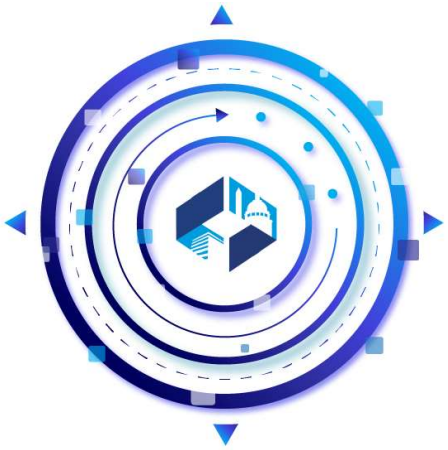
American Council for Technology – Industry Advisory Council



ACT-IAC

ENABLING BLOCKCHAIN INNOVATION IN THE U.S. FEDERAL GOVERNMENT

A Blockchain Primer

EMERGING TECHNOLOGY Community of Interest

Blockchain Working Group

Enabling Blockchain Innovation in the U.S. Federal Government

Date Released: October 16, 2017

Synopsis

This Primer is intended to be a foundational tool in the understanding of blockchain and its use cases within the United States federal government. To that end, it should help allay the concerns that some may have about this new technology by providing an introduction to blockchain and its related technologies, and how blockchain can be safely and securely applied to the right government use cases.

Blockchain has the potential to help government to reduce fraud, errors and the cost of paper-intensive processes, while enabling collaboration across multiple divisions and agencies to provide more efficient and effective services to citizens. Moreover, the adoption of blockchain may also allow governmental agencies to provide new value-added services to businesses and others which can generate new sources of revenue for these agencies.

American Council for Technology-Industry Advisory Council (ACT-IAC)

The American Council for Technology (ACT) is a non-profit educational organization established to create a more effective and innovative government. ACT-IAC provides a unique, objective, and trusted forum where government and industry executives are working together to improve public services and agency operations through the use of technology. ACT-IAC contributes to better communications between government and industry, collaborative and innovative problem solving, and a more professional and qualified workforce.

The information, conclusions, and recommendations contained in this publication were produced by volunteers from government and industry who share the ACT-IAC vision of a more effective and innovative government. ACT-IAC volunteers represent a wide diversity of organizations (public and private) and functions. These volunteers use the ACT-IAC collaborative process, refined over thirty years of experience, to produce outcomes that are consensus-based. The findings and recommendations contained in this report are based on consensus and do not represent the views of any particular individual or organization.

To maintain the objectivity and integrity of its collaborative process, ACT-IAC does not accept government funding.

ACT-IAC welcomes the participation of all public and private organizations committed to improving the delivery of public services through the effective and efficient use of IT. For additional information, visit the ACT-IAC website at www.actiac.org.

Emerging Technology Community of Interest

ACT-IAC, through the Emerging Technology Community of Interest, formed a Blockchain Working Group to give voice to and provide an authoritative resource for government agencies looking to understand and incorporate blockchain technology and functionality into their organizations. This working group includes government and industry thought leaders incubating government blockchain use cases. The ACT-IAC Emerging Technology Community of Interest (ET COI) mission is to provide an energetic, collaborative consortium comprised of leading practitioners in data science, technology, and research, engaged with industry, academia, and public officials and executives focused on emerging and leading technologies which transform public sector capabilities.

Disclaimer

This document has been prepared to contribute to a more effective, efficient, and innovative government. The information contained in this report is the result of a collaborative process in which

a number of individuals participated. This document does not – nor is it intended to – endorse or recommend any specific technology, product, or vendor. Moreover, the views expressed in this document do not necessarily represent the official views of the individuals and organizations that participated in its development. Every effort has been made to present accurate and reliable information in this report. However, ACT-IAC assumes no responsibility for consequences resulting from the use of the information herein.

Copyright

Further Information

For further information, contact the American Council for Technology-Industry Advisory Council at (703) 208-4800 or www.actiac.org.

This page is left blank intentionally

Contents

Executive Summary

The ACT-IAC Emerging Technology Community of Interest (COI) launched a Blockchain Working Group in May 2017, at the request of the Government Services Administration (GSA), to provide an authoritative resource for government agencies trying to understand and incorporate blockchain functionality into their organizations. The volunteer participants of the Blockchain Working Group represent more than a dozen federal agencies and a variety of industry partners to craft this blockchain "primer" to help incubate government blockchain use cases. Following this primer, the working group will craft a "playbook" on approaches to use blockchain within the government.

Blockchain technology began as the underpinning of a distributed ledger platform for cryptocurrencies, such as bitcoin, providing a way to securely and transparently store information in near real-time thereby providing transaction confidence in a trustless environment. The value of blockchain is in the distributed and tamper-resistant nature of its transaction recording, also known as the "ledger." A blockchain-based ledger also serves as a "distributed source of truth" for transactions. This type distributed ledger can be used to create an encrypted listing of assets or other records shared across a network of multiple sites. Any participant in the network can have their own identical copy of the ledger with each set of changes to the state of the ledger linked to the immediately preceding ledger-state. These changes are then cascaded to all network participants within minutes or even seconds, making ledger records maintained this way highly tamper-proof and resistant to subsequent unauthorized changes. Assets tracked on the blockchain could be financial, legal, physical, or electronic, with military-grade encryption providing security and accuracy about the transaction.[1]

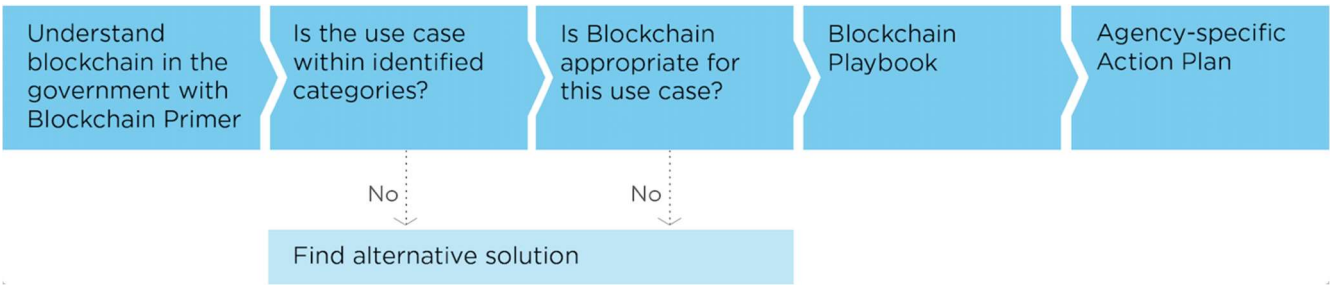
The algorithmic techniques used in blockchain and digital ledger technology have extended well-beyond its origins in cryptocurrencies to become tools to record, enable, and secure huge numbers and varieties of transactions, incorporating rules, smart contracts, and digital signatures among many new and emerging technologies. This technology has the potential to revolutionize the way the business of government is transacted, including the capture of voter information; collection of personal and corporate taxes; identification of recipients of healthcare, financial support and emergency aid; issuance of passports and visas; recording of patents and trademarks registries; recording of marriage, birth and death certificates; provenance (including jurisdiction of origin) and movement of goods and services to and within the U.S. market; regulation, verification and transfer between U.S. government agencies of government digital assets including federal funds, licenses, and personnel data; and generally to ensure the integrity of government records[2]. Although advances have been made at the state level in the use of blockchain, the U.S. lags behind many other countries in the use of blockchain to support the business of government.

It is important to understand that the association of blockchain with cryptocurrencies, like Bitcoin that also uses the technology, can cause suspicion among citizenry and government entities because of

Bitcoin's association with criminal transactions, ransomware, and "dark web" trading sites.[3] These activities have sensationalized the use of the underlying blockchain technology, in some cases instilling a misplaced sense of fear and casting the legitimate uses of the technology in a negative light. Another challenge to consider is the confusing combination of terminology and technologies that surround blockchain. Though all the potential uses or abuses of blockchain cannot be foreseen, it is important to know that it is rooted in a foundation of security, transparency, and integrity.

For agencies looking to embark on the blockchain journey, it is important to start with the foundational concepts and government use cases through this primer. The necessary steps are:

1. Understand the foundational elements of blockchain with this primer.
2. Research the government use cases to ensure best fit.
3. Consult the Blockchain Playbook to understand the steps and technology required.
4. Tailor an agency-specific plan with plays from the Playbook.

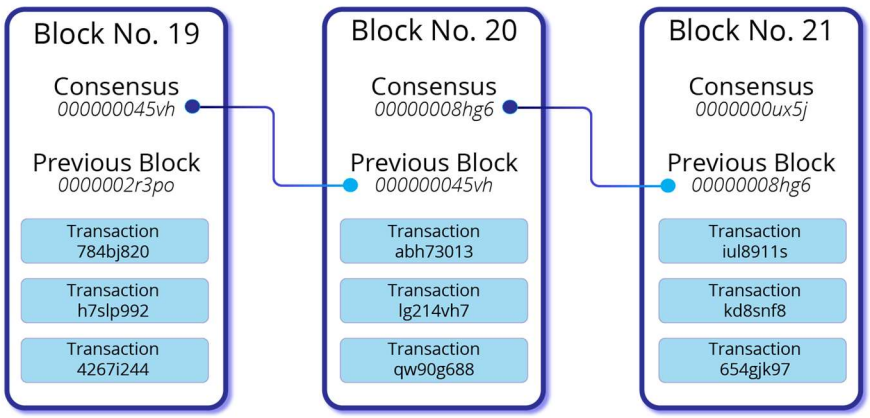


This primer is intended as a foundational tool in the understanding of blockchain and its use cases within the U.S. federal government to help allay fears that accompany this new technology. Blockchain has the potential to help government to reduce fraud, errors, and the cost of paper-intensive processes.

Definitions

Since blockchain is still new, it is important to first define a few technology and business terms. Standard definitions are yet to be agreed upon by all the blockchain technologists and user communities; however, the following terms and their explanations are what most people use while explaining the technology behind blockchain.

Blockchain: A blockchain is a type of distributed ledger "that stores a continuously growing list of grouped records, called blocks, which are linked and secured using cryptography."[4] Each block of records is "chained" to the next block using a cryptographic signature or hash. Because of this cryptographic link, every new block contains a reference to the immediately previous block, a timestamp, and any transaction data.[5] This improves the security of the distributed ledger and makes unauthorized additions, alterations, or deletions extremely difficult, if not impossible, to perform, hide or obfuscate.[6]



Consensus: Consensus is an umbrella term given to the variety of ways to assure the accuracy of a distributed ledger and accept or reject changes across the network. Different blockchain networks may use different consensus mechanisms - examples of consensus mechanisms include proof-of-work (PoW) and proof-of-stake (PoS). This quickly becomes a very complex topic; however, the important point is that the consensus mechanism used by a blockchain network is how additions are agreed upon and accepted. [7]

Cryptographic Hash: A cryptographic hash is a digital fingerprint of data. These fingerprints can be generated and used to very easily determine if two data sets match. This allows two or more parties to verify the accuracy of data without sharing the actual data. When a user logs into their bank, a cryptographic hash is often used to protect the password from being intercepted online. By comparing the digital fingerprint of the password, the user just entered with the password stored, the user's password is never transmitted but can be verified to allow access.[8]

Cryptography: "Cryptography is the practice and study of techniques for secure communication in the presence of third parties (adversaries)."[9]

Cryptocurrency: "A cryptocurrency is a digital asset designed to work as a medium of exchange using cryptography to secure the transactions and to control the creation of additional units of the currency."[10,11] "Cryptocurrencies are classified as a subset of digital currencies and are also classified

as a subset of alternative currencies and virtual currencies. Bitcoin is an example of a cryptocurrency."[12]

Digital Asset: "A digital asset...is anything that exists in a [computerized] binary format and comes with the right to use." These include but are not exclusive to: digital documents, audio content, motion picture, and other relevant digital data that are currently in circulation or are, or will be stored on digital appliances.[13]

Distributed Ledger: "A distributed ledger is a [decentralized] database that is consensually shared and synchronized [over a] network spread across multiple sites, institutions or geographies." Each participating node on the ledger can access the records shared across that network and generally maintains an identical copy of it. Any changes or additions made to the ledger are reflected and copied to all participants in a matter of seconds or minutes. Not all nodes that have access to, and can read data from, the ledger are able also to write to the ledger or create new entries. A blockchain is a type of distributed ledger.[15]

Blockchain and Distributed Ledger[14]

The terms "distributed ledger" and "blockchain" are often treated as synonyms in the industry, even though blockchain is a specific type of distributed ledger.

A distributed ledger can be implemented in many ways.

A distributed ledger can use any mechanism and protocol to share the ledger, achieve consensus, enable smart contracts, and provide a tamper-proof record of all its transactions.

Node: "In [communication] networks, a node is either a redistribution point or a communication endpoint."[16] In a peer-to-peer, distributed system like blockchain, every server touch-point is a node. Within blockchain, it is the "computer connected to the blockchain network using a client that performs the task of validating and relaying transactions."[17] This client gets a copy of the blockchain ledger downloaded automatically upon joining the blockchain network.[18]

Oracle: A trusted source of information about the real world maintained in an electronic form that can be accessed by a blockchain network. An example would be a database of interest rates that is accessed by a smart contract to allow the calculation of the amount of interest payable on a loan maintained as a digital asset.

Permissionless or Public Distributed Ledgers: A permissionless distributed ledger allows all the participants maintaining a full node on the ledger to contribute data to the ledger with all participants possessing an identical copy of the ledger. The consensus mechanism is also open to all the participants maintaining a full node. In these ledgers, there is *no single owner* of the ledger, which means that no single actor can prevent a transaction from being added to the ledger. "Participants maintain the integrity of the ledger by reaching a consensus about its state." These ledgers can be used as a tamper-resistant global record and are most suitable for non-regulated public use cases, where there is little-to-no trust between participants. **[19]**

Permissioned or Private Distributed Ledgers: Permissioned distributed ledgers allow access to identical copies of a ledger to a limited number of preselected trusted participants only. When a new record is added, the ledger's integrity is confirmed by a limited consensus process by trusted actors

only. This makes maintaining a shared record much simpler as compared to the permissionless ledgers. These ledgers may have one or more owners and hence are most suitable for inter/intra organization use cases, requiring simplicity, speed, and greater transparency, where there is some level of trust between participants. [20]

Smart Contracts: Smart contracts are small computer programs that rely on a distributed ledger system like a blockchain for execution. While smart contracts have a range of applications, they can be used to manage data and assets stored on a distributed ledger or blockchain, and model all or parts of legal agreements to create self-executing contracts with the terms of the agreement between the parties being directly written into lines of software code instead of natural human language (e.g., English) in a document or on paper. This code is maintained and runs across all nodes of a distributed ledger system and can potentially execute in an autonomous manner. Smart contracts can be triggered by trusted transactions to execute the agreements, "among disparate, anonymous parties without the need for a central authority, legal system, or external enforcement mechanism."[21] They render transactions traceable, transparent, and irreversible.

Smart Oracles: Smart oracles combine the idea of an oracle within the concept of smart contracts. "Separating the untrusted code execution from distributed networks reduces the complexity and thus increases the security of both systems." [22]

Transaction: In the context of blockchain, a transaction is a transfer of assets in or out of a ledger.[23]

Distributed Ledger / Blockchain Technology

Distributed Ledger Technology, or DLT for short, provides a way of securely and transparently storing information digitally. DLT brings together a combination of technological advantages such as peer-to-peer networking, distributed data storage, and cryptography to achieve consensus on the validity of a transaction. In addition, DLT operations can be pre-programmed to automate business processes that interact with the ledger. Blockchain technology is a specific form of distributed ledger technology.

Takeaways - DLT

Distributed Ledger Technology (DLT) uses a shared distributed replicated database to more efficiently transact between parties with varying degrees of trust.

Blockchains are an append-only type of DLT that record blocks of transactions to the ledger. Members of the network reach consensus before transactions are recorded.

Requirements around identity and information access should be considered when evaluating public versus private blockchain offerings.

Blockchains are not standalone systems. Integration with existing business processes, systems and interaction with partners must be considered.

Blockchain-as-a-Service is now being offered by vendors and may allow agencies to stand up a blockchain network more quickly and efficiently.

Similar to the functionality of a distributed ledger, a blockchain's core value is the ability to maintain an append-only book of record (i.e., the ledger or database). Transactions written to the ledger are tamper-resistant and hard to change. Updates generally can only be made by appending new information to the ledger record. The chain's stored data and data references serve as a multilaterally accepted common repository for members of the blockchain network. This is achieved using a cryptographic link between each block on the blockchain, as described in the Definitions section. Each blockchain network can be 'public', with open (or permissionless) access, or 'private', with permissioned access, and is jointly maintained. Participants submit transactions to the blockchain but no new data is accepted without consensus. Once consensus is reached by network members (called nodes), the transaction data is time-stamped and its corresponding metadata is appended to the end of the ledger in a permanent log and replicated to all other nodes (members) on the network, where applicable.

The consensus process is the means by which the various nodes on the blockchain verify that the new data obeys the rules and standards of that individual blockchain network and that the existing data maintains integrity. The security of a network generally grows with the number of members supporting consensus as more sharing and agreeing to data means that more nodes would need to be simultaneously tampered with (i.e., hacked) in any attempt to attack, corrupt, manipulate, or "fool" the system and its members' respectively contributing databases. Once consensus is reached (i.e., a majority of the nodes agree that the data is valid), data is then stored across the network of nodes as a new "block" in a chronological chain.

The decentralization characteristic of blockchains means that no central company, agency, or person owns the system but users can engage and transact while sharing maintenance and management. The collection of information stored in each block can consist of any digital transaction of content that includes simple text, structured messages, images, and videos. Because all nodes in a blockchain maintain all ledger records, for larger files, it is often more efficient to use a pointer or link to data stored "off-chain." A key decision for each individual blockchain implementation will be to determine what information is stored "on-chain" or in the ledger versus what information is stored "off-chain." Security controls and regulations may dictate some of these decisions when they involve PII (personally identifiable information) and/or PHI (protected health information) data. In these scenarios, the blockchain may contain both a pointer to the "off-chain" data along with a cryptographic hash used to validate that the data has not been tampered with.

Blockchains utilize cryptographic techniques such as digital signatures and cryptographic hash functions. Digital signatures are used to provide enhanced security by assuring that digital assets can only be transferred by valid owners. The use of digital signatures during the transfer of digital assets allows for the asset to be traced back from one cryptographic identity to the previous – all the way to the original creation of that digital asset. Cryptographic hash functions allow for data on the blockchain to be 'hashed' in each block, which results in the persistence of a mathematical fingerprint representing the respective information being stored. When a new block is written, the hashed value of the previous block is used to calculate the hashed value of the new block, thus creating this link between the blocks, forming the blockchain.

Distributed Ledger Networks

A peer-to-peer distributed ledger network may be a private or public blockchain. Public blockchains, sometimes also called permissionless blockchains, can allow users to be anonymous or pseudonymous and allow for open membership. These characteristics may not be suitable for all government use cases. Many organizations require greater control of transaction data where identity is required and accountability must be maintained.

Private blockchains, or permissioned blockchains, take a different approach. Participants must be invited to the network and have a known identity. They need the proper credentials to join the network and participate in transactions. The participant's identity and assigned permissions determine what information the participant may access or record on the ledger. Blockchain network participants for federal agencies could consist of one or more agencies, agency departments, commercial service providers, industry partners and other regulatory bodies. However, in a private blockchain, governance plays an important role in managing participant roles and is likely achieved through a central or multiple authorities (e.g., a governing body).

Participants in a distributed ledger may interact with the ledger directly, using smart contracts, and via intermediaries. Smart contracts may be invoked via application programing interfaces (APIs) to allow client applications to call for and execute a transaction. For example, a smart contract may contain executable rules allowing the transfer of the ownership of an asset from one participant to another once an agreed-upon action happens, such as a data or financial transaction. Smart contracts may also be used to process and orchestrate other business events as part of a transaction. By using smart contracts in conjunction with effective consensus agreement, networks may reduce the need for third-party intermediaries.

Blockchain-as-a-Service Emerges

As a result of both the complexity and diversity of the developing blockchain space and the continuing advancement of the technology more broadly, Blockchain-as-a-Service (BaaS)[24] has started to emerge in support of organizations exploring blockchain adoption. Similar to the shift in recent years towards Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS), BaaS will gain wider appeal and adoption as more organizations start to understand the benefits of blockchain. As different providers make blockchain technology functionally available, consumers and their organizations can have blockchain applications coded and built for them to help optimize and automate systems, processes, and business operations.[25]

This development provides a low barrier to entry for organizations wanting to explore blockchain applications. Additionally, as with other 'as-a-service' offerings, considering a service provider offers a few benefits. Those providers can help plan for a blockchain adoption and identify where optimizations can be made by leveraging their platform. This could significantly reduce the time required to deploy a new system, lower the cost of operations and maintenance, and organically provide support.

BaaS addresses several specific aspects, including:

- Externally facing distributed ledgers, such as peer-to-peer networks[26]
- Internally facing distributed ledgers (databases), meaning enterprise architecture for cross-business networks[27]
- Blockchain protocol data structure design (i.e., how an organization would define transactions and blocks)[28]
- Consortium (and resulting Peer-to-Peer network) management, governance, and related protocol creation[29]
- Smart contract programming and smart oracle implementation[30]
- Node management[31]
- Related software, system, and architectural model design[32]
- Related UI/UX design

Planning for an Evolving Landscape

Blockchain is continuing to evolve as governments and organizations around the world grapple with how best to properly employ the technology. As you consider how your agency or division might leverage blockchain, remember that the landscape will continue to change and some use cases might require more development prior to an achievable implementation. While the landscape is not fixed, there are major companies dedicated to this technology and their offerings are likely to become more stable as their customers depend on, and ultimately pay for, that stability.

When considering the utilization of DLT as part of a solution package, considerations include:

- Open source and open governance
- Permissioned versus permissionless blockchain approach
- Scalability, performance, auditability, and security requirements
- Development languages and tools are supported to develop smart contracts
- Extensibility needs, such as pluggable approach to consensus, identity, and encryption
- Usage of distributed consensus versus trusted third parties for transaction approval

Blockchain is not a single solution and it is not a technology that can be integrated in a plug-and-play manner. When architecting any blockchain solution, integration needs to be well thought out. Blockchain and DLT solutions either will need to completely replace or tightly integrate with existing systems. Smart contracts may trigger events or get called from internal or external business process systems. Data on the ledger may provide agencies with end-to-end views of an interagency business process. Analytics, cognitive, and machine learning capabilities can leverage trusted ledger data to improve business processes. Existing applications and microservices might trigger actions via secured APIs. New services may also be provided to citizens, businesses or other governmental players, potentially creating new revenue sources that can offset the cost of implementing blockchain technology. The possibilities are quite vast, so government actors will need to invest the proper time to plan any adoption of this new technology. Of course, planning ahead for an evolving landscape is not a new experience for any organization. Technology is always changing.

Benefits to the Business of Government

Although blockchain is still relatively new and there are few examples of blockchain in government, it is not difficult to identify the many potential benefits to the business of government that blockchain offers:

- Increased public trust achieved through transparent and verifiable platforms
- Increased citizen engagement through identity management and transaction validation
    - Electronic identities and records
    - Secure voting and verifiable results
    - Distributed registries for patents, property, settlements, etc.
- Transparent and traceable data
    - Acquisition and financial management
    - Procurement of goods and services
    - Supply chain management
- New revenue sources from value-add services
    - Automatically generated reports when information is updated (e.g., a new patent filed)
    - Cross-agency searches that save users time
    - New uses for census data

Almost every area of the public sector, from local to state to federal, could benefit from blockchain. For example, consider local businesses using a blockchain-based payroll and personnel system to leverage smart contracts to automate payments and reduce the risk of a missed pay period due to human error. Employees could complete their work, record their time in the company's performance blockchain, and get paid automatically by a smart contract function if their work passes a predetermined quality check. That same company could ensure that it meets state-mandated labor and safety reporting requirements by being connected to the state's safety tracking blockchain. Finally, both the company and the state could verify identities for employment and track employment records and taxes by leveraging the federal blockchains at the Internal Revenue Service and Department of Labor.

Among the many benefits of blockchain to the business of government, there are several specific use cases where blockchain could have an immediate impact. They include:

- **Citizen services** – including constituent engagement, voting, financial transactions, tax collection
- **Identity management** – including legal, birth, marriage, death, passport, visa, security tracking
- **Benefits management** – including Social Security, Medicare, Medicaid, Veterans Administration and many more
- **Contract management** – including vendor tracking, financial commitments and transactions, schedule tracking, performance tracking
- **Regulatory compliance** – including services deployment, timeline and schedule management, performance tracking, audit support and tracking
- **Disaster recovery** – including emergency supplies management and distribution, monetary donation tracking

Takeaways – Benefits to Government

Blockchain offers government:

- Public Trust
- Citizen Engagement
- Transparency
- New revenue sources

These benefits can be reflected in the following use cases:

- Citizen services
- Identity management
- Contract management
- Regulatory compliance

Some specific examples include:

- Health records could be completely secured and accessible at any hospital in the country simultaneously upon authorization by the patient or legal guardian (whose status also could be verifiable on another blockchain).
- Property titles and land ownership could be easily transferrable upon legal sale, negating the need for expensive and time-intensive third-party intermediary involvement.
- Mechanism for reducing friction in mission support systems and other shared services.
- Government agencies could vastly simplify their interagency operations via smart contracts, making government travel, leased vehicles, and facility management, at lower cost.

Realizing These Benefits

While the promise of blockchain is vast, the challenge of realizing these benefits is not insignificant. Any organization electing to implement a blockchain solution will first have to decide if blockchain is actually a good fit. To start that conversation, presented here are use cases specific to government.

Government Business Use Cases

While blockchain is widely adopted in private sector industries such as financial services and real estate, the opportunities for blockchain in government are only just starting to gain traction. Blockchain can be applied to use cases from contract management to aid tracking.

Blockchain can provide clear provenance and transfer of assets and ownership registries (deeds, jewelry, possessions); personal identification; identify attributes and attestations (health records, birth/marriage/death certificates); supply chain transfer chains (food products, machinery, weaponry); contract administration (contract identification, vendor awards, vendor payments); and healthcare, among many other use cases. It represents a cheaper, more secure, and publically auditable means of tracking, which would address major challenges governments have faced.

Takeaways – Evaluation Criteria to Consider

Is there a need to provide trust more efficiently when doing transactions in a business network?

Are there currently disputes or discrepancies between participants caused by invalid and/or incomplete data stored on existing systems of record?

Are there requirements to track the lifetime history of a part, record or an asset?

Are existing cross-organizational business processes manual or paper-based?

Can you implement this use case with a different technology such as a distributed database?

The core characteristics of blockchain make it suitable for business processes with certain types of requirements. When evaluating use cases, criteria to consider should include:

- Is there a need to more efficiently provide trust when transacting in a business network where participants may have little or no trust at all? Blockchain attributes such as consensus, a shared distributed ledger, and smart contracts add trust and transparency to use cases.
- Are there current disputes or discrepancies between participants caused by invalid and/or incomplete data stored on existing systems of record? The shared ledger can serve as a system of truth for transacting parties.
- Are there requirements to track the lifetime history of a part, record, or an asset? The ledger is append-only, which lends itself to the provenance of digitized assets or records.
- Are existing cross-organizational business processes manual or paper-based? Smart contracts can automate cross-organization business transactions and remove the need for third-party intermediaries.
- Can you implement this use case with a different technology such as a distributed database? Blockchain is still a relatively new and untested technology. Consider more mature existing technologies when appropriate.

Government at Work

Aid Tracking

In 2015, the Federal Emergency Management Agency (FEMA) began an initiative to transform the way the agency administers grants and disaster relief. The review came about in the wake of lessons learned from Hurricane Katrina (2005) when it spent over $61 billion in federal money,[33] and Superstorm Sandy (2012) when it spent $48 billion.[34] Over 450,000 people are expected to seek disaster assistance due to flooding from Hurricane Harvey (2017),[35] and a $7.9 billion bill to aid in the huge cost of storm damages.[36]

FEMA has initiated a Grants Management Modernization (GMM) program to streamline grants management across the agency's grant programs. In the same vein of modernization, FEMA can benefit from emerging technologies like blockchain to help improve the efficiency and effectiveness of FEMA's grant operations.[37]

Monitoring and controlling the use of grants is incredibly complex and subject to potential fraud or abuse. Using blockchain technology, FEMA can help reduce potential fraud and abuse through verification of assets, property, and land ownership. "Digitizing information about asset ownership and storing it on blockchain registers,"[38] can become a foolproof method to track true ownership of land registries and property titles. This verification can help ensure that FEMA disaster relief truly goes to those who own the property versus those who falsely claim ownership.

In addition to validation of assets, FEMA can use blockchain identity management to issue e-identities to citizens seeking aid and assistance. A blockchain e-identity can help ensure that FEMA has a unique record of every citizen and issue relief payments in a manner that is secure and transparent. This would eliminate the possibility of criminals using identity theft to pose as victims and receive financial assistance. A blockchain-based claims validation network can serve as a utility to record, in a blockchain ledger, all aid assistance issued and whether it was successfully received.[39]

By leveraging blockchain, FEMA has a unique opportunity to modernize and secure its processes, eliminate fraud and abuse, and provide transparency and accountability for its budget.

Contract Management

Federal, state, and local government buyers spent nearly $45 billion through General Services Administration (GSA) and Department of Veterans Affairs Schedule Contracts in fiscal year 2016.[40] To improve contract processing times and modernize contracting, GSA is piloting Distributed Ledger Technology along with machine learning and artificial intelligence (ML/AI). Currently moving through both the design and proof of concept phases, GSA is looking to use blockchain to intelligently automate the FASt Lane contract review process, reducing, "the amount of human interaction required to review new proposal documents, improve offeror experience," and reduce review time for proposal reviews to award.[41] GSA provides access to more than 25 million commercial products and services to federal, state, and local governments. Utilizing blockchain will aid in streamlining the order procedures while delivering agencies the tools and expertise needed to shorten procurement cycles, ensure compliance, and obtain the best value for innovative technology products, services, and solutions.[42]

Asset Tracking

The Department of Homeland Security (DHS) is using blockchain to transmit and store data collected by their operating devices used along various borders, from airports and ports to the borders with Mexico and Canada. With such a large amount of data, secure and transparent systems are essential for mission success. Although timing for implementation has not been disclosed, testing is currently being done to determine if a blockchain platform for this purpose is secure, efficient, and has the ability to transmit such large data amounts every day.

Healthcare

The Food and Drug Administration (FDA) has been exploring how blockchain can be used to exchange health information more efficiently and securely.[43] This includes the exchange of electronic medical records (EMRs) and other information such as genomic data, clinical trial information, and data collected from IOT devices and wearables. Blockchain can provide an audit trail by tracking changes to the EMR as well as help track and control access to the EMR. Blockchain can provide healthcare providers with the longitudinal data about a patient without having the actual protected health information (PHI) reside on the actual ledger.

Other Potential Use Cases

Improving Interagency Business Processes

Federal agencies need more efficient ways to transact and collaborate with other agencies and commercial entities. The challenge lies in the fact that interagency business processes are often manual or paper-based and need governance and data standards. There may be discrepancies in the information shared between agencies, or it may be incomplete. Regulations may also impede interactions between agencies and industry.

Agencies that are part of a blockchain network can securely and seamlessly share information stored on the shared ledger. Permissioned blockchain networks manage access to this information via blockchain access controls. The network agrees on the smart contracts which get executed on behalf of a transaction. Members reach consensus before writing transaction data to the shared ledger. This leads to increased trust and transparency for agencies and commercial entities transacting on the blockchain network. Data on the ledger can give agencies an end-to-end view of an interagency business process. Analytics, cognitive, and machine learning capabilities can also leverage ledger data to help improve business processes.

Enabling Regulatory Compliance

Federal agencies can also benefit by working with industry members in a blockchain network. Currently, federal agencies often rely on periodic reports and inspections to determine if industry members are in compliance. Through blockchain, network members can self-regulate by writing compliance data to the ledger. Agencies no longer need to request data from industry members. Instead, they can call for and read the compliance information off the ledger through automated requests, receipts, and data access. Smart contracts also can enforce compliance by testing for specific conditions to determine the outcome of a transaction's or submission's validity.

Data Governance and Information Sharing

All types of classified information sharing could function on a blockchain, such as those between federal government agencies, between federal and state/local (such as law enforcement), as well as non-classified but sensitive data. Such data can have classification markings, handling caveats, and other metadata such as source citation. Different agencies operate under different authorities and are limited to what they can do with the data. The immutability of blockchain is key in this use case category.

Governance

Successful implementation in the public sector will require an effective governance and policy model to develop rules needed to protect participants, stakeholders, and investors in ways that ensure the system is resilient to systemic risk, privacy issues and cybersecurity threats without hampering innovating toward the very efficiencies blockchain offers in public sector applications. The public sector is at times the target of perceptions, both real and imagined, of any large bureaucracy – poor information sharing as well as regulatory and process drag that unnecessarily delays and impedes accomplishment of mission. A considerate approach to governance and policy in the shift to blockchain will better enable the government to more effectively serve the people, reduce regulatory process friction, improve transparency and information sharing, and smooth partnering between and across government and industry.

Takeaways – Blockchain Governance

The role of governance, properly approached, in the public sector blockchain marketplace presents itself as an opportunity to more effectively serve the people.

There are no shortages of governance bodies and activities already available. Embracing and including these constructs in the public sector blockchain journey will further improve the likelihood of its success.

Governments have a supporting role to play in helping to grow a more effective and responsible blockchain ecosystem. In practical terms, this means working with industry to develop a set of common standards and frameworks that facilitate innovation, interoperability, and trust without overtaking our other important policy objectives, such as risk mitigation, consumer/investor protection, privacy, resiliency, and transparency.

The public sector should uniquely straddle its oversight role with a do-no harm approach.

The influence and importance of properly executing policy and governance, as it relates to the full life cycle of cybersecurity and privacy on public sector blockchains, is a critical component to ensuring the confidence and inspiring trust.

Governance, legislative, policy, and regulatory frameworks are, in essence, the very business rule constructs upon which public sector agencies govern and interact with one another, partners, citizens, and industry. Understanding and properly leveraging the influence of these frameworks in a public sector blockchain transformation is a step as essential as understanding the business processes, stakeholders, and desired outcomes that make-up traditional private sector transformations. Public sector blockchain counts perhaps among its greatest opportunity as that of reducing the current drag of regulatory, governance, and policy frameworks. It has the potential and promise to transform into minutes and hours, with higher quality and accuracy, processes that often take days, weeks, and months to complete.

Robust governance for any blockchain applications must take into consideration the interests and needs of the stakeholder community: citizens, state and local governments, other branches of government, and industry partners. As well, the influence and importance of properly executing policy and governance as it relates to the full life cycle of cybersecurity and privacy on public sector

blockchains is a critical component to ensuring the confidence and inspiring the trust necessary for adoption that will enable blockchain technology to solve public sector challenges and benefit the people. To that end, governance and policy frameworks should be structured to support these objectives. A key component of developing that policy framework is ensuring that regulations are efficient, effective, and appropriately tailored for the business at hand.

There are no shortages of governance bodies and activities across the many sectors of the government, all of whom may have some stake in a given blockchain application. For example, title management is a core aspect of documentation for lending for single-family homes, and there are a wide variety of governmental entities involved in the mortgage industry. From the federal perspective, the government guarantees billions of dollars of new single-family mortgages every year. On the federal side, the Office of Management and Budget and Treasury have financial oversight government-wide. Then there are the programmatic agencies who guarantee these loans. The Federal Housing Administration, Department of Veterans Affairs, and Department of Agriculture all have single-family housing guarantee programs. Ginnie Mae guarantees securities backed by these federally insured mortgages;[44] the lenders who make the loans and investors who buy the securities. Each state has its own laws and governance for credit programs and housing, and potentially may have housing finance agencies who are supporting affordable credit for these mortgages. There are the title companies and the homeowners too. Trying to build a comprehensive governance structure across just this one application would be extraordinarily challenging. Without any general standards, there is a risk of duplicative and one-off solutions that could negate the benefits. Blockchain offers the opportunity to logically harmonize and equitably enforce rules, workflows, inputs, and outcomes, while allowing each agency to retain jurisdiction and oversight over their respective subject matter and entities.

Over the past couple of years, a subcategory of financial services technology, *FinTech*,[45] has emerged to address the enormous challenges faced by organizations to comply with an increasing number of regulations, and an enhanced focus on and intensity of enforcement. Its name, *RegTech,* or regulatory technology, is defined as the application of innovative technologies to simplify and streamline the back-office systems and operations implemented by organizations specifically for regulatory compliance and risk management purposes, which represent increasingly high percentages of a company's overall expenditure. The transformative power of blockchain can also be extended to a broad array of areas in the administrative and operational side of government, giving rise to a third related category, *GovTech*, or RegTech from the other side of the table. Blockchain can be a policy-making, oversight, and enforcement mechanism. These attributes and goals are central to the oversight duties of government regulatory agencies and to the compliance and risk management duties of industry.

Another example of the power of blockchain is that of smart contracts, enabling the public-sector acquisition community, related policy and regulation, as well as stakeholders in government and

industry to bring its promise of timeliness, transparency, and improved accountability to fruition. The Federal Acquisition Regulation (FAR), Federal Travel Regulations (FTR), and the Treasury Financial Manual (TFM) lay out the important frameworks and rules for public sector procurement of goods and services from industry. There is opportunity for blockchain-based smart contracts to improve timeliness, reduce friction, and smooth procurement and invoice reconciliation between the public sector and vendor communities. Codifying and managing those life cycle aspects of acquisition policy and governance into a smart contract based blockchain will be essential to success.

Example Governance and Policy Bodies Influential to Adoption of U.S. Public Sector Blockchain	
• Securities and Exchange Commission • Federal Deposit Insurance Corporation • Federal Reserve Board • Office of Comptroller of the Currency	• Commodity Futures Trading Commission • Consumer Financial Protection Bureau • Ginnie Mae
• Office of Federal Financial Management • Office of Federal Procurement Policy • Office of eGovernment and Information Technology • Council of Economic Advisors • Office of Science and Technology Policy	• President's Management Council • Office of Information and Regulatory Affairs • Office of Performance and Personnel Policy • Office of the US Intellectual Property Coordinator
• GSA - Office of Government-wide Policy	
• Chief Acquisition Officers Council • Chief Financial Officers Council • Chief Human Capital Officers Council	• Chief Information Officers Council • Performance Improvement Council • Federal Privacy Council
• Business Standards Council • Small Agency Council • Council on Inspectors General and Efficiency • NIST Information Technology Laboratory	• OPM/Human Resources Line of Business • Treasury/FIT • Grants • Acquisition • Travel

Current state governance and policy bodies exist to mediate the dialogue and vision for improving government operations and efficiency. Many of these organizations comprise representatives from federal agencies and become conduits for identifying opportunity, flagging and addressing issues, and improving agency adoption. A progressive plan for blockchain governance will integrate governance

and policy and improve the likelihood that integrating and institutionalizing its incredible potential across the public sector will be successful.

Challenges to Overcome

Blockchain has the potential to transform both the effectiveness and efficiency of the public sector, but that potential is not without its challenges. The following are a few of the key challenges to overcome when considering the impact of blockchain on people, process, and technology in the public sector:

People	Process	Technology
• Infancy/Early Adoption—culture shift • Training • Risks to consumers	• Security • Operational & Legal Risks • Governance • Regulatory Compliance • Intellectual Property • Privacy vs Transparency • Decentralized Autonomous Organizations (DAOs) • Legal Enforceability of Smart Contracts • Need for Robust Standards • Paradigm Shifts • Decentralized Trust • Data Sharing • Maintenance Responsibilities in a Decentralized System • Quasi-Anonymity • Accountability & Responsibility • Competition	• Scalability & Resiliency • Adoption Cost • Interoperability • Large ecosystem with many different blockchains/protocols

What Does the Shift to Blockchain Mean for the U.S. Federal Government?

As more organizations adopt blockchain and specific applications are developed, implemented, and scaled, additional risks will certainly reveal themselves. However, these risks and their potential impact to the workplace should not take away from the benefits of blockchain adoption.

One of the greatest obstacles at any level of government will be the evolution of operations necessary to achieve the many benefits offered by blockchain technologies. Blockchain represents a fundamental change in the way an organization does business and a departure from the incremental improvements

the public sector typically implements. For some organizations, blockchain represents exponential improvement, but it also requires considerable adjustments to business rules and processes.

The flexibility of the blockchain ecosystem offers individual organizations multiple options for implementation to ensure the solution meets their needs. However, this diversity can impede the development of standards and best practices, creating a burden for training the workforce and building, operating, securing, maintaining, and defending the technology for users and consumers.

Blockchain solutions are currently built in modern programming languages. For example, Bitcoin uses C++; Ethereum is built around JavaScript and Solidity for smart contracts; and Hyperledger is built around the Go language and Java. While some training might be needed, the use of modern languages means programmers can shift from other work to blockchain development with minimal requirements. The issue that may affect the public sector most when it comes to the workforce is the combination of the technology industry's current shortage of skilled workers compounded by government's challenges to hire quickly.

Takeaways – Challenges to Overcome

Blockchain is a diverse ecosystem with a lot of options to choose from, offering a high degree of customization but also requiring a lot of planning.

Blockchain will most impact the processes of organizations, as well as the people and the technology. This is not insurmountable and has been done many times before.

Blockchain is being explored globally but will require significant planning to adopt and operate. It might not be the right solution for your organization.

Blockchain itself has yet to show vulnerabilities, but because it is a recently emerged technology, standards development and other guidance could mitigate current challenges surrounding implementation.

The current technology also has challenges. Many organizations have aging infrastructure and/or legacy information technology systems still serving critical roles, which may impede the adoption of blockchain. However, for organizations in the pre-planning or early stages of information technology modernization efforts, there is an opportunity to include a blockchain solution in their roadmaps now (assuming a need has been validated and a decision on a blockchain implementation has been made). Other organizations may find it more advantageous to wait until they are able to leverage lessons-learned and proven best practices from early adopters.

Regardless of an organization's decision around when to integrate blockchain into their enterprise, any discussion of implementation must address the criticality of interoperability. Blockchain is not a technology that can be implemented in a 'plug-and-play' manner but rather should be considered as a platform upon which existing systems or new systems can be built upon or seamlessly integrated into. In order for a blockchain adoption to succeed, organizations will have to consider their existing policies, procedures, and practices with an intent to update and revise those elements that would limit their

adoption. Legacy policies that have not been updated for modern operating models will create unnecessary hoops for blockchain developers to jump through and severely cripple IT operations from transitioning to distributed models. Similarly, legacy procedures, especially around data exchange, will make it extremely difficult for a blockchain platform to efficiently operate while also restricting the ability for that system to interact with others, both internally and externally across government. Finally, an organization that does not already have established procedures for identifying new technologies, assessing them, determining which to adopt, and then successfully integrating them will almost certainly fail to move to a blockchain ecosystem. Moreover, even if a blockchain system were adopted, it would likely not succeed long-term if the organization was unable to evolve with it. Blockchain is still a very early technology and will require a healthy amount of flexibility and adaptability for any early adopters. And as more government organizations transition to blockchain-enabled systems, the need and demand for those various systems to interact will only increase. However, these challenges are not unique to government and every organization exploring blockchain will have to address these interoperability issues.

While blockchain has challenges, they are not insurmountable. The adoption of any new technology will always carry an inherent risk, but the public sector has a history of successfully, if slowly and cautiously, navigating those risks. The most recent example is the adoption of government-wide cloud computing. This paradigm shift has been transformational for both the government and those affected, moving individual organizations from hosting their own data, applications, and enterprises to newly established centers of excellence leveraging the best industry standards that incorporate state and/or federal requirements for security, redundancy, transparency, etc.

Blockchain represents the next major paradigm shift in how the government does business, interacts with its citizens and partners around the world, and holds itself accountable.

What Does the Global Shift to Blockchain Mean?

With blockchain exploration occurring around the world, both in public and private sectors, the business of government as a whole will be impacted. New and evolving technologies bring risk and that risk is highest when organizations are first adopting a new technology. But the risk will not stop progress from continuing to spread, from isolated systems to enterprise-wide implementations.

And while some blockchain networks are standalone, most will augment current networks or establish new ones. Additionally, some blockchain systems have moved into cross-blockchain technologies, such as Polkadot, HyperLedger, Overstock's tØ, and Ripple. This demonstrates the possibility of nodes from one blockchain conducting transactions with nodes from another blockchain in real time. The need for cross-blockchain communication in the public sector will be an incredibly important capability to watch

as blockchain technology matures, allowing for more complex relationships to move from legacy processes to modern, even automated, modes of transaction.

Standards, policies, and procedures will need to be established for the types of security appropriate for each layer of these new blockchain networks. It might only take a revamp of current tools, or it might require entirely new security solutions, possibly some combination of both. Blockchain is leading a global shift in business and the governments of the world will have to adapt with their economies or risk holding their countries back as others embrace what many believe to be the next evolution of our connected world. However, until the future arrives, there are challenges to be faced in the blockchain of today.

Blockchain Landscape Today

In less than a decade, blockchain has evolved from an idea to a technology that governments and organizations around the world are exploring – from the bipartisan Parliamentary Blockchain Group[46,47] in Australia to BitFinance in Zimbabwe.[48,49] Many organizations see this technology as a new foundational piece of our digital society with the potential to impact all sectors of the economy.

Every day, more and more U.S. federal agencies announce that they are evaluating and experimenting with blockchain. The interest is so widespread that, in July 2017, GSA's Emerging Citizen Technology Program launched the U.S. Federal Blockchain Program[50] for federal agencies and U.S. businesses.[51] During the launch, agency teams submitted close to 200 use cases that could leverage the use of blockchain technology within government, many of which are described in this primer.

According to Juniper Research, 57% of large corporations are either actively considering or are in the process of deploying blockchain technology.[52] Juniper Research also reported that of those firms who have reached proof of concept, "two-thirds said they expect the technology to be integrated into their systems by the end of 2018."[53]

There is a vast array of sectors that are exploring blockchain implementation such as finance, real estate, law/contracting, insurance, human resources, transportation/ ride-sharing, manufacturing/ ecommerce, education, health, storage, identity, media, and energy. The table below illustrates some highlights of blockchain efforts in 2017, demonstrating how pervasive this emerging technology is even though it is still in the hype cycle.

	Organization	Blockchain Effort	More Information
U.S Government	**House of Representatives**	**Blockchain Caucus**	www.congressionalblockchaincaucus.com
	DHS	Exploration for Homeland Security	https://www.dhs.gov/science-and-technology/news/2017/01/10/snapshot-blockchain-technology-explored-homeland-security
	GSA	**Federal community and agency projects**	www.gsa.gov/portal/content/168102
	State of Delaware	Delaware Blockchain Initiative	https://delaware.gov
Foreign Government	**European Union**	**Blockchain Observatory and Forum**	https://ec.europa.eu/digital-single-market/en/news/eu-blockchain-observatory-and-forum
	Estonia	Digital Society	https://e-estonia.com/
	UAE	**The Dubai Blockchain Strategy**	http://www.smartdubai.ae/dubai_blockchain.php
	Australia	Parliamentary Friends of Blockchain	http://www.aph.gov.au/About_Parliament/Parliamentary_Friendship

	Organization	Blockchain Effort	More Information
Public Private Partnership	**GBBC**	30+ countries for implementation	https://www.gbbcouncil.org/
	Chamber of Digital Commerce	Education and advocacy	https://digitalchamber.org/
	ACT-IAC	**Knowledge bank and planning**	www.actiac.org/groups/blockchain-0
	IEEE	Ecosystem growth and capture	https://blockchain.ieee.org/
Platforms	**Hyperledger**	**Collaborative development of 100+ orgs**	www.hyperledger.org
	Enterprise Ethereum Alliance	Open development, standards, education, partnerships with 100+ of orgs.	https://entethalliance.org/
	R3	**Financial consortium platform**	https://www.r3.com/

Next Steps and Recommendations

In the World Economic Forum's survey on "Technological Tipping Points," Shift 16 was noted as "Bitcoin and the Blockchain."[54] The "tipping point" predicted 10% of global gross domestic product (GDP) would be stored on blockchain technology by 2027.[55] In Shift 18, Governments and the Blockchain, the WEF noted that taxes will be collected for the first time by a government via a blockchain, starting in 2023.[56] While blockchain and Distributed Ledger Technology are still very much in their infancy, the goal of this primer is to educate key decision makers in government on what blockchain technology is. This is not an endorsement of the use of blockchain technology nor is it an attempt to promote the technology. Instead, it is a call to engage with the hope that, as with any new technology, whether it be artificial intelligence, the Internet of Things, or blockchain, the U.S. do not fall behind. A Harvard Business Review article titled "How Blockchain Could Help Emerging Markets Leap Ahead" cites examples of how blockchain has the potential to help developing nations leapfrog more developed economies."[57]

The keys to blockchain rely on a network effort, or many different users cooperating and engaging with the technology. As financial markets look to save money with blockchain technology, with estimates of $8-12 billion a year in savings per bank,[58] there is no reason why government should not, at a minimum, be examining this technology for its potential. Much of the network effect in a blockchain relies on the distributed and transparent nature of a digital ledger. One of the most critical paths to success for the U.S. government is to find a way to deliver its services to citizens in a technologically sophisticated way that meets their demands and provide the necessary transparency, with as low a cost as possible. Since blockchain is a greenfield technology for development, there is nothing stopping U.S. government agencies from examining how blockchain technology may remove unnecessary intermediaries to reduce costs, while at the same time provide the transparency that U.S. citizens demand. In addition, blockchain may empower governmental agencies to identify fee-based, value-added services that allow for additional revenue without increasing taxes.

One of the most important aspects of the development of blockchain technology is in its ability to be interoperable with other blockchain networks in the private sector. With the growth of *RegTech* as described in the governance section, so too shall there be the emergence of *GovTech*, a way for government officials to innovate with technology. The blockchain is the best of both worlds, in that the transparency it offers in the nature of a distributed ledger, the efficiency in cost of eliminating unnecessary intermediaries in the delivery of citizen services, and the ability in the future to be interoperable with private sector companies across a public network.

What is being developed now, and what can be seen from this paper as the eventual overall goal of blockchain technology, is much as was seen with the development of electronic computing – the development of what are known as "Turing-complete" systems. A Turing-Complete Blockchain is one that can process computer code in the form of "smart contracts" to the exact same extent as if that

computer code were run on an actual computer. (Blockchain, 2017) A properly designed blockchain system provides public-private blockchain neutrality, is vendor-neutral, offers private, permissioned blockchains for enterprise and government use cases, and can protect billions of dollars in value on a public network. As of now, there is a community of almost 100,000 developers working on various types of blockchain technology. The hope within the blockchain community is for there to be 2,000,000 blockchain programmers by 2020, with the network effect achieved through the efforts of growing consortia such as R3, Hyperledger, and the Enterprise Ethereum Alliance.[59] In tandem with the planned blockchain playbook, this primer provides users an opportunity to be aware of this technology and simply ask the question, "what is it you would have done - whether differently or the same - when the internet approached the government in 1995?" And most importantly, "what is the blockchain strategy at your U.S. agency?"

Acknowledgements

The Blockchain Working Group wishes to thank the many contributors who provided a tremendous amount of time and good humor to bring *Enabling Blockchain Innovation in the U.S. Government – A Blockchain Primer* to completion.

The Blockchain Working Group would like to also thank, Jose Arrieta (GSA), Venkat Kodumudi (CGI Federal), Jacqueline Tame (Congressional Staff), Katherina Dimenstein (Congressional Staff), Dylan Yaga (NIST), and Lewis Cohen (Hogan Lovells US LLP) who provided invaluable feedback as reviewers.

Authors

Combiz Abdolrahimi	U.S. Department of Treasury
Sandy Barsky	General Services Administration
Jason Brett	ConsenSys
Frederic de Vaulx	Prometheus Computing
Duc Duong	Grant Thornton
Bill Engel	Rapid Cycle Solutions
Mark Fisk	IBM
Todd Hager	Macro Solutions
Sarah Lyberg	U.S. Department of Housing and Urban Development
Joshua Satten	Sapient Consulting
Sherri Sokol	Defense Information Systems Agency
Arushi Srivastava	NTT DATA
Jonathan Tame	Deloitte
Jeff Tennenbaum	IBM
Star Vanamali	Sapient Consulting | Public Sector
Andrew Vanjani	General Services Administration
Robert Wuhrman	General Services Administration
Aleksandar Zelenovic	Sapient Consulting | Public Sector

Contributors

Harold Affo	Prometheus Computing
Bob Ferrari	IBM
Mike Fischer	BRMi
Justin Herman	General Services Administration
Tommy Leander	Congressional Staff
Jean Lewis	Sapient Consulting | Public Sector
Juan Llanos	ConsenSys
Rene Nayman	ConsenSys
Cherrie Reid	TCG
Damanjit Padam	Macro Solutions
Bajinder Paul	InfoZen
Bo Shevchik	Association of Government Accountants
Liam Speden	Robbins-Gioia
Jeremy Wood	Millennium Challenge Corporation
Bobby Woodard	Department of Homeland Security

References

[1] https://www.gov.uk/government/publications/distributed-ledger-technology-blackett-review

[2] https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/using-blockchain-to-improve-data-management-in-the-public-sector and

https://techcrunch.com/2016/11/21/blockchain-technologies-could-transform-government-services/

[3] Keith Kirkpatrick, "Financing the Dark Web," *Communications of the ACM* 60, no. 3 (March 2017): 21-22.

[4] https://en.wikipedia.org/wiki/Blockchain

[5] https://www.processexcellencenetwork.com/pex-tools-technologies/columns/what-is-blockchain-and-what-does-it-mean-for-us

[6] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf

[7] Chris Hammerschmidt, "Consensus in Blockchain Systems. In Short.," https://medium.com/@chrshmmmr/consensus-in-blockchain-systems-in-short-691fc7d1fefe

[8] Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller and Steven Goldfeder, *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction* (Princeton: Princeton University Press, 2016), 1-26.

[9] Ronald L. Rivest, "Cryptography," 1990. Quoted in J. Van Leeuwen, *Handbook of Theoretical Computer Science* (Cambridge: The MIT Press, 1994).

[10] Andy Greenberg, "Crypto Currency," *Forbes*, April 20, 2011, https://www.forbes.com/forbes/2011/0509/technology-psilocybin-bitcoins-gavin-andresen-crypto-currency.html.

[11] Usman W. Chohan, "Cryptocurrencies: A Brief Thematic Review" (Discussion Paper, University of New South Wales, 2017), 1-5.

[12] Wikipedia contributors, "Cryptocurrency," *Wikipedia, The Free Encyclopedia,* https://en.wikipedia.org/w/index.php?title=Cryptocurrency&oldid=802787513 (accessed September 30, 2017).

[13] Wikipedia contributors, "Digital asset," *Wikipedia, The Free Encyclopedia,* https://en.wikipedia.org/wiki/Digital_asset (accessed September 30, 2017).

[14] https://www.federalreserve.gov/econresdata/feds/2016/files/2016095pap.pdf

[15] "Distributed Ledgers," *Investopedia*, http://www.investopedia.com/terms/d/distributed-ledgers.asp (accessed September 30, 2017).

[16] Wikipedia contributors, "Node (networking)," *Wikipedia, The Free Encyclopedia,* https://en.wikipedia.org/wiki/Node_(networking) (accessed September 20, 2017).

[17] "What is Blockchain Technology? A Step-by-Step Guide For Beginners: An in-depth guide by BlockGeeks," Blockgeeks, https://blockgeeks.com/guides/what-is-blockchain-technology/ (accessed September 30, 2017).

[18] "What is Blockchain Technology?"

[19] UK Government Chief Scientific Adviser, *Distributed Ledger Technology: beyond block chain*, United Kingdom: Government Office for Science, 2016, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf, 17.

[20] Brian Straight, "A guide to blockchain," FreightWaves, March 29, 2017, https://www.freightwaves.com/news/defining-blockchain-terminology (accessed September 30, 2017).

[21] "Smart Contracts," *Investopedia*, http://www.investopedia.com/terms/s/smart-contracts.asp (accessed September 30, 2017).

[22] Emschwartz, "Smart Oracles: A Simple, Powerful Approach to Smart Contracts," GitHub, last updated July 17, 2014, https://github.com/codius/codius/wiki/Smart-Oracles:-A-Simple,-Powerful-Approach-to-Smart-Contracts (accessed September 30, 2017).

[23] "Smart Oracles: A Simple, Powerful Approach to Smart Contracts."

[24] https://crossings.sapientglobalmarkets.com/2017/09/14/blockchain-use-cases-business-value/

[25] Joshua Satten, "Blockchain: Are We Nearly There Yet? And, More Importantly, Where Are We Going? Sapient Global Markets, September 2017, https://crossings.sapientglobalmarkets.com/2017/09/14/blockchain-use-cases-business-value/.

[26] "Blockchain: Are We Nearly There Yet?"

[27] "Blockchain: Are We Nearly There Yet?"

[28] "Blockchain: Are We Nearly There Yet?"

[29] "Blockchain: Are We Nearly There Yet?"

[30] "Blockchain: Are We Nearly There Yet?"

[31] "Blockchain: Are We Nearly There Yet?"

[32] "Blockchain: Are We Nearly There Yet?"

[33] http://www.govexec.com/management/2014/12/fema-spent-billions-disaster-assistance-overhead-during-last-decade/101619/ and

https://www.reuters.com/article/us-storm-harvey-fema/u-s-officials-say-450000-in-texas-likely-to-seek-disaster-aid-idUSKCN1B8177

[34] "What past federal hurricane aid tells us about money for Harvey recovery,"CNN, August 31, 2017, http://www.cnn.com/2017/08/31/politics/hurricane-harvey-recovery-money/index.html.

[35] "FEMA expects more than 450,000 Harvey disaster victims to file for assistance," *CNBC*, August 28, 2017, https://www.cnbc.com/2017/08/28/fema-expects-more-than-450000-harvey-disaster-victims-to-file-for-assistance.html.

[36] "Harvey aid: House overwhelmingly passes $7.9 billion relief bill," *ABC 7 Eyewitness News*, September 6, 2017, http://abc7.com/house-overwhelmingly-passes-$79-billion-harvey-aid-bill/2383214/.

[37] https://www.fema.gov/grants-management-modernization-program

[38] Steve Chang, Matthius Daub, Axel Domeyer and Martin Lundqvist, "Using blockchain to improve data management in the public sector," McKinsey & Company, February 2017, https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/using-blockchain-to-improve-data-management-in-the-public-sector.

[39] Dante Disparte, "Blockchain Could Make the Insurance Industry Much More Transparent," *Harvard Business Review*, July 12, 2017, https://hbr.org/2017/07/blockchain-could-make-the-insurance-industry-much-more-transparent.

[40] http://gsa.federalschedules.com/resources/gsa-schedule-sales-2016/

[41] Cassandra Stephenson, "GSA calls for blockchain and machine learning to speed acquisition," FedScoop, June 26, 2017, https://www.fedscoop.com/gsa-calls-blockchain-machine-learning-speed-acquisition/.

[42] "IT Schedule 70," U.S. General Services Administration, last reviewed September 14, 2017, https://www.gsa.gov/technology/technology-purchasing-programs/it-schedule-70 (accessed September 30, 2017).

[43] "IBM Watson Health Announces Collaboration to Study the Use of Blockchain Technology for Secure Exchange of Healthcare Data," IBM, January 11, 2017, https://www-03.ibm.com/press/us/en/pressrelease/51394.wss.

[44] Economic Policy Program: Housing Commission, *Ginnie Mae: How Does it Work and What Does it Do?* Bipartisan Policy Center, http://bipartisanpolicy.org/wp-content/uploads/sites/default/files/GinnieMae-final.pdf (accessed September 30, 2017).

[45] "The Complete Beginner's Guide To FinTech In 2017," Forbes, February 10, 2017, https://www.forbes.com/sites/bernardmarr/2017/02/10/a-complete-beginners-guide-to-fintech-in-2017/ - 7f8a9c8b3340

[46] https://www.cryptocoinsnews.com/australian-senators-establish-bipartisan-blockchain-group-parliament/

[47] http://www.aph.gov.au/About_Parliament/Parliamentary_Friendship.

[48] http://bitfinance.co.zw/

[49] https://www.gsb.stanford.edu/faculty-research/case-studies/bitfinance-revolutionizing-zimbabwes-fragile-economy-bitcoin

[50] https://www.gsa.gov/portal/content/168102

[51] "Blockchain," U.S. General Services Administration, last reviewed August 13, 2017, https://www.gsa.gov/technology/government-it-initiatives/emerging-citizen-technology/blockchain (accessed September 30, 2017).

[52] "Juniper Research: Blockchain Enterprise Survey August 2017," Juniper Research, July 31, 2017, https://www.juniperresearch.com/resources/infographics/blockchain-enterprise-survey-august-2017 (accessed September 30, 2017).

[53] "Juniper Research."

[54] Global Agenda Council on the Future of Software & Society, *Deep Shift: Technological Tipping Points and Societal Impact*, World Economic Forum, September 2015, http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf.

[55] Global Agenca Council on the Future of Software & Society.

[56] Global Agenda Council on the Future of Software & Society, 26.

[57] Vinay Gupta and Rob Knight, "How Blockchain Could Help Emerging Markets Leap Ahead," *Harvard Business Review*, May 17, 2017, https://hbr.org/2017/05/how-blockchain-could-help-emerging-markets-leap-ahead.

[58] Oscar Williams-Grut, "Blockchain tech could save top investment banks $8 billion a year," *Business Insider*, January 17, 2017, http://www.businessinsider.com/accenture-blockchain-could-save-top-10-investment-banks-up-to-8bn-a-year-2017-1.

[59] https://www.ft.com/content/f736b04e-3708-11e7-99bd-13beb0903fa3