Blockchain-Secured Electronic Apostilles

Enabling instant verification of Apostilles, anywhere in the world

By Natalie Smolenski (Hyland)

Executive Summary

- COVID-19 has made it clear to organizations around the world that digitization is key for continuity of business and to realize dramatic efficiencies and cost savings.
- Digitization of records is key, but digital records can be easily altered or forged.
- Digital signatures help prevent fraud, but they still rely on vendor services (like online databases or special software applications) to look up and verify records.
- Blockchain technology enables the creation of "self-verifying" records, including electronic Apostilles.
- These are digital files that recipients can store in a private wallet on their phones and share with anyone in the world with the click of a button.
- That "relying party" can then verify the record by scanning a QR code, clicking a button, or uploading the file to an open source public utility for verifying official records, like blockcerts.org.
- The result is records that recipients own and can be re-used (verified) an unlimited number of times—instantly and for free.

Introduction

The world is changing quickly. The COVID-19 pandemic has made it critical for organizations around the world—businesses, governments, educational institutions—to quickly digitize their operations. A big part of digitization is, of course, transitioning to electronic records. But traditionally, digital records have a big vulnerability: they can easily be altered or forged. For this reason, securing sensitive, official digital records with digital signatures has been key to their usability.

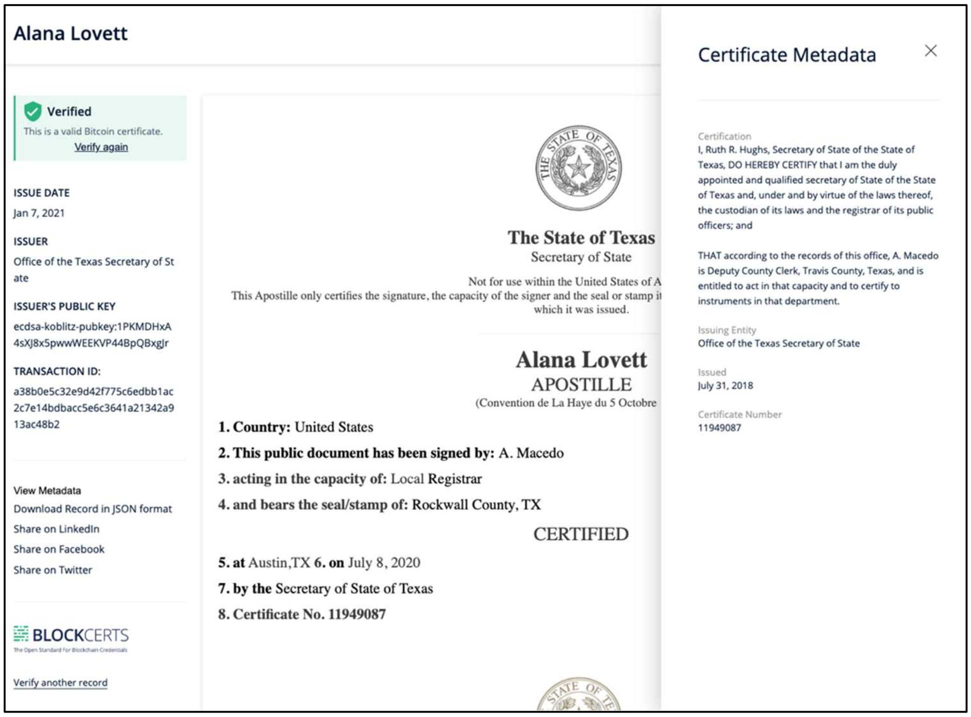
But digital signatures alone have not been able to solve the next problem: How does the recipient of a digitally-signed document easily store it, move it across borders, and quickly share it with anyone, anywhere, even multiple times, for instant and free verification?

This is where blockchain comes in.

What Is Blockchain?

Blockchain technology is a digital infrastructure for verifying the transfer of assets from one party to another. In this sense, the concept behind blockchain is actually very simple: a digital ledger that is distributed among many different computers ("nodes") around the world. All of the nodes update the ledger at the same time with the latest transactions. In this way, the entire ledger stays synchronized. Past entries cannot be edited once they are recorded. If anyone tries to change an entry in their local copy of the ledger, it will be quickly called out as fraudulent by all the other nodes running the true copy of the ledger.

Initially, blockchain ledgers were used to verify the transfer of digital money (cryptocurrency) from one party to another. Blockchain was the first technology that enabled the creation of natively digital money because it ensured that no one can make copies of that money and pretend they own more than they do. But because blockchain technology ensures the integrity of every transaction, people quickly realized that other kinds of data can “piggyback” on top of the ledger to secure different types of transactions as well. This data includes hashes or pointers to digital documents like birth and death certificates, marriage licenses, business registrations, trademarks, property titles, academic diplomas and transcripts, and Apostilles.



Alana Lovett

Verified

This is a valid Bitcoin certificate.

ISSUE DATE

Jan 7, 2021

ISSUER

Office of the Texas Secretary of St
ate

ISSUER'S PUBLIC KEY

ecdsa-koblitz-pubkey:1PKMDHxA
4sXJ8x5pwwWEEKVP44BpQBxgJr

TRANSACTION ID:

a38b0e5c32e9d42f775c6edbb1ac
2c7e14bdbacc5e6c3641a21342a9
13ac48b2

The State of Texas
Secretary of State

Not for use within the United States of A
This Apostille only certifies the signature, the capacity of the signer and the seal or stamp it
which it was issued.

Alana Lovett
APOSTILLE
(Convention de La Haye du 5 Octobre

1. Country: United States
2. This public document has been signed by: A. Macedo
3. acting in the capacity of: Local Registrar
4. and bears the seal/stamp of: Rockwall County, TX

CERTIFIED

5. at Austin,TX 6. on July 8, 2020
7. by the Secretary of State of Texas
8. Certificate No. 11949087

Certificate Metadata

Certification

I, Ruth R. Hughs, Secretary of State of the State of Texas, DO HEREBY CERTIFY that I am the duly appointed and qualified secretary of State of the State of Texas and, under and by virtue of the laws thereof, the custodian of its laws and the registrar of its public officers; and

THAT according to the records of this office, A. Macedo is Deputy County Clerk, Travis County, Texas, and is entitled to act in that capacity and to certify to instruments in that department.

Issuing Entity

Office of the Texas Secretary of State

Issued

July 31, 2018

Certificate Number

11949087

Example Apostille Certificate verified in a web browser using the Blockcerts open standard for blockchain-anchored digital records (https://www.blockcerts.org).

It’s important to note here that putting actual document data on a blockchain is not secure, because many parties have access to the ledger and can read it. So new technical standards were developed to cryptographically hide the data that is anchored to a blockchain in a way that no one can decipher from the ledger itself. These open source standards, called Verifiable Credentials and Decentralized Identifiers, make sure that no one’s privacy is compromised when using a blockchain to verify records. They ensure that there is no way to derive the contents of a record from the blockchain itself. However, if you have a file of the record, you can verify it against the blockchain using advanced cryptography.

Blockchain for Apostilles

Blockchain, when used in combination with the above open standards, enables a Secretary of State’s Office to issue digital versions of the Apostilles that can be verified independently of any vendor service—without needing to log into any database or look up any information. Thanks to blockchain technology, an Apostille can simply be scanned (using a QR code) or uploaded to a free, open source verification website for instant validation.

Best of all, the recipient of the Apostille can now store a digital version of their record in a private wallet on their smartphone, where they always have it at hand. They can share it with anyone by sending a link to it or by sending the Apostille file itself. And they can re-use the same digital record again and again; they don’t need to request a new Apostille every time the same document needs to be verified.

Imagine how much more convenient this is: not only is the record natively digital, but it’s easily portable and instantly shareable and verifiable anywhere in the world. It becomes much easier for people to keep track of their Apostilles and not lose them; it also dramatically lowers the time and cost of verifying the record, a process which today may take weeks or months. And the record is re-usable an infinite number of times, with no additional costs for sharing or verification.

Conclusion

Blockchain enables the creation of “self-verifying” or “self-attesting” digital records: files that can be stored, shared, and verified an unlimited number of times by anyone, anywhere in the world, with the highest level of security and integrity. Thanks to blockchain technology, recipients of Apostille records don’t need to rely on software vendors to create services (like online databases) to verify their records. They can simply hold the Apostille directly on their phone and then click a button to share it with anyone. That “relying party” can then verify it with the click of a button, or with a quick upload to a public utility like an open source verification website.

This empowers everyone—Secretaries of State, Notaries Public, other Governments, and Apostille holders—to conduct business quickly, efficiently, and at a much lower cost. In a post-COVID world, where digital business is the default standard, self-verifying records are poised to quickly gain widespread adoption.