WHITEPAPER

The Determination Layer

Chaingentic and the AIERC Protocol

Deciding whether a payment should happen — before it does

July 2026

AIERC Protocol · CIPO #3,304,029 · WIPO #PCT/IB2026/052205
Eternal Digital Assets Corp

Abstract

Chaingentic is a settlement-admissibility layer — for both manual users and autonomous, agentic value movement.

Sending money on a blockchain is the easy part; that problem was solved years ago. The hard part is deciding whether a payment should happen at all before it goes through: Is it allowed? What is the sender really trying to do? Does it make sense? Is it safe? No blockchain answers those questions. Chaingentic does, and it does it today, for a person holding a wallet right now — not only for the machine economy still being built.

That is the practical difference. A person approving a transaction sees a wall of code and has no way to know what they are agreeing to. If a website drains their wallet, there is no one to call. If they are tricked into signing, the money is gone the moment the payment is final. Every year billions are lost this way, and none of it is recoverable. The same gap, at machine speed and machine scale, is what will make AI agents moving money unmanageable — but the gap is costing real people real money now.

The protocol reaches money four ways — **AIERC-193**, **AIERC-RPC**, **AIERC-XT**, and **$AIERC** — all run by one engine, the **Benson Consensus Determination Mechanism (BCDM)**. The engine is running on Base and Ethereum today. The browser guard is live and stopping known drainers. Chaingentic itself is live, past 1.6 million blocks, and does something no other chain can: it holds a payment for a moment just before it becomes final, so the check can finish. It is protected by 2,584 patent claims filed at CIPO #3,304,029 and WIPO #PCT/IB2026/052205.

What You Get Today

You do not have to move anything, download a new wallet, or hand over your keys. You keep your wallet, your keys, and your money. Protection arrives three ways, and you can take one or all three.

The browser guard stops the theft before it reaches your wallet. Most people are not robbed by a broken blockchain; they are robbed by a website. A browser add-on checks each site against known scams and threats and sits between the site and your wallet, catching the dangerous request — a sneaky approval, a wallet-draining signature — before it ever becomes a real payment. This is the one place the system will flatly stop you, because this is where people get tricked most. A theft that never reaches the wallet cannot take anything. This is live now.

One setting makes your wallet explain itself. You change a single setting in the wallet you already use — an RPC URL. From then on, every payment is checked and explained in plain words before it is sent: what is being sent, where it is going, and what you are actually agreeing to. It warns you with specifics, not vague risk scores — *this address received funds from a sanctioned wallet three days ago; this contract has a hidden drain function; this website was set up yesterday.* On normal payments it stays quiet. You can ask it "why?" or "what if?" before you commit. It gives you the facts and leaves the decision to you.

The AI signs alongside you, and can never overrule you. On a smart wallet, the AI is added as a second owner, so a payment needs two signatures — yours and the AI's. If the risk is too high, the AI will not sign. It can never move, freeze, or take your money; all it can do is refuse, and you can always overrule it. You are never stuck.

And if fraud gets through, there is a window to undo it. After a payment is sent there is a short protected period in which a fraudulent one can be reversed. The reversal touches only that payment — not your balance, not anyone else's money — and needs no court order. This is the protection you take for granted from a bank card, brought to a blockchain for the first time.

What it costs. A check costs one cent at wholesale and 2.5 cents at retail. The rare cases that go to the full AI panel cost 75 cents, and they never happen without your consent. The price does not change with the size of the payment: the system works harder when more money is at stake, but you are not charged more for it.

The Gap in Every Digital Dollar

Compare crypto to a stolen credit card. The bank does not just shrug. Before the fraud even reaches you, systems like Visa's Advanced Authorization and Mastercard's Decision Intelligence check every purchase in real time. If a bad charge slips through, laws like Regulation E and the Fair Credit Billing Act give you the right to dispute it, the bank reverses it while it investigates, and the card network's zero-liability rule means you do not lose the money.

Crypto has none of this: no system watching the wallet, no way to dispute a payment, no way to reverse it, no regulator to call, and no insurance company willing to cover the risk — because the risk cannot even be measured. That missing safety net is the real reason banks, insurers, and big companies still hold back from crypto rails. It is missing for every digital dollar equally.

Chaingentic fixes it. Its checking layer is the safety net crypto never had: it reviews a payment before it moves, keeps a signed record of every check it ran, and leaves a short window in which a fraudulent payment can be undone. Once that is running and building a track record, insurers finally get what they need to offer coverage — a way to measure the risk, proof that controls are in place, and results they can verify. The protection every bank customer takes for granted becomes available on-chain for the first time.

Two Ways to Rank a Blockchain

There are two ways to rank a blockchain. The first is **settlement** — which chain finalizes payments for which. By that measure, Chaingentic is a Layer 2 (a chain that settles on top of Ethereum). The second is **thinking** — does the chain decide whether a payment should go through before it does? By that measure, every chain scores the same: zero. Ethereum, Solana, all of them. None of them check whether a payment makes sense; they just move the money. Chaingentic is the first chain that checks. On settlement, it is one Layer 2 among many. On thinking, it is the only one there is.

The Pause That Checks

Every blockchain today does the same thing with a payment: it takes it and finalizes it. There is no moment in between — the money is gone before anything could look at it. Chaingentic adds that moment. Because it runs its own blockchain (already past 1.6 million blocks), it can hold a payment for a second, right before it becomes final, check it while it waits, and then let it through or stop it. That hold happens at the exact point the payment is about to be sealed into a block. No other chain can do this. The same checking engine can also reach onto any other Ethereum-style chain that wants it, with about six lines of code, or for a single person just by changing one setting in the wallet they already use. No moving, no new chain, nothing to rebuild. The whole thing — the pause, the reasoning, and the ability to reverse a payment — is patented.

You already know this moment from a card machine: it says "Approving…", then a second later, "Approved." Nobody minds that second — it is the part that tells you something was checked. A machine firing off money at full speed with nothing watching does not reassure the people who manage risk; it worries them. A few seconds is a small price for a payment worth millions.

Taking a Payment Back — On Terms Both Sides Agree To

The pause is what lets a payment be checked before it goes through. A second feature lets a payment be undone after it goes through — and the two sides decide the terms themselves, up front.

This is not a fixed window like a credit card's dispute period. When the buyer and seller make a deal, they set how long the payment can be reversed — a minute, a day, a month, or longer — and whether a reversal returns all of the money or only part of it. If the system later finds fraud, or the agreed condition is met, it reverses exactly what the two sides agreed to, as a new signed payment. It touches only that one payment: no one else's money is affected, the issuer never has to step in, and the digital dollar itself is never changed. It is the everyday protection people expect from a card or a store return — a full or partial refund, over whatever time period both parties agreed to — brought to a blockchain for the first time, with the two sides writing the rules instead of a bank.

How It Works

One engine, called **BCDM** (the Benson Consensus Determination Mechanism), gathers the evidence around a payment, weighs it, and produces one signed decision before the money moves. The decision is not a simple yes or no — it can approve, wait, restructure, split, or reverse. It uses two "two-of-two" checks. The routine one is **AI + AI**: two separate AI reviewers, each looking at its own copy of the data, have to agree — the opposite of the single-reviewer, single-source setup that cost Kelp $292 million. The other is **AI + human**: on a smart wallet, the AI is added as a second owner, so every payment needs two signatures — the user's and the AI's.

The user is never stuck: only a registered owner can turn the AI's protection off for a set time, and the moment they do, the AI warns them that they are now unprotected. The AI never holds the money and can never move, freeze, or take it — all it can do is refuse to sign, and the user can always overrule it. Only the genuinely unclear cases get sent up — and only with the user's consent — to a panel of several different AI models. That panel is never the default. Fairness is built in: the reviewers lock in their answers before seeing each other's, the ones with the better track record count for more, and a share of the "all clear" results are pulled back and re-checked.

The protocol reaches money in four ways:

- **AIERC-193 — the Intelligent Token Protocol.** The token reasons about a transfer before it happens. `transfer()` and `transferFrom()` are overridden so the AI evaluates in the same transaction. For transfers that need longer, `requestTransfer()` charges the fee, moves the amount into the contract's own custody, and returns a request id — the sender cannot double-spend it while the AI thinks.

The AI's answer is recorded by `recordEvaluation()`, which only the evaluator address can call. It writes three things on-chain: the verdict, a confidence score from 0 to 100, and a `reasoningHash` — the hash or IPFS CID of the full off-chain analysis. The chain therefore holds the reasoning, not just a yes or no. Approve releases the held amount to the recipient; refuse returns it to the sender in the same call.

Three guarantees are written into the contract rather than promised. `cancelTransfer()` returns a sender's held tokens and works even while the contract is paused. `executeFailsafe()` can be called by anyone once a fixed block window has passed, so a silent AI cannot strand a transfer — but it explicitly cannot override a recorded refusal, which reverts with `TransferBlockedByAI`. The window is snapshotted per request, so the owner cannot retroactively lengthen it on transfers already in flight. `disableProtection()` turns the AI off for the caller's own address in one transaction, and `renounceOwnership()` reverts, so ownership can never be abandoned. An emergency `pause()` expires after roughly seven days, after which `forceUnpause()` is callable by anyone — a lost owner key cannot freeze the token permanently.

- **AIERC-RPC — the network check.** The single setting that makes a wallet explain and warn before every payment, described above.
- **AIERC-XT — the browser guard.** The add-on that stops scam sites and drainer signatures before they reach the wallet, described above. This is the one place the system flatly stops a user.
- **$AIERC — the fuel.** The credit that pays for the checking. One token pays for one check. Every check the system runs uses up some of this fuel, so as usage grows, demand for the fuel grows with it. The settlement dollar is the money that moves; $AIERC is what pays to make each move smart.

Every decision is written straight into the public record on the block explorer — the same place anyone already uses to look up a payment. It shows what was checked, whether it had to go to the panel, the decision, how confident the AI was, and the reasoning. It is permanent and anyone can read it. So when a regulator, an auditor, or a nervous business partner asks, the answer is not "trust us" — it is a link. A user can also add private notes to a payment that only they can see, right next to the public decision everyone can see.

What It Gives Every Blockchain That Connects

- **Checking before finalizing.** For the first time, a chain can decide whether a payment should go through before it becomes final — a moment that exists nowhere else.

- **Easy to connect — and the network makes money.** Any Ethereum-style chain can add the checking layer with about six lines of code — no moving, no swapping tokens, no new setup. And it is a source of income, not a cost: the network buys checks at one cent wholesale while its users pay 2.5 cents, so the network keeps the difference on every check that runs through it. Users get protection, the network gets a new income stream, and the protected dollar gets spread further — everyone wins.
- **Two reviewers, not one.** Every payment is checked by two independent AI reviewers, each using its own source of data, each comparing what the payment claims against what is actually on the chain.
- **Weighs the evidence, not a vote.** Decisions are argued against the real details — the actual code, the contract, the terms — and any strong disagreement is kept on the record, rather than settled by a simple majority.
- **Compliance built in.** The audit trail is a natural result of every check, built into every payment from the start. A chain that connects is compliant from its very first block.
- **Protects both directions.** It protects the user from bad actors, and it protects everyone else from the user's own software if that software is tricked or hijacked into sending money it should not.
- **Works offline.** For devices without a steady internet connection, the check runs locally and only reaches out to the cloud when unsure.

Proof — Why It Is Needed, and What Is Built

The need: $292 million, and the one check that was missing

In April 2026, $292 million was stolen from Kelp DAO — not because the encryption broke, but because of a single point of judgment. One reviewer, using one source of data, approved one fake message, and the money was gone the instant the payment was final. There was no second opinion, no independent check, no moment where anything asked whether the payment was really what it claimed to be. That is not just a Kelp problem — it is the shape of almost every big crypto theft: a payment that looks fine, with nothing in place to question it before it is final. It is the exact gap this system was built to close, which is why the need is not theoretical — it has already cost the industry billions.

Now imagine that same day with this system in place. Two independent reviewers, each with its own source of data, compare the payment against what is actually on the chain — so the fake message fails right away, because the two do not agree. On top of that, a $292 million transfer to a brand-new address gets flagged for review on its size alone, before a cent moves. Either check stops it on its own; together they make it basically impossible for one fake message to get through. The cost of running that check on the payment that took $292 million: one cent.

What is already built

This is a finished system, not a slide deck. The engine is running on Base and Ethereum today, giving real "clean or flagged" results on real traffic. A wallet-kit plugin passes all 36 of its 36 tests. The browser add-on is live and stopping known drainers; the public record is live and posting every decision; and Chaingentic is live, past 1.6 million blocks. The full set of patents — **2,584 claims** — is filed at CIPO application 3,304,029 and WIPO PCT/IB2026/052205, covering the checking method, the in-wallet helper, the marketplace, the enforcement points, cross-border compliance, and letting a machine act for its owner.

The AI Behind It

We are approved, verified members of Anthropic's **Claude Partner Network**, and Claude is central to how the engine reasons. Membership followed a long screening process: ten members of the team completed the first courses, passed the tests, and earned certifications, which qualified the project for full partner-portal access. Completing the remaining proctored exams — taken in person at Pearson VUE centers, 60 questions, a 120-minute limit, a pass at 72% — moves the project from the Basic tier to the Select tier, on track for the end of September 2026. At the Select tier, the project earns the right to use Anthropic's brand. The AI runs off the blockchain; a smart contract cannot run a model, so the token and the chain call an on-chain record of the AI's decision rather than the model itself. That separation is what lets the reasoning be as capable as a modern AI while the settlement stays fully on-chain and auditable.

The Economics

Ethereum built a trillion-dollar economy on one idea: every bit of computing on the network is paid for in one currency, ETH, and as activity grew, demand for that fuel grew with it. **$AIERC** is that fuel for the checking economy. Every check the engine runs — on every chain, in every wallet — uses some $AIERC. One token buys one check.

$AIERC is built as a usage credit, on purpose. Its price is tied to the work it buys — one token equals one check, priced at the cost of that check. Someone who never runs a check is never penalized; the same credit can be used for AI-platform time instead, and any rise in value simply shows up as a discount on future checks. That firewall is what keeps it a fuel rather than an investment, and it is what lets a regulated institution hold it without the risk a profit-seeking token would carry.

The economics work at every layer. A check costs a penny at wholesale and 2.5 cents at retail, so a network that resells checks keeps the margin on every one it passes through — protection becomes a revenue line, not a cost. For scale: the whole engine can evaluate every EVM chain for about $45,000 a day, while Ethereum spends millions a day just to order transactions — and that ordering cannot tell a payment from a theft. And the records the engine produces become products in their own right: an activity feed, a decision history, a registry of deals that could not be done, and a live risk feed — institutional subscriptions in a class where comparable feeds sell for $50,000 to $500,000 per year.

The Competitive Landscape

Nothing like this exists yet, but it is worth being precise about the nearest neighbours. Most blockchain-security tools do one of two things, and neither is determination.

The first kind writes rules ahead of time and returns a yes or no — the rule had to be written before the situation came up. An address that was approved before but later turns bad sails straight through a rule-matcher and is caught by a fresh determination. Rule-matching is a useful input; by its nature it cannot become intelligence.

The second kind scores risk: it gives a payment a number for how risky it looks. Scoring guesses at a probability; determination makes a judgment — it decides whether the payment should happen, holds it while it decides, and can reverse it after. A score is one of the many things the engine weighs before it reaches a determination. Notably, the closest company in this space holds no patents at all, while the AIERC portfolio spans the method, the wallet interface, the marketplace, the enforcement points, cross-border compliance, and machine principal-authorization. When those patents are granted, the tools around determination become licensing customers rather than competitors.

The Same Engine, When the Agents Arrive

Everything above protects a person today. The same engine answers a question that is about to get much larger.

Software programs called AI agents are already buying software access, paying for computing, buying data, and making deals on their own. An agent has no gut feeling. It does not pause and think, "this feels wrong." It just does what it was told. As agents begin moving money at machine speed, the gap that costs individuals their savings today becomes a gap no human can watch at all.

- **The rail is being set.** The agent-payment rail known as x402 launched with 40 founding members, including Stripe, Google, Coinbase, Cloudflare, Mastercard, Visa, American Express, and Shopify, and has already handled 165 million payments across 69,000 active agents, growing about 195% every quarter. Defaults chosen at machine scale do not flip. The one thing every payment rail lacks — and, as a neutral standard, always will — is a way to decide whether a payment should happen.
- **Regulation is arriving.** The GENIUS Act makes digital-dollar issuers regulated financial institutions with bank-grade anti-money-laundering duties; the final rules land this year, and enforcement begins on 18 January 2027. Every determination is a signed, human-readable record made before the payment settles — the exact audit trail those rules will require.
- **The machines are coming.** Barclays projects a $200 billion humanoid-robot market within ten years, and SoftBank projects $5 trillion in annual AI spending by 2040, and 100 trillion AI agents by 2040. Every one of those agents and machines needs a way to pay that can be trusted.

For that world the protocol adds pieces a person does not need today: a patented way to let a machine act on its owner's behalf — within limits, cancelable, and accountable; a marketplace where agents say what they want to do and every possible match is checked for sanctions, laws, jurisdiction, and suitability before the two sides ever meet; and a prudence ledger recording every deal an agent turned down, delayed, or walked away from, with the reason — proof of good judgment, valuable to insurers, regulators, and anyone deciding whether to trust an agent.

None of that is a promise about the future of this product. It is the same engine, already running, pointed at a bigger problem.

The Determination Layer

What is being built here is not a security feature, a compliance tool, or a data product. It is the determination layer: reasoning about a payment before it is final, with a signed record of the reasoning behind every result. Every deal in the world runs on one of three things: trust, lawyers cleaning up afterward, or a person in the loop. Trust breaks; lawyers are slow; people cannot keep up with machine speed. Chaingentic adds a fourth — a system that decides whether a payment is sound before it happens.

That is worth something to a person with a wallet this afternoon, and it is worth a great deal more to the economy arriving behind them.

> **The dollar became the reserve currency of the human economy by being the money of the most trusted settlement system. The reserve currency of the machine economy will be the money of the only system that determines whether a payment is sound before it happens — checked before it moves, and reversible the moment fraud is found, for a penny a payment.**

Chaingentic and the AIERC protocol — Eternal Digital Assets Corp. Patents filed at CIPO application 3,304,029 and WIPO PCT/IB2026/052205. This paper is for information only and is not an offer of any security or token.