SYM-AM-19-041

PROCEEDINGS
OF THE
SIXTEENTH ANNUAL ACQUISITION RESEARCH SYMPOSIUM

WEDNESDAY SESSIONS
VOLUME I

Acquisition Research:
Creating Synergy for Informed Change

May 8–9, 2019

Published: April 30, 2019

Prepared for the Naval Postgraduate School, Monterey, CA 93943.

Smart Contracts in the Federal Government—Leveraging Blockchain Technology to Revolutionize Acquisition

Michael Arendt—PhD, is a subject matter expert in innovative acquisition and contracting strategies across the Federal Government. Over the past 12 years, he has authored and co-authored numerous studies and reports including The *MITRE Innovative Contracting Implementation Framework*, *The MITRE Challenge-Based Acquisition Handbook*, *From Incentive Prize and Challenge Competitions to Procurement*, and *Pushing the Acquisition Innovation Envelope at the Office of Naval Research*. Arendt was a public-sector strategy and innovation consultant with IBM and a member of the research faculty at the University of Maryland's Center for Public Policy and Private Enterprise. He holds a PhD in Policy Studies from the University of Maryland, College Park.

Dave Bryson—is a lead engineer for the MITRE corporation with more than 20 years of experience designing and building software. In his current role as MITRE's blockchain technology lead, he performs research in applying the technology to the enterprise space and contributes to several leading open-source blockchain projects.

Kenyon Doyle—has more than 15 years of program management experience by serving in the United States Air Force, Federal Civilian workforce, and currently works in industry for The MITRE Corporation. Doyle has managed and supported defense acquisition programs covering aspects of the acquisition process, including research and development, integrating engineering, developmental and operational test, deployment, configuration management, production, manufacturing, and logistics support. Doyle has a BS in business administration from The Citadel and an MSA in general administration from Central Michigan University.

Patrick Staresina, COL, USA (Ret.)—is a retired member of the Army National Guard with more than 20 years of contracting officer experience, with the pinnacle of his Federal career serving as the Director of Contracting at the National Guard Bureau. Staresina continues to provide acquisition support the Federal Government through his service as an Acquisition Principal for multiple federally funded research and development centers (FFRDCs) managed by the MITRE Corporation.

Abstract

Across the government, the process of creating and enforcing contracts has not changed much in the past several decades. To this day, most government contracts require paperwork that must be routed across multiple parties, with physical signatures attested to by key personnel, and further rely on third parties such as private contractors or other government organizations for enforcement and storage. This results in a slow, opaque process that lacks transparency, efficiency, and auditability. Despite this reality, major advancements in blockchain technology in recent years have opened a new door to greatly improving the traditional government contracting process via the use of blockchain enabled, smart contracts.

Smart contracts have the potential to simplify many types of agreements (such as Government-Wide Acquisition Contracts and General Services Administration Schedules, among others) without the need for tedious paperwork and third parties. They can objectify contracts and policies while also storing the provenance of the information on a globally decentralized database. This research paper discusses how blockchain technology, coupled with smart contracts, can provide a next generation approach to automate and radically reduce acquisition lead time, improve contract performance, and sustainably decrease transaction costs.

Introduction

When most people think of blockchain, they immediately think of cryptocurrency and Bitcoin. For some, hearing these terms stimulates a cynical eyeroll as one recalls the last great, overhyped technological innovation whose promise far outweighed its practical, real-world benefits. While there are certainly some corners of the blockchain and cryptocurrency universe that will inevitably fail, there are many others that will meet and widely exceed promised expectations. Blockchain-based smart contracts are one of these innovations that has the potential to revolutionize the world as we know it.

This research paper provides a window into how blockchain-based smart contract technology can be leveraged across the federal, state, and local government to improve acquisition and procurement. Acquisition and procurement can be simply defined as the purchasing of goods and services. Both public and private sector entities acquire and procure a wide variety of things ranging from construction services to office furniture, from software licenses to printer paper, from IT consulting services to cloud-based technologies which serve as the backbone for day-to-day operations.

In the case of the government, whether it be federal, state or local, the process to acquire these goods and services tends to be complex. Irrespective of the level of government and department or agency doing the buying, a process exists for the express purpose of executing these transactions. Many involve a slew of requirements paperwork, reviews and approvals, bids and proposals, contract awards, administration, oversight of contract terms and conditions, inspection and acceptance criteria for delivery, and finally at some point taxpayer funds can be disbursed for payment. The resulting process can seem archaic for those in the government who practice it and twilight-zone-like for those in industry who are used to getting things done nearly on-demand. This is not to say that advancements have not been made in streamlining contracting processes, reducing acquisition lead-time, and making payment disbursements to vendors more efficient. But considerable opportunities for improvement remain to bridge the gap between government operations and commercial benchmarks for operating efficiency. Moreover, when examined today within the context of what is truly possible while employing a revolutionary technology like blockchain-enabled smart contracts, the promise for improvement may in fact be exponential. Numerous opportunities exist across a wide range of acquisition and procurement types to turn months into days or weeks to complete the very same transactions that currently drain the hope out of those caught in the middle of the process.

This research paper introduces blockchain technology; provides an overview of the status quo which may be colloquially referred to as “dumb contracts”; offers an introduction to blockchain-based smart contracts along with their benefits as well as drawbacks; describes a prototype including how we smart contracts may be leveraged to improve the agreement, tracking, and payment part of the procurement process; and, to illustrate how smart contracts might work when applied in the real world of government procurement, we will offer a notional use-case where smart contracts could be beneficial as part of a Federal Supply Schedule process.

Blockchain Technology Overview

Blockchain … Isn’t That Just Bitcoin Hype?

What is a blockchain? Believe it or not, a blockchain is pretty much exactly what it sounds like.

A blockchain is a series of blocks (or batch of transactions) cryptographically linked to one another to form a digital ledger. Each block may contain one or more transactions such as the amount of currency to exchange. A blockchain provides an immutable, transparent, irrefutable, record that is permanently stored on multiple machines or nodes. Trust between parties that may not otherwise trust one another is established through a blockchain without requiring assistance from an administrator or traditional centralized services.

To summarize, the key components of a blockchain include the following:

- P2P Protocol: the protocol that manages the peer nodes of the network that support blockchain
- Performs communication between node, flow control, node discovery, framing
- Smart Contracts (optional added feature): business rules or logic that can extend the functionality of a blockchain (Bryson et al., 2017)
- Cryptography: hash functions that link blocks together providing integrity of the chain and digital signatures providing integrity for the transactions
- Consensus Algorithm: the process by which parties to a blockchain decide on the ordering and presence of transactions on the ledger
- Distributed Ledger: a distributed, replicated, representation of all transactions

A blockchain is distributed over multiple nodes using peer-to-peer (P2P) networks. Each node within a blockchain is independent of one another and every transaction is redundantly verified and processed by every node for verification. Therefore, a single node failing on a blockchain network will not bring the whole system down as the other operating nodes can continue to run the blockchain. To compromise a blockchain, a hacker would need to have control over a large majority of the network.

A blockchain is often compared to a bank ledger containing transactions. A bank ledger records a series of transactions by collecting and reporting information. Every time a debit card is swiped at a grocery store, the bank ledger records the transaction and you'll find it next time you log into your banks app or website to review your account information. This type of ledger is traditionally done using a centralized database that is managed and stored by your bank. A database administrator oversees bank transactions which are then managed internally and reported back out for customers and other businesses to see such as the merchants bank. These transactions need to be reconciled every night.

These transactions may be changed by the bank without you having visibility into the changes themselves in real-time. For example, have you ever had a deposit hold on your debit card fall off? One day the transaction is pending, and your balance reflects this change, the next day the transaction falls off your ledger and disappears from your recent transaction list in your banks app never to be seen again. The result is that your balance is updated accordingly, but the history of the hold against the account one day and being removed the next day essentially disappears. This happens all the time with gasoline purchases, hotel stays, car rentals, and many other transactions of these types.

The blockchain solves this problem (and several others that we will discuss in more detail below) quite easily because every transaction that is written to the ledger in the blockchain is permanent so they cannot be changed or deleted. In the example of the deposit hold against the bank account, the blockchain records each transaction individually so the hold would be recorded on one day and a new block would record when the hold is removed on the next day allowing for complete transparency into the account ledger information at any point in time.

Each transaction is bundled into blocks and these blocks are linked to form the ledger, which is called a blockchain. At its core, a blockchain enables a network of peer computers (or nodes) to validate, settle, and agree on a record of transactions. It establishes a form of trust between parties that may not otherwise trust each other, and does so without relying on traditional centralized services, or trusted third parties (Bryson et al, 2017).

Centralized Databases vs. a Blockchain

Although a blockchain is a database in the form of digital ledger, a database is not a blockchain. A database is a ledger that is controlled and maintained by an administrator. The administrator can create, modify, and delete data stored in the database at any given time. The administrator can also delegate and provide rights to read or write data to other users.

A database is centralized as there is a single point of control of the data. Because of this centralized single point of control, a database is more inclined to be hacked or misused—recent revelations regarding Facebook's use of user data offers a contemporary example of what might happen when there is single point of control for your data (Lomas, 2018). According to blockchain expert Vince Tabora, "A company that has control of information can monetize it for third party use, but sometimes it is not in the best interest of users" (Tabora, 2018). Other differences (and drawbacks) of a centralized database are that since there's a single point of control of the database, a failed server will affect the entire system. Likewise, the data will not be recoverable if the information was not backed up and stored.

Traditional databases are optimized for transaction throughput. Transactions may be processed on a database in a matter of seconds while it may take several minutes for new blocks to be created on a blockchain as these new blocks work their way through each node of the blockchain.

Digital Ledger Technology (DLT) vs. Blockchain

Blockchain and DLT share common themes in that they are both decentralized and digitalized ledgers. Many people use blockchain and distributed ledger technology interchangeably, but they are vastly different.

Blockchain is a type of DLT where a series of blocks are interconnected. Each block contains data that is verified and validated before being attached to the chain of transaction records. Blockchain data is permanently stored and cannot be manipulated. There are several different types of DLT and blockchain is just one example. All blockchains are DLTs but not all DLTs are blockchains.

DLT is the "umbrella" term used to describe a database that is shared across various locations or multiple participants in a trusted environment. DLTs do not have a centralized administrator or centralized database. Like blockchain, DLT data has a timestamp that contains unalterable history of all transaction records in the network. Any of the participants on the DLT can view all the data. The data on a DLT is secure and stored using cryptography that can be retrieved with keys and cryptographic signatures (Buntinx, 2017). Comparing blockchain to DLT would be like using the analogy that a Lexus is a type of automobile (Kashyap, 2018).

Dumb Contracts vs. Smart Contracts: How the Status Quo Can Change

Dumb Contracts

Current methods for writing contracts could be described as "dumb." Often, requirements stakeholders, contracting officers, their specialists and representatives perform slow, manual, labor-intensive activities based in some form of a word document, spreadsheet, database file, or arcane contract writing system. In cases where requirements are truly unique, and customization is required, this type of approach can make some sense. However, for a vast number of the acquisitions and procurements for commercial goods and services, the process is repetitive.

Processes for contracting and acquisitions may or may not be documented within an organization leading to differences even between groups within the same office. As a result, the process may not always be 100% repeatable across an organization when buying the exact same good or service. In some cases, processes may appear to be completely digitized and have some sense of automation on the front end because of the use of a web-based interface, when in fact the backend is simply generating a slew of emails and forms that must be manually reviewed and approved to continue along in the process.

Change orders, for example, when something in the existing contract must be modified, may become tripwires that generate additional downstream churn and are often overlooked at contract initiation. These safeguards are in place to ensure taxpayer funds are spent appropriately.

Smart Contracts

Blockchain-based smart contracts enable automation of dumb contracts as noted above. Smart contracts achieve this by taking the ledger-based blockchain innovations previously discussed and overlaying some business logic on top of them enabling automatic execution when certain pre-defined terms and conditions are met. A common basic example of a smart contract is that of the vending machine whereby you insert a coin into the machine and in return the machine gives something to you. The machine is programmed to give you X when Y dollars/cents have been received. This is the business logic that has been pre-programmed into the machine. As compared with a dumb contract, in the vending machine example, the transaction occurs without the presence of a middleman. By comparison, when you go into a gas station convenience store and must walk up to the counter and hand the clerk the soda and your money in order to check out, the clerk is the middleman who must be present for you to complete the transaction. Moreover, if you happen to use a debit/credit card to purchase the soda in the store, the merchant’s credit card processing company and your bank or credit card issuer act as additional middlemen who must all be present for the transaction to be processed. By comparison to the “smart contract” vending machine example, if paying in cash, the transaction is solely between you and the machine itself because the machine has been preprogramed to dispense a soda once the correct amount of money has been deposited—no middleman required.

Smart contracts may be useful for purchasing basic goods and services and may also be beneficial for things like insurance policies, breach contracts, property and real estate transactions, issuing and managing credit, financial services, legal processes and crowdfunding agreements among others where typically the services of a middleman have been previously required (Blockgeeks, n.d.).

Benefits of Smart Contracts

Smart contracts offer numerous benefits that can be realized across the government acquisition and procurement process which are discussed in more detail below:

- **Autonomy—**Smart contracts allow the creation of a direct agreement between two parties without use of an intermediary. Moreover, because there isn’t an intermediary the transaction may not be manipulated by a third-party.
- **Trust**—Smart contracts permit trust to be built into the process because all information and associated documents/data are encrypted on a shared ledger, so they cannot be lost.

- **Backup**—Because the blockchain stores information related to an agreement on the shared ledger across a distributed network, there will be multiple copies of stored information.
- **Safety**—The blockchain is secured through cryptography; blockchain relies on two cryptographic primitives to help secure the chain—digital signatures and cryptographic hash functions. Both are used to verify and ensure the integrity of data.
- **Speed**—Smart contracts can automate tasks if business logic is pre-defined and built into the blockchain, as a result, previous tasks related to contracting that were done manually (such as quality reviews or multiple approvals) could be executed automatically.
- **Savings**—Smart contracts have the potential to save considerable amounts of money as intermediaries are no longer necessary. Moreover, business process improvement may be possible after the introduction of smart contracts in parts of the process where redundancy to include multiple human approvals was built in to explicitly improve trust, safety, and accuracy.
- **Accuracy**—Automated contracts avoid the errors that come from manually filling out endless amounts of paperwork like spreadsheets and word documents. If the appropriate business logic is built into the smart contract, only those spreadsheets or documents that meet the pre-defined accuracy criteria would be accepted (Blockgeeks, n.d.).

Drawbacks of Smart Contracts

The term *smart contract* is a bit misleading, as they are not inherently “smart” nor a “contract” in the legal sense. Smart contracts are essentially the business logic of the blockchain that run during blockchain transactions and are only as good as the logic programmed in to them. Smart contract functionality varies by platform as each may offer differ capabilities. However, in all cases the blockchain cannot prevent programmer error. So due diligence is needed to prevent introducing security problems via a smart contract. Additionally, it’s very important that smart contract logic executes in a deterministic fashion, whereby outcomes are precisely determined through known relationships among states and events as this plays a key role in the network reaching consensus on a given set of transactions.

Blockchain Smart Contracts Prototype: Agreement, Tracking and Payment in Action

MITRE’s research in applying Blockchain technology is focusing on three high-level areas that apply to acquisition and procurements: Agreement, Tracking, and Payment. We’re exploring how blockchain technology coupled with smart contracts may help to improve the efficiency and integrity of the process across these areas. Nearly all business processes rely on these areas to conduct day to day activities. We are building small prototypes in an incremental fashion. Our goal is *not* to build a production level system., but rather to demonstrate and evaluate the potential capabilities of blockchain and smart contracts as applied to the areas of agreement, tracking, and payment within acquisition as defined below.

- **Agreement:** Can we automate the process of establishing an agreement among parties without relying on centralized control or services? Why is this important? Agreements are used to establish trust among parties as well to enforce policy and procedures. In our use-case, this involves several documents related to approvals, terms and conditions when the government is procuring a good or service. Integrity and efficiency can be improved by eliminating the need for centralized control to enforce and process these agreements, along with automating the rules and verification via cryptography.

- **Tracking:** Every organization involved maintains their own system of record, yet parties to the contracting process, often need to have a shared view into the overall state of a given agreement or transaction. Sharing this information across organization boundaries via traditional technology has been a pain point for decades. Blockchain technology is very good at providing a tamper-resistant, audit logic that can be safely shared among all parties internal and external to the government.
- **Payment:** Moving money around and across governmental organizations and outside of government to pay vendors requires many checks and balances. If we could employ digital currency in the Enterprise, it may be able to streamline processes by eliminating spreadsheets and reconciliation services.

Current Blockchain Smart Contracts Prototype Achievements

Since the beginning of FY19 through date of this research, the prototype has demonstrated the following:

a. An agreement is created and processed. We use a blockchain and smart contracts to capture, track, and enforce the rules of an agreement. We use decentralized file storage to store the traditional documents associated with an agreement. The decentralized file storage also maintains a unique fingerprint of each document to ensure parties are collaborating on the correct version of an agreement—no more emailing documents around while trying to track the right version via the filename.

b. A cryptographic “wallet” was created for every user who intends to interact with the system. Any transaction sent to the system to digitally sign an agreement, assign a funding authority, etc., requires a cryptographically signed transaction from that user. The signature is checked several times by every permissioned validator node to verify the user before the transaction is accepted. This increases the integrity of the transaction and the transaction is permanently stored in the blockchain for auditability.

c. A decentralized notary service was established to verify, and process digital signatures required by the documents associated with the process. The notary service is implemented as a smart contract ensuring the integrity and authenticity of signatures simplifying the document approval process.

d. A rules-based flow was established to enforce the agreement through the process:

    i. User creates a request for purchase along with required signers.

    ii. When all signers have signed a funding authority is assigned by their cryptographic wallet address. Once the associated funding doc(s) are signed, the funding transfers the funding amount (in digital currency) to the selected contracting office.

    iii. The contracting office develops an RFQ and opens the process for bidding. Once the bidding process ends. The “best” bid is selected, and the winning bidder is recorded in the smart contract agreement.

iv. The contracting office then “pays” the winner bidder for the service via digital currency over the blockchain

v. When the purchase is received, creator of the agreement “closes” the agreement.

Using the approach, the entire process agreement generation, document signatures, money transfers, and so forth, are recorded on the blockchain in an immutable, auditable ledger and available for all parties to the process to examine.

Applied Use Case: How Smart Contracts Prototype Could be Implemented in the Government

The intent of this use is to examine how our prototype could be applied to a simple acquisition of standard Commercial Off-the-Shelf (COTS) software licenses using a Federal Supply Schedule.

This use case is organized in the following manner: a general introduction to the Federal procurement process, an example requirements generation process that describes the status quo, how smart contracts could be used, and potential benefits; an example contracting process that describes the status quo, how smart contracts could be used, and potential benefits; applicability of this use case; barriers to a smart contracts prototype implementation; keys to success for a smart contracts prototype implementation; and, a short conclusion.

Understanding the Federal Procurement Process

When an individual or an organization has an immediate need to procure a COTS item, such as geographic information system (GIS) mapping software, the process is simple enough. The individual consumer or corporate purchasing agent simply logs into the software sales point of entry, clicks on the subscription or product that best meets their needs, inputs their registration and payment information, and downloads the software. The process generally takes less than an hour. Conversely, when a government information technology (IT) specialist needs a similar piece of software, the process to fulfill that need could not be more different. Instead of going through an automated online purchase transaction, the IT specialist is directed to a much more subjective acquisition process, which could take up to 90 days to complete. This leads us to the following question: How might we introduce blockchain-based smart contracts to improve the procurement of COTS software?[1]

While the detailed nuances for procuring COTS software differs from agency to agency, the overall federal procurement process is relatively fixed. Below is a representative example of the wickets that an agency would have to navigate in order to acquire software licenses. For clarity’s sake, this process is broken down into two major groups: Actions of the Requiring Activity/Customer and Actions of the Contracting Team (see Table 1).

[1] While this process could be customized for federal COTS procurements at any dollar level, this particular case study process is focused on those software purchases between the ranges of the FAR Micropurchase Threshold and the Simplified Acquisition Threshold.

Table 1. Actions of the Requiring Activity/Customer and Actions of the Contracting Team

Actions of the Requiring Activity/Customer
Step 1. Determination of Requirements
Step 2. Seek Requirements Validation
Step 3. Secure, Commit, and Transmit Funds
Step 4. Transmit Requirement Package to Contracting Officer (CO)

Actions of the Contracting Team
Step 1. Review Package for Sufficiency
Step 2. Prepare the Request for Quotation (RFQ)
Step 3. CO Seeks RFQ Approvals (Legal, Policy, Manager, Peer Review) Step 4a. Post RFQ on eBuy Step 4b. Transmit RFQ to Specific Vendors Step 5. Receive Quotes
Step 6. Evaluation of Quotes
Step 7. Award Decision
Step 8. Award Notification
Step 9. Tracking Contract Performance
Step 10. Contract Payment
Step 11. Contract Closeout

This standard process for procuring simple commercial items or services follows many of the same steps as the procurement of more complex solutions or services. While this process may be scaled down somewhat for more “simplified acquisitions,” this approach is far from efficient. Upon quick review, the process is inefficient; requires unnecessary reviews and/or approval from members with little or no equity in the acquisition; and adds unnecessary schedule delays.

By automating those functions that can be processed using machine logic, the government should be able to realize the following second and third order effects:

- Reduction in the number of “touch points” needed to process a simple COTS acquisition,
- Greater standardization and simplification of requirements inputs to include requirements definition, cost estimating, market research, and evaluation of quotes,
- Reduced number of resources (i.e., employee hours) needed to execute the transaction through the reduction of said “touch points” listed above,
- Improved procurement acquisition lead-times,
- Faster delivery of software products and support services,
- Quicker processing of payment, and
- Automated enforcement of the process flow including redundant verifications.

So, how could we apply a blockchain-based smart contracts approach to this use case? The critical piece of this analysis starts with a detailed examination of the current procurement steps and analyzing each to see which, if any, steps can be automated—comfortably replacing human decisions with machine logic.

Requiring Activity Steps

Let's start by examining the first four steps executed by the Requiring Activity or Customer.

Step 1. Determination of a Requirement

One of the most difficult challenges in the area of procurement is the task of defining contract requirements. Traditional processes require the requiring activity to draft a Statement of Work (SOW) document identifying required salient characteristics that allow for multiple vendors to respond with formal quotes. Requirements definition is one of the primary points of contention between a contracting office and its customers, often resulting in numerous significant back-and-forth iterations of work statement reviews.

We recommend establishing an agency pre-approved menu of software license solutions available for the IT professional to select. The process of developing a work statement would essentially be replaced by completing an eForm requisition, which would include: a description and quantities of the license(s) requested; overall estimated cost; a list of sources and other simple market research data points; a short narrative or justification explaining why the software license is required; and a narrative/list of the equipment on which it would be installed.

By consolidating all these data points onto one eForm, we essentially eliminate the requirement to draft a Statement of Work (SOW), Independent Government Cost Estimate (IGCE), Market Research Report, and an agency needs justification document. This eForm would be certified by the preparer and would initiate the procurement process in the blockchain.

Step 2. Seek Requirements Validation/Approval from Agency (Processes Vary by Agency)

Once a purchase request is initiated, there is often an internal agency review process. This requirements validation process is established with the intent of ensuring that the need is valid, the requirement is an appropriate use of agency funds, and that the request agrees with the policies of that agency. It is not uncommon for this requirements validation process to be top-heavy and lengthy. In many cases, the process involves multiple layers of unnecessary approvals with final approval levels being established at the highest executive levels (who often have very limited schedule availability). The higher the approval authority that is established, the greater the number of people that review the requirement prior to final approval. Further, some organizations only perform this requirements validation process on a semi-annual or quarterly basis, adding even more time to the process. While this level of scrutiny may be appropriate for multi-million-dollar requirements, it would not be appropriate for simple low-dollar COTS software purchases.

To address this, we recommend establishing a blockchain-based smart contract with pre-defined business logic that automates the approval process for all requisitions to a Chief Information Officer (CIO) representative within the organization for approval if the requisition is (1) for a COTS software solution; and (2) under a pre-determined price threshold that the organization can accept as low-risk. Replacing a multi-layered requirements validation process with an automated step that is executed by the pre-programed smart contract, could reduce the procurement lead time by weeks and even months by eliminating the number of non-value-added reviews as often the degree of human checking is not proportionate with the dollar amount or complexity of the transaction.

Step 3. Secure, Commit, and Transfer Funding to Contracting Office and Step 4. Transmit Approved Requirements Package to the Contracting Officer

After a requirement is validated and approved, the next step is normally to secure, certify and transmit funding to the contracting office. In the traditional procurement process, this requires the customer to prepare a "purchase request" for funds, which would then circulate through a series of reviewing/approving steps before a representative with "commitment" authority certifies that funds are "available" for this procurement and provides a unique accounting code for the purchase. Once the funds are "certified," the procurement package is routed to the contracting office manually or electronically through email or another pre-approved agency system.

Again, this is a task that can be automated into a smart contract process. In this case, once the requirement is validated, the task would move to the next step, which would require the system ensure the correct funding account was being selected and would perform a comparison of the anticipated requirement cost vs the available budget and/or some other pre-determined approval dollar threshold. If the cost is less than both and the correct account was selected, the process could move forward to funds certification. In other words, the agency could set pre-established conditions (built in to the blockchain-based smart contract as business logic) under which the process could proceed without human interaction, until it reaches the final stage of "funds certification."

Because of the low-dollar amount of the requirement, the number of reviews could be reduced by introducing machine review gates into the smart contract business logic, which would validate funds being applied were of the appropriate time, purpose and amount required. The funds would then be forwarded to the funds certifying official in the blockchain for review/approval. Approval of these funds would then trigger the next automated step—Transmittal to the Contracting Office.[2]

Contracting Team Steps

Step 1. Review Requirement Package for Sufficiency

Once the customer submits the requirements package, the contacting office becomes the lead for further processing and facilitates the steps provided below.

Acceptance of a requirements package is often a hot spot in the procurement process. A primary reason for this friction is that the "clock" for Procurement Acquisition Lead Time (PALT) officially starts once the requirements package is accepted by the contracting office. This creates an environment where there is a reluctance to accept weak or incomplete requirements packages. Contracting offices will often reject the package and require the customer resubmit with corrections or improvements.

This need not be the case in a procurement as simple as the purchase of a COTS license. Assuming the IT specialist complied with the initial guidance, completed the

[2] Note: Federal agencies utilize numerous different processes and/or systems to track and certify funding. In order to integrate blockchain and smart contracts into this process, they would have to interface with those systems. Alternatively, the funds certification process could be performed outside of blockchain, and then integrated back into the process once funds are approve.

eForms/requisitions correctly, received adequate requirements validation, and secured enough certified funding, the acceptance of a procurement package should be easy to validate through pre-defined smart contract business logic that captures the specific requirements necessary for a complete requirements package to be permitted to move forward.

By standardizing and automating the required inputs of the requirements package, the acceptance process is made significantly easier. The contracting officer task of performing a complete procurement requirements package review (which includes the SOW, purchase request (PR), IGCE, Market Research Report, requirements validation, and funds certification) is instead reduced to a more simplified review of the completed requisition eForm, the simplified requirements validation, and the certification of funds.

Step 2. Prepare the RFQ

By standardizing and automating the required inputs of the requirements package, the acceptance process is made significantly easier. The contracting officer task of performing a complete procurement requirements package review (which includes the SOW, PR, IGCE, Market Research Report, requirements validation, and funds certification) is instead reduced to a more simplified review of the completed requisition eForm, the simplified requirements validation, and the certification of funds.

Once the contracting officer has accepted the requirements package, the contracting team prepares a Request for Quotation (RFQ) for distribution to the potential offerors. Depending on the details of the requirement, this RFQ can be prepared using a government form (i.e., SF 1449 or DD 1155), a formal letter, an email, or even an oral request over the phone.

As mentioned previously, this use case capitalizes on the use of Federal Supply Schedules to procure the said software licenses. One of the greatest benefits of utilizing Federal Supply Schedules is that all the terms and conditions are pre-negotiated and automatically wrapped into the price of the software. This allows the government to focus almost exclusively on price for the individual order. Because we are using these schedules, the RFQ can be dramatically simplified using a standard fillable letter or email. This process could be easily automated by the smart contract pre-populating a standard RFQ form letter with the information provided in the original requisition eForm and a few additional inputs. Unlike other more complex solicitations, all the clauses, provisions and other terms for the RFQ are already pre-defined under the governing schedule.[3] Using this approach, the system could easily generate an RFQ by populating a form simple letter utilizing standardized automated inputs.

Step 3. Seek RFQ Approval From Contracts Chain (Legal, Policy, Manager, Peer Review)

Many contracting offices require multiple layers of review before a solicitation is released to potential bidders. Normally, the RFQ is prepared by a contract specialist and reviewed by the contracting officer. However, some organizations require additional

[3] Note, some organizations such as the DoD have mandatory specialized clauses in addition to the pre-negotiated GSA terms and conditions. In such cases, these additional terms can be added to the RFQ eForm.

solicitation reviews from independent peers, branch supervisors, policy teams, and legal counsel. These reviews could add weeks to the procurement process.

We recommend that the review requirements be minimized as much as possible, especially in cases such as this where the acquisition is simple, low-dollar, and utilizes pre-established Government-Wide Acquisition Contracts (GWACs). However, if additional RFQ reviews are required, this process could be greatly simplified and expedited by establishing a "Smart Contracts Analyst" who would be specially trained to perform compliance reviews with a focus on issues related to COTS acquisitions using a blockchain-based smart contract with pre-defined business logic. These reviews, adjudications, and approvals would be recorded transactions on the blockchain with the supporting data being stored in decentralized file storage. Once all compliance approval is received and all concerns are adjudicated, the contracting officer/contract specialist can proceed to the next step—transmitting the RFQ to vendors.

Step 4a. Post RFQ on eBuy IAW FAR 8.405-1(d)(3)

Step 4b. (Alternate to 4a above) Transmit RFQ to Specific Vendors

Step 5. Receive Quotes

The rules for procuring solutions under the Federal Supply Schedules is uncharacteristically explicit. The Federal Acquisition Regulation specifically outlines the contracting officer's processes and requirements under subpart 8.405-1, Ordering Procedures for Supplies and Services Not Requiring a Statement of Work, and further explains the required procedures under subparagraph (c), Orders exceeding the micro-purchase threshold but not exceeding the simplified acquisition threshold. Under this section, the FAR states that the agency shall survey at least three schedule contractors through the GSA Advantage! online shopping service by:

- Reviewing the catalogs or pricelists of at least three schedule contractors. An automated process can be established to collect pricelists from GSA Advantage to assist determining which vendors offer the most competitive pricing. Machine logic can then be applied to compare prices to each other.

- Requesting quotations from at least three schedule contractors. If the contracting officer elects to solicit multiple quotes, the transmittal of an RFQ to one or multiple GSA vendors can be achieved through automated systems using blockchain to record the transmittal. Not only would blockchain record the transmittal of the RFQ, but it would also provide a tamper-proof method to certify (i.e., date stamp) when that transmittal occurred by building such business logic into the smart contract.

- Posting the RFQ on GSA's competition web platform and seek responsive quotes through that eBuy portal (FAR 8.405-1(d)(3)(i)). If the contracting officer elects to solicit quotes from all GSA schedule holders through the use of the GSA eBuy system, the RFQ that is transmitted could include explicit instructions for offerors to submit their quotes to the government through a method or system that is also recorded on the blockchain.

Once vendors have the opportunity to review the RFQ and prepare their quotes, those vendors would then transmit their offers to the contracting office utilizing the prescribed blockchain-based system, which would leverage the pre-defined smart contract business logic to record the transaction and assign a date/time stamp as proof of submission.[4] For ease of processing and evaluation, the government could require that the quote be provided through automatically populating a pre-established eForm again based on pre-determined smart contract business logic.

Step 6. Evaluation of Quotes

Step 7. Award Decision

A traditional federal procurement process normally goes through a manual evaluation and decision-making process. This process involves multiple components:

- A review to determine if the offer is "responsive" (i.e., meets requirements of the RFQ);
- A technical review of the offer to ensure proposed solution meets the technical requirements of the RFQ; and
- A review of price.

If the quotes are prepared in accordance with the standards set forth in the RFQ and the required eForms, Step 6, Evaluation of Quotes, and Step 7, Award Decision, should be relatively straight forward and easy to complete. The quotes would be provided in a manner that allows the smart contract business logic to compile the information, to filter out non-compliant quotes, and to compare "apples to apples." Lastly, evaluations and awards could be further simplified by building in the template the smart contract business logic that can provide the contracting officer with quotes that are pre-organized for ease of analysis and automatic export into an award decision document that has also been built into the pre-determined smart contract business logic.

By automating the requirements package inputs, the RFQ, and the mandatory structure of the quotes, the information can be screened, consolidated, and organized in a manner that allows the contracting officer to simply validate the information and certify the award decision result.[5] This result would also be recorded on the blockchain and the associated files would be archived in distributed storage. This step would also include the contracting officer's task of preparing the award document. Normally the award document would be prepared using government forms SF 1449 or DD 1155, which are generated utilizing federal contracting systems, outside of the smart contract construct. Once the award is executed in the government contracting system, the award document could be extracted and fed back into the blockchain. It may also be possible to integrate directly into the government contracting system depending on the nature of the interfaces and technical architecture.

Step 8. Award Notification

Once the contracting officer receives internal approval and signs the contract, he/she would traditionally transmit that contract to the awardee via email. Similarly, all unsuccessful offerors would receive a letter via email notifying informing them that they were not selected

[4] Note: this is a particularly useful feature when there are questions regarding the timeliness and acceptability of the offeror's quote.

[5] This assumes the contracting officer adopts a "lowest-price technically acceptable" selection approach, which is highly compatible with the procurement of COTS.

for award and providing them with pertinent information (i.e., name of awardee, amount of award, etc.).

The process of Award Notification involves nothing more than the transmittal of information—a process that a blockchain-based smart contract can be easily designed to support with the corresponding business logic built-in. Once an award decision is made by the contracting officer, that information could be quickly processed using smart contract business logic in the form of a template/letter notifying all interested parties of the selected awardee and relevant award information. The information would be transmitted, and delivery would be recorded on the blockchain providing the government an error free proof of receipt. This approach saves the government time in preparing award notification, and instead allows the contracting officer to focus on his or her review responsibilities, rather than getting bogged down in administrative tasks that can be executed as part of the smart contract's automated business logic.

Step 9. Tracking Contract Performance

Step 10. Contract Payment

Since this use case involves the procurement of a software solution, the government function of tracking performance is greatly simplified. The actual software license generally is treated as a supply purchase, and performance is met when the software is delivered. The ongoing software support services (i.e., patches, help desk, troubleshooting support) is normally treated as a subscription. As with delivery of software, the support subscription is typically considered complete and payment is made when the subscription services are initiated. No long-term contractor performance surveillance is required for the follow-on upgrades, patches, and help desk support. Agencies utilize multiple methods for certifying delivery. Most agencies use electronic systems such as the DoD's Wide Area Workflow (WAWF) System to certify when delivery occurs, which triggers an authorization to make payment.

As stated above, the oversight and payment processes are already highly automated. As such, a blockchain-based smart contracts approach would have to be fully integrated into these existing systems in order to record those activities. Alternatively, a new system could be implemented which could automatically track delivery of software and support services with the vendor notifying the government when both were provided (like the smartphone app used by Amazon). The government could utilize this same system to confirm receipt and authorize payment utilizing a Government Purchase Card rather than electronic funds transfer. All transactions would be recorded on the blockchain and executed based upon the pre-defined business logic built into the smart contract for the software. This approach would require special authorizations and would likely have to meet or exceed the requirements of the Prompt Payment Act of 1982 (FAR 12.301(b)(3) and FAR 52.212-4).

By utilizing a smart contracts approach and the use of the Government Purchase Card, payment could be made automatically within hours of receipt of the software and subscription services, rather than some 30 days later. This would be much more in-line with commercial best practices and would encourage the vendor to offer more competitive pricing to the government as well as reduce risk of incurring interest penalties. Moreover, this would reduce the burden to smaller or other non-traditional government vendors who simply can't wait a month to get paid for a good or service that has been delivered and accepted by a customer.

Step 11. Contract Closeout

Finally, after the transaction is fully completed, all goods are provided and services are received, the contracting office is normally required to “closeout” the contract for archiving and eventual destruction. In many offices, this is performed utilizing a manual process. Specifically, a government employee or contractor will review the contract and determine if there are any outstanding disbursement balances. If all payments have been made, the employee will prepare a close-out document for contracting officer approval and add it to the contract file. If outstanding unpaid balances exist, the file is set aside for further resolution.

Many organizations already have an automated closeout process for simple, low-dollar acquisitions. This type of transaction could easily be applied by building the closeout process into the smart contract business logic. The simple smart contract agreement could consider easily programable syntax questions whereby the answers have already been recorded as previous transactions on the blockchain such as the following:

- Final payment made (Y/N)?
- Outstanding/undispersed funds(Y/N)?
- Any outstanding performance issues(Y/N)?
- Is it now 30 days or greater beyond performance end-date (Y/N)?

By applying this process, the government would no longer have to manually review each file. Instead, they could focus on only those files that need special adjudication, saving both considerable time and resources.

Applicability of This Use Case

As shown above, the employment of blockchain-based smart contracts could greatly improve the trust, autonomy, and security within a simple procurement of software licenses under Federal Supply Schedules. Once greater trust, autonomy, and security are introduced into the procurement system, it permits business processes to be re-engineered purposefully to reduce the redundancy and inefficiency. As described, such inefficiency is often built-in as a result of the numerous errors that occur in a manually driven, centrally managed environment. Speed, accuracy, and efficiency all become second order benefits realized upon the blockchain paradigm shift once embraced by the organization.

Can this approach be used to procure software outside of Federal Supply Schedules? The simple answer is yes. Use of the above discussed blockchain-based smart contracts process can be leveraged in procuring COTS when utilizing other software GWAC vehicles.

One of the first examples for additional consideration to implement blockchain-based smart contracts is the DoD’s family of Enterprise Software Agreements (ESAs) which provide a full complement of pre-negotiated COTS blanket purchase agreements (BPAs) to provide Remedy, Adobe, Redhat, SAP, and numerous other software and support solutions.

Another primary source of COTS for civilian federal agencies is NASA’s Solutions for Enterprise-Wide Procurement (SEWP) V GWAC, providing a full complement of IT commercial software products through multiple-award Indefinite Delivery/Indefinite Quantity (IDIQ) contracts. In both cases, a similar approach can be used to build, validate and fund the requirements package, as well as execute many of the same contracting process steps outlined in this case using machine-logic.

Barriers to Implementation of the Smart Contracts Prototype

As with any proposed innovative solution, there are often obstacles that need to be overcome for successful implementation. The following is a discussion of three potential barriers to employing this technology in a federal acquisition environment.

- **Contracting Officer Discretion.** It must be acknowledged that by its very nature contracting absolutely must involve the business judgement of a warranted contracting officer. If the government were to develop a blockchain-based smart contract system to procure simple goods and services, it cannot (at least in the short term) replace automated business logic built into smart contracts with individual contracting officer judgement in a few key areas: Determination of Acquisition Strategy; Determination of the Best Value of the Government; and Final Selection of the contract awardee. All these determinations are inherently governmental, reside exclusively with the contracting officer, and must be completed before he/she will make a contract award obligation on behalf of the government. Accordingly, any established blockchain-based smart contracts process must make room for contracting officer discretion in the award process for procurement of software.

- **Brand Name and Related Competition Concerns.** The FAR spends considerable time laying out special rules and processes for acquiring “brand name” solutions (See FAR 6.302-1(c), 8.405-1(e), and 8.405-6(b)), which requires requiring activities to explicitly identify and justify those “salient characteristics” associated with the “brand name” product in order to foster a more fair and just competitive environment. This issue is especially pronounced when multiple firms produce a COTS product that is of a similar type. For instance, there are multiple COTS solutions that provide security protections for laptops (i.e., Symantec, McAfee, Kaspersky, Bitdefender). The FAR normally prohibits the customer from arbitrarily selecting their preferred product. Instead, the FAR requires the government to define the salient characteristics needed for that software (in this case security software) and allows the entire segment of industry to compete in the RFQ. Unless Congress is willing to relax the requirements of the brand name restriction, this will remain an impediment to simplifying Step 1, Determination of a Requirement. The smart contract business logic could be programmed to leverage previous software contract performance characteristics as part of the process to generate a new agreement.

- **Scale.** The point of employing blockchain-based smart contracts into acquisition of software process is to realize organizational efficiencies and savings that come with improving trust, autonomy, and security in the process. It must also be recognized that building a blockchain-based smart contract solution also requires government resources. The agency exploring the use of this solution should perform a cost/benefit analysis to determine if the return (benefits achieved in software acquisition) are worth the investment (resources needed to build the system). While the return on investment (ROI) results will vary for each agency, one common premise exists—the scale of the software requirement(s) is determinative. In other words, the greater the scale for COTS software need across a department, agency or government-wide, the more benefit that a blockchain-based smart contracts solution provides.

- **Legal Concept of Remedy.** If something goes wrong in paper based legal system, the “remedy” is very malleable. In a blockchain-enabled world, the "remedy" is a set of additional blockchain transactions. This requires an updated mindset, and a blockchain-enabled capability that can distinguish between the original transactions, recognition of an issue, and the remedy transactions.

Conclusions and Recommendations for Successful Implementation of the Smart Contracts

It is unlikely that the government will ever be able to make the software acquisition process completely mirror industry best practices. However, tremendous progress can be made in working towards achievement of that goal by improving trust, autonomy, and security in the process that can ultimately result in improved efficiency and cost savings for the government.

In order to make the successful implementation of blockchain-based smart contracts, there are several special considerations related to software acquisition that need to be in place. First, the agency needs to have access and authority to utilize enterprise-sized software acquisition vehicles to achieve savings through economies of scale such as the GSA's IT 70 or the DoD's ESAs. It's not enough to make the existing in-house process simpler as a result of the introduction of blockchain technology that adds trust, autonomy and accuracy to business operations which will ultimately yield greater efficiencies and cost savings.

Second, the efficacy of using a blockchain-based smart contract solution would be increased significantly if, in the requirements development step, the customers are able to select COTS solutions that are pre-approved by the agency for use and are not be required to develop a list of "salient characteristics" needed for software procurement. In other words, the agency needs to establish pre-competed COTS solutions for agency use within software segments of competing vendors (i.e., Symantec vs. McAffe, ArcGIS vs. Geosoft, Tableau vs. Lumira). By establishing agency-wide pre-selected/pre-competed solutions, the government enables more standardized contracting requirements, as well as terms and conditions that can be built into the smart contract business logic.

Third, establish pre-set requirements needed to receive software validation approval which can be built into the smart contract business logic. Organizations may be compelled to procure software for an entire group of people, even though only a small subset of users require it. Normally, this rationing or scrutiny is applied during the validation step. In order to make this step go much smoother, it would help if the agency CIO publish pre-established screening criteria or other thresholds that must be met in order to receive requirement validation approval. Without clear, definitive guidance on what "will or won't fly" with the CIO, customers may unwittingly be wasting their time seeking validation of their software request. With clear guidance from the CIO representative, this ambiguity is reduced or eliminated.

References

Arrietta, J., & Hager, T. (n.d.). HHS emerging technology. Retrieved from https://www.actiac.org/system/files/ACT-IAC HHS Emerging Technology Day.pdf

Bahuguna, A. (2018, July 24). Blockchain smart contract security—Blog by Saama. Retrieved from https://www.saama.com/blog/blockchain-smart-contract-security/

BBVA. (2018, April 26). What is the difference between DLT and blockchain. Retrieved from https://www.bbva.com/en/difference-dlt-blockchain/

Belin, O. (n.d.). The difference between blockchain & distributed ledger technology. Retrieved from https://tradeix.com/distributed-ledger-technology/

Blockgeeks. (n.d.). Smart contracts: The blockchain technology that will replace lawyers. Retrieved from https://blockgeeks.com/guides/smart-contracts/

Bryson, D., Goldenberg, D. C., Penny, D., & Serrao, G. (2017). Blockchain technology for government. Montgomery, AL: The MITRE Corporation.

Buntinx, J. (2017, March 25). Distributed ledger technology vs blockchain technology. Retrieved from https://themerkle.com/distributed-ledger-technology-vs-blockchain-technology/

Centralization vs. decentralization. (n.d.). Retrieved from https://blockchain.wtf/what-the-faq/centralization-vs-decentralization/

Chesebro, R. (2015, February). A contract that manages itself. Retrieved from https://apps.dtic.mil/dtic/tr/fulltext/u2/a620401.pdf

Choudhury, O., Sarker, H., Rudolph, N., Foreman, M., Fay, N., Dhuliawala, M., … & Das, A. (n.d.). Human subject regulations using blockchain and smart contracts. Blockchain in Healthcare Today. Retrieved from https://doi.org/10.30953/bhty.v1.10

De, N. (2017, October 24). HHS architect talks blockchain’s potential role in healthcare administration. Retrieved from https://www.coindesk.com/hhs-it-architect-talks-blockchain-white-paper-results?amp

DeBreuck, F. (2018, July 5). The core principles of smart contracts. Retrieved from https://www.openaccessgovernment.org/the-core-principles-of-smart-contracts/47369/

Dikusar, A. (2017, October 17). Smart contracts: Industry examples and use cases for business. Retrieved from https://xbsoftware.com/blog/smart-contracts-use-cases/

Dimov, D., & Juzenaite, R. (2016, August 17). Security of smart contracts. Retrieved from https://resources.infosecinstitute.com/security-smart-contracts/#gref

Dobesh, S. (2017, November 14). Blockchain for additive manufacturing to optimize DoD supply chains. Retrieved from https://www.gbaglobal.org/blockchain-additive-manufacturing-optimize-dod-supply-chains/

Federal Acquisition Regulation (FAR), 48 C.F.R. 12.301 (2019).

Federal Acquisition Regulation (FAR), 48 C.F.R. 52.212-4 (2019).

Federal Acquisition Regulation (FAR), 48 C.F.R. 6.302-1 (2019).

Federal Acquisition Regulation (FAR), 48 C.F.R. 8.405-1 (2019).

Federal Acquisition Regulation (FAR), 48 C.F.R. 8.405-6 (2019).

Frank, J., Newhard, A., & Silverstein, S. (2018, October 3). How smart contracts will work. Retrieved from https://www.businessinsider.com/how-smart-contracts-can-work-2018-10

Friedman, S. (2017, September 21). GSA looks to blockchain for speeding procurement processes. Retrieved from https://gcn.com/Articles/2017/09/21/GSA-looks-to-blockchain-for-procurement.aspx?m=1

GitHub. (n.d.). Awesome smart contracts. Retrieved from https://github.com/Overtorment/awesome-smart-contracts

Greenspan, G. (2016, March 17). Blockchains vs. centralized databases. Retrieved from https://www.multichain.com/blog/2016/03/blockchains-vs-centralized-databases/

GSA. (2019, February 26). Blockchain. Retrieved from https://www.gsa.gov/technology/government-it-initiatives/emerging-citizen-technology/blockchain

Hayzlett, J. (2018, February 15). 3 major industries in which blockchain technology is changing life as we know it. Retrieved from https://www.entrepreneur.com/article/308987

Hertig, A. (n.d.). How do ethereum smart contracts work? Retrieved from https://www.coindesk.com/information/ethereum-smart-contracts-work

Department of Health and Human Services (HHS). (2018, March 13). HHS announces health data provenance challenge winners. Retrieved from https://www.hhs.gov/about/news/2018/03/13/hhs-announces-health-data-provenance-challenge-winners.html

Jeremy, Y. (2017, August 24). DoD eyes blockchain technology to improve cybersecurity. Retrieved from https://www.dlt.com/blog/2017/08/24/dod-eyes-blockchain-technology-improve-cybersecurity/

Johnson, D. B. (2018, January 3). Will 2018 be the year for blockchain for government? Retrieved from https://fcw.com/articles/2018/01/03/blockchain-goverment-hype-reality.aspx?m=1

Kariuki, D. (2018, April 13). Blockchain use-cases in enhancing government services. Retrieved from https://www.cryptomorrow.com/2018/04/13/blockchain-use-cases-in-enhancing-government-services/

Kashyap, R. (2018, July 31). DLT vs. blockchain. Retrieved from https://cryptodigestnews.com/dlt-vs-blockchain-a4f7b97f8b2c

Kendall, F. (2014, September 19). Better buying power 3.0 [White paper]. Retrieved from http://www.acqnotes.com/Attachments/Better-Buying-Power-3.0-White-Power.pdf

Kirkman, S. S., & Newman, R. (2017). Using smart contracts and blockchains to support consumer. Retrieved from https://csce.ucmss.com/books/LFS/CSREA2017/GCC3688.pdf

Lomas, N. (2018, March 27). Zuckerberg refuses UK Parliament summons over Fb data misuse. Retrieved from https://techcrunch.com/story/facebook-responds-to-data-misuse/

Martin, Z. (2016, February 11). Blockchain partnership, GSA deploys identity-monitoring tool. Retrieved from https://www.secureidnews.com/news-item/blockchain-partnership-gsa-deploys-identity-monitoring-tool/

McConaghy, T. (2017, July 15). Blockchain infrastructure landscape: A first principles framing. Retrieved from https://medium.com/@trentmc0/blockchain-infrastructure-landscape-a-first-principles-framing-92cc5549bafe

Mearian, L. (2018, February 14). IBM sees blockchain as ready for government use. Retrieved from https://www.computerworld.com/article/3254202/ibm-sees-blockchain-as-ready-for-gover

Moehrke, J. (2016, August 29). Blockchain and smart-contracts applied to evidence notebook. Retrieved from https://healthcaresecprivacy.blogspot.com/2016/08/blockchain-and-smart-contracts-applied.html?m=1

Nayak, N., & Nguyen, D. T. (2018, March 27). Blockchain, AI and robotics: How future tech will simplify federal procurement. Retrieved from https://www.federaltimes.com/acquisition/2018/03/23/blockchain-ai-and-robotics-how-future-tech-will-simplify-federal-procurement/

Nene, V. (2018, October 19). Smart contracts for drones using blockchain. Retrieved from https://dronebelow.com/2018/10/19/smart-contract-for-drones-using-blockchain/

Novak, M. (2017, September 22). Blockchain & smart contracts for government entitlements & payments. Retrieved from https://www.slideshare.net/MichaelNovak9/blockchain-smart-contracts-for-government-entitlements-payments

Ozelli, S. (2018, January 23). US government implements blockchain programs to improve transparency and efficiency: Expert blog. Retrieved from https://cointelegraph.com/news/us-government-implements-blockchain-programs-to-improve-transparency-and-efficiency-expert-blog

P., H. (2018, July 12). Smart contracts use cases and examples in blockchain (Simple guide). Retrieved from https://itradeico.com/2018/07/smart-contracts-use-cases-and-examples-in-blockchain-simple-guide/10945

Petersen, J. (2018, October 22). IDC report describes HHS implementation of blockchain in acquisition record-keeping. Retrieved from https://www.executivegov.com/2018/10/idc-report-describes-hhs-implementation-of-blockchain-in-acquisition-record-keeping/

PolySwarm. (2018, March 7). 5 companies already brilliantly using smart contracts. Retrieved from https://medium.com/polyswarm/5-companies-already-brilliantly-using-smart-contracts-ac49f3d5c431

Radocchia, S. (2017, November 9). What are some ways blockchain smart contracts can improve government? Retrieved from https://www.quora.com/What-are-some-ways-blockchain-smart-contracts-can-improve-government

Ryan, P. (2017, October). Smart contract relations in e-commerce: Legal implications of exchanges onducted on the blockchain. Retrieved from https://timreview.ca/sites/default/files/article_PDF/Ryan_TIMReview_October2017.pdf

Schneider, T. K. (2018, July 23). HHS unveils blockchain-powered acquisition assistance. Retrieved from https://gcn.com/articles/2018/07/23/hhs-blockchain.aspx?m=1

Serbu, J. (2017, February 28). The legacy of better buying power: DoD's gambit to reform acquisition "from within." Retrieved from https://federalnewsnetwork.com/defense/2017/02/bbpndaa-special-report-part-1/

Sharma, M., Ramakrishnan, A., & Rahgozar, A. (2018, June 4). The possibilities of blockchain: Use cases for B2B, B2C and government services. Retrieved from https://tech.economictimes.indiatimes.com/news/corporate/the-possibilities-of-blockchain-use-cases-for-b2b-b2c-and-government-services/64411513

Shrier, A. A., Chang, A., Diakun-thibault, N., Forni, L., Landa, F., Mayo, J., & Van Riezen, R. (2016, August 8). Blockchain and health IT: Algorithms, privacy, and data. Retrieved from http://blocktonite.com/wp-content/uploads/2017/04/15-Winning-HHS-Papers-on-Blockchain-09.2016.pdf

Singh, P. (2018, February 2). What's the difference between blockchain and a database. Retrieved from https://www.quora.com/Whats-the-difference-between-blockchain-and-a-database

Stephenson, C. (2017, June 26). GSA calls for blockchain and machine learning to speed acquisition. Retrieved from https://www.fedscoop.com/gsa-calls-blockchain-machine-learning-speed-acquisition/

Tabora, V. (2018, August 4). Databases and blockchains, the difference is in their purpose and design. Retrieved from https://hackernoon.com/databases-and-blockchains-the-difference-is-in-their-purpose-and-design-56ba6335778b

Waedt, H. (n.d.). 10 use cases: Blockchain for the government. Retrieved from https://www.linkedin.com/pulse/10-use-cases-blockchain-government-holger-waedt/

ACQUISITION RESEARCH PROGRAM
GRADUATE SCHOOL OF BUSINESS & PUBLIC POLICY
NAVAL POSTGRADUATE SCHOOL
555 DYER ROAD, INGERSOLL HALL
MONTEREY, CA 93943

www.acquisitionresearch.net