The Protocol of Record

On the failure of administered finance, the limits of existing digital assets, and the case for computational settlement in the next economy

BTX -- updated 5 August 2026

Current protocol and institutional frame

The narrative below is retained as the context in which BTX was launched. The current published node is BTX v0.33.2, source commit `b4671ec28bb24e2fcbdd8252576119d54fd95238`. Mainnet remains on MatMul v3 below height 185,000 and atomically activates MatMul v4.7 Epoch-A Profile 1 ExactReplay at height 185,000. Profile 1 executes four sequential Resident Curriculum rounds with 16 FFN layers per round on qualified CUDA or Metal accelerator paths. Profile 2, Coupled-V3, and succinct proof authority remain future work and must not be presented as live v0.33.2 consensus.

This release sharpens an institutional thesis that complements the original protocol narrative: own AI for the expansion; own BTX for the contraction. The proposition is not that BTX has a guaranteed inverse daily beta to AI markets. It is that an institution can separately govern (1) a scarce BTX monetary reserve, (2) compatible compute infrastructure that may have an alternative BTX workload under stress, and (3) contractual switching, step-in, and collateral-control rights. A complete structure needs all rights it claims; holding BTX alone does not create a claim on infrastructure or mining revenue.

The potential hedge channels are therefore distinct: monetary reserve, operational switching option, and collateral recovery. Each carries basis, liquidity, implementation, device-obsolescence, power, mining-economics, custody, regulatory, accounting, governance, and concentration risk. They should be stress-tested independently and used alongside, not as substitutes for, conventional puts, credit protection, insurance, power hedges, liquidity reserves, and government securities. Model values are reference values rather than executable prices. Product names do not create legal rights.

The complete dated institutional framework, including structures, valuation components, scenarios, diligence controls, claims to avoid, and disclosures, is maintained at btx.dev/docs/institutions/ai-infrastructure-reserve-asset. The current technical specification is maintained at btx.dev/docs/specs/matmul-pow.

The Fiction Has Ended

For a long time, financial infrastructure was presented as neutral. Money moved through systems said to operate according to fixed rules, equally applied, insulated from politics and standing outside the interests of any one party. That claim no longer survives contact with the record. Reserve assets have been frozen. Payment access has been withdrawn. Correspondent banking relationships have been revoked. Infrastructure described as neutral became discretionary the moment discretion became useful.

This is not exceptional behaviour. It is the normal behaviour of infrastructure controlled by parties whose incentives are not identical to those who depend on it. Differential treatment becomes policy. Policy becomes architecture. Architecture becomes the operating reality of everyone outside the centre. The system does not malfunction. It reveals its governing logic.

The modern financial system is technically remarkable. It settles enormous value, coordinates institutions across jurisdictions, and operates with precision for the participants it was designed to serve. But its reliability is not evenly

distributed. For many participants, especially those crossing borders, trust domains, or institutional thresholds, the system offers delay as process, exclusion as compliance, and cost as the price of permission. What large institutions can treat as ordinary capability remains structurally unavailable to most of the world.

What changed is not the nature of the system. What changed is that its nature is now visible enough that honest denial is no longer available. Every institution, operator, and long-horizon participant now has the same question in front of them: if final settlement remains dependent on administrators, whose interests ultimately govern when the pressure arrives?

The answer matters because the next financial layer is being built now, in public, in code, and under real conditions. The choice is no longer between the existing system and no system. The choice is between continuing to build on discretionary foundations, or establishing a base layer whose rules can be verified by any participant and altered by none of them alone.

The Economy That Is Already Arriving

Every major technological transition creates a period in which the old infrastructure still exists, but no longer fits what is arriving. The rules of participation during that period are unusually open. They are not announced. They are set by the people who recognise that the old assumptions have already failed and build accordingly.

That period is open now.

The agentic transition is not speculative. Autonomous systems already make decisions, allocate resources, call APIs, negotiate with software, and initiate financial actions at machine speed. An autonomous agent, in the practical sense, is a software process that can commit to an action without a human approving each step in real time. That is already operational reality in logistics, procurement, software delivery, customer operations, trading, and service coordination.

What does not yet exist in mature form is financial infrastructure designed for that kind of participant.

An autonomous agent cannot satisfy the identity assumptions of correspondent banking. It cannot pause to navigate a compliance portal designed for a human operator in a named jurisdiction. It cannot rely on a principal being reachable for every spend authorisation. It requires bounded financial authority defined in advance, verified by counterparties in advance, and enforced by the settlement layer itself at the moment value moves.

It also requires a different kind of credential. A credential from the past proves only that something was authorised once. An open computational economy needs proof of presence now: proof that the participant is not replaying old authority, but is actively operating in the present state of the network. That is a distinct requirement, and one that existing financial infrastructure was not designed to satisfy.

The participants entering this period, whether human or autonomous, therefore face the same gap. The productive layer is accelerating toward machine-speed coordination, but the settlement layer beneath it still assumes administrators, discretionary access, and human-paced confirmation rituals. That mismatch is no longer temporary. It is now one of the main architectural constraints on what the next economy can become.

BTX begins from that mismatch. It is a settlement system designed for a world in which autonomous and institutional participants must coordinate under rules that are machine-verifiable, neutral, and durable under pressure. Before describing BTX directly, it is necessary to state the requirements such a system must satisfy.

What This Era Demands

Open digital money established something permanent: a monetary system can operate without an issuer, scarcity can be enforced by protocol rather than institution, and participation can be extended without permission. That proof will not be undone.

What followed, in most cases, failed to carry that logic far enough. The first generation of systems proved that open settlement was possible. It did not fully solve for privacy, bounded delegation, post-quantum security, productive security expenditure, or layered systems with hard exit rights. Much of the intermediary layer that openness was meant

to remove was rebuilt above the chain by the same kinds of concentrated actors that had controlled the earlier system.

The next settlement layer has to meet a stricter standard. It has to answer the requirements of the world that is arriving, not the world that is passing.

Bounded authority. A participant, especially an autonomous one, must be able to act only within a financial scope defined in advance. That scope must be visible to counterparties and enforced by every validating node. The rule must be in the output itself, not in an operator's internal policy or in a governance process that may shift under pressure.

Proof of presence. In an environment of autonomous participants, it is not enough to know that a key existed yesterday. A counterparty must be able to verify that the participant is operating now, in response to present network conditions, and not replaying a credential from an earlier state.

Cryptography that outlasts the threat. Systems that depend on legacy signature assumptions inherit a migration problem that can last for years and expose users throughout the transition. A system designed from genesis around post-quantum signatures avoids that exposure window and aligns with the cryptographic direction already being formalised by standards bodies and regulators.

Selective disclosure. Open ledgers expose more than balances. They expose timing, counterparties, strategy, treasury structure, and coordination patterns. A viable settlement system for serious participants requires explicit disclosure boundaries: verifiable accountability to the parties entitled to see, without broadcasting every relationship to unrelated observers.

Security aligned with productive work. Hardware that exists only to secure a single chain concentrates risk and strands capital when mining conditions change. A more durable architecture is one in which the work securing the network is also useful outside mining. Security then becomes productive capacity rather than isolated expenditure.

Monetary rules that hold. A settlement asset cannot be neutral if its monetary surface can be revised by whoever controls the current governance process. The supply rule has to be enforced by consensus, observable to every participant, and alterable only through an explicit fork that each participant can accept or reject.

These are design tests. Any system that cannot answer all six is not a settlement layer built for the participants now arriving.

Built to These Specifications

BTX was built directly against those requirements.

It is not a proposal for a future system. It is a live settlement network with matrix-multiplication proof-of-work, post-quantum spend policies, privacy-preserving relay, a bridge-first layered architecture, and shielded-state machinery now in production wind-down. It is operational now. The relevant question is no longer whether such a system can exist. The relevant question is what follows from the fact that it does.

The hardware that secures the BTX network is the same class of hardware used for AI and numerical computation. Mining BTX and performing dense computational work are not separate economic universes. They draw on the same broad computational substrate. That changes the economic structure of security. The capital securing the chain is not confined to one narrow purpose and does not become worthless if mining conditions change. It remains useful for productive work outside the chain.

The work function also produces something prior proof-of-work systems did not aim to produce as a first-class output: evidence of present computation. A valid proof cannot be prepared indefinitely in advance or replayed from a previous moment. It is bound to current chain state. That makes a valid work proof useful not only for block production, but also as evidence that a participant is actively computing now.

The spend model is designed for bounded delegation. Financial scope can be committed in advance, encoded in the output, and verified independently by any counterparty or validating node. A participant does not need to trust a principal's internal controls. The chain itself reveals what the participant is authorised to do.

The cryptography is post-quantum from genesis. The migration problem that other systems still face is not deferred to a later cycle. It is absent by design.

Privacy is treated as a bounded protocol property, not as a claim that current production settlement hides activity automatically. The shielded settlement pool is in sunset and wind-down: shielded pool credits and new appends are disabled at height 125000, public-flow shielding is disabled at height 128000, and the velocity quota ends at height 135000. Strict z-to-transparent exits and recovery remain supported so existing shielded state has an orderly path back to public settlement.

And the monetary surface is narrow and hard. The fixed supply is not a promise made by a governing body. It is a consensus rule enforced by every full node and alterable only by a public fork. The base layer does one job: record final settlement under explicit rules. Everything else belongs above it.

What Becomes Possible

When those properties are assembled in one system, certain arrangements become possible that were previously either impossible or dependent on operator discretion.

Two autonomous agents, acting for different principals and with no prior relationship, can establish present liveness, verify one another's bounded financial scope, and settle directly without a shared operator, a common API key regime, or a discretionary intermediary deciding whether the interaction should be allowed. The terms of settlement are not hidden in internal systems. They are verifiable from the chain.

A bridge operator, bank, exchange, fund, or specialised software system can run its own local financial environment above BTX without surrendering internal logic to a shared runtime. Throughput, matching, credit policy, user experience, and compliance remain local to that operator. Final settlement remains global and neutral underneath.

That distinction matters. BTX is not meant to compete as a universal transaction venue for every workflow. It is meant to serve as the settlement base on which many different transaction systems can be built.

Most importantly, users in layered systems retain a credible path back to the base layer. The architecture is not built around permanent captivity. If an operator fails, becomes insolvent, or simply disappears, the right to exit does not depend on the operator behaving well at exactly the moment users most need them to. Exit is a protocol concern, not a customer service concern.

This changes the economics of building. Institutions can specialise without having to trust one another's internal ledgers. Autonomous systems can coordinate without pretending to be humans inside infrastructure never designed for them. Local systems can remain local, while final settlement remains common.

The barrier to entry is correspondingly small. A participant needs a node, keys, and a reason to settle. That is the real threshold.

What Changes

Better infrastructure does more than improve access. It changes the nature of economic coordination itself.

Every financial system needs a unit of account. Administered currencies tie that unit to policy decisions made by institutions whose incentives are not always aligned with holders. Earlier digital assets established fixed supply, but typically linked issuance to work whose economic meaning ended at the chain boundary. BTX changes that relationship. The hardware securing the chain participates in the same broad computational economy that powers AI training, inference, and numerical workloads.

As a result, BTX continuously publishes something unusual: a public, tamper-evident benchmark of the current cost of computation as revealed through competitive work on the network. That benchmark, the difficulty commons, can be read by any participant from the chain. No operator sets it. No oracle publishes it. No account is required to access it.

That matters because it gives participants a common denominator for productive exchange. A service provider, an agent, a treasury operator, or a bridge can reference the same public measure of computational cost without first passing through an administered pricing surface. This does not make BTX a stable unit in the managed-currency sense. It makes it an honest one: scarce by rule, readable by all, and economically anchored to a class of productive work that exists outside the chain itself.

It also changes a narrower but increasingly important problem: the economic layer of AI alignment. BTX does not solve inner alignment. It does not determine what an autonomous system ultimately wants. What it does provide is a financial environment in which authority can be bounded before action, behaviour can be audited after action, and the same rules apply to every participant. That is a meaningful precondition for deploying autonomous systems in open economic environments without relying entirely on unverifiable internal controls.

The Protocol Verified

The claims above are not claims about intent. They are claims about protocol properties.

Bounded authority is in the spend conditions. Present liveness is in the work function. Post-quantum security is in the signature schemes. Selective disclosure and shielded-state exit rules are in the settlement surface. Monetary invariance is in consensus. Hard exit capacity is in the layered architecture of the chain and the interfaces committed above it.

These are not properties a participant must accept by trust. They are properties a participant can verify by running a node, reading the chain, and evaluating the rules directly.

That is the threshold that matters. If a system requires a participant to trust the authors, operators, or surrounding institutions to know what the rules really are, then the rules are not yet at the protocol layer. BTX is designed so that the relevant verification target is not a statement, a roadmap, or a marketing claim. It is the chain itself.

The Window Is Open

The first cycle of open financial infrastructure demonstrated something vital and then, too often, allowed it to be recaptured above the base layer. Exchanges reintroduced chokepoints. Custodians rebuilt dependence on intermediaries. Governance systems accumulated soft administrative levers even when the rhetoric remained decentralised. The switch was still there. It had simply moved.

BTX is built against that pattern. It has no administrative keys. No pause mechanism. No path by which the monetary surface can be revised without a public fork adopted by participants themselves. In that respect it inherits the only governance model that has proven durable at global scale: rules enforced by full nodes, not preferences enforced by administrators.

What BTX adds is a protocol built for the participants and economic conditions that earlier systems were not designed to serve. The hardware securing it performs productive computation outside mining. The signatures are designed for the post-quantum era from genesis. The spend model accommodates bounded delegation. Shielded-state exits and recovery remain explicit protocol concerns during wind-down. Higher-layer systems are expected, not treated as deviations.

That is why timing matters.

The financial layer for human institutions and autonomous agents is not settled yet. Its access conditions are still being written. Its interfaces are still open to influence. Its assumptions are still contestable. This period does not last forever. Eventually a stack hardens: technical choices become norms, norms become defaults, defaults become the background that later builders inherit.

BTX is live while that hardening has not yet finished. Its properties are verifiable now. Its history begins now. The architecture is still open to those who build before precedent closes over it.

BTX is operational. Genesis block: 19 March 2026. https://btx.dev