

Proof of Evolution.

Draft 0.1, October 2026

Draft. Sections marked Planned describe a design that does not run yet.

18 October 2026

1. Abstract

Proof of Evolution is a passport of a person's path in crypto. It is built only from facts that anyone can check: on chain history first, exchanges and deals between people later. It needs no name, no documents and no biometrics, and it cannot be bought, sold, transferred or reset. Each fact carries the transactions that prove it. Open, versioned rules turn facts into branches and warning levels; there is no single total score. A hash of each record is planned to be attested on Solana and signed by Noventia, so anyone can check it. This draft describes the data model, the first rule pack, the warning levels, attestation, privacy, the threat model and the rollout. Stage 2 runs today: a fact collector for Solana and passport cards for public wallets. Everything from stage 3 on is design.

2. Problem

Ecosystems, funds and projects spend large budgets on grants, incentives and airdrops. Each program sees only its own slice of history: its own recipients, in its own window. What the same wallets did before and after a distribution is outside its view. A program cannot easily tell a builder who stayed from a wallet that sold on the first day and moved on to the next program.

People have the opposite problem. A person with a long, clean history has no portable record of it. To prove anything, they either hand over identity documents or make claims that nobody can check.

Proof of Evolution addresses both with one record: facts that anyone can verify, owned by the person they describe, readable by others only with permission.

3. Design goals and non-goals

Goals

- **Facts only.** Every fact has a proof that anyone can open. If a fact cannot be proven, it is not recorded.
- **Owned by the person.** A passport cannot be sold, transferred or reset, by anyone, Noventia included.
- **Checkable by anyone.** A fingerprint of every record lives on Solana. Planned for stage 3.
- **Read only with permission.** A public card for everyone, private branches that the owner opens.
- **Open rules.** Rules are pure, versioned functions. The same facts and the same thresholds always give the same result.
- **One core for every source.** Seven primitives cover every product planned. A new data source adds an adapter and a rule pack, never a new primitive.

Non-goals

These are red lines.

- **No custody.** Noventia does not hold user money and has no access to it.
- **No single score.** There is no total score per person. Branches and four warning levels only.
- **No KYC.** No names, ID documents or biometrics.
- **No own chain.** Everything runs on Solana.
- **No signals.** No investment advice and no trading signals.
- **No automatic “scammer” label.** Facts and the four warning levels only.

4. Data model

Status: In progress

Every product is a combination of seven primitives. Their types exist in the engine today. Code that uses them is written only for what the current stage needs: subjects of type wallet, facts from Solana and the first rules.

Primitive	Meaning	Key fields
Subject	Who or what has a history	<code>subjectId</code> , <code>type</code> (<code>wallet</code> , <code>person</code> , <code>project</code> , <code>org</code> , <code>agent</code>), signed links between subjects
Fact	Something that happened	<code>factId</code> , <code>subjectId</code> , <code>kind</code> , <code>value</code> , <code>source</code> , <code>observedAt</code> , <code>proofs</code>
Promise	A signed commitment with conditions and a deadline	<code>promiseId</code> , <code>subjectId</code> , <code>terms</code> , <code>signature</code> , <code>startsAt</code> , <code>endsAt</code> , <code>status</code>
Rule	Open, versioned, pure function from facts and promises to branches, warnings and promise status	<code>ruleId</code> , <code>version</code> , <code>inputs</code> , <code>outputs</code>
Case	A dispute with evidence, decided by the council	<code>caseId</code> , <code>subjects</code> , <code>evidence</code> , <code>status</code> , <code>decision</code>
Permission	Owner consent: who sees what, until when	<code>grantee</code> , <code>scope</code> , <code>expiresAt</code> , audit log of views
Attestation	Fingerprint on chain, signed by Noventia	<code>hash</code> , <code>version</code> , <code>rulesVersion</code> , <code>sasAccount</code>

A wallet subject has the id `wallet:solana:<address>`. A fact id is `<kind>:<signature>:<part>`, where the part is the mint or the transfer index.

5. Facts and proofs

Status: Live

Adapters

Every data source is an adapter. An adapter reads one source and emits facts with proofs, nothing else. It never computes a card number or a level.

The Solana adapter is the only one today. It reads the full history of a wallet through Helius Parsed Events on the free plan¹, cross-checks token accounts through standard Solana RPC, and finds the pools of launched tokens through the public DexScreener API. It emits five kinds of fact:

Kind	Value	Proof
<code>solana.firstTransaction</code>	<code>blockTime</code>	Earliest transaction
<code>solana.tokenCreated</code>	<code>mint</code> , <code>program</code> , <code>blockTime</code>	Create or mint initialization transaction
<code>solana.tokenMovement</code>	<code>mint</code> , <code>direction</code> , <code>kind</code> , <code>rawAmount</code> , <code>blockTime</code> , <code>counterparty</code> , <code>inLaunchTx</code>	The transaction
<code>solana.liquidityRemoved</code>	<code>mint</code> , <code>blockTime</code>	Removal transaction paying the token to the creator
<code>solana.latestSwap</code>	<code>mint</code> , <code>pool</code> , <code>blockTime</code>	Newest swap of the token

Paid endpoints replace the free sources only after a paid plan is bought. The adapter boundary keeps that switch from changing any rule.

No proof, no fact

A fact without a transaction behind it is not recorded. The proofs of a card number are the proofs of the facts it used, so a reader can open every one of them in an explorer.

If the collector reaches a read limit or a rate limit, it stops with an error. It never produces a card from a partial history.

Chain data is hostile input

Token names, symbols, descriptions, links and metadata are written by anyone. The first step after reading a transaction keeps only base58 addresses and signatures, integers and short machine labels. Names never reach a fact, a card or a log, and links in metadata are never fetched. Cards use fixed words only.

6. Rules

Status: Live

Rules are pure functions: facts, thresholds and the current time in; card numbers and a warning level out. Rules never read the network, the clock or the config. Every result records the rules version and the thresholds version that produced it. The plan is to publish the rules and the engine as open source; no stage is set for it yet.

Worked example: the stage 2 rule pack

Card rules version 2 and thresholds version 2. N is 72 hours and X is 50%, both confirmed on 18 October 2026.

Fact	Definition
<code>onSolanaSince</code>	Timestamp of the wallet's earliest transaction
<code>tokensLaunched</code>	Pump.fun: tokens where this wallet is the creator in the create instruction. Other tokens: this wallet is the initial mint authority in the mint initialization. The fee payer alone does not count
<code>tokensAlive</code>	Launched tokens with at least one swap in the last 30 days. Proof: the latest swap transaction
<code>liquidityPulls</code>	Launches with liquidity removed by the creator within N hours of launch
<code>firstDayDumps</code>	Launches where the creator sold at least X% of their own allocation within 24 hours. Own allocation: tokens received in the launch transaction plus any mint to the creator in the first 24 hours. Every sale in the first 24 hours counts, including tokens bought after launch. With no own allocation the fact is "not applicable" for that launch
<code>movedOutFirstDay</code>	Launches where the creator transferred at least X% of their own allocation to other wallets within 24 hours. Never counted as a sale
<code>longestHoldMonths</code>	Longest time the creator held their own token without selling it all, where "all" means below 1% of the peak balance

The warning level follows from those numbers:

- **Level 3, high risk:** at least one launch with a liquidity pull, or first day dumps in at least 2 launches.
- **Level 2, warning signs:** exactly one first day dump, or any move out on day one.
- **Level 1, little history:** a wallet younger than 90 days or with fewer than 3 launches, and nothing from level 2 or 3.

One event never makes level 3, except a liquidity pull, the clearest proof on chain.

Example A. Example wallet, illustrative data. First transaction on 14 March 2022; 3 launches, all alive; no liquidity pulls; no sales or moves on day one; longest hold 14 months. The wallet is older than 90 days and has 3 launches, so level 1 does not apply, and no level 2 or 3 fact exists. The card shows no warning.

Example B. Example wallet, illustrative data. First transaction on 28 August 2026; 5 launches, 1 alive; liquidity pulled in 2 launches; sold on day one in 2 of 5 launches. One launch had no dev buy, so the day one facts leave it out. Both level 3 conditions hold, so the card is high risk and says “The owner can appeal to the PoE council”.

Stamps

The 3 most recent launches each get a stamp: “Launch, {Month YYYY}” with the value “Liquidity pulled”, “Alive” or “No swaps in 30 days”. A wallet with no launches gets one stamp: “On Solana since {Month YYYY}”.

7. Warnings, cases and the council

Status: In progress

A warning is always shown with the facts behind it and the right to appeal.

1. **Little history.** A new address with few facts. Not a negative.
2. **Warning signs.** Set by the rules, with the facts listed.
3. **High risk.** Set by the rules only under strict open rules with clear proof on chain.
4. **Confirmed fraud.** Only after review by the PoE council. The owner is told first and can answer first.

A complaint never switches on a label by itself. It opens a case. The evidence in a case is facts with proofs. One case does not end a passport; patterns matter. At the start, Noventia acts as the council. Cases and appeals are planned for stage 5. Until then, appeals go to support@noventia.app.

Evaluation at later stages

Branches built from deals and vouches follow these rules:

- Only kept promises count: events where something was at stake and the result can be verified.
- A person can rate someone only after a real deal with them.

- The weight of a rating depends on the rater's passport and the size of the deal.
- Rings of passports that only praise each other get no weight, in the style of EigenTrust².
- Vouching puts the voucher's own passport at risk.
- Growth is limited by time. Recent bad behavior weighs more, and old behavior fades slowly.

The launch order is fixed: facts from the chain, then deals, then vouches, then the council.

8. Attestation

Status: Planned, stage 3

A hash of the facts and the result of a record is written through the Solana Attestation Service and signed by the Noventia key. The attestation holds the hash, the record version, the rules version and the Solana Attestation Service account.

Key handling. The signing key lives in Google Cloud KMS, and only one service can use it. The public key is published on noventia.xyz when attestation starts.

How anyone verifies.

1. Take the facts and the result of a record.
2. Compute their hash.
3. Compare it with the hash attested on Solana.
4. Check the signature against the published public key.

The web passport runs this check for its reader.

Checking a card

Status: Planned, stage 3

Every card carries a QR code and a short code. Both open noventia.xyz/verify, which reads the attestation from Solana, checks the Noventia signature and shows whether the card matches. The MRZ gets a check digit derived from the attestation hash, so a copied or edited card fails the check.

Independent verifiers that recompute every record and sign it too are planned for stage 6.

Stage 2 cards carry no attestation and show no hash.

9. Privacy and permissions

Status: Planned, stage 4

A passport has a public card that anyone can see, and private branches that the owner opens when they choose. A permission names who gets access, to what, and until when. Every view of a private branch is logged, and the passport owner can see the log.

Where	What
On Solana	A hash of the facts and the result, the branch levels, the rules version and Noventia’s signature
On Noventia servers	The facts with their proofs, wallet links and permissions
Nowhere	Names, documents, seed phrases, private keys

Rules that hold today, before permissions exist:

- Cards are made only for wallets that their owners made public.
- Reports on many wallets publish totals only. No single wallet is named unless it belongs to the project analyzed or its owner made it public.
- Personal data is never sold.
- Noventia’s own products get no data or rules that partners cannot get through the same API.

10. Threat model and known limits

Status: In progress

Wallet farms. One actor controls many wallets to collect a distribution many times. Reports measure farm clusters: recipients funded from the same source within a short window. This is a heuristic, labeled as such, and it can be wrong. A passport also limits growth by time, so a new wallet cannot buy a history.

Praise rings. Groups that only rate each other. Ratings need a real deal, their weight depends on the rater's passport and the deal size, and rings get no weight in the style of EigenTrust. Planned with the deals branch.

Selling through a second wallet. Not caught. The card shows a move out on day one, never counted as a sale. The list of exchange deposit addresses is empty at stage 2, so transfers to exchanges also count as moved out.

False positives and appeals. Level 3 needs clear proof on chain, and one event is never enough except a liquidity pull. Complaints never switch on a label. Only the council sets confirmed fraud, and the owner answers first.

Key compromise. The signing key lives in a key management service that one service can use. If an incident happens, access and keys are revoked first, the incident is reported in plain words, and then the cause is fixed. An incident is never hidden or quietly patched.

Hostile metadata. Token names, symbols and links are never displayed as HTML, never fetched and never executed. Cards use fixed words only.

Unconfirmed data shapes. Some parts of the Helius data are not yet seen on a launching wallet: Pump.fun trade instruction names, how a mint initialization names the mint authority, which DEX programs are summarized as a liquidity removal, and how a new mint appears in token transfers.

11. Rollout

Status: In progress

The order of stages is fixed.

Stage	What
0. Decisions	The decisions and the vision are approved. Done
1. Sites (current)	New noventia.xyz and noventia.app
2. Test (current)	Fact collector, cards for 5 public wallets, one airdrop report
3. Atom	Indexer, rules engine, web passport, free wallet check, attestation
4. First money	Reports for projects and funds, developer panel, permissions, Pro
5. Council and deals	Cases, appeals, the council, fund panel, public API
6. Token and platform	Token (legal entity and white paper first), more chains, verifiers

Current stage: 1 and 2, in parallel.

12. Token

Status: Planned

No token exists. Not before 2027, and only after proven retention, a community and legal clarity. A legal entity and its own white paper come first. A token never buys or changes a passport.

This website does not constitute an offer to sell or a solicitation of an offer to buy any tokens.

13. Open questions

- The hash function and the exact encoding of a record for attestation.
- The rules for branch levels at stage 3.
- Whether the Noventia ID becomes a stored field of its own at stage 3, instead of being derived from the app account.
- The sources for the list of exchange deposit addresses.
- How independent verifiers are chosen at stage 6.

1. Helius, Parsed Events documentation: <https://www.helius.dev/docs/parsed-events>. The free plan allows Parsed Events at 10 credits per request with up to 100 transactions per page. [Back](#)
2. Kamvar, Schlosser and Garcia-Molina, “The EigenTrust Algorithm for Reputation Management in P2P Networks”, Proceedings of the 12th International World Wide Web Conference, 2003. [Back](#)

Appendix A. MRZ format

The machine readable zone (MRZ) is the band at the bottom of a card. It has two lines of exactly 44 characters each. Only **A** to **Z**, **0** to **9** and **<** are allowed. Lines are padded on the right with **<**.

Line 1

POE<SOL<NVT{ID}<<{ROLE}

- **{ID}** is the Noventia ID without the **NVT-** prefix.
- **{ROLE}** is the holder role, with spaces written as **<**.
- When the wallet has no Noventia ID: **POE<SOL<UNCLAIMED<<{ROLE}**.

Line 2

{FIRST 8 OF WALLET}<<SINCE{YYMMDD}<<LAUNCH{N}<ALIVE{N}<RUG{N}

- **{FIRST 8 OF WALLET}** : the first 8 characters of the wallet address.
- **SINCE{YYMMDD}** : the date of the wallet’s earliest transaction.
- **LAUNCH{N}** : tokens launched.
- **ALIVE{N}** : launched tokens alive.
- **RUG{N}** : launches with a liquidity pull.

A line longer than 44 characters is cut on the right.

Example

From the clean example card. Example wallet, illustrative data.

```
POE<SOL<UNCLAIMED<<ANONYMOUS<BUILDER<<<<<<<<
DEMOCXEA<<SINCE220314<<LAUNCH3<ALIVE3<RUG0<<
```

The wallet is not claimed, the role is “Anonymous builder”, the wallet starts with **DEMOCXEA** , its first transaction was on 14 March 2022, it launched 3 tokens, all 3 are alive, and none had a liquidity pull.

Appendix B. Glossary

Adapter. A module that reads one data source and emits facts with proofs, nothing else. See Data sources and adapters.

Alive. A launched token with at least one swap in the last 30 days.

Attestation. A fingerprint of a record on Solana: a hash of the facts and the result, written through the Solana Attestation Service and signed by Noventia. Planned for stage 3.

Branch. One part of a passport, built from one kind of source, with its own facts and level. The Solana path is the first.

Card. One page of a passport, made from the public history of one wallet whose owner made it public.

Case. A dispute about a passport, decided by the PoE council. Planned for stage 5.

Check digit. A character in the MRZ derived from the attestation hash, so a copied or edited card fails the check. Planned for stage 3.

Council. The body that decides cases and is the only one that can set level 4, confirmed fraud. At the start, Noventia acts as the council.

Day one. The first 24 hours after a launch.

Dev buy. On Pump.fun, the tokens the creator receives in the launch transaction.

Example data. Data made up to show how something looks. Always marked “Example wallet, illustrative data”.

Fact. Something that happened, recorded with its source and its proofs.

Launch. A token this wallet created: on Pump.fun, the wallet is the creator in the create instruction; for other tokens, it is the initial mint authority.

Liquidity pull. Liquidity removed by the creator within N hours of launch (N is 72 hours).

MRZ. The machine readable zone: the two 44 character lines at the bottom of a card. See MRZ format.

Moved out on day one. A launch where the creator transferred at least X% of their own allocation to other wallets within 24 hours. Never counted as a sale.

Noventia ID. The passport number: **NVT-** followed by 6 uppercase letters and digits.

Own allocation. The tokens a creator received in the launch transaction, plus any mint to them in the first 24 hours.

Passport. The record of one person’s path in crypto, built from facts. It cannot be bought, sold, transferred or reset.

Permission. The owner’s consent: who sees what, until when. Planned for stage 4.

Proof. A verifiable reference behind a fact. On Solana, a transaction signature.

Rules version. The number of the rule set that made a card. Today: card rules version 2.

Sold on day one. A launch where the creator sold at least X% of their own allocation within 24 hours.

Solana Attestation Service. The Solana service that holds attestations.

Stage. One step of the fixed rollout order. See Status and stages.

Subject. Who or what has a history: a wallet today, later a person, project, organization or agent.

Thresholds version. The number of the threshold set a card or report was made with. Today: version 2.

Verify page. noventia.xyz/verify, opened by the QR code or the short code on a card. It reads the attestation from Solana, checks the Noventia signature and shows whether the card matches. Planned for stage 3.

Warning level. One of four levels: little history, warning signs, high risk, confirmed fraud. Not a score.

Appendix C. Document changes

Version 0.1, 18 October 2026

- First public draft.
- Covers the data model, the stage 2 rule pack (card rules version 2, thresholds version 2), warnings, attestation, privacy, the threat model and the rollout.