BLOCKCHAIN RECORDKEEPING: A SWOT ANALYSIS

Blockchain and distributed ledger technology promise to deliver trusted and immutable records in a wide variety of use cases. In a relatively short time, it has become the innovation to watch, according to just about every technology research and advisory firm, global consultancy, and international think tank. Is this just hype, or will this technology really deliver?

Victoria L. Lemieux, Ph.D., CISSP

Blockchain – which is a type of distributed ledger technology in which confirmed and validated sets of transaction records are held in blocks that are chained together – is meant to make records of these transactions immutable.

While this emerging technology is already transforming the recordkeeping landscape in health care, real estate, and financial services, to name but a few sectors, many organizations are just considering its use. This article explains the technology and describes its promises, perils, and future in a way that will help information professionals provide their organizations sound advice about its potential for their business.

How Blockchain Works

As described in *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction,* each chain starts with an original, or genesis, block, followed by a time-ordered sequence of blocks. Blocks are chained together cryptographically using *hashes*, which are 256-bit random numbers computationally generated from input information. This forms a long, continuous chain of hashes – hence the name *blockchain* (see Figure 1).

Validation

Each blockchain has a consensus mechanism that ensures that updates are agreed to and communicated transparently across the entire network, so the order in which transaction records enter the blockchain is undisputed, and any changes to what has been written to the ledger will be detectable.

Distribution

Once validated using the consensus mechanism, blocks are broadcast through a distributed peer-to-peer mesh network of nodes (see Figure 2); the nodes, in theory, are unlimited in number and can operate from any location. Each node usually retains a complete copy of the ledger (though some retain only a partial copy), and the copies on each node should match exactly. When the information on one or more of the nodes does not match, that node is no longer considered to have valid information.

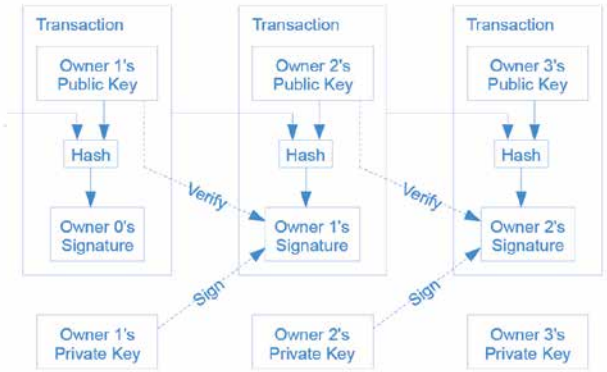


Figure 1. Blockchain structure (Source: *Bitcoin:* "A Peer-to-Peer Electronic Cash System," Nakamoto, 2008).

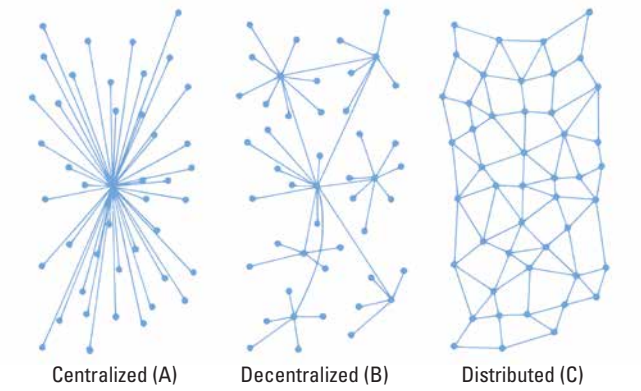


Figure 2. Three kinds of networks

Transactions

When individuals want to make a transaction on a blockchain network, such as to transfer ownership of property, they transfer control of the asset by transferring the blockchain representation of it (sometimes called a *token*) from their blockchain address to the other person's blockchain address. An address is denoted by the hash of a public key – a hash that functions somewhat like a zip code by indicating the destination of a particular transfer of value. For each public key, there is a matched private key. The individual uses the private key to digitally sign the transaction (see Figure 3) to make the transfer of ownership happen.

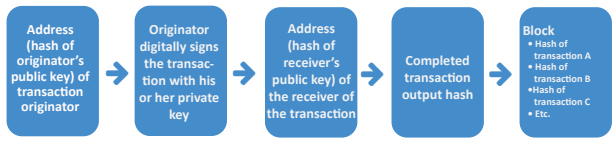


Figure 3. Transaction processing using public-private key pairs on the blockchain

Decentralized Blockchains

In addition to being distributed, some blockchains (such as public blockchains) operate as decentralized systems – that is, their nodes do not operate under the control of a centralized server, but in a fully independent, albeit coordinated, manner.

These blockchains may also be characterized by decentralized governance; in other words, they may not operate under the formal authority of a single person or organization, even though groups of individuals or organizations may wield informal control over their operation, as noted in "The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk" in *Legislation and Public Policy 18*. Examples of these types of blockchains include Bitcoin and Ethereum.

Other blockchains operate under the control of a single authority such as Ripple, which connects banks, payment providers, and others, or under the authority of a consortium such as R3, which leads more than 70 large financial institutions in developing blockchain use in the financial services industry.

Public/Private, Permissioned/Permissionless

As spelled out by I.C. Lin and T.C. Liao in "A Survey of Blockchain Security Issues and Challenges" in *IJ Network Security 19[5], public* blockchains are those that any participant may use and access. They are often *permissionless*; participants do not require special authorization or authentication to access, read, write, and participate in transactions and in the consensus process.

Permissioned blockchains, on the other hand, are ones in which nodes must have a member identity, and participants must have authority and authentication to access them. These are often *private blockchains*, meant only for the use of members of a shared ledger – a single ledger that multiple participants may access and use. Permissioned blockchains have membership services that manage the identity, privacy, confidentiality, and auditability within the system.

Blockchain in Recordkeeping

It is tempting to think of blockchains only in terms of cryptocurrency, like Bitcoin. The use of blockchain technology for other cases is growing rapidly, including for recordkeeping.

According to the article "Georgia Expands Project to Secure Land Titles on the Bitcoin Blockchain" in *Cryptocoin News,* the Republic of Georgia piloted the registration of land titles using a private blockchain in 2016. The article said there are plans to expand the service to sales of land titles, mortgages, rentals, new land title registration, property demolition, and notary services.

The Swedish land registry authority, Lantmäteriet, has been testing a way to record property transactions on a blockchain, as described in "The Land Registry in the Blockchain – Testbed," a 2017 report from the Lantmäteriet and others.

A pilot for applying blockchain technology to land transfer registration in the municipality of Pelotas in Brazil has recently been launched by the local real estate registration authority, according to Garrett Keirns' August 2017 "Blockchain Land Registry Tech Gets Test in Brazil" in *CoinDesk*.

Recording of land transactions is by no means the only recordkeeping use case. According to the University of British Columbia's unpublished 2017 "Records in the Chain" project report, Estonia is one of many jurisdictions that use blockchain to securely keep medical records and a host of other types of government records.

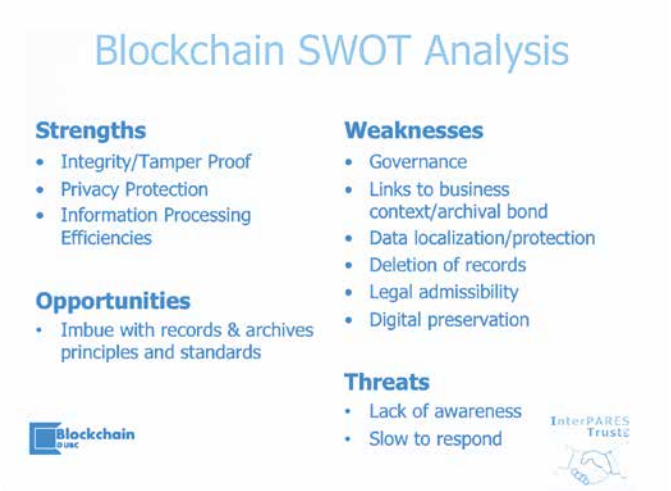


Figure 4: Overview of blockchain recordkeeping SWOT analysis

Blockchain in Recordkeeping: SWOT Analysis

With the use of blockchain for recordkeeping growing, information professionals must know how to determine the benefits and risks of its use. The "Records in the Chain" project mentioned above is reviewing blockchain recordkeeping solutions around the world and has identified the following strengths, weaknesses, opportunities, and threats (SWOT).

Strength: Detects Alterations

A key strength of blockchain technology is that it helps ensure the integrity of records through the way transactions are recorded and validated. For example, in Bitcoin it is through solving a cryptographic puzzle that permits detection of any alteration to transaction records after they have been validated.

In another example, the Government of Estonia's e-Health database uses Guardtime's keyless signature infrastructure solution to capture hashes of data to ensure that any changes to, or tampering with, the medical records of Estonian citizens can be detected.

Strength: Protects Privacy

Blockchain recordkeeping solutions might also enable better privacy protection for citizens and governments by enabling more individual control over their personal data. With blockchain technology, they can determine who can access their data, for what purpose, and for how long.

The Respect Network – a personal data network (*respectnetwork.com*) with a vision of having members feel a sense of privacy and security when they share information – proposes to use XDI, an OASIS standard for semantic data interchange, to produce *smart contracts* with blockchain-based digital signatures to establish

As as an information management veteran, you likely can name someone who was particularly instrumental in your professional growth. Now it's your turn to pay it forward – and we're here to help you make a connection for sharing your knowledge and expertise.

ALLOW US TO INTRODUCE YOU!

The recently launched ARMA International mentorship program has attracted many people who are eager for professional guidance, and we need you to sign up at ***surveymonkey.com/r/ARMAMentorship*** so we can make a match that will help ensure their success. Though the commitment is minimal, it can change careers!

For more details, see ***http://discoverarma.org/mentorship*** and the mentor FAQs at ***http://discoverarma.org/mentorFAQ.***

commitments about private data use that are "well-defined, non-abstract and non-repudiable, and enforceable between individuals, corporations and governments." (See sidebar "Blockchain Applications and Services" for more about smart contracts.)

In the United Kingdom, Mydex and the Qiy Foundation (*https://www.qiyfoundation.org/about-qiy/*) offer a model similar to the Respect Network's, aiming to enable individuals to exchange information privately and securely.

Strength: Increases Efficiency

Additionally, blockchain technology can deliver significant information processing efficiencies. This capability is what financial services firms are most excited about. Through enabling peer-to-peer "trustless" trade reconciliation and settlement, for example, financial institutions can shave millions off the cost of operation.

Rather than having to run large back-office operations where staff reconcile trade confirmations, counterparties can make and settle trades instantaneously on the blockchain, cutting out the need for back-office operations. Other sectors are exploring ways to reduce inefficiencies in information processing through the application of blockchain technology.

Weakness: Lacks Sufficient Control

Even though protecting the integrity of records and detecting when integrity has been breached are strengths of blockchain technology, it is not inconceivable for a validated transaction to be overturned after the fact by a government or group of individuals in control of a blockchain.

In theory, public blockchains are decentralized and self-governing, but in practice their operation is often in the hands of a core group of developers. If organizations intend to rely on blockchain-based recordkeeping, they must consider the effect on the integrity of records.

Given the uncertainty of relying on public blockchains over which it may be virtually impossible to exercise control, many organizations are turning to private, permissioned blockchains where governance is the responsibility of a single body or consortium of bodies. This does not eliminate threats to the integrity of blockchain records presented by hard forks or forced editing of the ledger, but it does present the possibility to establish rules of operation and procedures for any changes to what is intended to be an immutable record.

The downside of using private, permissioned ledgers, on the other hand, is that organizations need to trust that the body or group of bodies responsible for the operation of the blockchain will do so in a manner that does not affect the authenticity, integrity, or long-term availability of the records. Organizations likely will have to resort to traditional legal contracts for such assurances, and, moreover, will need to look carefully at the track record of the service provider.

Blockchain Applications and Services

There are also applications and services associated with blockchains and distributed ledgers that add to their usefulness for recordkeeping. These include blockchain applications that run over blockchain networks and permit participants to easily interact with these networks.

Smart Contracts

According to Nick Szabo in his "The Idea of Smart Contracts," *smart contracts* are blockchain applications that express business logic associated with a transaction and execute on a blockchain platform. Smart contract code determines what transactions are recorded into the blockchain and the information they will contain. Through the use of smart contracts, many kinds of contractual clauses may be made partially or fully self-executing and self-enforcing.

Oracles provide a trusted service designed to supply external data to a smart contract or blockchain system. Asset registries link digital currencies to other assets or records on top of a distributed ledger, according to InterPARES Trust Terminology Project: "Key Blockchain Terms and Definitions."

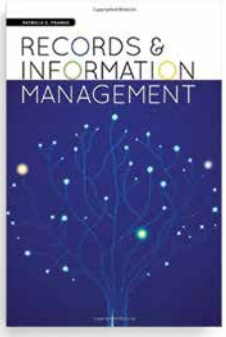
Off-Chain Services

Off-chain services provide secure means to access capabilities outside a blockchain system, such as trusted data sources or functions. *Sidechains* are physically separate blockchains associated with a main blockchain, and they can participate in transactions with it, typically in both directions.

In contrast, *subchains* are logically separate chains that form part of a blockchain. Each subchain may be owned by a different entity and may be accessible to a different set of users. Nodes may be set up so that some nodes participate in certain subchains and not in others. The result of this configuration is that the ledger on some nodes contains transactions for that subchain while the ledgers on other nodes do not.

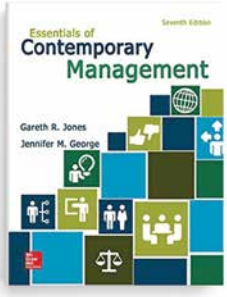
The New CRM Study Pack

The ICRM Exam Development Committee recommends these books as preparation resources for the CRM exam.



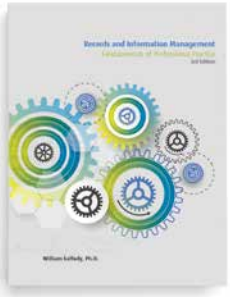
Records and Information Management

Patricia L. Franks, Ph.D., IGP, CRM, CA, FAI



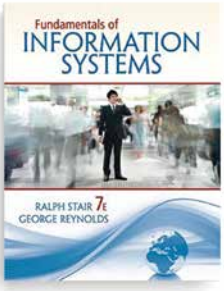
Essentials of Contemporary Management, 7th Ed.

Gareth R. Jones
Jennifer M. George



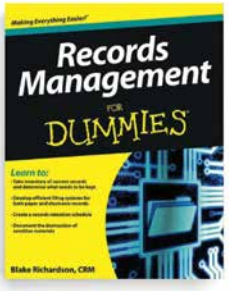
Records and Information Management: Fundamentals of Professional Practice, 3rd Ed.

William Saffady, Ph. D.



Fundamentals of Information Systems, 7th Ed.

Ralph Stair
George Reynolds



Records Management for Dummies

Blake Richardson, CRM

Members Save 20% Off the Cover Prices

(when purchased together)

Order online today at ***www.arma.org/bookstore*** ARMA INTERNATIONAL BOOKSTORE

Weakness: Doesn't Link Records to Business Context

Another weakness in most blockchain solutions is the absence of a mechanism to link records on the chain back to the business context of their creation. This may make it difficult to rely on blockchain records as evidence of business transactions.

Consider a blockchain solution, like those piloted in Sweden and Brazil, in which land transfer records have been recorded on a public blockchain along with millions of other transactions. How would it be possible to retrieve the hash recorded on the blockchain associated with a specific land title unless there is a means of linking the transaction with its business context? How would it be possible to comply with e-discovery orders?

In the case of the Swedish and Brazil land transaction recording pilots, the problem is solved by using "colored coins" – blockchain transactions specially annotated with metadata that links them back to the transaction to which they relate. As these pilots demonstrate, it is possible to establish the bond between records on the chain and their business context using hash pointers "on chain" to metadata or registers stored "off chain," but not without careful solution design that pays attention to this important recordkeeping requirement.

"Breaking open the MtGox case, part I" in a July 2017 WizSEC blog post.

Weakness: May Violate Data Laws

Data localization laws may stem from laws and rules requiring retention of documents at a business premises or from laws that address data protection and privacy in relation to technology. In the European context, an example is the incoming General Data Protection Regulation (GDPR), which has requirements for processing personally identifiable information (PII).

For countries relying on storing elements of their public records on any blockchain not operating entirely within their sovereign jurisdiction, it is necessary to consider if the system complies with data localization, data protection, and privacy laws and rules.

In the case of the Brazilian pilot, for example, the platform's metadata files contain details of property transfers that are kept on a Colu server in Israel. Although there are no laws or rules that preclude this architecture, the company that built the Brazilian pilot system, Ubitquity, is looking at providers in Brazil to ensure adherence to good practice with data handling and in anticipation of possible data localization requirements.

Laws and regulations governing the admissibility and weight to be given such evidence differ according to jurisdiction, and thus it is difficult to generalize...

Weakness: Admissibility as Evidence Is Uncertain

With the potential for more records to be created natively on chain using smart contracts, attention must also be given to the question of legal admissibility. Although proponents of smart contracts and blockchain technology envision a future where contracts code is law, it is unlikely the need for dispute mechanisms, such as courts, will be eliminated, at least in the near term.

It is, therefore, important to consider the issue of legal admissibility and weight of information recorded and stored on the blockchain. Laws and regulations governing the admissibility and weight to be given such evidence differ according to jurisdiction, and thus it is difficult to generalize about how such evidence might be treated by the courts, beyond saying that uncertainty prevails.

Existing laws must be interpreted to apply to these emerging forms of records until jurisdictions change laws and regulations explicitly to address the admissibility and weight of blockchain records. In the meantime, information professionals may draw insights, if not legal precedent, from those few cases that consider this type of evidence. A recent case is the U.S. grand jury indictment in July of Alexander Vinnik in a $4 billion bitcoin laundering scheme that also linked him to the 2014 collapse of Japan-based bitcoin exchange Mt. Gox. For details, see

In some jurisdictions, privacy laws, such as the GDPR, require protection of PII. Norms for public availability of PII about land holders should follow what is prescribed by any relevant laws. For solutions that affix metadata to transactions recorded on a public blockchain, consideration should be given to encrypting metadata to protect the privacy of transacting parties to comply with good practice and legal requirements.

Weakness: Disposition Is Difficult

"Right to be forgotten" provisions may also need to be followed, which can be problematic when blockchain records are meant to be immutable, not editable. This raises the larger issue of how to delete records from blockchains, which is also a consideration for implementing records retention policies or correcting inaccuracies in the record.

Some organizations have proposed "editable" blockchains, but this flies in the face of the primary value proposition of blockchain recordkeeping – immutability. Information professionals may look to techniques used for managing write-once-read-many storage for guidance, including the segregation of blockchains into channels according to retention requirements so that entire sub-chains can be deleted if need be when the time

comes –a sort of blockchain "big bucket" approach.

Another approach is to delete the "off chain" records to which "on chain" pointers point, but this approach may not be practical for many organizations, and so the question of how to handle deletion of blockchain records remains open.

The InterPARES TRUSTER Project is investigating how to extend the guarantee of authenticity for digital records by replacing traditional digital signatures, which rely on digital certificates issued by a trusted certificate authority, with blockchain-based digital signatures that have no need of trusted third parties or digital certificates. And there are many other possibilities to consider.

It is generally assumed that lots of copies available on participating, distributed nodes will keep blockchain records safe and accessible over the long term…

Weakness: Long-Term Preservation Is Challenging

The question of how to preserve blockchain records over the long term is still an open one as well. Traditional approaches to digital preservation rely on centralized repositories operated by archival institutions. Will these approaches translate to decentralized recordkeeping?

It is generally assumed that lots of copies available on participating, distributed nodes will keep blockchain records safe and accessible over the long term, but what happens when the operator of a privately operated blockchain disappears? Or when nodes on a public blockchain no longer have an incentive to keep validating transactions? Who would be responsible for identifying the whereabouts of all the copies? How many copies would be needed to ensure continued trust in the records? And, who would be responsible for maintaining these nodes, and how? There are no clear answers yet.

Opportunity: To Be a Trusted Advisor

As more and more organizations begin to see the value of blockchain-based recordkeeping, there exists a major opportunity for information professionals to advise their organizations on its use. To take advantage of the opportunity, however, they must bring themselves up to speed on how blockchain technologies operate, how they are used in recordkeeping, and how to ensure the application of these technologies adheres to global recordkeeping standards and professional principles.

The Blockchain Education Network offers a wide selection of online resources information professionals can draw upon to build their knowledge. Those who fail to update their technical knowledge may find themselves identified with outmoded paper or centralized recordkeeping paradigms and therefore be sidelined.

Opportunity: To Innovate Professional Practice

Just as blockchain technology is beginning to impact organizational recordkeeping, there is an opportunity for information professionals to innovate their practices through its use. Smart contracts, for example, to automatically implement the publication of data, are being explored by the UK National Archives.

Info Pros Are Compelled to Act

Blockchain technology is transforming traditional digital recordkeeping from a centralized operating model under human control to a decentralized, autonomous model. Information professionals must understand the strengths and weaknesses of this emerging technology to be able to advise the increasing number of organizations that are looking to implement it for recordkeeping.

As with any emerging technology, there are significant opportunities – for greater business efficiency, privacy protection, and security, for example – but there are also great risks. Perhaps the greatest risk will be if information professionals fail to take up the challenge of understanding the capabilities of blockchain-based recordkeeping, allowing its implementation to march ahead without their wisdom and guidance. That could lead to costly mistakes that might otherwise have been avoided. Information professionals should feel compelled not to let that happen. E

About the Author: Victoria Lemieux, Ph.D., CISSP, is an associate professor of archival science and Sauder School of Business Distinguished Research Scholar at the University of British Columbia and adjunct associate professor of research at the University of Maryland. Her research focuses on risk to the availability of trustworthy records, particularly in financial contexts, and how these risks impact upon transparency, financial stability, public accountability, and human rights. She holds a doctorate in archival studies from University College London, is a Certified Information Systems Security Professional, and won the 2015 Emmett Leahy Award for outstanding contributions to the field of records management. Lemieux can be contacted at *v.lemieux@ubc.ca.*