Nown: What is Nown?

Anonymous
nown.to github.com/nownto/nown

Abstract: A peer-to-peer protocol for portable trust between strangers. Built from eight concepts.

1. Keys

- Every participant acts through a public/private keypair.
- The public key is the account others know and the anchor for its record.
- The private key proves control without being revealed.
- Public-key cryptography lets others verify control without seeing or holding it.
- Keys are property, kept, transferred, or sold.
- One person may hold any number of keys.

2. The record

- One public, append-only, permanent record.
- Independent nodes hold and serve it, so there is no central store and no single point of loss.
- Ordered by block time, a public clock no participant controls.
- It holds karma marks and seals, and nothing else. A dealing is never written to it.
- A reader learns what a key has done without learning anything about the doing.
- Anyone may verify it.

3. Karma

- Karma is a key's score on the record: the sum of its marks, tied to the key, not to any platform.
- Anyone can compute it from the public record, and two readers reach the same figure.
- A dealing ruled correct writes a mark up, one ruled incorrect writes a mark down, and only a recorded mark moves the score.
- A mark is a mark. Karma is not fractionable, and there is no limit in either direction.
- Karma is minted, never moved: nothing is taken from anyone to write a mark, and karma is never staked, escrowed, or transferred.
- A key at zero confers nothing. It can receive a mark from a key that carries karma, and it can give none, so empty keys write nothing to each other however often they deal.

4. Dealings

- A dealing is any exchange a key puts something behind, and it is the only kind of entry there is.
- Both keys agree everything before it opens: the outcomes, the oracle, and whether a quorum may be called.
- Money is voluntary: a dealing that carries money is the same object with deposits attached.
- Between two keys a dealing has three possible rulings: a mark up for both, or up for one and down for the other, either way round.
- A deadline that passes with no attestation and no verdict closes the dealing as correct for both.
- The marks are written once, at the close.

5. Oracles

- An oracle supplies the fact an interaction depends on, and the parties name it before they deal.
- The parties may settle by mutual agreement.
- If they disagree, or if the dealing called for it at creation, a quorum decides between the outcomes agreed before the dealing.
- Those two, the parties and the quorum, are the only oracles.
- A panel with no power over the event is a witness, not an oracle.
- The ruling is enforced by consequence: where money rides, signing the ruled path is the last act of the dealing, and a party who refuses has failed a dealing.

6. Quorums

- A panel of strangers of high karma, called for one case, each free to answer the call or decline it.
- Eligibility is karma above a bar that moves with the network, and every key tests it privately against its own record. No list of the panel exists anywhere.
- Signing is seating: a steward signs every outcome his seat can have at the moment he accepts, and the stewards sign the oracle side together.
- The evidence reaches him encrypted, and it opens only for a key that was called and took a seat.
- Each steward privately picks one of the outcomes the dealing fixed, commits his choice, and opens it after the deadline, so no one can read a running count.
- The outcome most of the opened choices carry is the verdict, and it is final. A steward who matches it takes his bond back, a bounty out of the fee, and a share of the bonds forfeited by the seats that missed; one who misses it, or stays silent, forfeits his bond to the seats that matched.
- The panel is one side of a dealing and each steward is the other, so every steward deals with a part of himself, one share in the total size of the quorum.
- The quorum decides the outcome, never takes custody of the funds, and writes nothing to a steward's key.

7. Seals

- A seal is what someone else certified about a key: a credential, membership, ownership, authorship, or another attestation.
- Issued by a key, or ratified by a quorum where no single signer can carry the fact alone.
- A seal is a dealing, so its outcomes are fixed at issuance and a challenge calls a panel to pick one.
- No seal lands without the subject's countersignature. A denied certification marks the issuer alone.
- A seal mints karma from nothing, and nothing caps how many a key may issue or hold: an issuer is read through the keys he sealed.
- Every seal is permanent, and a seal meant to lapse carries its ending inside it: a voiding mark appended at a stated block, which a reader sees as a term that has run.

8. The application layer

- Every conforming application computes the same karma from the same record.
- The application decides how to filter and present the record.
- Metrics live here: Karma DOT is a key's score divided by its age plus a settling constant, the density of dealing over time.
- The constant is what keeps a key one block old from outranking every veteran, and it keeps the division from breaking at a key's first appearance.
- Gates live here too: reading a record as a bar for access or eligibility, an oracle only in a figurative sense.
- Client-side rules never change the record or the karma beneath.