citizen monitoring can take various forms based on the cultural, political and industry context. The monitoring process can be “open” or “closed”, with the former allowing the participation of the public at large, and the latter restricting the monitoring team to a preselected group of reputable individuals.[59] Within closed processes, monitoring can fall to a specific civil society organization (CSO),[60] a curated group of relevant experts or a single individual. Ideally, citizen monitoring occurs throughout the procurement process – from the initial government needs assessment through contract completion.

Countries across the world have experimented with public procurement citizen monitoring programmes in various forms – from public bid openings in Argentina and South Korea, to in-depth partnerships between CSOs and government agencies in the Philippines, to the strategic use of subject-matter experts in Mexico and Bulgaria.[61] The information dissemination capacity of modern procurement platforms could organically magnify these efforts by publicizing accurate documentation of, and insights into, the entire procurement auction.[62]

The following factors will remain key to the success of citizen monitoring:

i. **Mandate legally empowered citizen monitors and Integrity Pacts**: Whether by legislative decree or binding contract, the role of citizen monitors should be well-defined and backed by the force of law. To date, only a few countries legally mandate citizen monitors across the board.[63] The more common approach is applied on a case-by-case basis and uses legally binding agreements between the tenderer, the participating vendors and the citizen monitors. For example, Transparency International's Integrity Pacts[64] clarify expectations and responsibilities and, through clearly enumerated standards and prohibitions, bind all parties involved to upholding a corruption-free procurement process. The anti-corruption standards contained in such agreements can mirror or exceed existing public law.

   These agreements serve two key purposes: (1) promoting a collaborative and supportive partnership between authorities and citizen monitors; and (2) ensuring an even playing field among competing vendors.[65] Each party to the agreement may report irregularities, which, if not remedied, can lead to the dissolution of the agreement and sanctions against the offending party. Depending on the legal environment, disputes could be resolved in the national court system or an arbitral tribunal; in practice, complaints rarely escalate to this level.[66]

   Since the 1990s, Transparency International has helped launch hundreds of Integrity Pacts across more than 20 countries producing a variety of well-documented positive outcomes at a low cost.[67] They have been found to increase competition – even in historically monopolistic industries, decrease costs of public contracts, and enhance public perceptions of participating government agencies.[68] However, if treated as a box-checking exercise, these results will not come to fruition. Ideally, the agreement's content should be pre-established (rather than negotiated), participation should be mandatory, and processes for flagging and sanctioning violations should be clearly defined.[69] To maintain these robust procedural safeguards, such agreements may be reserved for higher-cost or higher-risk government contracts.[70]

ii. **Develop easy-to-use monitor tools:** Even when experts are involved, easy-to-use tools, such as checklists and report templates, greatly enhance the citizen monitoring process.[71] Best practices also advocate the development of only three to four metrics to be monitored and assessed throughout the procurement process.[72] For example, Transparency International USA created the Civil Society Procurement Monitoring Tool – a web-based and interactive guide and monitor checklist, which allowed all monitors to share their experiences and flag concerns. Such tools can strategically focus on the monitoring process and expand the pool of well-equipped monitors beyond those with specialized expertise.[73]

iii. **Act on citizen findings:** "Nothing motivates more than seeing results from one's work".[74] Citizen audit findings should be systematically shared, and concerns should translate into prompt government action. While some sort of financial compensation – especially to cover monitoring costs – may be beneficial, citizen monitoring initiatives are largely fuelled by a "spirit of volunteerism". Experience from countries worldwide has demonstrated that little incentivizes monitor retention more than receptive government agencies and systemic reform.[75] To promote accountability and transparency in the implementation of audit recommendations, governments should provide clear, objective criteria for recommendation review and avenues for monitoring government response.[76]

iv. **Explore creative solutions for public monitoring:** E-procurement systems can explore creative solutions to support the safety and privacy of the public monitoring auction processes. For instance, one could imagine a monitoring reciprocity programme where auctions in one state or country are monitored by people in a different state or country with which it has few ties. Citizens in each region could monitor risky behaviour in the partner region's auctions and vice versa. Alternatively, monitors overseas could also monitor multiple simultaneous e-procurement auctions in a country or across countries.

E. Provide safe and efficient avenues for challenging bids

As advocated by the OECD, WTO and United Nations, states should provide all stakeholders with a secure avenue for raising complaints throughout the procurement process. Whether through Integrity Pact-like agreements or more general avenues for citizen monitoring, the procedures and criteria for flagging and screening irregularities should be well-established and protection for whistle-blowers should be guaranteed.[77] The anti-corruption potential of advanced e-procurement systems can only be achieved if people feel empowered to act on the information they receive. Importantly, states should embrace a constructive, rather than retaliatory, approach to receiving complaints. Procurement system success metrics should also avoid discouraging complaints, but instead could frame them as a positive indicator of user engagement.

Development and deployment strategies for blockchain-based e-procurement

In addition to complementary policy proposals, several technical development and deployment strategies can help maximize the value of blockchain-based e-procurement or e-procurement more generally.

Project management process:

Problem identification and solution-matching: Before deciding to deploy blockchain, institutions should identify the specific problems within public procurement they seek to address, and the feasibility of blockchain technology to help resolve these problems.

Strong developer operations framework: A strong developer operations framework would benefit the project. This includes well-defined version control and quality control policies.

Cost–benefit analysis of blockchain technology: During the design phase, a cost–benefit analysis could be conducted evaluating the value of employing blockchain technology and its various permissioning configurations as compared to status quo processes or alternative procurement solutions. The entire software architecture should be evaluated. Such analysis should consider a variety of economic, procedural and social costs and benefits that may be incurred.

Periodic reporting and evaluation: The project development or management team should keep stakeholders appraised of the platform's progress and challenges via periodic updates throughout its development and deployment. The project team should also evaluate auction performance once deployed. To this end, the *Transparency Project* team developed a model evaluation framework, which can be found in the *Supplementary Research Report*. Such efforts can bolster project integrity, buy-in and solution identification.

Solution design transparency: It may be beneficial to provide transparency in how the software solution is designed and programmed, in order to provide understanding and confidence to participants and the public. The software code itself could also be open-source and publicly viewable, which can allow citizen monitors to gauge the software's fairness or identify any encoded biases or vulnerabilities. Open-source technology and data would also allow for the software solution to serve as a digital "public good" and to be adopted, improved and scaled by other jurisdictions.

Stakeholder involvement, civic engagement and design:

Multistakeholder design and deployment: Solution development and outcomes will be enhanced if the relevant stakeholders contribute to design or deployment. This can include civil servants from procurement institutions and bidding agencies, directly affected citizens (i.e. the children who benefit from Colombia's PAE programme and their families), vendors, lawyers, relevant government officers, technology engineers, and others. It may be advisable to construct a "stakeholder matrix" or map of the universe of relevant contributors.

Notably, cross-sector stakeholder alignment and engagement, including that of industry and government leaders, is crucial to project success. Resistance to change and vested interests may pose a challenge to project development; where possible, early and frequent engagement and clear communication of project goals may help cultivate buy-in among these actors.

Research on key procurement corruption conditions: Research into the sources and patterns of corruption within the country of deployment will provide valuable insights into solution design. Automatic alerts and functionalities could be built into a system to detect suspicious activity where it most frequently occurs.[78]

Training and user guides: User guides or manuals can be developed to guide the various types of participants (tenderers, vendors, citizens and other monitors) to successfully engage with the procurement platform. It may be beneficial to conduct public workshops or practice runs to teach various parties how to use the system and to increase adoption. The project sponsor should closely consider potential participation hurdles for the tenderer, vendors and the public, with a focus on costs, awareness, accessibility and usability.

An understanding of user constraints and motivations: Policy-makers should consider constraints local citizens may have related to e-procurement monitoring. The public must have adequate internet connectivity, digital literacy and access to computers or

smartphones to participate in the system. Policy-makers should also identify motivations for citizens to participate in auction monitoring and, where appropriate, seek to activate those motivations.

Vendor and tenderer incentives and motivations: In general, it may be difficult for jurisdictions to incentivize or compel the use of new e-procurement software to both vendors and tenderers if it is not legally required. Consideration as to the challenges of incentivizing vendors or tenderers to participate in the system should be taken before technology deployment.

Public communication strategy: A strategy for managing public perception and expectations related to the new e-procurement system should be developed. Perhaps most importantly, it should be clear that the new solution is not a "silver bullet" for ending corruption. The expectations and goals of the system should be clearly communicated, realistic and empower citizens to understand both its potential and limitations. It may also be appropriate to tailor communications for different audiences: certain groups may already possess a baseline understanding of blockchain technology or procurement procedures whereas others may not.

Town halls and targeted engagement: Depending on the preferred approach to citizen monitoring, several strategies can engage and educate the public on the opportunity to help audit procurement auctions. Local government offices may host live town hall meetings or public discussions, or they may provide educational pamphlets and electronic materials. Spreading awareness of the opportunity to participate is critical. It may also be helpful to target specific groups of stakeholders.

Legal environment:

Use of government sandboxes and supportive policies: Where available, innovation "sandboxes" can be explored for trailing e-procurement and anti-corruption technology experiments in a manner that does not need to comply with restricting regulation. Additional policies upholding domestic policy innovation may also be available to support project work.

Evaluation of legal constraints and political climate: The legal and political climate, including election cycles and potential legal roadblocks or regulatory constraints should be researched to inform the project approach, timeline and risks. The following issues or legal roadblocks should be assessed:

- Relevant political election cycles
- A relevant tender auction timeline (accounting for any effects from political election cycles)
- Legal clarity or a framework on the use or purchase of cryptocurrencies by tendering public institutions (required only for solutions based on public, permissionless blockchain networks)
- Legal barriers against the use of cryptocurrency for transaction costs by vendors (required only for solutions based on public, permissionless blockchain networks)
- Legal requirements related to solution integration with other systems, such as existing domestic e-procurement systems
- The legal context for motivating the use of the new e-procurement solution by vendors and tenderers
- Legal and regulatory compliance with respect to sensitive data protection or personal information
- Legal and regulatory compliance with respect to procurement data storage (i.e. geographic requirements)
- All other relevant legal and regulatory compliance requirements

Technical considerations:

Clear user interface and strong usability: Ease of use for all relevant parties should be a top priority in order to maximize participation. User interface and user experience design should include testing by the general public with a strong emphasis on cognitive and technical accessibility.

Evaluation of technical trade-offs: In the solution research and design phase, trade-offs and preferences should be evaluated and determined based on requisite cost, complexity, security, privacy and scalability. Blockchain systems entail trade-offs, and the priorities, costs and benefits for each of these parameters should be identified and carefully evaluated.

Gradual transition to a new system: During the initial implementation of a new e-procurement platform, if feasible, a schedule to gradually transition to the new platform can be implemented so that vendors and

tenderers are not impeded by technical roadblocks that can arise during the transition phase. During transition, the new e-procurement system can integrate with any existing e-procurement system and run in parallel to accommodate users who are not yet prepared for the new system and to reduce risk in the event of a failure or malfunctioning in the new system. All relevant documentation can be published to both systems for public review and redundant data management.

Additionally, the new solution can support a limited set of auctions, beginning with small purchases of common or standardized goods. Full transition to the new system can occur when the solution successfully manages the procurement of complex purchases, services and public works. Focusing first on the purchase of similar goods would also support performance measurement through better comparability between outcomes between the old and new systems.

Analysis of attack vectors and vulnerabilities: Any production-level implementation of a blockchain-based e-procurement system should carefully research, evaluate and predict its full range of vulnerabilities. Where possible, these vulnerabilities should be addressed prior to deployment. It is important that the entire system infrastructure should be evaluated for vulnerabilities, including application programming interfaces (APIs), browsers and data storage functionalities. It may be beneficial to avoid the use of APIs due to their centralization and vulnerability to attacks that could compromise the system. Any functionalities dependent on intermediaries, humans or centralized functions should be assessed for potential malfunctions, human failure or undue intervention.

Security auditing and review: It is advisable to conduct a third-party security audit and review for any new blockchain-based e-procurement system to more fully understand risks and identify software errors and vulnerabilities. For any production-level deployment, a professional, independent security audit is likely essential to reduce risk.

Civic engagement in the *Transparency Project*

Civic engagement is central to the *Transparency Project*. During the project's initiation in the second half of 2018, the World Economic Forum and the Colombian Inspector General's Office organized a workshop in Bogotá, Colombia with representatives from civil society, the media, government and other sectors to inform the project. Throughout the project's course, project leaders actively engaged local officials, CSOs and the local and global offices of leading international organizations such as Transparency International and the World Bank.

One project goal was to develop a system that supports the Office of the Inspector General Office of Colombia's public procurement auditing and investigatory capacity. Currently, the institution does not have the capacity to monitor all public procurement auctions for suspicious activity. By harnessing the power of citizen monitors to complement and inform the institution's own auditing activities, the Office would be able to more rapidly identify and investigate suspicious contracting behaviour. Notably, the software solution is designed to publish a complete record of the vendor selection process so that it is visible in real time online, allowing journalists, Colombians and interested stakeholders – in the country or overseas – to monitor the entire auction process.

The following civic engagement elements were raised over the course of the *Transparency Project*. Additional strategies, such as aforementioned considerations related to public communication, outreach and town hall meetings, will be employed if or when the software solution is approved for pilot deployment.

- **Strong user interface and user experience design:** To better facilitate public engagement within the new blockchain-based procurement system, the system was developed to have an intuitive user interface. One of the highest priorities for the system is to be very clear and usable for the public and interested stakeholders. User testing and feedback was conducted for the development of the software solution.

- **User manuals and training:** A user guide was developed to clearly explain the system to various types of users: citizens, tenderers and vendors. The user guide developed for the project can be found at this link: User Manual.

- **Confidential public participation:** Maintaining the confidentiality of public citizens, journalists and other stakeholders who raise concerns through the e-procurement platform is of paramount importance to prevent possible reprisal. Within the *Transparency Project*, the public makes comments through a website that does not require the commenter to provide any identifying information. The Secure Socket Layer (SSL) protocol is employed with the HTTP application protocol to ensure that citizen comments are sent over a secure website and browser connection. Comments are then securely submitted to and recorded on the blockchain. The connection between the website and the API server is also secured over an SSL protocol.

- For the *Transparency Project*, user IP addresses are visible only to the administrators of the web servers where comments arrive. In the project and in many cases, this administrator is located overseas where

interference incentives are low. Notwithstanding, any implementation of an e-procurement system where the public makes anonymous comments should consider the risks and vulnerabilities of commenter identification, including those stemming from the web server administrator. All digital transactions, including website comments, are traceable by nature and there always remains the chance that a highly resourced and motivated attacker can uncover commenter information or conduct other attacks on users within the system.

Experiences from Colombia: Legal and policy context for the *Transparency Project*

The experience developing a blockchain-based e-procurement system for the PAE in Colombia provides valuable lessons for similar work undertaken around the world. Of course, each country's implementation experience will vary according to its domestic legal, social and economic context.

– Political election cycles – After multiple conversations with the staff of the sitting Mayor of Medellín, where the software solution intended to pilot, a mayoral office change forced the project team to restart deliberations, coordination and relationship-building with the new mayoral staff. Additional local government election cycles throughout the project development period led to changes in the procurement calendar, creating a degree of unpredictability in the timing of the PAE auction pilot.

– Domestic blockchain laws and policies – The project's blockchain-based e-procurement software solution employs a public, permissionless blockchain network, which requires the use of cryptocurrency for transaction fees (ether, in the case of the project, for use with the Ethereum blockchain). Were the system to be adopted for across-the-board deployment in Colombia, clarity on the use of cryptocurrencies and a legal framework for their purchase by government parties would likely be required.

  Currently in Colombia, the government and public sector, as well as the general public, can employ cryptocurrency, as there is no law or regulation prohibiting its use. However, specific regulatory clarity supporting its use in the public sector would provide greater confidence in the development and deployment of public-sector blockchain-based applications that require cryptocurrency. Moreover, the Colombian financial authority, the *Superintendencia Financiera de Colombia*, has sent guidance to commercial banks indicating that they are not allowed to engage with cryptocurrencies, such as bitcoin, ether, or others. This policy is based in part on the use of cryptocurrencies in money laundering schemes and the financial authority's desire to maintain a high appearance of integrity among Colombian banks. This action has apparently translated into reticence towards cryptocurrencies among public-sector actors as well. Additional information on the regulatory framework for blockchain and cryptocurrency in Colombia can be found in the *Supplementary Research Report*.

– Policies related to e-procurement

1. Currently in Colombia, vendors participating in public auctions would not be compelled to use the new e-procurement system developed in the *Transparency Project*. At the same time, vendors are required to use the country's existing e-procurement system for public auctions.[79] The system, SECOP (*Sistema Electrónico de Contratación Pública*) is now in its second generation (SECOP II) and is required for all municipalities that are departmental capitals, including Medellín. As a result, the project's software was required to integrate with the SECOP system.

   Because of the requirement to integrate with the country's existing e-procurement system (SECOP II), software development was considerably more complex and time-consuming. The hours dedicated to the integration with SECOP II came at the expense of value-add solution features. In addition, the SECOP II software system provider, an independent overseas company, requested substantial compensation to open the connection (in the form of a web API) between the two systems. This resulted in a period of discussion and negotiation addressing this fee and the continued role of SECOP II in the country. Notably, this issue has resulted in a standstill in the deployment of the software solution as of the time of this report's publication.

2. In Colombia, vendors cannot be required to pay an extra cost for participating in a new e-procurement system, yet, as explained, transaction fees are a necessary aspect of bid submission in the Ethereum blockchain system. Here, the law in Colombia may also need to be clarified; it can be argued that the new software solution does not increase costs to vendors: if they were to submit paper bid offers, they would pay for the cost of stamps and envelopes to mail them – a cost likely greater than that of sending a blockchain transaction fee. If they were to submit electronic bid offers in traditional e-procurement systems including SECOP II, they would also need to bear costs for internet connectivity, computers and electricity.

   Nonetheless, to work around this restriction, the vendor accounts in the project software solution were designed to be pre-funded so that vendors would not need to pay transaction fees. This process is discussed in the following section.

Results: Key challenges, lessons learned and the way forward

Key challenges and lessons

Several conclusions can be drawn from the technical challenges that arose over the course of the *Transparency Project*. Many of the project takeaways also translate into commentary on the value and limitations of public, permissionless blockchains as a technology for corruption reduction in general and for public procurement specifically.

1. Key technical challenge: Vendor anonymity

In a blockchain-based e-procurement system where participation in transaction verification, or the consensus process, is open and permissionless, vendor anonymity presents a key challenge. The public, permissionless Ethereum blockchain, employed in the *Transparency Project* PoC, creates such challenges as vendors are required to send transaction fees with their bid offers. Because all system transactions are publicly viewable, steps must be taken so this transaction fee does not reveal the submitting vendor's identity. Of note, permissioned blockchain-based systems, where transaction verification is performed by a private set of predesignated parties, often do not require the use of transaction fees, obviating this challenge.

As part of the effort to address this hurdle, the *Transparency Project* PoC employed a cryptographic primitive called a "commitment scheme".[80] To help preserve a vendor's anonymity, vendors generate, in an "off-chain" manner, a one-time blockchain address or username, called a "hidden ID" in this project, from which they submit their bids and interact with a given tender offer. This "hidden ID" is linked secretly to the vendor's main blockchain address, called a "vendor ID". The link is proven when vendor identities are revealed during the bid evaluation stage. By submitting transactions from the "hidden ID", the transaction fee does not point to a vendor's known identity (blockchain address or "vendor ID" in the system), protecting its anonymity during bidding.

However, challenges with this scheme remain with respect to the attainment of cryptocurrency by the one-time "hidden ID" accounts for the purpose of paying transaction fees. The following list describes various approaches that can be taken to fund these "hidden ID" accounts as well as alternative strategies.

– **Vendor self-funding or reimbursement:** If the vendor is functionally and legally able to pay the cryptocurrency transaction fees itself, it can purchase cryptocurrency and send it to its "hidden ID" account. For this approach to succeed, vendors would need to be trained on how to purchase the cryptocurrency (ether in the PoC). Then, funds must be either sent from a cryptocurrency wallet address not known to be associated with the vendor or, if sent from the vendor or associated party, in a manner that masks the sender's identity.

  For the latter, modern cryptography techniques such as zero-knowledge proofs (ZKPs), or privacy-focused cryptocurrency such as Zcash which employs a ZKP construction called a "zk-SNARK",[81] could potentially be employed to mask sender identity. Trade-offs related to computational intensity and cost should be evaluated when considering such cryptography techniques. Research into the feasibility of implementing the cryptography scheme on the particular blockchain network must also be conducted.

  Furthermore, the "hidden ID" account should only be funded with an amount approximately equal to the amount required to perform necessary transactions, if possible. Otherwise, remaining funds may be stolen from the account after its private key is published during the procurement processes' bid evaluation phase (the private key is published so the previously encrypted bid offer can be decrypted and read). Alternatively, as soon as the private key is revealed, the "hidden ID" account can transfer the remaining balance to the vendor's main account (or any other account) without compromising its anonymity.

  If relevant or required, after the bidding period or entire procurement process, the vendor could be reimbursed by other parties such as the national bidding agency or commerce ministry. The transaction fee amount could be sent to the vendor's publicly known, main account address after the auction closes, reimbursing the vendor without compromising its identity during the bidding period.

– **Account pre-funding by other parties:** Another approach, relevant if vendors should not purchase cryptocurrencies for legal or other reasons, is for the "hidden ID" account to be pre-funded by another party. In this scenario, the other party should not know the vendor's identity in order to preserve its anonymity during the bidding period.

  This approach is employed in the *Transparency Project* PoC, although it entails a vulnerability. The vendor's "hidden ID" account sends a request to an API in the procurement system to fund its account from the API's predesignated pool of cryptocurrency. The funding goes to the "hidden ID" account on-demand and automatically. To preserve vendor anonymity, the vendor is not required to provide identifying information. However, without any requirements, this API would accept requests from all parties indiscriminately. As a result, sophisticated external actors could drain the API's account and steal funds. Because of the PoC's constrained software development timeline, this vulnerability exists in the end solution. With more development time, solutions could be devised. As an example, vendors could be required to submit a uniform

secret code they receive upon registration alongside their funding request. This code would generally preclude external actors from requesting funds from the API while not revealing the vendor's identity.

– **Additional and forward-looking strategies:** Additional strategies should be considered for next-generation solutions in order to preserve vendor anonymity with respect to transaction fees in the bidding process. These approaches constitute additional areas of investigation for blockchain-based public procurement, and for anonymous blockchain-based bidding auctions in general.

  For instance, the Gas Station Network, which was created to ease new Ethereum user onboarding by creating a mechanism for users to conduct transactions without needing ether cryptocurrency for transaction fees, could potentially be adapted to this situation.[82] Innovations in cryptography should also be monitored. The successful implementation of zk-SNARKs would mask sender and receiver (and transaction amount) information, which would preserve full vendor anonymity in bid submission and remove the need for the creation of "hidden ID" accounts in the first place. Additional relevant research under way includes the AZTEC Protocol,[83] decentralized private computation schemes,[84] "universal SNARKs"[85] and zk-STARKs,[86] all of which improve upon the efficiency of today's zk-SNARKs and can help achieve anonymous vendor bidding.

2. Key implementation challenge: Integration with official state public procurement software

Because Colombian law demands that all public procurement processes be registered into the official state public procurement system, the project's software solution was required to be compatible and integrate with the official state system (SECOP II). The result was a markedly more complex and time-intensive development process. This issue is discussed in detail on page 28.

3. Key attack vectors: Spamming and draining attacks

For the *Transparency Project* PoC, the most salient attack vectors identified relate to "spamming" or "draining" attacks by external actors. This vulnerability takes multiple forms:

Draining of funding pools intended for vendor transaction fees

– As indicated above, the software system can include predesignated pools or accounts designed to hold cryptocurrency to help pre-fund, or potentially reimburse, vendor transaction fees. If the public is also able to access these accounts, which may occur to avoid requirements around identifying participating vendors, then actors outside the system may also access these accounts and steal the funds, draining the balance.

Draining attacks related to public comments

– If the system runs on a permissionless blockchain, it may require a pre-funded account of cryptocurrency employed behind-the-scenes to fund the transaction fees associated with anonymous comments submitted by external actors (citizens, journalists, etc.). An attacker can continuously make high volumes of comments, draining this fund so that no one else can make comments until the fund is replenished. To help address this risk, the public could be required to pay the transaction fees themselves, as they are likely nominal – less than the cost of a postage stamp. However, this may dramatically reduce participation.

– If the system runs on a permissioned blockchain without use of transaction fees, then public comments would be costless in terms of fees, but there may be other downsides to this approach. While there is no longer a fund of cryptocurrency to drain, the public could continuously post comments, crowding out legitimate comments or perhaps overwhelming the network.

Spamming attacks related to public comments

– Whether the e-procurement system is implemented in a permissioned- or permissionless-consensus blockchain system, spamming attacks from public comments and complaints sent to the system could interrupt or delay the procurement process. As designed, the *Transparency Project* PoC would allow anyone around the world to leave public comments and raise red flags in case of noted irregularities. This feature is critical to the anti-corruption potential of the project, as public monitoring supports oversight efforts and incentivizes vendors and tenderers to act more responsibly. However, because these commenters must also remain anonymous for user protection, they generally cannot be screened, identified or blocked.

– Negative consequences associated with these types of attacks include instigating unfounded investigatory diversions or falsely accusing honest vendors or tenderers of fraudulent or corrupt behaviour. Moreover, such comments could be preserved in the blockchain records permanently. The tenderer should not necessarily postpone or deny awarding contracts based on comments alone, in order to prevent undue interruptions to the contracting process that can arise from these issues. Rather, the contract could be awarded to the winning tenderer accompanied by investigation by third-party institutions.

One could imagine risks related to high volumes of comment spamming from "bots". By automating elements of the procurement process and opening processes to public comment, the prevalence of malfeasance and fraud in procurement auctions may unintentionally increase. Rather than reducing corruption, the system may end up enabling malicious or corrupt actors around the world to more easily interfere with and harm procurement processes.

It may be possible to establish safeguards and rules within the system to protect against this behaviour by, for instance, automatically blacklisting the IP addresses of commenters who are spamming the system. This is unlikely to be effective, as sophisticated attackers can simply resume the activity from new computers (new IP addresses), through IP address rotation or by employing virtual private networks (VPNs) to circumvent the blacklist. Of course, it may also be difficult to distinguish between someone genuinely making multiple comments to flag suspicious activity and someone attempting to thwart a competitive procurement auction. Moreover, granting a party the power to blacklist a commenter can introduce the human discretion that enables corrupt activity. Additional approaches could involve requiring accounts for commenters, but this could jeopardize their anonymity as well as the goal of truly public and open commenting. Institutions interested in developing blockchain-based procurement systems should ask themselves what measures can be taken to counter the increased "attack surface" and risks that a global and public procurement system enables.

4. Key features from blockchain technology: System integrity – permanent record-keeping, censorship resistance and transparent software code

Perhaps the strongest advantage of blockchain technology in anti-corruption and government transparency use cases is the technology's ability to support nearly fully permanent and tamper-evident record-keeping. For public procurement, the tender offer and modifications, the bidding process and associated documentation, the bid scoring and evaluation, and the public comments can be fully and permanently recorded, saved and auditable in the blockchain system.

Further, tender offer and vendor bid offer documents, and public comments, can be submitted to a general-purpose and publicly available hash function whose output serves as a "fingerprint" or "timestamp" of the document or comments' contents at that time. The hash output can be stored on a blockchain ledger in a manner that is very difficult to remove. While hash functions are by no means dependent on the use of blockchain technology, their records on blockchain ledgers are indisputable and challenging to remove.

A simplified blockchain solution for public procurement could only focus on recording documents and comments prone to corruption or removal in tamper-resistant and permanent manners using hash-function outputs recorded on distributed ledgers, without additional functionalities. This could serve as a complementary component within non-blockchain-based e-procurement systems.

Of course, it is possible for non-blockchain-based databases to employ cryptography, such as public-key cryptography, to also create record-keeping systems where document or record modifications would be difficult and evident. However, in such systems, it is impossible (or at least very difficult) to guarantee that a central administrator has not deleted records entirely – a function that is possible with blockchain technology and is very relevant to public-procurement process integrity and transparency. Further, compared with centralized database systems, blockchain technology also entails a very high degree of embedded public transaction transparency and censorship resistance, where transactions (e.g. a vendor's bid offer submission) are visible in real time, difficult to block, and undeniably sent to and from a specific address that can be known to be associated with particular actors (e.g. a vendor).

One qualification to this capability should be mentioned: it is likely possible for a centralized vendor registration process, as is used in most contexts, to knowingly block certain vendors from registering to participate in tender processes in the first place. As indicated earlier in this report, vendor registration constitutes a centralized process at risk for corruption, and solutions should account for this risk where possible.

The hash output, or "fingerprint", becomes a tamper-proof reference of the documents' contents at the specific point in time when the hash was taken. At any later point, the documents can be resubmitted to the same hash function by any parties to verify whether the outputs are consistent. If the outputs are inconsistent, it indicates edits or changes to the documents have been made.

Table 5 lists the most important benefits of employing blockchain technology, rather than traditional database architectures, for e-procurement. These benefits are maximized in a public, permissionless blockchain.

TABLE 5: **Key benefits of blockchain-based e-procurement**
Public, permissionless blockchain
Permanent and irrefutable records (of public comments, tender offer and bidding documents and their "hashed" timestamped records, tenderer scoring and evaluation decisions, etc.)
Censorship-resistant vendor bids (note: the vendor registration process may entail censorship depending on its design)
Transparent and tamper-evident procurement process software code

Trade-offs: Towards a hybrid or permissioned-consensus blockchain system?

Based on the project's findings, a blockchain-based e-procurement system that employs a public, permissionless-consensus blockchain system, such as Ethereum, maximizes benefits related to data permanence and censorship resistance but also faces critical challenges with respect to scalability and vendor anonymity. The scalability challenge is intractable at present but may be minimized with future technological developments in next-generation protocols or "layer 2" solutions. The vendor anonymity challenge is more addressable today through constructions such as zk-SNARKs, although these presently require non-trivial engineering and computational costs.

A solution based on a public, permissionless-consensus blockchain protocol also faces vulnerabilities related to draining, spamming and vendor defamation. Because this type of protocol requires the use of cryptocurrency for transaction fees, it may also raise legal roadblocks in jurisdictions where the use of cryptocurrency by public institutions or in public processes is prohibited or unregulated.

Table 6 lists the key challenges or limitations associated with a public, permissionless blockchain-based e-procurement system.

TABLE 6: **Challenges and limitations of blockchain-based e-procurement**
Public, permissionless blockchain
Anonymity
Funding of vendor accounts for requisite transaction fees (to submit bid offers)
Sending of bid offers from vendor accounts
Cryptocurrency use in transaction fees
Potential legal or regulatory roadblocks
Potential need to train vendors and tenderers on cryptocurrency use
Spamming and draining attacks
Crowding out of legitimate comments with numerous fraudulent or low-value comments
Permanent defamation of honest vendors (in comments)
System interruptions from draining attacks on transaction-fee funding accounts meant to fund vendor bids and public comments
Other
Low transaction scalability
Difficulty in implementing protocol-level governance decisions or security fixes

As a result of the above challenges, policy-makers stand to benefit from exploring a permissioned-consensus blockchain system (also called a "public, permissioned blockchain") or a hybrid system. In a permissioned-consensus blockchain, predesignated or invited node operators would perform transaction verification and consensus. Transaction fees would not be required. Hybrid solutions employ both permissioned and permissionless base-layer protocols, where each performs certain activities. For instance, the Ethereum blockchain could be used to record hash records of bid and tender offers in a permanent and highly secure manner, while most other operations like bid submission and evaluation decisioning could occur on the permissioned blockchain protocol.

A permissioned-consensus blockchain implementation appears to resolve six challenges associated with permissionless blockchains:

- By removing the need for transaction fees, it would eliminate the threat to vendor anonymity that would otherwise occur when funding pseudonymous vendor accounts (e.g. "hidden ID" accounts in the project) that are used to submit bid offers.
- By removing the need for transaction fees, regulatory roadblocks or constraints associated with the use of cryptocurrency are bypassed.
- By removing the need for transaction fees, the need to train tenderers and vendors on the purchase and use of cryptocurrency is avoided.
- By removing the need for transaction fees, the system is no longer vulnerable to account draining attacks meant to provide transaction-fee funding to vendors or to public comments.
- The system can achieve markedly more transaction scalability, necessary for a widely used e-procurement system. It should be noted that the number of nodes and specific consensus algorithm greatly affect scalability.
- The system can implement software fixes, upgrades or governance decisions much more easily as a smaller group of nodes is needed to implement the changes (e.g. it can immediately pause all activity given a threat or unforeseen activity or make an important software update).

Some downsides remain in permissioned blockchain implementations. For instance, only one of the two vendor anonymity challenges can be easily resolved: vendor bid offers may still need to be encrypted and submitted from a one-time pseudonymous account, because accounts that bid offers are sent from would remain visible (the use of obfuscating cryptography techniques notwithstanding). Challenges related to undue comment spamming also remain or are augmented. As comments from the public may be completely costless (a back-end transaction fee is not required for their submission in a permissioned network), external actors could indefinitely post comments in a manner that generates denial-of-service attacks and significantly slows or thwarts the system.[87]

Related to permanent defamation of honest vendors through fraudulent comments made by the external actors, a permissioned blockchain network's ability to change such records depends on the consensus algorithm and mutually agreed upon network governance rules. It may be desirable to encode the ability for nodes to vote to take measures on such comments. On the other hand, this could introduce discretion and opportunities for further corruption (e.g. deleting legitimate comments about risky or fraudulent behaviour made against vendors).

Key downside to a permissioned blockchain implementation: Permissioned-consensus networks arguably entail weaker record-keeping security and data integrity. As there are fewer nodes in the system, the nodes conducting transaction verification can more easily collude to block transactions or change information stored in the system. In brief, they are more vulnerable to double-spend attacks and other attacks that can affect transactions and records.

The decentralization of blockchain technology, and its accompanying benefits of data security, integrity and honest disclosure, is greatest in public, permissionless blockchain networks. However, permissioned-consensus blockchain systems still provide more decentralization than the status quo. The designation of a highly trustworthy set of validating nodes can also greatly improve security and procedural integrity, creating a system that is more resistant to collusion or corruption.

Key benefit of the hybrid system: The use of a hybrid system offers many of the same benefits as a permissioned-only system, but with one substantial improvement: It can likely achieve greater data integrity and permanence, near or equal that of a permissionless-consensus protocol (as hash outputs and other records are stored on a permissionless-consensus protocol). This capability depends on the nature of implementation.

What benefits and limitations remain in both permissioned and hybrid systems? A hybrid blockchain configuration can provide many of the same benefits as a public, permissioned system. For instance, scalability is achievable as most operations and transactions occur over permissioned network. Further, most governance decisions and security fixes can relate to operations conducted over the permissioned network, which would be generally easy to implement.

The challenge of fraudulent or low-value comment spamming or crowding out remains with hybrid networks. The risk of undue permanent defamation of honest vendors through fraudulent comments also remains. The ability to remedy such defamation comments depends on the permissioned blockchain's consensus algorithm and mutually agreed upon governance rules.

The left-hand column of Table 7 lists the challenges and limitations associated with a public, permissionless blockchain network such as Ethereum. The table adds the relative or incremental benefits or downsides of a public, permissioned blockchain (permissioned-consensus) and a hybrid blockchain system. Note that the specific implementation and design of blockchain networks vary, and the information below is generalized.

TABLE 7: **Relative challenges and limitations of blockchain-based e-procurement**

Public, permissionless blockchain	Public, permissioned blockchain	Hybrid: public, permissionless and permissioned blockchains	Considerations
Anonymity			
Funding of vendor accounts for requisite transaction fees (to submit bid offers)	Issue addressed	Issue may be addressed, depending on design and implementation	*Modern cryptography techniques (i.e. zero-knowledge proofs) can likely address the issue*
Sending of bid offers from vendor accounts	Issue may be addressed, depending on design and implementation	Issue may be addressed, depending on design and implementation	*Cryptographic primitives like commitment schemes, or constructions such as zero-knowledge proofs, can address the issue*
Cryptocurrency use in transaction fees			
Potential legal or regulatory roadblocks	Issue addressed	Issue may be addressed, depending on design and implementation	
Potential need to train vendors and tenderers on cryptocurrency use	Issue addressed	Issue may be addressed, depending on design and implementation	
Spamming and draining attacks			
Crowding out of legitimate comments with numerous fraudulent or low-value comments	Issue potentially heightened	Issue potentially heightened	
Permanent defamation of honest vendors (in comments)	Issue depends on the consensus algorithm and network governance rules	Issue depends on the consensus algorithms and network governance rules	*The ability to affect comments can introduce more corruption and must be well-designed*
System interruptions from draining attacks on transaction-fee funding accounts meant to fund vendor bids and public comments	Issue addressed	Issue addressed	
Other			
Low transaction scalability	Issue addressed	Issue addressed (for transactions on the permissioned blockchain)	*Issue depends on node count and consensus algorithm* *Technology innovation may address issue in future (i.e. "layer 2" or next-generation protocols such as Ethereum 2.0)*
Difficulty in implementing protocol-level governance decisions or security fixes	Issue addressed	Issue addressed (for issues on the permissioned blockchain)	
[Of special note]	Introduces weaker record-keeping and process security and integrity	Can potentially provide strong record-keeping and process security and integrity, depending on implementation	*Designation of highly trustworthy nodes in permissioned-consensus system can help maintain record and process integrity*

Node governance in permissioned-consensus or hybrid systems

A key challenge in implementing a permissioned-consensus blockchain, whether standing alone or as part of a hybrid implementation, is the identification of suitable and trustworthy agents to serve as nodes for transaction verification. Depending on the network's consensus algorithm, it will need to have a certain portion of trustworthy and non-corruptible nodes to preserve data record integrity. The system engineers and developers must justify and design the blockchain network such that it minimizes node collusion to the greatest extent possible (e.g. if a group of bidders collude to overtake transaction verification and alter new records).

Under a blockchain system with permissioned transaction validation, the following high-level questions must be carefully considered and resolved, taking into account the blockchain network and consensus algorithm:

Organization

- How many nodes should constitute the network?
    - How many nodes should be in the country where the auctions are conducted as opposed to transnational or overseas nodes?
- Who should serve as nodes?
    - Do the relevant parties have biases or stand to benefit from certain outcomes in the procurement process?
    - Can these parties invest the funds necessary to set up and run the nodes securely and adequately?
    - How diverse should the nodes be in terms of interests, sector, management and other factors?
- What are the incentives for the participants to maintain their nodes and participate in the system?
    - How could these incentives change over time?
- In designing the protocol, should any nodes be given special permissioning or powers, such as transaction approval "veto" powers?

Security and maintenance

- Who is responsible for the set-up and maintenance costs of the nodes, and for maintaining the security of the nodes?

Governance

- How will decisions related to network security and software updates be made?
- How can assurance be gained that one or more actors cannot unduly pressure the rest of the participants to adopt certain unfair governance practices or to interrupt the network?
- Which rules and governance processes can be developed to incentivize honest behaviour and reduce the likelihood of collusion over time?
- To what extent could nodes collude with each other or the tenderer, or receive bribes from vendors submitting bids to the system?
- How would dishonest node behaviour be identified, and what would be the repercussion for the node operator(s)?
- When and how should records (e.g. defamatory comments made maliciously or fraudulently against honest vendors) be altered, corrected or removed from the database?

Conclusion

The case for blockchain-based e-procurement
Overall, blockchain-based e-procurement systems provide unique benefits related to procedural transparency, permanent record-keeping and honest disclosure. However, blockchain technology also presents certain challenges, most notably scalability and vendor anonymity. A blockchain-based solution is also unable to reduce corruption risk in certain human activities that can occur outside the electronic procurement system, most notably bribery or collusion among vendors or between vendors and tenderers. Given the challenges and limitations, the case for a blockchain-based e-procurement system is ambiguous and depends most on the specific country context, institutional goals and the technology's design, configuration and implementation.

Blockchain permissioning and technology innovations
The use of a fully permissionless blockchain network capitalizes on blockchain's unmatched data permanence and censorship-resistant capabilities. That said, current challenges with scalability and anonymity highlight potential advantages of permissioned or hybrid systems, at least in the context of today's technological limitations. Yet these solutions may weaken the unique capabilities that made a blockchain solution so compelling in the first place.

Specifically, permissioned blockchain networks generally have weaker data permanence and censorship resistance – both of which are particularly valuable in the anti-corruption context. Nonetheless, a permissioned network that carefully identifies highly trustworthy nodes to operate the system may achieve high levels of security and integrity while addressing the scalability and anonymity downsides of permissionless networks. Such a system would need to be very strategically designed and designated. Hybrid blockchains possibly achieve the best of both worlds by marrying the scalability of a permissioned blockchain network with the greater integrity of a permissionless network. While this middle-ground solution would not achieve the full degree of scalability or decentralization of fully permissioned or permissionless networks, respectively, it potentially presents the strongest case in the anti-corruption context.

Innovations in the blockchain technology ecosystem may also address scalability and anonymity challenges in the future, strengthening the case for permissionless blockchains and reducing the incremental value of permissioned blockchains. The challenge of maintaining vendor anonymity may be addressable with modern techniques such as ZKP cryptography. This technology is available today although it entails non-trivial computational and engineering costs. These costs are likely to decline in the future. The challenge of scalability may be addressed in the future with "layer 2" blockchain scalability solutions such as "state channels" for Ethereum, or with second-generation base-layer protocols such as Ethereum 2.0.

Ultimately, the challenges and limitations associated with the public procurement use case highlight the most fundamental trade-offs and limitations associated with permissioned versus permissionless blockchain networks – a critical question for most institutions and enterprises considering blockchain deployment. The challenges also highlight the importance of relevant innovations under way in the realms of cryptography and scalability. Policy-makers and project owners must evaluate present-day trade-offs in the context of their specific social, political and environmental circumstances, while monitoring technological innovations that might alter the balance towards one blockchain solution over another.

Appendices

Further research: Modifications and developments for a second-generation project

This section communicates additional areas of functionality expansion that could be pursued in a second-generation project. The intent is to provide inspiration for institutions considering a blockchain-based e-procurement system. These approaches are merely suggestions and should be considered along with the unique project goals, constraints and requirements.

1. **Direct contract monitoring**: In the wake of the COVID-19 pandemic, many governments around the world began emergency direct contracting for the procurement of necessary health services and supplies. A new e-procurement system could develop greater functionality for direct contracting, where the motivation, contract values, vendor(s) and other records are documented in real time so they are subject to public scrutiny during or after the award process.

2. **"Upvoting" and weighting red flags and comments**: Developing functionality for public commenters to support red flags and comments made by others can at once help oversight and investigatory institutions prioritize risky activities and also help reduce congestion in the number of comments in the system. Citizens, journalists and other stakeholders can provide support to comments they agree with or that capture their views rather than adding new comments.

3. **Vendor- and contract-performance tracking**: The vendor selection process would be greatly benefited by an accurate tracking of vendor performance in similar contracts that it has won in the past. One approach could be for a vendor's blockchain-based account to hold records of past contract performance. Awarding positive bonus points for strong contract performance in prior auctions may be more politically feasible than deducting points from past poor performance. This concept is further illustrated in the annex of the Model Request for Proposal document. Other approaches could involve live reporting of contract performance.[88]

4. **Fraud detection and analytics**: Leveraging the open database of procurement data available in a public blockchain-based e-procurement system, it could be possible to conduct advanced analytics to identify correlations or patterns in the procurement auctions that point to corrupt activity. For instance, a tenderer may systematically favour certain vendors in scoring and awarding contracts. Along this vein, it could be advantageous to develop functionalities to query and search data from past tender auctions conducted on the blockchain system to more easily detect anomalies and fraudulent behaviour.

   Another example could be investigating and uncovering familial records to identify first-, second- or third-degree family relationships between vendors and tenderers or among vendors. Databases documenting beneficial corporate ownership could also be leveraged. At scale, analytics can potentially help identify patterns or clues that can indicate fraud or conflicts of interest more easily than analysing procurement records by hand.

5. **Additional encoded red-flag functionalities**: Additional automatic alerts and programmatically triggered red flags can be encoded in the system to help meet its goals. Georgia's Tender Monitor e-procurement website provides a relevant list of additional examples of high-risk activity for which automatic red flags can be developed.[89]

6. **Obfuscating cryptography techniques**: A second-generation project can experiment with applying ZKP constructions such as zk-SNARKs, privacy-focused cryptocurrencies or other cryptography innovations to mask the identity of vendors who submit bid offers in blockchain-based systems. In effect, the successful implementation of these technologies could fully address vendor anonymity challenges, as sender (vendor account) and receiver (tender offer smart contract) information could be masked. This would support vendor anonymity in both permissionless and permissioned blockchain implementations.

7. **Contract payment tracking**: The solution described in this report does not include functionality for tracking the payments made to vendors or their subcontractors. A second-generation solution could extend the scope of the system to track payments from the tenderer to the vendor after the contract is awarded and when the vendor is implementing the contract. Payments transparency and traceability could also help reduce the risk of fraudulent practices with respect to subcontractors.

8. **Fully automated evaluation process**: Much of the vendor selection phase of an e-procurement process can be automated, which can both improve the speed and efficiency of the bid offer evaluation and reduce discretion in the evaluation that may foster corrupt activity. At least two issues must be considered if developing a heavily or fully automated evaluation and scoring process:

   – The tenderer should still manually review and confirm the scoring decisions and calculations conducted by the e-procurement system for fault or errors. In some areas, it may be prudent and appropriate to interject and modify scoring and calculation results. Human discretion, while sometimes enabling corrupt activity, can also correct for digital processes that stimulate corruption.

- The software logic for bid evaluation and scoring should also be publicly viewable in order to verify that the correct code is running in a manner that does not favour or bias outcomes. Regardless of the degree of automatic scoring and evaluation, special care should be taken so that potential biases and abuses are not encoded in the system. Blockchain technology can support transparency in the computational logic for bid scoring.

9. **Full software client account and data recovery via a 12-keyword mnemonic feature**: For vendors, a complete backup of the data for their software client can be saved in the form of a ZIP file encrypted with the vendor account's private key and uploaded to a decentralized file storage system (e.g. IPFS). If the software client is deleted from a computer, or there is a need to install the client in another computer, the 12-keyword mnemonic phrase can recover this ZIP file, decrypt it and restore the client's record to its original state as of the latest backup.

10. **Governance and incentive mechanisms to promote honest behaviour**: The opportunity exists to explore how incentive mechanisms, perhaps employing cryptocurrency, could be used to change behaviours when using the software. For example, these mechanisms could potentially encourage journalists, citizens or even analytics providers to review records for risky behaviour.

11. **Open-source and digital public good**: A next-generation solution could be developed in an open-source manner with public disclosure of and input to the software code. The solution could be strengthened through wide scrutiny and input, as well as more easily adapted to suit the requirements of individual jurisdictions where it could be implemented.

Supplementary Research Report

Additional information supporting the project can be found in the *Supplementary Research Report*. This addendum includes the following components:

- Measuring success: Evaluating a blockchain-based e-procurement solution
- Colombian public-school meal programme background information
- Regulatory framework for the use of blockchain and cryptocurrency in Colombia
- Existing efforts to curb procurement corruption
- Anti-corruption and government transparency: Additional use cases for blockchain
- Further reading

Contributors

Lead authors

Ashley Lannquist, Project Lead, Blockchain and Digital Currency, World Economic Forum LLC

Rachel Davidson Raycraft, University of Virginia School of Law, USA

Technical design and project management

Mauricio Tovar Gutiérrez, Angel Rendón, Diego Mazo, Anni Piraguata, Luis de la Peña, Ronald Sarmiento, Julián Jiménez, Paula Andrea Valencia and **Pablo Enrique Rodríguez**, ViveLab Bogotá and InTIColombia Research Group, National University of Colombia

Sebastian Banescu, Senior Research Engineer, Quantstamp, USA

Max Fang, Adjunct Professor, University of California, Berkeley, USA

Project and report contributors

Danny Brown Wolf, Head, Partnerships and Strategy, Orbs, USA

Santiago de la Cadena Becerra, Human Development Specialist and Economist, World Bank Group, Washington DC

Rafael Carvalho de Fassio, Lead Counsel of Public Procurement, Attorney General's Office of the State of São Paulo, Brazil

David Lehrer, Chief Executive Officer, Conatix, United Kingdom

Lawrence Lundy-Bryan, Partner and Head of Research, Outlier Ventures, United Kingdom

Leonardo Passos, Senior Research Engineer, Quantstamp, Brazil

Carlos Rodriguez Cabrera, Head, Strategy and Business Development, Open Canarias, Spain

Howard Wu, Cryptography Researcher, University of California, Berkeley, USA

World Economic Forum

Erdi Ay, World Economic Forum LLC Fellow, Yapi Kredi, Turkey

Sumedha Deshmukh, Platform Curator, Blockchain and Digital Currency, World Economic Forum LLC

Justine Humenansky, World Economic Forum LLC Research Fellow

Ximena Maria Lombana, World Economic Forum LLC Fellow, Office of the Inspector General of Colombia

Sheila Warren, Head of Blockchain, Digital Currency and Data Policy; Member of the Executive Committee, World Economic Forum LLC

World Economic Forum Centre for the Fourth Industrial Revolution Affiliate Centre in Colombia
Clementina Giraldo, María Isabel Vélez, Sara Ramírez and **Carolina Valencia**

The authors and the World Economic Forum would additionally like to thank the following contributors and organizations for their support in this project:

Fernando Carillo, Diego Arisi, Victor Muñoz, Delia Ferreira Rubio, Silvia Constain, José Manuel Restrepo, Carlos Santiso, Tomicah Tillemann, Olga Mack, Cathy Barrera, Stephanie Hurder, Stela Mocan, Caroline Malcolm, Justin Andrews Valentine, Andrew Ballinger, Vasyl Zadvornyy, Zvika Krieger, Katja Bechtel, Ernesto Dal Bó, Dolly Montoya, Federico Gutiérrez, Carlos Andres Agudelo Mora, Jorge Eliecer Amargo Mendoza, Mauricio Ulate, Georg Neumann, Natalya Thakur, Ayman Omar, Fabienne Stassen and Jean-Philippe Stanway

The Inter-American Development Bank, the Office of the Inspector General of Colombia (*Procuraduría General de Colombia*), the Office of the Mayor of Medellín, the Ministry of Education of Colombia, Transparencia por Colombia, Colombia Compra Eficiente, the Chamber of Commerce of Santander, the Comptroller General of Colombia, the National Association of Entrepreneurs of Colombia (*Asociación Nacional de Empresarios de Colombia* – ANDI), FENALCO Bucaramanga, Revista Semana, Red PaPaz and the Institute of Family Welfare (*Instituto Colombiano de Bienestar Familiar*)

References

Basel Institute on Governance, *Learning Review: Transparency International's Integrity Pacts for Public Procurement*, Transparency International, December 2015, https://www.transparency.org/files/content/ouraccountability/2015_IntegrityPacts_LearningReview_EN.pdf.

Boehm, Frédéric and Juanita Olaya, "Corruption in public contracting auctions: The role of transparency in bidding processes", *Annals of Public and Cooperative Economics*, vol. 77, no. 4, 2006, pp. 431-452, https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1467-8292.2006.00314.x.

de Michele, Roberto, Joan Prats and Isaias Losada Revol, "Effects of Corruption on Public-Private Partnership Contracts: Consequences of a Zero-tolerance Approach", Discussion Paper no. IDB-DP-625, Inter-American Development Bank, 2018, https://publications.iadb.org/publications/english/document/Effects_of_Corruption_on_Public%E2%80%93Private_Partnership_Contracts_Consequences_of_a_Zero-tolerance_Approach_en_en.pdf.

Dinero, "Estudio revela que los contratos adjudicados con soborno aumentan su costo final 71%", 8 November 2019, https://www.dinero.com/economia/articulo/estudio-revela-que-los-contratos-adjudicados-con-soborno-aumentan-su-costo-final-71/278808?fbclid=IwAR2E9HSbc-rujqwC-oaSYb2jBFcXwXOGOoKlzl6XDi4dMXnbFmzQZSK9LY4.

El Tiempo, "Una pechuga de pollo a $40.000 y huevo a $900, en sobrecostos del PAE", 21 November 2017, https://www.eltiempo.com/justicia/investigacion/sobrecostos-en-programa-de-alimentacion-escolar-en-colombia-153590.

El Tiempo, "Casi $18 billones se habrían perdido por corrupción", 18 September 2019, https://www.eltiempo.com/justicia/delitos/dinero-que-se-habria-perdido-por-corrupcion-en-colombia-informe-de-transparencia-por-colombia-413654.

Gutiérrez, Hernan, "Colombia: Overview of corruption and anti-corruption", U4 Expert Answer, Anti-Corruption Resource Centre, Transparency International, 15 March 2013, https://knowledgehub.transparency.org/helpdesk/colombia-overview-of-corruption-and-anti-corruption.

Gutman, Jeffery and Vinay Bhargava, *A Decade of Helping Civil Society Fight Corruption in the Philippines: Results and Lessons*, Partnership for Transparency Fund (PTF) Asia, 2015, https://ptfund.org/wp-content/uploads/2018/07/A-Decade-of-Helping-Civil-Society-Fight-Corruption-in-the-Philippines.pdf.

Huter, Mathias and Giorgi Chanturia, "OpenGov Voices: How Georgia is handling procurement transparency", Sunlight Foundation, 16 January 2014, https://sunlightfoundation.com/2014/01/16/opengov-voices-how-georgia-is-handling-procurement-transparency/.

Kahn, Theodore, Alejandro Baron and Juan Cruz Vieyra, *Digital Technologies for Transparency in Public Investment: New Tools to Empower Citizens and Governments*, Inter-American Development Bank, 2018, https://publications.iadb.org/en/digital-technologies-transparency-public-investment-new-tools-empower-citizens-and-governments.

Landell-Mills, Pierre, *Citizens Against Corruption: Report from the Front Line,* Partnership for Transparency Fund (PTF), 2013, https://www.ptfund.org/publication_page/citizens-against-corruption-report-from-the-frontline/.

Luijken, Thomas and Maira Martini, "Anti-corruption helpdesk: The role of technology in reducing corruption in public procurement", Transparency International, 28 August 2014, https://www.transparency.org/files/content/corruptionqas/The_role_of_technology_in_reducing_corruption_in_public_procurement_2014.pdf.

Martini, Maira, "Anti-corruption helpdesk: Public procurement law and corruption", Transparency International, 12 June 2015, https://knowledgehub.transparency.org/assets/uploads/helpdesk/Public_procurement_law_and_corruption_2015.pdf.

OECD, *Preventing Corruption in Public Procurement,* 2016, http://www.oecd.org/gov/ethics/Corruption-Public-Procurement-Brochure.pdf.

OECD, *Reforming Public Procurement: Progress in Implementing the 2015 OECD Recommendation*, 2019, https://www.oecd-ilibrary.org/sites/1de41738-en/index.html?itemId=/content/publication/1de41738-en.

Open Contracting Data Standard (OCDS), "OCDS for the Agreement on Government Procurement", n.d., https://standard.open-contracting.org/profiles/gpa/master/en/.

Open Contracting Partnership (OCP), "Emergency procurement for COVID-19: Buying fast, smart, and open", n.d., https://www.open-contracting.org/what-is-open-contracting/covid19/.

Open Government Partnership, *Anti-Corruption Initiatives: Open Contracting*, Open Government Partnership Global Report, 2019, https://www.opengovpartnership.org/wp-content/uploads/2019/05/Global-Report_Open-Contract.pdf.

Reuters, "Brazil's Odebrecht files for bankruptcy protection after years of graft probes", 17 June 2019, https://www.reuters.com/article/us-odebrecht-bankruptcy/brazils-odebrecht-files-for-bankruptcy-protection-after-years-of-graft-probes-idUSKCN1TI2QM.

Transparency International, *Curbing corruption in public procurement: A practical guide*, 2014, https://www.transparency.org/whatwedo/publication/curbing_corruption_in_public_procurement_a_practical_guide.

Transparency International, "Corruption Perceptions Index 2019", 2019, https://www.transparency.org/cpi2019.

Transparency International, "Contrataciones públicas en estados de emergencia: Contratações públicas em situações de emergência", 2020, https://www.transparency.org/files/application/flash/COVID_19_Public_procurement_Latin_America_ES_PT.pdf.

Transparency International Georgia, *Simplified procurement – Corruption Risks in Non-Competitive Government Contracts*, 2013, https://www.transparency.ge/sites/default/files/post_attachments/Simplified%20procurement%20-%20Eng%20–%20Dec%209.pdf.

Transparencia Mexicana, *A New Role for Citizens in Public Procurement*, Citizens&Markets, 2012, https://www.scribd.com/document/110224943/Citizens-and-Markets-A-New-Role-for-Citizens-in-Public-Procurement.

Trevisani, Paulo, Samantha Pearson and Luciana Magalhaes, "Odebrecht Bankruptcy to Hurt Brazilian State-Owned Banks", *The Wall Street Journal*, 18 June 2019, https://www.wsj.com/articles/odebrecht-bankruptcy-to-hurt-brazilian-state-owned-banks-11560873874.

United Nations Commission on International Trade Law (UNCITRAL), *UNCITRAL Model Law on Public Procurement*, United Nations Publication, 2014, https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/2011-model-law-on-public-procurement-e.pdf.

United Nations Office on Drugs and Crime (UNODC), "United Nations Convention against Corruption" (UNCAC), General Assembly resolution 58/4 of 31 October 2003, U. N. T. S. Doc. A/58/422, https://www.unodc.org/documents/treaties/UNCAC/Publications/Convention/08-50026_E.pdf.

United Nations Office on Drugs and Crime (UNODC), *Good practices in ensuring compliance with article 9 of the United Nations Convention against Corruption: Guidebook on anti-corruption in public procurement and the management of public finances*, 2013, https://www.unodc.org/documents/corruption/Publications/2013/Guidebook_on_anti-corruption_in_public_procurement_and_the_management_of_public_finances.pdf.

United States Department of Justice, U.S. Attorney's Office Southern District of Florida, "Former National Director of Anti-Corruption in Colombia Extradited to the United States to Face Wire Fraud and Money Laundering Charges Related to Foreign Bribery", 18 May 2018, https://www.justice.gov/usao-sdfl/pr/former-national-director-anti-corruption-colombia-extradited-united-states-face-wire.

Wells, Jill, "Corruption and collusion in construction: A view from the industry", in T. Søreide and A. Williams (Eds), *Corruption, grabbing and development,* Edward Elgar Publishing, 2014, pp. 23-34, https://pdfs.semanticscholar.org/79e9/1919263a91d3eb4fba3e82b996c93007b991.pdf.

World Bank, *Corruption and Technology in Public Procurement*, 2007, http://documents.worldbank.org/curated/en/946171468151791174/pdf/481060WP0Corru10Box338882B01PUBLIC1.pdf.

World Bank, *Benchmarking Public Procurement 2017: Assessing public procurement regulatory systems in 180 economies*, International Bank for Reconstruction and Development, 2016, http://documents.worldbank.org/curated/en/121001523554026106/Benchmarking-Public-Procurement-2017-Assessing-Public-Procurement-Regulatory-Systems-in-180-Economies.pdf.

World Trade Organization (WTO), "Revised Agreement on Government Procurement", 2014, https://www.wto.org/english/docs_e/legal_e/rev-gpr-94_01_e.htm.

Endnotes

1. El Tiempo, 2017 [in Spanish].
2. Electronic procurement ("e-procurement") refers to "the use of any internet-based inter-organizational information system that automates and integrates any parts of the procurement process in order to improve efficiency, transparency and accountability in the wider public sector" (Basel Institute on Governance, 2015, p. 67). Further discussion is included in the *Supplementary Research Report*.
3. OECD, 2016; Transparency International, 2014.
4. OECD, 2016; UNODC, 2013; World Bank, 2016.
5. Martini, 2015; World Bank, 2007.
6. OECD, 2016; Transparency International, 2014.
7. OECD, 2016; UNODC, 2013.
8. World Bank, 2007.
9. OECD, 2016; World Bank, 2007.
10. Kahn, Baron and Vieyra, 2018; World Bank, 2007.
11. Transparency International, 2014.
12. Transparency International Georgia, 2013; World Bank, 2007.
13. Wells, 2014.
14. OECD, 2016; Transparency International, 2014; World Bank, 2007.
15. Transparency International, 2014, p. 4.
16. Reuters, 2019.
17. de Michele, Prats and Losada Revol, 2018; Trevisani, Pearson and Magalhaes, 2019.
18. Trevisani, Pearson and Magalhaes, 2019.
19. Landell-Mills, 2013.
20. Kahn, Baron and Vieyra, 2018; OECD, 2016; Transparency International, 2014; UNODC, 2003; UNCITRAL, 2014; World Bank, 2007.
21. El Tiempo, 2019 [in Spanish].
22. Transparency International, 2019.
23. El Tiempo, 2017 [in Spanish].
24. Gutiérrez, 2013.
25. US Department of Justice, 2018.

26. The proof-of-concept was intended for pilot deployment in a public-school meal programme procurement auction in Medellín, Colombia, in 2020. Owing to integration and regulatory hurdles, the solution has not yet been piloted. At the time of publication, the tentative expectation is that the programme will be piloted towards the end of the 2020 calendar year. These challenges are discussed further on page 28.

27. Colombian procurement regulation follows several laws and decrees, such as Law 80 of 1993 and Law 1150 of 2007 (Law 80, Official Gazette No. 41,094 of 28 October 1993 available at http://www.secretariasenado.gov.co/senado/basedoc/ley_0080_1993.html, and Law 1150, Official Gazette No. 46,691 of 16 July 2007 available at http://www.secretariasenado.gov.co/senado/basedoc/ley_1150_2007.html).

28. IPFS, or the InterPlanetary File System, is a protocol for sharing and storing files and documents in a distributed manner. It was developed by Juan Benet and Protocol Labs and is compatible for use in the Ethereum network (see the IPFS website at https://ipfs.io/).

29. A hash function is a mathematical algorithm that maps or converts data from an arbitrary size into a bit-string output of fixed size. Within a public procurement process, tender and bidding documents, as well as public comments about the bidding process, can all be submitted to hash functions. The hash output can be stored in a secure database, including a blockchain database. If the same input (tender or bidding documents, etc.) is then submitted to the same hash function, it should produce the exact same output. If the hash output is different, it indicates a change to the document has occurred.

30. In distributed ledger technology, "nodes" consist of the individual computers or servers that take input and perform functions in the system. Typically, nodes route information and perform transaction verification in the network according to a specific distributed consensus algorithm. They may earn transaction fees and/or, depending on the network, a "block reward" or "mining reward" for transaction verification.

31. Transaction fees are denominated in the blockchain network's native cryptocurrency (e.g. ether for Ethereum). Their price is determined by multiple factors including network congestion and activity, and the cryptocurrency's market price. In many networks such as Ethereum, the computational effort required to perform smart-contract operations also affects the transaction cost.

32. Colombia's procurement agency, Colombia Compra Eficiente, currently publishes all of its public contracting data in the OCDS (see https://www.colombiacompra.gov.co/transparencia/gestion-documental/datos-abiertos).

33. OECD, 2016; Luijken and Martini, 2014.

34. In the procurement context, blacklists are used to sanction vendors recently found to have acted corruptly. States should enumerate necessary reforms that would allow a company to be removed from a blacklist. Whitelists, by contrast, are used to promote the participation of companies who conduct business with integrity. Such lists can also be used to incentivize participation in non-compulsory anti-corruption measures, such as the Integrity Pacts discussed in this report (see Basel Institute on Governance, 2015).

35. Martini, 2015; Transparencia Mexicana, 2012.

36. Dinero, 2019 [in Spanish]; Transparencia Mexicana, 2012.

37. Luijken and Martini, 2014.

38. The Slovakian e-procurement website can be found at https://tender.sme.sk/en/. The Georgian website can be found at http://tendermonitor.ge/en.

39. Huter and Chanturia, 2014; Transparencia Mexicana, 2012.

40. Transparencia Mexicana, 2012.

41. Boehm and Olaya, 2006; Luijken and Martini, 2014; World Bank, 2016.

42. Open Government Partnership, 2019.

43. World Bank, 2016.

44. OECD, 2016.

45. Landell-Mills, 2013; Martini, 2015; Transparencia Mexicana, 2012.

46. Basel Institute on Governance, 2015.

47. Martini, 2015.

48. Transparencia Mexicana, 2012.

49. Martini, 2015.

50. Open Contracting Partnership (OCP), n.d.

51. The Colombia Compra Eficiente website lists contracts awarded in response to the COVID-19 emergency on the country's existing e-procurement systems, SECOP I and SECOP II [in Spanish]: https://app.powerbi.com/view?r=eyJrIjoiMGQ5YTkwNzItZWVhMC00ZTgxLWJmYzgtODE1NWE0ZGZmNDVkIiwidCI6IjdiMDkwNDFlLTI0NTEtNDlkMC04Y2IxLTc5ZDVlM2Q4YzFiZSIsImMiOjR9.

52. Transparency International, 2020 [in Portuguese].

53. Transparency International, Public procurement, Press release, "Coronavirus sparks high risk of corruption across Latin America", 26 March 2020, https://www.transparency.org/news/pressrelease/coronavirus_sparks_high_risk_of_corruption_across_latin_america.

54. Luijken and Martini, 2014.

55. Martini, 2015.

56. Transparency International, 2014.

57. In blockchain networks, oracles are mechanisms for external ("off-chain") data from various sources to connect with the blockchain-based system (i.e. to connect with the smart contracts operating a decentralized application). Oracles can serve several purposes, such as connecting the application to external pricing or other data feeds that inform or trigger smart-contract activities and responses in the application. For public procurement, an oracle could potentially link a tender offer smart contract directly with external benchmark pricing data.

58. Landell-Mills, 2013.

59. Basel Institute on Governance, 2015.

60. This can include community-based organizations, policy research centres, professional associations, faith-based groups and the independent media (see Landell-Mills, 2013).

61. Gutman and Bhargava, 2015; Landell-Mills, 2013; Transparencia Mexicana, 2012.

62. Landell-Mills, 2013.

63. Gutman and Bhargava, 2015; Transparencia Mexicana, 2012.

64. For more information on Transparency International's Integrity Pacts, see https://www.transparency.org/whatwedo/tools/integrity_pacts/5.

65. Boehm and Olaya, 2006; Gutman and Bhargava, 2015; Landell-Mills, 2013; Transparencia Mexicana, 2012.

66. Boehm and Olaya, 2006; Transparencia Mexicana, 2012.

67. Basel Institute on Governance, 2015; Gutman and Bhargava, 2015; Landell-Mills, 2013.

68. Boehm and Olaya, 2006; Gutman and Bhargava, 2015; Landell-Mills, 2013; Transparencia Mexicana, 2012.

69. Basel Institute on Governance, 2015; Landell-Mills, 2013.

70. Transparencia Mexicana, 2012.

71. Gutman and Bhargava, 2015; Landell-Mills, 2013.

72. Gutman and Bhargava, 2015.

73. Basel Institute on Governance, 2015.

74. Gutman and Bhargava, 2015, p. 29.

75. Gutman and Bhargava, 2015.

76. OECD, 2019.

77. Basel Institute on Governance, 2015.

78. For example, if a common practice in the region is for vendors to submit abnormally low-price bid offers to win auctions, often followed by contract non-completion or post-award cost additions, then reasonable minimum price floors and benchmarks could be made a system requirement. Automatic red flags can also occur where bid offers are below a certain percentage of benchmarks or the auction's average bid offer value.

79. In Colombia, the use of SECOP in public procurement processes is mandatory, in accordance with the provisions of Law 1150 of 2007, Decree 1082 of 2015 and External Circular No. 21 of 22 February 2017 of the national public procurement agency, Colombia Compra Eficiente. Additional information can be found in "Circular Externa Unica de Colombia Compra Eficiente" (https://www.colombiacompra.gov.co/sites/cce_public/files/cce_circulares/cce_circular_unica.pdf) and "Circular Externa No. 1 de 2019" (https://www.colombiacompra.gov.co/sites/cce_public/files/cce_circulares/circular_externa_no._1_de_2019.pdf).

80. A cryptographic primitive is a low-level cryptographic algorithm that is well tested and frequently used in cryptographic operations for computer systems.

81. A zk-SNARK (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge) is a prominent "zero-knowledge proof" construction where one party can prove possession of certain information without revealing the information, and without interaction between itself and the verifier. Zk-SNARKs can be used to enable payments where the sender, receiver and transaction information are masked. Currently, Ethereum supports the verification of zk-SNARK proofs natively. Depending on the application, a zk-SNARK verifier could be deployed directly in a smart contract on Ethereum or through a third-party technology provider offering services for zk-SNARK proofs on Ethereum. The computational cost of running zk-SNARKs must be considered, as it is generally non-trivial today. That said, research on zk-SNARKs continues to progress and experts believe the computational costs and limits will decrease in the next few years.

82. As one approach with the Gas Station Network, vendors could potentially deploy their bid smart contracts via their "hidden IDs" using a "BidSmartContractCreator-SmartContract". Such a smart contract would be pre-funded, but it would be prone to draining attacks by malicious participants. Furthermore, additional avenues for exploration can be explored that, like the Gas Station Network, employ relayer-based systems. In these schemes, the vendor signs transactions with its public or private key but sends transactions off-chain to a private "relayer" who submits the transaction. This relayer could be a digital tool with a pre-funded cryptocurrency account that automatically submits transactions sent to it to a specific address. This tool could be a central point of failure and subject to draining attacks depending on implementation.

83. The AZTEC Protocol aims to develop a high-speed and cost-effective system for implementing zk-SNARKs in the public, permissionless Ethereum blockchain. It currently enables transactions to be sent with masked amounts. The roadmap includes the obfuscation of sender and receiver information (see Walton-Pocock, Thomas, "Aztec: Fast Privacy with ZK2 Rollup", 27 March 2020 at https://medium.com/aztec-protocol/aztec-fast-privacy-with-zk%C2%B2-rollup-7c742f45457).

84. "ZEXE" is an example of a decentralized private computation protocol that could allow for ZKPs to be more easily implementable by developers and could entail lower computational cost and run-time in the future (see Bowe, Sean, et al., "ZEXE: Enabling Decentralized Private Computation", 21 February 2019, at https://eprint.iacr.org/2018/962.pdf).

85. Universal SNARKs improve upon a key challenge of today's zk-SNARKs: the need for a new, potentially costly, cryptographic set-up for each new instantiation of zk-SNARKs, even when the same or similar programme has already been developed elsewhere. Universal SNARKs instead allow for only one cryptographic set-up for the SNARKs that is employable for all programmes using the same instantiation. "Marlin" is the name of a new universal SNARK protocol with high efficiency (see Chiesa, Alessandro, et al., "Marlin: Preprocessing zkSNARKs with Universal and Updatable SRS [structured reference string]", 1 January 2020, at https://eprint.iacr.org/2019/1047.pdf). As an example with public procurement, an initial institution that develops a blockchain-based e-procurement system where universal SNARKs are employed to mask vendor identities could perform the one-time system set-up that is then enjoyed by all other institutions or governments that seek to run similar systems, rather than each institution needing to set up the zk-SNARK itself.

86. A zk-STARK (Zero-Knowledge Transparent Non-Interactive Argument of Knowledge) is another new, prominent form of ZKP construction that enables a transparent set-up scheme with faster verification time. Zk-STARKs also boast quantum-computer resistance or post-quantum security. Today, zk-STARKs are not yet efficient for general programmes; however, experts believe they may become more efficient and deployable in the intermediate and longer-term horizons (see Ben-Sasson, Eli, et al., "Scalable, transparent, and post-quantum secure computational integrity", 6 March 2018, at https://eprint.iacr.org/2018/046.pdf).

87. In a denial-of-service attack, a perpetrator seeks to make a network resource unavailable to intended users through disruption of the system's host or web servers. In this example, perpetrators can flood the system with comments, using up its capacity to accept honest comments or operate properly.

88. For a public-school meal programme, for instance, after the contracts are awarded to specific vendors, teachers and parents could potentially take photos of meals and submit them to the vendor management database or institution, or to an independent institution investigating allegations of corruption (the Inspector General's Office in Colombia).

89. Transparency International Georgia, Tender Monitor, "Risk Flags", 2 March 2020, https://tendermonitor.ge/en/flags.

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744

contact@weforum.org
www.weforum.org