Executive Summary: Blockchain Technology for the Information Professions
Prepared for the Blockchain National Forum by Alessandro Voto
7/16/18

Blockchain technology offers a powerful new way to store, synchronize, and protect sensitive information, making it an indispensable tool for the future of the information professions. After nearly a decade of experimentation and research developers have expanded the usability and maturity of blockchain technology, enabling use beyond digital currency transfers. It's time for information professionals to take the lead on using these emerging tools to better preserve and spread our heritage and collective memory.

What is a blockchain?

Blockchains are databases that store multiple users' records together as chronologically-ordered "blocks" at regular intervals. Each new block is linked to prior blocks using a form of cryptography called a hash function, making it more and more difficult to retroactively alter or delete individual records in the chain. The blockchain database is copied to all participants in the network, and these participants synchronize with each other over time to form a single, shared version of history. Like the term "cloud", the term "blockchain" is used to describe a wide assortment of technologies with similar architectural properties.

Benefits of blockchain technology

- Blockchains distribute records to multiple untrusted actors. By holding records in many places instead of a central repository, blockchain systems can improve record availability, redundancy, and censorship resistance.
- Blockchains can be used to store arbitrary information on-chain, or can store a "digest" of information stored off-chain via hashes that ensure the document has not been changed whatsoever since it was first received. Both help to keep the correct state of a record visible to multiple parties for later reference.
- The relative order of blocks and records are kept intact using linked hashes, protecting the provenance of information, for example in supply chain-related applications.
- Blockchains enable provably scarce digital assets and decentralized marketplaces. These can be natively digital assets like cryptocurrencies, or can serve as title certificates to physical property or off-chain digital property.
- Newer blockchain systems like Ethereum allow users to store computer programs known as "smart contracts" across a blockchain network, rather than just transaction data. These smart contracts provide a technical framework for decentralized applications of all kinds that require trustworthy code execution and data storage without a third party, especially those in which there is very low-trust amongst participants. They can also be used to escrow funds and move assets without a central intermediary.
- [Note: this list is by no means exhaustive, but these functions can be aggregated to create quite a few opportunities in almost any sector.]

How could blockchain technology impact the information professions?

- Archivists can store sensitive historical information, data, websites, 3D renderings, etc. on multiple computers to prevent deletion or tampering.
    - Tools like Protocol Labs' Interplanetary File System (IPFS) and Filecoin can be used to incentivize data holders and route users directly to the content wherever it is held, rather than to servers that may be taken down.
    - Hashes can be used as a checksum to make sure the data sets are complete and unaltered since they were first submitted.
    - Permissions can be managed using blockchain-based identity and end-to-end encryption tools.
    - This is especially useful for politically sensitive data, like environmental data.
- Rented objects can be backed by an escrow payment, to be paid back automatically when the item is verifiably returned.
    - Asset collections can be tracked between facilities (inside and outside of the library system) using a shared supply chain tracking system.
    - Reputation systems can be developed which enable access to higher-value rentals based on past behavior and increased funds in escrow.
- Digital books, music, and other media can be rented out to people on a per-second, per-page, per-kilobyte, etc. basis using state channel technology.
    - State channels enable quick transactions between parties in small increments, settling to the main blockchain only when one of the two parties chooses to close out the channel and receive their net funds or commit some data sent during the interaction. This contributes to the scalability of blockchain applications, since the main chain isn't burdened with every single transaction.
    - The same approach to micropayments for access can be used for physical machinery.
- Communities can co-create media, tracking contributions on a blockchain and paying out for any future sales or use of the media.
    - Legal usage rights and other metadata can be linked to the media using a blockchain system. Users can cryptographically sign off on the terms and conditions for consuming or building on the media.
    - Creators can instantiate a decentralized organization using smart contracts. This means any time their work is used, a payment, equity, rights, or other forms of compensation can be automatically and fairly distributed to contributors according to the license terms.
- Academic credentialing can be handled using a decentralized identity service, allowing any individual or institution to attest to a person's learning achievements.
- Analytics and search tasks can be farmed out to a decentralized pool of people who rent out their computers' storage and computing capabilities to solve the task.

Implementation advice

- Consider whether to use a public blockchain system or a private/permissioned chain. Both have tradeoffs worth considering. In a nutshell, public blockchains enable easy integrations and extensive decentralization, but are slow and lack advanced privacy features. Private/consortium blockchains enable permissioned access to information, but suffer from limited decentralization and siloing from public network integrations.
- Blockchains are not yet ready to store private information directly on-chain, even when encrypted. Because records are spread out to many nodes, any network participant with sufficient time and resources could receive the message and break its encryption.
    - Instead, store certificates on-chain that link back to encrypted data stored elsewhere, such as a mobile phone. When sending data between parties, use traditional encrypted messaging channels.
- Consider whether data really should be made permanent and publically accessible, and how this capability might be misused.

Partnering for successful blockchain networks

- Many blockchain-based tools and networks are open source and free to access. Try to use these off-the-shelf, audited and battle-tested systems rather than creating your own from scratch or giving the entire project to a consultancy that would do the same.
- Create implementation standards to ensure that multiple systems can interoperate and use the same pooled data.
- Form a non-profit academic consortium to develop standards, share best practices and reference architectures, and build relationships between organizations to drive network adoption and collectively invent new solutions.
- Use hackathons to explore the limits of technology. Don’t expect that viable solutions will come directly from these; the primary goal will be growing awareness of the information profession’s needs in the blockchain space, forging alliances between developers and institutions, and allowing for limitless exploration to surface new ideas.
- Attend Meetups, conferences, and other local events where innovators discuss the newest developments in the space.