IS THERE A ROLE FOR BLOCKCHAIN FOR ENHANCING PUBLIC PROCUREMENT INTEGRITY?

CHAN YANG
yc.annabelle@gmail.com

Key words: Corruption, Public Procurement, Blockchain

Abstract

Public procurement is one of the government activities most prone to corruption. Every year, 20-25% of national procurement budgets are estimated to have been lost to corruption. Governments worldwide have started to leverage new technologies to improve procurement integrity. Among these, blockchain is expected to hold strong promise against corruption and inefficiencies. This concept paper will discuss three potential applications of blockchain for public procurement integrity, their benefits and limitations: (i) integrate blockchain to track full-cycle procurement workflows to prevent record tampering; (ii) create interoperable supplier profiles across fragmented e-procurement systems to reduce asymmetry of information in purchasing or pre-tender assessment; and (iii) “decentralise” bid evaluation to disincentivise bribery and biased decision-making. This paper does not prescribe whether blockchain should be used for enhancing procurement integrity, rather it focuses on illustrating the circumstances that may make it desirable. Further feasibility studies are required for specific use cases in order to determine the acceptable level of trade-offs brought by the technology.

The opinions expressed and arguments employed herein are solely those of the author and do not necessarily reflect the official views of the OECD or of its member countries.

This document and any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

This paper was submitted as part of a competitive call for papers on integrity and anti-corruption in the context of the 2019 OECD Global Anti-Corruption & Integrity Forum.

The author is grateful for the insights shared by the Mexican National Digital Strategy team with its implementing partners and many practitioners from both the public and private fields.

1. Problem statement

At 13% of GDP in OECD countries and 1/3 of overall government expenditures, public procurement is one of the government activities most prone to corruption. Every year, governments worldwide spend USD 9.5 trillion procuring everything from roads, dams, to hospitals and printers. OECD estimates that corruption drains 20-25% of national public procurement budgets, which limits competition, hurts development and public welfare, and damages trust in government (OECD, 2016).

Governments around the world have started to implement new technologies to improve integrity, efficiency and value-for-money of their procurement processes. Among these, blockchain is expected to hold strong promise against corruption and inefficiencies. While blockchain exists in a large number of variants, it can be considered as a log of sequential entries shared and written by a group of non-trusting parties, without a central administrator (Greenspan, 2016). Its essential attributes of immutability and disintermediation seem to make it a natural ally for anti-corruption. The programmable and self-executing smart contract is also hailed as a powerful weapon for trust and efficiency, by limiting scope of human errors and discretion in decision-making.

While these potentials seem promising to increase efficiency and transparency in public procurement, their effects on eliminating corruption are less clear-cut, notably for the sophisticated forms such as conflict of interest. Since 2017, several governments have turned to blockchain to improve their e-procurement systems: Japan primarily aims to bolster information security; the United States focus on cost-saving and value-for-money by automating pricing analysis (HHS) and contract review (GSA); Mexico (State of Jalisco) seeks to increase transparency and curb corruption; and South Korea (Seoul) looks to improve bid evaluation.

This concept paper will discuss three potential applications of blockchain for reducing corruption in public procurement, and their respective benefits and limitations: apply blockchain to track full-cycle procurement workflows (section 2); reduce asymmetry of information in pre-tender assessment (section 3); and "decentralise" bid evaluation (section 4). It does not prescribe whether blockchain should be used by public procurement professionals, as this should be assessed against clearly identified problems and needs on a case-by-case basis and that choice of technology be decided after a systemic review of the trade-offs entailed. Instead, this paper will focus on illustrating the circumstances that may make blockchain desirable (section 5), with the following questions in mind:

- When may there be a role for blockchain for public procurement integrity?
- What integrity risks can blockchain tackle, and for which may it yield advantages over regular e-procurement systems?
- Do these gains outweigh the costs and efforts required for implementing blockchain?

2. Track full-cycle procurement workflows, notably records of decisions and documentation

Various forms of integrity risks exist along the public procurement cycle, related to the contracting body, the suppliers, their potential connections and the procurement tool itself. Empirical research over the last 15 years has established numerous integrity and efficiency gains of e-procurement system (OECD, 2016). Many of these benefits are, however, contingent upon the measures taken to ensure security and transparency of the e-procurement system, without which it would present numerous lacunae and pitfalls facing insider frauds and outsider attacks. Table 1 gives an example of such flaws based on evidence from India, Indonesia and Mexico (Kohli, 2010, 2012; S N Huda et al, 2017; OECD, 2018). As procurement information is usually stored in a centralised server, it is inherently more vulnerable to tampering and attacks. Audit trails at both application and operating system (OS) levels can still be fudgeable, and OS-level reports are rather complex and impractical to analyse. If a malware is planted at the kernel[1] level, there may not even be any audit trail (Kohli, 2010).

Table 1. Integrity risks due to flaws in e-procurement systems

Insider frauds	• Server/network bandwidth limitation or misuse of firewalls to restrict bid submissions • Document changes[2] by system admins, usually with the server access log erased • Subjective assessment or fraud during bid evaluation • Leakage of confidential information regarding system security framework
Outsider attacks	• Hacking aimed to strike down whole system or impede tender process[3] • Intrusion or infiltration causing change/removal of files or change of server's time • Sabotage by dissatisfied ex-system admins[4]
Other system design flaws	• Bid sealing/encryption for guaranteed confidentiality is missing or flawed • Functionality of digital signatures[5] is flawed or not supported • Other technical or procedural gaps[6] undermining procurement activities' traceability

Source: Author's elaboration based on Kohli (2010, 2012); S N Huda et al (2017); OECD (2018).

It is possible that most of these risks could be minimised if the e-procurement systems are adequately parameterised to be security-robust and compliance-driven[7]. This will require strong IT capacity and a

[1] A computer programme that is the core of a computer's operating system, connecting the application software to the hardware of a computer, and is designed to be as "untouchable" as possible.

[2] These could include document deletions at different steps of the procurement cycle; modification of bid submission deadline, bid proposals or evaluation results to favour particular suppliers; modification of tender specifications and evaluation criteria after call for bid; alternation of contract versions or significant contract variations after contract award.

[3] Often enabled by inadequate firewall protection or unsecure data communication protocol.

[4] Possibly due to absence of a clear and standard operating procedure for mutation or resignation process of system admins.

[5] A digitally signed electronic file, for instance by a bidder during online bidding, establishes the authentication, non-repudiation and integrity of the signed data (Kohli, 2012).

[6] E.g. when e-procurement system is disconnected to planning/budgeting systems, when contracts are awarded directly or through closed tender, or when necessary checkpoints (e.g. upload complete information or required documents) are missing before procurement processes can progress to the next stage (OECD, 2018).

[7] A sound security framework could build on: two-factor authentication, digital signatures to ensure non-repudiation, database-level bid encryption, online antivirus scanning, audit trail of every activity, privilege-based user access, time stamping, firewall

culture of integrity in data management. While many advanced OECD economies have a relatively strong tradition of robust information system management, e-procurement systems in less developed regions can be exposed to more design flaws and manipulations[8]. Typically, when unauthorised data manipulation is commonly observed, an e-procurement system operated by a central entity (or its service provider) may inspire little public trust.

Blockchain, if adequately designed, may find its merits in this scenario. Figure 1 illustrates how a blockchain typically works. Its most obvious strength lies in its **security** in ensuring integrity of the procurement system, in four ways: making system corruption technically quasi-impossible (tamper proof), economically costly (tamper resistant), easily and immediately detectable (tamper evident), and irrefutably attributable to specific entities (BitFury, 2016). This is underpinned by blockchain's three architectural characteristics:

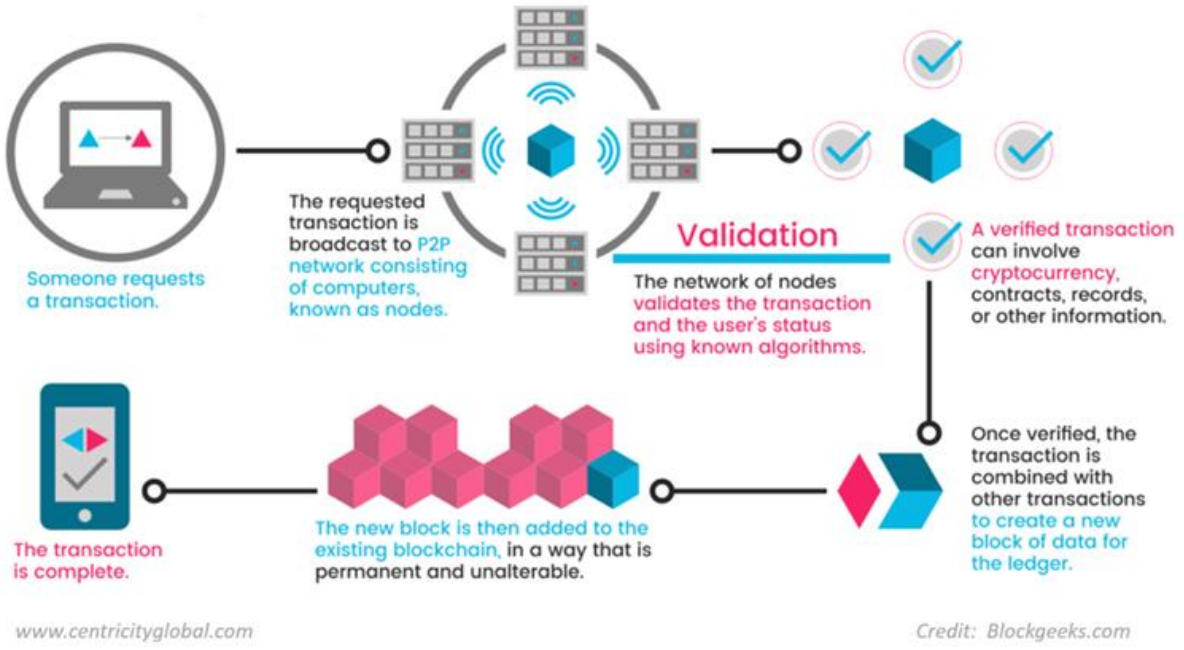
- Blockchain is a hashed chain of blocks containing records of transactions[9]. Each block is connected to all those before and after through a hash pointer. Changing an entry retroactively requires calculating a new hash for the block it's in as well as every subsequent block, and this has to be done before any new blocks are added to the chain.
- Plus, it is a continually updated and synchronised peer-to-peer network. Data record cannot be changed from one single computer as it is stored in a distributed ledger. Depending on the ruling protocol and scale of the network, massive computing power may be required to access every node and alter them all at once.
- On-chain record integrity is secured through advanced cryptography (asymmetric encryption and hashing). Each record contains information on the provenance, timestamp and list of transactions. If a record is altered, its signature and hash will become invalid so the network can quickly identify the source of incident.

screening system access, access control, intrusion detection (network and host), regular data back-up and disaster recovery site (Bikshapathi and Raghuveer, 2010).

[8] For instance, security breaches causing illegal payments were found in Kenya's e-procurement system in 2015, which is a customised version of Oracle's E-Business Suite (Standard Digital, 2015).

[9] Large amounts of data are uniquely represented by a numeric hash value that is used to identify records but not reconstruct data inside the file. In public procurement, participants of the e-procurement system will continuously publish new transactions, to be added by validators to the blockchain.

Figure 1. How a blockchain works



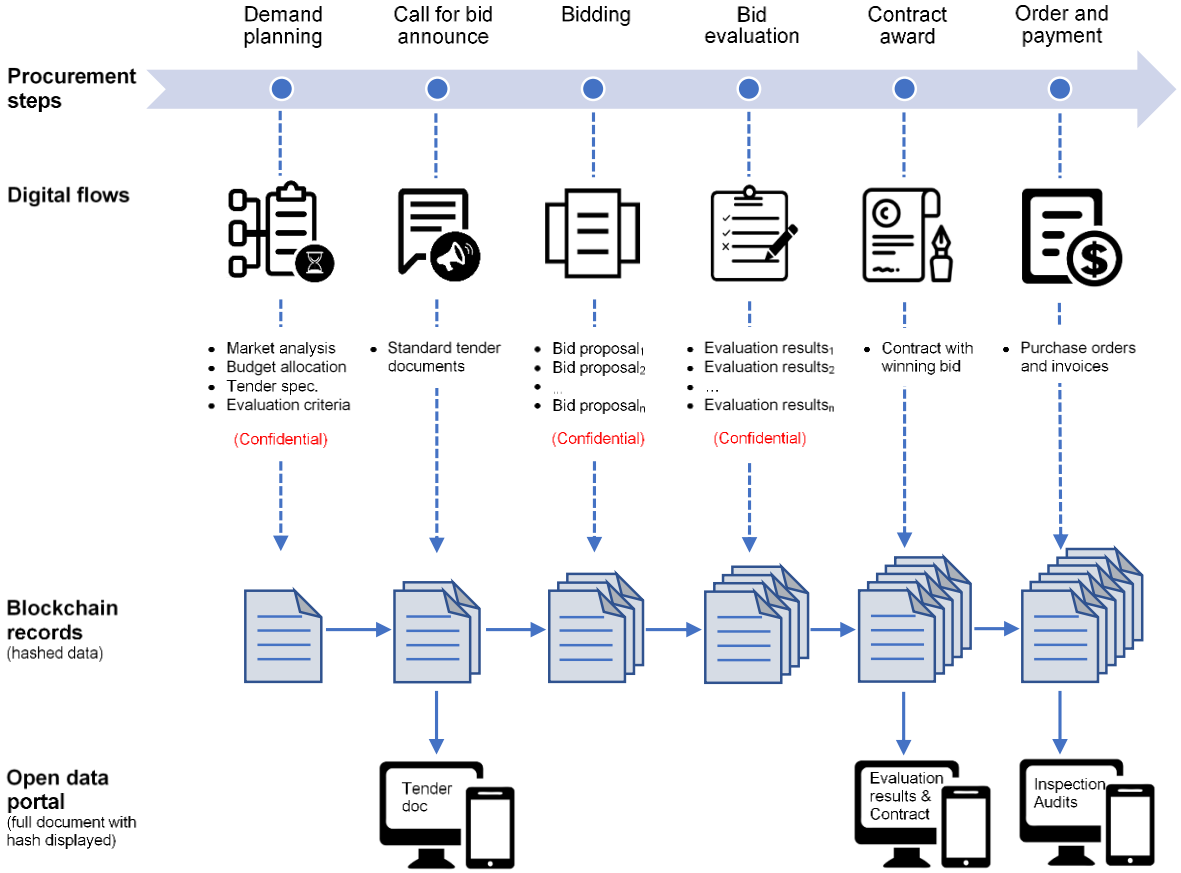
Applying blockchain to track procurement workflows (notably decisions and documentation[10]) would strengthen audit trails immutability and provide real-time traceability of irregularities (Figure 2). As the system will enable all parties involved to view each step simultaneously, auditing can be conducted in real-time targeting high-risk areas, unlike currently when a misconduct often surfaces only after an insider leak or an *ex post* audit. It would also be faster and easier to pin down accountability when red flags are raised as each participant can now be identified with a unique identity. Furthermore, blockchain helps overcome obstacles of coordination between government agencies[11] in a more secure and efficient way, which could minimise delays and duplicative processes in the approval of procurement needs and the final contract. Auditing may also gain more credibility as data used for analysis are now protected against unauthorised access and manipulation, although the completeness[12] of data matters as much as its integrity for drawing high-quality insights. Compliance with document upload processes and open data practices would therefore be the prerequisite.

[10] E.g. At six points along the procurement cycle: (i) needs assessment and tender documents submitted by demand originator for budget planning/approval; (ii) tender documents (including technical specifications and evaluation criteria) released by procuring authority upon call for bid; (iii) bid proposals submitted by bidders; (iv) bid evaluation results; (v) awarded contract; and (vi) invoices and orders.

[11] E.g. Finance and budget, central procurement authority, tax, competition/anti-trust, anti-corruption audit.

[12] Completeness can be understood as: (i) the blockchain system should capture as much procurement expenditure as possible, including when a contract is awarded directly or through closed tender; (ii) it should be connected to planning and contract management software; (iii) necessary documents should be uploaded.

Figure 2. Tracking procurement workflows on blockchain



Source: Author's elaboration.

However, one needs be cautious that there is no absolute immutability on blockchain. Its level depends on how blockchain is configured, including the openness to participate in the network[13], the consensus protocol[14] used to validate transactions, the concentration level of validators and how they are chosen[15]. Key determinants appear to be who should be validators and what are the incentive-penalty mechanisms to ensure their integrity, all while keeping in mind the effect on the trade-offs between security (against attacks), scalability (throughput and latency), and decentralisation (against censorship and collusion). Depending on the classification criteria used, there could be four types of blockchain, categorised by the level of anonymity of validators and the level of trust in validators (Figure 3; Kravchenko, 2016). Typically, a permissionless public chain is fully open to anonymous validators as long as they have enough computing resources to validate transactions. Such a structure offers the

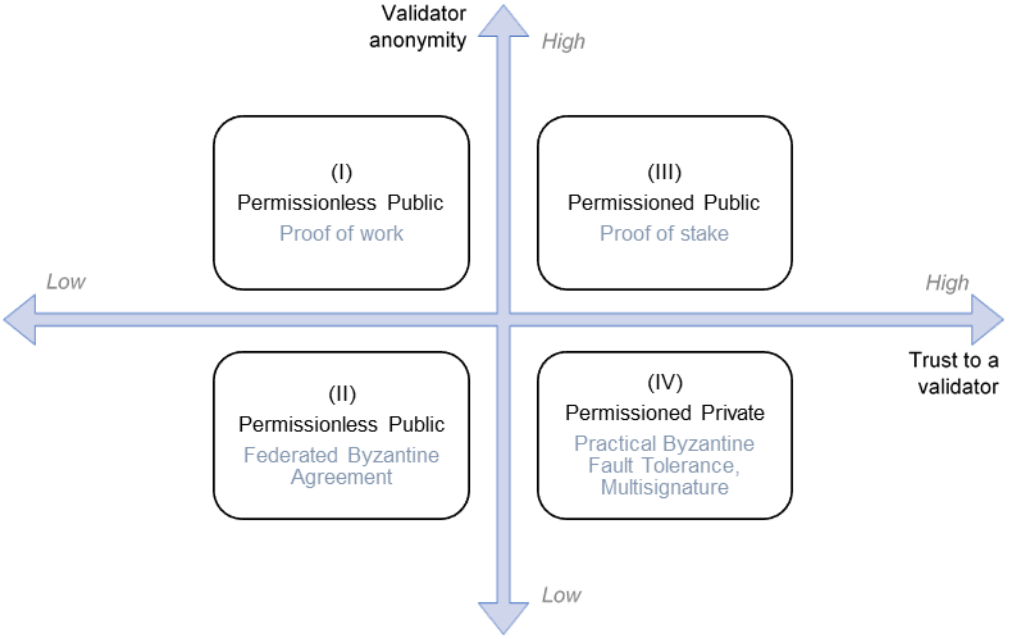
[13] Which determines who can access the network and do what. Generally, permissioned chains are often designed for the needs of governments and large corporates to offer stronger confidentiality and control.

[14] The algorithmic process by which a network of nodes confirms the record of previously verified transactions, and by which it verifies pending transactions and maintains the shared ledger in sync.

[15] Validator of a transaction should ideally never be either of the transacting parties to preserve integrity of the record. The risk of collusion (i.e. transaction censorship or biased conflict resolution) is typically lower when validators are chosen randomly or controlled by different stakeholders.

strongest security/immutability and is suitable for fully anonymous system out of government control, but is slow to process transactions or grow in scale as the proof of work consensus algorithms is highly inefficient and resource-intensive. Opposite to this is permissioned private chains, which, for sake of confidentiality and control, only choose trusted validators that are bound by certain off-chain relationships. They seem applicable for public sector use cases and more efficient and scalable due to fast consensus algorithms, albeit at the expense of immutability as the latter really depends on agreement between validators (Kravchenko, 2016).

Figure 3. Typology of blockchain



Source: Kravchenko (2016).

While permissioned private chain may appear most fit for public procurement as it accelerates the verification processes all while allowing the government to retain control over the network, its power in deterring “system fraud” would be undermined if corruption stems from the inside and there is not a large enough set of validators to preserve blockchain record integrity, or when the validating mechanisms and incentives/penalties are not effectively designed to counter malicious behaviour or collusion. Each node is running on a computer system controlled by a certain entity or person, and blockchain alone cannot force them to behave ethically. Records can be rewritten If the majority of its participants wish to adopt new rules or if someone (e.g. nation-state) has enough resources to do so (Greenspan, 2017). As of today, a solution that combines all desired features may not yet be achieved without significant trade-offs. Governments desiring to implement blockchain for enhancing procurement integrity face the challenge of selecting the right consensus protocol and system architecture, all while understanding the pros and cons each approach has to offer (Andoni et al., 2019).

Furthermore, applying blockchain to track procurement workflows is simply adding a layer of validation[16] before an entry can be recorded permanently into the system. While the record integrity can be trusted, the data may not, nor does it replace physical trust between two entities in reality – in particular when their iterations happen off-chain. Although blockchain enhances digital trust in the procurement process and makes low-level corruption more easily detectable, if used alone, it could not prevent sophisticated forms of corruption from happening, such as:

- Public officials leaking sensitive information or designing biased tender specifications to favour certain bidders (conflict of interest, favouritism);
- Bidders bribing public officials and offsetting with substandard materials (supported with fake invoice) or poor-quality goods/services (in collusion with public officials);
- Bidders colluding to rig the bid;
- Other obscure forms such as secrecy of beneficial ownership.

Poor practices can be easily perpetuated through e-procurement system – blockchain-enabled or not, as it cannot ensure that processes are open, fair and appropriate to the needs of each procurement, nor replace the need to ensure that participants are well-trained and act with integrity (OECD, 2018).

3. Create interoperable supplier profiles across fragmented e-procurement systems

Public trust in government tends to be higher in countries with sound governance of rule of law and robust checks and balances. Their procurement systems have largely been digitalised and regarded more resilient against manipulation. There may be less need to use blockchain to authenticate the digital integrity of the procurement process. Nonetheless, public procurement in these countries is equally vulnerable to corruption, which takes increasingly sophisticated forms of conflict of interest, beneficial ownership secrecy or collusive bidding. When designing specifications for complex projects, problems of asymmetry of information would arise, creating room for dependence on external consultants that may lead to unfair practices when the consultants are not subject to proper obligations of confidentiality or restriction. Moreover, most countries, particularly large economies such as the United States, China, India and Australia, operate multiple e-procurement systems that may not be shared by all government agencies, let alone those at sub-national level (Somasundaram and Hasan, 2018)[17]. There could be massive gains of money and time if data on supplier profiles and contract records could be shared among various entities and synchronised in a secure and efficient way.

There may be a role for blockchain in this scenario, with its immediate potential to boost productivity and value-for-money – which may inadvertently contribute to limiting opportunities of corruption that arise from asymmetry of information (e.g. supplier pricing opacity) or reliance on third-parties during

[16] Validators cannot verify anything substantive (i.e. content inside the document) except math (i.e. procedural elements such as the authenticity of digital signatures, state of accounts and data feeds).

[17] Under siloed systems, a supplier may not be distinctly identified across these systems if he is not required to authenticate his identity vis-à-vis pre-established national registry database (Somasundaram and Hasan, 2018).

pre-tender planning. This can be achieved by either adding blockchain as a layer that references all the contracting data of the government – starting with one department before propagating to all public institutions[18]; or generating a unique identity (linked to previous work record) for each supplier that can be authenticated across fragmented e-procurement systems, in a real-time and decentralised manner[19]. Both approaches enable data-level interoperability without disrupting existing business processes. The following cost-efficiency and integrity gains are expected (Table 2).

Table 2. Linking supplier and contract data across e-procurement systems

Direct cost-efficiency gains	Indirect integrity gains

• De-silo supplier registries across departments, ministries and jurisdictions, to enable secure & efficient information-sharing
• When combined with AI analytics[20]:
  ○ Gain real-time visibility into supplier pricing and contract conditions, for faster and more accurate budget planning and specifications assessment[21]
  ○ Increase buyer's negotiating power through demand aggregation, notably for small-value frequent purchases[22]
• Provide finer insights into supplier qualifications based on immutable work experience records[23]
	• Limit discretion available to public officials to unduly influence demand/preferences or inflate budget needs
	• Expose and minimise unfair pricing practices by suppliers (e.g. territory-based arbitrage)
	• To the extent possible, reduce asymmetry of information and reliance on third-parties[24] for determining tender specifications and evaluation criteria, including for projects where there is an internal lack of know-how/expertise
	• Provide central supervisory body with aggregate visibility over fragmented e-procurement systems for monitoring compliance performance

Source: Author's elaboration based on experiments of the US HHS and ADB.

It is important to note that many benefits cited above are the results of combining blockchain-layer data with AI analytics: the former guarantees data integrity and traceability, while the latter extracting patterns to help shape more adequate procurement assessment. The use of blockchain would only be meaningful if it adds onto an existing quality and complete database. Moreover, while this approach may lower corruption risks related to dishonest middlemen or vendor pricing opacity, it has to rely on

[18] Blockchain will hold a timestamped record of data stored in a standardised format, see approach of the US Department of Health and Human Services.

[19] See approach proposed for ADB, to deploy blockchain across worldwide governments' e-procurement systems, with each participating as network nodes to access supplier databases (incl. qualifications, contract awards history and current workload) in different jurisdictions.

[20] In HHS' experience, robotic process automation and machine learning (ML) are added to the blockchain-layer data, with ML used for data cleansing after extraction from legacy contract systems. Natural language processing is used to analyse the terms, conditions and pricing in the contracts.

[21] Pricing estimates would be notably harder facing complex procurements that involve high-level technology.

[22] HHS is projected to save USD 720 million minimum by identifying the lowest price possible for bulk purchases of everyday items (Federal News Network, 2018).

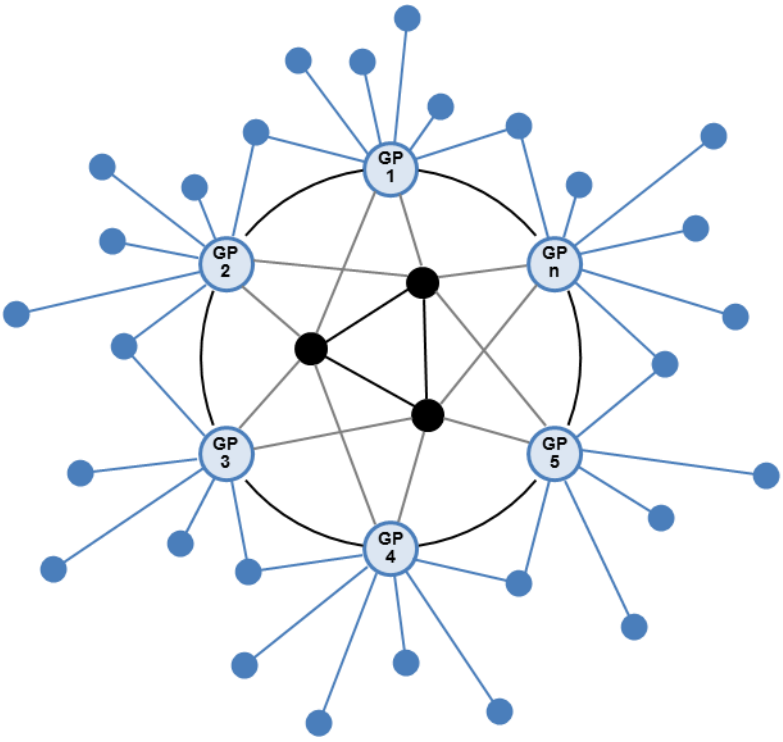
[23] This may include past awarded contracts, current workload, work experience certificates and contract performance evaluation/rating.

[24] Including agents, middlemen, consultants, who may not necessarily be most competent or act with integrity.

the integrity of public officials to uphold an ethical code of conduct. When there are "rats" inside the system, only properly-conducted auditing and public scrutiny may help expose wrongdoing.

Take a step even further, the advantage of having a network of interlinked e-procurement systems could be considered for empowering a central supervisor (through read-only nodes) to monitor cross-jurisdiction/multi-level spending and enforce local accountability, without being perceived as visibly intrusive while also alleviating administrative burdens in the reporting process (Figure 4).

Figure 4. "Policing" a network of e-procurement systems



Notes: Black nodes represent higher-level supervisory bodies (e.g. anti-trust, anti-corruption, budget and finance); large light-blue nodes represent parallel e-government procurement systems that are in operation; small dark-blue nodes represent suppliers.

Source: Author's elaboration.

Three potential scenarios may be considered; their political desirability and regulatory feasibility require further deliberation:

- A central/federal government (e.g. China, India[25], Mexico) monitoring provincial/state operation of their e-procurement systems, covering procurement financed by national budget;

[25] India has over 50 e-procurement systems in operation.

- A supranational institution (e.g. European Commission) seeking to gain granular view of procurement practices by its member states, thereby enforcing best practice compliance and level playing field;
- A multilateral development bank (e.g. World Bank) reviewing procurement practices by recipient countries, or as an effort to facilitate international bidding with easily cross-authenticated documentation.

4. Decentralise bid evaluation process in a secure way

During bid evaluation, bidders' technical capability is usually evaluated by the technical department, before their business capability and financial position are assessed separately by the procuring entity. It is not uncommon that a peer review of the evaluation results may be required, and that third-parties be invited to evaluate bids when complex goods/works requirements are involved. A certain level of competence and professionalism is required for making objective assessment. While this capacity may seem standard in many OECD economies, it could be a challenge in lower income countries, where the state's institutional capacity is weaker and that competent procurement staff are scarce. When corruption stems from the inside, the risk of biased bid evaluation would also increase.

It is conceivable to open up bid reviews to a much wider range of experts, whereby limit biased or dishonest selection. Such thinking is based on two assumptions:

- Assumption 1: "decentralising" bid evaluation by bringing in a greater number of competent evaluators would favour more objective assessment, compensate capacity shortage and mitigate insider fraud;
- Assumption 2: as the number of co-decision-makers increases, the "crooked" bidder would be disincentivised to pay bribes as the total price can go up quickly.

When such a pool of experts is not yet available, they could be selected against pre-identified criteria, e.g. absence of conflict of interest (no publicly-disclosed affiliation with any of the suppliers); recognised authority (e.g. certificates and other qualification credentials); ideally disconnected from each other to avoid collusive behaviour; positive integrity verification response; and proper level of security clearance, if applicable. Their identity shall be kept anonymous until announcement of the winning bid, and their public addresses (registered on blockchain) altered each time they are brought onboard a review panel. Bids shall be reviewed anonymously, and all proprietary information in the tender should be disguised, so that one may well evaluate responses to a tender that is beyond his jurisdiction (city, province, country) without the least knowledge of it. Evaluation results will be stored on a blockchain for record-keeping, and disclosed for public scrutiny upon contract award. They should also be considered in selecting the contractor, and explanations should be given in event of large discrepancies between the final selected bidder and the dominant view among experts. The pool of evaluators should also enlarge progressively.

This approach presents several challenges and limitations:

- First, while it provides better assurance that the first-best bidder gets selected, it does not offer redress when tender specifications and evaluation criteria are drafted to favour one particular supplier, or when collusive bid-rigging occurs.
- Second, selection of the "right" experts (i.e. competent and law-abiding) is a crucial step; there may be a risk of capture by interest groups or criteria may be inadequately defined if the procuring entity lacks the capacity/knowledge. Nevertheless, if the project is financed by international donors, the latter may play a role in defining expert selection criteria or recommending names of qualified experts.
- Third, although anonymity of evaluators and bidders can in principle prevent them from establishing contact during bid review, it does not prevent dishonest evaluators from proactively seeking bribe. This risk may be bigger at the start when the pool of qualified evaluators is small, but would likely decrease when it enlarges. Adequate "carrots and sticks" are key to incentivise experts to participate and behave honestly in the evaluation.
- Fourth, barriers to adoption may be high as the state must agree to distribute their decision-making power to potentially non-state even foreign actors. It might be easier in transition countries having experienced recent regime change, which need a quick shortcut to establish credibility in their governance or attract funding from international donors and investors.

5. Is there a strong case to use blockchain for public procurement integrity?

Sections 2-4 have shown blockchain's potential – if adequately designed – to mitigate certain integrity risks in public procurement under specific circumstances. Table 3 presents an overview of these approaches. Some middle-income countries that possess decent IT infrastructure and governance capacity, with a tradition of operating e-procurement systems and committed to strengthening public sector accountability to gain constituency support and high-quality investments, could be potential candidates for the first and last approaches. Particularly, when trust in government is low, the e-procurement system is weakly designed and that technical capacity to tamper with the system is easily available, the case for using blockchain to curb corruption would be stronger.

Table 3. Overview of potential blockchain applications for public procurement integrity

	Approach One	Approach Two	Approach Three
Scenarios where blockchain may have a role	• Public trust is low, and government committed to winning public support and investments • Rampant IT system manipulations	• Multiple e-procurement systems operate in silo • Lack of internal expertise or information in defining tender specifications and estimating pricing	• Aid-reliant or post-regime change countries • Lack of capacity and/or competence in procurement staff
How blockchain is introduced	Track full-cycle procurement workflows, notably important documentation and decisions	Enable data-level interoperability on supplier & contract data across e-procurement systems	Open up bid evaluation to a large pool of algorithms-selected evaluators, and store results on blockchain
What integrity risks may be mitigated	"System corruption": insider document tampering or outsider cyber-attacks	• Middleman corruption in pre-tender assessment • Asymmetry of information & supplier pricing opacity	Sub-optimal or biased bid evaluation, due to incompetence or corruption
Potential advantages over regular e-procurement systems	• Stronger system integrity (security) • Facilitated traceability and auditability	• Mutualised supplier & contract data in a secure and flexible way without imposing unified process • Aggregate visibility for a supervisor/fund provider to monitor fund recipient accountability	Potentially more objective, secure & tamper/censorship resistant bid evaluation
Other necessary conditions	• Inspection and audit • Good data management, including commitment to open data practices	• Combination with big data analytics • Adequate data analytics skills • Standardised data digitisation process	• Well-defined criteria for selecting evaluators • Mutual anonymity until end of bidding • Enlarging evaluators pool • Proper mechanisms to ensure evaluator integrity
Limitations and challenges	• Ineffective in preventing corruption other than IT system manipulation • Does not replace the need for physical trust (e.g. dishonest data) • Measures to ensure system integrity may undermine other features	• Ineffective against insider corruption without proper inspection and audit • Political barriers to adoption may be high if the purpose is to monitor procurement practices of fund/loan recipients	• Ineffective in preventing specifications to be drafted in a biased way • Biased or inadequate evaluators selection due to political capture or incompetence • Political or institutional barriers to adoption

Source: Author's elaboration.

Large economies with robust but fragmented e-procurement systems may find merits in the second approach, although the first motivation of using blockchain will likely be to enhance efficiency and value-for-money, which probably owes more to the power of big data analytics tools. Multilateral development banks may also appreciate this approach for benchmarking compliance performance across jurisdictions and projects. The last approach might be envisaged for aid-dependent countries with weaker institutions and governance capacity, or for post-regime change countries that need to quickly re-establish public and business confidence. Nonetheless, the case would be less strong when internet access is largely unavailable or as other developmental priorities (e.g. peace and order) prevail.

There are other ways to apply blockchain in public procurement, for instance, by adding smart contract[26] on blockchain-based shared ledgers to automate bid evaluation, contract negotiation or payment (Hardwick et al., 2018; EU Blockchain Observatory & Forum, 2018). They are not discussed here as their direct implications on anti-corruption are less obvious without a thorough technical review of the potentials and limitations[27]. For all applications, there will be costs of learning, integration and trade-offs, as well as barriers to adoption from institutions and current users. Today, blockchains need to overcome several technical challenges to deliver the promise of scalability, security and decentralisation without significant trade-offs. Breaches and malfunctions are highly likely before the technology matures. The development costs are high as blockchain developers are scarce and expensive and new infrastructure may be required or repurposed. The cost for computation would vary depending on how computationally intensive the validation process is, but the cost for storage would increase rapidly if records need to be stored permanently on every full node in the network. Furthermore, as any changes in the ruling protocols must be approved by the system nodes, flexibility and fragmentation concerns may arise when blockchains become largely adopted to create an interconnected network of e-procurement systems.

Aside these technical complexities – for which solutions are being developed but the viability of large-scale adoption is still being tested, blockchain's potential for social impacts may have all too often been overstated (Pisa, 2018). Blockchain is inherently political as it is designed to govern behaviours of groups of people and organisations through social and/or financial incentives, hence implementation would be slow and contentious (Graglia and Mellon, 2018). Moreover, combatting corruption requires a holistic approach to close off all loopholes and change incentives and misconceived rules. Blockchain alone cannot bring substantial transformative outcomes. As corruption involves dishonest behaviours in the real off-chain world, blockchain can at best enhance integrity of the IT system and hence trust in the on-chain records, thereby forcing corruption to get more sophisticated, but the need for human agency to properly manage the procurement process and proactively inspect[28], audit and enforce accountability will always remain. Auditors shall also be shielded from political interference and adequately skilled to perform data-driven analysis, and civic oversight including through external

[26] A piece of code that automatically executes all or parts of an agreement and is stored on a blockchain-based platform (Levi and Lipton, 2018).

[27] For further reading, see Levi and Lipton (2018).

[28] E.g. regular/random inspections to check contract performance or avoid collusion between suppliers and supervising public officials.

stakeholders (e.g. NGOs, journalists) would be crucial when there is systemic corruption within the government. A good integrity policy framework – including an independent justice system to enforce laws and regulations, should also be supported by efforts to buttress the ethical and moral foundation of human behaviour.

Ultimately, whether there is a strong case to use blockchain (or alternative technologies) for enhancing public procurement integrity would depend on three key questions:

- First, what are the major forms of integrity risks along the procurement cycle, and how adequate the existing procurement system is to address those risks. Importantly, whether record tampering is frequently observed, and whether the technical capacity to perform such an act is easily available.
- Second, how important the anti-corruption agenda is over other policy objectives, such as achieving efficiency in workflows and value-for-money in the allocation of resources. This will affect one's level of acceptance of the potential trade-offs brought by the technology.
- Third, what is the expected value of benefits brought by the technology relative to the amount of resources and efforts one is ready to commit, in terms of development costs and time requirements, level of operational complexity and flexibility, amount of re-training, and other barriers to adoption and implementation.

All things considered, if corruption happens predominantly off-system, the cost of over-engineering the procurement tool to achieve zero-corruption tolerance "on paper" could quickly outweigh the benefits, with no substantial developmental impacts. Discussion of the role of technology for anti-corruption should not dilute the importance that commitment of decision-makers is key to all successful anti-corruption efforts. Given blockchain's current levels of technological maturity and ease of adoption, it may be more cost-efficient and easier to focus one's anti-corruption efforts on improving compliance with public procurement best practices, especially for countries where non-compliance is still common. Blockchain and other analytics technologies could come as the next step to reinforce the integrity and intelligence of the procurement system, building on a culture of accountability and open governance that will have been nurtured in the first place.

References

Andoni, M. *et al.* (2019), "Blockchain Technology in the Energy Sector: A Systemic Review of Challenges and Opportunities", *Renewable and Sustainable Energy Reviews*, Vol. 100, p. 143-174.

Bikshapathi, K. and P. Raghuveer (2010), *Implementation of E-Procurement in the Government of Andhra Pradesh: A Case Study*.

BitFury (2016), *On Blockchain Auditability: White Paper*.

World Bank (2018), Enterprise Surveys database.

EU Blockchain Observatory & Forum (2018), *Blockchain for Government and Public Services*.

Graglia, J. and C. Mellon (2018), "Blockchain and Property in 2018: At the End of the Beginning", *Innovations: Technology, Governance and Globalization*, Vol. 12, No. 1-2, 2018, p. 90-116.

Greenspan, G. (2017), *The Blockchain Immutability Myth*, 4 May 2017.

Greenspan, G. (2016), *Blockchain vs Centralised Database*, 17 March 2016.

Hardwick, F. et al. (2018), *Fair and Transparent Blockchain-based Tendering Framework: A Step Towards Open Governance*, 15 May 2018.

Kohli, J. (2012), *Red Flags in E-Procurement / E-Tendering for Public Procurement and Some Remedial Measures*.

Kohli, J. (2010), *E-Procurement Integrity Matrix*, Transparency International India.

Levi, S. D. and A. B. Lipton (2018), "An Introduction to Smart Contracts and Their Potential and Inherent Limitations", *Skadden*, 26 May 2018.

OECD (2018), *Mexico's E-Procurement System: Redesigning CompraNet through Stakeholder Engagement*, OECD Publishing.

OECD (2016), *Preventing Corruption in Public Procurement*, OECD Publishing.

Pisa, M. (2018), *Reassessing Expectations for Blockchain and Development*, Centre for Global Development.

Singh, N. (2018), "Hybrid Blockchain – The Best of Both Worlds", *101 Blockchains*, 6 October 2018.

S N Huda *et al.* (2017), "Potential Fraudulent Behaviours in E-Procurement Implementation in Indonesia", *IOP Conference Series: Materials Science and Engineering*, 185 (2017) 012003.

Somasundaram, R. and Q. Hasan (2018), "Development of a Global e-Government Procurement Architecture using Blockchain Technology", *ADB Technical Assistance Consultant's Report*, 2018.