Nown: A Peer-to-Peer Protocol for Portable Trust and Merit-Based Arbitration

Anonymous
nown.to github.com/nownto/nown

v0.4 Released into the public domain (the Unlicense)

Abstract: Trade between strangers needs trust before the trade and judgment after it. Markets supply both through a trusted third party: a platform, an escrow agent, a rating bureau, a court. That party can be censored, bribed, subpoenaed, or shut down, and it owns the reputations and verdicts it issues. This protocol removes it from both functions. Reputation, called karma, is earned through costly action and carried between contexts. It proves baseline trustworthiness to any stranger: no introduction, no identity document, no platform. Disputes are decided by a quorum of high-karma accounts drawn at random, anonymous to the traders and to each other, judging only the evidence each side submits. The quorum is an oracle. It attests a verdict that a pre-signed escrow executes; it never holds the funds. Honest judgment is made the paying strategy by the structure of the reward, not by appeal to a higher authority, because there is none. There is no company, no token, and no owner. The protocol charges nothing and rules on the trade, never on the person. It cannot be proven in advance. Its worth is a market question, answered by adoption.

1. The problem

Two strangers agree to trade. Each must decide whether the other will perform. If one defects, someone must decide who is owed what. Today a trusted third party makes both decisions.

Each such party is a single point of control. A platform censors, extracts rent, and dies by regulation. A named arbiter can be bribed, coerced, or subpoenaed, and carries the legal liability alone. A rating bureau owns your reputation and rents it back to you. A vote weighted by tokens sells influence to whoever buys the most. Reputation built on one platform stays there and vanishes with it.

Judgment is the function that has not been decentralized. Settlement of money became trustless once it was made objective and replicated. Judgment resisted, because a verdict is a preference with no sum to check it against. Here judgment stays subjective. The protocol makes honest judgment the paying strategy and removes each party that could be captured.

2. Karma

Karma is a reputation a person earns and carries: one measure of demonstrated trustworthiness, readable at a glance without a name, location, or past. It does for trade between strangers what a credential does inside an institution. A degree says a stranger was taught to behave. Karma says a stranger has behaved.

Karma is the product; dispute resolution is one use of it. Actions move it up or down: a settled dealing, a vouch that holds, a case judged well add to it; a defection, a broken vouch, a careless verdict take it away. Its standing spends wherever trust is priced: buying, selling, borrowing, hiring, joining a community with an entry threshold. A platform that reads karma gains a user base expensive to fake and cheap to filter, with no central moderator. The reputation belongs to the person, not the platform, and travels when the person leaves.

Karma is held by no one. It is computed from a public record of signed events, as a balance is computed from a ledger. Two accounts praising each other in a closed loop earn nothing: the measure is trust flowing in from the rest of the graph, and an isolated ring has no inflow.

Everyone must derive the same number, or the number is an opinion. Each event is signed by its actor, stamped against a public clock no participant controls, and appended to a log whose past cannot be rewritten. The weights that turn the log into karma are fixed by the protocol version, not by an administrator, so every client that replays the log derives the same standing for every account. Replaying the whole log is heavy, so anyone may post a bond and publish the totals as a signed summary. The summary is a convenience, never an authority. A client that recomputes any slice and finds a discrepancy proves the fault from the log itself; the publisher's bond is forfeited and the summary discarded. Disagreement is settled by arithmetic, not by standing.

How far an action moves karma is set by five factors, each a curve, not a fixed amount. The change scales with what the actor put at risk. Each further unit from the same source is worth less than the last, so no single stake or relationship can be repeated into dominance. The whole sits under a ceiling set by tenure, which no money lifts. A dealing with a fresh, independent party counts for more than another with a familiar one. Inflowing trust is weighted by the standing and independence of its source, so trust routed through a captured cluster arrives discounted. Standing earned broadly and slowly compounds. Volume bought quickly does not.

3. The costly signal

A rating that costs nothing to give is worth nothing. Speech is nearly free, and a man may say one thing and do another. Action expends scarce time or capital and reveals, irreversibly, what the actor valued at the moment of choosing. What he paid for is who he is.

A choice that costs something is the only evidence of a preference. So karma moves only on paid-for acts. Completing a trade under bond, standing on a verdict, vouching for a stranger: each costs something the actor cannot recover, and each is worth recording. A profile description, a self-endorsement, a free rating: each is speech, and moves karma by nothing.

Giving karma costs the giver. A vouch stakes your own standing on another account; if that account is later judged a fraud, your stake is cut. A vouch is a demonstrated preference, priced in the one currency that cannot be printed: reputation that took real time to earn.

Endorsement is rationed. Each further vouch within a period costs sharply more than the last, so one sincere vouch is cheap and a hundred are not. A fraud is charged back along the edges that endorsed it, so a careless voucher pays for the account he certified.

4. The price of a signal is time

If the only cost were money, the protocol would fall to whoever holds the most. Money is a poor measure of commitment for the same reason it is a poor measure of a man.

Time is the honest price. No one can buy more of it. A day costs the wealthiest attacker and the poorest honest user the same, and neither can purchase a longer past. Time cannot be run

in parallel inside one identity: a computation that takes a year takes a year on one machine or a million, a fact that can be proven rather than assumed.

Karma is therefore bounded by tenure. Standing accrues only as real time passes with the account in good standing, measured against a public clock no participant controls. Money enters as one input, held at risk and with sharply diminishing effect: capital buys a fast start, never a commanding position. A wealthy attacker reaches the ceiling the buyable inputs allow within a day, then waits years under the same clock as everyone else. The remaining advantage is seniority, not wealth, a milder bias that dilutes as the network grows.

5. Escrow

A verdict must move funds or it is only an opinion. Handing the funds to whoever enforces the verdict restores a trusted party at the last step. The protocol splits the problem instead. Judging the dispute is subjective and left to the quorum. Checking that the quorum ran correctly is objective and left to arithmetic anyone can repeat.

Funds sit in a two-of-two output controlled by the buyer and the seller alone. It holds the price and both parties' deposits, and its outcomes are signed in advance. If both agree, at the start or on completion, they close it cooperatively and the quorum is never called. If the trade stalls and no dispute opens, a timeout returns the funds. Either party alone may open a dispute by a signed opening that consumes the escrow, so the timeout can no longer execute. A dispute may be opened only up to a fixed margin before the timeout matures, sized so a case opened at the last valid moment still concludes first; a later opening is void and the timeout stands. A dispute is not a freeze. The parties hold the only keys, and the cooperative close stays open until the verdict signs; most disagreements end when both sides face the cost of judgment. Settlement before the panel is drawn costs nothing more. After it, the pre-posted fee pays the work already begun: the parties may buy back their dispute, never the stewards' time. Failing agreement, the funds move by exactly one of the pre-signed verdict outcomes, buyer paid, seller paid, or funds returned, each completed only by the quorum's single signature over its verdict. Failing every verdict, a pre-signed default becomes valid after a generous delay, described with the deadline. Funds can wait. They cannot be imprisoned.

The quorum attests and never holds. It cannot take the funds, cannot freeze them, and owns no key to the escrow. The two traders are the only signers, so no third party has custody and no custodial liability arises.

A verdict can rule only on facts that reach the record. A forged image of a bank transfer, against a claim that nothing arrived, no one can judge. The protocol therefore handles disputes over facts that can be shown: proof of payment, delivery committed to a hash, a signed carrier receipt. Claims resting on a private, reversible rail wait for a proof that can be checked.

6. The quorum

A dispute empanels a quorum: an odd number of accounts, called stewards, drawn from those above a karma threshold and several steps from both parties in the trust graph, so that no one who knows either trader can sit. Stewards are anonymous to the traders and to each other. They never speak. Each reads the same case file, the evidence and statements both sides submit, and votes alone.

These filters assume a populated graph. In a young network they can empty the pool: with few accounts above the threshold, everyone is near everyone. The protocol degrades openly. While the eligible set is small, the required distance from the parties relaxes on a schedule fixed in advance, and

the bound on how much may sit in any escrow tightens in proportion. Both traders see which regime they trade under before they commit. As the graph grows, the filters return to full strength and the bound lifts. Weak protection disclosed is a price a young network can choose. Weak protection disguised would be a fraud by the protocol itself.

Within a case the quorum holds all the power. There is no judge to overrule it and no court of appeal. The absence is deliberate. Every arbitration system before this one ends at an authority that can be captured. The protocol puts in that place a crowd no one can find, bribe by name, or coordinate, and takes its verdict as final. Finality is itself the value: a dispute settled once, in days, is worth more than one litigated for years. An appeal path was considered and left out, because any right to reopen a case invites the patient and the rich to grind the poor into surrender.

Each side states its case and submits evidence under the sealed procedure of the next section, and the quorum decides on that record alone. Some people argue better than others. The protocol does not correct for this. It weighs the case as presented, as any reader of evidence must.

7. The case file

A verdict is only as good as its record, so the record is built under one discipline: seal first, unveil second. Neither side composes its evidence with the other's in view.

When a dispute opens, a sealing window begins. Within it each side reduces every exhibit it will rely on to a fingerprint: a short value computed from the exhibit, the case, the submitting side, and a fresh random blind, which commits to the exhibit exactly and reveals nothing. The side publishes, signed on the public record, the ordered list of its fingerprints and their count, nothing more. The opponent learns only how many exhibits exist. Each fingerprint is bound to the case and to the side that sealed it, so neither side can adopt the other's fingerprints and ride on its unveiling. Sealing first removes the forger's chief advantage: a document invented to rebut an exhibit must be invented before the exhibit is seen, against a case still unknown.

When the sealing window closes, an unveiling window begins. Each side publishes every sealed exhibit in full, with its blind, onto the same record. An exhibit is admitted only if it opens its recorded fingerprint exactly. Unveiling is all or nothing: a side that unveils fewer exhibits than it sealed, or fails to open one, has its whole submission struck and is judged as if it had submitted nothing. There is no holding back a surprise after seeing the other hand, and waiting within the window buys nothing, since a side can unveil only what it sealed.

Because the exhibits themselves enter the record, not merely their fingerprints, the case file is one public object. Whether a submission stands or is struck is a pure function of the record at the close of the window, so every observer reaches the same answer. Every steward reads the same file, and the verdict is signed over the file's own fingerprint, so the signature names exactly what was judged. A party cannot show one version to some stewards and another to others; there is only the record. What is unveiled stays public, so a party strips from its exhibits, before sealing, whatever it is not prepared to have read by anyone. Both parties know that price when the trade is formed.

Submissions are bounded: a fixed count of exhibits, a fixed size for each, a fixed total, and a written statement under a fixed length. The bound makes full publication cheap and denies the tactic of burying a panel under volume. What the bound cannot hold is probed, on a grave case, by the written questions the quorum may put to both parties, described with the verdict; the answers join the file under the same discipline, sealed then unveiled in full, within their own windows.

Silence carries defaults. A side that seals nothing, or fails to unveil, loses standing to contest. The panel judges the record that remains, and the remaining side must still carry its own claim: an unopposed claim is not thereby proven, and the unresolvable ballot stays open. If neither side

produces a valid submission, the funds return, as in an abandoned trade. The quorum attests that outcome, and confirming that the record holds no valid submission asks arithmetic of it, not judgment.

The draw of the quorum opens only after the unveiling window closes. The file is complete and immutable before a single steward exists, so there is no panel to tailor a packet to and no steward to reach before the record is fixed. Each steward's client lays the exhibits before him in an order drawn from his own private selection, so a file built to steer its reader cannot count on the sequence in which it is read.

8. Sortition

The quorum must be unpredictable before it is drawn and unknown after, or it can be bribed, threatened, or packed. Randomness from an outside committee would restore a trusted party, so the randomness is taken from the protocol's own activity.

Every account carries a seed that changes as it acts. Each action folds a committed trace of itself into the seed at the moment it happens, on an append-only log, so the trace cannot be altered or chosen after the fact. The seed is the account's irreversible history, reduced to entropy.

The order of events is fixed so that timing buys nothing. A dispute opens with a signed record on the log naming exactly one escrow. The first such record for an escrow is the only one that counts, and the mark under which the public clock receives it fixes the moment of opening. Eligibility is frozen there: the karma threshold, the distance from both traders in the trust graph, and the cluster caps are all evaluated on the ledger as it stood then. Nothing done afterward changes who can be drawn.

The entropy for the draw is collected only after the case file has closed. A window of fixed span opens at that close, and the seeds of accounts that act inside it are combined into one value. The disputants' own actions are excluded. If too few independent clusters contribute, the window extends by fixed steps, a bounded number of times, and the draw then proceeds with what has arrived.

The combined value alone is not safe. The last account to act inside the window could try many actions and keep the one that steers the draw, and the party who opened the dispute could choose a quiet hour and supply the window's activity himself. So the combined value, joined with the opening record and the clock's mark upon it, is passed through a delay function: a computation that takes a fixed span of wall-clock time to run, an instant to check, and that no amount of parallel hardware can hurry. The clock's mark did not exist when the opening was chosen and is set by a process no participant controls, so even a party who supplies every action in the window commits each act before the input is complete. The delay runs longer than the window can extend, so no one, not even a machine started the moment the window opened, holds the output before it has closed. Its output is the seed for the draw.

Each eligible account then checks privately whether it was selected, by evaluating a verifiable function of the seed under its own key. Selection proves itself and reveals nothing about the others. An account learns only that it was drawn, and can prove that fact without naming itself. The set that decides a case is a group of pseudonyms that exists for that case alone, unknown to the traders, to each other, and to the operators of any relay. There is no list to subpoena and no colleague to conspire with.

Anonymity of the drawn is only as strong as the messages that reach them. A case file addressed to its panel would name the panel to whoever carries the message, so nothing is ever addressed. The case is published once, to everyone, and every eligible account fetches every case, so fetching

reveals nothing. Ballots and shares return through the same open channel, uniform in size and cadence, and accounts not drawn post traffic of the same shape, so sending reveals no more than fetching. A drawn steward acts under a key created for that case alone. The tie to the account behind it is never published. Pay, penalty, and standing settle later by proofs that name no seat, described with the verdict. The carriers of messages are assumed hostile. They can refuse to carry, and the protocol routes around refusal by using many. They can watch, and see only that everyone fetched and everyone spoke. There is no roster of any panel, held anywhere, at any moment.

No randomness of this kind is perfectly unbiasable, and this is not. The delay function rests on a bound on how fast the fastest hardware can run it. The draw can be skewed only by an actor who both dominates the activity in the window and holds a decisive speed advantage over everyone else. The design drives that margin small enough that skewing a draw costs more than winning the dispute it would decide. That is the standard the protocol holds, in place of a proof of the impossible.

Three further rules keep the draw clean. First, if a panel fails to fill, there is no second roll. The seed fixes, once, an order over every eligible account, and the panel is filled from the front of it. A drawn account takes its seat by acting under its case key within a fixed span. A seat never taken passes to the next account along the same fixed path, at no penalty, because a silence no one can tell from not being drawn cannot be priced. Commitment begins at the claim, and seats already taken do not move, so an absence shifts exactly one seat, to a successor settled in advance. Neither stalling nor engineered silence can shop for a friendlier panel. Second, a dispute may be opened only up to a fixed margin before the escrow's timeout matures, so the time a party can sit on a grievance, waiting for the eligible set to drift his way, is bounded by the life of the trade. Third, the share any single trust cluster can hold, of the eligible set and of the panel actually drawn, is capped, so a group that certifies itself cannot pack a quorum however large it grows.

9. The verdict

The quorum does not find the truth. No crowd can, and the protocol makes no such claim. It aligns the reward with honest reporting, and lets the honest report win.

Only the stewards who land with the majority are paid. Those in the minority are not. A steward who votes without reading gambles against everyone who read, so the paying move is to read the evidence, judge it, and expect others who read to judge as he does. Payment for agreement, with a penalty for lazy or dishonest votes, makes honest attention the profitable strategy.

Plain majority reward has a known failure. A panel can measure agreement and nothing else, so it pays a good guess about the crowd as it pays a good judgment of the case, and a steward may vote for the obvious answer instead of weighing the evidence. The protocol prices this strategy out, and asks the steward nothing beyond his verdict. A steward serves a batch of cases and is scored across all of them: not for agreement alone, but for agreement above what his and the others' voting habits would produce by coincidence. A fixed answer, a coin, or any rule that ignores the evidence agrees only by coincidence and earns nothing over the batch. Reading is the only strategy that pays, whatever the others do, a guarantee that holds across many cases and never on a single one. A verdict also follows the steward who cast it. Later quorums can find it wrong at his expense, so the profitable vote is the one that survives the judgment of people not yet drawn, and no reading of today's crowd reveals what that is. Votes are sealed until all are cast, and there is no deliberation, so there is no channel to coordinate through and no shared error to amplify.

Two defenses hold the vote honest under pressure. Ballots are sealed, and only the counts ever open, never a single vote. And the panel grows with the stake, few stewards for a small claim and

many for a large one, so the pay for reading always clears its cost and no large sum rests on a handful.

A seal requires an opener, and an opener is where a trusted party would hide. The protocol appoints none. The panel opens its own tally. When a quorum forms, its members jointly build a key for the case, each holding a fragment. The whole key never exists, so there is no holder to subpoena and no machine to tap. The same ceremony builds the key behind the verdict signature, so the seal adds no authority the verdict does not already require.

A ballot is the steward's answer, sealed under the joint key and signed under his key for the case. Sealed ballots add without opening: combined, they yield a sealed count for each answer, and each ballot carries a short proof, checkable by anyone and revealing nothing, that it holds one valid answer. When voting closes, anyone can form the sealed counts. The panel opens the counts and nothing else. Each member contributes its fragment of the opening with a proof that the fragment is honest, so a false fragment is caught at once and a withheld one names its owner, who pays by the same rule as a withheld share of the verdict signature. The counts become public. No single ballot ever does.

A steward may replace its sealed ballot before the close, and the last cast is counted. Every ballot is sealed freshly, and stewards re-post at random moments as ordinary behavior, so a replacement that changes the vote and one that changes nothing look the same to any watcher of the record. A coerced steward complies under observation and defects in private, and nothing on the record betrays it. What the seal cannot survive is its owner. A steward who proves its sealed vote to a buyer, or hands over its key and secret, has sold the vote outright, a limit stated with the others at the close.

The seal rests on a stated bound. Members holding enough fragments could, together and off the record, open a single ballot as easily as a count. The number required is therefore a majority of the panel, so the coalition that could break the seal is the coalition that already writes the verdict, and it faces the same answer either way: error in unison is punished toward the whole of the stake, and a majority that completes the escrow signature against its own opened counts acts on the record and pays as a bloc. One arithmetic edge is stated plainly. A unanimous count reveals every vote by subtraction. No design conceals a panel that agrees completely, and a briber who buys unanimity to read ballots has bought the verdict at full price, in the open, under the heaviest penalty the protocol carries.

Scoring opens nothing further. Each sealed ballot is also a binding commitment, so once the counts are public every seat's score is fixed: a stated function of the hidden vote and the open totals, one rule for every seat. The steward collects from a fresh key tied to nothing it has used, by a proof checked against the public record and revealing nothing else: that it holds one of the case's sealed ballots, that the hidden vote sits with the majority, and a ticket, derived from the ballot's own secret, spendable once. Two claims from one seat collide on the ticket, and the proof names inside itself the key it pays, so no seat collects twice and no watcher can redirect a claim. A case pays each majority seat one equal share; the pool divides among the claims standing at the deadline, at most one per ballot, and an unclaimed share rolls forward. The record shows that some seat collected, never which. Claims travel the channel ballots travel, uniform in shape, each posted at a client-drawn random moment inside a stated window, so the hour of a claim names no one.

The batch's judgment rides on the bond, not the pay. The bond locked at seating is fixed by the panel's tier, the same for every seat, so nothing posted there measures the account behind it. It returns along one road: a proof of the same kind that the seat's agreement above coincidence, a sum of hidden votes against open totals, clears the stated bar. A claim that spans a steward's seats declares none of them: it ranges over every ballot settling in the window, shows how many seats it covers and nothing of where they sat, one ticket for each, so the crowd it hides in is the whole

settlement. A clean seat proves and reclaims. A seat that erred cannot, and its bond lapses to the pool at the deadline. A slash is collected by silence, so paying one shows nothing, and escaping one requires a false proof. The price is named: a clean seat silent past the deadline loses its bond as a dirty one does, and against that stand a long window, a one-message claim, and any hand to deliver it. A verdict stays open to review for a stated span, and its scores settle only after it runs out. An overturn inside the span restates the totals, and settlement runs on them by the same proofs. Nothing in the recast shows where any steward stood; the overturned majority's loss lands as bonds that lapse, unattributed. What stays visible is the counts: each side's size is public, the unanimous edge stated above stands, and the hiding is as wide as the panel. A small panel is a small crowd to hide in, and the panel that grows with the stake grows the crowd with it.

The penalty for a wrong verdict rises with how many stewards err together on the same case. An isolated mistake costs little. A bloc that moves the same wrong way pays toward the whole of its stake, because strangers sworn to silence and drawn apart should not fail in unison, and when they do, coordination is the likeliest cause. Punishing correlated error hardest turns the profit of collusion negative before a bloc can form. It also frees the honest dissenter: voting a private doubt risks little, joining a bloc that errs risks much, so the doubt is voted rather than swallowed.

One case lies beyond any scoring and is stated plainly: evidence built so well that every steward is sincerely deceived. No reward rule detects a mistake everyone makes honestly. What stands against it is the ballot and the questioning described next, and the bound on how much may rest on any single verdict while the mechanism is young.

The ballot is guilty, not guilty, or unresolvable. The last returns the funds. It exists because the most common hard case is ambiguity, not deceit, and forcing a call would reward whoever engineered the ambiguity.

On a grave case, when a majority of the quorum calls for it and an added bond is posted, the stewards may put written questions both parties must answer, so a packet built to mislead can be probed. The quorum ranks its own questions with no moderator. Each steward spends a fixed budget of weight at a rising cost per question, so only what matters draws weight, and a question pressed by both sides of a divided quorum rises above the merely popular one. The few at the top go to the parties. The ordinary dispute carries no such round and stays cheap to settle.

A steward is judged in turn. A verdict is a recorded action, and later verdicts can bear on it. Standing follows by the same instrument. Clean service converts into karma by a proof over a wide span of settled cases, landing at stated epochs in coarse steps, so the record shows that the account served and how well, never where or when within the span. Overturned service converts to nothing and its bond lapses, and karma decays unless renewed, so a steward whose verdicts are repeatedly overturned is drawn less often, and one who serves well gains standing. No authority reviews the stewards. Their record reviews them, as every account's record governs its standing. This carries personal responsibility into the one role that decides other people's disputes, without appointing anyone to watch the watchers.

10. The deadline

A court that can hang is a hostage taker. If a verdict could be withheld forever, the power to withhold would be worth money, and a party facing loss would pay for delay instead of judgment. Every dispute therefore ends, on a clock no participant can hurry, through one of four exits: the parties' own late agreement, a verdict, a tie read as unresolvable, or a default that needs no signer.

The deadline is hybrid: it passes only when the public clock and the delay function have both run their stated course. The public clock beats with the work supplied to it. Adding work quickens

it for a while, withdrawing work slows it, and both directions are priced far beyond any dispute the protocol will carry, since shifting the clock by a tenth means commanding a tenth of all the work in the world to gain hours in a week. The protocol does not lean on that price alone. The delay function cannot be hurried by adding machines, only by outrunning the fastest machine anyone holds, the same narrow margin the draw rests on, so the deadline cannot meaningfully be brought forward. It can be pushed back, by slowing the public clock, and slowing resolves nothing. It delays every path equally, including the attacker's own exit, and forfeits, for every day it runs, the income the withdrawn work would have earned.

Each panel tier publishes a quorate threshold, an odd number of ballots, and the draw seats more stewards than the threshold, so absences are expected and absorbed. If at least the threshold arrive sealed by the deadline, the panel is quorate and the answer with the most ballots is the verdict. A steward who took a seat and did not vote earns nothing and its bond lapses; a seat held silent is a seat denied to someone who would have judged. A tie at the top is not a stall. It is read as the verdict unresolvable, and the refund outcome is signed. A panel that reads one file and cannot lean either way is itself evidence of ambiguity, and ambiguity already has a verdict. No steward profits from engineering a tie: ballots are sealed, so a tie cannot be aimed at, and a tie pays no one.

The verdict moves funds through one signature assembled from the stewards' shares. The assembly is not deliberation. The shares travel as sealed arithmetic between pseudonyms that exist for the case alone, carry no room for argument, and reveal nothing before the tally; whatever narrow channel their timing could hide is an instance of the outside coordination already named among the limits. Every step of the tally and the signing either completes or names the members who withheld a share. A named withholder is excluded from the retry and pays, and the penalty rises steeply with how many withheld in the same round: one silence is likelier a failure, many together are likelier a plan. To block the signature outright, colluders must fill every seat of the margin the oversample leaves, seats assigned by a draw they could not predict, and every one of them is named and stripped together. Silence is not anonymous here. It is the one act the transcript attributes.

If a panel fails, too few ballots or a blocked signature, the failed seats are struck and the panel is refilled exactly once, along the same fixed order the seed set at the draw, under the same frozen eligibility, so a failed panel cannot be shopped for a better one. There is no third filling. If the second panel also fails, the funds move anyway. At escrow setup the parties pre-sign a ladder of long-stop outcomes that spend the disputed funds after a generous delay, with no quorum and no signer required at the time. The ladder is ordered by what the record objectively committed. If a milestone named at setup was met and committed to the record, a carrier's signed receipt matching its hash, a revealed handover secret, the outcome that milestone selects becomes valid first. Only where the record commits nothing does the last rung, a symmetric refund, become valid. The ordering matters. A bare refund default would pay the one party who wants deadlock: a buyer already holding the goods would keep the goods and take the money back. And because a trace can be manufactured around a hollow performance, the bound on any single verdict covers the best rung as well: forcing the default must cost more than the default can pay. The last rung rides the public clock alone, so its delay carries a margin of several times the longest case a dispute can run.

On a long-stop exit the pre-posted fees are burned, the stewards who failed pay, and neither trader gains or loses standing. Both sides lose time and the fee. The party who would profit from a standstill cannot cause one alone: it requires silencing enough stewards to close the oversample margin, stewards no one can identify before the draw, twice in succession, each silencer named and stripped. The default turns the worst failure from a permanent hostage into a bounded delay, and a hostage that must be released is not worth taking.

11. Sovereignty

The protocol rules on the trade, not on the person. It decides who owes what under an agreement two parties entered freely. It does not decide whether the trade should have been made, whether it was legal, or whether either party is virtuous. Those belong to the individual, who bears the consequences.

This is the third commitment, beside karma and the quorum: sovereignty. No supervising authority sits in the protocol or above it. Rules hold because participants keep them, and hold only over what participants have agreed to, as a network keeps a rule its members chose to run.

Sovereignty extends to the reputation itself. Karma belongs to the account, and an account can be sold as a business or a brand is sold, carrying its standing with it. The protocol cannot verify who holds a key, and does not try. That a key's holder is unknowable is what keeps identity sovereign, the same property that lets money be held without permission. What the protocol can do is mark a sharp change in how an account behaves. It reports the change as evolution, not suspicion, because people do change, and it never claims to know whether the hands changed with the conduct. A recently transferred account carries a visible marker of the transfer, and nothing more.

A key can be lost or stolen. An account may retire its key by signing a successor with it, effective after a fixed public delay, and the history carries over. An account may also register, at creation or later, a hidden recovery key, published only as a commitment. If the working key is compromised, revealing the recovery key displaces it after the same delay, and the older commitment wins any contest between the two, so a thief cannot outrun a commitment made before the theft. The commitment itself is replaced only by a supersession signed with the recovery key, never the working key. An account therefore changes hands fully only when its recovery lineage does, and a buyer who does not demand that supersession has bought an account the seller can take back. A recovery, like a transfer, stamps the visible marker of a discontinuity. An account that loses every key is gone. No one can restore it, because anyone who could would be an authority over accounts, and the protocol has none. What remains is what every abandoned account has: a fresh start at zero.

One person may hold many accounts, unlinked, revealing only what a given dealing requires, because privacy is the power to selectively reveal oneself. And a person may abandon an account and begin again, at the low standing every new account starts from, carrying none of the old history, good or bad. A fresh start is real, and so is its cost.

12. Economics

Both traders post their deposits and the dispute fee into the escrow when the trade is set, so opening a dispute costs no new money and a poor honest party is never priced out of defending itself. Deposits scale down with karma, an established account posts little and a fresh one much, and up with the amount in dispute, so a dishonest party risks capital in proportion to the prize. The cost of corrupting the verdict itself is governed separately, by the panel that grows with the stake.

Karma opens doors and never carries the money. Standing decides who may steward and how large a dealing an account may enter. The capital that makes fraud unprofitable is the fresh deposit posted for this trade, sized to it, and lost on it if the account defects. The reason is stated under sovereignty: an account can be sold, so a history proves what was done, never who now holds the key. Good conduct prices the deposit down, but the discount has a floor: however high the standing, the deposit never falls to where defection on this trade turns profitable. A reputation earns a cheaper entry, never a free one, and a bought reputation buys only the discount, because the stake that

must be lost is posted fresh, by whoever holds the key today.

A rule that prices one dealing at a time has a hole: nothing yet bounds how many dealings a key may hold open at once. An established seller posts a thin deposit on each, so a patient fraud can open many dealings in one week, collect every payment that moves outside the escrow, deliver nothing, and abandon the account. The standing he forfeits was already spent in his plan. Karma would become a credit line with no limit, and years of good conduct the loan application.

The protocol therefore caps a key's total open exposure. Every dealing states, in its signed opening, the value its counterparty stands to lose if the key defaults and the escrow's own return path cannot cover it. The sum of that value across a key's unsettled dealings may not exceed a fixed multiple of a bond the key holds locked for the purpose. The bond is held as the escrow is held. The owner alone can reclaim it, only after a timeout that outlasts every dealing it backs, and each opening adds to it a pre-signed outcome, completed only by a verdict against the owner in that dealing, that pays the wronged counterparty. Deposits inside the key's open escrows do not count toward the bond: a deposit answers only to its own dealing, and one placed with a friendly counterparty is recovered by a quiet cooperative close after the exit. Only the bond is capital a verdict is sure to reach. The multiple is a protocol constant, the same for every key, and karma never raises it. Anyone who plans to disappear surrenders his standing anyway, so a limit that grew with standing would be secured by the one asset the defaulter has already written off. Only capital a verdict can seize changes the arithmetic of an exit.

The cap enforces itself. An opening counts against the cap from its position on the public record, and openings that land together take a fixed order every client derives the same way, so the sum at every position is checkable by anyone. Before funding a dealing or paying on an outside rail, a counterparty's client reads the record, sums the other key's open exposure, confirms the bond outlives the dealing, and refuses to sign an opening that would breach the cap. A breaching opening moves no karma and convenes no quorum, so no informed counterparty accepts one. An opening never funded releases its place after a short deadline stated in the opening itself, and settlement by any path removes a dealing from the sum. No authority polices the limit, as no authority polices a signature.

The cost falls on honest volume, and is accepted. A trader who wants more dealings open at once must lock more capital, not more history, as a merchant posts a reserve against his float. The cap buys a hard bound on the whole, not a promise to each victim. The bond is one sum, seized once, while every dealing keeps its own deposit, so a counterparty's certain recovery is its deposit, and the value at risk it co-signed remains its visible, accepted price. A key that defaults on everything at once takes at most the capped multiple of the capital it forfeits, once, at the price of the account. A fresh account cannot play the same hand, because it posts deposits near the full price and exposes almost nothing. The cap does not make such an exit worthless. It makes the take small, bounded, and bought with real capital burned, where before it was limited by nothing.

On resolution, the losing side's deposit and the lapsed bonds of the seats that erred pay the seats that judged with the outcome, through the same nameless claims. Attacking and losing burns the attacker's capital. The winner is made whole.

A verdict moves standing as it moves money. The losing side's karma is cut in proportion to the value, the cut is charged back to those who vouched for a party judged a fraud, and a party wrongly accused is restored what the accusation put at risk. A verdict of unresolvable has no loser, so it is paid differently: the dispute fees both sides posted at setup fund the panel in equal parts, and both deposits return with the funds. The fees are set so this pay clears the cost of reading and stays below the pay of a decided verdict, so the safe call never outpays the right one. Judging that a case cannot be judged is work, and unpaid work would force a call on every hard case.

The protocol takes nothing. Every fee flows to the people who did the work of judging. There is

no issuer to pay, because there is none. The absence of an earning model is a requirement. Anyone who could profit from the court could sell it, and a court that can be sold is a court that will be. A fee-taking company is a standing target for a subpoena and a bribe. A token is judicial power for sale, and turns the court into the property of whoever buys the most. The protocol has neither, and is funded as shared infrastructure is funded, by grants and by the people who want it to exist. Neutrality is the product. An owner would be the flaw.

13. Sybil resistance

The security of the protocol is the cost of faking karma. That cost must be real, and cheap neither to a patient attacker nor to a rich one.

Creating an account costs an irreversible sacrifice, uniform for everyone, so a thousand accounts cost a thousand times one and no volume discount exists. Karma is minted only by settled dealings with distinct counterparties, never by self-endorsement, so a ring trading with itself earns nothing. Standing accrues slowly, each further unit from the same source worth less than the last, and decays unless renewed by fresh conduct with distinct counterparties. A burst of early activity bleeds away. A ring cannot maintain itself at a trickle. No account can hoard standing before the network is populated. Weight flows in from the established graph, so an account is only as trusted as the independent accounts that vouch for it.

The hunt for fabricated accounts is itself a paid trade. Anyone may post a bond and accuse a cluster of coordinated fabrication, putting the accusation and its evidence to a quorum like any other question. If the quorum finds fabrication, the cluster's standing is burned, the stakes of those who vouched for it are charged back, and the accuser is paid from those stakes. If the accusation fails, the bond pays the accused. A failed accusation settles nothing forever: fresh evidence founds a fresh accusation under a larger bond, so a ring can neither wear down the honest cheaply nor buy absolution by staging a weak case against itself. A large ring must fear its own members most. The member who knows its shape is the best-paid witness against it. The bounty turns a conspiracy's size from strength into exposure.

One problem stays open and is stated plainly. Telling distinct persons apart without an identity document is unsolved at scale, and the defense against an attacker who can cheaply create real-seeming humans is only as strong as the best answer to that problem. The protocol raises the cost of an attack. It does not claim to make one impossible.

14. Adoption

The protocol cannot be tested in a laboratory. Trust between strangers is a network good, worth little to the first user and much to the millionth, and no simulation produces the thing tested: a large population of real people with real reputations at stake. The protocol will be adopted gradually if it is useful, or not at all. Every protocol that replaced a trusted party with a network faced the same condition, and no engineering removes it.

The path is to earn karma inside systems that already exist. A marketplace, an exchange, or a community that adopts the protocol gives its users a reputation they can carry out, and gains a filter against fraud that no central moderator can match. Where a costly reputation graph already exists, the protocol can read it, so standing earned elsewhere seeds standing here and the first quorum is not conjured from nothing. Chronicle Network, an open, ownerless graph of costly signed reputation built by Luka Dover, is one such source and a companion to this work: it holds the standing, this protocol holds the judgment. One key participates in both, so a verdict here can be a marked event

there, and a steward who judges well is credited on a graph wider than this one. Where Chronicle carries a person's standing, the cold start is borrowed rather than bootstrapped.

15. Beyond disputes

The quorum is a general instrument. It can decide any question that needs an impartial answer and has evidence to decide on, not only who is owed money after a trade. A group can put a decision to it. A community can settle a rule with it. Any process that relies on a trusted counter, moderator, or authority can be handed to a crowd that cannot be found or bought.

A question outside trade has no losing deposit to pay the stewards, so it funds itself. Whoever poses it posts a bounty that becomes the reward, and each steward posts a bond of standing to take part. Many such questions have no outcome to check a vote against, so the stewards are scored on one another: each submits a sealed answer and a sealed forecast of how the others will answer. Both add without opening, as ballots do, and each forecast is proven well formed when cast, in the form the rule reads, so two totals are the rule's whole input. The panel opens those totals and nothing else, how the answers fell and how the forecasts expected them to fall, and the answer that beats its own expected support wins. Each seat's score follows from its hidden answer, its hidden forecast, and the open totals, collected and enforced by the same nameless claims and lapsing bonds as a verdict. No single answer or forecast ever opens. In trade, the batch of cases and the judgment of later quorums supply the standard a vote is measured against. A solitary question has neither, so it must carry its own standard, which the forecast supplies. A forecast averaged over a few stewards is noise, so a question scored this way convenes a wide panel or none, and the bounty must be priced to fund it. The panel is settled against itself, with no outside loser and no owner to subsidize it. Every such decision is recorded as an action, so the standing earned in trade is the standing staked in judgment, and one reputation follows a person across everything the protocol touches.

The furthest form of this is a binding collective decision that no one can quietly corrupt, at a cost of corruption far above the value of any single outcome. A vote fails where the count, the roll, or the authority can be captured. A verdict drawn from an unfindable, bonded, uncoordinated crowd removes each of those targets. Whether it replaces anything is for its users to decide. The protocol only makes it available.

16. Limits

The protocol rests on reasoning about how people act, not on evidence that it works, and it keeps the two apart. It cannot be proven in advance, and a correlation in early data would not prove it either. What can be shown is where it must hold and where it cannot.

Four limits survive every part of the design and are named rather than buried. A signing key can be bribed, and no sealed ballot stops its owner from selling the vote or proving it to the buyer. What the sale cannot deliver is a score: a bought vote fails the batch's bar and forfeits the bond behind it. Stewards who find a channel outside the protocol can coordinate, and the reward for honest reporting weakens when they do; against this stands only that the stewards know nothing of each other, so coordinating means building a conspiracy among people the system keeps apart, against the very system their standing is worth something in. Telling distinct persons apart without an identity document is unsolved, and the defense against mass-produced identities is only as strong as the answer to that problem. And the final defense against an attacker who has bought the whole graph is that the graph is expensive to buy, not that it cannot be.

One defense stands behind the last limit. Karma is not an instrument an attacker can own. It is a computation over a public log under fixed weights. If a portion of the graph is shown to be captured, bought standing certifying bought standing, no one is obliged to keep computing it. Clients can adopt a rule that discounts the captured lineage and recompute every standing without it, in the open, from the same log. Such a recomputation is a new version of the fixed weights, published whole, so within any version everyone still derives one number; what forks is the choice of version, not the arithmetic inside it. Nothing is confiscated and nothing is voted on. Each user chooses which version to trust, as before. The attacker keeps his entries and loses his audience. This is a recourse of coordination, not of arithmetic, and the protocol claims no more for it. But it makes the prize for capturing the graph a graph whose readers have left, the cheapest kind of nothing an attacker can buy.

The protocol therefore does not claim to be unstoppable. It claims to be the first way to resolve disputes and carry reputation with no single party to bribe, subpoena, or switch off, and to make the cost of capturing it exceed the value it protects, for stakes kept within that bound while the network is young.

17. Conclusion

Trade between strangers has rested on someone trusted to vouch and someone trusted to judge, and each such someone has been a point of failure. This protocol earns the vouch from costly action, draws the judgment from a crowd no one can find, holds the funds with the traders alone, and keeps no power for itself. The pieces are known: reputation from real conduct, selection at random, sealed votes, an oracle over an escrow, a clock no one owns. What has not been built is their assembly into a whole that no one owns and no one can capture. The result belongs to the public domain, to use, to build on, and to improve, without permission and without an owner, because a thing meant for everyone must be owned by no one.

References

1. J. R. Douceur. The Sybil Attack. 2002.
2. S. D. Kamvar, M. T. Schlosser, H. Garcia-Molina. The EigenTrust Algorithm for Reputation Management in Peer-to-Peer Networks. 2003.
3. A. Cheng, E. Friedman. Sybilproof Reputation Mechanisms. 2005.
4. E. Friedman, P. Resnick. The Social Cost of Cheap Pseudonyms. 2001.
5. S. Micali, M. Rabin, S. Vadhan. Verifiable Random Functions. 1999.
6. D. Boneh, J. Bonneau, B. Bunz, B. Fisch. Verifiable Delay Functions. 2018.
7. D. Prelec, H. S. Seung, J. McCoy. A Solution to the Single-Question Crowd Wisdom Problem. Nature, 2017.
8. A. Dasgupta, A. Ghosh. Crowdsourced Judgement Elicitation with Endogenous Proficiency. 2013.
9. V. Shnayder, A. Agarwal, R. Frongillo, D. C. Parkes. Informed Truthfulness in Multi-Task Peer Prediction. 2016.
10. C. Komlo, I. Goldberg. FROST: Flexible Round-Optimized Schnorr Threshold Signatures. 2020.
11. T. Dryja. Discreet Log Contracts. 2017.
12. L. von Mises. Human Action. 1949.
13. M. N. Rothbard. Toward a Reconstruction of Utility and Welfare Economics. 1956.

14. E. Hughes. A Cypherpunk's Manifesto. 1993.
15. Chronicle Network (L. Dover, Cartographers Guild): an open, ownerless graph of costly, signed reputation.
