2019

Understanding Blockchain's Role and Risks in Trusted Systems

Contents

Executive Summary

Without trust, our ability to engage in meaningful activities is diminished. However, distrust in societal institutions remains high despite recent gains. According to the 2019 Edelman Trust Barometer, trust in societal institutions such as government, business, the media and non-governmental organizations (NGOs) rose 3 points between 2018 and 2019, but only 1 in 5 respondents believes the system is working for them. According to an April 2019 report by the Pew Research Center, American trust in government is near an all-time low with only 17 percent of Americans saying they can trust the government in Washington to do what is right most of the time. The reasons for distrust are numerous and complex, but there's a potential for blockchain distributed ledger technology to contribute to a reversal of this trend. Today, entities worldwide are investigating the use of blockchain technologies to build trust with citizens and consumers, protect data, and reduce operating costs. This whitepaper, the result of a year-long collaboration among representatives from the public and private sector, will help the reader understand the challenges, opportunities, benefits and risks of transferring trust from institutions to blockchain distributed ledger technology solutions.

Introduction

This document provides the layman with an introduction to the concept of trusted information in relation to the use of blockchain technology as a form of Distributed Ledger Technologies (DLT). It provides guidance for Information Governance Professionals responsible for information assets within their organizations. This document defines the key characteristics of the current market as well as existing challenges and opportunities. It provides industry information and analysis regarding the potential use of DLT (aka blockchain for the purposes of this paper) for Elections, Identity Management for Online Transactions, Supply Chain Management/Food Fraud, Business Process/Workflow, and Internet of Things (IoT) use cases.

This document should be used as an analytical resource for senior executives and information governance professionals in business and government when investigating DLT, developing DLT strategies, and / or planning DLT programs. It defines the key characteristics of the current market, as well as existing challenges and opportunities (at the time of publication).

This document does not suggest that Blockchain is a replacement for all enterprise systems, such as enterprise content management systems and trusted digital repositories. Instead, for the foreseeable future Blockchain will work alongside those types of products and provide additional capability.

This is an evolving area where a great deal of work is taking place under the auspices of several standards' development organizations.

Terms & Definitions

For the purposes of this document, the following terms and definitions apply.

Authentication
the act of verifying identity.

[SOURCE: ISO 16484-5:2017]

Archival Science
n., ~ 1. The process of verifying that a thing is what it purports to be, that it is acceptable as genuine or original.

[SOURCE: SAA Glossary]

Blockchain
a digital database containing information (such as records of financial transactions) that can be simultaneously used and shared within a large decentralized, publicly accessible network.

[SOURCE: Merriam-Webster]

Note 1 to entry: The **blockchain** is an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value.

[SOURCE: Blockchain Revolution, Don & Alex Tapscott, 2016.]

Data lake
a collection of storage instances of various data assets additional to the originating data sources.

[SOURCE: Gartner IT Glossary]

Distributed Ledger
a distributed ledger is a database that is consensually shared and synchronized across multiple sites, institutions or geographies.

[SOURCE: Investopedia]

Distributed Ledger Technology (DLT)
Distributed Ledger Technology refers to the technological infrastructure and protocols that allows simultaneous access, validation and record updating in an immutable manner across a network spread across multiple entities or locations

[SOURCE: Investopedia, 2018]

Note 1 to entry: DLT is a family of technologies that employs a shared database architecture to maintain multiple, identical copies of an auditable, up-to-date distributed or decentralized ledger of transactions or data (Advancing Blockchain Cybersecurity: Technical and Policy Considerations for the Financial Services Industry, Microsoft, 2018).

Distributed Trust Model
a framework that relies on multiple, independent authorities in a community of users that is independent of a single arbiter

[SOURCE:I-trust Terminology Project, 2018]

Information governance (IG)
the specification of decision rights and an accountability framework to ensure appropriate behavior in the valuation, creation, storage, use, archiving and deletion of information.

[SOURCE: Gartner, 2019]

Personally Identifiable Information
PII
any information that identifies or can be used to identify, contact, or locate the person to whom such information pertains from which identification or contact information of an individual person can be derived, or that is or might be directly or indirectly linked to a natural person.

[SOURCE: ISO/IEC 29100]

Provenance
relationships between records and the organizations or individuals that created, accumulated and/or maintained and used them in the conduct of personal or corporate activity.

Smart contract
a computer protocol intended to digitally facilitate, verify, or enforce the negotiation of performance of a contract.

[SOURCE: Wikipedia]

Note 1 to entry: Smart contracts are lines of code that are stored on a blockchain and automatically execute when predetermined terms and conditions are met. At the most basic level, they are programs that run as they've been set up to run by the people who developed them.

[SOURCE: IBM, 2018]

Trust
confidence in another party with respect to specific actions or benefits.

[SOURCE: InterPARES Glossary, 2019]

Note 1 to entry: In the context of blockchain technology, the first party places trust not in the party to the agreement or in a third party but in the blockchain network itself.

Concepts

Distributed Trust

If data and information are the "new currencies" for the digital enterprise, then trust is the "grease" that lubricates and drives digital transformation. In fact, trust is central to any interaction between two parties—be it two individuals or two organizations. Rachel Botsman (www.rachelbotsman.com), an author, trust expert, and lecturer at Oxford University's Saïd Business School, states, "Like any currency that we value, trust needs time, care and investment." Rachel continues, "We are living in an age of trust on speed. We need to learn to ask: is this person, company or thing worthy of my trust?" In fact, the lack of trust may increase the cost and possibly the risk associated with the interaction. In other words, costs may outweigh the benefits. Martin Wolf in the Australian Financial Review states, "A recent Geneva Report on the Impact of Blockchain Technology on Finance, argues that such technology can "mitigate the 'cost of trust'" and so "lower overall costs, reduce economic rents and create a more secure and fairer financial system" (Wolf, 2019).

To minimize the "cost of trust" associated with a transaction between two or more parties; the parties can rely on a technical solution—a consensus mechanism that negates the need for an intermediary. Proof of Work (PoW), used by Bitcoin and Ethereum and the most well-known consensus mechanism, requires the solution of a mathematical puzzle requiring large energy consumption and confirmation by the consensus of more than 51% of the nodes in the network. Proof of Stake (PoS), also supported by Ethereum) eliminates the need for the mining process by randomly selecting validators for block creation. Participants are attributed mining power in proportion to the percentage of coins held by a miner. In Delegated Proof of Stake (DPoS) systems, users elect delegates (also called witnesses) they "trust" to validate transactions. Since voting is a continuous process, a witness can be replaced by a user who is considered more trusted and, therefore, gets more votes; users can vote to remove a witness who has lost their trust. When the parties enter into the interaction without the aid of a third party, a model of distributed trust is created. Distributed trust changes the theoretical perspective and the practical application of a "trusted interaction" in technology platforms by removing the trusted third party. "Distributed trust fundamentally transforms boundaries of organizations, and challenges assumptions about internalizing organizational functions to overcome market trust coordination issues." (Seidel, 2018, p 42) Seidel goes on to state, "Centralized positions were assumed to be a source of power … [while] historically these have been valid assumptions, the recent emergence of distributed trust systems such as blockchain databases fundamentally [challenges] these core tenets …" (p 40).

The "trust interaction" can extend to technology and platforms. DLT removes the need of a central authority to validate the PoW in order to complete the interaction. Since the ledger is transparent to all nodes in the network, they can validate the ledger when a majority of nodes agree with the information entered into the ledger. Therefore, a democratization process of collaborating and distributing the trust across a majority of the nodes establishes trust in the ledger, i.e. a community of nodes distributes the concept of trust across the network by maintaining the authenticity of the ledger.

Email is an early example of a technology that transformed sending mail by removing the need for a trusted third party such as the post-office or a courier service. This greatly reduced the transaction cost of communicating with one or more parties. In fact, trusting technology platforms in which trust is distributed across millions of users underpins the rise of the "sharing economy" (a peer-to-peer economic model). Uber, Lyft, and AirBnb are platforms designed to enable trust between strangers for driving and lodging, while crowd funding platforms such as Kickstarter and Indiegogo are designed to enable trust between innovators and investors. However, these platforms have a transaction cost for each transaction. Now, if the two parties can eliminate the third party, then the trust is distributed between millions of users without the need of a central authority to legitimize and authorize the transaction. Seidel states "Trust is at the core of organizational creation … [and] transactional cost economics … rely upon fundamental trust assumptions which need to be updated." (p 42). An example of a couple of practical applications:

> "The Bill and Melinda Gates Foundation is starting to use distributed trust technologies with the aim of providing financial services through noncentralized platforms to the more than 2 billion worldwide people who do not have bank accounts … [and] … Individual solar panel owners are already selling excess electricity directly to other consumers in automated peer-to-peer transactions without the involvement of centralized utility companies or centrally owned electric grids by using smart contracts on the Ethereum blockchain in New York." (Seidel, 2018, p 42)

Trusted Information

The concept of trusted information is a combination of two complex concepts, "trust" and "information," each of which has varied meanings and usages. This combination has become increasingly more important in the digital age as information through its normal life-cycle has proven itself inherently absent of trust unless deliberate effort is made to safeguard its creation/receipt, active use and transmission, storage and maintenance, and eventual disposition. Information is made and kept in a multitude of digital environments, creating opportunities for new kinds of use and reuse, yet challenges to transparency and accountability exist. The value of the paired combination of "trust" and "information" are apparent when organizations and users must make decisions based on the information they can access, regardless of its format. Trusted information has business value requiring its governance and retention. Deliberate frameworks/constructs must be adopted to protect information and its characteristics of authenticity, reliability (accuracy), integrity, and usability, allowing for trust/trustworthiness to persist in the processes and systems used (ISO 15489-1:2016, pp 4-5).

Trustworthiness of Systems

Trustworthiness encompasses the characteristic of accuracy, reliability and authenticity of a record. It implies dependability, honesty, and truthfulness. Victoria Lemieux states "… trustworthiness in archival theory encompasses the concepts of accuracy, reliability and authenticity of a record and is intertwined with the concept of provenance." (Blockchain Technology for Recordkeeping, *Social Sciences and Humanities Research Council of Canada*, p 18) In terms of information systems, in 1999, Schneider stated that trustworthiness of [a Networked Information System] asserts that the system does what is required—despite environmental disruption, human user and operator errors, and attacks by hostile parties—and that it does not do other things. Design and implementation errors must be avoided,

eliminated, or somehow tolerated. Addressing only some aspects of the problem is not sufficient. Moreover, achieving trustworthiness requires more than just assembling components that are themselves trustworthy (Schneider, 1999 (†536 p. 2)).

Trusted Systems

Trusted systems are concerned with the preservation of information within a system comprised of human processes aided by software and hardware. The defining characteristic of a trusted system is that one can be certain that information that enters into the system does not change while it is in the system unless the change is authorized. This characterization holds for systems that store information at rest or in transit and whether the information is comprised of structured or unstructured data.

Currently, two types of systems are recommended to maintain the trustworthiness of information considered records: trusted recordkeeping systems and trusted preservation systems. Trusted recordkeeping systems adhere to rules that control the creation, maintenance, use and disposition of the records and provide circumstantial probability of the authenticity of the records and the tools and mechanisms used to implement those rules (InterPARES 2, 2018). Likewise, trusted preservation systems adhere to similar rules but control the preservation and use of records.

The advent of blockchain technology may eventually cause a convergence of these systems, as all records stored on a blockchain will, in theory, remain permanently. For the foreseeable future, transactions occurring on a blockchain may link to records that remain off-chain within trustworthy recordkeeping systems and trustworthy preservation systems requiring integration of such systems with the blockchain.

Off-chain Storage and Provenance

From one perspective, blockchain is a record storage solution (Lemieux, 2016). All nodes in the network must verify the information for each transaction via a consensus mechanism in order to verify and trust the immutable record. The immutable record is stored permanently, and the information is transparent to all users on that blockchain. Blockchain has the potential to change fundamentally how information is stored and retrieved. Blockchain is critical as to how information will be stored in the future.

Off-chain storage and processing may seem counter-intuitive to blockchain's fundamental principle of decentralization and a covenant of trust in the immutable record. Yet, this is a reality. Before the information is stored on the blockchain, it is generated "somewhere"—and in most cases, the information is created off the blockchain. At some point in the information lifecycle, the information will exist in physical form and then be converted into a digital format and stored "somewhere" or created digital and then stored "somewhere." Examples include medical records, sensory data, mortgage papers, property records, personal financial information, payment transactions, deposits and withdrawals, voting transactions, smart contracts, birth and death certificates, and voter lists. Other examples are data backups, copies of data when moving off a blockchain network while keeping only a portion of data on a blockchain, and more. In these cases, the information will exist "somewhere" off-chain.

This information— such as "who sent what to whom and the details"—must be validated before it is put into a blockchain's ledger as a trustworthy and immutable record. Knowing the origin of the information is essential because "… there can be no automatic guarantee of reliability for records created off-chain but hashed on chain, as factors affecting their reliability will be outside the purview of the blockchain system" (Lemieux, 2016, p 16). Therefore, the information's integrity at the point of generation is essential before storing the information into the blockchain. This raises the question of provenance—establishing a linkage between the off-chain data and the blockchain record. Provenance demonstrates the ownership of information from the point of creation off-chain and its authenticity until it is hashed on chain. Lemieux quotes Gideon Greenspan, CEO of Coin Sciences, "Provenance is one of the backbones of economies … There has always been a need to authenticate that a party actually owns an asset prior to any business dealings involving that asset, to ensure that the asset is 'true' rather than stolen or faked" (Ibid, p 13). Lemieux further states, "The significance of provenance stems from its use as an indicator of … [the] … trustworthiness of records" (Ibid, p 18)

The blockchain ledger contains information in the form of immutable records regarding transactions. Hashing the information without any independent validation and verification (IV&V) is potentially risky. "By creating a hash of … an electronic record, the data can be placed on a blockchain, where changes can be tracked. While this doesn't solve the problem of a falsified source document, it can verify that a record has not been altered … starting from the time the document's hash is uploaded to the blockchain" (Prentiss, 2018).

An IV&V process to audit the proof of work requires the blockchain platform to develop the infrastructure and implement quality assurance processes to achieve a level of assurance. The infrastructure and processes must verify the source of the information, when it was generated, and audit other details to ensure the information was not tampered with when it was off-chain. The infrastructure and processes must be transparent to everyone. Since the blockchain is a ledger of information, it is critical and paramount that the information that is hashed is correct and accurate.

Blockchain and Sustainability

Blockchain technology is useful for static information and describing the activity of an entity over time. This is particularly the case for archival records and the long-term preservation of other records such as pension information, life insurance policies, real-estate records, etc. Therefore, a blockchain may not be a suitable solution for all data management and data storage requirements. The following is a list of challenges organizations could face when choosing blockchain solutions:

- **Technology*:*** As with any solution, the supporting technology will change. This includes the physical infrastructure housing the data and applications, the software solutions that make up the hosting environment, and the vendor providing the hosting platforms. This can result in challenges for the individual or business whose data is being managed.

- **Changes in Supporting Infrastructure**: The data in a blockchain is housed across a broad range of technical infrastructures. While the data may remain stable over time, there is a possibility that the technology itself may not continue to support it successfully or efficiently. Although the structure of the data is intended to be technology independent, there could be some points of

vulnerability with respect to the encryption and hash tags, which may cause problems over time. Another issue is the impact of successive implementations of new operating software and the hardware that impedes the blockchain's ability to support the data and applications.

- **Changes in Software Mix:** Software solutions are often not single-sourced; they are a collection of vendor and open source applications working together. The combination works well for periods of time, but it is unclear what the impact will be in the future when elements of that collection change. The risk will be that neither the hosting organization nor the company's internal IT department can find solutions quickly enough to address sudden product gaps that emerge when vendors abruptly depart from the market. This may disable their software functionality and may make the blockchain data unavailable, at least for periods of time.

  This could also be an issue when two different types of technologies become inter-dependent. An example is when blockchain links point to content off-chain, such as in a data lake, data warehouse, etc. While some linking methodologies are based on content rather than physical or logical location, it still depends on the links being valid over time. In this instance, if the relationship between key metadata (the blockchain) or data (the content outside of the Blockchain) is broken, the solution itself fails.

- **Vendor Abandonment:** As with any business, vendors supporting all or a portion of the blockchain applications can fail. This can be a strategic withdrawal from a market, a hostile takeover where a vendor wishes to remove a competitor, or a bankruptcy. In such instances the data becomes vulnerable and access by the owner of the data may be lost.

- **Data Scalability:** Blockchain data continues to grow over time. Solutions to this issue include improvements to the underlying software and hardware to handle more data, the movement to a different vendor or platform that can handle the larger data, or a conversion to another type of application. The question will be how dependent the data is on the current environment and the resources and time necessary to do the conversions.

- **Supporting Standards:** As part of the multi-vendor and multi-technology environment, it is important to have standards to support interoperability. Standards often lag behind the software development cycle. This is an issue that may impact the stability or mobility of the data, as standards are developed retroactively.

Before deciding to employ blockchain technology to resolve a specific problem, consideration must be given to the suitability of the solution. Several models have been developed to help one decide if a traditional database should be used instead. One model, *Criteria to Consider When Deciding on a Blockchain Use Case*, is provided in Annex A. The model helps an organization to ask a series of strategic questions to ascertain whether blockchain is an appropriate solution.

Blockchain Technology Modalities

As mentioned, blockchain is a specific implementation of DLT. If a blockchain technology solution is warranted, three key modalities should be considered:

- Permissioned (private) versus permissionless (public) blockchain
- On-premise versus a cloud-based blockchain
- Build versus Buy

The blockchain architectures are divided into two broad architectures – permissionless (aka public) and permissioned blockchains. Permissionless blockchain are open to anyone, i.e. the public. Bitcoin or Ethereum blockchain are permissionless blockchain and permit any user to access and view the distributed ledger, add new blocks to the ledger, and validate transactions by following specific protocols. Permissioned blockchains are NOT open to the public. Therefore, the organization managing the permissioned blockchain needs to validate the user's identity and give him / her access rights. Permissioned blockchains limit access to the distributed ledger to certain known or trusted third parties. For example, IBM Food Trust is a permissioned blockchain for the food industry supply chain. Companies that join the blockchain pay a monthly subscription fee.

The blockchain solution can be hosted on a cloud platform or it can be on-premise. Organizations seeking to experiment with blockchain may develop an on-premise solution using hardware available.

If a commercial product is not available that meets the specific needs of the organization, organizations may choose to develop the solution in house provided they have the necessary resources.

These three modalities can be represented conceptually as a "3-D decision cube" illustrated in Figure 1, where each modality is a dimension of the cube:

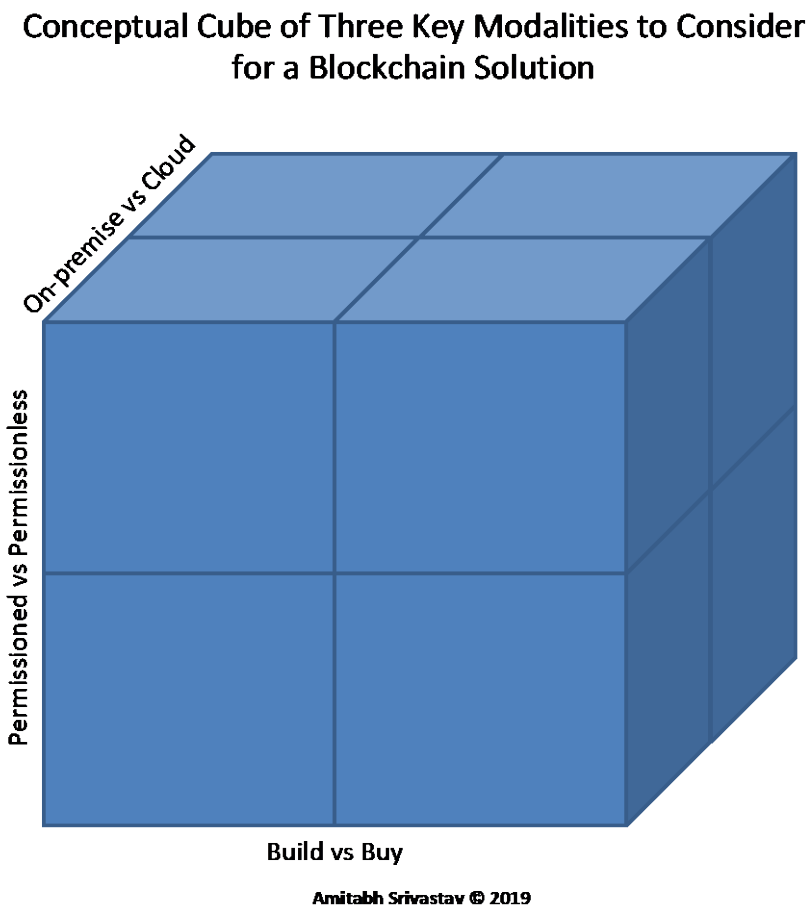


Figure 1: Conceptual 3-D Decision Cube for a Blockchain Solution

The same conceptual cube can be formatted into a decision matrix to aid management in their decision-making process, included in Annex B.

Information Governance

Information Governance professionals might expect benefits from blockchain solutions because they value data based on its authenticity, integrity, reliability, and auditability—all affordances of blockchain DLT.

Since Information Governance includes the processes, roles and policies, standards and metrics that ensure the effective and efficient use of information in enabling an organization to achieve its goals, each of the Information Governance functions and stakeholder roles and responsibilities must be considered when implementing blockchain technology solutions, whether permissioned or permission less.

Typical functions and roles described within the Information Governance Maturity Model are business, records management, privacy and security, information technology, legal, and risk management. When considering the implementation of blockchain technology, each of these facets must be examined. A few examples follow.

Business Operations

Blockchain Technology is designed to record both static data (e.g., registry) and dynamic data (e.g., transactions) in an immutable form. It is sometimes referred to as a new type of *system of record*. This system of record is useful in documenting current actions for future review. However, internal and external factors impact business operations and necessitate changes to the way the records are managed that must be considered when investigating blockchain distributed ledger solutions.

- **Data Separability and Integration**: Mergers and acquisitions are common in the business world. When this occurs, data merges or separates. There will be challenges doing this in the current blockchain environment. Once data is written, the security around access is not totally flexible. The question will be how to selectively strip data about the business activity and intellectual assets that are no longer the property of the organization that holds the original data. It is unclear if there are security overlays, which can address changes in access with existing data.

  When business activity and intellectual assets are acquired, the challenge will be how to link them into a blockchain so that they integrate within the context of existing data. This can be added as new data to the blockchain, but it will be out of sequence with the timing of other elements. This may cause problems with reporting or analytics for decision-making.

  Organizations also reorganize internally resulting in the strategic realignment of functional activities and their associated data elements. This will require additional information to be maintained off-chain so that the information is associated over time. For example, department names, table values, abbreviations, etc.

- **Data Ownership:** When dealing with third party hosting, such as Blockchain as a Solution (BaaS), data ownership can become an issue. If in a shared environment or in a mergers and acquisition situation data cannot be removed, relationships with public or private blockchains may need to be severed so that the data no longer exists in the original environment.

- **Changes in the Political Environment**: Regardless of the type of blockchain configuration, there is always a risk that access to data or data validation resources are lost when political barriers to access are imposed. This can result in the inability for a blockchain to sufficiently validate its own data, causing data integrity and quality issues. This could result in entities on the wrong side of the political barrier only having access to obsolete data, to the development of two different blockchains, and to access to data whose sensitivity has changed given the change in political environment. In the USAID's *Primer on Blockchain*, the following question is posed: "If a blockchain DLT is intended to address corruption, would a corrupt regime be persuaded to

adopt [or allow continued use of] a DLT application that targets misuse of power?" (Nelson, n.d.).

- **Legislation:** The political and legislative environment continues to evolve. As a result, sometimes the data that is stored must be modified or removed, as with the current emergence of "right to erasure" laws. This can become more complex when data is passing through multiple jurisdictions with contradictory requirements.

Records Management

Records and information management professionals must take an interest in blockchain technology, as the potential use of DLT in document and records-rich industries, such as healthcare and supply chain fields, increases. Although at this time, blockchain DLT does not present an alternative to electronic records and information management practices, there is no doubt that implementation of blockchain DLT within an organization will impact those practices. From one perspective, blockchain is essentially a recordkeeping technology!

Blockchain integration for Records Management

There are three aspects to records and information management that should be considered:

1. implementing a records management system on the blockchain,
2. blockchain records management as a service, and
3. managing records created on a blockchain regardless of use case.

When prioritizing use cases, records management is low on the list. While creating a blockchain-based records system could provide some protection against forged or erroneous documents, in 2016 the Vermont state legislature concluded, "The cost of using an implementation of the blockchain for a public records management system would outweigh any potential benefits" (Higgins, 2016). They envisioned blockchain technology implementations supporting, not replacing their existing records management infrastructure.

By 2018, proof-of-concepts (POCs) were emerging within the records management industry. Some POCs extend the capabilities of existing software and services. For example, Sphereon, a Dutch startup by software specialists, provides two extensions for Alfresco's Content Services & Process services. The first, Blockchain Audit Trail, provides a Proof of Process, by allowing the client to create, browse and verify transaction audit trails using blockchain. The second, Blockchain Authentication, allows the client to register and verify data, records and objects on a blockchain for independent, tamper-proof, Proof of Authenticity. The first extension supports use cases for records management, compliance, and transparency for external stakeholders. The second extension supports use cases for certification of digital objects (e.g., titles, claims, diplomas, and file transfers). Sphereon also provides a SharePoint Add-in or SDKs (Software Development Kits) to add blockchain as part of workflows.

Trustworthy Records

Trustworthy records are those that possess the characteristics of authenticity, reliability (accuracy), integrity, and usability (ISO 15489-1:2016, pp 4-5). Stakeholders of records need to be able to trust that

a record of an activity is what it purports to be, having been created or sent by the agent purported to have created or sent it, and having been created or sent when purported (Ibid, 4). Stakeholders must trust that a record is complete and unaltered—that it has not been changed in any way that affects its representational content. This demands evidence of a chain of custody (or in archival terms, provenance), which is satisfied by the blockchain itself. Equally important, stakeholders must trust that a record can be located, retrieved, presented, and interpreted within a mutually acceptable timeframe.

Records on the blockchain are securely linked in a shared trusted ledger. The records are transparent and immutable, ensuring integrity. All participants of the network can inspect the records at any time. The distributed nature of the technology guarantees access to the records in spite of the failure of any node within the network.

The concept of trust that applies to the record extends to the stewards of the records in normal circumstances. Such "trusted custodians" must be able to demonstrate that they have no reason to either alter nor allow others to alter the preserved records and that they are capable of implementing all of the requirements for the storage and preservation of trustworthy records. With the advent of blockchain technology, trusted custodians are replaced by a built-in "trust protocol."

Immutable Records and DLT

The immutable nature of the records on a blockchain instills trust. Traditionally records were "declared" as such and stored so that they could not be tampered with. In the case of physical records, file cabinets with locks and keys to records rooms helped give a sense of security. In the digital world, moving records to a digital repository or locking them in place with read/write access provided a similar sense of security. The move to the cloud brought the issue of vulnerability to unauthorized individuals to the forefront with one popular potential solution: encryption both in transit and in the cloud.

In the context of solutions based on DLT technology, cryptographic hashes of records can be stored on a blockchain. The process using complex algorithms is irreversible; a hash can never be turned back into the original record. The time stamp encrypted with each record can be used to ensure trust. Proof of tampering is evident if the hash of the current record differs from the hash of the blockchain-stored record.

Integration of records and information systems and DLT

As with other emerging technologies, DLTs based on blockchain will traverse the Gartner hype cycle from innovation to the plateau of productivity. This technology has already arrived at the peak of inflated expectations and is now moving down into the trough of disillusionment, as many of those expectations are not being met.

As stated, records and information management systems will not be a high priority for DLT initiatives. However, use cases that compliment records and information management will impact recordkeeping practices; for example:

- *Legal Industry:* Both OpenLaw and Integra provide blockchain driven systems that allow lawyers to automatically generate legal agreements and build smart contracts that can be executed on a

blockchain. Rather than store records on the blockchain, OpenLaw explains that clients can create, store, and execute legal agreements that interact with blockchain-based smart contracts without the need for any intermediaries.

- *Healthcare industry*: MedRec is an initiative out of the Massachusetts Institute of Technology (MIT) to leverage the blockchain to manage patient records throughout the patients' life as they (and their data) move between healthcare providers. MedRec does not store the record directly; rather it encodes metadata that allows records to be accessed securely by patients. The metadata contains information about ownership, permission, and the integrity of the data being requested.

For the foreseeable future, most blockchain technologies and DLTs will interact with existing systems off-chain to access records stored in legacy systems, work areas (e.g., in SharePoint), and digital storage services (e.g., Dropbox). This is due in part to the cost and performance issues of encrypting large volumes of data and adding to a blockchain. However, DLT will be increasingly used from the creation of some records through their disposition.

In February 2019, the National Archives of the United States released their *Blockchain Whitepaper* to reveal the potential implications for records management within the federal government. The key points extracted from the paper underscore the challenge presented by the conflict between current policies and practices and this new technology. Specifically, NARA recommends:

- Developing policies to address the records management implications of blockchain
- Implementing systems that can execute those policies
- Ensuring blockchain records/transactional data can be accessed over time
- Executing the disposition of blockchain records/transactional data by deleting them or transferring them to the National Archives (NARA, 2019)

The use of blockchain creates new records that must be identified and considered the responsibility of the organization. Records and information management professionals who keep abreast of blockchain and DLT will be in a position to help the organization meet the challenges that arise.

Blockchain Records Management as a Service

RecordsKeeper is one vendor that offers a public and open blockchain for recordkeeping and data security that can be implemented on-premise or in their cloud. Organizations can also use the public blockchain, which promises the following benefits: data immutability, integrity, authenticity, and verifiability. When a user uploads a file, a condensed record along with metadata information is signed and pushed into the RecordsKeeper ledger. The actual data is pushed to the encrypted storage layer for later retrieval.

Managing records created on a blockchain regardless of use case

DLT is a consensus database of replicated, shared, and synchronized digital data dispersed geographically without a central administrator or centralized data storage. Organizations are starting to move from PoC projects to real-world applications based on places where there is a good fit, such as voting, Internet identity, cloud storage, real estate, healthcare, and supply chain management. Examples of use cases in several of these industries are provided in the Use Cases Section.

Privacy (including GDPR)

Organizations considering deploying blockchain / DLT technologies must determine whether the implementation is consistent or advances their objectives to comply with information privacy laws and ethical standards. Information privacy is a broad and rich concept that implicates numerous moral and legal rights and responsibilities. These include rights concerning the creation, use, disclosure, and processioning of information. In the US context, concerns about access, control and confidentiality are central. In the EU context, to these concerns are added interests in processing and decision making, especially in relation to the allocation and distribution of fundamental goods. Assessing whether blockchain implementations promote privacy objectives and compliance or undermine one or both of these objectives is an important consideration for potential implementations.

Challenges

Organizations under the jurisdiction of the General Data Protection Regulation (GDPR) or the California Consumer Privacy Act of 2018 (CCPA) or similar privacy regimes, should proceed with caution before using blockchain DLT to write, process, or store personal data. Rights and responsibilities under these legal regimes may present challenges given the indelible and distributed nature of the technologies. Cross-border transfers (GDPR) and rights of erasure and correction (GDPR, CCPA, and others) present challenges. Permissioned / private blockchains can better address cross-border transfer issues than permissionless/public blockchains by segmenting data by jurisdiction. They can also avail themselves of ". . . standard contractual clauses, binding corporate rules, codes of conduct or even certification mechanisms . . ." (CNIL, n.d., p. 5). Public blockchains are inherently global and more difficult to control. Erasure poses a technical challenge. The CNIL (Commission Nationale Informatique & Libertes) notes that, while erasure is incompatible with operations of a blockchain, technical means might be available to render encrypted data unusable, though not strictly speaking erased. These methods, however, would need to be evaluated for their feasibility and cost effectiveness and would not be available for unencrypted personal information (clear text) (CNIL, n.d., pp. 8-9).

It should also be borne in mind that privacy laws often require the production of information, inspection of records, and other process-oriented activities. Privacy by design features should be built into enterprise information systems and should enable organizations to discharge their responsibilities effectively. Therefore, the feasibility of deploying a permissioned blockchain for encrypted personal data will depend how well they integrate with enterprise systems.

Opportunities

The promise of blockchain is to transfer trust from parties to the technical architecture. Third party intermediaries who normally perform the function of validating the trustworthiness of the parties will become obsolete as the algorithms of DLTs validate transactions using pseudonymous identities. Organizations will still often wish to capture personal information about the customers or constituents, but in some cases the amount of data needed to carryout transactions may be minimized. With fewer third parties involved, the risks that arise from storing personal data in centralized systems in multiple organizations may be reduced. Digital signatures and hashes may serve as proxies in certain transactions, with personal data stored off-chain by the end user organization for normal business

purposes. Deployed strategically, blockchain may contribute to the objective of data minimization when combined with the minimum needed off-chain personal data storage.

Disposition

A major benefit of the pubic blockchain is that recorded transactions are immutable—unchanging over time and unable to be deleted (altered). Both recipient and provider of data can be certain the data has not been altered. In the case of financial transactions, this benefit is useful. However, permanent retention of most enterprise records is neither defensible nor advisable. The question then arises, "How can legal requirements embedded in GDRP and numerous nation and state privacy laws for the deletion of personal information be complied with when the information is stored on an immutable ledger?"

The EU considers public keys on a blockchain to be personal data because repeated use of the pubic key can build a pattern from which an individual can be determined. Personal data encrypted on a blockchain can be read by an entity holding the key or an expert who can decrypt it. Hashed (encrypted) personally identifiable data is considered "pseudonymous"—not "anonymous"—because hashes enable records to be linked. Because the GDPR and similar privacy legislation allowing parties to request modification and/or deletion of data is recent legislation that may be subject to revision, the easiest solution would be to provide an exemption for personal data encrypted to a blockchain. However, that may not happen in the near future, and even if it does, similar privacy laws must be considered.

If a blockchain is implemented for records management—or for another purpose but containing records that should not be retained permanently—a method for disposing of old data must be established. One possibility is "burning." Burning can be accomplished in one of two ways:

1. "forgetting" the associated public key or
2. assigning the data asset to an address for which no one has the key.

To date, the EU has not commented on the use of burning to comply with the erasure clause of the GDPR, since data is not actually deleted but merely made inaccessible.

Perhaps the most reliable workaround is to store personally identifiable data off-chain and store only the individual's public key, a hash of their personal data, and a reference to the data on the blockchain. Permissions would be established to ensure only authorized parties could access the data. This solution presents additional questions: Who would control the off-chain database? Setting compliance requirements aside, would this solution be more or less secure than storing information on a blockchain?

The response to the first question, "Who would control the off-chain database?" contradicts one of the tenets of a true permissionless blockchain—disintermediation. Some blockchain initiatives attempt to implement this type of arrangement whereby an intermediary holds customer data, protects it, and honors all of the requirements for GDPR or California's law. The answer to the second question, "Would this be more or less secure than storing information on a blockchain?" would depend upon the intermediary and ownership of data. Privacy risk would be outsourced to the third party, but the owner of the data (whether a party to the contract on the blockchain or the third party) is responsible for compliance with overarching regulations.

Use Cases

The underlying DLT for blockchain can be categorized according to generation of the blockchain implemented. The first generation—BitCoin—had just one use case: financial transactions. The second generation introduced by Ethereum enabled the coding of smart contracts and decentralized applications that reside atop the blockchain. The third generation provides extensibility beyond the blockchain protocol to connect with other systems, services, analytics, and, more broadly, the outside world.

Because of the hype around blockchain, it can be said that in many instances blockchain is a solution in search of a problem. However, as the following use cases illustrate, there are a wide range of problems that may be addressed through the use of some type of blockchain digital ledger technology.

Elections Use Case

Problem Description

Elections are an essential way to elect government and organization officials. The election process is under constant scrutiny and subject to claims of corruption. Voter turnout is another concern of those being elected. Technology may address, some, if not all, of these concerns.

Business Challenge

Voting requires citizens to verify their identity and eligibility to vote by producing government-approved identification. Once the individual's identity and eligibility are confirmed, the identity of the person must be kept separate from the ballot. It is imperative that the secrecy of the voter is maintained throughout the election process. Elections should be controlled so that the results are not compromised and claims of corruption can be easily resolved without challenges being introduced. As technology is introduced to the election process, building trust among the voting population is key.

Solution

Blockchain voting would have some similarities to our current voting process. Citizens would continue to need to register and prove they are eligible to vote in their given jurisdiction. Once voting eligibility is verified, a voting token would be deposited to their blockchain account. The token would have a date associated with it as to when it would expire, which would coincide with the close of the voter's designated polling station. If the token is not used within the time limit, it would expire and the ability to use it to vote would be canceled for that election. When a person voted, the vote would create a blockchain transaction that will be used to track the votes. Using blockchain technology, everyone would be able to count the votes for themselves and verify that the results and each vote were not tampered with, removed, or changed.

The voter registration (i.e. voter information) will be generated and recorded off-chain. The voter's eligibility must be verified prior to a key or token being distributed that would allow the voter to vote one time for a given election. The transparency of blockchain will allow voting results to be audited and recounted with ease.

Blockchain relies on digital secret keys. If a key is lost or compromised, there is no recourse. In order to receive the digital secret key, the voter would need to agree to a voting smart contract. In this type of

implementation, blockchain will need proven security. The process for authenticating voters and verifying their eligibility to vote will need to also ensure that a voter only votes at his / her designated voting stations and does not vote more than once. It is imperative that the voter's anonymity be maintained.

The key to the successful implementation and use of blockchain will involve educating the public about blockchain technology. It is important to build trust in the blockchain technology with all segments of the voting population. While it may be a given that the younger voters would be more receptive to blockchain technology being used in elections and using a mobile phone or computer to vote, all voters will need to be educated on the technology and its benefits.

Blockchain voting is in use with some success. In 2018, West Virginia experimented with the use of blockchain in the midterm elections. They designated one small segment of their voting population as the test group. In this instance, the test group consisted of military personnel who were deployed overseas, which made voting in the election problematic for them. The deployed military personnel were able to vote, and their votes were easily included in the tabulation of votes for West Virginia.

Blockchain voting was used a second time in the US in the 2019 Denver municipal elections, allowing approximately 4,000 service members and overseas citizen voters to cast their ballots (Bryanov, 2019).

Military personnel stationed overseas will again be able to cast their ballots using blockchain technology in West Virginia in the 2020 elections.

Other countries such India, Switzerland, South Korea, Japan, and Thailand have trials or are planning trails for various types of e-voting initiatives using blockchain.

NASDAQ ran a trial for shareholder e-voting in Estonia (MarketInsite, 2017). Another example is India's National Stock Exchange, which is also running an e-voting trial using blockchain.

At the time of publication, several products were available for eVoting that are based on blockchain technology as shown in Table 1:

Table 1. eVoting Products based on Blockchain

Product	Description	URL
Follow My Vote	An online voting open source solution	https://followmyvote.com/
Democracy Earth	A blockchain voting startup	https://democracy.earth/
Votem	A mobile voting platform	https://votem.com/
VoteWatcher	A voting and election service	http://votewatcher.com/
Voatz	A mobile focused election voting and citizen engagement platform	https://voatz.com/#page-top
Smartmatic	An elections technology company	https://www.smartmatic.com/us/about/

Benefits

In addition to potentially increasing voter turnout, blockchain technology will benefit elections in other ways. Blockchain transactions record data in virtually tamper-proof cells, which reduces the potential for fraud and rigging. The voting process will be more transparent using blockchain and the ability to track the vote to ensure it is included in the final tally. Votes will be able to be tallied in real-time. Blockchain technology will make voting more convenient with mobile telephones for voting which may improve voter turnout.

Implementation Considerations

The following questions should be asked and answered:

- How can the privacy of the voter be maintained in a public blockchain environment?
- How can voter anonymity be maintained?
- Can the voter's information be kept separate from their vote so that the public cannot determine how a specific individual voted in an election?
- How can trust for these eVoting systems be built?
- What should the voting smart contract cover?
- Can the blockchain based voting system be scaled to handle national elections?
- How can voter identity be verified? How are voters authenticated?
- What centralized authority should confirm identity? Does the voter need to use a secure VPN to vote?
- Is an open source voter application used?
- Is a voter able to change their vote based on the up-to-the-minute results that would be available in a blockchain environment? Should voters be able to change their votes? What legal risk does this present?
- If voters should not change their votes once cast, what safeguards can be implemented to prevent this?

Identity Management for Online Interactions Use Case

Problem Description

User identification and verification is essential for secure interactions with online retailers, financial institutions, medical facilities, suppliers, education institutions, social media companies, etc. Trust of the mechanisms is essential for consumers to use these systems. Given the growing volume of online transactions and interactions, the management of digital identities is susceptible to fraud and abuse. Mobile device use increases the vectors for misuse, fraud, and theft.

Business Challenge

User identification and verification must be repeated for each site and organization, sometimes for each transaction. The duplication of effort by creating a separate identity for each site and/or transaction wastes time and resources and increases risk because each user has multiple digital identities. User information is shared between online sites, often without user permission. Increased risk of credentials being stolen has become endemic. Companies must store customer credentials for future reuse, which is an added business expense and security risk. Consumers want security, ease of use, and speed in their online transactions and interactions. Existing systems—biometrics, knowledge-based authentication, and one-time passcodes for two-factor authentication—are the most trusted, and they all have weaknesses. Passwords are another weak link.

Solution

The Identity Management of your personal identification information (PII) can improve and strengthen the security of an individual's digital identity. The self-sovereign identity principle empowers the individual to control their PII directly, giving them full control over their digital identity. The question of trust is central to any solution. A single digital identity that can be shared across all platforms and is managed by the individual user on both desktop and mobile devices may be the best option. Trust is crucial, so a set of standardized and accepted protocols, standards, and processes in the system will ensure that users, businesses, and other organizations are confident enough that they use the system. These standards should include quality assurance and levels of assurance tools to verify the digital identity. The user should be able to interact with the system to ensure that their digital identity is secure. Backup procedures are necessary to ensure redundancy protection.

Benefits

Some of the benefits of blockchain identity management for online interactions are:

- Increased user confidence that their PII is protected.
- Decreased incidents of identity theft.
- Increased user confidence in online transactions and interactions.
- Lowered costs and reduced risks for businesses that stop storing and managing user digital identities.

Implementation Considerations

The following questions should be asked and answered:

- Which parts of the identity management process can be strengthened with blockchain?
- What standards and protocols should be developed to facilitate the creation, implementation, and management of a self-sovereign personal identity system?
- What standards and protocols should be developed to facilitate the creation, implementation, and management of a trusted IM transaction system?
- How is trust in the new systems encouraged?
- What will encourage business buy-in of the new systems?
- What is the blockchain platform's support for Business Intelligence (BI) and other analytical tools for real-time predictive analytics, support and evolution of AI to provide insights, and tools to access data and generate compliance reports for regulators and other industry stakeholders?

Supply Chain Management: Food Fraud Use Case

Problem Description

Today economies and their industries are more connected than ever via sophisticated and complex supply chains that span the globe from one continent to another. Given the large and growing volume of global trade and integration across industries, the marketplace is susceptible to fraud. This fraud is also evident in the agriculture and food distribution industries, including instances of food fraud and food safety with respect to distribution, traceability, validation and verification.

Business Challenge

Improving and streamlining the agriculture-industrial supply chain is essential in order to more accurately track the food from origin to destination, and thereby help increase food safety, improve food quality, reduce food fraud, and improve the enforcement of agricultural regulations. By 2050, the global population will grow to almost 10 billion people (HOW 2050, 2009). As a result, farm output will have to increase by about 70 percent to satisfy food demand. Due to improved living standards and increased awareness around the world, consumers are demanding a safe and secure food supply chain and governments are enforcing regulations to provide a LoA. So, the question remains—can consumers trust what they are eating, and trust the government to enforce the regulations?

Solution

The question of trust concerning food touches several areas of the supply chain—from source to destination. Provenance is essential so that the complete history of food is available from point of origin to final destination, including how the food moves through the chain of possession. In this supply chain, many third parties "touch" the food before it reaches the consumer. The solution must demonstrate that consumers can trust what they are eating and feeding their families. Some key areas of trust concerning food are food fraud, food origin, and food quality. Food fraud can include mislabeling the food items and / or substituting one item for another. Food origin can involve trade in food from questionable sources and / or farming methods. Food quality is closely related to food contamination, standards, and grades where the food item does not meet the expected quality. While these three areas might be somewhat distinct, in reality they are closely interrelated. Food fraud can begin at the source or occur anywhere along the supply chain, where the original food item is replaced by an item of lower quality. The blockchain can identify the exact point where the substitution occurred and provide the evidence to prosecute the perpetrators. The blockchain can also identify all the food items that were affected so that consumers are notified and protected.

Benefits

In the consumer's mind, there is an increased perception of trust in the food items—produce, dairy, meats, and other unprocessed food—from "the field to the table." This will also include food and other raw inputs for packaged goods. From the organization's perspective, benefits will coalesce around better governance, risk management, and compliance. This can help reduce costs, and improve operational efficiencies, public perceptions, and return on investment (ROI). Another benefit is providing more transparency, agility, responsiveness, and insights to market trends, consumer's needs, producer's outputs, etc.

Implementation Considerations

The following questions should be asked and answered:

- Which blockchain platforms are common in the food industry for the products and services your organization provides?
- Are private, public, or hybrid blockchain platforms used by your organization's multiple suppliers' part of multiple supply chains?
- If the supply chain spans international jurisdictions, does the platform support interoperability between multiple regulators in multiple jurisdictions?
- How will consumers, industry organizations, non-governmental organizations public interest groups, activists, etc. access the information stored in the blockchain to validate the origin and quality of the food?

- What are the industry trends affecting the evolution to BaaS?
- Is real-time tracking available, especially when multiple supply chains are involved?
- What is the blockchain platform's support for BI and other analytical tools for real-time predictive analytics, support and evolution of AI to provide insights, and tools to access data and generate compliance reports for regulators and other industry stakeholders?
- How does the platform provide or support high availability, operational resiliency, business continuity, and disaster recovery?

Business Process Management/Workflow Automation & Blockchain

Business process management is central to the operations of every organization and orchestrates processes, people, systems, data, and business rules. The processes are inspected, discovered, documented, analyzed, modeled, streamlined, implemented, enhanced and re-engineered to represent end-to-end process flows and make operations more efficient. Once the process is streamlined, the business rules are defined along with the flow of information, triggers are identified that allow the process initiation, process paths based on business rules exchange bits and pieces of process components towards the completion of a process life-cycle. Business process automation is implemented through a workflow automation platform within an organization.

Business Challenges

Business processes management within a single organization can succeed, since all business units/parties are collaborating and aiming to be successful as one organization. The business process within an organization is automated through workflow platforms that are considered private to one organization. Once the business processes cross multiple organizations, becoming public, and interaction happens with the disparate systems of each other party, challenges of different process models, gaps in data/information-systems exchange, reconciling between different entities, business rules, etc. are presented—resulting in a lack of trust in sharing data and processes. A typical example is the insurance claims processing between two different insurance companies. Different companies have different internal processes and use different workflow platforms for automation.

Solution

Blockchain technology could be promising in cross-organization process automation that may improve efficiency of process management, reducing cost of processing transactions by cross-collaboration, model and business rules unification across organizations, well identified conditions and triggers, and data-system exchanges that can standardize the trust between different organizations.

Benefits

Among the benefits that could be realized by the introduction of blockchain DLT are:

1. Improved process operations efficiencies through workflow automation, elimination of the middleman (typical in smart contracts use case), removal of the need to reconcile data repeatedly between disparate systems and organizations, increased transparency and data trust. For example: in Human Resource recruiting systems, verification is a major issue. Over 50% of resumes do not present the real qualifications of the candidates. Building a central verification mechanism through blockchain where it will serve as a trusted source of

qualifications such as transcripts, certificates, and diplomas, could be a use case for blockchain solution.
2. Increased processing performance through the use of smart contracts executed based on automated processes through workflow automation platforms. Smart contracts eliminate human interventions which results in increased processing speed.

Implementation Considerations

Before implementing a blockchain solution for business process management/workflow automation, consider the following:

1. Blockchain Implementation will require a drastic change, basically complete re-engineering of the business process and workflow automation. The steps taken to purchase a car through smart contracts is a case in point: "You might not even need documents for your car in order to prove ownership, ownership could be documented in the blockchain. The insurance agency could sign the smart contract to prove insurance. No paperwork, no regulatory authority, no bank involved at all! This is a radical change that will take a long time to happen—in this case it is much more likely that we will get autonomous cars first" (Rücker, 2018).
2. Drastic changes have to happen in re-engineering business processes across organizations at the same time, if different parties are willing to adopt blockchain technology. Practically it may not be feasible to unify the changes in different organizations simultaneously.

Risk Considerations

Storing information in a central storage (database, super ledger) to be shared by all parties will introduce a level of risk related to information confidentiality and sensitivity, and it may lead to risk of information security and privacy.

Integration: Internet of Things and Blockchain

The Internet of Things involves billions of devices that collect and receive data and exchange transactions between each other using distributed applications to communicate. This takes place off-chain. Two examples are smart devices and sensors. The data are stored in central locations, and the online identities of the devices or individuals accessing and receiving the data are not stored or embedded in the transaction process, so there is the question of trustworthy transactions and the capacity of networks or communication protocols (see Off-chain Storage and Provenance section). "Blockchain is designed as a basis for applications that involve transaction and interactions." DLT shares commonalities with the distributed applications used by IoT, so DLT will play a big role on revolutionizing IoT.

Business Challenge

With the myriad of devices that comprise the IoT, security is already a concern and a challenge. A few issues to consider are:

- The orchestration of many aspects/devices of IoT poses operational challenges.
- Companies are not equipped to scale up the verity of IoT today.

- Since data is stored in central databases, associated problems emerge, in particular "a single point of failure."

Solution

"Blockchain is seen as the answer to IoT challenges" because of the decentralized nature and framework used for blockchain systems to ensure trustworthy and secured distributed transactions and interactions.

Benefits

Using blockchain for IoT will improve security, trust between integration and transactions of the devices, reduce operational costs, and accelerate transactions.

Implementation Considerations

Some of the questions that must be addressed before implementing blockchain technology with IoT are:

1. Can a blockchain-enabled IoT system be used for the production-chain fraud reduction?
2. Do the devices possess the processing power to directly participate in a blockchain?
3. Can online identities of devices and users be stored and be authenticated in order to increase the security of interactions between IoT devices?

Risk Considerations

Storing information in a central storage (database, super ledger) to be shared by all IoT devices, can pose a risk to information confidentiality, information security and privacy. For example: "The proof-of-work step in blockchain creates costs for someone who might want to flood a network with fake information" said Christian Catalini, an assistant professor at the MIT Sloan School of Management in Cambridge, Massachusetts (Compton, 2017).

Risk Implementation and Audit Considerations

As with any new technology, there are numerous risks, many of which are unknown, as organizations start to adopt the technology. Blockchain is such a technology. As blockchain technologies evolve, organizations will share their real-world experiences and risks of implementing and operating blockchain solutions. In the meantime, organizations must continue to apply prudent risk management practices. This white paper attempts to provide an unbiased view of potential benefits and possible risks of using a blockchain solution. The risks discussed below are by no mean an exhaustive list, but they are some of the key risks that have emerged from current real-world experiences.

This white paper does not purport to provide a risk management framework. Instead, it provides context for assessing and considering the risks of selecting and implementing a blockchain solution. An organization can identify the risk using a quadrant approach – strategic risk, design risks, implementation risks, and operational risks, as represented in Figure 2.

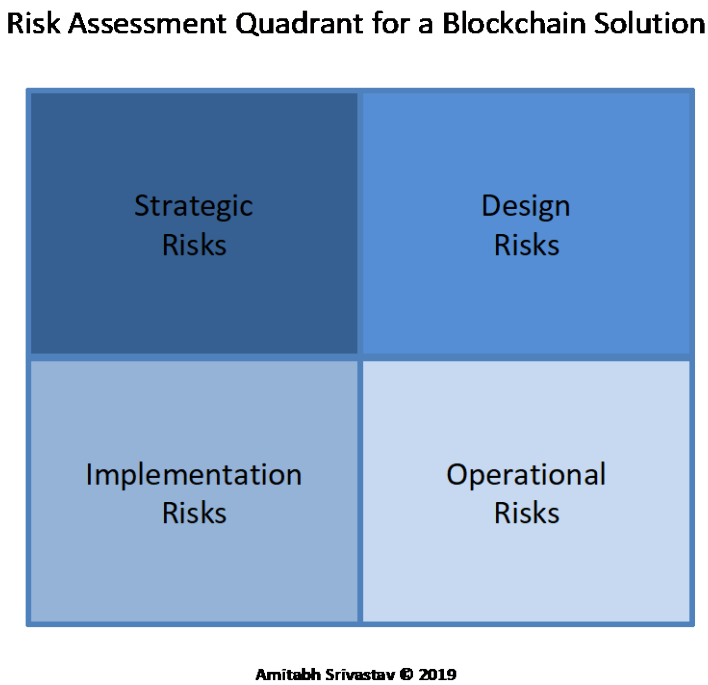


Figure 2: Risk Assessment Quadrant for a Blockchain Solution

To assess the strategic risks, the organization can use the questions shown in Annex C. From a process perspective, the next step is to assess the design risks. The design risks can help define scope of the implementation and its risk. The implementation risks in turn dictate the operations risks. These four risk levels are illustrated in Figure 3:

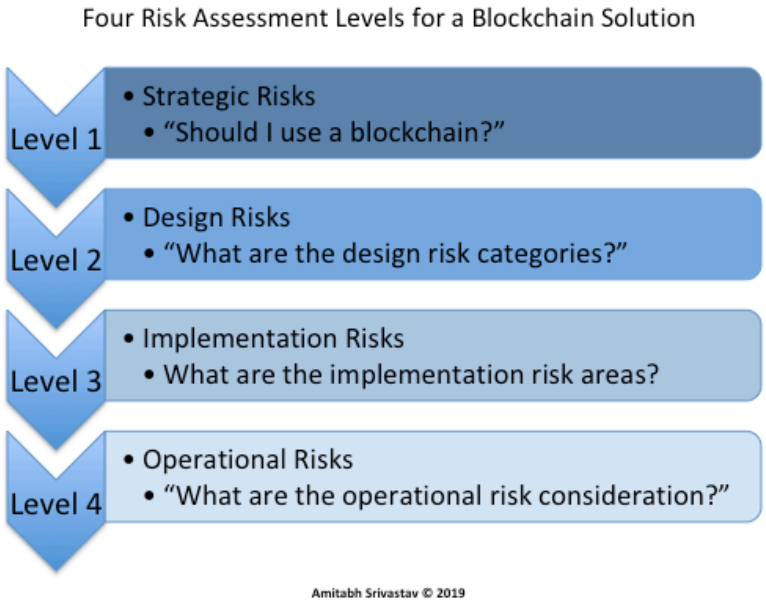


Figure 3: Four Risk Assessment Levels for a Blockchain Solution

The risks become more specific moving from Level 1 to down to Level 4. Thus, the Level 2 design risks are divided into seven categories:

- Governance
- Operational Structure
- Reputation
- Blockchain Architecture
- Legislation and Regulations
- IT Operations and Network Security
- Project Planning

Each Level 2 design risk category is further divided into one or more Level 3 implementation risk areas. Finally, each Level 3 implementation risk area has one or more Level 4 operational risks. Figure 4 below illustrates Levels 1 to 3 of a Risk Breakdown Structure (RBS). Level 4 is not shown in this illustration. However, this white paper includes the RBS as part of a risk assessment tool that lists a series of Level 4 operational risk assessment questions detailed in Annex C, *Blockchain Implementation Risk and Audit Considerations.*

The organization should use the RBS to evaluate and consider the risks. Note that all risks may **not** apply to every organization considering to use a blockchain solution.

The same risk assessment tool presents an approach for auditing the blockchain solution. This whitepaper does not purport to offer an audit framework for auditing the risks of using a blockchain solution. Instead, the white paper presents an approach to consider when preparing an audit framework.

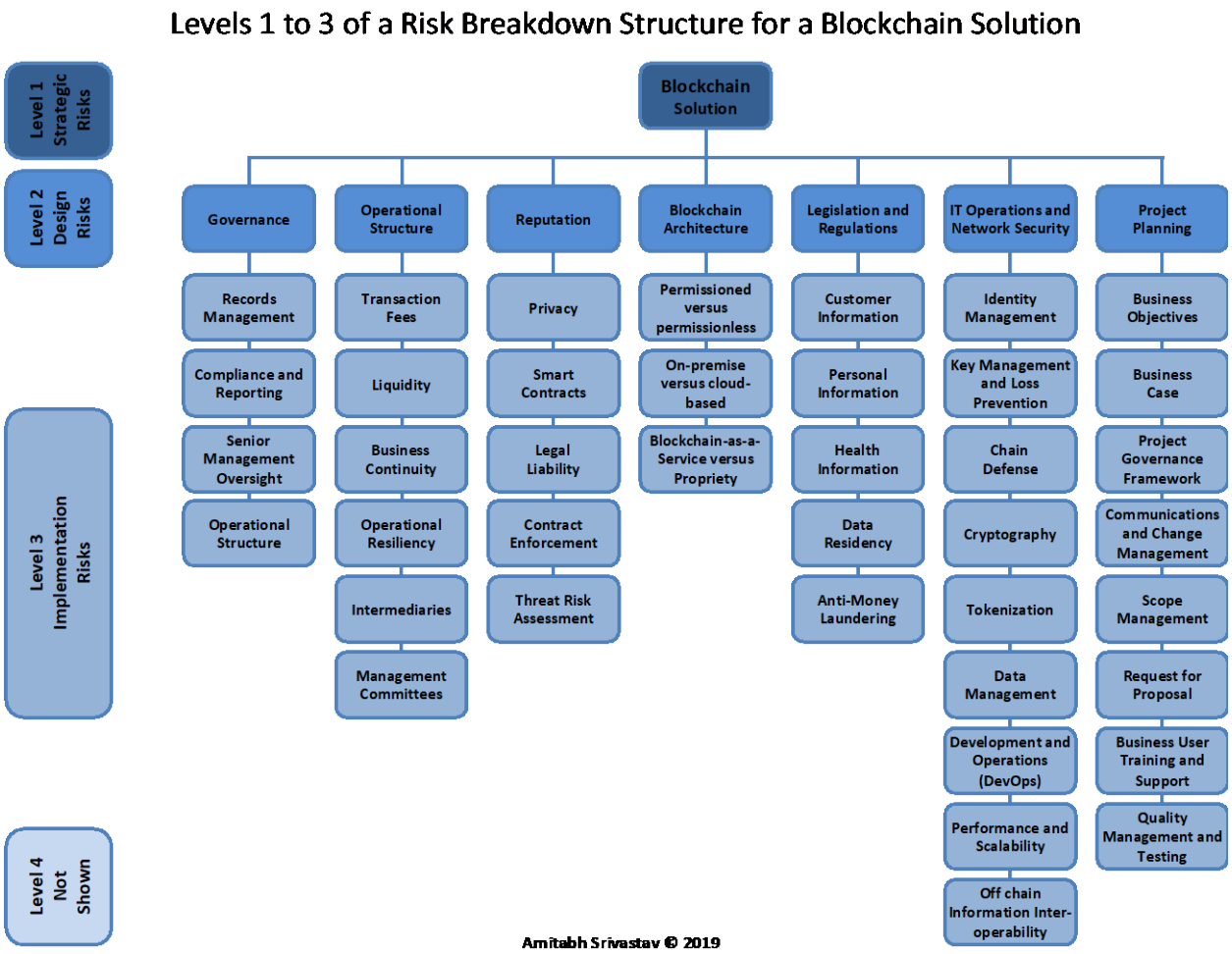


Figure 4: Levels 1 to 3 of a Risk Breakdown Structure for a Blockchain Solution

Conclusion

Since 2009, blockchain technology has exerted a disruptive influence on the way business is conducted across the globe. The first use case, Bitcoin, was designed to facilitate financial transactions by eliminating the intermediary and placing trust, instead, in public, permissionless, distributed networks and immutable files. In 2015, the Ethereum blockchain was released, which brought with it distributed applications and smart contracts that reside across the blockchain. Distributed applications and smart contracts make it possible to build cases across all industries. Ethereum blockchain technology enabled both public and private networks to operate, which motivated organizations and consortiums to consider how permissioned blockchain solutions might better fill their needs. Today, connections between the blockchain network and other systems and services are recognized as essential.

Care must be taken when deciding if blockchain DLT is right for your organization or if a traditional database is sufficient. A decision tree similar to the one offered in Annex B can be used to determine which solution is the most appropriate. Even when the use of the technology appears to be the best choice, risk considerations must be examined. The *Blockchain Implementation Risk and Audit Consideration* table in Annex C classifies level 3 risks into seven level 4 categories. The questions listed, while not all-inclusive, will assist the organization in determining if the risks presented by the implementation of blockchain DLT should be avoided, transferred, minimized or accepted.

Current uses cases can be found within specific industries, but if blockchain and DLT is to be integrated into the operations of most industries, extensibility beyond the blockchain is essential. Connections between the blockchain network and other systems and services are required, since not all data will reside on a blockchain.

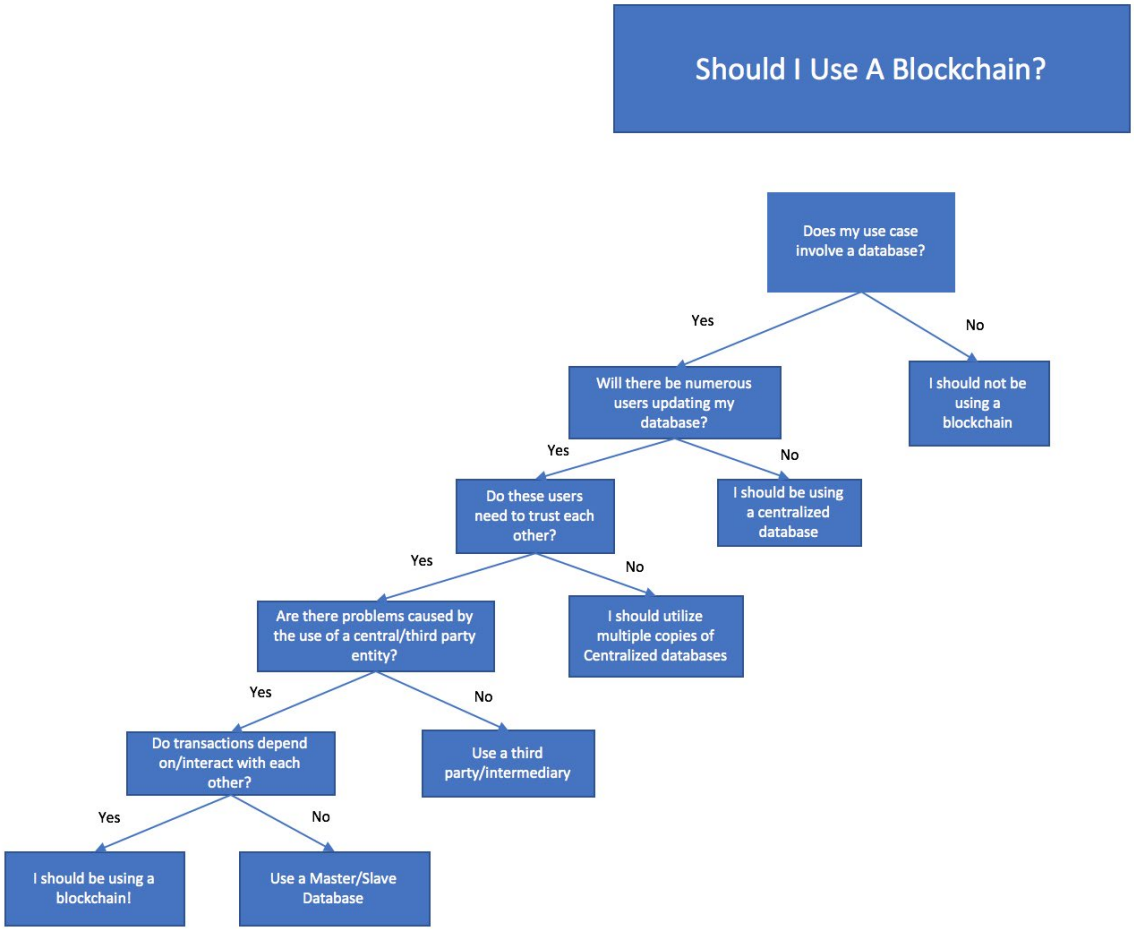
For the foreseeable future, as Saeed Einaj (2019) predicts, "blockchain solutions will be limited within industry verticals, solving specific business problems with limited transformational impact. This might be similar to the impact of the relational database technologies in the 70s."

At this time, the majority of blockchain DLT solutions are implemented to relieve pain points for the organization or industry resulting in cost avoidance or efficiency, as evidenced by the use of blockchain technology to enable military personnel located overseas to participate in the voting process. However, the results of blockchain DLT projects may eventually lead to new opportunities for the organization, such as new business models and services.

Annex A

Criteria to Consider When Deciding on a Blockchain Use Case

This model asks a series of strategic questions to help an organization determine if a blockchain solution is appropriate for it.



Caption: Flowchart that acts as a checklist for those considering implementing blockchain technology. *Source*: With permission, Graham, Wesley. Building it Better: A Simple Guide to Blockchain Use Cases, *Blockchain at Berkley*, https://blockchainatberkeley.blog/building-it-better-a-simple-guide-to-blockchain-use-cases-de494a8f5b60

Annex B

Decision Matrix for Key Modalities for Blockchain Solution

If a blockchain technology solution is warranted, this matrix will help the organization determine which of the three key modalities is most appropriate for its situation and meets its business requirements.

The purpose of this decision matrix tool is to convert the three key modalities in the 3-D conceptual cube into a matrix grid to simplify decision-marking. The matrix grid consists of 16 cells. The steps to use the matrix grid are:

1. The organization decides whether to build or buy a blockchain solution.
2. Next, the organization decides whether to host the blockchain solution on-premise or in the cloud. The options analysis in step #1 may affect step #2
3. Finally, the organization decides whether to use a permissioned or permissionless blockchain solution.

As the options analysis moves from step #1 to step #3, the organization will eventually refine the decision to one of the 8 cells. As an example, the options analysis may lead the organization to decide to buy a blockchain solution and host it on-premise. Next, the options analysis; may lead the organization to decide to use a permissioned blockchain.

Decision Matrix using Three Key Modalities for a Blockchain Solution

	Build		Buy	
	Permissioned	Permissionless	Permissioned	Permissionless
On-premise				
Cloud				

Annex C

Blockchain Implementation Risk and Audit Considerations

The organization can use the questions in Annex C to assess the strategic, design, implementation, and operational risks of a blockchain implementation and to develop an approach for auditing the blockchain solution.
The purpose of this worksheet is to provide a "forward-looking" checklist and risk analysis tool. Once an organization decides to use a blockchain solution, the organization can use the worksheet to analyze key design, implementation, and operational risks. The steps to use the worksheet are:

1. The organization analyzes all seven (7) design risks, noting that some design risks are more significant than others. This will depend on each organization's environment and requirements. The organization will assess more carefully the significant design risks versus the less significant design risks.
2. Next, the organization analyzes all 40 implementation risks. For the significant design risks identified in step #1, the organization will assess its implementation risks more carefully and thoroughly. Within these implementation risks, some of them might be more significant than others.
3. Finally, the organization analyzes all operational risks. For the one or more significant design and implementation risks identified in step #1 and step #2, the organization performs a "deep dive" analysis of their operational risks. Similar to above, some operational risks might be more significant than others.

As the risk analysis moves from analyzing higher-level design risks to lower-level operational risks, the worksheet will help the organization "zero in" and identify "unknow know" risks and convert them into "know know" risks. As an example, the risk analysis may lead the organization to identify design risk's impact on the organization's reputation as significant, and the implementation risk of smart contact as the most significant. Next, for smart contracts, the operational risk of knowing the legal limits within a jurisdiction is the most significant.

Blockchain Solution Risk Assessment Considerations					Blockchain Solution Audit Considerations				
Design Risks	Implementation Risks	Operational Risks	Risk Priority (i.e. H, M, L, NA)	Risk Assigned To (team member)	Audit Objective (i.e. purpose and desired results to manage the risk)	Audit Controls (i.e. monitoring, measuring, procedural, etc.)	Audit Type (i.e. automated, manual, physical, 3rd party, etc.)	Audit Classification (i.e. preventive, corrective, etc.)	Audit Frequency (i.e. monthly, quarterly, annually, etc.)
Governance	**Records Management**	-Do you have electronic records of the mission-critical digital assets? -Do you have a large volume of digital content (structure and unstructured) that needs to be managed? -Do you need to classify your digital assets that will be stored on the blockchain? -Do you currently classify your digital assets? -Do you require long-term preservation of your digital assets? -Do you plan to monetize your digital assets such as a subscription-based service? -Do you need to validate information from off chain sources before hashing the information to the blockchain?							
	Compliance and Reporting	-Do you have an authoritative source for your digital assets? -Do you have specific blockchain audit requirements for the transaction records in order to be compliant? -Do your third parties need to comply with the same or similar regulations? -Do you need to have access to the third party's digital content in order to validate compliance? -Do you need to establish provenance of the off chain information before hashing the information to the blockchain?							
	Senior Management Oversight	-Does your board have knowledge and experience to provide pro-active oversight for the DLT initiative using a blockchain solution? -Does your board have access to expert opinions to provide information for the DTL using a blockchain solution?							
	Business Impact Assessment (BIA)	-Do you need to store all of you digital content or just the mission-critical digital assets on the blockchain? -Do you have specific recovery time objectives (RTO) and recovery point objectives (RPO) for the blockchain infrastructure? -Do you have "buy-in" from board and / or management level committees for the BIA report?							

Blockchain Solution Risk Assessment Considerations					Blockchain Solution Audit Considerations				
Design Risks	Implementation Risks	Operational Risks	Risk Priority (i.e. H, M, L, NA)	Risk Assigned To (team member)	Audit Objective (i.e. purpose and desired results to manage the risk)	Audit Controls (i.e. monitoring, measuring, procedural, etc.)	Audit Type (i.e. automated, manual, physical, 3rd party, etc.)	Audit Classification (i.e. preventive, corrective, etc.)	Audit Frequency (i.e. monthly, quarterly, annually, etc.)
Operational Structure	**Transaction Fees**	-Do you want to reduce your transaction cost but not use third parties? -Do you need to reduce your unit transaction ?							
	Liquidity	-Do you have a plan to resolve disputes and counterparty risks without intermediaries to take on liquidity risks? -Do you have a plan to resolve financial transaction disputes that cross jurisdictional boundaries without intermediaries?							
	Business Continuity	-Do you manage digital assets that are critical to your operations? -Do you require high availability and recoverability of your blockchain infrastructure? -Do you have "buy-in" from board and / or management level committees for the business continuity plan and / or disaster recovery plan?							
	Operational Resiliency	-Do you have specific requirements to confirm that the blockchain infrastructure will continue to operate after a security breach, other specific types of failures -Do have specific projections or forecasts for the increase or sudden spikes in transaction volumes, etc.?							
	Intermediaries	-Do you work with third parties that act as "middlemen" to complete the transaction? -Do you partner with other organizations to run your business? -Do you need to work with a trusted third party to complete the transaction? -Do you need multiple third parties to verify and validate transactions? -Do you need one or more the third parties to be anonymous to one another?							
	Management Committees	-Does your management committee have board-level support for the DTL using a blockchain solution? -Does management committed have senior-level participation to monitor and manage pro-actively the risks and issues?							

Blockchain Solution Risk Assessment Considerations					Blockchain Solution Audit Considerations				
Design Risks	Implementation Risks	Operational Risks	Risk Priority (i.e. H, M, L, NA)	Risk Assigned To (team member)	Audit Objective (i.e. purpose and desired results to manage the risk)	Audit Controls (i.e. monitoring, measuring, procedural, etc.)	Audit Type (i.e. automated, manual, physical, 3rd party, etc.)	Audit Classification (i.e. preventive, corrective, etc.)	Audit Frequency (i.e. monthly, quarterly, annually, etc.)
Reputation	**Privacy**	-Do you have "buy-in" from board and / or management level committees for the privacy impact assessment of sensitive information that will be stored on the blockchain? -Do you have a plan to address privacy issues when using a permissionless blockchain?							
	Smart Contracts	-Do you need to maintain the order in which buy and sell transaction were completed? -Do you know the legal limits of using smart contracts in the jurisdictions that you are operating within?							
	Legal Liability	-Do you need to provide transparency to your transaction information and digital content? -Do you know the liabilities of using permissioned and / or permissionless blockchains in the jurisdictions that you are operating within? -Do you need liability insurance that is specific to using a blockchain solution?							
	Contract Enforcement	-Do you need to manage contracts in the blockchain or off chain in order to stay compliant? -Do you know the jurisdictional limits when managing contract on the blockchain?							
	Threat Risk Assessment (TRA)	-Do you have a prioritized list of quantitative and qualitative risks and corresponding risk management strategies? -Do you have "buy-in" from board and / or management level committee for the TRA report? -Do you have a crisis management plan to respond to failures when using the blockchain solution?							

Blockchain Solution Risk Assessment Considerations					Blockchain Solution Audit Considerations				
Design Risks	Implementation Risks	Operational Risks	Risk Priority (i.e. H, M, L, NA)	Risk Assigned To (team member)	Audit Objective (i.e. purpose and desired results to manage the risk)	Audit Controls (i.e. monitoring, measuring, procedural, etc.)	Audit Type (i.e. automated, manual, physical, 3rd party, etc.)	Audit Classification (i.e. preventive, corrective, etc.)	Audit Frequency (i.e. monthly, quarterly, annually, etc.)
Blockchain Architecture	**Permissioned versus permissionless**	-Do you need to use a permissionless or permissioned blockchain solution? -Does the permissionless blockchain solution have capacity to "scale up" as transaction volumes increase?							
	On-premise versus cloud-based	-Do you have resources, skills, and experience to manage on-premise blockchain infrastructure? -Do you need to have the blockchain infrastructure on-premise, cloud-based, or hybrid?							
	Blockchain as a Service (BaaS) versus Proprietary	-Do you need an enterprise-wide blockchain only for internal use? -Do you have one more or use cases that fit a BasS solution?							
	Consensus Protocol	-Do you know which consensus mechanism is appropriate for the blockchain solution? -Do you need to consider whether a Proof of Work (PoW) or Delegated Proof of Stake (DPoS) consensus algorithm can handle large volumes of transactions? -Do you need to consider a whether DPoS consensus algorithm can delay or prevent completing the transfer for value?								
	Mining Architecture	-Do you expect the volume of digital content to increase rapidly? -Do you need to support a high volume of transaction? -Do you require hybrid architecture where some nodes are off-premise? -Do you require nodes to be distributed, but not decentralized?							

Blockchain Solution Risk Assessment Considerations					Blockchain Solution Audit Considerations				
Design Risks	Implementation Risks	Operational Risks	Risk Priority (i.e. H, M, L, NA)	Risk Assigned To (team member)	Audit Objective (i.e. purpose and desired results to manage the risk)	Audit Controls (i.e. monitoring, measuring, procedural, etc.)	Audit Type (i.e. automated, manual, physical, 3rd party, etc.)	Audit Classification (i.e. preventive, corrective, etc.)	Audit Frequency (i.e. monthly, quarterly, annually, etc.)
Legislation and Regulations	**Customer Information**	-Do you need to manage and secure commercially sensitive digital information on the blockchain platform?							
	Personal Information	-Do you need manage and secure personally identifiable information (PII) on the blockchain platform? -Do you need to remove information from the blockchain to comply with legislation and regulations?							
	Health Information	-Do you need to manage and secure personal health information (PHI) on the blockchain platform?							
	Data Residency	-Do you know all of the jurisdictional constraints if you use BaaS? -Do you have specific data residency restrictions to consider if you use BaaS?							
	Anti-Money Laundering	-Do you know how to identify suspicious financial transactions when using a permissionless blockchain? -Do you have a process in place to know your customer (KYC) when using a blockchain solution? -Do you have a plan to comply with anti-money laundering (AML) regulations when using a blockchain solution?							

Blockchain Solution Risk Assessment Considerations					Blockchain Solution Audit Considerations				
Design Risks	Implementation Risks	Operational Risks	Risk Priority (i.e. H, M, L, NA)	Risk Assigned To (team member)	Audit Objective (i.e. purpose and desired results to manage the risk)	Audit Controls (i.e. monitoring, measuring, procedural, etc.)	Audit Type (i.e. automated, manual, physical, 3rd party, etc.)	Audit Classification (i.e. preventive, corrective, etc.)	Audit Frequency (i.e. monthly, quarterly, annually, etc.)
IT Operations and Network Security	**Identity Management**	-Do you need to validate the participant's identity before confirming the transaction?							
	Key Management and Loss Prevention	-Do you have processes and technology tools that will ensure the security of private keys and wallets? -Do you have processes to manage the loss or theft of private keys? -Do you have a plan to manage hot and cold storage of private keys?							
	Chain Defense	-Do you have a response plan in the case when a hacker takes control of 51% of the notes on the network? -Do you have security information and event management (SIEM) software and hardware tools specifically to monitor the nodes on the blockchain network for vulnerabilities, intrusion detection, DDoS attacks, etc.?							
	Cryptography	-Do you have the requirements to evaluate the different cryptography protocols used by the nodes on the network to arrive at a consensus to update the DLT? -Do you know which consensus mechanism is appropriate for the blockchain solution?							
	Tokenization	-Do you have the requirements to evaluate the different tokens that might be used on the permissionless blockchain network? -Do you know the underlying value of item the token will represent? -Do you know which consensus mechanism is appropriate for the blockchain solution?							
	Data Management	-Do you need to secure off chain data by encrypting it databases? -Do you need to encrypt data when it is in transit to / form the blockchain to off chain storage?							
	Development and Operations (DevOps)	-Do you have Service Level Agreements that specifically address the blockchain solution? -Do you have skilled resources to develop and maintain and proprietary and on-premise blockchain solution?							
	Performance and Scalability	-Do you need the blockchain solution to scale up quickly during peak periods? -Do you require 24/7 availability even during a disaster recovery situation?							
	Off chain Information Inter-operability	-Do you need to manage and integrate digital information that is off chain? -Do you need provide regulatory reports regarding information that is stored the blockchain and off chain?							

Blockchain Solution Risk Assessment Considerations					Blockchain Solution Audit Considerations				
Design Risks	Implementation Risks	Operational Risks	Risk Priority (i.e. H, M, L, NA)	Risk Assigned To (team member)	Audit Objective (i.e. purpose and desired results to manage the risk)	Audit Controls (i.e. monitoring, measuring, procedural, etc.)	Audit Type (i.e. automated, manual, physical, 3rd party, etc.)	Audit Classification (i.e. preventive, corrective, etc.)	Audit Frequency (i.e. monthly, quarterly, annually, etc.)
Project Planning	**Business Objectives**	-Does the blockchain solution align with the strategic objectives?							
	Business Case	-Do you have "buy-in" from all key stakeholders to approve the selection option? -Do you have "buy-in" from board and / or management level committees for the business case?							
	Project Governance Framework	-Does the project steering committee have pro-active participation from business team's management?							
	Communications and Change Management	-Do you need a communications and change management plan that is designed specifically for the blockchain solution that the board and / or management committee approved?							
	Scope Management	-Do you have "buy-in" from board and / or management level committees for the scope of the blockchain solution?							
	Request for Proposal	-Do you need to issue an RFP to for the blockchain solution approved in the business case?							
	Business User Training and Support	-Do you need to develop a training plan and on-going support plan that is designed specifically for the blockchain solution that the board and / or management committee approved?							
	Quality Management and Testing	-Do you need to develop a quality management plan that is designed specifically for the blockchain solution that the board and / or management committee approved?							

Bibliography/References

Blockchain and the Internet of Things: the IoT blockchain opportunity and challenge, i-Scoop, online at: https://www.i-scoop.eu/blockchain-distributed-ledger-technology/blockchain-iot/ (last accessed April 11, 2019)

Bryanov, Kirill. (2019, March 18). Denver Municipal Election: Another Small Stop on the Road to Universal Blockchain Voting, CoinTelegraph, online at: https://cointelegraph.com/news/denver-municipal-election-another-small-stop-on-the-road-to-universal-blockchain-voting (last accessed August 8, 2019)

Compton, Jason, How Blockchain Could Revolutionize The Internet of Things, Forbes, June 27, 2017, online at: https://www.forbes.com/sites/delltechnologies/2017/06/27/how-blockchain-could-revolutionize-the-internet-of-things/#544796c76eab (last accessed April 11, 2019)

DeMarinis, Richard, et. Al., Nasdaq, Is Blockchain the Answer to E-Voting? NASDAQ Believes so, 2017, online at: https://business.nasdaq.com/marketinsite/2017/Is-Blockchain-the-Answer-to-E-voting-Nasdaq-Believes-So.html (last accessed August 7, 2019)

Dunietz, Jesse, Scientific American, Are Blockchains the Answer for Secure Elections? Probably not, August 15, 2018, online at: https://www.scientificamerican.com/article/are-blockchains-the-answer-for-secure-elections-probably-not/ (last accessed April 11, 2019)

Edelman. (2019). 2019 Edelman Trust Barometer: Global Report, *Edelman*, available online at https://www.edelman.com/sites/g/files/aatuss191/files/2019-02/2019_Edelman_Trust_Barometer_Global_Report.pdf (accessed August 8, 2019)

Elanj, Saeed. (2019, January 29). What does blockchain's future look like following Bitcoin's disastrous 2018?," Forbes Technology Council [Blog}. Available online at: https://www.forbes.com/sites/forbestechcouncil/2019/01/29/what-does-blockchains-future-look-like-following-bitcoins-disastrous-2018/#769c1dbd604a (last accessed August 7, 2019)

FINRA. "Distributed Ledger Technology: Implications of Blockchain for the Securities Industry1," Report on Distributed Ledger Technology | January 2017, online https://drive.google.com/file/d/1P2w_-YJONoeC_HuQkn25elwn6jfG8tvE/view (last accessed April 16, 2019).

Franks, Patricia C, Doyle, Allen, and Morrison, Jane. (2016, May 17). Retention and Disposition in a Cloud Environment, [InterPARES Trust Report]. Available online at https://interparestrust.org/assets/public/dissemination/NA06_20160902_RetentionDispositionInCloud_FinalReport_Final.pdf (last accessed April 11, 2019)

Gartner. (2019). Information Governance. *IT Glossary*. Retrieved March 24, 2019, from https://www.gartner.com/it-glossary/information-governance/ (last accessed August 7, 2019)

Gopie, Nigel, PhD, What are smart contracts on blockchain?, July 2, 2018, online at: https://www.ibm.com/blogs/blockchain/2018/07/what-are-smart-contracts-on-blockchain/, (last accessed April 11, 2019)

Guest Writer, Can Blockchain Provide a Secure Platform for M2M Transactions?, iot for all, February 27, 2019, online at: https://www.iotforall.com/can-blockchain-provide-secure-platform-for-m2m-transactions/ (last accessed April 11, 2019)

Higgins, S. (2016, January 20). Vermont Says Blockchain Record-Keeping System Too Costly. CoinDesk. Retrieved April 4, 2019, from https://www.coindesk.com/report-blockchain-record-keeping-system-too-costly-for-vermont (last accessed August 7, 2019)

HOW 2050. Global agriculture towards 2050, High-Level Expert Forum, , p. 1, Rome, October 12-13, 2009, online at: http://www.fao.org/fileadmin/templates/wsfs/docs/Issues_papers/HLEF2050_Global_Agriculture.pdf (last accessed August 7, 2019)

InterPARES Glossary 2018, online at: https://www.interpares.org/ip2/ip2_terminology_db.cfm, (last accessed April 11, 2019)

InterPARES 2, online at: https://www.interpares.org/ip2/ip2_index.cfm, (last accessed April 11, 2019)

Investopedia, 2018, online at: https://www.investopedia.com, (last accessed April 11, 2019)

I-trust Terminology Project, online at: https://www.interparestrust.org/terminology, (last accessed

ISO/IEC 29100, *Information technology – Security techniques – Privacy framework*

ISO 15489-1:2016*, Information and documentation—Records management, Part I: Concepts and principles.*

ISO 16484-5:2017, *Building automation and control systems (BACS) – Part 5: Data communication protocol*

ISO/DTR 23245*, Blockchain and distributed ledger technologies - Security risks, threats and vulnerabilities.*

Katz, Frances, The Week, *Can blockchain fix America's voting systems?*, online at: https://theweek.com/articles/762519/blockchain-fix-americas-voting-system (last accessed August 7, 2019)

Lemieux, V. L. (2016, October). *Blockchain Technology for Recordkeeping, Volume 1, Report*. SSHRC Knowledge Synthesis Grant, University of British Columbia. Retrieved April 5, 2019, from https://www.researchgate.net/profile/Victoria_Lemieux/publication/309414363_Blockchain_for_Recordkeeping_Help_or_Hype/links/580f539408ae009606bb62f6.pdf

MarketInsite. Is Blockchain the Answer to E-Voting? NASDAQ Believes So. MarketInsite, January 23, 2017, online at https://business.nasdaq.com/marketinsite/2017/Is-Blockchain-the-Answer-to-E-voting-Nasdaq-Believes-So.html (last accessed August 8, 2019)

McClelland, Calum, What is IoT? – A Simple Explanation of the Internet of Things, iot for all, January 6, 2019, online at: https://www.iotforall.com/what-is-iot-simple-explanation/ (last accessed August 7, 2019)

Mendling, Jan, et. Al., *Blockchains for Business Process Management – Challenges and Opportunities,* ACM Transactions on Management Information Systems, January 2018. Retrieved April 11, 2019, from: https://www.researchgate.net/publication/316076240_Blockchains_for_Business_Process_Management_-_Challenges_and_Opportunities

National Archives and Records Administration (NARA). (2019, February). *Blockchain Whitepaper*, online at https://www.archives.gov/files/records-mgmt/policy/nara-blockchain-whitepaper.pdf (last accessed November 13, 2019.

Nelson, P. (n.d.) Primer on Blockchain. *USAID*, p.7. Retrieved April 5, 2019, from https://www.usaid.gov/sites/default/files/documents/15396/USAID-Primer-Blockchain.pdf

NIST, Draft NIST Interagency Report (NISTIR) 8202: Blockchain Technology Overview, from: https://csrc.nist.gov/CSRC/media/Publications/nistir/8202/draft/documents/nistir8202-draft.pdf (last accessed August 7, 2019)

Penfield, S. (2017, December 15). A Practical Approach to Blockchain Analytics. SAS Blogs. Retrieved April 5, 2019,from https://blogs.sas.com/content/sascom/2017/12/15/practical-approach-blockchain-analytics/ (last accessed August 7, 2019)

Pew Research Center. (2019). Public Trust in Government: 1958-2019. Available online at: https://www.people-press.org/2019/04/11/public-trust-in-government-1958-2019/ (last accessed August 8, 2019)

Pollock, Darryn, Blockchain for Elections: Advantages, Cases, Challenges, May 17, 2018, Cointelegraph, online at: https://cointelegraph.com/news/blockchain-for-elections-advantages-cases-challenges (last accessed August 7, 2019)

Prentiss, T. (2018, June 24). UK National Archives Tests Using Blockchain for Historical Document Preservation. *ETH News*. Retrieved April 5, 2019, from https://www.ethnews.com/uk-national-archives-tests-using-blockchain-for-historical-document-preservation

Ray, Rachel, Smart Contracts 101: Unleashing the Power of Blockchain, October 1, 2018, Hackernoon.com, online at: https://hackernoon.com/smart-contracts-101-unleashing-the-power-of-blockchain-348a742d2a23 (last accessed August 7, 2019)

Rücker, Bernd, How blockchain can drastically simplify business processes, Berndruecker Blog, online at: https://blog.bernd-ruecker.com/how-blockchain-can-drastically-simplify-business-processes-cc0828918b85 (last accessed May 6, 2019)

Seidel, March-David L. (2018, January). "Questioning Centralized Organizations in a Time of Distributed Trust," *Journal of Management Inquiry*, 27(1), pp. 40-44. Available online at: https://journals.sagepub.com/doi/full/10.1177/1056492617734942 (last accessed August 7, 2019)

Srivastav, Amitabh. "Risk Management and Virtual Teams: An Exploratory Empirical Investigation of Relationships between Perceived Trust and the Perceived Risk of Using Virtual Project Teams." Thesis in Project Management, Université du Québec en Outaouais, 2014, p 39. Abstract available at *http://di.uqo.ca/id/eprint/719* (last accessed August 7, 2019)

Violino, Bob, ZDNET, Blockchain voting: Can it help secure our elections?, online at: https://www.zdnet.com/article/is-blockchain-voting-on-the-way/ (last accessed August 7, 2019)

Wikipedia, online at: https://www.wikipedia.org.

Wolf, Martin. (2019, February 13). "The Libertarian fantasies of cryptocurrencies," *Financial Review*. Retrieved March 24, 2019 from https://www.afr.com/news/world/the-libertarian-fantasies-of-cryptocurrencies-20190213-h1b6tm (last accessed August 7, 2019)

About 3D PDF Consortium

The 3D PDF Consortium is a community of end user companies, software developers, and system integrators who are passionately dedicated to 3D ubiquity and are working together to make that a reality.

The 3D PDF Consortium is the administrator of the U.S Technical Advisory Group (TAG) to ISO/TC171, Document management applications, SC2, Document file formats, EDMS systems and authenticity of information. On behalf of the American National Standards Institute (ANSI), the 3D PDF Consortium is the committee manager for ISO/TC171/SC2.

The 3D PDF Consortium is a non-profit organization that works with its members to develop the necessary technical resources to assist in fostering implementation of 3D PDF and PDF, represents the overall requirements with participation in the international standards processes, and generate awareness of the opportunities for 3D PDF and PDF to deliver dramatic business benefits. Visit us at www.3dpdfconsortium.org.

About White Paper Development/Approval Process

This document was developed by a voluntary committee of subject experts. Upon completion, the draft document was reviewed and vetted with a group of peer reviewers and the Standards Board, an oversight committee for the Standards Program. For approval, the document obtained more than a simple majority vote favoring the publication and release of the document. All objections and comments received on the draft were discussed by the committee prior to approving the document. This document will be reviewed upon its 3-year publication anniversary and revised as necessary.

At the time this report was approved, the Standards Board of the 3D PDF Consortium had the following members:

Member	**Company/Organization**
Stephen Levenson, Chair	
Owen Ambur	
Robert Blatt	EID, Inc.
Kevin DeVorsey	NARA
Matthew Hardy	Adobe
Donna Johnston	Sutter County Clerk – Recorder
Rick Laxman	Church of Jesus Christ of Latter-Day Saints
Lisa Sisco	Sisco Records
Phil Spreier	3D PDF Consortium

This report was approved by the ECM Standards Working Group x, name. At the time this report was approved, the ECM Standards Working Group 2, Trustworthy Document Management Integrity and Assessment Technologies and Practices, had the following members:

This report was drafted and approved by the ECM Standards Blockchain Committee. At the time this report was drafted and approved, the ECM Standards Blockchain Committee had the following members:

Member	**Company/Organization**
Patricia Franks, Chair*	San Jose State University
Abigail Bonk	
William Borici	Suanpan Solutions
Bill Corey*	University of Virginia (Library)
Corro'll Driskell	Xclients Technology, LC
Terri Jackson*	Jackson Beggs Limited
Anthony Johnson	
Donna Johnston	Sutter County Clerk – Recorder
Piergiorgio Lucidi	Apache Software Foundation
Elizabeth Mariani*	
Regina Marjani*	USAC
Norman Mooradian*	
David Simmons	
Amitabh Srivastav*	Helux
Edward Sumcad*	LA County Records Management & Archiving
Cassandra Taylor-Wilson	
Jennifer Topping*	

*Denotes author and editing contributions to the paper.

