# Looking for an Electronic Signature Solution?

## Here's a Key Capability You Should Demand

**jsign.com**
+1 (833) 717-1154

jsign

# Contents

# Why You Shouldn't Settle for **Anything Less than Blockchain**

If you're investigating electronic signature solutions for your business, you're probably focusing on factors such as affordability, ease of use, and whether the application can integrate into your existing workflow tools. Those are all valid considerations that should be on your checklist.

But in this paper, we'll argue for another characteristic you should be looking for as you research providers: **the use of blockchain to store and safeguard your eSignatures.**

You won't hear or read much about this technology from electronic signature companies—because almost none have figured out how to use it cost-effectively. But as we outline its unique capabilities below, you'll understand why blockchain should be the basis of any eSignature app, and why your business shouldn't implement one that doesn't leverage blockchain.

Nor do you need to take our word for it. Here's what the head of DocuSign, one of the world's largest providers of eSignature apps, said on the topic in December 2020:


*"We look at blockchain as an underlying technology that we think is actually quite intriguing." But "it is still too expensive for the kinds of things [our] company does."* [1]

**—Daniel Springer, DocuSign CEO**

We would take Mr. Springer's sentiment a step further. Blockchain is more than quite intriguing as an underlying technology for electronic signatures. It is the ideal mechanism for recording, securing, and storing the entire eSignature process. In the pages that follow, we'll demonstrate why.

Then we will introduce you to one company that has built an enterprise-caliber eSignature solution on the blockchain foundation—and offers its solution at a more affordable price than most of its competitors, including DocuSign.

First, though, let's briefly review what constitutes a legally recognized electronic signature. This description will prove relevant to our discussion below—because you'll find that satisfying the elements required for a legal signature also becomes far easier using blockchain.

# What Does the Law Require for **an Electronic Signature?**

Electronic signatures in the US are governed under the federal eSign (Electronic Signatures in Global and National Commerce) Act of 2000. According to the text of this law, several provisions must be met for a signature to be considered legally binding. The three most important for our discussion are:

**Signer intent.**
To meet the legal definition of an electronic signature, the eSign Act requires that the consumer (signer) "has affirmatively consented to such use and has not withdrawn such consent" to add a legally binding signature. [2]

**Record retention.**
The law also demands that a business capturing electronic signatures from consumers (or patients) "maintain electronic records accurately reflecting the information contained in applicable contracts, notices, or disclosures and that they remain accessible to all persons who are legally entitled to access for the period required by law in a form that is capable of being accurately reproduced for later reference." [2]

**Record integrity.**
According to the Performance Standards of the eSign Act, government regulators or auditors may "specify performance standards to assure accuracy, record integrity, and accessibility of records that are required to be retained." [3]

In other words, if you need to maintain electronically signed documents from customers or patients under your industry's data-protection regulations, the law requires your business to be able to prove your customers signed these documents willingly and with full knowledge that they were in fact created a legally binding agreement. The law also places the responsibility on your business to prove those records have remained secure and unaltered since your customers applied their electronic signatures.

Now let's review why blockchain technology is uniquely positioned to help your business meet these standards—and why it's the best electronic signature solution to support your operations in other ways as well.

# 3 Reasons Blockchain is **the Best Technology for eSignatures**

## 1. Providing your company with non-repudiation protection.

One of the most common concerns of businesses closing deals via eSignature is that a client or customer will later deny having signed the document. If you are not using the right solution to capture and store these records, your contract might not stand up to a challenge from a customer or their legal counsel.

The strongest protection against this risk is an electronic signature solution that provides non-repudiation—meaning the application captures enough verifiable data that it becomes essentially impossible for the signer to dispute the signature's authenticity and eSigning process later.

**Use case: financial services**
Let's say you're with an investment brokerage firm, and you need legally binding agreements from all clients giving your firm permission to access their accounts to execute trades.

Now let's imagine the worst: A series of equity purchases on behalf of a new client results in a significant paper loss to their portfolio, and the client decides to claim that they never authorized your firm to make the trades in the first place. If you have your

standard new-client agreement on file only as a PDF document containing a digital image of the client's signature, you could face difficulty withstanding that legal challenge. You still need a way to verify the signature is valid.

Blockchain provides a unique advantage here because the technology allows you to record every step of the signing process and store that data in a tamper-proof manner. Documents can be verified at a later time using the same system that applied that signature to the document and contains information about the signing process.

With the right solution, for example, you will be able to capture detailed data on each electronic signature—including timestamp, signer's device ID and IP address, even the latitude and longitude of the signing location. The application will then automatically store these digital records using blockchain's distributed and unalterable database structure.

**Bottom line: Blockchain-based eSignatures give you irrefutable legal proof of the authenticity your customers' signatures.**

## 2. Capturing and proving signer intent.

A related risk is that a customer or client challenges the legality of their electronic signature on the grounds that your business cannot prove you secured their consent at the time of the signing, or that you failed to offer them a chance to opt out of the signature process.

As we noted above, the eSign Act states that if a business cannot prove a signer's affirmative consent, the law might not recognize the electronic signature as legally enforceable.

With the right eSignature solution, you can capture your signer's intent to create a legally binding agreement in several ways. For example, you can include a mandatory button asking the signer either to confirm their consent to sign the document or to decline and opt out of the agreement.

You can also require the signer to check an affirmation text, such as an "I Agree" box acknowledging that by taking the requested steps, they understand that they will be adding a legally enforceable signature to the document.

**Use case: real estate**

Along with providing a good faith deposit, a client of your real estate firm electronically signs a document confirming their intent to move forward with the purchase of a home, provided the seller removes the listing from the market immediately while the parties complete the inspection, appraisal, loan completion, and other steps.

At some point in the process, however, your client decides to back out of the purchase. To retrieve their good faith deposit—which the parties agreed would be nonrefundable—your client claims they did not realize that the agreement you sent them to sign was legally binding.

Again, if your eSignature process consists simply of sending a PDF and asking your clients to drop in an image of their signature, the law might deem that agreement unenforceable.

Blockchain provides an added layer of protection here as well. As we noted above, the right eSignature app will allow you capture a timestamped record of every step your signer takes. This includes checking your "I agree" box, for example, acknowledging that they recognize they are creating a legally binding signature.

And remember, the right solution will also capture a wealth of data about the entire eSignature process—including your client's device ID and precisely where and when they signed. When you've collected all this data, including your client's affirmative steps to show consent, your blockchain-based eSignature app will then distribute this data to a private or external distributed network using the uniquely secure and tamper-proof nature of the blockchain digital ledger.

Now your firm has the irrefutable proof of your client's intention to sign the agreement accompanying their good faith money deposit. And thanks to blockchain, you can also prove that this record was stored securely and never altered from the moment your client signed it.

**Bottom line: Blockchain-based eSignatures allow you to prove a signer's knowledge of the legally binding nature of their signature—as well as their consent to sign.**

## 3. Achieving regulatory compliance with your customer records.

Implementing the right eSignature solution can streamline your operations and save your staff enormous time and frustration from having to manually gather customer signatures and securely store those documents.

But you also need to find out whether an eSignature provider's security protocols are sufficient to satisfy the privacy requirements of your industry's regulators. After all, those electronic signatures will in most cases be attached to documents containing highly personal, sensitive information about your customers or patients. The process your company uses to store and protect such documents could make the difference between compliance and noncompliance.

**Use case: healthcare**
Your medical practice maintains electronic records of numerous forms containing patients' personal health data and various administrative documents—along with signatures from both the patients themselves and other providers in their continuum of care.

Question: Does the eSignature process your practices uses to collect and store these electronic records meet HIPAA standards for patient data confidentiality and security?

Additionally, keep in mind that HIPAA—along with other industries' data-privacy regulations, such as SOX and GLB—demand not only the security of personal data but also the ability to quickly retrieve that data upon consumer request or to meet a regulatory audit.

Once again, blockchain offers unique advantages. First, it's important to remember that most federal data-privacy laws, including HIPAA, are intentionally vague about which systems and processes regulated businesses should use. Regulators expect businesses to identify and deploy the most sophisticated and proven data-protection solutions feasible. And few technologies have ever been demonstrated to be more secure or tamper-proof than blockchain.

Also, because blockchain-based data is broadcast to numerous, decentralized private or external networks, and every update to those sites is recorded in chronological order, it is impossible to alter an existing block of data in any way without creating a record of the update. From a regulatory standpoint, this means your practice will be able to demonstrate to auditors that your patient data is not only secure but that it has never been altered or otherwise compromised since your team placed it in secure electronic storage.

**Bottom line: Blockchain-based eSignatures give your company a method of storing and securing electronic records in a way that will meet even the strictest data-privacy laws.**

# jSign: **eSignature Solution Based on Blockchain**

With all the business, legal, and regulatory benefits of using blockchain to support your electronic signatures, you'd have more than enough reason to limit your search to apps to those built on blockchain technology.

But blockchain also offers many other operational improvements for your eSignature processes. In fact, blockchain is such a logical and compelling fit for businesses that need to regularly collect and store electronic signatures, it's unfortunate that most providers haven't yet found a way to implement the technology cost-effectively.

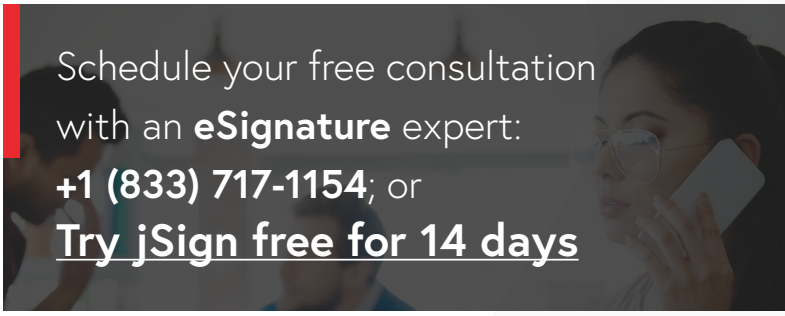
Fortunately, there is one eSignature company already offering such a solution that lets you capitalize on all these advantages of blockchain: jSign.

With jSign, your business can:

- ☑ Deploy a cost-effective, easy-to-use alternative to existing eSignature solutions.
- ☑ Leverage the security, accessibility, and regulatory compliance of blockchain technology.
- ☑ Sign, send, track, and collect eSignatures in minutes.
- ☑ Receive certificates of completion when recipients finish signing documents.
- ☑ Integrate eSignature capability into your other apps, such as Salesforce or your EHR.
- ☑ Access signed documents anytime from an intuitive cloud management portal.
- ☑ Maintain full audit trails of signed documents, including timestamps and signers' locations.
- ☑ Capture signatures on many file types, including PDF, DOC, PPT, and others.
- ☑ Set signature reminders and due dates for every document.
- ☑ Upload directly from Google Apps, One Drive, Dropbox, and other file management apps.

**About jSign**

Part of the Consensus Cloud Solutions family (NASDAQ: CCSI), jSign is a leading eSignature provider for heavily regulated businesses. The only solution of its kind built on blockchain technology, jSign offers businesses a simple, highly affordable eSignature platform with enterprise-level capabilities—including certificates of completion, full audit trails, non-repudiation protection, and fraud prevention.




**References**

1. *Quartz Media: The simple reason DocuSign doesn't use blockchain*
2. *FDIC.gov: Summary of the Electronic Signatures in Global and National Commerce (eSign) Act*
3. *GOVINFO.gov: Full text of the eSign Act*