How blockchain technology has medieval roots

November 10 2017, by Victoria Lemieux

Credit: Karolina Grabowska from Pexels

Blockchain is an emergent technology that may be as transformative as the internet, according to many predictions. But this innovative new technology has a surprising link to the days of medieval treasuries.

Blockchain is a distributed ledger that uses cryptography—mathematical code—to chain together records of transactions in a tamper-resistant and transparent manner. It is being used as an alternative or replacement for national currencies, contracts, internet device authentication and more.

This form of record-keeping, though technologically novel in the digital era, is not so new after all. Historian M.T. Clanchy tells us that it existed in the medieval era, during the transition from oral to written forms of memorialization. At that time, symbolic objects played a crucial role in providing evidence of transactions, rights and entitlements.

I've been researching how governments and businesses around the world are either planning for or already piloting the use of blockchain for record-keeping. The goal of my research is to determine what these applications of the technology actually do—as opposed to what the marketing hype says they do.

I've been to Estonia to study how the government there is using distributed ledger technology to protect the integrity of citizens' medical records. I've been to Sweden to discuss how its land registry is testing blockchain to record the transfer of land ownership. I've reviewed proposed blockchain systems for land title registration in Honduras, new pilot implementations for land transaction records in Brazil. And I've spoken with innumerable new ventures looking to transform record-keeping with blockchain technology.

Three patterns for blockchain records

From this research, I've noticed three specific design patterns for blockchain record-keeping, which need explanation to understand how blockchain relates to medieval practices. I have classified these categories as mirror, digital record and tokenized systems.

The first of these design patterns is what I call the "mirror" type system. I characterize this type of system as being the most similar to current centralized record-keeping.

In these types of systems—be they for medical records, land titles, public archives or some other kind of records—digital records are neither created nor kept "on chain," despite some claims by blockchain companies to the contrary. Instead, a kind of digital fingerprint of the records in the form of a 256-bit random number, known as a "hash," is entered into the blockchain.

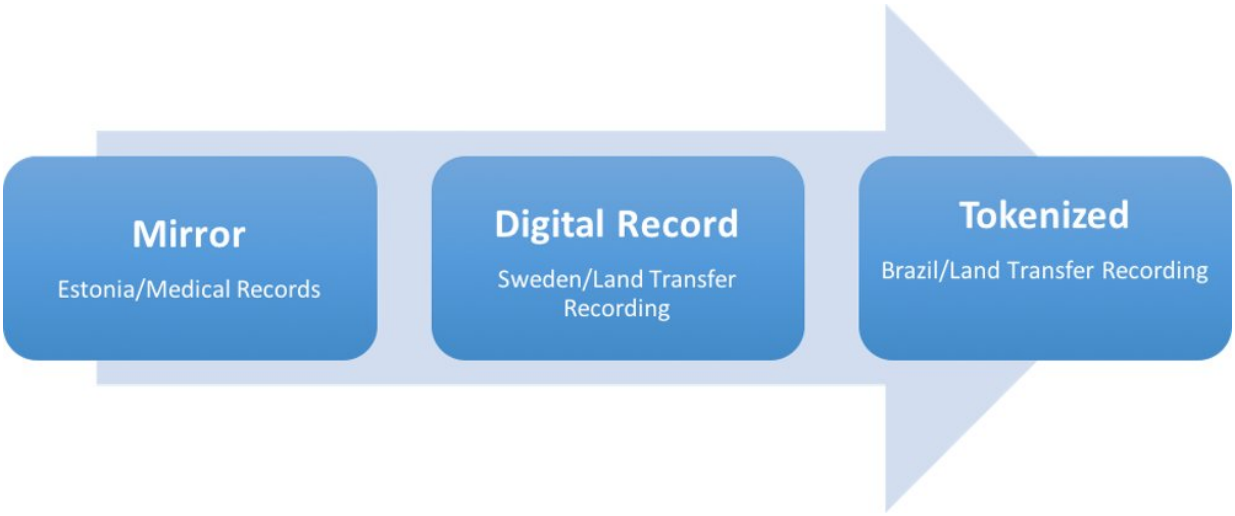
The purpose of recording this digital fingerprint in the blockchain is to protect the integrity of the records and be able to detect if they were tampered with. To prove that the records are tamper-free, the original digital records must be preserved in off-chain trustworthy digital repositories alongside preservation of their hashes in the blockchain.

Proving integrity of the records involves matching the hash of the record you want to validate with its digital fingerprint on the blockchain. If the hashes match, then the record you hold has not been altered.

Digital records

The second type of approach I've noticed is one that I call the "digital records" design pattern. In this type of system, new digital records are actually created within the blockchain itself, primarily by using smart-contracts.

Smart-contracts are computer programs that instruct the blockchain when to carry out a transaction, such as sending funds from one user to another. In these types of systems, the text of records is no longer in natural language that people can read. It is written in computer code for machines to read.



Three major categories of blockchain systems classified with examples. Credit: Victoria Lemieux

The rise of the smart contract raises a number of challenging and currently unanswered questions, such as what to do in case an error occurs and a smart contract doesn't behave as expected.

In the 2016 Decentralized Autonomous Organization (DAO) incident, for example, the attacker exploited poorly written smart code to siphon off 3.6 million Ether—an alternative to the popular cryptocurrency Bitcoin—roughly equivalent to $68 million at the time of the attack.

Equally importantly, current principles, standards and practices for managing and preserving digital records are not designed for smart-contracts and other distributed autonomous records created on chain. Ensuring that society's evidence infrastructure remains intact presents challenges similar to the early days of email and other electronic records. New approaches, yet to be developed, will be needed.

The third type of blockchain record-keeping design pattern is the "tokenized" type of solution. This is arguably the farthest from our current form of record-keeping, and many would argue the most innovative. With this type of system, not only are records captured on chain but valuable assets are represented and captured on chain.

These assets can symbolize anything of value: currency such as a primary use blockchain, Bitcoin; land, fine wine, food, diamonds, artworks—you name it.

In this third, tokenized form we can find centuries-old predecessors to blockchain.

Medieval objects parallel digital tokens

Are these assets really records? For answers, we may turn to the English archival theorist Sir Hilary Jenkinson, who observed in his 1937 Manual of Archive Administration that "there is a case where an old pair of military epaulettes; and among enclosures to letters, forming in each case an integral part of the document, the writer can recall portraits, human hair, whip-cord (part of cat-o'-nine-tails), a penny piece inscribed with disloyal sentiments, and a packet of strange powder destined to cure cancer."

In Jenkinson's view, these "exhibits" formed part of the archive, or collective body of records, because they provided evidence of business transactions.

We now have come to view these so-called exhibits more as museum objects than records because before the digital era, the physical awkwardness of these objects meant that they could not be managed with other records. Just as coins and paper currency once represented records of reserves of gold in a national treasury, Jenkinson's exhibits

were themselves tokens that represented other things.

Today, what once had a material form can be essentially dematerialized. Paper currency can be transformed into cryptocurrency. Land, fine wine, artwork, diamonds, food and other material objects—though still physically in existence—can be transformed into virtual representations called "tokens." In this way, in a tokenized, blockchain record-keeping system, literally every thing potentially becomes a record.

This is not a new idea.

At the time of the Norman Conquest, many grants were conferred by the bare word (*nude verbo*) without a writing or charter, but only with a sword, helmet, horn or cup. One example is the broken knife of Stephen de Bulmer kept in the archives of Durham Cathedral. It bears a parchment label recording the details of a gift of land made in the middle of the 12th century—which the knife itself symbolizes.

Just like the knives, horns, cups, rings and other objects customarily used in the conveyance of land during the medieval period, today's tokenized blockchain record-keeping systems use valuable cryptocurrencies such as Bitcoin as symbolic representations of assets like land.

This raises the question of whether blockchain technology will return today's archival repositories to their medieval roots as the treasure storehouses of kings. Will it be back to the future?

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation