*Developer in Residence:*
Juan Mescher, Leandro Manzanal y Mario Zito

# Identicon

24th April 2022

## OVERVIEW

**Identicon is our proposal for a trustless verification protocol providing "proof of life" and "proof of identity" for “real people” in the NEAR Network.** It uses a set of decentralized and random selection of human nodes (citizens) which will produce the “on-site” and “off-chain” verification of the solicited proof of identity or proof of life.

More detailed information can be found in: Identicon Network Draft

Our plan is to use it to solve a use case with high social impact: the requirement of pensioned people in Argentina (may be other places too) to fulfill a “proof of life” test (or “fé de vida” as is generally called) every single month to get access to their pension funds (centrally controlled by ANSES: a government institution which manages them for more than seven million people).

Additionally to this use case, the protocol opens the door to a whole set of use cases (such as providing verified KYC in Defi dapps) and may be used by other Dapps in NEAR which require some proof of identity, proof of existence, or proof of compliance.

Key performance indicators:

- A fully functional and documented protocol API, for the referred use case.
- A fully functional and tested MVP Website and Dapp, for the referred use case.
- A minimum of ten (10) initial validators to bootstrap the protocol.
- A minimum of ten (10) verifications done after bootstrapping.

**Short term (DiR) risks:**

- Because all of our team is currently working in full time paid jobs now, eventual work spikes may disturb or delay our weekly objectives. *We will compensate this with weekends overtime or by redistributing team work if this happens.*

- Though all of us are highly committed and trained senior engineers, full time paid jobs and other life pressures may make it unsustainable for some of us to keep up with the proposed timelines. *We will have to compensate with overtime the loss of one team member, or adjust the project deliverables, but because of the limited time (three months) we don't envision this to happen.*
- Technical risks: because the protocol is not yet fully designed, we may encounter some technical challenges (such as external storage, calling external APIs, async contract calls, wallet integration with mobile, dapp and extra node hosting) which may delay some decisions or implementations.
- Acquiring the first validators and subjects to verify may be a non-technical but demanding task.

**Long term (full project) risks:**

- The need to be recognized as a valid "proof of life" by the banks which control the pension funds. This may be easier in privately owned banks, but much more complex in state owned banks (Provincia, Nación).
- It is not yet clear for us who will pay the verification costs: The people to be verified (or their families) ? The banks which control the pensioned accounts ? ANSES ? This risk may be mitigated if we have enough funding at public bootstrap.
- We need to reach ample public diffusion so that people know how to request the verification.
- We will have to provide extra security measurements to validators and requesters to assure that malicious third parties don't "fake themselves" as validators and commit frauds to requesters.
- The interaction of the general public with a wallet and also a way to pay for verification in fiat currency may be an important limitation.
- Also the NEAR wallet has no Spanish translation, so this may be a problem for public adoption.
- The project needs to acquire a certain number of validators in a short period of time, so that verification work can be performed in time and across some initial geographical zone.

- Building a fully working and legally recognized DAO (involving possible investors, the dev team and validators as active members with governance rights) will require a careful and evolving process with legal risks and challenges.

## Target Audience

*Clearly define your target audience*

Our target audience are pensioned people (and their families) who need to fulfill every month a “proof of life” in order to get access to their pension funds, controlled by a paying bank. Their pressure may be the driving force for banks and government institutions to use the service, and recognize the proof as valid.

Banks may be another target audience, as the service may mitigate the risk of lost funds due to fraud and other causes (such as funds of a dead person being used by some other person in control of the account, which generate an irrecoverable loss to banks).

## Objectives

DiR objectives:

1. Define and implement a trustless verification protocol (as a set of smart contracts over the NEAR network) which will allow to uniquely bind physical persons and assets to their digital counterparts, by performing proof of life, proof of identity, and other proofs of existence and proofs of compliance.
2. Analyze a set of possible use cases which can benefit from this protocol, and define protocol requirements for them and (possible) phases needed to accomplish full potential.
3. **Define a clear, easy to use, and documented API for potential users of the protocol so they can integrate it into their own Dapps.**
4. Build a MVP dAapp for the first selected use case: “proof of life” verification. The Dapp must include the ability to request and pay for the verification, allow new validators to register in the pool of validators, report their results and receive their payment,
5. Define and implement a Decentralized Identifier for the verified Identity, following DID-spec-near/DID-Method-NEAR · GitHub.

6. Define and implement a **soulbounded, non-transferable NFT for each “proof of life” verification**, which can act as a digital certificate for banks and institutions.

## Why this project

Tell us why is this project important to you

The "digital interface" between us and the real world implies that in many cases we really don't know who we are interacting with. Is this person who he/she says he/she is ? Is he/she a fake ? Is he/she alive ?

This lack of knowledge has also a whole set of implications in the OpenWeb, such as knowing and identifying contributors, clients, avoiding rug pull and scams. The list of frauds increases day by day allowed by the lack of identity on projects and the people who operate them.

We think that providing solutions to this problem will result in anticipated social and identity fraud detection, preserving reputations, generating huge savings in lost funds, and avoiding many other social and economic losses.

### Our first use case

In developing countries (such as Argentina) assessing people identities (proving they are who they say they are) and assuring they are still alive (*proof of life* or "*fe de vida*") is a demanding and recurring need both for governments and all type of organizations (ONG, Social Orgs, Cooperatives, Banks, etc).

In many cases this verification implies access (or, if lacking, denial of access) to his/her pension  funds, social assistance, health or housing and other social impacts.

But, in many cases, the people that need to be verified can not use any of the given methods. Old age, physical incapacities, no way to displace themselves, no access to technology or incapable to use it, are some (but not all) of the reasons.

And even when governments and organizations put an increasing effort in this, it is still an open issue, with the consequence that many assigned government funds don't reach the people who really need them in an efficient and equitable way.

Please see this article: Fe de vida de jubilados: ANSES precisó qué bancos no la piden y dio detalles del trámite | Un requisito que complica a los beneficiarios | Página12. We have captured some of the most meaningful comments on this doc: Fe de Vida

***Solving this problem in a transparent, secure and fully accountable way will have a high social impact on the life and well being of some million people every month.***

***It can also provide a small (but sustainable) extra income (or even full time jobs if the project is highly successful) to the citizens who may act as validators, or who take part in the managing DAO.***

We also think this can be a valuable addition to the NEAR protocol, as it:

- Will allow thousands of new accounts to be created in NEAR, both for people to be verified and for validators which will take the job of on-site verification and on-chain registration.
- It will generate a high number of transactions on NEAR, as each validation takes at least seven transactions (one request, three verifications, and three payments), though this may be optimized to decrease total fees per full verification.
- It will showcase the full power and scalability of NEAR with its high TPS and very low fees, because thousands of people will need to be validated every month across the country over a very short period of time (five to ten days).
- It will provide a verification protocol and API which can be used by other developers to request/delegate verification: a common requirement in many dApps (such as KYC in Defi, verified goods and service providers in marketplaces).

## What will you do

Tell us in detail what this project is about and what the success of this project looks like.

We will build:

**A whitepaper describing the proposed verification protocol: what it is, why it is needed, how it works and potential use cases,** and (if time permits) a landing page for the protocol.

**A smart contract which implements the described protocol,** including (but not limited to) the methods:

- *`request_verification`*: Registers the new request in the blockchain and assigns validators to verify it.
- *`cancel_verification`*: When the requester cancels the request for some valid reason.
- *`assign_validators`*: When the request is filled, we must select a number of validators at random from the validators pool, and assign them to the request.
- *`register_as_validator`*: The NEAR account owner registers itself as a validator.
- *`unregister_as_validator`*: Used by some validator to unregister from the network.
- *`pay_validators (private)`*: After reception of all the validators results, we must pay each of the validators the corresponding compensation (0.x NEAR). Validators which did not complete the verification will not receive payment.
- *`report_verification_result`*: Report the result of the verification. If the verification was not possible, or the validator will not do it then the validator must include a descriptive cause.
- *`evaluate_results`*: Every time we receive a verification result we must evaluate if all verifications have been done, and which is the final result for the request. While the verifications are still in progress, the request state is Pending.
- *`get_verification_transactions`*: Return the set of verification transactions done on a particular subject.
- *`get_all_verifications_history`*: Get the set of all verification transactions filtered by some criteria. Needed by institutions which may request verifications on multiple subjects.
- *`mint_proof_of_life_cert`*: Emit a soulbound, non-transferable NFT for the approved verification. The NFT should be bound to the subject DID.
- *`get_my_assigned_verifications`*: Get the set of pending assignments of a particular validator.
- *`get_my_verifications_history`*: Get the set of all verifications performed by a particular validator.

**A fully documented API for the mentioned contract**.

**A website for the service** which will allow people to request the “proof of life”, be informed of the requests they made and also allow them to pay for the service (not in fiat, but with their NEAR wallet). Also motivate potential validators to register for doing work in the service.

**A dapp for the validators for capturing results and reporting them.** Also will keep them notified of current assignments, and when payments have been processed.

## How will you do it

Tell us how are you going to implement this project

As a general methodology note, all team members will be involved in each of the phases and its tasks. We consider this to be important because, as we are all involved in full time outside jobs, we can give each other support when some of us are required by external events, and cover each other without impacting delays in the project. It also implies that all of us will be current on the project status at any time.

This does not imply that each of us will not have some main roles and areas of responsibility (aligned with our areas of expertise), which will be clearly defined in Phase 1.

**Phase 1:**

We will include a first stage of service and product analysis and documentation, including the product requirements, off-chain and on-chain required services and APIs, features and goals.

We have some questions we need to answer here:

- Analyze a number of other possible use cases for the protocol, so we can be sure we can provide a useful verification protocol for NEAR, and usable by other third parties.
- Define params for the protocol (such as number of validators, validators selection strategy, approval criteria, etc) which may vary for different use cases.
- How are we going to provide Identity proofs to other interested third parties, once someone is verified (such as NFTs, etc) and how are we going to store identity data taking into account privacy concerns.

- Should validators be fully anonymous ? If that is the case, how can we avoid multiple accounts with the same validator ? Or must they also be verified in order to be accountable for malicious actions ? How can they be anonymous to the full network but still accountable ?
- Should we pay validators a fixed price or can validators compete for a certain verification, so validators closer to the subject will give a lower quote ?
- Can we provide an easier way of creating the NEAR wallet when first registering as a requester or validator ? Can we fund the wallets with a minimum initial amount to simplify onboarding ?
- Architecture for allowing easy inclusion of future use cases (one contract, additional contracts, etc), without impeding a rapid development for the first use case.

The deliverable will be a White paper, a Product Requirements Document and a (Trello) Roadmap for the next phases of development detailing tasks and goals.

We estimate this phase to take up to two (2) weeks.

**Phase 2:**

Next we will focus on smart contract development using RUST. Though we have a naive implementation for the contract (https://github.com/identicondapp/identicon), many aspects of that implementation must be reinforced (such as security).

NOTE: this phase may require some additional development or use of an off-chain API (for example, for finding a subset of validators geographically closer to the subject), but it is not clear yet how it will be done (Phase 1 will clarify this point).

We think this will take most of our time, since all our team members are new and inexperienced in RUST, and we also find here an excellent opportunity to learn it while doing so.

The deliverable will be a documented API for the contract, the developed controntract installed in Testnet,  and a set of unit tests and end to end test cases.

We estimate this phase to take up to four (4) weeks.

**Phase 3:**

After that, and having a working contract and API, we will focus on the product website, including the already mentioned features for requesters and validators.

The site will include the following features:

- Information describing the service: what it is,  why,  how it works, cost of the service, and how it can be requested.
- Tutorials (how to create the wallet, how to request the service, how to pay for it, etc) and FAQ for additional questions.
- A “call to action” and form for requesting the “proof of life”. If he/she is a first time user this form must also onboard them by creating their wallet, and after that will ask for the subject data (national doc, names and surnames, address, age, and may be other required info). If he/she is not a first time user, he will login using the wallet and this information must be also prefilled.
- A “call to action” and form for registering new validators. This form must also onboard them by creating their wallet, and after that will ask for the validator data (national doc, names and surnames, address, age, and may be other required info).
- A section for people who have requested their “proof of life” to get the certificate and send it to the bank who asked for it. Also a way to access previous certificates.
- A validators section enabling them to download/access the validator dapp.

We plan to use React/Nextjs with ChackraUI for this development, as it is one of the most used frontend JS frameworks, and some members of our team have experience using it and in frontend development and Javascript.

We will find/buy some “nice” templates to simplify the website design and obtain a site with good UX and clear design.

Because this is an informational site, we must provide faq and help files informing requesters and validators of how to use the service, cautions, etc. So our roadmap for this will be:

- Create the site architecture and navigation structure.
- Create the site content (pure text, no web design or graphics here).
- Create faqs and helpers for the site.

- Select templates which match the content architecture (we can adapt to the template visuals here).
- Develop the site using the given template and content (this will be a static site).
- Develop the interactions with the contract API and NEAR wallet.
- Write E2E tests.

NOTE: we will use only the NEAR wallet for login, so all activity in the site must be conducted using a NEAR account, but we may request mails or mobile phone number when registering (in the future we may message the subject or the validator using SMS or Telegram).

This is a critical path for the project, as it will be the public face for the project, and (mostly) all functionality will be finally tested here.

The deliverable will be a fully functional website compliant with the Product features and requirements defined in Phase 1. We will include (some) E2E testing using Cypress on the main site functions.

We estimate this phase to take up to three (3) weeks.

**Phase 4:**

Finally, we will implement the validators Dapp, specially designed to facilitate the validator workflow. It includes the following features:

- The app will be accessible as a Launch button from the website.
- Login to the dapp using the NEAR wallet. This identifies the validator and enables/disables other features in the Dapp.
- A home page with two sections: a worklist section (with all pending verification tasks assigned to the logged in validator), and a history section (with all verifications already completed by the validator, including its payment status).
- A verification form page (partially filled with the subject data), which will be completed by the validator and dispatched when the verification is completed. This will be a signed transaction using the NEAR wallet. This form will be linked to the worklist items.
- A read only view page for already completed verifications, with data taken, payment status and final verification status (from all validators). This view page will be linked to the history items.

- A preferences page for some settings such as font-size, dark/light mode and may be some additional options.

We plan to use React/Nextjs with ChackraUI for this development.

This will be a single page app with a simple navigational structure (Home page, Preferences page, Verification form page, Verified view page)

The deliverable will be a fully functional dapp for validators compliant with the Product features and requirements defined in Phase 1. We will include (some) E2E testing using Cypress on the main dapp functions.

We estimate this phase to take up to three (3) weeks.

## MILESTONES-

### Milestone 1:

When: Week 2

Deliverables:

- Protocol white paper
- Product Requirements Document (PRD)
- (Trello) Roadmap for the next phases

### Milestone 2

When: Week 6

Deliverables:

- Documented API for the contract
- Fully developed contract installed in Testnet
- Set of unit tests and end to end test cases.

### Milestone 3

When: Week 9

Deliverables:

- Fully functional website compliant with the PRD

- E2E test cases  on the main site functions using Cypress.

**Milestone 4**

When: Week 12

Deliverables:

- Fully functional dapp for validators compliant with the PRD
- E2E test cases  on the main dapp functions using Cypress.

## Team

Tell us about your current team if any or future team roles that you may require

The team is formed by Leandro Manzanal, Juan Mescher and Mario Zito. The three of us are committed Senior Engineers with more than ten years (each) in software development, and support and operation of enterprise software, deployed both in-house and on the cloud. All of us have completed both NCA and NCD certifications.

We may require for a latter phase of the project some help from a UX/Web designer, and also help from communications people to create an official website, landing pages and educational and marketing materials.

## Key Assumptions

Tell us about your key assumption that you have taken into account to ensure the success of this project

Key assumption is that all three team members will be part of a funded DiR, so we can focus our time in developing the project without other considerations, or distract ourselves with extra work on other projects.

The other key assumption is that, even if the “proof of life” use case fails (for political or economic reasons, not technical ones), the work done and the implemented protocol will be useful for an ample number of other use cases.

## Why will this fail

Tell us the reasons and factors which will lead to the failure of this project

On the team side:

- Failure of one of the team members to fulfill the committed time to the project will obviously result in delays, but may be attenuated or even solved depending on some other factors.
- Failure of two team members will surely make it impossible to carry it to an end.

For the selected use case (proof of life), there may be economical and political reasons which may make it fail, or at least not extend to a wider audience:

- Lack of integration with fiat payments may be a general user blocker.
- Banks or institutions not willing to pay for the service.
- Customers (or their families) are not willing to pay for the service.
- Political reasons, such as not having been done by a government team.
- Other companies "lobbying" for a gov contract to develop a similar solution.

### Project Roadmap after the fellowship

Post DiR objectives:

1. Bootstrap the protocol and Dapp with a limited number of validators and requesters on the Mainnet to demonstrate the solution to the general public, in a restricted geographical area.
2. Analyze and integrate the possibility of payment in fiat currency, besides using the NEAR wallet.
3. Prepare educational and marketing materials and (if necessary from the previous step) improve the UX so it can be easier to use and more attractive to the general public.
4. Create a DAO which will provide the verifications services and find funding for it so we can acquire validators, increase the number of verifications, and spread the word about the solution to a wider audience.
5. Work with banks and institutions so they can accept the "proof of life", and convince them to pay for it for its pensioned customers.
6. If steps 3 and 4 are successful, operate the DAO and extend it to the whole territory.

7. Lastly, extend the protocol to other use cases.

## **Compensation** (in USD to be paid in NEAR Tokens)

What are your expectations of compensation for your work?

We expect each team member to commit 20 hours a week of development time, for a weekly compensation of 500 USD per team member.