

# AdaSign

Signing and storing legal documents at Cardano

Migamake Pte Ltd

June 9, 2022

## Contents

<b>Problem statement</b>	<b>2</b>
<b>Summarize your solution to the problem</b>	<b>2</b>
<b>Summarize your relevant experience</b>	<b>2</b>
<b>IMPACT</b>	<b>2</b>
Please describe your proposed solution . . . . .	2
Please describe how your proposed solution will address the challenge?	4
What main challenges or risks do you foresee to deliver this project successfully? . . . . .	4
Acquiring customers . . . . .	4
Competition with other document signing solutions. . . . .	5
<b>FEASIBILITY</b>	<b>8</b>
Please provide a detailed plan and timeline for delivering the solution.	8
Please provide a detailed budget breakdown. . . . .	8
Please provide details of your team members required to complete the project. . . . .	9
<b>AUDITABILITY</b>	<b>9</b>
Please describe how you will measure the progress and the development of the project? . . . . .	9
What does success for this project look like? . . . . .	10
Please provide information on whether this proposal is a continuation of a previously funded project in Catalyst or an entirely new one.	10

## Problem statement

In the era of businesses, jobs and meetings conducted remotely with no physical contact; we need an easy way to upload legal documents in distributed yet reliable way, allow to sign them by involved parties in a controlled and secure manner, and then store them and share to involved parties.

## Summarize your solution to the problem

The dApp allows uploading any document, storing it in a distributed environment (IPFS storage), and signing it with a digital signature by defined participants.

## Summarize your relevant experience

Migamake is a company specializing in high-performance Haskell projects, including parsing, data summarization, and blockchain services.

Our developers have already participated in Cardano development.

Some projects of Migamake are on [company page](#).

This [StreamCardano.com](#) project was accepted in Fund8.

Website/GitHub repository (if relevant): <https://adastamp.com>

## IMPACT

### Please describe your proposed solution

The application will allow uploading a document of any format. It will be stored on IPFS, and pinned by IPFS service (e.g. [Storj IPFS Pinning Service](#)) for a period of time (in years) specified in a parameter, with the ability to further extend it as required by the local archive policy.

Then, the document owner will specify (by entering or choosing from an address list):

- a list of users (Cardano wallets or just e-mail addresses) who are to sign off the document,
- a list of users (e-mail addresses) who will be notified as soon the document is signed by all parties.

Each signer will be notified of the document to be signed by the StreamCardano notification service. If a user were specified by e-mail address, the application would allow him to connect to the existing Cardano wallet or create a new one. Then, each signer will be able to sign off the document, and the signature will be stored on the blockchain. If necessary, all signers will be able to sign off the document simultaneously at the same time, for example, when participating in

an online meeting with a notary, allowing the notary to immediately check the validity of the signatures.

The legal validity of a signature will be established if the signing wallets have passed a KYC procedure provided by [Blockpass solution](#). The procedure will include:

- verification of the authenticity of the customer's identity document,
- validation of the customer's name and date of birth against data printed on the identity document,
- face match with the identity document photo.

The KYC policy will not require an AML check, as document signing has no relevance to possible money laundering. AML will be optional since a signer may accept payment upon signing a document (see later). A user will have to perform KYC just once and then can use the verified Cardano wallet when signing documents. The signature stored on the blockchain will include (encrypted) basic data of signers (first name, surname, no. of identity document, and date of birth) so that users with granted access to the document will know by whom it has been signed. According to [Blockpass vendor](#), the price of KYC is "starting at \$1.0 per individual screen".

As soon as all signers have signed off the document, users from the second list will be notified by the StreamCardano notification service that the document has been signed.

We establish special support for signing PDF documents, which is the most often used form of electronic legal documents. A signature made by a signer and stored on Cardano can be inserted into the PDF document itself as a visual signature. This will produce a self-contained PDF with a signature, which will be the same signature as the one stored on Cardano. A user may use either the source, an unsigned PDF together with a Cardano signature, or a self-contained PDF with an embedded signature.

For organizations that sign large numbers of documents of the same content, differing just in personal details, the solution will offer the ability to prepare a document template - a document with predefined content and fields to be filled automatically with, e.g. personal data. As personal data of multiple signers will be given, e.g. in a CSV file, the solution will generate a separate, personalized PDF document for each signer (similarly to the mail-merge function in word processors does) and will automatically start a signing process for it (including necessary notifications).

Another feature significant for large organizations is signing workflow, which will include:

- defining order of signers,
- allowing specific signers to make decisions (e.g. approve or reject the document),

- Choosing a workflow path depending on certain conditions based on document contents (for example, contracts with a value exceeding a given amount must be additionally signed by the CEO),
- making a payment at a certain step of the workflow (e.g. when a delivery protocol has been signed by both parties),
- calling a specified smart contract at a certain step of the workflow.

The solution will consist of the following:

- a smart contract that manages signatures of documents,
- decentralized document storage on IFPS,
- a frontend application that allows uploading and sign-off documents,
- a notification service running on [StreamCardano](#), sending e-mail notifications related to document status.

Each signing workflow will be implemented as a separate smart contract that embodies and codifies the specific workflow rules. The solution will include a framework for developing such smart contracts, i.e. a smart contract generator that will generate the smart contract code based on a configuration file that specifies the order of signers, as well as possible human and automatic decisions and actions.

### **Please describe how your proposed solution will address the challenge?**

We will allow the transformation of organizations' bureaucracy into blockchain with tamperproof permanent record and cloud storage of the signed documents. This would radically simplify the bureaucracy by enabling the signing and storing of legal documents in a distributed and remote environment, in compliance with legal regulations. The advanced features of the solution (document templates, workflow) will be especially useful for large organizations that produce large numbers of documents of the same content (differing just in personal details), which are processed in the same way (e.g. standardized contracts for telecommunication, electricity and similar services). Such organizations will save tons of time on bureaucracy related to preparing and processing such documents.

### **What main challenges or risks do you foresee to deliver this project successfully?**

#### **Acquiring customers**

There is a risk of a lack of customers using the solution. There is a need to publicize the solution and its potential use cases. Especially acquiring one or several large and well-known organizations would boost the market appearance of the solution. Therefore we left a significant adoption and transformation budget in order to publicize the solution and acquire customers.

### **Competition with other document signing solutions.**

There are well-known solutions that allow signing documents both online and offline, with which our solution will compete.

One of the most widely used solutions is Adobe Acrobat's built-in functionality to sign PDF documents. It requires a certificate - to be compliant with legal regulations and be accepted by courts, it has to be an Advanced or Qualified Electronic Signature (AES or QES), as defined by eIDAS (electronic IDentification, Authentication and trust Services) European Union regulation, and United States' UETA Act and E-Sign Act. One of the nice things is that the signature is stored within the PDF document that is being signed and can be rendered on the document. However, there is no storage of documents nor sharing/transferring between participants. On the contrary, AdaStamp offers storage and sharing of documents but does not allow for visible signatures inside a document.

There are also commercial solutions available which are already integrated with blockchain, like [DocuSign](#). In this solution, only the document signature is stored in a blockchain (currently only Ethereum), and the solution does not support storing nor sharing/transferring the document. One needs to have a copy of the document to verify the signature: "Anyone with a copy of the agreement can check it against the blockchain-stored evidence to verify the copy's integrity against the original DocuSigned file." AdaStamp offers added value to DocuSign and similar solutions by allowing storage and sharing of documents that are to be signed.

Another significant competitor is [HelloSign](#). It is the most advanced solution that includes integration with Dropbox (and thus allows to store signed documents), visible signatures, signing workflow and document templates. So this solution exceeds AdaStamp functionality. However, it is a proprietary solution of one commercial vendor, not yet integrated with any blockchain (the vendor performs some [research](#) in this direction, but it is not yet integrated within the product).

[Scrive](#) is another advanced competitor with features similar to HelloSign, that include storing documents, notifying involved parties, visible signatures, document templates and forms. It even stores signatures in [Guardtime] blockchain solution. But again, it's a proprietary vendor's solution, especially when it comes to document storage.

[PandaDoc](#) is a complex, unified solution for signing documents, which allows preparing document templates and forms to be filled by converting existing PDF or Word documents or even by creating them from scratch in a visual environment. A template may include text fields to be filled by a signer, as well as signature placeholders that specify locations of signatures. Documents are stored in a proprietary format in PandaDoc's own storage. The solution notifies signers by e-mail and allows them to define the signing order.

Below is a comparison of AdaStamp's proposed solution and leading competitors.

9

Feature	AdaStamp	PDF embedded (Adobe)	DocuSign on Ethereum	HelloSign	Scrive	PandaDoc
Compliant with legal regulations and be accepted by courts	Yes, if the signing wallets have passed a compliant KYC procedure	Yes, with QES	Yes	Yes	Yes	Yes
signature visible in a document	Yes (M2)	Yes	No	Yes	Yes	Yes
storage of documents	Yes	No	No	Yes	Yes	Yes
Sharing of documents, notifications, etc.	Yes	No	No	Yes	Yes	Yes
Signing workflow	Planned for M3	No	No	Yes	Yes	Yes
Document templates, filling forms	Planned for M2	Yes	No	Yes	Yes	Yes
Open-source solution	Yes	No	No	No	No	No

Feature	AdaStamp	PDF embedded (Adobe)	DocuSign on Ethereum	HelloSign	Scrive	PandaDoc
Distributed, non-proprietary storage	Yes	N/A (no storage)	N/A (no storage)	No	No	No

## FEASIBILITY

**Please provide a detailed plan and timeline for delivering the solution.**

M0 (technology teaser) - 1 month from project start:

- signing a local file with Cardano CLI,
- storing the signature on Cardano blockchain,
- verifying signatures.

M1 - 3 months after M0:

- document storage on IFPS,
- document retrieval,
- document signing,
- e-mail notifications,

M2 - 2 months after M1:

- KYC,
- address list
- document access rights

M3 - 2 months after M2:

- signature visible in PDF,
- document templates, mass generating, signing and storing of documents,

M4 - 3 months after M3:

- customizable workflow
- smart contract generator
- calling another smart contract
- pay as you sign

**Please provide a detailed budget breakdown.**

Software production (including analysis, development, testing, deployment, documentation and project management) and maintenance:

- M0 (technology teaser) - 21K
- M1:
  - basic functionality, user and wallet management - 16K
  - storage and retrieval of documents, signing documents, verifying signatures - 56K
  - open source library support for JSON Web Token authentication using Cardano Wallet, including forwarding credentials from another application - 15k\$
- M2:
  - address list - 12K



- access rights to documents - 25K
- extend document storage period - 7K
- perform KYC - 5K
- M3:
  - sign-off PDFs - 28K
  - document templates, mass generating documents from templates - 15K
- M4: smart contract generator for workflows - 86K
- Software maintenance (6 months) - 24K
- Support of deployment of workflow apps (6 months) - 24K

Software production size and cost have been estimated using [COSMIC Function Points method](#).

Marketing and promotion:

- project website - 2K
- speeches at 9 conferences - 104K
- content marketing - articles and translations - 24K
- social media ads and posts - 11K
- producing and sharing viral - 50K

Subtotal software production and maintenance: 319K

Subtotal marketing and promotion: 191K

Total: 510K

**Please provide details of your team members required to complete the project.**

TODO

## AUDITABILITY

**Please describe how you will measure the progress and the development of the project?**

Development progress will be audited by:

- commits to our open-source GitHub repo,
- using an open-to-the-public, well-established agile management tool (Jira or similar) to:
  - manage sprints,
  - assign, manage and deliver tasks,
  - gather, manage and solve problems, bugs, etc.
- publishing documentation.

KPIs:

- number of signatures made,
- Number of documents stored,
- Number of registered users,
- Number of generated smart contracts that realize specialized workflows.

### **What does success for this project look like?**

After M1: the solution is used by individuals and small organizations to sign off and store legal documents. The signature is being recognized as compliant with legal regulations and (with KYC passed) as an equivalent to AES or QES.

After M3: the solution is successfully used by at least one large organization to automate their standard document workflows.

### **Please provide information on whether this proposal is a continuation of a previously funded project in Catalyst or an entirely new one.**

This is a new, redefined approach to our [earlier proposal](#).