NATIONAL ARCHIVES

OFFICE *of the* CHIEF RECORDS OFFICER

Blockchain White Paper

National Archives and Records Administration

February 2019

Introduction 3
Blockchain Overview 3
Conceptual Description 3
Technical Description 3
Blockchain Parts 4
What is a Hash 5
Blockchain Types 6
Blockchain Platforms 7
Blockchain Smart Contracts 8
Blockchain in the Federal Government 8
Records Management Implications and Analysis 9
Records on a Blockchain 9
Authenticity and Integrity Opportunities 10
Records Scheduling 10
Transferring Records 11
Decentralization Challenge 11
Archival Science and Disciplinary Integration 12
Blockchain and Archival Veracity 12
Blockchain and Success Criteria 12
Conclusion 13
Glossary 14
Selected Bibliography 16

Introduction

The National Archives and Records Administration (NARA) undertook a research project in fiscal year 2018 to understand how blockchain works, to learn how it is being used in the Federal government, and to discuss the potential implications for records management.

This white paper represents NARA's findings as of July 2018. Research consisted of attending various interest group meetings, webinars, symposiums, and discussions with external experts. The research team also performed a technical review and analysis of articles surrounding blockchain. This paper contains a selected bibliography of these articles as a resource. This paper also contains various terms in ***bold italics***, which are defined in a glossary.

This white paper is intended to help federal records managers to better understand blockchain technology and to consider the records management implications at their own agencies. On the whole, NARA's current guidance issued for federal records management applies to records created by blockchain technology. NARA will continue to monitor how blockchain use evolves in government and will determine if any future guidance is needed to address specific aspects or implications for blockchain records.

Blockchain Overview

Conceptual Description

Blockchain, or ***distributed ledger*** technology, is a database that is consensually shared, replicated, and synchronized.

To better understand the technical aspects of a blockchain, it is helpful to explain the concept through an example. When an individual deposits a sum of money into a banking institution, the individual trusts that the sum will be there until they decide to exchange it for goods or services. The individual trusts the bank will have an accurate record of the transaction, such as the amount, depositor, date, and time of the deposit. More broadly, society relies on central repositories, such as banks or governments, to collect, maintain, and protect the recorded actions of individuals or institutions.

Blockchain differs from centralized repositories in that it decentralizes the source of trust. An individual deposits funds into a digital wallet and the value is captured on the blockchain. If this individual purchases a digital song, the transaction is captured in the blockchain along with the change in fund level in the digital account. The bank is not required as a trusted third party. The trustworthy record is recorded in the blockchain shared by all the parties on the network.

Technical Description

The replication and storage of transactional data by each party, or node, on a blockchain network is known as a distributed ledger. Conflicts, or inaccuracies within the database, are automatically resolved with predefined ledger rules. The fundamental characteristics of the distributed ledger include:

- Operation with peer-to-peer networks,
- Decentralized transaction record keeping,
- Consensus or trust-based transactions, and
- Tamper resistance.

Blockchains, while similar to databases, are not used for general data storage, but rather hold information about transactions (see Figure 1). Sometimes the blockchain will contain the transactions themselves or may include the proof a transaction is valid**.**

Blockchain Parts

Blockchains contain three core parts:

- **Block**: A list of recorded transactions over a period of time. Transactions can represent virtually any type of activity from registering a land deed to a single purchase. Any rules relating to the block itself are established when the network is first created. For example, the maximum number of transactions in a block or the size of each block can be limited.

- **Chain**: When the block reaches its maximum size of transactions, it is chained or linked to the preceding block through a ***hash*** as described in the section below. The hash value of one block is inserted into the next block. This makes a link between the new block and the previous block. Repeating a hash function on an unaltered block of data will always generate the same fixed-length value. If a block of data is altered, the resulting hash output will be different. A user can then see the hashes are different and will know the original block has been altered and may no longer be trustworthy. (See Figure 2)

- **Network**: The network is made up of nodes each containing a complete record of all transactions on a blockchain. No centralized "official" copy exists and no node is "trusted" more than another. The data integrity is maintained by the blockchain being replicated on all of the nodes.

  Think of a node as a cluster of servers running a blockchain. Node operators are incentivized to operate a node by receiving rewards for their efforts. For example, with cryptocurrencies, nodes compete to solve crypto-puzzles. The first node completing the puzzle has its solution verified by other nodes. Once the solution is verified, the node completing the puzzle adds the next block to the blockchain and is also rewarded with cryptocurrency for its effort. This process is called mining, with the resources involved called miners. Nodes are found across the globe and are challenging to operate. For example, the infrastructure of one cryptocurrency is supported by approximately 5000 nodes. Incentivized miners are required for cryptocurrency platforms, but are not necessarily part of other blockchain uses.

Behind the scenes, each blockchain has its own rules or algorithms governing how nodes validate transactions intended for entry into the blockchain. These rules are called a ***consensus mechanism*** and are established when the blockchain is created. By embedding a consensus mechanism, blockchains create a way for parties who do not know if they can trust each other to agree an entry should be added to the blockchain. This addresses the so-called ***Byzantine Generals Problem***. Each blockchain has its own consensus mechanism depending on the type of transaction it is capturing. Some consensus mechanism are known as "proof of work", "proof of space" or "proof of stake". The mechanisms facilitate authenticity, or the immutability of transaction records.

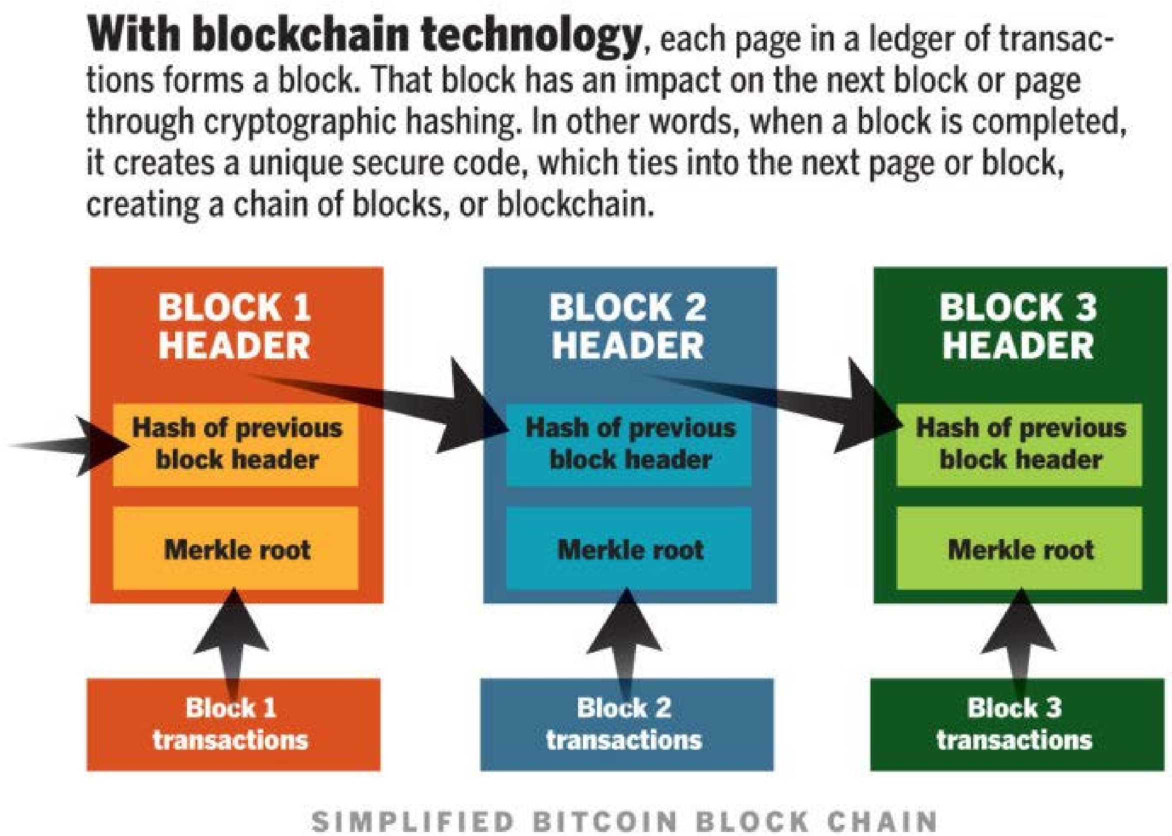

Figure 1. Pursel, Bart. (2018, January 28). Blockchain is Here to Stay. Retrieved from http://sites.psu.edu/ist110pursel/2018/01/28/blockchain-is-here-to-stay/

What is a Hash

A ***hash*** is an algorithm that takes a variable string of data and generates a fixed length value. The data about the transactions must be small so the validity of the transaction can be quickly calculated and distributed to other nodes. Large amounts of data are often stored "***off chain***" with pointers or hashes of the data stored within the blockchain. Traditionally, ledgers were used to record transactions of property or goods: only the transaction was captured in the ledger with the real property being handled separately.

For example, a Secure Hash Algorithm generating a 256-bit signature (***SHA-256***) generates different hash values for slight variations in the spelling of the words "National Archives".

Variable Text String Entry Value	**Hash Value**
National Archives	6429799b9af2d91cbf915cb0290f3a50281193a977b3457d63e4541cc5788c5b
National Archives *(an extra space)*	d926fe7e72d09b249701dbcde2dad0ccb9b4bb653e053e461a67bbb951dcae0b
Nati0nal Archives	5f2d570fc940d5f8de89310db43f789fdd99f51e89c021e1a50acb7a6fe2cf83

Figure 2. Xorbin (2018). Retrieved from https://www.xorbin.com/tools/sha256-hash-calculator

Oftentimes, to save space, multiple hash values can be brought together and hashed again, creating a single hash value or Merkle root that represents multiple hashes. This technology is called a ***Merkle tree***.

NARA began hashing electronic records when the Electronic Records Archives (ERA) was deployed in 2008. NARA has been using the SHA-256 algorithm to prove file ***fixity*** when electronic records are ingested into ERA. The files are automatically hashed and this hash can be used to verify the authenticity of a file. The hash is stored in log files and the processing archivist has access to this information, usually through reports. In the future, it might be feasible to store this information in a blockchain.

Blockchain Types

There are three types of blockchains:

Public: Large distributed blockchains are available for anyone to participate in and are generally open-sourced with the code maintained by a broad community. For example, Bitcoin, one of the most commonly known blockchain networks, is a public blockchain.

Permissioned: Large distributed blockchain network with established roles that individuals can fill when using the blockchain. For example, a group of banks may share sensitive cash reserve information with each other through the blockchain.

Private: Oftentimes a smaller blockchain is tightly controlled and is established between trusted entities that wish to share sensitive information. For example, an organization could use an internal blockchain to certify documents for its own use.

Blockchain network participants utilize public and private keys to digitally sign and make secure transactions within the system.

Public Key Infrastructure (PKI) mathematically pairs two long numbers or keys together that are not identical. This is called asymmetric cryptography. Both keys can be used to encrypt and decrypt messages. One key can be shared publicly, known as the public key and one is held privately known as the private key. For example, anyone using the public key can send and encrypt a message, but only the individual with the private key can decrypt and read the message. Within the blockchain context, a user can sign a transaction with their private key and anyone can verify the signer by using the corresponding public key. NARA has issued guidance on PKI.

Blockchain Platforms

Blockchain is made up of a collection of underlying technologies that can be bound together in multiple ways. This allows blockchains to be configured in multiple ways to serve different purposes. Our review of various blockchain platforms identified four different approaches represented by the options outlined below.

1. **Bitcoin**: Bitcoin is a ***cryptocurrency*** with a related open-source platform. Bitcoin's blockchain is primarily designed to support the exchange of cryptocurrency without an intermediary third party. Bitcoin assumes no trust between parties and requires numerous decentralized nodes to ensure the blockchain has not been corrupted by malicious actors.

2. **Ripple**: Much like Bitcoin, Ripple is based on an open-source protocol that uses blockchain to exchange value. Ripple has an established user-base of regional and global banks that need to transact international payments in real-time. Ripple also allows the trade of goods, property, and items of value.

3. **Ethereum**: Whereas the two platforms above are primarily focused on their own currency trade, Ethereum launched in July 2015 with the goal of providing a fully functioning programming language to allow users to build full applications with an integrated blockchain. Ethereum is a crowd-funded and open-source programming language. Users of Ethereum can program executable ***smart contracts*** and ***decentralized applications*** using the blockchain.

4. **Hyperledger**: The Hyperledger project focuses on developing an open source and collaborative approach to distributed ledgers. By developing standards and an overall framework for blockchains, Hyperledger has gained support from organizations including

Cisco, American Express, and IBM. Some library and information science schools are incorporating Hyperledger into their curriculum. Hyperledger has stated they will never build a cryptocurrency.

Blockchain Smart Contracts

A smart contract is a contract that has been translated into the software language of the blockchain, stored on the blockchain, and can be autonomously executed by a triggering event. Put differently, a smart contract is a series of if/then statements programmed and saved on the blockchain. Once the requirements of the smart contract are met, the contract will automatically be executed and the resulting action will be stored and shared across the blockchain. For example, a songwriter can sell a digital song at a certain price in an online music app. This agreement could be programmed into Ethereum as a smart contract. The smart contract will automatically distribute payment to the songwriter when a fan buys the digital song and capture the transaction in the blockchain.

During the development of blockchain platforms, system developers have the ability to program smart contracts that will render transactional data, or records, ***cryptographically inaccessible***. This means the records are not deleted from blockchain, but are cryptographically redacted to block the data from general view. It is not clear yet if cryptographically inaccessible data means will be permanently inaccessible and therefore could be considered “removed” from a complete record.

From a records management perspective, features like cryptographically inaccessible data indicates that records retention and disposition was not included as part the original intention of blockchain developers. The use of these smart contracts could potentially address record access, retention, disposition, and litigation hold requirements, depending how the blockchain rules, roles, and features are developed.

Blockchain in the Federal Government

Within the Federal government, GSA is leading a forum exploring the long-term viability of blockchain. The community started a U.S. Emerging Citizen Technology website consisting of proposed use cases and program initiatives occurring across Federal government and state agencies. The atlas promotes openness by providing a platform for Federal agencies to share information and concepts before and during actual program development to avoid duplication of effort and unnecessary spending.

GSA shares details on current agency initiatives on the GSA Blockchain Programs in Action webpage. GSA advised agencies to stay focused on their business needs and assess whether the new technology is the best solution for their problem. As with any procurement, agencies should thoroughly identify their program and system requirements before evaluating blockchain applications. The webpage lists some blockchain use cases agencies submitted for exploration such as personnel workforce data, IT asset management, and supply chain management.

Congressman David Schweikert (R-AZ), is the co-chair for the Congressional Blockchain Caucus. As a keynote speaker at a U.S. Federal Blockchain Forum in July 2017, he spoke about the use of distributed ledgers and the existing use of blockchain smart contracts for financial transactions. Continued congressional focus on blockchain will help ensure agencies are supported in their efforts to implement blockchain technologies.

State governments, such as Delaware, Illinois, and Vermont, have been exploring and adopting initiatives for state services. These services may include deed registrations, licensing, and general financial transactions. Vermont, through a pilot with Propy, a decentralized title registry, registered on a blockchain the first real estate deed transaction in the United States in February 2018.

Although the Federal government has only a handful of pilots in place, private industry is forging ahead with implementations in the areas of financial transactions, supply chain management, and health records. The technology is being extended to land records, digital identity, and asset management. The general public, as well as Federal, state, and local governments, are studying and piloting blockchain-based applications to determine viability and practicality.

Records Management Implications and Analysis

Records on a Blockchain

The definition of a Federal record is:

> [A]ll recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of data in them (44 U.S. Code § 3301).

The term “recorded information” includes all traditional forms of records, regardless of physical form or characteristics, including information created, manipulated, communicated, or stored in digital or electronic form.

The hash, block header, and transactional data could be Federal records, particularly if they are made in connection with the transaction of government public business and are appropriate for preservation. The records within the blocks may consist of a variety of record types accumulated from multiple transactions. Blockchain’s inherent capability drives decentralized record keeping of transactional data, meaning records will be stored on the blockchain network, or platform, and shared among all subscribing nodes.

Authenticity and Integrity Opportunities

One of the fundamental issues for records management has been ensuring the authenticity and integrity of records. Blockchain presents records managers a new way to ensure electronic systems offer integrity. Three examples of blockchain use might include:

- Digital signatures, a common form of transactional data, can be stored on a blockchain. Currently when we digitally sign an electronic textual document, such as a PDF, the signature is stored in the document itself. Signatures must be applied sequentially, and if the certificate expires, the validity of the document can be questioned. Storing signatures, along with a hash of the document, removes the requirement for sequential signing and certificates. This could be particularly useful for long-term records, such as land deeds and wills.

- A blockchain can be used to determine authenticity of a physical object or real property. In the art world, a buyer would want to ensure the painting being purchased is authentic. Since the certificate of authenticity is retained in the blockchain, it would be difficult to counterfeit, and conversely the certificate for a counterfeit painting would not validate against the authentic one.

- Similarly, a blockchain could be used to provide authenticity for a record. When an organization provides a record to users, it can usually provide provenance and certification that it is a true and accurate copy. If there is any question afterwards, it would have to be compared to the original. If the certificate of authenticity is retained in a blockchain, the record could be re-hashed to determine if any changes or alterations have been made. Photographs can be altered, cropped, or otherwise modified by a researcher and if the hash fails upon comparison, then they would be able to prove the image has been changed.

Records Scheduling

As blockchain technology is used to create federal records, it could impact how NARA approaches scheduling. At this time, the use is not wide-spread and appraisal and scheduling would follow traditional models evaluating the content and context of the subject of the records to determine the value of the records and the retention periods for the records.

What may change is the disposition instructions for transfer of any permanent blockchain records or deletion of any temporary records. For example, would the disposition instruction require NARA to be made a node or part of the blockchain in order to have access to the records for eventual transfer? Would the entire blockchain have to be transferred by the federal agency on the blockchain to NARA? Is it possible to transfer parts of blockchain?

Transferring Records

Transferring blockchain records to the National Archives is a completely theoretical discussion, at this point. No blockchain records have been scheduled as permanent records, yet. Some of the questions to consider are:

- Are there special resources needed to archivally store blockchain records, such as node/network administration skills?
- Since the records within the blocks may consist of a variety of record types accumulated from multiple transactions, would NARA be able to access the formats contained in the blocks?
- How would NARA manage, preserve, or provide access to blockchains containing cryptographically inaccessible parts? The blocks could not be removed because that would invalidate the blockchain, but they could not be accessed because of how the blockchain rules were established.
- If multiple agencies are on the blockchain network, each with their own node, would a single creating agency or owner need to be responsible for transferring the records or transactional data? The blockchain is literally exactly identical for every organization.
- What if NARA become a node itself? In that scenario, the physical “transfer” of the blockchain records becomes irrelevant. Would the legal transfer of the blockchain records happen when NARA is included on the blockchain?

Decentralization Challenge

Current records management models rely on a centralized collection of electronic records captured and maintained within the structures and systems of an organization. For example, some agencies use content management systems to locate, tag, and govern collections of photos. Some agencies use Microsoft Office 365 to manage-in-place electronic records created with desktop applications. Blockchain shifts the responsibility and trust for maintaining electronic records from the structures and systems of the organization to a distributed network. This represents a change in the role of centralized records management systems and tools; a shift to the blockchain itself performing the validity and trust that records management systems performed.

More broadly, this shift from a centralized model of trust to a network-based model is becoming more common across various technology sectors. Whether it be technology (the Internet) or the way we communicate (e.g. Facebook, Instagram, or Twitter), networks are becoming a primary organizing principle. This shift is reflected in archival description projects, such as Social Networks and Archival Context (SNAC), which seeks to place historical figures in the broader context of their relationships with other people and uses a networked approach to show how multiple archival repositories have related collections telling their stories in multiple ways.

This shift may impact how records are organized and arranged and maintained over time, which in turn will impact how records managers collect records, apply intellectual and access controls, and execute disposition rules.

Archival Science and Disciplinary Integration

It's fairly common for archival professionals, especially those working with electronic records, to have computer or IT skills. While most library and information schools include database management, coding, and digital curation, Dr. Victoria Lemieux, associate professor at the University of British Columbia, sees a trans-discipline approach to future record keeping, involving computer scientists and software engineers as well as archivists. She is teaching her students how to create blockchains using Hyperledger. Dr. Lemieux is active in the blockchain community and has been exploring using blockchain for property transactions, especially in areas where there has been a lack of trusted record keeping. Dr. Lemieux compared using blockchain to medieval record keeping systems where objects were used to document transactions.

Blockchain and Archival Veracity

Video, audio, and photo manipulation present a unique challenge to the National Archives and its mission to collect, maintain, and provide access to the authentic records of the Federal government. For example, there are video editing applications for facial manipulation of YouTube videos, as well as highly accurate voice editing software, which allows users to more easily create "fake videos" without detection.

In order to solve the challenge of archival veracity, NARA recently used hashes. Specifically when NARA released additional JFK assassination material, each of the bulk download items included a hash in the metadata so external entities could validate the digital material had not been altered. Blockchain technology could be part of future archival veracity solutions.

Blockchain and Success Criteria

NARA provided high-level records management guidance to agencies on how to manage electronic records with two documents: the Criteria for Successfully Managing Email Records, and more recently Criteria for Successfully Managing Permanent Electronic Records. In addition, NARA issued the Universal Electronic Records Management (ERM) Requirements, containing requirements derived from existing statutes, regulations, standards, and other guidance products to describe the overall management of electronic records.

As agencies adopt blockchain technologies, they will need to address the principles in these guidance products by:

1. developing policies to address the records management implications of blockchain,
2. implementing systems that can execute those policies,
3. ensuring blockchain records/transactional data can be accessed over time, and
4. executing the disposition of blockchain records/transactional data by deleting them or transferring them to the National Archives.

Conclusion

This document described what blockchain technology is, how the Federal government is exploring blockchain use, and some of the records management implications. This document is a snapshot in time, based on research conducted in 2018. It is important to note blockchain technology is evolving and being used in new and interesting ways. Blockchain may eventually change basic government functions, such as information certification, financial transactions, and citizen identification. Changes in these areas have the potential to fundamentally impact the government's role as a trusted information repository or records holder. NARA, agencies, and federal records managers will need to monitor how blockchain technology matures and is implemented over time to ensure that records management issues are identified and addressed.

Glossary

Term	Definition
Byzantine Generals Problem	At a conceptual level, blockchain attempts to address the challenge posed by a paper published in 1975 that outlines what has become known as the Byzantine Generals Problem. Two generals commanding their own armies are attacking a common enemy. Neither army is powerful enough to defeat the enemy on its own, so the generals must send messengers to each other confirming the time of attack. General 1 sends a messenger with the specified time of attack to General 2. If the messenger is not captured and arrives, how does General 2 know that the messenger has not been compromised by the enemy? Even if the messenger has not been captured or compromised, how does General 1 know that the messenger returning with the confirmed time of attack has not been compromised? The Generals can never be sure that the information they are receiving is accurate and valid.
Consensus mechanism	The newest blockchain must be consistent and accepted by the majority of computers online. The method by which the new blockchain is accepted is defined by the algorithm used.
Cryptocurrency	A digital currency that encryption techniques use to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank.
Cryptographically inaccessible	Platforms have controls that can make hash metadata unavailable to members. Akin to redaction, individual metadata pieces or entire transactions can be shielded from view. In a blockchain, transactions cannot be removed without breaking the chain, so making items cryptographically inaccessible retains the chain while making data unreadable.
Decentralized applications	Google Play and the Apple Store centrally vet the apps that are offered through their stores. A decentralized application is an app that can be made available on a blockchain platform without a centralized vetting point.
Digital ID	Information on an entity used by computer systems to represent an external agent. That agent may be a person, organization, application, or device.
Distributed ledger	A replicated database shared across many nodes.
Fixity	File fixity ensures that property of a digital file is fixed, or unchanged. Fixity checking is the process of verifying that a digital

Term	Definition
	object has not been altered or corrupted.
Hash	A function that takes an input string, which can be of any length, and generates an output of fixed length. The output, or hash, is used to authenticate information. The values returned by a hash function are called hash values, hash codes, digests, or simply hashes.
Merkle tree	In cryptography, a Merkle tree is a tree in which every leaf node is labelled with the hash of a data block and every non-leaf node is labelled with the cryptographic hash of the labels of its child nodes. Hash trees allow efficient and secure verification of the contents of large data structures.
Mining	The process by which nodes compete to add transaction records or blocks to the blockchain.
Off-Chain	Objects or data referenced via links or pointers, but stored separately from the blockchain.
Peer-to-peer	A distributed network in which nodes are interconnected and share data directly with each other without a centralized service.
Permissionless/Public Ledger	Anyone can insert transactions into a block to be included in the blockchain.
Permissioned/Private Ledger	Restricted to a limited set of authorized nodes and only an authorized user can access, generate transactions, and update the ledger.
Public/Private Key Infrastructure	Keys that are mathematically related to each other. The public key can be used to verify a signature generated using a private key.
SHA-256	Secure Hash Algorithm (SHA) used to generate a 256-bit hash.

Selected Bibliography

What is Blockchain?

- Gupta, Vinay. "A Brief History of Blockchain." Harvard Business Review, February 28 2017. URL: https://hbr.org/2017/02/a-brief-history-of-blockchain
- Lewis, Antony. "Gentle Introduction to Blockchain." Bits on Blocks: Thoughts on Blockchain Technology, September 9, 2015. URL: https://bitsonblocks.net/2015/09/09/gentle-introduction-blockchain-technology/
- Szabo, Nick. Devcon 1: History of the Blockchain. Filmed November 13, 2015. YouTube video, Duration 18:24. Posted November 25, 2015. URL: https://www.youtube.com/watch?v=7Y3fWXA6d5k
- Wikipedia. The Free Encyclopedia, s.v. "Blockchain." URL: https://en.wikipedia.org/wiki/Blockchain

Blockchain Impact

- Gupta, Vinay. "The Promise of Blockchain is a World Without Middlemen." Harvard Business Review, March 6, 2017. URL: https://hbr.org/2017/03/the-promise-of-blockchain-is-a-world-without-middlemen
- Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." Bitcoin, 2008. URL: https://bitcoin.org/bitcoin.pdf

Smart Contracts

- Lewis, Antony. "A Gentle Introduction to Smart Contracts." Bits on Blocks: Thoughts on Blockchain Technology, February 1, 2016. URL: https://bitsonblocks.net/2016/02/01/gentle-introduction-smart-contracts/
- Lewis, Antony. "Three Common Misconceptions about Smart Contracts." Bits on Blocks: Thoughts on Blockchain Technology, March 7, 2017. URL: https://bitsonblocks.net/2017/03/07/three-common-misconceptions-about-smart-contracts/

Advanced Technical Articles

- "Blockchain Underpinnings: Hashing." ConsenSys, January 12, 2016. URL: https://medium.com/@ConsenSys/blockchain-underpinnings-hashing-7f4746cbd66b
- NISTIR 8202 Blockchain Technology Overview. National Institute of Standards and Technology, October 2018. URL: https://csrc.nist.gov/publications/detail/nistir/8202/final.

Records Management and Archival Implications

- ARCHANGEL - Trusted Archives of Digital Public Records. UK Research and Innovation. URL: https://gtr.ukri.org/projects?ref=EP%2FP03151X%2F1
- Ballu, Deep. "World's Largest Archive Testing Blockchain for Records Management." Bitcoin News, August 6, 2018. URL: https://bitcoinnews.com/worlds-largest-archive-testing-blockchain-for-record-management/
- Computational Archival Science (blog). URL: http://dcicblog.umd.edu/cas/

- Desouza, Kevin C, Chen Ye, and Kiran Kabtta Somvanshi. Blockchain and U.S. State Governments: An Initial Assessment. Techtank, April 17, 2018. URL: https://www.brookings.edu/blog/techtank/2018/04/17/blockchain-and-u-s-state-governments-an-initial-assessment/
- Findlay, Cassie. “Ideas on using appraisal techniques on Blockchain technology.” June 15, 2017. URL: https://cassiefindlay.com/2017/06/15/appraisal-blockchain/
- Lemieux, Victoria. Blockchain and Distributed Ledgers as Trusted records keeping Systems: An Archival Theoretic Evaluation Framework. Conference Future Technologies Conference 2017. URL: https://www.researchgate.net/publication/317433591_Blockchain_and_Distributed_Ledgers_as_Trusted_Recordkeeping_Systems_An_Archival_Theoretic_Evaluation_Framework
- Lemieux, Victoria. “Blockchain Technology for Recordkeeping: Help or Hype?” October 2016. doi>10.13140/RG.2.2.21736.67842
- Lemieux, Victoria. “Evaluating the Use of Blockchain in Land Transactions: An Archival Science Perspective.” European Property Law Journal 6 (2017). doi>10.1515/eplj-2017-0019.
- Lemieux, Victoria, and Manu Sporny. “Preserving the Archival Bond in Distributed Ledgers: Data Model and Syntax.” Proceedings of the 26th International Conference on World Wide Web Companion (2017): 1437-1443. doi>10.1145/3041021.3053896.
- Lemieux, Victoria. “Trusting records: is Blockchain technology the answer?” Records Management Journal 26, no. 2 (2016): 110-139. doi>10.1108/RMJ-12-2015-0042
- Lemieux. Victoria. “A Typology of Blockchain Recordkeeping Solutions and Some Reflections on their Implications for the Future of Archival Preservation.” 2017. URL: http://dcicblog.umd.edu/cas/wp-content/uploads/sites/13/2017/06/Lemieux.pdf

State Blockchain Implementations

- Vermont Secretary of State. Blockchain Technology: Opportunities and Risks. January 15, 2016. URL: https://legislature.vermont.gov/assets/Legislative-Reports/blockchain-technology-report-final.pdf
- Illinois Department of Innovation & Technology. Blockchain in Illinois. URL: https://www2.illinois.gov/sites/doit/Pages/BlockChainInitiative.aspx
- Blockchains: Moving Digital Government Forward in the States. National Association of State Chief Information Officers, 2017. URL: https://www.nascio.org/Portals/0/Publications/Documents/2017/NASCIO%20Blockchains%20in%20State%20Government.pdf

Courses

- Coursera: Bitcoin and Cryptocurrency Technologies URL: https://www.coursera.org/learn/cryptocurrency/

Potential Standards

- Roadmap for Blockchain Standards Report. Standards Australia, March 2017. URL: https://www.standards.org.au/getmedia/ad5d74db-8da9-4685-b171-90142ee0a2e1/Roadmap_for_Blockchain_Standards_report.pdf.aspx

Audio/Video Editing

- "Breaking News." Radiolab, July 27, 2017. URL: https://www.wnycstudios.org/story/breaking-news
- Lardinois. Frederic. "Adobe's Project VoCo lets you edit speech as easily as text." Techcrunch, November 3, 2016. URL: https://techcrunch.com/2016/11/03/adobes-project-voco-lets-you-edit-speech-as-easily-as-text/
- Solon, Olivia. "The Future of Fake News: Don't Believe Everything You Read, See or Hear." Guardian, July 26, 2017. URL: https://www.theguardian.com/technology/2017/jul/26/fake-news-obama-video-trump-face2face-doctored-content

Articles about implementation

- Bindi, Tas. "Doc.ai launches blockchain-based conversational AI platform for health consumers." ZDNet, August 24, 2017. URL: https://www.zdnet.com/article/doc-ai/
- Irrera, Anna. "Accenture, Microsoft team up on blockchain-based digital ID network." Reuters, June 19, 2017. URL: https://www.reuters.com/article/us-microsoft-accenture-digitalid-idUSKBN19A22B
- Korjus, Kaspar. "Estonia is Enhancing the Security of its Digital Identities." Medium, October 30, 2017. URL: https://medium.com/e-residency-blog/estonia-is-enhancing-the-security-of-its-digital-identities-361b9a3c9c52
- Miller, Ron. "IBM unveils Blockchain as a Service based on open source Hyperledger Fabric technology." Techcrunch, March 19, 2017. URL: https://techcrunch.com/2017/03/19/ibm-unveils-blockchain-as-a-service-based-on-open-source-hyperledger-fabric-technology/

Framework for Government Implementation

- "Building the Hyperconnected Future on Blockchains." World Government Summit, February, 2017. URL: http://internetofagreements.com/files/WorldGovernmentSummit-Dubai2017.pdf
- GSA. Emerging Citizen Technology: Blockchain. URL: https://www.gsa.gov/technology/government-it-initiatives/emerging-citizen-technology/blockchain

Associations

- Government Blockchain Association. URL: https://www.gbaglobal.org/

- American Council for Technology-Industry Advisory Council (ACT-IAC). URL: https://www.gbaglobal.org/

* DISCLAIMER: Reference to any commercial products or services in this presentation is not an endorsement or Government sanction of those non-Federal entities, its services or products.