THE COLUMBIA
SCIENCE & TECHNOLOGY
LAW REVIEW

VOL. XX STLR.ORG FALL 2018

ARTICLE

DISTRIBUTED LEDGER TECHNOLOGIES AND CORRUPTION THE KILLER APP?[†]

Jesse Marks[*]

[†] This article may be cited as http://www.stlr.org/cite.cgi?volume=20&article=marks. This work is made available under the Creative Commons Attribution–Non-Commercial–No Derivative Works 3.0 License.

[*] Jesse Marks is a manager at Schmidt Futures. Schmidt Futures is a venture facility for public benefit, founded by Eric and Wendy Schmidt, that advances society through technology, inspires breakthroughs in scientific knowledge, and promotes shared prosperity (see schmidtfutures.com). He is a graduate of Yale Law School, where he was co-editor-in-chief of the Yale Human Rights and Development Law Journal. Prior to Yale, Jesse worked as a strategic adviser to the Ethiopian government and as a management consultant with McKinsey & Company. Jesse has also served as a graduate fellow with the Governance Lab (GovLab) at New York University, where he helped launch the Smarter Crowdsourcing Against Corruption Initiative, a collaboration between GovLab, the Inter-American Development Bank, and Mexico's Secretaría de la Función Pública to identify new technological solutions to fight corruption in Mexico. This Article benefited greatly from conversations with a range of experts—both for the Smarter Crowdsourcing Initiative and specifically for this Article—including Susan Rose-Ackerman (Henry R. Luce Professor of Law and Political Science, Yale Law School and Yale University), Beth Simone Noveck (Jerry Hultin Global Network Professor, New York University's Tandon School of Engineering; Director, GovLab), Eduardo Bohórquez (Executive Director, Transparencia Mexicana), Tomicah Tillemann (Director of Bretton Woods II, New America), Brian Behlendorf (Executive Director, the Hyperledger Project), Rafael Garcia Aceves (Program Coordinator, Transparencia Mexicana), and Alice Xiang (Associate, Gunderson Dettmer). All views expressed in this Article are the author's and do not reflect the positions of Schmidt Futures, GovLab, or interviewed individuals.

I. INTRODUCTION

As recently as three years ago, few would have expected that Bitcoin, the virtual currency famous for its anonymity and ubiquity in the black market, would prove to be the source of one of the most widely heralded technological breakthroughs ever to be applied to the fight against corruption. While much of the world focused on Bitcoin's novelty as a purely digital asset, its imperfect fit under commonly accepted definitions of "currency," and its uses for money laundering, in reality, it was Bitcoin's underlying technological architecture that would prove most consequential.

"Blockchain," as that architecture has come to be known, is a "distributed, decentralized transaction ledger," which is shared with, maintained by, and updated by each "node" (i.e., connected computer) in a network.[1] It is a peer-to-peer system, with no central authority managing the transaction flow. Because records are stored in many places, because no single user has the ability to change a given record, and because all nodes in the network are responsible for validating attempted updates or transactions, the end result is an immutable ledger that is virtually impossible to falsify.[2] Blockchain technology has uses beyond digital currency: blockchains and a range of similar technologies, collectively known as distributed ledger technologies (DLTs), can be used to create immutable, automatically validating ledgers of virtually any nature, such as land registries and health records.

In the anti-corruption realm, some have already speculated that DLTs will have game-changing effects. Initiatives to transfer national land registries into DLT-based ledgers have already begun in Ghana, Georgia, and Sweden, while other countries are considering using DLTs to track government grants, fight bank fraud, and manage supply chains.[3]

As futurists continue to speculate about DLTs' seemingly limitless potential, and as pilots begin on a range of potential applications of the technology to anti-corruption efforts, this Article contextualizes these developments and considers DLTs' big-picture implications. This Article proceeds in five parts. Part II provides a

[1] Alan Morrison, *Blockchain and Smart Contract Automation: Blockchains Defined*, PWC: U.S. BLOGS (Mar. 19, 2016), https://usblogs.pwc.com/emerging-technology/blockchains-defined/ [http://web.archive.org/web/20160917232842/http://www.pwc.com/us/en/technology-forecast/blockchain/definition.html]. These features are further detailed later in this paper.

[2] *Id.*

[3] *See* discussion *infra* Section IV.A.

brief background on DLTs: what they are, what they do, and where they originate. Part III positions this discussion within the broader anti-corruption literature and offers a framework for government officials, aid agencies, and reformers considering whether to deploy new technologies in the fight against corruption. Applying that framework to DLTs, Part IV identifies three anti-corruption use cases for which governments should particularly consider DLTs. Part IV also examines some of the key risks in using blockchains to fight corruption and outlines strategies governments can use to mitigate those risks. Part V recommends some short- and long-term steps for governments interested in exploring DLTs. Part VI concludes with a note of caution about the rapidly evolving nature of these technologies.

II. Background on Blockchain and Distributed Ledger Technologies (DLTs)

A. Origins and Brief Explanation

Blockchain traces its origins to a 2008 white paper by the pseudonymous Satoshi Nakamato.[4] Nakamato's work focused on the problem of trust in electronic transactions. In previous eras of commerce, trust was easy to establish, since transactions took place in physical marketplaces, often among familiar parties, and with immediate transfers of goods and services. To the extent that trade relied on credit, such credit was typically extended at arm's length—or at least after some form of in-person interaction. Now, in the era of e-commerce, transactions regularly take place among individuals who have never met one another, based on largely unverifiable assurances that they are who they say they are and can deliver what they say they can deliver.

Until 2008, financial institutions filled the void, verifying identities of actors, ensuring that the transfers actually took place and resolving disputes as they arose.[5] This model was neither efficient nor equitable. It relied on profit-driven third parties to serve as gatekeepers to e-commerce, excluding many who lacked sufficient funds or credit to make such an extension of trust profitable; it gave significant market power to the middlemen, who took hefty fees on each transaction; and, it did not always work, since third-party

[4] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* (2008), https://bitcoin.org/bitcoin.pdf.

[5] Don Tapscott & Alex Tapscott, Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World 4-5, 10-11 (2016).

institutions were imperfect protectors against fraud or deceit.[6] Nakamato sought a new model. His approach would cut out the middleman and replace trust with cryptographically-enabled transparency, made possible by a technology known as "blockchain."[7]

In 2009, Nakamoto launched Bitcoin, the world's first completely decentralized digital currency.[8] A Bitcoin is an individually identifiable digital "coin," of finite but slowly-growing supply,[9] that can be freely exchanged for goods and services or converted, at market-defined rates, into traditional currencies.[10] Since its launch in 2009, Bitcoin has gained fame as an interesting economic experiment,[11] as a potential new tool for e-commerce,[12] as a new way to get rich,[13] and, of course, as a currency of choice for drug dealers, child pornographers, and money launderers.[14]

[6] *Id.*; *see also* Nakamoto, *supra* note 4.

[7] Nakamoto, *supra* note 4, at 8.

[8] Jeffrey Brito & Andrea Castillo, *Bitcoin: A Primer for Policymakers* 1 (2013), https://www.mercatus.org/system/files/Brito_BitcoinPrimer.pdf.

[9] The "money supply" will eventually be capped at 21 million units. *Free Exchange: Money from Nothing*, ECONOMIST (Mar. 15, 2014), http://www.economist.com/news/finance-and-economics/21599053-chronic-deflation-may-keep-bitcoin-displacing-its-fiat-rivals-money.

[10] *Id.*

[11] Such studies have largely centered on whether Bitcoin is a "currency." *See* David Yermack, *Is Bitcoin a Real Currency? An Economic Appraisal* (Nat'l Bureau Econ. Res., Working Paper No. 19747, 2013) (finding Bitcoin to be more of a speculative investment than a currency due to its low transaction volume, high volatility, and minimal exchange rate correlation to other currencies); *see also* I.R.S. News Release IR-2014-36 (Mar. 25, 2014), https://www.irs.gov/uac/newsroom/irs-virtual-currency-guidance (deciding that Bitcoin would not be treated as a currency for tax purposes). *But see* Case C-264/14, *Skatteverket v. Hedqvist*, ECLI:EU:C:2015:718, par. 24 (Oct. 22, 2015), http://curia.europa.eu/juris/document/document.jsf?docid=170305&doclang=EN (finding that digital currencies like Bitcoin cannot be defined as "tangible property" within the meaning of Europe's VAT directive).

[12] This, of course, was Nakamoto's stated purpose in designing Bitcoin. *See supra* note 4.

[13] *See* Erik Franco, *Inside the Chinese Bitcoin Mine That's Grossing $1.5M a Month*, MOTHERBOARD (Feb. 6, 2015), https://motherboard.vice.com/en_us/article/chinas-biggest-secret-bitcoin-mine (touring a "mining farm," where massive banks of supercomputers solve complex puzzles to validate Bitcoin transactions and are rewarded with bitcoins for each transaction they validate).

[14] Although Bitcoin provides transparency into which user owns which Bitcoin, user accounts can be set up without showing any identification. If transactions are made through a masked IP address, Bitcoin users are almost completely untraceable. In this way, illegal marketplaces operating on the "darknet" (i.e., only accessible through an anonymous browser like Tor) can facilitate untraceable, peer-to-peer transactions. For perhaps the most famous

At its most basic level, Bitcoin is fueled by a publicly-accessible, cryptographically-enabled distributed ledger, known as the "blockchain." A "ledger" is any kind of record capable of being stored as text or numbers,[15] while a "distributed ledger" is one that is "collectively owned and maintained by all the participants of the system, rather than by one central party."[16] It works like this: each time two parties seek to enter into a transaction, they broadcast their intentions to the network. Other computers in the network, called "nodes," review their own copies of the ledger to ensure (1) that the request has the digital "signature" that it is supposed to have and (2) that the requesting parties actually possess the Bitcoins that they intend to trade. Once a validating node has confirmed a transaction, it "broadcasts" it to other nodes, which then review the first node's work and make sure that it was correct. Eventually, the network achieves "consensus" on the legitimacy of the transaction by either rejecting or clearing it. If a Bitcoin changes hands, each node updates its ledger to reflect the new state of affairs.[17] As the list of transactions grows, it becomes bundled into a "block," which is then connected to other blocks like a "chain," hence the term "blockchain." Should one chain become inconsistent with the others, as would occur if a hacker sought to falsify a given record, the other nodes would identify the inconsistency and reject the change.[18]

This chain grows infinitely long, as transactions are never deleted—only added.[19] As the ledger grows longer, ensuring its immutability becomes a computational challenge. Here, another technical innovation, known as the "hash function," comes into play.

example of how Bitcoin enabled a billion-dollar online drug bazaar, see Joshua Bearman & Tomer Hanuka, *The Rise & Fall of Silk Road*, WIRED (May 2015), https://www.wired.com/2015/04/silk-road-1/.

[15] VT. SEC'Y OF STATE ET AL., BLOCKCHAIN TECHNOLOGY: OPPORTUNITIES AND RISKS 4 (Jan. 15, 2016), http://legislature.vermont.gov/assets/Legislative-Reports/blockchain-technology-report-final.pdf.

[16] H.K. APPLIED SCI. TECH. RES. INST. (ASTRI), H.K. MONETARY AUTH., WHITEPAPER ON DISTRIBUTED LEDGER TECHNOLOGY 10 (2016), http://www.hkma.gov.hk/media/eng/doc/key-functions/finanical-infrastructure/Whitepaper_On_Distributed_Ledger_Technology.pdf; *see also Bitcoin's Future: Hidden Flipside*, ECONOMIST (Mar. 13, 2014), http://www.economist.com/news/finance-and-economics/21599054-how-crypto-currency-could-become-internet-money-hidden-flipside.

[17] ASTRI, *supra* note 16, at 10-15.

[18] *Id.* at 16.

[19] Scott Driscoll, *How Bitcoin Works Under the Hood*, IMPONDERABLE THINGS (July 14, 2013, 8:14 PM), http://www.imponderablethings.com/2013/07/how-bitcoin-works-under-hood.html.

This function reduces entries into a series of 256-bit numbers or "hash values." The value of these numbers is highly sensitive to any modification of the underlying data—changing even a single character leads to dramatic differences in the ultimate "hash value." This hash function cannot be reverse-engineered, thus making it a trusted tool for detecting anomalies in a ledger without the need to review the data in the ledger itself.[20]

Strictly speaking, a blockchain is not immutable. After all, one can conceivably tamper with a ledger, compromise a series of nodes, use those nodes to "validate" the tampered ledger, and trick the other nodes into adopting the falsified records. In practice, however, manipulating a blockchain in this manner is virtually impossible. First, in a blockchain like Bitcoin's, such a practice would require compromising a remarkable number of computers or colluding on a grand scale. Second, and more importantly, blockchains contain another layer of protection, called "proof of work," which requires any node seeking to validate a transaction to first solve a very complex math problem.[21] Each problem essentially requires a computer to make a massive number of guesses—so many that, on average, it would take a single computer years to solve it. Therefore, multiple computers try to solve the problem concurrently, racing to find the right answer. With many nodes racing against one another, the odds of the compromised node actually being the first to validate the transaction are quite low. And even if it was the first to validate, the compromised node would have to post a "proof of work" that the other nodes check before validating the transaction. Unless those nodes are compromised as well, the transaction will automatically be rejected. This verification process takes much less time and computational power than the initial computation. With Bitcoin, the difficulty of the problem is automatically adjusted to accommodate variable transaction volumes and computational capacity, yielding an average per-transaction clearing time of about ten minutes.[22] Requiring validating nodes to race one another means that one cannot co-opt the network simply by taking over more than half of

[20] Hash functions can also be useful for other purposes, such as a "proof of existence." For instance, one could demonstrate existence of a given document by sharing its hash value with the document-holder, rather than compromising information. The other party could then check that hash value against the original document to ensure that the other part was telling the truth. *Id.* at 25-26.

[21] Nakamoto, *supra* note 4, at 3.

[22] Driscoll, *supra* note 19.

the nodes. Instead, one must take over more than half of the *processing power*, which is uneconomical for any one actor to do.[23]

One final technological feature of blockchain is the digital signature. Digital signatures consist of two elements. One is a user's "public key," which is essentially his or her "send to" address. The other is a user's "private key," which is used to verify the user's identity. Through a mathematical process similar to the hash function described earlier, a user can "sign" a transaction using his or her private key, which then generates a new value which can be used to match the user to his or her public key.[24] This "signature" is easily verifiable by the other nodes, and any attempt to sign the transaction without the private key would "be easily detected as bogus."[25]

B. The Wide Reach of Blockchain's Advantages

Only in recent years have observers begun to seriously explore blockchain's potential applications outside the world of cryptocurrency.[26] The first tentative moves came from the financial sector, where Bitcoin had already proven the concept of blockchain-enabled transactions.[27] It was not long, however, before others observed blockchain's potential to solve longstanding business problems. That initial trickle of interest has given way to a cascade of research initiatives, pilots, and startups. The global consultancy McKinsey & Company estimates that, from 2015 through 2016, venture capital funds put more than $1.2 billion into blockchain startups—fifty startups received more than $1 million each.[28] Today, a wide range of industry executives and observers frame blockchain

[23] Nakamoto, *supra* note 4, at 3.

[24] This rather complex mathematical process also predates blockchain, but it is a critical enabler of its success. For the least confusing description of digital signatures (I have yet to find a description that is, in fact, clear), see Driscoll, *supra* note 19.

[25] ASTRI, *supra* note 16, at 26.

[26] For instance, Google Trends indicates that the term "blockchain" was rarely searched for prior to 2013 (when most articles about "blockchain" focused on its applications for Bitcoin), followed by a rapid increase in interest starting in early 2015 and continuing to today. *See* GOOGLE TRENDS, https://trends.google.com/trends/explore?date=all&q=blockchain (last visited Nov. 20, 2018).

[27] *See* Nathaniel Popper, *Bitcoin Technology Piques Interest on Wall St.*, N.Y. TIMES (Aug. 28, 2015), https://www.nytimes.com/2015/08/31/business/dealbook/bitcoin-technology-piques-interest-on-wall-st.html.

[28] Steve Cheng et. al., *Using Blockchain to Improve Data Management in the Public Sector*, MCKINSEY & COMPANY: DIGITAL MCKINSEY (Feb. 2017), http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/using-blockchain-to-improve-data-management-in-the-public-sector.

in revolutionary terms, comparing its transformative potential to that of the Internet itself. Canadian business writer Don Tapscott captures the prevailing mood in the opening chapter of his latest book, *The Blockchain Revolution*:

> It appears that once again, the technological genie has been unleashed from its bottle. Summoned by an unknown person or persons with unclear motives, at an uncertain time in history, the genie is now at our service for another kick at the can—to transform the economic power grid and the old order of human affairs for the better. If we will it.[29]

Exactly how blockchain will shape our future remains somewhat of a mystery—it is simply too soon to tell.[30] Nonetheless, there is value in starting to think ahead, which first requires a clarification of the foundational characteristics that set blockchain apart.

C. The "Blockchain Bundle"

Proponents of blockchain technology all tout different features. Richard Gendal Brown, the Chief Information Officer of R3 Corda, a financial services distributed ledger company, refers to the benefits provided by the blockchain technology as the "blockchain bundle."[31] The five key elements of the "blockchain bundle" are (1) consensus, (2) validity, (3) uniqueness, (4) immutability, and (5) authenticity.

Feature 1: Consensus

The first and most important feature is that blockchains "create a world where *parties to a shared fact* know that the fact they see is the same as the fact that other stakeholders see."[32] These "shared facts" typically center on two questions: (1) what is the status of the objects the ledger is designed to record (e.g., dollars in a given user's account), and (2) what would need to happen for that record to be

[29] TAPSCOTT & TAPSCOTT, *supra* note 5, at 3.

[30] *See The Promise of Blockchain: The Trust Machine*, ECONOMIST (Oct. 31, 2015), https://www.economist.com/leaders/2015/10/31/the-trust-machine ("[T]he history of peer-to-peer technology suggests that it is likely to be several years before the technology's full potential becomes clear.").

[31] Richard Gendal Brown, *Introducing R3 Corda^{TM}: A Distributed Ledger Designed for Financial Services* (Apr. 5, 2016), https://gendal.me/2016/04/05/introducing-r3-corda-a-distributed-ledger-designed-for-financial-services/.

[32] *Id.*

validly changed (e.g., for a dollar to be validly spent)?[33] Consensus regarding these two types of facts enables exchange between mutually untrusting parties by an authoritative showing that both parties have what they are offering to exchange and that they are empowered to make the deal. This consensus feature is useful beyond just one-off transactions. In fact, it can be applied wherever an item changes hands frequently and where a complete record of those exchanges is important, as with money flowing through an organization, trades executed on an exchange, products travelling through a supply chain, or even a diamond making its way from a mine to a dealer to a partner's finger.

Feature 2: Validity

In coming to a consensus on what each party owns and on the rules that govern any potential exchange, a blockchain rapidly validates a given transaction, eliminating the need to wait for a transaction to "clear" (or a third-party intermediary to bear the risk that it does not).[34] This same feature can regulate virtually any exchange where the assets and rules of exchange are tracked on a blockchain, as when governments manage funds from budgeting to disbursement and need technological help ensuring that rules are followed and budgets are not exceeded.[35]

More broadly, blockchain's validation feature has accelerated the deployment of self-executing agreements, known as "smart contracts." These contracts take the form of computer code with a range of automatically-triggered conditional terms.[36] Although smart contracts (and artificial intelligence more broadly) pre-date blockchain, blockchain's validation capabilities provide untrusting

[33] *Id.* One alternative formulation highlights the distinction between "native records" and "references." "Native records" are those pieces of information that come into existence only when they are entered on the ledger. Examples of such records include virtual goods (e.g., bitcoins) or contracts. References, meanwhile, are things that exist separately from the ledger but which the ledger tracks. That could include personal health records or "digital passports" for goods travelling across supply chains. *See* Peter Evans-Greenwood et al., *Bitcoin, Blockchain & Distributed Ledgers: Caught Between Promise and Reality*, DELOITTE AUSTRALIA – CENTRE FOR THE EDGE 20 (2016), https://www2.deloitte.com/content/dam/Deloitte/au/Images/infographics/au-deloitte-technology-bitcoin-blockchain-distributed-ledgers-180416.pdf.

[34] Nakamoto, *supra* note 4, at 1.

[35] *See infra* Section IV.A.1.

[36] GOVERNMENT OFFICE FOR SCIENCE, DISTRIBUTED LEDGER TECHNOLOGY: BEYOND BLOCK CHAIN 23-24 (2016) (U.K.), https://www.gov.uk/government/news/distributed-ledger-technology-beyond-block-chain.

actors with greater assurance that the smart contract's conditions will be triggered only by actual occurrence of the underlying event.[37] Previous models of smart contracting still required both ex ante reputation mechanisms and post hoc dispute resolution processes to work, which limited their usefulness.[38] Smart contracts have a wide range of potential applications. They can be used to create conditional purchase orders, [39] help consumers manage access to their personal information,[40] and even create entirely machine-run organizations.[41]

Feature 3: Uniqueness

A user cannot "double-spend" a bitcoin by selling it to multiple parties at the same time, because a transaction can only be cleared after at least half of the nodes agree that it is valid. Once a node has confirmed one transaction, it will reject any subsequent attempt by the same user to sell the same bitcoin. Logically, only one trade of a given coin can clear that fifty percent threshold, making "double-spending" impossible.[42]

[37] *Id.* Smart contracts trace their origins to a 1997 paper by Nick Szabo. S*ee generally* Nick Szabo, *Formalizing and Securing Relationships on Public Networks*, FIRST MONDAY (1997), http://firstmonday.org/ojs/index.php/fm/article/view/548/469#Dimensions (outlining the idea of smart contracts and how they work, more than a decade prior to Nakamoto's white paper on blockchain).

[38] *Id.*

[39] *Blockchain's Smart Contracts: Driving the Next Wave of Innovation Across Manufacturing Value Chains*, COGNIZANT 20-20 INSIGHTS, June 2016, at 4, https://www.cognizant.com/whitepapers/blockchains-smart-contracts-driving-the-next-wave-of-innovation-across-manufacturing-value-chains-codex2113.pdf.

[40] GOVERNMENT OFFICE FOR SCIENCE, *supra* note 36, at 22-24.

[41] This is known as a "decentralized autonomous organization," or DAO. The first such DAO, called "The DAO," was launched to serve as a venture fund of sorts for the Blockchain. *See* Seth Bannon, *The Tao of "The DAO" or: How the autonomous corporation is already here*, TECHCRUNCH (May 16, 2016), https://techcrunch.com/2016/05/16/the-tao-of-the-dao-or-how-the-autonomous-corporation-is-already-here/ (outlining how a DAO could work in theory). *But see* ALLEN & OVERY LLP, DECENTRALIZED AUTONOMOUS ORGANIZATIONS 4 (2016), http://www.allenovery.com/SiteCollectionDocuments/Article%20Decentralized%20Autonomous%20Organizations.pdf (describing how a hacker compromised The DAO and stole its funds).

[42] Driscoll, *supra* note 19.

Feature 4: Immutability

Because records are stored in multiple places and validated by consensus mechanisms, they are essentially unchangeable.[43] Although a blockchain will allow valid transactions or updates, those records are *added* to the ledger and do not replace past records, which remain intact.[44] This feature is useful any time a trusted custodian of records is hard to come by,[45] there is concern about a record's physical integrity,[46] or records are vulnerable to manipulation—either by rogue insiders or hackers.[47] Blockchain-based smart contracts also benefit from assurances of immutability.[48]

[43] In records management terms, this is known as the "authenticity" of the record. "Authenticity is defined as the trustworthiness of a record as a record, meaning that the record is what it purports to be, free from tampering or corruption." Luciana Duranti & Corinne Rogers, *Trust in Digital Records: An Increasingly Cloudy Legal Area*, 28 COMPUTER L. & TECH. REV. 521, 525 (2012); *see also* VT. SEC'Y OF STATE, *supra* note 15, at 10 (extrapolating from Duranti's and Rogers' definitions to discuss the benefits of blockchain for state record-keeping).

[44] Further, as blockchains "grow," modifying an earlier record becomes exponentially more difficult. Nakamoto, *supra* note 4, at 7 ("Given our assumption [that 'malicious' actors do not possess more than 50% of processing power], the probability [of record manipulation] drops exponentially as the number of blocks the attacker has to catch up with increases. . . . [I]f he doesn't make a lucky lunge early on, his chances become vanishingly small as he falls further behind.").

[45] Such is the case with land registries. *See* discussion *infra* Section IV.A.1.

[46] For instance, the 2010 Haiti earthquake destroyed sixty years of public records, "including civil registration papers, administrative documents issued by the presidency . . . and similar papers registered with Haitian municipalities." *Haiti Quake Destroyed or Damages 60 Years of Archives*, AGENCE FRANCE PRESSE, Dec. 11, 2013, accessed on LexisNexis Academic.

[47] In fact, even Bitcoin has helped the U.S. Government identify fraud by rogue federal agents, as when Shaun Bridges and Carl Mark Force IV of the Baltimore Silk Road Task Force were found to be laundering money from their investigation. In this case, they succeeded in using their database access and authority as federal agents to destroy evidence held by the government and private companies, but they were unable to cover their tracks on the Bitcoin blockchain itself. For a fascinating account of the investigation, see Kathryn Haun, Assistant U.S. Attorney and Digital Currency Coordinator for U.S. Department of Justice, *How the U.S. Government is Using Blockchain to Fight Fraud / Kathryn Haun / TEDxSanFrancisco*, YOUTUBE (Oct. 26, 2016), https://www.youtube.com/watch?v=507wn9VcSAE.

[48] Tania H., *A Guide to Smart Contracts and Their Implementation*, RUBYGARAGE, https://rubygarage.org/blog/guide-to-smart-contracts (last visited Nov. 28, 2018).

Feature 5: Authentication

Authentication is how users demonstrate that others are who they say they are.[49] Digital signatures, as discussed in Section II.A, enable this. Blockchain's approach to authentication also provides two additional benefits. First, because blockchains are decentralized, there is no single omnipotent administrator. As R3 Corda's Brown explains, "this is quite different to traditional enterprise systems where these 'super-user' accounts are prevalent and petrifying from a security perspective."[50] Second, the system does not need to actually know a user's private key to verify his or her digital signature. This means the system is not required to maintain the kind of centralized repository of passwords that could leave users vulnerable to hacking.

Digital signatures and smart contracts offer a particularly interesting combination. On the one hand, digital signatures replace physical signatures for parties entering legal obligations through smart contracting. On the other hand, smart contracts can also be used to specify access controls for an account, identifying exactly whose digital signature should be needed for a given transaction to take place. Requiring multiple signatures for more consequential actions can add an extra degree of security and prevent unauthorized transfers.[51]

D. Other DLTs: Adapting the "Blockchain Bundle" for New Applications

Since Bitcoin's launch, developers have created new distributed ledgers and applied them to manage a variety of new types of records. Seemingly overnight, the term "blockchain" has transformed from a niche term for cryptocurrency record-keeping into the new buzzword in the tech community. It has quickly eclipsed "the cloud" as the thing that will change the world but that few seem to understand. Technology developers have ridden the wave of venture capital funding and willing customers by creating new "blockchains," each of which, though bearing the same name, is starting to look less and less like the original Bitcoin blockchain.

[49] GOVERNMENT OFFICE FOR SCIENCE, *supra* note 36, at 13.

[50] Richard Gendal Brown, *supra* note 31.

[51] This type of authentication is called "multi-sig." For a discussion of multi-sig's benefits and the various ways it can be set up, see Ben Davenport, *What is Multi-Sig, and What Can It Do?*, COIN CENTER (Jan. 1, 2015), https://coincenter.org/entry/what-is-multi-sig-and-what-can-it-do.

As a result, the term "blockchain" has taken on a life of its own, with a meaning that extends well beyond its actual, technical definition.[52]

The Bitcoin blockchain described in Section II.A. is a rather limited technology. For one, its "proof of work" validation process requires a significant amount of computing power, making it slow and energy-intensive. Processing just one Bitcoin transaction requires as much energy as a typical U.S. household consumes in *1.5 days*.[53] Bitcoin can make up for the costs by rewarding its validators with new bitcoins that they "mine" by validating transactions. But all told, this is both an expensive and environmentally destructive way of ensuring network security. Additionally, "mining" may become less profitable, as the bitcoin reward is periodically "halved" and will eventually cease.[54] Finally, proof-of-work validation takes substantial time: about ten minutes per transaction. This works for Bitcoin, but it is hardly ideal for networks set up for high-frequency, routine transactions.[55] That is not to say that distributed ledger technologies cannot serve such purposes—just that the Bitcoin blockchain cannot. This distinction illustrates the importance of being clear about the meaning of terms such as "blockchain" and "distributed ledger technologies."

The term "blockchain" refers specifically to one type of distributed ledger technology: that which takes a number of records, collates them into a block, and then chains those blocks together through cryptographic signatures.[56] Another platform that utilizes this technology is Ethereum, which, like Bitcoin, is open to any user and validates transactions through the same energy-intensive "proof of work" mechanism. Unlike Bitcoin, however, the supply of cryptocurrency in Ethereum is fixed. Instead, users pay transaction

[52] *See* DELOITTE AUSTRALIA, *supra* note 33 (outlining the expansiveness of common definitions of "blockchain" and positing that, while "blockchain" is itself a limited technology, distributed ledger technologies have significant potential for wide application).

[53] Christopher Malmo, *Bitcoin is Unsustainable*, MOTHERBOARD (June 29, 2015), https://motherboard.vice.com/en_us/article/bitcoin-is-unsustainable.

[54] Robert Devoe, *What is Bitcoin Halving? Complete Guide to this Mining Change*, BLOCKONOMI (Mar. 20, 2018), https://blockonomi.com/bitcoin-halving/.

[55] DELOITTE AUSTRALIA, *supra* note 33, at 7. *See also How Will Blockchain Change European Market Structure?*, BANK OF AMERICA MERRILL LYNCH – INDUSTRY OVERVIEWS (Feb. 1, 2016), http://www.longfinance.net/images/reports/pdf/BAML%20(2016)%20How%20will%20blockchain%20change%20European%20market%20structure.pdf ("Blockchain is too slow to power a trading venue; we think that it is physically impossible for a distributed solution to reach the performance of even the existing generation of trading platforms.").

[56] GOVERNMENT OFFICE FOR SCIENCE, *supra* note 36, at 17.

fees through small payments known as "gas."[57] Other DLTs organize their records in different ways. Iota, a cryptocurrency designed to connect the "Internet of Things" (IoT), stores records in a "tangle," which offers computational efficiency and security.[58] Ripple, a cross-border transaction service, tracks a "chain of ledgers" rather than a chain of transactions. Each ledger consists of a "current net state" (each node's assets and liabilities), all previous "net states," and the updates required to get from previous net states to the current one. This makes it computationally easier to calculate each participant's current assets but harder to follow the full history of transactions—a tradeoff that, in the case of cross-border transactions, cuts in favor of this design, but which may not be appropriate for other uses.[59] Note that none of these applications actually uses blockchains and hence should be referred to simply as "DLTs."[60]

Another important distinction is that between "permissioned" and "unpermissioned" DLTs. In an unpermissioned DLT, anyone can download the ledger, join the network, and start making or validating transactions. Of course, since anyone can join the network, nobody can really be trusted. To solve this, many DLTs rely on the energy-intensive "proof of work" validation process discussed earlier.[61] This type of DLT is most useful for "public goods"—cryptocurrencies like Bitcoin or blockchains that can be used by a wide range of actors, for a wide range of purposes. In contrast, permissioned DLTs are different in that the participating nodes are all predetermined. Presumably, each node is trusted, which reduces the risk of dishonest parties misappropriating records. Predetermined access also makes it impossible for one infiltrator to overwhelm the network by creating so many nodes that it can achieve a "consensus." Consensus validation still occurs, but usually without the added barrier of complex problem-solving ("mining") that shifts the balance of power from those who control the most nodes to those who control the most processing power.[62] Permissioned DLTs can facilitate faster, more secure, and more cost-effective transactions than can unpermissioned DLTs like Bitcoin's blockchain. However, they are, by design, less open to outsiders. Additionally, depending on how their consensus mechanisms are set

[57] ASTRI, *supra* note 16, at 35.

[58] SERGUEI POPOV, THE TANGLE (Jinn Labbs 2016), https://www.iotatoken.com/IOTA_Whitepaper.pdf.

[59] DELOITTE AUSTRALIA, *supra* note 33, at 21.

[60] ASTRI, *supra* note 16, at 17.

[61] *Id.* at 47.

[62] *Id.* at 20-22.

up, they can be less secure if one or more of the participants is hacked or compromised.

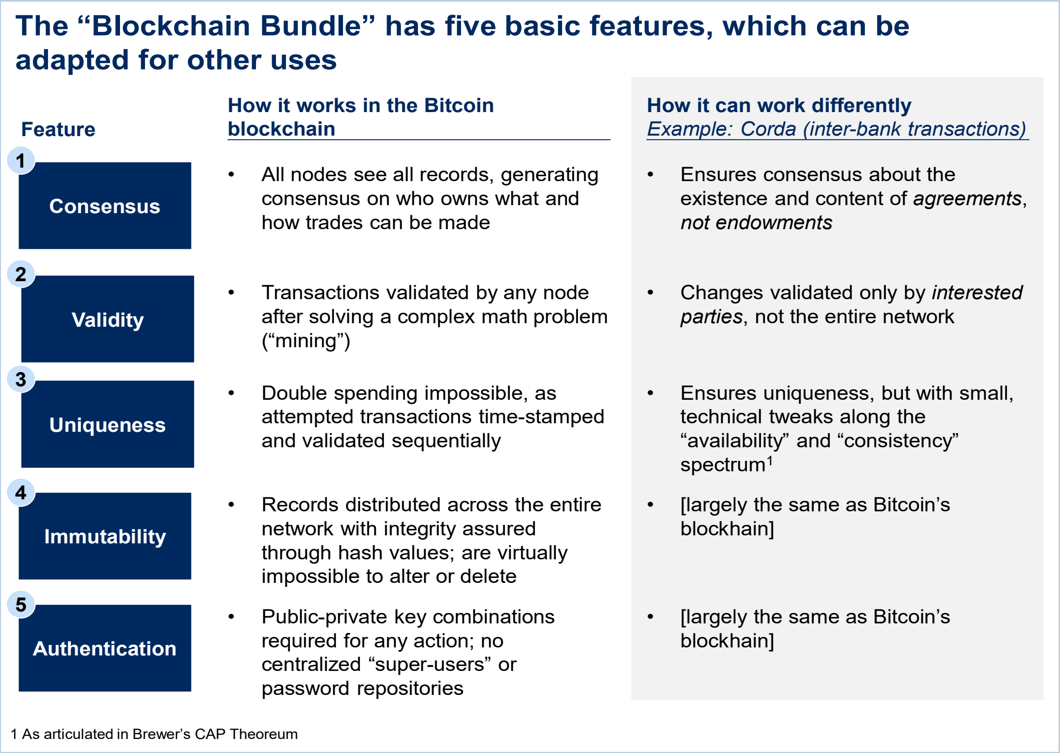
A good example of a permissioned DLT is R3's Corda, used for recording and processing interbank financial agreements. Through smart contracting, banks share "state objects" with their counterparties. A state object is "a digital document which records the existence, content, and current state of an agreement between two or more parties."[63] Updates are applied through "transactions," which create new "state objects." One interesting aspect of Corda is that consensus takes place only at the bilateral level. When Bank A and Bank B enter into an agreement, only those two banks need to agree on what that contract says. Should Bank B subsequently seek to exercise an option outlined in the original agreement, it need only point Bank A to their shared record of the original agreement (of course, through smart contracting, this can all be done automatically, in accordance with pre-set conditions). In the context of interbank smart contracting, there is no reason for Bank C to know about agreements between Banks A and B. Therefore, Corda's consensus mechanism can be much more limited and, by extension, more secure.[64]

Corda represents a significant departure from Bitcoin's blockchain design, but it still applies the blockchain bundle effectively. Figure 1 on the following page summarizes the five benefits of the blockchain bundle and how Corda, as an example, can be adapted to address new challenges.

[63] *See generally* RICHARD GENDAL BROWN ET AL., CORDA: AN INTRODUCTION (2016) (outlining the basics of Corda's technology, how it differs from Blockchain, and how and why it does not require universal sharing of records to nonetheless ensure their validity), http://www.r3cev.com/blog/2016/8/24/the-corda-non-technical-whitepaper; *See also* Richard Gendal Brown, *The Corda Way of Thinking*, GENDAL.ME (Feb. 21, 2017) (providing a much more accessible description of how Corda works), https://gendal.me/2017/02/21/the-corda-way-of-thinking/.

[64] *Id.*

Figure 1 – Features of the "Blockchain Bundle"



The "Blockchain Bundle" has five basic features, which can be adapted for other uses

Feature	How it works in the Bitcoin blockchain	How it can work differently *Example: Corda (inter-bank transactions)*
1 Consensus	All nodes see all records, generating consensus on who owns what and how trades can be made	Ensures consensus about the existence and content of *agreements*, *not endowments*
2 Validity	Transactions validated by any node after solving a complex math problem ("mining")	Changes validated only by *interested parties*, not the entire network
3 Uniqueness	Double spending impossible, as attempted transactions time-stamped and validated sequentially	Ensures uniqueness, but with small, technical tweaks along the "availability" and "consistency" spectrum[1]
4 Immutability	Records distributed across the entire network with integrity assured through hash values; are virtually impossible to alter or delete	[largely the same as Bitcoin's blockchain]
5 Authentication	Public-private key combinations required for any action; no centralized "super-users" or password repositories	[largely the same as Bitcoin's blockchain]

[1] As articulated in Brewer's CAP Theoreum

As new DLT applications arise, the ideal technology will depend on the underlying use. For example, where all nodes are known and trusted entities, some permissioned ledgers may emphasize speed and ease of use over the time- and resource-intensive cryptography required by untrusting, unpermissioned networks. Some, like Corda, may focus on bilateral rather than universal consensus in order to exchange more sensitive information. Yet others, like Ethereum, may be designed for maximal smart contracting compatibility. All of these DLTs apply the basic "blockchain bundle," but they optimize for different features, illustrating the tradeoffs inherent in the design of any technological system.

III. Cutting Through the Noise: A Framework for Considering the Nexus Between DLTs and Corruption

As entrepreneurs and venture capitalists have invested more in DLTs, commentators have begun to speculate on potential applications in the fight against corruption. The anti-corruption realm has not been immune from the hyperbolic terms with which DLTs have been discussed in other sectors, with commentators exclaiming that DLTs are anti-corruption "game changers" without clearly explaining how or why. "How Bitcoin's Blockchain Could

Mark an End to Corruption," proclaimed one recent headline.[65] "Goodbye Corrupt Charities: Hello Blockchain," declared another.[66] "New Initiative Aims to Eliminate Corruption With Blockchain Technology," said a third.[67] Some have even come to refer to blockchain as the "killer app" in the fight against corruption.[68] Such hyperbolic discussions, however, have thus far failed to consider the myriad root causes of corruption or how blockchain could actually help tackle them.

Startups and pilot projects are already underway. Many of these have focused on securing government land registries, with pilots launched by Bitland Global in Ghana,[69] Chromaway in Sweden,[70] and Bitfury in the Republic of Georgia[71] and in Ukraine.[72] Some experts have argued that DLTs can help fight corruption beyond just land registries. For example, a report by the U.K. Government Office for Science as recommended using DLTs to strengthen

[65] Tibi Puiu, *How Bitcoin's Blockchain Could Mark an End to Corruption*, ZME SCI. (Oct. 29, 2015, 6:02 AM), http://www.zmescience.com/research/technology/bitcoin-blockchain-corruption-04232/.

[66] Ameer Rosic, *Goodbye Corrupt Charities: Hello Blockchain*, HUFFINGTON POST (Nov. 25, 2016), http://www.huffingtonpost.com/ameer-rosic-/goodbye-corrupt-charities_b_13207806.html.

[67] Laura Shin, *New Initiative Aims to Eliminate Corruption With Blockchain Technology*, FORBES (June 20, 2016), https://www.forbes.com/sites/laurashin/2016/06/20/new-initiative-aims-to-eliminate-corruption-with-blockchain-technology/#d396d8f13094.

[68] *Id.* (quoting Tomicah Tillemann, director of the Bretton Woods II Initiative at New America, a D.C.-based think tank) ("Blockchain has the potential to be the killer app for corruption.").

[69] Roger Aitken, *Bitland's African Blockchain Initiative Putting Land on the Ledger*, FORBES (Apr. 5, 2016), https://www.forbes.com/sites/rogeraitken/2016/04/05/bitlands-african-blockchain-initiative-putting-land-on-the-ledger/#79f0ca917537. *See also* L. CHRIS BATES, BITLAND GLOBAL WHITE PAPER (2016), http://www.bitland.world/wp-content/uploads/2016/03/Bitland_Whitepaper.pdf (detailing the plan for Ghana's blockchain land registry).

[70] Pete Rizzo, *Sweden's Blockchain Land Registry to Begin Testing in March*, COINDESK (Jan. 10, 2017), http://www.coindesk.com/swedens-blockchain-land-registry-begin-testing-march/. *See also The Land Registry in the Blockchain – Testbed*, KAIROS FUTURE (Mar. 2017), https://chromaway.com/papers/Blockchain_Landregistry_Report_2017.pdf (providing a detailed report of early tests of the technology and analyses of its economic, legal, and social implications).

[71] Laura Shin, *The First Government to Secure Land Titles on the Bitcoin Blockchain Expands Project*, FORBES (Feb. 7, 2017, 9:52 AM), https://www.forbes.com/sites/laurashin/2017/02/07/the-first-government-to-secure-land-titles-on-the-bitcoin-blockchain-expands-project/#5febb2dc4dcd.

[72] Gertrude Chavez-Dreyfuss, *Ukraine Launches Big Blockchain Deal with Tech Firm Bitfury*, REUTERS (Apr. 13, 2017, 2:35 AM), http://www.reuters.com/article/us-ukraine-bitfury-blockchain-idUSKBN17F0N2.

international aid systems by deploying digital coins, which would allow governments to cut out the middlemen and "trace exactly where the currency has been spent and by whom."[73] Others have called for the use of DLTs to track research grants and municipal finances.[74]

Although these initial forays into DLT-based record-keeping appear promising, no one has yet developed an overall theory as to how DLTs will influence the fight against corruption. Those pilots currently underway focus on a narrow set of use cases, while no academic literature yet bridges the fields of technology and anti-corruption in a way that sheds light on the broader set of DLTs' potential uses. Thus, public officials and anti-corruption reformers are left mostly with research reports that focus on the technology in broad terms, advertisements put out by technology providers looking for business, and breathless news stories. In the absence of clear guidance on where and when DLTs may be a worthwhile investment, policymakers are faced with an unenviable choice between either jumping into the fray and making potentially wasteful investments or sitting on the sidelines and failing to harness what could become a vital technology. In the corporate world, many are taking the former approach. Gideon Greenspan, CEO of Coin Sciences Ltd., a blockchain startup, writes:

> Here's how it plays out. Big company hears that blockchains are the next big thing. Big company finds some people internally who are interested in the subject. Big company gives them a budget and tells them to go do something blockchainy. Soon enough they come knocking on our door, waving dollar bills, asking *us* to help *them* think up a use case. Say what now?[75]

Needless to say, this is not the right way to consider any major investment, particularly when public dollars are on the line.

[73] GOVERNMENT OFFICE FOR SCIENCE, *supra* note 36, at 68.

[74] Matthew Hancock, U.K. Minister of State for Digital and Culture, has called for the use of blockchain to track utilization of research grants, while George Galloway, London mayoral candidate, called for a "blockchain budget" (but ultimately lost the election). *See* Gautham, *Transparent Governance and the End of Corruption with Blockchain Technology*, NEWS BTC (June 20, 2016, 5:30 PM), http://www.newsbtc.com/2016/06/20/transparent-governance-and-the-end-of-corruption-with-blockchain-technology/.

[75] Gideon Greenspan, *Avoiding the Pointless Blockchain Project*, MULTICHAIN (Nov. 22, 2015), http://www.multichain.com/blog/2015/11/avoiding-pointless-blockchain-project/.

How can governments do this better? The first step is to understand the problem. Richard Gendal Brown, Chief Technology Officer of R3 Corda, writes: "Solutions based on selecting the design first and then trying to apply it to arbitrary problems never work out well. Every successful project I've worked on started with the *requirements*, not some cool piece of technology."[76]

In the anti-corruption context, such an exercise requires first being clear about what, exactly, policymakers mean by "corruption" and what causes it. This is a basic step that much of the existing writing on blockchain and anti-corruption fails to take. Among public integrity practitioners and academics, one commonly-used definition of corruption, proffered by Transparency International, a leading anti-corruption organization, is "the abuse of entrusted power for private gain."[77] This definition provides a starting point.

While defining corruption is actually relatively easy, pinpointing its causes often requires a nuanced and context-specific analysis. That said, academics focusing on public integrity have developed some basic frameworks, as well as a growing body of empirical literature. At a simple level, corruption is a relatively easy problem to abstract: the public needs a government to provide public goods, collect taxes to pay for them, regulate markets, and perform a range of other duties. To complete these tasks, governments must hire thousands of workers, each performing duties of varying degrees of complexity. In many cases, such workers have broad discretion in the execution of their duties and have access to a great deal of public money, act as gatekeepers to vital licenses or resources, and have the ability to direct the coercive power of the state. Ideally, public officials would all faithfully perform their duties, but in reality, power sometimes comes with the temptation of personal enrichment. In theory, the public could prevent such misappropriation by monitoring government officials, but such vigilance is impractical in large governments, not least because most members of the general public have their own jobs or families about which to worry. Hence, in many places, corruption abounds.

This phenomenon is known formally as the "principal-agent" problem: the public (the "principal") entrusts execution of key tasks to public officials ("agents"), whom it cannot perfectly monitor. The challenge is to design a government that brings the interests of the principal and agent back into alignment either by changing systems

[76] Brown, *supra* note 31.

[77] *What is Corruption?*, TRANSPARENCY INTERNATIONAL, http://www.transparency.org/what-is-corruption/#define (last visited Nov. 20, 2018).

and power structures to reduce the temptation to cheat or through better monitoring that ensures rogue agents get caught.[78] An alternative but analogous formulation of this problem, put forth by Robert Klitgaard, says that corruption is a function of "M + D – A," which stands for an individual's monopoly power ("M"), his or her discretion to use that power ("D"), and the level of accountability for the individual's actions ("A").[79]

Applying such frameworks to public integrity, the challenge for policymakers considering DLTs is to identify where and when DLTs can help address the principal-agent problem by reducing discretion, either through automation and immutability of records, or by improving the monitoring of officials' actions through replicated ledgers. In making that determination, policymakers need to answer several critical questions.

First, will DLTs actually solve the problem? As Part IV will discuss, not all problems are solvable through information technologies. For instance, while DLTs can help to protect records that have already been created, they are of little use in ensuring the integrity of the underlying data. Consider the example of traffic enforcement: if a police officer pulls over a citizen for speeding, he or she can use a DLT to record the fine. Since records in properly-run DLTs can never be deleted, the DLT can help to prevent other officials from extracting bribes to make the problem "go away." The DLT can also be used to track the identities of all public officials who play roles in shepherding the case through the justice system, including judges responsible for adjudicating disputes and officials responsible for collecting fines. Nonetheless, the DLT cannot guarantee that the citation is for good cause, that it is resolved through formal channels, or that public funds are managed properly.[80] In many contexts, such a function represents a necessary

[78] *See* ROBERT KLITGAARD, CONTROLLING CORRUPTION 10-12 (1988). *See generally* JEAN-JACQUES LAFFONT & DAVID MARTIMORT, THE THEORY OF INCENTIVES (2002) (providing a comprehensive treatise on incentive theory and its applications to the principal-agent problem).

[79] Robert Klitgaard, *International Cooperation Against Corruption*, 35 FIN. & DEV. 3, 4 (Mar. 1998). *But see* Matthew Stephenson, *Klitgaard's Misleading "Corruption Formula"*, GLOBAL ANTI-CORRUPTION BLOG (May 27, 2014), https://globalanticorruptionblog.com/2014/05/27/klitgaards-misleading-corruption-formula/ (arguing that, while this formula may often be true, it is not always true—and it may be misleading in its seeming simplicity).

[80] VT. SEC'Y OF STATE, *supra* note 15, at 9-10. Of course, that is not to say that other technological approaches cannot help here. Automation of passport control stations, deployment of police body cameras, and application of advanced statistical techniques prove promising. Those ideas, however, are well beyond the scope of this study.

if not independently significant condition for cleaning up traffic enforcement.

Second, even if DLTs will help, what else needs to be in place in order to harness those potential benefits? For example, electronic procurement systems, whether enabled by DLTs or not, only reduce corruption if the systems' rules are properly designed and if credible accountability mechanisms are put into place, including a realistic threat of prosecution.[81] Likewise, a DLT-based open contracting platform will only increase accountability if there is an active civil society willing and able to review the records, identify instances of fraud, and voice their concerns in ways that lead to action.[82]

Third, even if DLTs will work, are they cost-effective? Such an analysis should consider not just determinate factors like the up-front investment required and expected operational costs, but also the risks inherent in applying new and as-yet unproven technologies.[83] Choosing an established, non-DLT solution, if one exists, is likely easier, cheaper, and less risky.[84] Applying DLTs to new use cases may entail lengthy proofs of concept and piloting before full deployment. That said, there are some benefits to pushing the frontiers of DLTs' applications, including greater availability of philanthropic funding for first-movers, as well as the greater potential for public acclaim and political capital that comes with doing something novel.

Finally, another factor to consider is whether DLTs may benefit the government in other ways. For instance, digitizing and automating disbursement of public benefits has the potential to limit not just corruption, but also fraud and error,[85] while safeguards built

[81] Glenn T. Ware et al., *Corruption in Public Procurement*, *in* THE MANY FACES OF CORRUPTION 295, 318-319 (J. Edgardo Campos & Sanjay Pradhan eds., 2007), https://openknowledge.worldbank.org/handle/10986/6848.

[82] *See infra* Section IV.A.2.

[83] Greenspan, *supra* note 75.

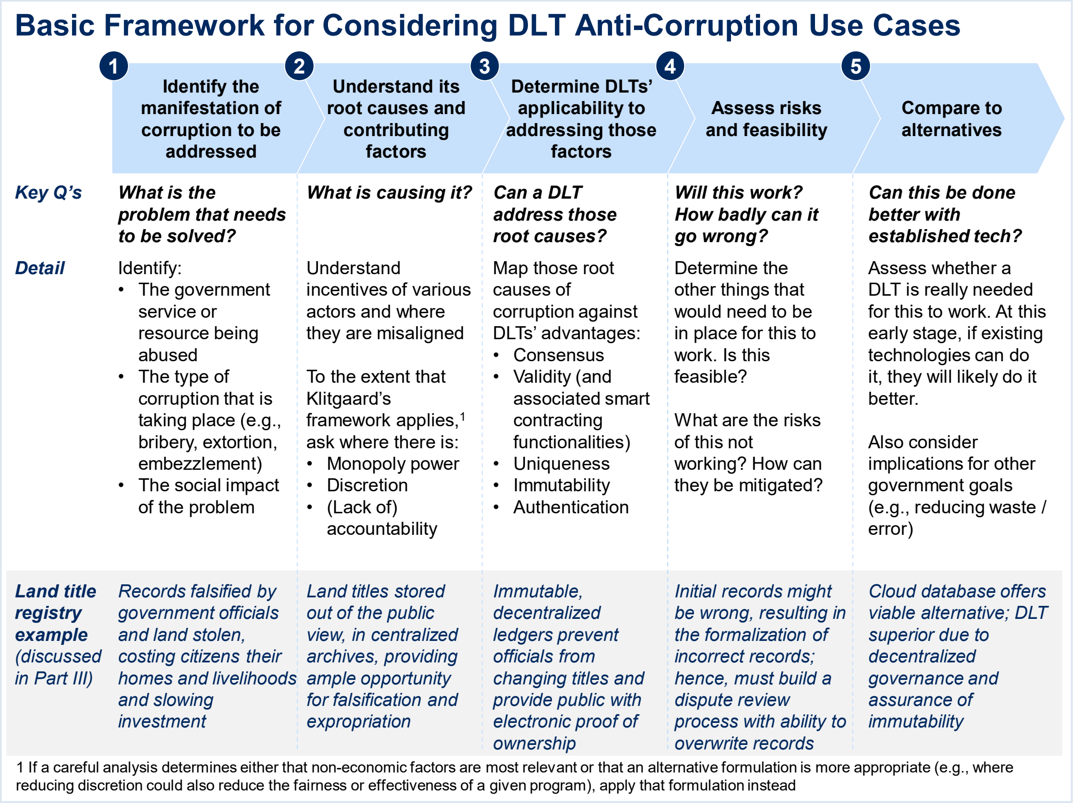
[84] *Id.* ("If your requirements are fulfilled by today's relational databases, you'd be insane to use a blockchain. Why? Because products like Oracle and MySQL have decades of development behind them. They've been deployed on millions of servers running trillions of queries. They contain some of the most thoroughly tested, debugged and optimized code on the planet, processing thousands of transactions per second without breaking a sweat. And what about blockchains? Well, our product was one of the first to market, and has been available for exactly 5 months, with a few thousand downloads. . . . [T]his entire product category is still in its diapers.")

[85] *See, e.g.*, GOVERNMENT OFFICE FOR SCIENCE, *supra* note 36, at 67 (outlining the case for DLTs in the British Department for Work and Pensions, quantifying potential value in terms of fraud, claimant error, and official error, all of which can be solved using the same technological solution).

into public financial management systems may protect simultaneously against corruption and hacking. For example, a hacker succeeded in breaking into Kenya's financial management system and falsifying contracts but was not able to collect funds due to a safeguard requiring a second official to sign off prior to disbursement.[86]

Upon answering these questions, policymakers should have a reasonably clear grasp of how DLTs can help in the fight against corruption. Figure 2 below arranges the questions chronologically and provides a five-part decision framework for policymakers to use as a checklist for considering potential DLT use cases.

Figure 2 – Five-Step Framework for Considering DLT Use



Basic Framework for Considering DLT Anti-Corruption Use Cases

	1 Identify the manifestation of corruption to be addressed	2 Understand its root causes and contributing factors	3 Determine DLTs' applicability to addressing those factors	4 Assess risks and feasibility	5 Compare to alternatives
Key Q's	***What is the problem that needs to be solved?***	***What is causing it?***	***Can a DLT address those root causes?***	***Will this work? How badly can it go wrong?***	***Can this be done better with established tech?***
Detail	Identify: • The government service or resource being abused • The type of corruption that is taking place (e.g., bribery, extortion, embezzlement) • The social impact of the problem	Understand incentives of various actors and where they are misaligned To the extent that Klitgaard's framework applies,[1] ask where there is: • Monopoly power • Discretion • (Lack of) accountability	Map those root causes of corruption against DLTs' advantages: • Consensus • Validity (and associated smart contracting functionalities) • Uniqueness • Immutability • Authentication	Determine the other things that would need to be in place for this to work. Is this feasible? What are the risks of this not working? How can they be mitigated?	Assess whether a DLT is really needed for this to work. At this early stage, if existing technologies can do it, they will likely do it better. Also consider implications for other government goals (e.g., reducing waste / error)
Land title registry example *(discussed in Part III)*	*Records falsified by government officials and land stolen, costing citizens their homes and livelihoods and slowing investment*	*Land titles stored out of the public view, in centralized archives, providing ample opportunity for falsification and expropriation*	*Immutable, decentralized ledgers prevent officials from changing titles and provide public with electronic proof of ownership*	*Initial records might be wrong, resulting in the formalization of incorrect records; hence, must build a dispute review process with ability to overwrite records*	*Cloud database offers viable alternative; DLT superior due to decentralized governance and assurance of immutability*

1 If a careful analysis determines either that non-economic factors are most relevant or that an alternative formulation is more appropriate (e.g., where reducing discretion could also reduce the fairness or effectiveness of a given program), apply that formulation instead

[86] *See* John Max, *IFMIS System Hacked and How Over KSHS 800,000,000 Fictitious Contracts Were Almost Approved*, TECHSAHARA (June 22, 2015), http://techsahara.com/ministry-of-devolution-ifmis-system-hacked-and-how-over-kshs-800000000-fictitious-contracts-were-almost-approved/.

IV. Promising Applications of DLTs in the Fight Against Corruption

Since distributed ledger technology is still in its infancy, and since its applicability to the fight against corruption remains largely unproven, practitioners should iteratively apply the framework discussed in Part III as new developments occur. At the same time, early uses of DLTs already indicate that three use cases are ripe for exploration. Each of these deploys a different combination of features of the blockchain bundle, enabling reform in a way that simply was not possible prior to the advent of DLTs. This Part will explore each of those three applications in detail, as well as the potential risks that require careful mitigation—and may, in some cases, stand in the way of DLT adoption. The first potential use case is the safeguarding of private rights by creating immutable, distributed registries. Those registries may track land ownership, copyrights, vehicle registration and titles, entitlement eligibility, or other records. Second, DLTs can enhance the stewardship of public resources by making it easier to trace the flow and allocation of public resources and by automating routine decisions. Third, private sector DLTs can address the "demand" side of corruption by automating payment of taxes and tariffs and by improving private-sector record-keeping, which can then be cross-referenced against government records to identify potential instances of fraud or corruption.

A. Three Use Cases

1. Safeguarding Individual Entitlements and Rights

> When the Honduran police came to evict her in 2009, Mariana Catalina Izaguirre had lived in her lowly house for three decades. Unlike many of her neighbours in Tegucigalpa, the country's capital, she even had an official title to the land on which it stood. But the records at the country's Property Institute showed another person registered as its owner, too—and that person convinced a judge to sign an eviction order. By the time the legal confusion was finally sorted out, Ms. Izaguirre's house had been demolished.
>
> It is the sort of thing that happens every day in places where land registries are badly kept, mismanaged and/or corrupt—which is to say across much of the world. This lack of secure

> property rights is an endemic source of insecurity and injustice. It also makes it harder to use a house or a piece of land as collateral, stymying investment and job creation.[87]

For many living in the world's poorest countries, uncertainty is a fact of life. Geopolitical instability, economic volatility, and unreliable basic services all conspire to ensure that long-term planning is difficult, if not impossible. For Peruvian economist Hernando de Soto, this is a vicious cycle, both resulting from and contributing to poverty:

> Of the 7.3 billion people in the world, only two billion have a title that is legal and effective and public regarding their control over an asset. . . . [W]hen something is not legally on record as being owned, it can therefore not be used . . . as collateral to get credit, as a credential that you can be able to transfer part of your property to invite investment in. Things are owned, but when they're not adequately paperized or recorded, they cannot fill the functions of creating capital and credit.[88]

This problem typically traces its roots to more than mere public mismanagement. In many cases, dishonest politicians, government officials, and businesspersons profit behind the scenes.

Honduras provides an interesting case study both in how land registries can become tools for corruption and in how technological solutions may be limiting absent broader political reform. In 2014, Asociación por una Sociedad más Justa (ASJ), Transparency International's Honduran partner, published a report that revealed how politicians had been using offers of land titles to buy votes from impoverished citizens. They sold plots of desirable land to the wealthy in exchange for bribes and took advantage of the ten-month land title processing time to further extract rents from citizens. In one case, an official accepted a bribe to clear a title in a mere two

[87] *The Great Chain of Being Sure About Things*, ECONOMIST (Oct. 31, 2015), http://www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable (providing early coverage of Honduras' blockchain initiative).

[88] Laura Shin, *Republic of Georgia to Pilot Land Titling on Blockchain with Economist Hernando De Soto, BitFury*, FORBES (Apr. 21, 2016, 6:00 PM), https://www.forbes.com/sites/laurashin/2016/04/21/republic-of-georgia-to-pilot-land-titling-on-blockchain-with-economist-hernando-de-soto-bitfury/#5ba9f8444da3.

hours.[89] In Honduras, this report led to understandable public outrage and put pressure on the government to act.

This pressure created a window of opportunity for Factom, an Austin-based blockchain startup, which met with government officials and proposed the conversion of public land registries to a DLT. To Peter Kirby, Factom's then-CEO, corruption involving land titles was purely a technological problem. Referring metaphorically to the country's paper-based registries, he said: "In the past, Honduras has struggled with land title fraud. . . . [T]he country's database was basically hacked. So bureaucrats could get in there and they could get themselves beachfront properties."[90] Kirby and his team believed that blockchain could solve the entire problem. Don Tapscott, in *The Blockchain Revolution*, summarizes their reasoning:

> Here's how it works: the blockchain is an open ledger, meaning that it could reside on the desktops of the Honduran officials who needed to reference it, the mobile devices of field workers who input data, and citizens who want to maintain a copy. It's a distributed ledger, meaning that none of the parties owns it, and it's a P2P network, meaning that anybody could access it. In jurisdictions like Honduras, where trust is low in public institutions and property rights systems are weak, the bitcoin blockchain could help to restore confidence and rebuild reputation.[91]

To Kirby and others, blockchain could do more than just solve land rights in Honduras: it could also help the country to "leapfrog systems built in the developed world," later putting those same tools to use to secure mortgages, contracts, and even mineral rights.[92] By May of 2015, Reuters reported that Factom had entered into an agreement with the Honduran government to create the database,[93]

[89] *Honduras: Beating Corruption in Land Registration*, TRANSPARENCY INT'L (Aug. 21, 2014), http://www.transparency.org/news/feature/honduras_beating_corruption_in_land_registration (summarizing the longer Spanish-language report from ASJ).

[90] Gertrude Chavez-Dreyfuss, *Honduras to Build Land Title Registry Using Bitcoin Technology*, REUTERS (May 15, 2015, 12:28 PM), http://in.reuters.com/article/usa-honduras-technology-idINKBN0O01V720150515.

[91] TAPSCOTT & TAPSCOTT, *supra* note 5, at 197.

[92] Chavez-Dreyfuss, *supra* note 90 (citing Factom's then-CEO Peter Kirby).

[93] *Id.*

a report that Factom later reproduced on its own website.[94] Honduras, it seemed, was well on its way to eradicating corruption.

There was a big problem, however: the agreement did not exist. June and July passed with no further updates on the project. It took until December of that year for Kirby to finally admit that the project would not move forward.[95] Since then, Honduras appears to have made no meaningful attempts to transition its land registries to DLTs or to address the underlying grievances behind the country's land disputes. Uninvolved parties may never know exactly what caused the Honduras project to fall through or why both sides failed to correct the record for so long, but a purported transcript of an online chat between an anonymous user and Factom's then-Chief Architect and current CEO, Paul Snow, offers some clues. According to Snow, Reuters "jumped the gun" with its report of an agreement, but when Factom's executives spoke with their contacts in the Honduran government, the Hondurans asked Factom not to correct the record: "[T]hey preferred us to let it lie than to try and fix it."[96] Factom would subsequently post the Reuters announcement on its website and then refrain from correcting both the Reuters report and the multiple reports that followed until four months after the fact.

In this case, both sides had much to gain from keeping up the appearance of a collaboration even while doing little. [97] Factom was able to assuage concerned investors by pointing to a willing client, and the Honduran government was able to create the appearance of reform all while doing little to actually address the problem. This story provides a lesson for others considering deploying DLTs in the fight against corruption—ensure that those involved in the initiative are not themselves corrupt.

Another lesson is the naivety of thinking that technology alone can solve a problem as deeply-rooted as Honduran land rights. As MIT researchers Chelsea Barabas and Ethan Zuckerman wrote in *The Atlantic*:

[94] *See Articles, industry reports, videos and podcasts featuring Factom®*, FACTOM: NEWS, https://www.factom.com/company/news/ (last visited Jan. 9, 2019) (maintaining a long list of hyperlinks to third-party publications discussing Factom, including the Reuters report, dated May 15, 2015, in that list).

[95] Peter Kirby, *A Humble Update on the Honduras Title Project*, FACTOM (Dec. 25, 2015), https://www.factom.com/blog/a-humble-update-on-the-honduras-title-project.

[96] JP Buntinx, *Factom Purposefully Twisted the Truth Regarding Deal with Honduran Government*, BITCOINIST, (Dec. 25, 2015, 5:15 AM), https://bitcoinist.com/factom-purposefully-twisted-the-truth-regarding-deal-with-honduran-government/.

[97] *Id.*

> [U]sing the blockchain to "solve" land-title problems rests on a shallow, incomplete understanding of the challenge at hand. The complexities of how land titles are managed in developing countries is the result of long-standing conflicts between grassroots communities, their governments, and large multinational corporations. By assuming the problem is mainly about bureaucratic inefficiencies and paper-based processes, Bitcoin enthusiasts ignore the hardest part of the situation: long-standing conflicts over rights and power. Sadly, the focus on documentation via blockchain overlooks the key insights we can learn from de Soto's work: that land rights struggles are a high-touch, long-term issue.[98]

In this sense, perhaps Honduras was always the worst place to attempt to use DLTs for land records, where land conflicts between campesinos and plantation owners have been called the "most intense agrarian conflict seen in Central America in the last 15 years."[99] These long-simmering tensions set the backdrop for the more immediate crisis of ASJ's damning report and the resulting public protest. Under such conditions, it appears that Factom may have offered a convenient smokescreen for government officials who had no intention of changing the corrupt practices they relied on for their political backing. It seems clear that, at the very least, well-intentioned entrepreneurs, donors, or non-profits should ensure that they have a trustworthy champion in government who has the authority to ensure that the project moves forward.

Since then, other attempts at blockchain registries have had significantly more success. In Ghana, Bitland Global appears to have found an eager partner in the country's Land Administration Project, a joint initiative of Ghana's Lands Commission and the World Bank. Bitland Global has approached this project with more humility and with an emphasis on partnership with a government that appears genuinely willing to shepherd the initiative along. "Since Ghana has been trying to solve this problem, it's a natural place to start trying to implement these types of solutions," says Bitland's Chief Security Officer.[100] Bitland has also taken a more cautious approach: rather

[98] Chelsea Barabas & Ethan Zuckerman, *Can Bitcoin Be Used For Good?*, ATLANTIC (Apr. 7, 2016), https://www.theatlantic.com/technology/archive/2016/04/bitcoin-hype/477141/.

[99] *Honduran Movements Slam Campesino Repression in Land Fight*, TELESUR (June 25, 2015), http://www.telesurtv.net/english/news/Honduran-Movements-Slam-Repression-of-Campesinos-in-Land-Fight-20150625-0011.html.

[100] Roger Aitken, *Bitland's African Blockchain Initiative Putting Land on the Ledger*, FORBES (Apr. 5, 2016, 2:44 PM), https://www.forbes.com/

than opt for a nationwide launch, they have started with a pilot in twenty-eight communities, allowing them to ensure that the technology works and that the integrity of public record-keeping actually improves before they make a significant investment. Finally, rather than international technologists helicoptering in to "solve" a deeply-rooted problem, Bitland is led by a Ghanaian businessman with a clearer understanding of the country's opportunities and challenges.[101] As of this Article's writing, Bitland has been operating throughout Ghana and has received acclaim for its success in addressing the problem of land ownership.[102]

Bitfury's collaboration with the Ukrainian government shows similar promise, with the post-revolution government determined to continue the momentum brought about by recent reforms[103] and to build upon the credibility gained through ProZorro, an open contracting platform that has already saved the government hundreds of millions of dollars in averted waste and abuse.[104] This initiative will eventually cover more than just land registries, with initial pilots being explored in "state registers, public services, social security, public health, and energy."[105]

Building off the lessons of Honduras, Ghana, and Ukraine, it seems clear that, under the right circumstances, there is a viable use case for DLTs in improving public record-keeping related to land titles. However, DLTs can be used to secure other types of government registries as well. Kausik Rajgopal, head of McKinsey's payments practice summarizes: "Documentation for ownership from

sites/rogeraitken/2016/04/05/bitlands-african-blockchain-initiative-putting-land-on-the-ledger/#79f0ca917537 (quoting Bitland Global CSO Larry Christopher Bates). *See also* L. CHRIS BATES, BITLAND GLOBAL WHITEPAPER (2016), http://www.bitland.world/wp-content/uploads/2016/03/Bitland_Whitepaper.pdf (detailing the plan for Ghana's blockchain land registry).

[101] Narigamba Mwinsuubo, LINKEDIN, https://www.linkedin.com/in/narigamba/?ppe=1 (last visited Nov. 20, 2018) (identifying Mr. Mwinsuubo as Founder and CEO of Bitland Global).

[102] *See The 50 Most Genius Companies of 2018*, TIME.COM (2018), http://time.com/collection/genius-companies-2018 (last visited Jan. 9, 2019) (lauding Bitland's work on securing land rights in seven African nations, plus India).

[103] For an overview of ongoing reform efforts in Ukraine, see *Reforming Ukraine*, CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE, http://carnegieendowment.org/specialprojects/Ukraine/ (last visited Nov. 20, 2018).

[104] *See* discussion *infra* Section IV.A.2.

[105] Gertrude Chavez-Dreyfuss, *Ukraine launches big blockchain deal with tech firm Bitfury*, REUTERS (Apr. 13, 2017, 1:35 AM), https://www.reuters.com/article/us-ukraine-bitfury-blockchain/ukraine-launches-big-blockchain-deal-with-tech-firm-bitfury-idUSKBN17F0N2.

patents to houses is extraordinarily paper-based, and there's no reason it should be, other than history. Blockchain works with any transaction or interaction where property rights and timing matters [sic]."[106] Initial pilots seem to suggest that, provided the right political preconditions, a valid use case for DLTs can exist wherever establishing ownership is important, the temptation for corruption is present, and the potential to streamline transactions exists.

Of course, DLTs are not the only option for digitizing public registries, although they are often the best. For instance, while governments could simply digitize their land registries and publish them online, thereby achieving "consensus" regarding the state of a ledger at a given time, such a solution would not assure immutability. Unless somebody was regularly matching copies of the ledger against previous versions (or created a script to do this automatically), changes could go undetected. Even if such regular review was being conducted, any errors would likely be discovered too late to stop invalid changes from taking place and could take years to reverse. Finally, use of a blockchain ensures that there is no "super-user" lurking behind the scenes, capable of changing or deleting records without anyone noticing, as digital key-based authentication ensures that any actions that do take place can be traced back to individual key-holders.

Of course, this is not to say that DLTs are a panacea for public record-keeping. For this to work, people must be able to access those records. In many countries, and particularly in rural areas, access requires significant investment in technology and connectivity. It also requires investment in a public-key infrastructure and education on how to use and secure such keys. Finally, careful foresight and planning are needed to ensure that the DLTs are designed with the flexibility to reflect changing legal regimes, court orders, or other legitimate government actions.

2. Reforming Government Processes

As the prior subsection has outlined, one potential use for DLTs is the protection and transfer of *private rights*, but what about stewardship of *public resources*? For public management, two features of DLTs stand out: consensus and validity. DLTs' consensus-generating properties can allow for radical transparency of resource flows throughout the government in ways that would normally require either official audits or lengthy freedom-of-information requests. DLTs' validation mechanisms, meanwhile, can

[106] TAPSCOTT & TAPSCOTT, *supra* note 5, at 197.

enable smart contracts that limit official discretion over routine decisions, thus reducing the possibility of fraud or theft.

Unlike with land titles, there are few case studies proving that these applications can work. Nonetheless, we can draw lessons from blockchain experts' discussions of the technology's potential and from similar attempts to apply transparency and automation to public resources prior to the advent of DLTs. This subsection will first discuss past initiatives aimed at increasing government transparency and automation and then outline how DLTs can enhance such efforts.

a. Managing Public Resources—Increasing Transparency

Under the formulation of corruption as a principal-agent problem, where the "principal" is broadly defined as the "public" and the "agent" as a given public official, one root of the problem is the difficulty in monitoring the agent's day-to-day activities.[107] It follows, then, that innovations aimed at improving such monitoring may be able to reduce corruption. In some cases, that monitoring can take place within government, while in others, civil society must be engaged. As for internal monitoring, many governments have at least some form of internal controls aimed at spotting and addressing instances of waste and fraud from within.[108] Often, legislatures, independent executive agencies, the judiciary, or civil society supplement such monitoring with their own external audits.[109] Civil society in particular can play a role in improving government integrity (or, at least, the public's perception of government integrity), with increased oversight generally correlating with improved scores on Transparency International's Corruption Perception Index.[110] One key to enabling this citizen participation is to ensure adequate granularity, reliability, and frequency of relevant reporting.[111]

[107] *See* Matthew Stephenson, *Corruption is BOTH a "Principal-Agent Problem" AND a "Collective Action Problem"*, GLOBAL ANTICORRUPTION BLOG (Apr. 9, 2015), https://globalanticorruptionblog.com/2015/04/09/corruption-is-both-a-principal-agent-problem-and-a-collective-action-problem/.

[108] *See generally* William Dorotinksy & Shilpa Pradhan, *Exploring Corruption in Public Financial Management*, *in* THE MANY FACES OF CORRUPTION: TRACKING VULNERABILITIES AT THE SECTOR LEVEL 267 (J. Edgardo Campos & Sanjay Pradhan eds., 2007), https://openknowledge.worldbank.org/handle/10986/6848 (outlining sources of corruption in public fiscal management).

[109] *Id.* at 276.

[110] *Id.* at 281.

[111] *Id.* at 280.

Case studies abound of open government's effectiveness in increasing public accountability and rooting out corruption. Perhaps the most inspiring story is that of Ukraine's ProZorro. Previously, officials estimated that corruption in procurement resulted in at least a twenty percent premium on Ukrainian government purchases.[112] ProZorro, a centralized open contracting platform, was designed to change that. ProZorro publicizes data on the entire procurement process (from planning all the way to post-completion payment), placing it in a searchable online portal. The site integrates various accountability-driven tools, including a business intelligence tool to spot issues in tender data, a complaints mechanism, and even an information portal on Ukrainian procurement law and policy.[113]

Watchdog groups like Transparency International, as well as Ukrainian journalists, have been using ProZorro to spot suspicious contracts, resulting in several high-profile discoveries. In one case, a local journalist discovered that healthcare facilities were attempting to circumvent the e-procurement system by tailoring terms of reference to advantage certain suppliers. Most notably, one oncology center purchased cleaning mops for $100 per unit under the description "a device with a nozzle and a holder."[114] ProZorro's initial pilot was so successful that the Ukrainian Parliament later passed a public procurement law requiring that all government contracting be carried out via ProZorro; the platform has saved government more than $200 million.[115]

Unlike those seeking to "hack" corruption, ProZorro's team appears aware of their project's limitations. Max Nefyodov, one of the project leaders, offers his perspective:

> Corruption involves an unethical choice of a person who works in the tender committee. No I.T. program in the world can completely save this situation. What we're doing is actually giving more instruments to [monitor] these people, we're giving less subjectivity to the decisions, we're encouraging more bidders to decrease the risk of collusion, we're making the complaints process easier, we're training people, we're making central purchasing bodies, we're

[112] *See* Open Contracting Partnership, '*Everyone Sees Everything' – Overhauling Ukraine's Corrupt Contracting Sector*, MEDIUM (Nov. 28, 2016), https://medium.com/open-contracting-stories/everyone-sees-everything-fa6df0d00335 (telling the story behind ProZorro).

[113] *Id.*

[114] *Id.*

[115] *Id.*

> making typical specifications of what is being acquired, we're building risk management systems, and so on.[116]

Similar open-contracting initiatives are underway in other countries, often under the guidance of the Open Contracting Partnership, a global NGO that provides technical assistance, promotes collaboration, and publishes data standards to facilitate transparency in government.[117] Other open-contracting initiatives under the auspices of this partnership have proven similarly impactful, as when Mexican newspaper *Milenio* discovered through the country's open-contracting platform, Compranet, that President Vincente Fox's Chief of Staff had purchased $500 towels for the presidential palace.[118] Outside public procurement, open-data initiatives have generally shown promise in improving public accountability in sectors ranging from education[119] to mining royalties.[120]

Of course, just making data public does not guarantee better outcomes. For accountability to occur, there must also be principals interested in ensuring positive outcomes. Those principals must view the information being shared as important, and the information must be readily available to them.[121] Finally, there must be some mechanism through which change can occur, be it through the principals' own actions, through support from senior officials within government, or through some coordinated action that generates such support.[122] Where that concerned constituency is broad rather than concentrated, collective action can prove challenging, but not

[116] *Id.*

[117] *About*, OPEN CONTRACTING PARTNERSHIP, http://www.open-contracting.org/about/ (last visited Oct. 19, 2018).

[118] Julia Scheeres, *Mexico Wants an E-Revolution*, WIRED (Feb. 25, 2002), http://archive.wired.com/techbiz/media/news/2002/02/50622.

[119] For instance, Mejora Tu Escuela is a Mexican online platform used to track school performance and spending. It was recently used to find that 1512 teachers on public school payrolls were more than 100 years old and that some made more than the president of Mexico. STEFAAN VERHULST & ANDREW YOUNG, THE GLOBAL IMPACT OF OPEN DATA 198 (2016), http://www.oreilly.com/data/free/the-global-impact-of-open-data.csp.

[120] Consider, for instance, Where My Money Dey?, a website which allows communities to track mining royalties owed to them, relative to what they have actually been paid. *Where My Money Dey?*, CODEFORAFRICA.ORG, http://wmmd.codeforafrica.org/ (last visited Oct. 19, 2018).

[121] Vanessa Williamson & Norman Eisen, *The Impact of Open Government: Assessing the Evidence* 2 (Brookings Ctr. for Effective Pub. Mgmt., Working Paper, 2016), https://www.brookings.edu/wp-content/uploads/2016/12/gs_20161208_opengovernment_report.pdf.

[122] *Id.*

impossible.[123] In any case, transparency initiatives should either tap into existing constituencies or "endogenously build large constituencies against corruption made up of 'the shareholders of the public administration,' that is, citizens and taxpayers who will help the media and the judicial system to identify cases of corruption."[124]

b. Managing Public Resources—Reducing Discretion in Routine Activities

Monitoring alone will rarely be sufficient to solve corruption, since governments are far too complex for principals to obtain perfect information about the comings and goings of all agents, at all times. In some cases, a better idea may be to reduce the power entrusted to agents to begin with, by automating routine decisions (i.e., the "D" in Klitgaard's "C = M + D – A" formula).[125] For instance, electronic tax payments can reduce the threat of distortion, automated traffic enforcement can reduce the possibility of bribery of corrupt police officers, and RFID tags at ports of entry can automate the calculation of customs duties and prevent fraud.[126] Automation can also ensure that the required steps are followed prior to a transaction or change in records, reducing a rogue official's ability to undercut approval processes[127] or directly modify documents.[128] However, automation also has its limits. Pure automation will never be ideal. For instance, there are scenarios

[123] Stephenson, *supra* note 107.

[124] Gustavo Piga, *A Fighting Chance Against Corruption in Public Procurement?*, *in* 2 INTERNATIONAL HANDBOOK ON THE ECONOMICS OF CORRUPTION 141, 142 (Susan Rose-Ackerman & Tina Søreide eds., 2011).

[125] *See* Klitgaard, *supra* note 79.

[126] SUSAN ROSE-ACKERMAN & BONNIE J. PALIFKA, CORRUPTION AND GOVERNMENT: CAUSES, CONSEQUENCES, AND REFORM 144 (2d ed. 2016).

[127] *See* Chris Matten & Chay Yiowmin, *The Changing Treasury: Optimal Use of Technology*, PWC EDGE (2007), http://www.pwc.com/sg/en/financial-services/assets/publication-treasury200704.pdf (outlining how automation can help with corporate treasury controls and approvals); *see also IFMIS System Hacked and How Over Kshs 800,000,000 Fictitious Contracts Were Almost Approved*, TECHSAHARA (June 22, 2015), http://techsahara.com/ministry-of-devolution-ifmis-system-hacked-and-how-over-kshs-800000000-fictitious-contracts-were-almost-approved/ (recounting how hackers were able to break into the Kenyan financial management system but, importantly, were not able to receive disbursed funds due to the system's requirement for approval from an officer whose account was not yet compromised).

[128] Piga, *supra* note 124, at 164 (discussing how changing prices by modification of tender offers has gone "increasingly out of fashion thanks to secure IT" in the context of public procurement).

where all the factors behind a decision are hard to foresee ex ante, as with procurement of more complex items like weapons systems;[129] regulation of sectors with changing practices or technologies; or administration of public benefits, where adherence to rigid formulae could cause irreversible harm and run afoul of constitutional protections.[130]

c. What DLTs Can Offer

Even before DLTs, governments had found ways to increase automation and transparency, and many reform efforts in the future will similarly forego such technologies. That said, DLTs can help by significantly easing implementation of such initiatives, increasing their scale, decreasing costs, creating finely-tuned access controls, and decreasing the potential for tampering. Here, DLTs' consensus and validity features do most of the work.

Most importantly, DLTs can provide instant visibility into the status of money or other assets traveling through the government bureaucracy, as well as how grants are spent by their ultimate recipients.[131] Centralized IT projects like ProZorro can do this too, but they do it by replicating all of this information into one massive centralized database, which is both time-consuming and prone to failure and hacking. A DLT can be much cheaper and less risky.[132]

DLTs can also increase the granularity of data. For instance, a combination of cryptocurrencies and smart contracts can facilitate

[129] *See, e.g.*, JOHN M. WALTON ET AL., NGIP: THE INSTITUTE FOR PUBLIC PROCUREMENT, BEST VALUE IN GOVERNMENT PROCUREMENT 3 (2013), https://www.nigp.org/docs/default-source/New-Site/position-papers/150105_best-value_position-paper-complete_updated.pdf?sfvrsn=4 ("Because of the danger in oversimplifying all the variables, in policy situations like this where one size *does not* fit all, the [optimal] policy defines a process for making decisions and includes standards for accountability."); *see also* Piga, *supra* note 124, at 152 ("If the agent is competent, discretion offers valuable flexibility, especially in complex procurement situations.").

[130] *See generally* Virginia T. Vance, *Applications for Benefits: Due Process, Equal Protection, and the Right to be Free from Arbitrary Procedures*, 61 WASH. & LEE L. REV. 883 (2014), https://heinonline.org/HOL/Page?handle=hein.journals/waslee61&id=893&collection=journals (outlining the U.S. Supreme Court's current approach to applying due process doctrine to public benefits, arguing for a "freedom from procedural arbitrariness" that is grounded in substantive due process, but ultimately concluding that an equal protection claim may be more likely to succeed where traditional procedural due process claims fail).

[131] *See, e.g.*, GOVERNMENT OFFICE FOR SCIENCE, *supra* note 36, at 67-68 (outlining potential use cases in welfare administration and foreign aid delivery).

[132] *Id.*

the creation of dollar-linked "coins" for foreign-aid spending. Coins can be given different "colors" that, in turn, impose different rules on how and by whom they can be used. Aid recipients and intermediaries can receive private keys, which allow them to take possession of and transfer these coins, provided they follow the rules associated with their individual accounts and with the coin types they are given. Each "coin" would be individually traceable, allowing for monitoring all the way to the intended final recipient, who would convert it into the desired currency. Smart contracts can also ensure that such disbursements are done in accordance with program rules and, if required, that the proper documentation or "proof of existence" of such documents is provided first.[133]

Of course, for DLTs to help manage public spending, some prerequisites need to be in place. All users must have access to a private key, knowledge of how to use it, Internet connectivity, and, if needed, a "gateway" for converting that "coin" to actual cash.[134] Even five years ago, these preconditions may not have existed in most parts of the world. Today, however, increased penetration of both mobile phones and mobile payment infrastructure is making use of DLT-based coins more feasible.[135]

Other features of DLTs can help with public financial management as well. For instance, the immutability of records can prevent corrupt officials from covering their tracks, key-based user authentication can trace each action to the responsible party, and decentralized governance and control can prevent a "super-user" from changing the system or its rules without detection. How all of these benefits best come together for a given program is not clear, nor is it obvious when DLTs are superior to existing technologies. Further complicating matters, different types of DLTs may prove superior for different types of records or processes. A technology called "pegged sidechains" can enable multiple DLTs to run side-by-side, allowing for the creation of different DLTs for different objectives.[136]

To summarize the key points from this subsection: DLTs show promise where one needs to track or control the flow of a given item from one end of a process to another. This subsection has shown

[133] *Id.*

[134] *Id.*

[135] *See, e.g.*, *Cell Phones in Africa: Communication Lifeline*, PEW RES. CTR. (Apr. 15, 2015), http://www.pewglobal.org/2015/04/15/cell-phones-in-africa-communication-lifeline/ (discussing the rapid proliferation of mobile phone networks throughout Africa).

[136] ASTRI, *supra* note 16, at 31.

how that might work in the context of public procurement and public fiscal management, but the potential for DLTs is much broader. Pilot programs are already underway, for instance, to track petition signatures[137] and to facilitate e-voting.[138] Where DLTs will go next is still an open question. That may explain why the Ukrainian government's contract with Bitfury covers not just land registries, but also a set of as-yet unidentified use cases (see Section IV.A.1). Reformers in other parts of the world should take a similarly open-minded approach to the use of DLTs as they continue to evolve.

3. Enhanced Private Sector Monitoring and Enforcement

Governments seeking to reduce corruption can often find willing partners in the private sector, as it is in both sides' interests to improve government integrity. The private sector, like governments, may also want to use DLTs to keep track of products and reduce the potential for fraud. Private industry has already taken the lead in this area. For example, IBM has partnered with Chinese supply chain manager Hejia to create a trade finance platform for pharmaceuticals.[139] Everledger is fighting diamond insurance fraud through a combination of laser inscriptions and a DLT history that tracks the diamonds' movement from owner to owner.[140] Maersk and IBM have partnered to create a blockchain system for managing cargo.[141] Finally, Provenance has created a blockchain that can be used by both consumers and companies to track products through

[137] For example, Mudamos, a blockchain-based smartphone app, enables Brazilian voters to electronically sign petitions that would create draft bills on which the Brazilian Congress must vote. *See* Ronaldo Lemos, *Using the Blockchain for the Public Interest*, MEDIUM (Oct. 31, 2016), https://medium.com/positive-returns/using-the-blockchain-for-the-public-interest-2ed1f5114036.

[138] For example, BitCongress is a proposed blockchain-based platform for legislation and voting. *See* Morgan Rockwell, *BitCongress – Process for Blockchain Voting & Law*, http://docplayer.net/31500366-Bitcongress-process-for-blockchain-voting-law.html (last visited Nov. 24, 2018).

[139] *IBM is Going All In on Blockchain for Trade Finance*, BUS. INSIDER (Apr. 12, 2017, 12:30 PM), http://www.businessinsider.com/ibm-is-going-all-in-on-blockchain-for-trade-finance-2017-4.

[140] Marc Prosser, *Today Corrupt Officials Spend Your Money—Tomorrow Blockchain Will Stop Them*, SINGULARITYHUB (Oct. 20, 2015), https://singularityhub.com/2015/10/20/today-corrupt-officials-spend-your-money-tomorrow-blockchain-will-stop-them/.

[141] David Z. Morris, *Maersk Tests Blockchain-Based Freight Tracking*, FORTUNE (Mar. 5, 2017), http://fortune.com/2017/03/05/maersk-tests-blockchain-based-freight-tracking/.

every step in a supply chain and to ensure that all supply chain actors have used responsible business practices.[142]

Connecting these DLTs to customs or tax authorities and automating regulatory compliance could preempt fraud and corruption. For instance, tax authorities could digitize value-added tax (VAT) payments through the creation of a "VATCoin," which would eliminate the potential for a cash payout to perpetrators of "carousel fraud."[143] Customs authorities could also verify records from trade finance or supply chain DLTs to confirm the accuracy of customs declarations and to collect automated customs payments, reducing the potential for bribery at the border.[144] Streamlining government interactions is, in fact, the whole idea behind the Maersk-IBM blockchain. As *The New York Times* reported:

> For Maersk, the problem was not tracking the familiar rectangular shipping containers that sail the world aboard its cargo ships—instead, it was the mountains of paperwork that go with each container. Maersk had found that a single container could require stamps and approvals from as many as 30 people, including customs, tax officials and health authorities.
>
> While the containers themselves can be loaded on a ship in a matter of minutes, a container can be held up in port for days because a piece of paper goes missing, while the goods inside spoil. The cost of moving and keeping track of all this paperwork often equals the cost of physically moving the container around the world.
>
> What's more, the system is rife with fraud. The valuable bill of lading is often tampered with or copied to let criminals siphon off goods or circulate counterfeit products, leading to billions of dollars in maritime fraud each year.[145]

[142] Luke Parker, *Provenance to Restore Consumer Trust with the Blockchain*, BRAVE NEW COIN (Dec. 4, 2015, 6:30 PM), https://bravenewcoin.com/news/provenance-to-restore-consumer-trust-with-the-blockchain/.

[143] Richard Ainsworth & Musaad Alwohaibi, *Blockchain, Bitcoin, and VAT in the GCC: The Missing Trader Example (Part 2)*, BLOOMBERG BNA (Feb. 2, 2017), https://www.bna.com/blockchain-bitcoin-vat-n57982083240.

[144] Wolfgang Lehmacher & Jesse McWaters, *How Blockchain Can Restore Trust in Trade*, WORLD ECONOMIC FORUM (Feb. 1, 2017), https://www.weforum.org/agenda/2017/02/blockchain-trade-trust-transparency/.

[145] Nathaniel Popper & Steve Lohr, *Blockchain: A Better Way to Track Pork Chops, Bonds, Bad Peanut Butter?*, N.Y. TIMES: DEALBOOK (Mar. 4, 2017),

This blockchain has been designed to be open to everyone who is involved with a shipment and has been developed in consultation with both U.S. and Dutch customs authorities. Each time somebody touches the cargo, a new record is added. Everybody can track the shipment and see its full history, providing a shared set of facts if a dispute arises.[146]

Before DLTs, this type of record-keeping system, spread among so many parties with instant consensus and near-certain immutability, was simply not technologically feasible. One Walmart executive who has spent years trying to better ensure the safety and authenticity of the company's grocery products spoke of learning about DLTs' potential: "I became increasingly convinced that maybe we were onto the holy grail."[147]

Barriers still stand in the way, particularly in the collective action problem of getting the wide array of actors in an even wider array of supply chains to adopt the same standards. However, these issues will likely work themselves out as influential first movers like Walmart and Maersk exercise their market power alongside their smaller partners.

4. Summarizing the Three Top Use Cases

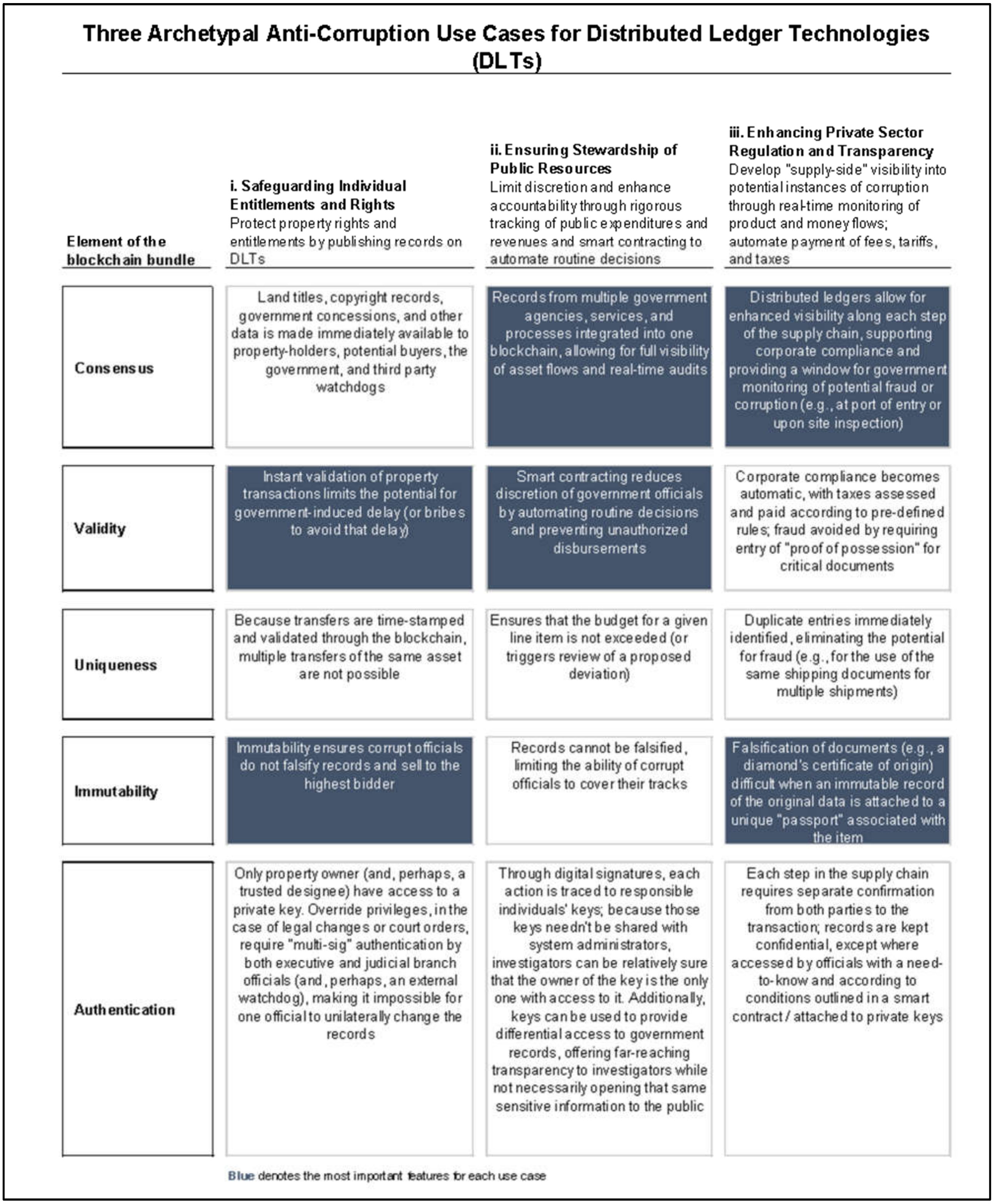
Figure 3 on the following page summarizes these three promising DLT use cases and outlines the specific features of the blockchain bundle that enable them.

https://www.nytimes.com/2017/03/04/business/dealbook/blockchain-ibm-bitcoin.html.

[146] *Id.*

[147] *Id.*

Figure 3 – Summary of Top Three Anti-Corruption DLT Use Cases



Three Archetypal Anti-Corruption Use Cases for Distributed Ledger Technologies (DLTs)

Element of the blockchain bundle	i. Safeguarding Individual Entitlements and Rights Protect property rights and entitlements by publishing records on DLTs	ii. Ensuring Stewardship of Public Resources Limit discretion and enhance accountability through rigorous tracking of public expenditures and revenues and smart contracting to automate routine decisions	iii. Enhancing Private Sector Regulation and Transparency Develop "supply-side" visibility into potential instances of corruption through real-time monitoring of product and money flows; automate payment of fees, tariffs, and taxes
Consensus	Land titles, copyright records, government concessions, and other data is made immediately available to property-holders, potential buyers, the government, and third party watchdogs	Records from multiple government agencies, services, and processes integrated into one blockchain, allowing for full visibility of asset flows and real-time audits	Distributed ledgers allow for enhanced visibility along each step of the supply chain, supporting corporate compliance and providing a window for government monitoring of potential fraud or corruption (e.g., at port of entry or upon site inspection)
Validity	Instant validation of property transactions limits the potential for government-induced delay (or bribes to avoid that delay)	Smart contracting reduces discretion of government officials by automating routine decisions and preventing unauthorized disbursements	Corporate compliance becomes automatic, with taxes assessed and paid according to pre-defined rules; fraud avoided by requiring entry of "proof of possession" for critical documents
Uniqueness	Because transfers are time-stamped and validated through the blockchain, multiple transfers of the same asset are not possible	Ensures that the budget for a given line item is not exceeded (or triggers review of a proposed deviation)	Duplicate entries immediately identified, eliminating the potential for fraud (e.g., for the use of the same shipping documents for multiple shipments)
Immutability	Immutability ensures corrupt officials do not falsify records and sell to the highest bidder	Records cannot be falsified, limiting the ability of corrupt officials to cover their tracks	Falsification of documents (e.g., a diamond's certificate of origin) difficult when an immutable record of the original data is attached to a unique "passport" associated with the item
Authentication	Only property owner (and, perhaps, a trusted designee) have access to a private key. Override privileges, in the case of legal changes or court orders, require "multi-sig" authentication by both executive and judicial branch officials (and, perhaps, an external watchdog), making it impossible for one official to unilaterally change the records	Through digital signatures, each action is traced to responsible individuals' keys; because those keys needn't be shared with system administrators, investigators can be relatively sure that the owner of the key is the only one with access to it. Additionally, keys can be used to provide differential access to government records, offering far-reaching transparency to investigators while not necessarily opening that same sensitive information to the public	Each step in the supply chain requires separate confirmation from both parties to the transaction; records are kept confidential, except where accessed by officials with a need-to-know and according to conditions outlined in a smart contract / attached to private keys

Blue denotes the most important features for each use case

B. Risks and Showstoppers

Although each of these three use cases demonstrates how DLTs can help in the fight against corruption, it is not certain that their benefits will outweigh their costs. Furthermore, as a new technology, blockchain presents several potential hazards for early adopters. Five types of risk merit noting here: (1) socio-political risk, (2) security and operational risk, (3) behavioral risk, (4) legal risk, and (5) governance risk. Policymakers can mitigate each to some extent—but some chance of negative outcomes will ultimately remain.

1. Socio-Political Risk

As discussed in Part IV, while DLTs can ensure that records remain immutable and that the network only accepts valid changes, they cannot ensure the accuracy of the data that was initially entered.[148] This limitation may be particularly concerning where DLTs are formalizing individuals' entitlements or property rights, as with land registries. It takes little imagination to envision a world in which a corrupt official places bogus records on a DLT, assigning land to political patrons, giving them the only private key to subsequently sell that land, and, in so doing, formalizing a corrupt state of affairs. In light of that risk, any DLT impacting private rights should have a dispute resolution process attached to it, and that process should be designed to minimize the required time, money, and frustration.

Similarly, the fact that a government is piloting a DLT does not mean that it is actually interested in reform.[149] This reality was evident in the Honduran case, where the government benefited from a fake partnership with Factom.

Vitally, DLTs should also not be confused with democratization. After all, it is not just enlightened governments that are piloting DLTs—Russia and China are two of the most enthusiastic early adopters.[150] Transparency can cut both ways. The same tools that

[148] VT. SEC'Y OF STATE, *supra* note 15, at 10-11.

[149] *See* Harlan Yu & David Robinson, *The New Ambiguity of Open Government*, 59 UCLA L. REV. DISC. (2012), http://www.uclalawreview.org/pdf/discourse/59-11.pdf (discussing how open-data initiatives can be used by opaque and accountable governments alike and proposing greater definitional nuance to ensure that open-data initiatives aimed at enhancing political accountability are not bunched with those aimed at improving service delivery, as they are now).

[150] Stan Higgins, *Russian PM Orders Research on Public Sector Blockchain Use*, COINDESK (Mar. 7, 2017), http://www.coindesk.com/russian-pm-orders-government-research-public-sector-blockchain-use/; Bradley Fink, *China's*

can be used to keep track of government spending or to help governments avoid tax fraud can also be used to spy on or repress citizens. Tying all financial transactions to a DLT, for instance, may reduce money laundering, but it also may allow for unprecedented levels of government surveillance.

As business processes and government services shift to decentralized ledgers, we also must be careful that this does not result in the *centralization* of social and economic power in the hands of DLT designers. Permissioned DLTs may risk delegation of too much power and authority to the contractors responsible for designing and hosting the system. Unpermissioned DLTs can suffer from a dearth of volunteers with the time and technical knowledge needed to meaningfully take part in their governance.

At a societal level, a transition to "smart contracting" and law-through-code should ideally be accompanied by a concerted effort to educate politicians and constituencies on what the technology is, the key policy debates and tradeoffs, and how private rights will be impacted. Failure to fully understand these questions may consolidate power in the hands of those few engineers who understand how the system functions.[151]

2. Security and Operational Risks

Although well-designed DLTs will likely prove more secure than legacy systems (particularly paper records), security and reliability are still not guaranteed. For unpermissioned ledgers, scalability may prove difficult due to the massive amounts of processing power required to clear each transaction. Bitcoin, for instance, has come to rely on large, Chinese "mining" operations, which offer massive amounts of processing power, but which may also collectively have enough processing power to compromise the integrity of the network itself.[152] This is a problem for any unpermissioned DLT.[153]

Although distributed denial-of-service (DDoS) attacks are a risk for any network, DLTs are probably more resistant to them than are

Blockchain Invasion, NASDAQ (Apr. 27, 2017), http://www.nasdaq.com/article/chinas-blockchain-invasion-cm780659.

[151] *See* Marcella Atzori, BLOCKCHAIN TECHNOLOGY AND DECENTRALIZED GOVERNANCE: IS THE STATE STILL NECESSARY? (Dec. 1, 2015) (unpublished manuscript), https://ssrn.com/abstract=2709713 (discussing how such dynamics would play out in a government-less society).

[152] Lester Coleman, *Video: Just how Significant is Chinese Miners' Control on Bitcoin?*, CRYPTOCOINS NEWS (Oct. 17, 2016), https://www.cryptocoinsnews.com/video-just-how-significant-is-chinese-miners-control-on-bitcoin/.

[153] ASTRI, *supra* note 16, at 49.

centralized networks due to the redundancy inherent in having many nodes and miners. [154] Nevertheless, DDoS attacks could still slow down the network, which could in turn make it vulnerable to other types of attacks.[155] Other attacks have already succeeded in disrupting the connections between nodes to allow malicious actors to disrupt the consensus mechanism or reroute incoming bitcoins.[156]

For permissioned DLTs that do not rely on proof-based cryptography, it is vital that all of the nodes are trustworthy. A permissioned DLT consisting of three nodes—two in separate government agencies and one with a watchdog—can easily be compromised through the creation of false records within the two government agencies. Even a larger network, spread among other agencies, could conceivably be compromised.

It is also important to remember that DLTs can only ensure that the correct authentication protocols are used, not that the identities of the people using the protocols are legitimate.[157] Private keys may be more secure than traditional passwords, but they can nonetheless be stolen. It is generally recommended that users keep their private keys offline—this practice is known in the industry as "cold storage."[158] Still, private keys can be stolen and used for fraudulent transactions, which, depending on how the DLT is designed, can be virtually impossible to reverse. This risk of unauthorized action can be mitigated by requiring multiple private keys for a given transaction ("multi-sig") or through escrow services where a trusted third party's key is also required to make a change.[159] However, the latter feature would insert a third party back into the picture, whereas the whole point of a DLT is to cut out third parties. In the anti-corruption context, this "trusted" party could itself prove corrupt, refusing to release a key until a bribe is given.

[154] A DDoS attack is "an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources." DIGITAL ATTACK MAP (2013), http://www.digitalattackmap.com/understanding-ddos/; ASTRI, *supra* note 16, at 50.

[155] One study has demonstrated that the Ethereum blockchain (used by R3) could be compromised by a single machine in twenty minutes, leaving the blockchain open to double-spending. This attack would work by delaying network communications between multiple subgroups of nodes to allow the rogue machine to build a chain of records that is longer than the others, resulting in acceptance of that chain instead of the legitimate ones. Christopher Natoli & Vincent Gramoli, *The Balance Attack Against Proof-of-Work Blockchains: The R3 Testbed as an Example*, (Working Paper, Dec. 30, 2016), https://arxiv.org/pdf/1612.09426.pdf.

[156] *Id.* at 2.

[157] VT. SEC'Y OF STATE, *supra* note 15, at 11.

[158] ASTRI, *supra* note 16, at 44.

[159] *Id.* at 50.

More broadly, as with any new technology, there is always the risk that a DLT will simply not work due to coding errors, issues with hardware compatibility, or unreliable infrastructure. This risk is compounded by the fact that many of the companies currently offering software for DLT applications are early-stage startups, which may not outlive their service agreements.[160]

3. Behavioral Risk

DLTs' potential to limit corruption will only be realized if DLTs are adopted widely. For citizens or other users of government services in the developed world, this may not be a particularly difficult barrier to overcome, provided the DLTs are well-designed and improve government service delivery.[161] It is the world's poor and vulnerable, however, who typically suffer most from corruption.[162] If they do not have access to the technology or the knowledge required to use DLTs, they will not benefit from them. To the extent that such technologies improve public perceptions or distract attention from the broader problem of corruption, they may exacerbate rather than solve corruption for those who need help the most. Hence, governments must simultaneously put into place programs aimed at providing mobile telephone and Internet access for the poor.

Governments and anti-corruption reformers also need to be aware of the risk posed by private DLTs. A DLT without appropriate governing rules and policies, such as know-your-customer requirements, can be used for money laundering or other nefarious purposes. More broadly, DLTs' abilities to achieve trust through consensus can be co-opted to create new networks that facilitate, rather than prevent, crime and corruption. Imagine, for instance, a DLT that allows drug cartels to monitor the flow of drugs from coca farms in South America through distribution in U.S. cities.

[160] Greenspan, *supra* note 75.

[161] "Block chains must be made user friendly. The customer need not know that they are trading in coloured coins, nor that their ID card login uses hash-function cryptography. In this sense, a blockchain acts as a silent, more efficient workhorse behind a solution that looks familiar: a mobile payments app, an online crowdfunding and trading platform, or a login portal." Alastair Brockbank, *Case Study 2: Estonian Block Chains Transform Paying, Trading, and Signing*, *in* GOVERNMENT OFFICE FOR SCIENCE, *supra* note 36, at 80.

[162] For a fascinating study of corruption's interaction with inequality, see Brian Fried et al., *Inequality at the Crossroads: A Multi-Method Study of Bribery and Discrimination in Latin America*, 45 LATIN AM. RES. REV. 76 (2010) (finding that traffic officers are more likely to demand bribes from poor drivers).

Such a DLT could even be used to automate bribe payments, eliminating the need for risky exchanges of cash or for paper trails. DLTs could further enable organized criminals to design computer-optimized distribution networks, routing their trade past those officials accepting the lowest bribes. Although designing this system would require a relatively high degree of technological sophistication, many of these capabilities could be adapted from open-source software, like that provided by Hyperledger.[163]

4. Legal Risk

Digitization of government or customer records is a legal and ethical minefield. To the extent that a DLT stores sensitive personal records, governments will need to ensure that such storage complies with applicable privacy and security laws.[164] Here, smart contracting may help, as smart contracts can allow citizens to clearly outline if and when they want their information to be shared, per their rights under national or local laws.

Perhaps the most important tension here will be between the immutability of digital ledgers and laws regarding data retention or the "right to be forgotten." Although a "key" could conceivably be created that would allow for the deletion of some records in a DLT, it would have to be designed in a way that avoids creating the type of "super-user" that DLTs are designed to avoid.[165] Additionally, it is not clear that deletion of records is a technical possibility with some forms of DLTs already in operation, such as blockchain.[166]

Finally, DLTs must be designed in ways that allow them to adapt to changes in the law. For instance, land registry DLTs should allow their validation rules to reflect changes to laws governing the transfer, sale, or seizure of property. Likewise, privacy laws are bound to change, requiring DLTs to change with them.

5. Governance Risk

For unpermissioned DLTs, governance is perhaps the biggest barrier to at-scale adoption. According to the British Government's

[163] For a list of Hyperledger's products, see https://www.hyperledger.org/.

[164] For an overview of data protection laws in the U.S., see Ieuan Jolly, *US Privacy and Data Security Law: Overview*, WESTLAW PRACTICAL LAW (2017).

[165] One potential solution would be to create a "super-user" account requiring action by a large number of stakeholders, all holding individual keys (e.g., a judicial officer, executive branch official, and the affected parties).

[166] I am far from qualified to say that definitively, but Nakamoto's white paper makes this appear quite difficult. *See* Nakamoto, *supra* note 4.

Office for Science, "unpermissioned distributed ledger systems are sometimes thought to exist independently of human rule-making, governed only by mathematical algorithms. This is a misconception. Just like legal code, technical code needs to be produced and maintained by humans who define the rules that the code embodies."[167] Developers typically constrain their powers through charters outlining what decisions can be made and how. The real power, however, appears to lie with those with the most processing power—the "miners." Updates must be installed by a majority of miners (as measured by the computer processing power of the DLT), placing significant amounts of power in their hands.[168] In the case of Bitcoin, decentralized governance has worked for small technocratic changes but has run into issues for larger-scale debates, particularly those regarding the maximum size of a "block," which determines how many transactions the network can process. With big economic stakes on both sides of the debate, the result has been a schism in the Bitcoin community and a capping of processing power at a level that is insufficient to accommodate growing transaction volumes. If change does not come soon, this cap may spell the end of Bitcoin.[169]

The lesson from Bitcoin appears to be that, even in a decentralized, libertarian project, political economy will always lurk beneath the surface. One observer writes: "It should be acknowledged that social-technical systems cannot—by virtue of their embeddedness into a social and cultural context—ensure their own *self-governance* and *self-sustainability* through technology alone."[170] Careful thought must, therefore, be put into designing governance processes that facilitate important decisions regarding the technology's future, while remaining fair to the parties involved.

Governance is often simpler for permissioned ledgers, since there is usually one party with clear legal and technical authority.[171] For permissioned ledgers, the concern is not about decentralized control and collective action, but rather that the centralized control may itself be a problem. A governance structure must be put into place that allows all interested parties, including citizen-stakeholders,

[167] GOVERNMENT OFFICE FOR SCIENCE, *supra* note 36, at 43.

[168] *Id.*

[169] Primavera De Filippi & Benjamin Loveluck, *The invisible politics of Bitcoin: governance crisis of a decentralised infrastructure*, INTERNET POL'Y REV., Sept. 2016, at 1, 157, https://policyreview.info/articles/analysis/invisible-politics-bitcoin-governance-crisis-decentralised-infrastructure.

[170] *Id.*

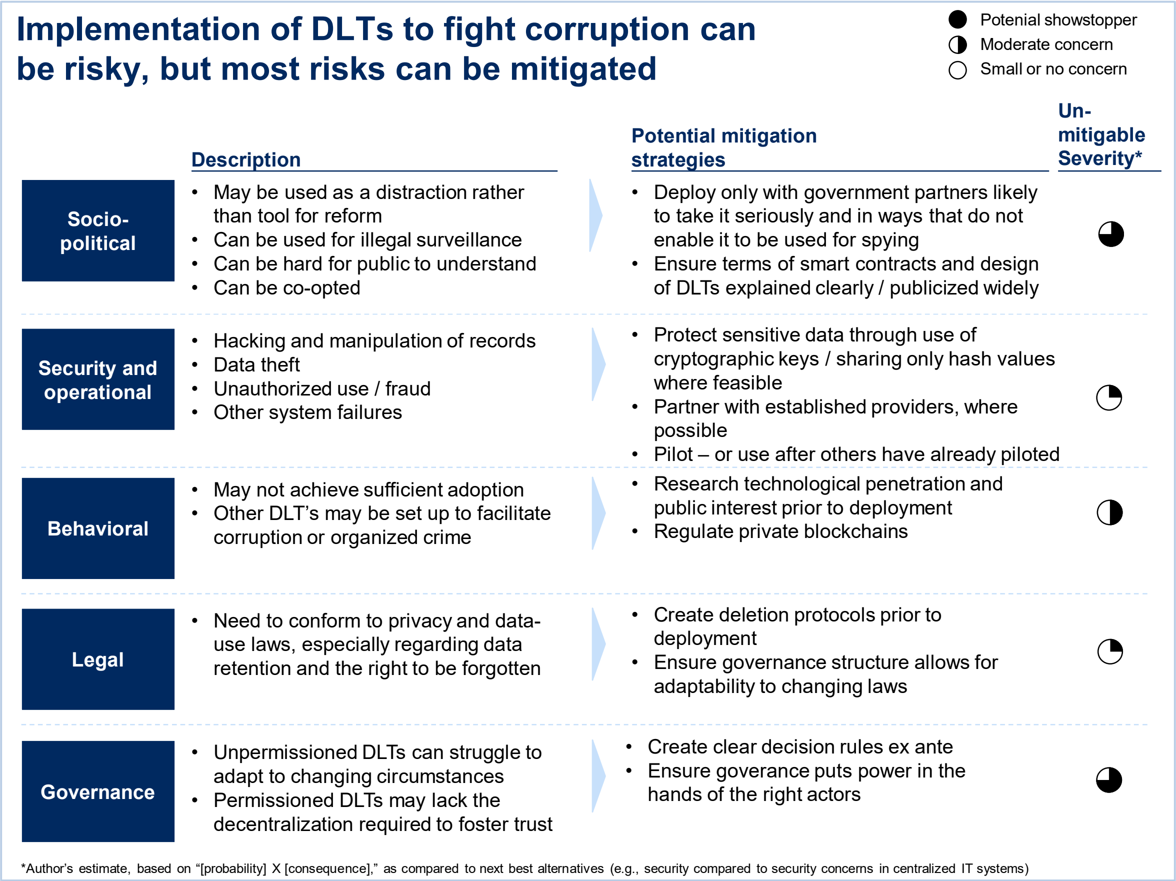
[171] GOVERNMENT OFFICE FOR SCIENCE, *supra* note 36, at 44.

a fair say. Otherwise, the DLT risks becoming a tool for corruption instead.

6. Summarizing the Risks and Showstoppers

Figure 4 on the following page summarizes DLTs' key risks, potential mitigation strategies, and the remaining, unmitigable risks after such actions are taken. Behavioral and legal concerns can largely be addressed through proper programmatic design. Security and operational risks are still significant, but DLTs are likely less vulnerable than legacy systems. Operational difficulties can be further mitigated by using technologies only after small-scale pilots (or full-scale launches by others). The biggest remaining risks pertain to the behavioral, socio-political, and governance elements, because addressing each risk requires delicately managing complex societal dynamics. The common theme behind each of these risks is that a technology like a DLT does not exist separate from broader socio-political issues. Just as DLTs can be used to increase accountability, they can also be used to cement power imbalances and perpetuate fraud. This danger can be mitigated, but to some degree the risk is unavoidable.

Figure 4 – Risks and Mitigation Strategies for Anti-Corruption DLT Use



Implementation of DLTs to fight corruption can be risky, but most risks can be mitigated

● Potenial showstopper
◑ Moderate concern
○ Small or no concern

	Description	Potential mitigation strategies	Un-mitigable Severity*
Socio-political	• May be used as a distraction rather than tool for reform • Can be used for illegal surveillance • Can be hard for public to understand • Can be co-opted	• Deploy only with government partners likely to take it seriously and in ways that do not enable it to be used for spying • Ensure terms of smart contracts and design of DLTs explained clearly / publicized widely	◕
Security and operational	• Hacking and manipulation of records • Data theft • Unauthorized use / fraud • Other system failures	• Protect sensitive data through use of cryptographic keys / sharing only hash values where feasible • Partner with established providers, where possible • Pilot – or use after others have already piloted	◔
Behavioral	• May not achieve sufficient adoption • Other DLT's may be set up to facilitate corruption or organized crime	• Research technological penetration and public interest prior to deployment • Regulate private blockchains	◑
Legal	• Need to conform to privacy and data-use laws, especially regarding data retention and the right to be forgotten	• Create deletion protocols prior to deployment • Ensure governance structure allows for adaptability to changing laws	◔
Governance	• Unpermissioned DLTs can struggle to adapt to changing circumstances • Permissioned DLTs may lack the decentralization required to foster trust	• Create clear decision rules ex ante • Ensure goverance puts power in the hands of the right actors	◕

*Author's estimate, based on "[probability] X [consequence]," as compared to next best alternatives (e.g., security compared to security concerns in centralized IT systems)

V. AMBITION AND CAUTION: A PATH FORWARD FOR DLTS AND ANTI-CORRUPTION

Considering the anti-corruption applications of DLTs, the three most promising use cases, and both inherent risks and possible mitigation strategies, what are the implications of all of this? What should government officials, multilateral institutions, or other anti-corruption reformers do with this knowledge?

First and foremost, they should focus on piloting initiatives aimed towards addressing the first two use cases discussed in this Article ("safeguarding rights and property" and "managing flows of money and resources"). Using the framework discussed in Part III, they can start by clearly identifying the instances of corruption they seek to solve and the causes of such instances. Subsequent analysis can then determine the potential for DLTs to be part of that solution, followed by small-scale piloting of the DLT to prove the concept.

The idea, in the short-term, would be to test the technology and measure its ability to solve the problem.

In the meantime, governments should also monitor those DLTs being developed by the private sector, with an eye for opportunities to join consortia in order to facilitate more proactive regulation. Legislatures and public agencies should also pass laws and regulations that mandate such cooperation. Governments can also consider actively encouraging the development of blockchains in certain sectors, through subsidies or tax credits on blockchain R&D.

Looking beyond the next five years and considering government delivery as a holistic problem, the biggest potential benefit of blockchain may be enabling at-scale e-government. Here, governments can follow Estonia's lead, where a national Public Key Infrastructure (PKI) enables citizens to access government services from their telephones, automates routine interactions with government (such as tax payments, vehicle registry, and medical record-keeping), uses smart contracting to allow citizens to elect what information to share with whom, and enables radical transparency in government actions. For example, a citizen can see a complete list of which government officials have viewed his or her records and when.[172] Estonia's e-government project has earned the country the nickname "E-stonia"[173] and has increased public trust, as evinced by the country's rapid improvement on the Transparency International Corruption Perception Index, on which it now ranks as the 22nd least corrupt nation in the world.[174] This accomplishment is all the more impressive when one considers that Estonia is still less than three decades removed from the tumultuous fall of the Soviet Union. Although Estonia's digital transformation happened before the development of DLTs, DLTs offer the potential to add security and efficiency to this model of e-government.[175] For instance, Estonia has recently deployed GuardTime's Digital Signature Infrastructure to secure the "record of state" (i.e., hash values) of the entire

[172] Sten Tamkivi, *Lessons From the World's Most Tech-Savvy Government*, ATLANTIC (Jan. 24, 2014), https://www.theatlantic.com/international/archive/2014/01/lessons-from-the-worlds-most-tech-savvy-government/283341/.

[173] ALINA MUNGIU-PIPPIDI, THE QUEST FOR GOOD GOVERNANCE 143 (2015).

[174] *Corruption Perceptions Index 2016*, TRANSPARENCY INT'L (Jan. 25, 2017), http://www.transparency.org/news/feature/corruption_perceptions_index_2016.

[175] For an overview of Estonia's e-government system, see Jaanus Karv, *E-Government and Its Ability to Reduce Corruption – The Case of Estonia*, (Unpublished Graduate Thesis, Lund University Department of Political Science, 2015), https://lup.lub.lu.se/student-papers/search/publication/5425282.

government's records, essentially making the government's records entirely immutable.[176]

E-stonia did not happen overnight. Rather, the country reaped the dividends of an early commitment to modernization, investments in free Internet access points throughout the country, passage of laws mandating the digitization of government records and creating the PKI system, continued political support,[177] and frequent collaboration with technology companies and telecommunications operators.[178] Although e-government has not "solved" Estonia's corruption problem, it has led to significant improvements and helped streamline government delivery more broadly.

Governments would be well-advised to study the Estonian case. To the extent that its model appears attractive, early investments in digital inclusion and PKI, passage of laws to mandate digitization and integration of government records, and aggressive citizen and industry engagement can pave the way for e-government in the future.

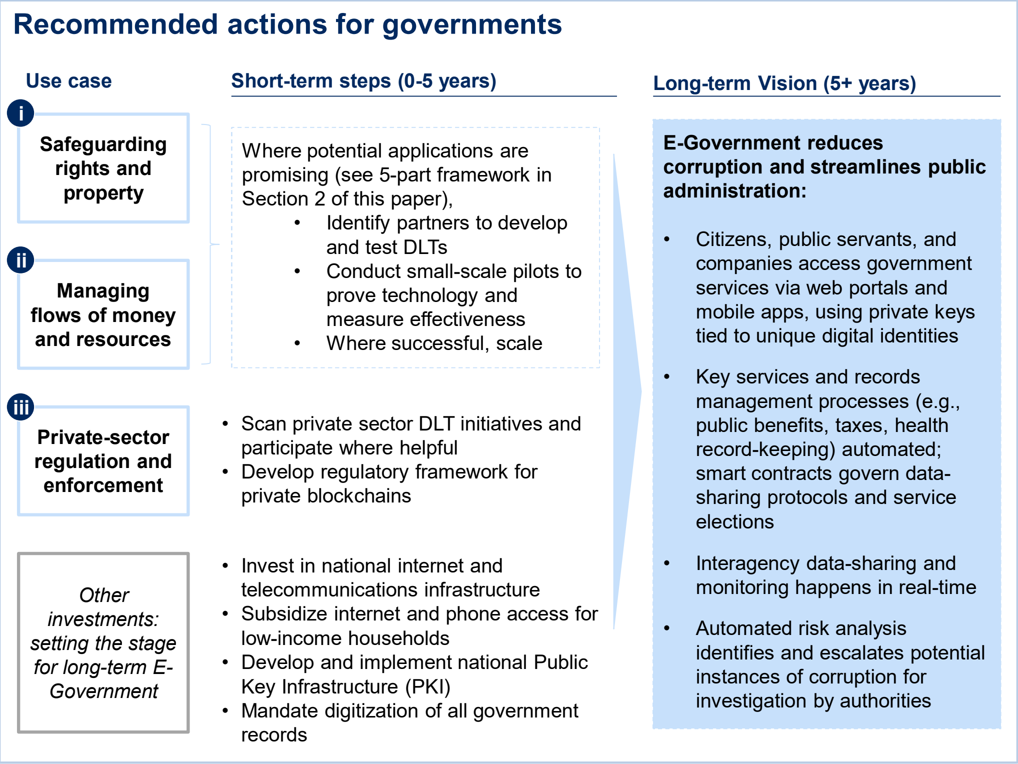
Figure 5 on the following page summarizes these key steps that governments can take, in both the short and long terms, to harness blockchain to fight corruption while moving towards long-term e-government.

[176] GOVERNMENT OFFICE FOR SCIENCE, *supra* note 36, at 83; *see also KSI Blockchain: Blockchain Meets Security*, GUARDTIME, https://guardtime.com/technology/ksi-technology.

[177] MUNGIU-PIPPIDI, *supra* note 173, at 142-144.

[178] Tamkivi, *supra* note 172.

Figure 5 – Recommended Actions for Governments



Recommended actions for governments

Use case

i **Safeguarding rights and property**

ii **Managing flows of money and resources**

iii **Private-sector regulation and enforcement**

Other investments: setting the stage for long-term E-Government

Short-term steps (0-5 years)

Where potential applications are promising (see 5-part framework in Section 2 of this paper),

- Identify partners to develop and test DLTs
- Conduct small-scale pilots to prove technology and measure effectiveness
- Where successful, scale

- Scan private sector DLT initiatives and participate where helpful
- Develop regulatory framework for private blockchains

- Invest in national internet and telecommunications infrastructure
- Subsidize internet and phone access for low-income households
- Develop and implement national Public Key Infrastructure (PKI)
- Mandate digitization of all government records

Long-term Vision (5+ years)

E-Government reduces corruption and streamlines public administration:

- Citizens, public servants, and companies access government services via web portals and mobile apps, using private keys tied to unique digital identities
- Key services and records management processes (e.g., public benefits, taxes, health record-keeping) automated; smart contracts govern data-sharing protocols and service elections
- Interagency data-sharing and monitoring happens in real-time
- Automated risk analysis identifies and escalates potential instances of corruption for investigation by authorities

VI. CONCLUSION

To the author's knowledge, this paper is the first systematic study of DLTs' anti-corruption applications. In the coming months and years, more information about DLTs, their uses, and their limitations will undoubtedly come to light. In this nascent and fast-moving field, the inevitability of change is the only certainty. Although such change may render the specific recommendations outlined in this paper moot, my hope is that the frameworks used to form those recommendations will nonetheless prove useful to those attempting to build a big-picture perspective on how technology can help in the fight against corruption and how this perspective can be translated into action.