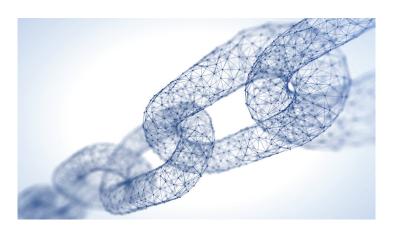# Blockchain for Archives FAQ

What is blockchain?

A blockchain is a distributed database stored on multiple computers across a network; it is a distributed ledger technology. The "blocks" of a blockchain are digital information, which are most often records of digital transactions and associated metadata, including the unique identifier of the block—a hash—and other transactional information like timestamps and parties involved. The "chain" is the networked database which is protected by consensus protocols and the use of encryption. For a distributed database such as this, there is no master copy. The authoritativeness of a given block is determined by consensus of all the distributed networked nodes holding a copy. Check out this piece on **Reuters Graphics** for a helpful visualization of how blockchain works.

What are consensus protocols?

Consensus protocols are the agreed-upon method for the computers in the network to determine which submitted transactions are well-formed and authentic, and can be added to the chain. Cryptography plays a large role, as hashing algorithms and digital signatures provide authenticity to said transactions. Once enough transactions are completed, those become a block which is then broadcast to the network and, if accepted, added to the chain. Once part of the chain, the cryptographic algorithm that is combined with key pieces of data contained in the block determines if the block is authentic. A blockchain will use a defined proof (e.g. proof of work, proof of stake, proof of authority, proof of time, etc.) as part of its protocols.

Who can participate in a blockchain network?

It depends on the nature of the blockchain network. A blockchain can be open to everyone with anonymous membership, or it could be privately controlled and open to authorized users only. The assumption is that if users can prove themselves according to the protocols that comprise the blockchain's logic, they are therefore trustworthy actors. Once the user has shown they can perform the necessary actions, they become part of the network and can add and check blocks. It is possible for a private blockchain of trusted partners to be developed. However, the original objective of blockchain (for example, in cryptocurrency) was to substitute mathematical proofs for trust in human relationships or co-developed policies. A formally-permissioned blockchain system would likely have to offer transparent and traceable transactions just as are in a regular blockchain system.

Is blockchain a preservation system?

No. Blockchain isn't a preservation system or a mechanism for managing data. A blockchain is a distributed database. While the consensus protocols can help ensure the data is what it claims to be, the data is not preserved in the sense that it is managed over the entire life of the electronic record. Individual blocks, or sets of blocks, or even the entire chain can be held by multiple individuals or organizations, but in a public blockchain there would be no guarantee that anyone would preserve data using bit-for-bit digital preservation practices. Digital preservation of electronic records includes description and metadata, transfer, format migration, media migration, long-term storage, access, and representation of the electronic record among other activities. Due to the validation mechanisms used in blockchain, bad actors could work to weight the networked decisions and manipulate the consensus of the network. Principles like distributed storage, networked databases, and multiple copies of data are good archival practices but are merely techniques; they do not represent the full body of digital preservation activities which include both technology and policy.

Does blockchain show chain-of-custody?

Chain-of-custody information is transactional and could be put into a block. This block of data would then become part of the blockchain and would be voted upon by other computers in the network as to its authenticity and accuracy. In a controlled network of trusted partners, archives might find this an acceptable way to record chain of custody.

Are there practical applications for blockchain in state government?

Not really. While blockchain could be used to show provenance and hold chain-of-custody information in blocks, there are existing software solutions that manage provenance information. If agencies submit permanent state electronic records in a blockchain, it might be helpful to archives to maintain that record in its original state. However, it would be possible to export the information contained in the blockchain and manage it using existing archival practices.

Does blockchain offer advantages that other distributed data networks don't?

Blockchain is a distributed data network—all members in a block have and verify all the data. This means that the data is replicated and can be authenticated. It does not, however, mean that the data is managed in a way that follows standards or practices of digital preservation. There are distributed data storage systems and communities (such as **LOCKSS**) that provide geographic distribution, a number of copies of the data, and other advantages of a distributed data network while also following digital preservation standards.

About CoSA

Formed in 2002, the Council of State Archivists (CoSA) is a national nonprofit using collaborative research, education, and advocacy to provide leadership that strengthens and supports state and territorial archives in their work to preserve and provide access to government records. Its members comprise the state archivists in the 50 state, 5 territorial and District of Columbia archives. These individuals oversee agencies that hold a legal mandate to document government and protect the rights and history of the American people across our country.

Support for this publication was provided by the Institute of Museum and Library Services (IMLS) through a National Leadership Grant to the Council of State Archivists (CoSA) for Archives Collaborating and Cooperating with External Strategic Stakeholders (ACCESS), a project of the State Electronic Records Initiative (SERI).