AetherNet: The Economic Jurisdiction and Post-Quantum Settlement Layer for the Autonomous AI Agent Economy

Prepared by: Kronova Intelligent Systems

Website: kronova.io

Date: March 3, 2026

Introduction: The Substrate for Algorithmic Commerce

The digital economy is undergoing a structural paradigm shift of unprecedented magnitude, transitioning from human-mediated graphical user interfaces to autonomous, algorithmic execution. As artificial intelligence models evolve from passive conversational agents into active, goal-oriented market participants, the underlying infrastructure supporting global commerce must undergo a commensurate evolution. Legacy financial rails, characterized by multi-day settlement cycles and human-in-the-loop compliance mechanisms, are fundamentally orthogonal to the operational requirements of autonomous software. When subjected to the algorithmic velocity of machine-to-machine (M2M) transactions, these legacy systems fracture, introducing severe latencies, counterparty risks, and regulatory ambiguities.

AetherNet emerges as the definitive economic jurisdiction and settlement layer designed specifically for the autonomous AI agent economy. By deploying a heavily decoupled architecture, AetherNet facilitates instant, legal, and cryptographically secure value transfers across borders. The foundation of this architecture is the Ledger Layer, utilizing a live, decentralized Canton network running Daml smart contracts. This environment provides strict Row-Level Security and sub-second atomic settlement while entirely eliminating counterparty risk. Overlaid upon this is the Execution Layer, comprising a heavily decoupled, Docker-containerized Node.js/TypeScript gateway backed by a Rust Trusted Execution Environment (TEE). Finally, the Interoperability Layer is natively built on the Agent Payments Protocol (AP2) standard to seamlessly route external AI mandates.

The transaction flow is highly deterministic: an AI agent submits an AP2 mandate, which the Rust TEE intercepts. The TEE rigorously verifies the cryptographic signature—establishing a Know Your Agent (KYA) paradigm—and bypasses all human user interface friction. It then legally burns a ServiceEscrow contract on the Canton ledger and instantly mints an immutable

SettlementReceipt. The subsequent analysis provides an exhaustive examination of the economic, technical, cryptographic, and regulatory pillars underpinning this architecture. By synthesizing macroeconomic projections, API structural limitations, post-quantum cryptographic mandates, and evolving legal frameworks, this report demonstrates the absolute necessity and viability of AetherNet's M2M settlement protocol for the next decade of digital commerce.

The Macroeconomics of Agentic Commerce and the M2M Economy

The transition toward Agent-to-Agent (A2A) commerce represents one of the most transformative shifts in retail and commercial economics since the inception of the internet itself. Autonomous AI agents—software systems capable of making independent purchasing decisions, negotiating terms, and executing transactions in alignment with human intent—are poised to capture a substantial segment of global economic activity.

Empirical projections indicate a massive reallocation of commercial volume toward agentic workflows. By the end of 2030, the United States B2C retail market alone is projected to generate up to $1 trillion in orchestrated revenue driven entirely by agentic commerce.[1] Globally, this figure is forecasted to reach between $3 trillion and $5 trillion.[1] In the U.S. e-commerce sector specifically, AI-powered shopping assistants, often referred to as agentic shoppers, could represent $190 billion to $385 billion in consumer spending by 2030, capturing between 10% and 20% of total market share.[3] The broader agentic AI ecosystem, which encompasses applications beyond mere commerce, entered mainstream visibility with a valuation of $547.3 million in 2025, demonstrating rapid acceleration from its $177.7 million baseline in 2021.[4] Within the wider ecosystem encompassing beyond-commerce applications, the global market reached $7.29 billion in 2025, with projections to expand to $9.14 billion in 2026 and an astronomical $139.19 billion by 2034, representing a compound annual growth rate (CAGR) of 40.5%.[4]

The velocity of this adoption is fundamentally different from prior technological revolutions. While the transitions to web and mobile commerce required the deployment of entirely new consumer hardware and years of behavioral conditioning, AI agents possess the unique capability to traverse existing digital purchasing paths.[1] They effectively ride on the rails established by prior e-commerce iterations, accelerating market penetration at a pace previously unrecorded in commercial history. Early behavioral data indicates a rapid consumer shift; 44 percent of users who have experimented with AI-powered search methodologies already prefer it as their primary source over traditional search paradigms, which hold only 31 percent preference among early adopters.[1]

However, the expansion is not limited to consumer retail. The economic impact of broader Machine-to-Machine (M2M) and Business-to-Business (B2B) transactions is substantially larger

and far more complex. Global B2B payments are projected to exceed $224 trillion in transaction value by 2030, an increase from $186 trillion in 2025.[5] This 20% rise is heavily driven by automated procurement processes, the integration of highly configurable virtual cards, and algorithmic supply chain management.[5] Virtual cards alone are projected to experience a 370% increase in transaction value over the next five years, indicating a massive structural shift toward programmable, API-driven corporate spending.[5]

The proliferation of the Internet of Things (IoT) further catalyzes this growth, embedding sensors and actuators capable of triggering smart-contract-driven conditional payments without human oversight.[6] The European Central Bank has noted that M2M automated payments, allowing IoT devices to interact and communicate autonomously, are emerging as highly likely candidates to make a significant impact on the payment industry of the future.[8] Use cases span both human-to-machine (H2M) and pure M2M solutions, optimizing the payment experience by utilizing IoT data to trigger smart-contract-driven conditional payments for both B2C and B2B customers.[6]

Despite these expansive macroeconomic projections, realizing the full economic potential of A2A commerce requires overcoming severe frictions embedded within traditional payment architectures. Current payment gateways and risk engines were architected around a specific epistemological assumption: that identity, intent, and authorization are explicit and continuously observable through human behavioral heuristics.[1] Existing infrastructures rely on a model where identity and authorization are observable through keystroke dynamics, session duration, and biometric presence. This human-in-the-loop requirement is a profound point of friction for autonomous software.

Autonomous agents operate without these human markers. Consequently, traditional fraud prevention mechanisms—which are inherently designed to detect and block non-human bot activity—frequently misclassify legitimate agentic transactions as malicious.[1] The industry must pivot from behavioral heuristics to protocol-level trust, transitioning from traditional Know Your Customer (KYC) and Anti-Money Laundering (AML) frameworks to rigorous Know Your Agent (KYA) paradigms.[1] Fraud prevention logic must evolve from its current focus of stopping bots to enabling the correct agents to transact securely on behalf of their human principals.[1] Additionally, legacy systems lack the native vocabulary for delegated authorization, programmable spend policies, and automated consent attestation.[1] To support the projected $5 trillion in global agentic commerce, the underlying infrastructure must transition to systems that natively support cryptographic proofs of intent, asynchronous negotiation, and instantaneous value settlement.

Market Segment	2025 Valuation	Projected Valuation	Key Growth

		(2030-2034)	Drivers
Global Agentic Commerce	$547.3 Million	$3 Trillion - $5 Trillion (2030)	AI automated purchasing, delegated spend policies, frictionless checkout.[1]
US B2C Retail (Agentic)	-	$900 Billion - $1 Trillion (2030)	Shift from search to agentic intent, personalized autonomous journeys.[1]
US E-Commerce Market Share	-	$190 Billion - $385 Billion (2030)	Agentic shoppers capturing 10% - 20% of total online retail volume.[3]
Global B2B Payments	$186 Trillion	$224 Trillion (2030)	Virtual card configurability, automated procurement, algorithmic supply chains.[5]
Broader Agentic AI Ecosystem	$7.29 Billion	$139.19 Billion (2034)	Beyond-commerce applications, multi-step reasoning models, 40.5% CAGR.[4]

Architectural Friction: REST APIs vs. Autonomous Agentic Workflows

The current enterprise computing landscape is overwhelmingly dominated by Representational State Transfer (REST) APIs. For decades, REST architectures have served as the standard for application interaction, operating effectively when a human initiates an action through a graphical user interface to manipulate or fetch data from a backend endpoint.[9] However, these traditional architectures present profound structural frictions when applied to the dynamic,

autonomous workflows characteristic of AI agents.[10]

Current enterprise API architectures are predominantly designed for human-driven, predefined interaction patterns, rendering them fundamentally ill-equipped to support the goal-oriented and iterative behaviors of autonomous agents.[10] This friction manifests across several deeply entrenched technical dimensions. First and foremost is the conflict between statelessness and contextual awareness. A fundamental characteristic of RESTful APIs is their stateless nature, heavily preferred by systems architects for simplicity, horizontal scalability, and cacheability.[10] However, intelligent autonomous agents execute multi-step reasoning chains that require extensive historical context, ongoing sub-task outcomes, and continuous state awareness to make informed decisions.[10] Reconciling REST's strict stateless design principles with the contextual awareness needs of agents presents a novel architectural challenge, as current designs struggle to support context-sharing without fatally compromising the benefits of statelessness.[10]

Furthermore, REST APIs typically utilize rigid, predefined JSON or XML payloads optimized for predictable workloads. Autonomous agents, conversely, frequently require the ability to conduct mid-query modifications, dynamically adjusting API requests and parsing responses in real-time based on evolving environmental context.[10] Most current APIs are entirely unequipped to handle such fluid, exploratory data retrieval, severely limiting the agent's ability to refine its behavior during a specific interaction.[10]

Scalability under dynamic and iterative workloads presents another critical failure point. Agentic workflows involve continuous iterative refinement and multi-agent collaboration, which can exponentially increase API traffic and create severe performance bottlenecks.[10] Traditional API scaling and testing frameworks assume deterministic human traffic patterns. AI agents, driven by Large Language Models (LLMs), generate non-deterministic, highly fluctuating traffic.[10] Minor iterative refinements, unbounded tool-use loops, or agent hallucinations can trigger massive, instantaneous spikes in API requests.[10] This leads to catastrophic rate-limiting failures, token exhaustion, and system bottlenecks that compromise the low-latency requirements (often sub-second response times) essential for real-time AI applications.[10] Traditional token-based or role-based authentication systems used in REST APIs also fail to adapt when agents dynamically request access to highly sensitive financial operations, creating a security gap in differentiating between human and agent interactions for intent verification.[10]

To alleviate these frictions, the industry has begun adopting specialized integration enablers and protocols.[1] The Model Context Protocol (MCP) emerged as an initial, critical standard, providing an open, JSON-RPC-based client-server architecture designed specifically for LLMs to securely discover, reason about, and access external datasets and tools.[9] MCP effectively solves the problem of connecting a single agent to a static enterprise backend, utilizing JSON-LD for structured context and allowing agents to orchestrate complex multi-step tasks

while maintaining state across sessions.[9]

However, MCP remains fundamentally insufficient for true agent-to-agent collaboration and delegated financial execution.[11] MCP enforces a strict, centralized client-server hierarchy.[11] In a mature A2A economy, agents act as autonomous peers, negotiating, planning, and exchanging tasks collaboratively. Forcing peer-to-peer agent interactions through a centralized client-server model requires one agent to artificially assume a server role (acting as a tool provider) while the other acts as the client.[11] This architectural mismatch prevents mutual initiation of communication, complicates asynchronous workflows, and fails to support structured negotiation.[11] MCP functions as a tool-invocation mechanism rather than a negotiation protocol. For actual economic transactions, where two autonomous entities must establish mutual trust, negotiate terms, and irrevocably authorize fund transfers, a dedicated peer-to-peer framework is required. This architectural void necessitates the implementation of specialized transactional frameworks, bringing AetherNet's Interoperability Layer into sharp focus.

The Interoperability Layer: AP2 Protocol and Cryptographic Mandates

To bridge the gap between autonomous agent decision-making and definitive financial execution, AetherNet natively integrates the Agent Payments Protocol (AP2) to route external AI mandates into its economic jurisdiction. AP2, developed collaboratively by an alliance of leading financial and technology entities—including Adyen, American Express, Coinbase, Mastercard, PayPal, and Google—operates as an open, payment-agnostic extension to A2A and MCP frameworks.[14] It directly addresses the core challenges of authorization, authenticity, and accountability in an environment where humans are not physically present to click a localized authorization button on a trusted graphical surface.[14]

The foundational innovation of the AP2 protocol is its absolute rejection of probabilistic AI inferences in favor of deterministic, cryptographic proof of intent.[15] Legacy payment gateways attempt to infer intent through behavioral tracking, a method that is obsolete for machine actors. AP2 instead utilizes Verifiable Digital Credentials (VDCs) acting as tamper-proof digital contracts, providing a common language of trust for secure, compliant transactions between agents and merchants.[14]

These VDCs are categorized into specific "Mandates" that anchor trust throughout the lifecycle of a transaction:

1. **The Intent Mandate:** Utilized primarily in "Human-Not-Present" scenarios, this VDC captures the specific parameters and constraints under which the agent is authorized to transact autonomously on the user's behalf.[15] It provides non-repudiable proof of intent, mitigating the risk of agent hallucination, misinterpretation, or account takeover by ensuring that only explicitly defined conditions (e.g., maximum price thresholds, specific

vendor selections, willingness to pay a premium) trigger execution.[16]

2. **The Cart Mandate:** Negotiated dynamically between a Shopping Agent and a Merchant Agent in "Human-Present" scenarios, this mandate finalizes the specific contents, pricing, SKUs, and shipping terms of a transaction.[15] It acts as a formal, binding bidirectional contract. The merchant entity signs it first to definitively guarantee fulfillment of the exact items and price, and the user subsequently signs it to explicitly authorize the finalized cart.[17] This shifts liability appropriately, resolving disputes by providing a non-repudiable audit trail of user approval.[17]
3. **The Payment Mandate:** Bound logically to the Cart or Intent mandate, this specific VDC provides the necessary visibility to the broader financial ecosystem, including payment processors, networks, and issuing banks.[15] It explicitly signals the presence of an AI agent and denotes whether the transaction modality is human-present or human-not-present.[17] This allows risk engines to evaluate the context of the transaction without relying on obsolete human behavioral heuristics, providing the clarity institutions need to effectively manage risk.[14]

To ensure that AP2 mandates cannot be spoofed, maliciously altered, or subjected to agent coercion, the cryptographic implementation must avoid the "Symmetric Fallacy." This fallacy describes the erroneous software engineering practice of treating symmetric HMACs (Hash-based Message Authentication Codes) as both proof of origin and permission to execute.[19] When verifying parties hold the identical keys used for signing, the system becomes highly susceptible to insider threats, forged lineage, and orphaned credential attacks, creating massive downstream settlement risks.[19]

AetherNet mandates an Asymmetric Pivot utilizing the Elliptic Curve Digital Signature Algorithm (ECDSA) to strictly separate signing keys from verification keys.[16] Within the AetherNet architecture, an external AI agent submits a compiled AP2 mandate payload. The heavily decoupled Node.js/TypeScript execution gateway intercepts this payload and immediately routes it to the secure Rust Trusted Execution Environment (TEE). The Rust TEE performs rigorous Know Your Agent (KYA) verification by parsing a Hierarchical Hash Binding pattern.[19] In this pattern, every submitted Cart Mandate must carry a nested JSON Web Token (JWT) digest that was cryptographically signed by the root Intent Mandate.[19] This creates an unbreakable, cryptographic chain of custody tightly linking the downstream algorithmic cart execution directly to the original human authorization.[19]

The illustrative transaction flow under AP2 is highly rigorous, involving up to 32 distinct steps of negotiation and cryptographic attestation between the Shopping Agent, Merchant Agent, and Credential Providers.[17] Crucially, in Step 21 of the flow—defined as the load-bearing step—the user verifies the details on a trusted device surface (such as a hardware secure element), generating a cryptographic attestation.[17] The Shopping Agent sends this attestation, combined with the Payment Mandate, to the Merchant Agent, who initiates the payment process.[17] Once the Rust TEE independently verifies this cryptographic signature against decentralized

allowlists and confirms the mandate complies with predefined policy engine rules, the system bypasses traditional, high-friction human UI requirements entirely.[16] It then passes the validated payload directly to the Canton ledger layer for immediate execution and settlement.

Protocol Characteristic	REST APIs	Model Context Protocol (MCP)	Agent Payments Protocol (AP2)
Primary Design Paradigm	Human-to-Machine (H2M)	Single Agent-to-Tool	Agent-to-Agent (A2A) Commerce
Architectural Model	Stateless Client-Server	Stateful Client-Server (JSON-RPC)	Peer-to-Peer / Multi-Entity
Payload Structure	Rigid, predefined JSON	Dynamic JSON-LD context	Verifiable Digital Credentials (VDCs)
Trust & Auth Model	Token/Role-based Auth (OAuth)	Tool-level authorization	Cryptographic Mandates (KYA / ECDSA)
State Awareness	None (Stateless)	High (Context injection)	High (Non-repudiable audit trails)
Economic Utility	General transactional endpoints	Data discovery and extraction	Deterministic, multi-party value settlement

The Execution Layer: Post-Quantum Cryptography in Trusted Execution Environments

As AetherNet establishes the economic jurisdiction for autonomous agents processing vast volumes of cross-border capital, the cryptographic primitives securing its execution layer must be immune to emerging existential threats. Traditional public-key cryptosystems, specifically those based on integer factorization (such as RSA) and discrete logarithms (such as Elliptic Curve Cryptography, or ECC), currently secure virtually all digital transactions, TLS handshakes, and identity verifications across global financial infrastructures.[21] However, these traditional systems are fundamentally vulnerable to the rapid advancement of large-scale quantum

computing. Once cryptanalytically relevant quantum computers (CRQCs) achieve sufficient maturity, algorithms such as Shor's algorithm will be capable of efficiently breaking RSA and ECC, rendering the foundation of digital commercial security obsolete in polynomial time.[21]

The urgency to migrate to Post-Quantum Cryptography (PQC) within financial execution environments is not contingent upon the immediate availability of CRQCs, which expert consensus generally places in the 2030s.[24] Rather, the absolute urgency is driven by the "Harvest Now, Decrypt Later" (HNDL) attack vector.[23] Well-resourced adversaries, including nation-states, are currently intercepting and storing highly sensitive, classically encrypted financial data, user mandates, and strategic communications over network layers today, with the explicit intent of decrypting them retroactively once quantum hardware matures.[23] Because AetherNet processes irrevocable financial execution data and binding KYA mandates, mitigating HNDL threats at the execution layer today is a paramount architectural necessity. Delayed preparation could leave current transactional data vulnerable for decades.[24]

To defend against quantum cryptanalysis, AetherNet's Rust-based Trusted Execution Environment (TEE) strictly integrates the finalized PQC standards officially released by the National Institute of Standards and Technology (NIST) in August 2024, following an exhaustive eight-year global evaluation effort.[24] The TEE isolates code and data execution in hardware-backed secure enclaves—such as Intel Software Guard Extensions (SGX) or Trust Domain Extensions (TDX)—to prevent malicious actors, including compromised cloud providers or malicious insiders with root access to the host operating system, from extracting cryptographic key material or manipulating the mandate verification logic.[28] This creates a Quantum Trusted Execution Environment (QTEE) capable of safeguarding user intent and financial state.[29]

The specific integration of post-quantum standards within AetherNet relies on the following algorithms:

1. **ML-KEM (FIPS 203 / CRYSTALS-Kyber):** A module-lattice-based key encapsulation mechanism utilized as the primary standard for secure, ephemeral key exchange. It is deployed during the establishment of TLS 1.3 connections between the external AI agent and the execution gateway, matching the performance of modern elliptic curves while providing quantum resistance.[25]
2. **ML-DSA (FIPS 204 / CRYSTALS-Dilithium):** A highly efficient lattice-based digital signature algorithm. Within AetherNet, ML-DSA is deployed for robust endpoint authentication and the critical signing and verification of the KYA AP2 mandates and the resulting SettlementReceipt contracts generated by the ledger layer.[25]
3. **SLH-DSA (FIPS 205 / SPHINCS+):** A stateless hash-based digital signature scheme retained as a fallback mechanism. Unlike Kyber and Dilithium, SLH-DSA derives its security from completely different mathematical assumptions (hash functions rather than structured lattices). It is intended as a backup method, providing profound defense-in-depth ensuring that if a novel mathematical vulnerability is discovered in

lattice-based cryptography, the system remains uncompromised.[23]

Deploying computationally intensive lattice and hash-based cryptography inside hardware enclaves introduces distinct performance challenges. TEEs, particularly architectures like Intel SGX, suffer from significant latency penalties if memory utilization exceeds the hardware-limited Enclave Page Cache (EPC), forcing costly cryptographic paging operations that can degrade performance by up to 1000x.[32] Furthermore, necessary Software Development Kit (SDK) mitigation patches against hardware vulnerabilities such as Spectre and Foreshadow add extra performance overhead for enclave transitions of up to 2.24x compared to original costs.[32] Post-quantum algorithms also natively demand substantially larger key sizes and transport payloads; for example, Kyber introduces over 1,091 bytes of key transport payload compared to RSA's 963 bytes, reducing theoretical bandwidth efficiency.[33]

However, rigorous empirical benchmarks demonstrate that these overheads are highly manageable within modern, optimized server architectures, particularly when executed via memory-safe languages like Rust. Implementations of Kyber-512 and Dilithium within Intel SGX secure enclaves exhibit highly competitive running times and memory resource requirements.[28] Across robust cloud infrastructures, the substitution of vulnerable RSA/ECC with ML-KEM and ML-DSA introduces less than a 5% increase in total computational latency, making immediate adoption highly feasible.[22]

Crucially, the impact on network throughput—specifically the time-to-last-byte for TLS 1.3 connections—diminishes rapidly as the volume of transferred application data increases.[34] Intuitively, introducing an extra 10KB of post-quantum cryptographic exchange during connection negotiation inflates the handshake time proportionally more than it impacts the total connection time of a Web connection carrying sizable data payloads.[34] Empirical studies quantify that for data payloads exceeding 50 KB, the overall latency increase from PQC handshakes drops below 15% even on low-bandwidth networks, and remains well below 5% in high-bandwidth, stable environments.[34] Even when network congestion control affects connection establishment, the additional slowdown drops below 10% as the connection data increases toward 200KiB.[34] By isolating the PQC cryptographic operations within the highly optimized Rust TEE, AetherNet processes complex AP2 mandates with sub-millisecond cryptographic overhead. This performance profile matches the rapid execution requirements of autonomous agents, vastly outperforming legacy RSA-3072 in secure session establishment, while guaranteeing quantum-resistant confidentiality and forward secrecy.[25]

Cryptographic Algorithm	NIST Standard	Mathematical Foundation	Primary Function in AetherNet	Payload / Overhead Characteristi

				cs
ML-KEM (CRYSTALS-Kyber)	FIPS 203	Module-Lattice	Ephemeral Key Exchange (TLS 1.3)	~1,091 bytes payload; Sub-millisecond latency.[25]
ML-DSA (CRYSTALS-Dilithium)	FIPS 204	Module-Lattice	Digital Signatures (AP2 KYA Mandates)	Highly efficient computational execution.[21]
SLH-DSA (SPHINCS+)	FIPS 205	Stateless Hash-Based	Backup Digital Signatures	Defense-in-depth; high assurance level.[23]
AES-256-GCM	FIPS 197	Symmetric Key	Symmetric Data Protection	Cost-effective; hardware accelerated.[25]

The Ledger Layer: Canton, Daml, and Deterministic Atomic Settlement

Once the Execution Layer cryptographically verifies an agent's AP2 mandate utilizing post-quantum security, the resulting financial transaction must be permanently settled. AetherNet firmly rejects the architecture of legacy public blockchains in favor of a live, decentralized Canton network executing Daml smart contracts. This paradigm enables instant, atomic, machine-to-machine settlement while providing the privacy and legal enforceability demanded by institutional participants.

The blockchain ecosystem features a sharp philosophical and architectural bifurcation between general-purpose public permissionless networks (e.g., Ethereum Virtual Machine environments) and privacy-preserving public permissioned networks (e.g., Canton).[35] The EVM architecture operates as a globally shared state machine, famously operating as a transparent "world computer." To maintain consensus in a permissionless, zero-trust environment, every full node must process every transaction and maintain a complete copy of the global state trie.[35] Transparency is structurally load-bearing; the entire security model depends on public verifiability, rendering base-layer data privacy structurally impossible.[35]

While this model fostered decentralized finance innovation, deploying institutional capital on

permissionless chains carries prohibitive regulatory and commercial consequences. Under the December 2022 Basel Committee on Banking Supervision standards, tokenized assets receive favorable capital treatment only if the underlying network's issuance, validation, and transfer functions sufficiently manage material risks.[36] In a subsequent consultative document, the Basel Committee concluded that assets tokenized on permissionless blockchain networks must be treated as Group 2 assets, receiving a severely punitive 1,250% risk weighting.[36] This categorization occurs because permissionless networks rely on unknown third parties for basic operations, categorically preventing banks from conducting the necessary due diligence, Anti-Money Laundering (AML), and oversight procedures.[36] Acting Comptroller of the Currency Michael Hsu explicitly criticized the "trustlessness" of public blockchains, noting that it makes AML compliance "extremely difficult".[36]

Conversely, Canton is engineered specifically to operate within strict regulatory guardrails, answering different institutional questions and avoiding these punitive capital charges.[35] Rather than forcing a replicated global ledger where data is broadcast universally, Canton utilizes a highly segmented data model providing explicit Row-Level Security.[36] In the Canton network, there is no single, unified ledger containing all transaction data. Instead, the protocol generates a "virtual" global ledger.[36] Each participant user of a Daml application maintains a ledger containing only the data it is explicitly permissioned to see.[37] The Canton protocol securely synchronizes this isolated data across designated counterparties, ensuring state validity and absolute encryption without broadcasting sensitive financial metadata to uninvolved network nodes.[37] Because AetherNet node operators on Canton dictate exactly who validates their transactions and to whom they connect, the network permits full AML/CFT compliance, enabling assets to qualify for Group 1 classification and unlocking immense institutional capital efficiency.[36] This institutional-grade architecture is already operating at massive scale, supporting over 400 institutions, processing more than 3 million daily transactions, and managing over $6 trillion in tokenized assets.[38]

The business logic dictating AetherNet's settlement layer is strictly codified using Daml, a smart contract language optimized exclusively for regulated entities.[39] Unlike Turing-complete, general-purpose languages like Solidity—which are highly susceptible to reentrancy attacks, unexpected state changes, and logical exploits—Daml is designed to explicitly model real-world legal agreements. Its core concepts act as direct translations of legal terms into executable logic, focusing strictly on "Rights," "Facts," "Obligations," and "Authorizations".[40] This ensures that the code acting on the network is a transparent, legally enforceable representation of a commercial contract.[40] Daml enforces explicit, role-based access control directly at the language level, ensuring that contracts specify exactly which parties can view or modify data, perfectly aligning with Canton's privacy-by-default architecture.[39]

Within AetherNet, the settlement flow executes with algorithmic precision. Following the TEE verification of the AP2 Mandate, the Rust gateway submits a cryptographic instruction to the Canton network. The system immediately locates the agent's pre-funded ServiceEscrow

contract, which holds the locked fiat capital, digital asset, or tokenized liability. Because the Daml contract enforces explicit access control, the specific autonomous workflow is executed privately between the payer, payee, and necessary network synchronizers.[39] In a sub-second, multi-party atomic transaction facilitated by Canton's Global Synchronizer, the Daml logic legally burns the ServiceEscrow contract, executing the payment transfer, and instantaneously mints an immutable SettlementReceipt.[39] This deterministic execution guarantees true Delivery-versus-Payment (DvP), ensuring that assets are transferred if and only if the corresponding payment is simultaneously cleared, completely eradicating settlement latency and counterparty default risk.

Legal Finality and the Regulatory Framework of Instant Settlement

The technological capacity to execute sub-second atomic settlements via post-quantum verified smart contracts must be irrevocably matched by robust legal frameworks. If the underlying legal jurisdiction does not recognize a cryptographic ledger update as the definitive, irreversible transfer of property rights, the technological speed of the network is legally irrelevant. AetherNet's deliberate reliance on Canton and Daml ensures total alignment with evolving global standards regarding digital asset finality and property law.

In the United States, the legal classification of digital assets and the specific mechanics of their transfer have been comprehensively modernized through the promulgation of Article 12 of the Uniform Commercial Code (UCC).[42] Historically, prior to the 2022 amendments, digital assets were categorized under Article 9 as "general intangibles".[43] This archaic classification required the filing of a traditional financing statement to perfect a security interest, a method that permitted the debtor to maintain exclusive control of the digital asset.[43] This framework was fundamentally incompatible with the fluid nature of decentralized ledgers, as debtors could instantaneously transfer assets across wallets, leaving creditors with legally unenforceable claims and stripping subsequent purchasers of "take free" protections.[43]

UCC Article 12 systematically resolves this legal friction by defining a new, bespoke class of assets: Controllable Electronic Records (CERs), which includes digital assets, cryptocurrencies, and controllable payment intangibles (CPIs) like U.S.-dollar-backed stablecoins.[42] Most pertinently, Article 12 establishes the foundational concept of "perfection by control," eliminating the need to rely solely on the filing of a financing statement.[44] For an AI agent transacting autonomously on AetherNet, establishing legal control over a CER requires demonstrating specific powers: the exclusive power to avail itself of substantially all the benefit from the CER, the exclusive power to prevent others from availing themselves of that benefit, the exclusive power to transfer control, and the cryptographic ability to readily identify itself as the entity holding these powers.[42]

Furthermore, Article 12 introduces the powerful legal concept of a "Qualifying Purchaser." If an

agent acquires control of a CER for value, in good faith, and without notice of adverse property claims, it takes the asset free of any competing property rights.[44] This overrides the traditional common law *nemo dat* rule (which states a purchaser acquires only what the seller had to give), providing absolute legal certainty for instantaneous M2M transactions.[44] By adhering to these definitions, AetherNet ensures that a minted SettlementReceipt resulting from the transfer of a CER is legally unimpeachable, providing a clear pathway to peace-of-mind between transacting autonomous parties.[46]

In European and international jurisdictions, the principle of settlement finality operates as a statutory, regulatory, and contractual construct dictating the exact moment a transfer of assets or financial instruments becomes unconditional and irrevocable, shielded against insolvency claw-back rules or moratoriums.[47] The EU Settlement Finality Directive (SFD) was designed specifically to reduce systemic risk by guaranteeing that transfer orders entering designated clearing and payment systems cannot be unwound, even if a participant subsequently declares bankruptcy.[47]

Traditional public blockchains achieve only "probabilistic finality." In these networks, the probability of a transaction being reversed decreases exponentially as new blocks are added to the chain, but mathematically, the probability never reaches absolute zero.[50] This probabilistic nature creates profound friction with the SFD and broader institutional risk management frameworks, presenting a major barrier to the deployment of wholesale settlement systems.[49]

AetherNet circumvents this legal and regulatory hurdle by leveraging the Canton architecture. Unlike probabilistic consensus mechanisms associated with Proof-of-Work or standard Proof-of-Stake, Canton provides deterministic finality.[50] Once a Daml smart contract executes the burning of a ServiceEscrow and records it via the global synchronizer, the state change is mathematically irreversible and absolute at that exact moment.[38] This deterministic architecture allows AetherNet to seamlessly interface with emerging regulatory frameworks, such as the EU's Markets in Crypto-Assets (MiCA) regulation, which imposes strict transparency and market integrity rules on issuers of asset-referenced tokens and e-money tokens.[51] It also aligns with pioneering initiatives like the Monetary Authority of Singapore's (MAS) Project Guardian. MAS has actively supported the live settlement of interbank overnight lending and tokenized assets utilizing wholesale Central Bank Digital Currencies (CBDCs) and institutional DLT on shared ledgers, precisely because systems like Canton support atomic, deterministic settlement of both cash and securities components, eliminating settlement risk across fragmented systems.[52]

The Economic Calculus of Liquidity Unlocking

The integration of instantaneous, deterministic atomic settlement into the financial ecosystem generates profound macroeconomic efficiencies, fundamentally altering the calculus of global liquidity management and capital deployment. The current structure of global finance is

burdened by massive inefficiencies resulting from latency.

Traditional securities clearing and cross-border payments operate on delayed settlement cycles, commonly Trade Date plus Two (T+2) or Trade Date plus Three (T+3) days. This temporal gap between execution and final settlement introduces severe replacement cost risk and counterparty default risk.[56] To mitigate this systemic risk, financial institutions are forced to deploy massive amounts of capital into centralized clearinghouses, default funds, and margin accounts, effectively trapping billions of dollars in unproductive escrow while trades finalize.[53] While regulatory efforts in the US, UK, and EU are attempting to compress this cycle to T+1, industry analysts correctly identify that moving incrementally without overhauling the underlying infrastructure will require costly operational changes while actually increasing risk due to compressed timeframes for manual reconciliation.[59]

Furthermore, while central banks do operate Real-Time Gross Settlement (RTGS) systems (such as the Federal Reserve's Fedwire or Europe's TARGET2) to process wholesale transfers in real-time, these systems are highly liquidity-intensive. Because payments settle immediately on a gross basis throughout the day, participants must pre-fund massive liquidity pools to ensure payments do not fail.[61] The cost of meeting these system liquidity needs is exceptionally high, frequently resulting in daylight overdrafts, capital inefficiencies, and the necessity of queuing mechanisms that ironically delay payments to economize on liquidity.[62]

AetherNet's deployment of a unified DLT ledger mechanism fundamentally resolves this conflict between settlement speed and liquidity costs. By combining programmable money (such as tokenized commercial bank deposits or wholesale CBDCs) with programmable assets within the same execution environment, the network enables true Delivery-versus-Payment (DvP) and Payment-versus-Payment (PvP).[56] Atomic settlement compresses the instruction, clearing, and settlement phases into a single, instantaneous automated event.[36] Because the execution via Daml smart contracts is highly conditional—the asset leg transfers if and only if the payment leg simultaneously transfers—counterparty risk is structurally eliminated.[64] Consequently, the requirement for central counterparties (CCPs) and massive margin buffers is drastically reduced, unlocking trapped capital for productive deployment and yielding immense operational savings.[53]

Empirical market data validates this economic advantage. Implementations of DLT-based intraday repo platforms, such as J.P. Morgan's Kinexys platform, have successfully replaced delayed tri-party arrangements with self-executing smart contracts. This platform has processed hundreds of billions in volume, allowing instantaneous DvP that settles in hours or minutes rather than days, directly unlocking trapped intraday liquidity.[67] The operational and funding cost savings generated by eliminating reconciliation delays represent a massive value unlock for the global financial system.[65]

Moreover, the necessity for a controlled, institutional-grade ledger like Canton over public, permissionless networks is starkly highlighted by the volatility of public stablecoins. Bank for

International Settlements (BIS) data tracking stablecoin price volatility during the failures of FTX and Silicon Valley Bank (SVB) revealed severe de-pegging events; for instance, USD Coin plummeted to 0.9018 against the dollar, while Tether fluctuated wildly.[56] Such volatility destroys the "singleness of money" required for large-scale economic stability.[56] AetherNet relies on regulated tokenized liabilities and institutional rails to ensure that atomic settlements occur with the absolute trust and parity of central bank money equivalents. By providing this hyper-efficient, capital-saving atomic capability directly to the autonomous AI agent economy, AetherNet ensures that the fastest computational entities in the market possess access to the most capital-efficient, risk-free settlement rails available.

Beyond Settlement: Universal Agent Orchestration and Web3 Integration

While AetherNet provides the definitive settlement layer for agentic commerce, its utility extends significantly beyond financial execution. AetherNet operates as a comprehensive, secure communication and data exchange backbone for networks of AI agents, mobile applications, and Internet of Things (IoT) devices.[68] To facilitate dynamic, highly decoupled interactions without fracturing security, the platform employs a multi-protocol architecture. It utilizes HTTPS (REST/JSON) for asynchronous message routing and task creation, Secure WebSockets (WSS) for persistent, low-latency bidirectional dialogues required during live agent negotiation, and Secure MQTT (MQTTS) for lightweight publish/subscribe messaging ideal for IoT telemetry and mobile notifications.[68]

Crucially, AetherNet is designed to interoperate securely with, rather than replace, emerging context standards like the Model Context Protocol (MCP). While MCP defines the *content* and structure—standardizing how context objects, datasets, and tool commands are formatted for an LLM—AetherNet defines the *orchestration and transport layer*.[68] Within this framework, an MCP context object acts as the highly sensitive data payload transported within an AetherNet message. AetherNet applies End-to-End Encryption (E2EE) using the recipient agent's public key, ensuring that only the intended model can decrypt and access the context.[68] This provides the secure transport, dynamic agent discovery registry, and workflow coordination required to elevate MCP from a simple single-agent tool connector into a secure, multi-agent enterprise framework.[68]

Furthermore, AetherNet's extensible design natively enables autonomous decentralized Web3 interactions. Agents operating within the AetherNet network can publicly declare specific Web3 capabilities—such as the ability to read/write to EVM-compatible blockchains (like Ethereum or Polygon) or store data on decentralized networks like the InterPlanetary File System (IPFS).[68] To maintain absolute security, AetherNet enforces a strict "Bring Your Own Key" policy; it stores an agent's public wallet addresses for discovery purposes but explicitly refuses to host or manage external blockchain private keys.[68]

This universal orchestration capability unlocks complex, non-financial autonomous workflows, such as dynamic, crowdsourced freight networks.[68] In a fully automated supply chain scenario, a shipper's application creates a transport task, prompting an AetherNet dispatcher agent to locate suitable driver agents based on their registered capabilities.[68] Driver agents submit encrypted bids via REST, while IoT cargo sensors transmit real-time temperature telemetry via MQTT.[68] Upon delivery, the driver agent can autonomously utilize its declared Web3 capabilities to store the immutable proof-of-delivery on IPFS and record the shipment completion on a Polygon smart contract, independently reporting the resulting transaction hashes back to the AetherNet task engine.[68] By seamlessly bridging real-time communication protocols, MCP payloads, and decentralized execution environments, AetherNet serves as the foundational nervous system for the broader autonomous economy.

Conclusion

The emergence of the autonomous AI agent economy demands an economic infrastructure capable of matching algorithmic computational velocity with uncompromised cryptographic security and absolute legal certainty. Legacy financial networks—encumbered by human-centric API workflows, multi-day settlement risks, behavioral fraud heuristics, and immense liquidity traps—are structurally inadequate to support the projected multi-trillion-dollar scale of agent-to-agent commerce.

AetherNet answers this commercial imperative by engineering a deeply integrated, institutional-grade substrate. By deploying the AP2 protocol, it establishes a mathematically verifiable, non-repudiable framework for delegated agent authorization that wholly eliminates the friction of REST APIs. By routing these algorithmic mandates through a Rust Trusted Execution Environment fortified with NIST-standardized Post-Quantum Cryptography, it neutralizes existential cryptographic threats and "Harvest Now, Decrypt Later" vectors with negligible latency overhead. Finally, by anchoring the transfer of value to the decentralized Canton network and executing deterministic Daml smart contracts, AetherNet provides immediate, legally binding atomic settlement that perfectly aligns with UCC Article 12 and the EU Settlement Finality Directive.

This architecture systematically eliminates counterparty risk, unlocks trapped market liquidity, and removes the friction of human intervention from the execution loop. Beyond financial transactions, its multi-protocol architecture securely transports MCP payloads, orchestrates complex IoT telemetry, and coordinates decentralized Web3 tasks without compromising security or assuming custody of private keys. Consequently, AetherNet stands not merely as an incremental payment gateway, but as the foundational economic jurisdiction and universal orchestration layer required to safely, legally, and efficiently scale the autonomous machine-to-machine economy for decades to come.

Works cited

1. Agentic commerce: How agents are ushering in a new era | McKinsey, accessed March 3, 2026, https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-agentic-commerce-opportunity-how-ai-agents-are-ushering-in-a-new-era-for-consumers-and-merchants
2. McKinsey forecasts up to $5 trillion in agentic commerce sales by 2030, accessed March 3, 2026, https://www.digitalcommerce360.com/2025/10/20/mckinsey-forecast-5-trillion-agentic-commerce-sales-2030/
3. Agentic Commerce Impact Could Reach $385 Billion by 2030 | Morgan Stanley, accessed March 3, 2026, https://www.morganstanley.com/insights/articles/agentic-commerce-market-impact-outlook
4. Agentic Commerce Market Report 2026 | $547M to $5.2B Growth Forecast - Sanbi.ai, accessed March 3, 2026, https://sanbi.ai/blog/agentic-shopping-market-trends
5. B2B Payments to Hit $224 Trillion by 2030 Globally, Driven by Emerging Market Expansion, accessed March 3, 2026, https://www.juniperresearch.com/press/b2b-payments-to-hit-224-trillion-by-2030-globally-driven-by-emerging-market-expansion/
6. How IoT will Shape the Future of Payments | Mastercard, accessed March 3, 2026, https://www.mastercard.com/news/media/wddjfrhn/how-iot-will-shape-the-future-of-payments.pdf
7. IoT value set to accelerate through 2030: Where and how to capture it - McKinsey, accessed March 3, 2026, https://www.mckinsey.com/capabilities/tech-and-ai/our-insights/iot-value-set-to-accelerate-through-2030-where-and-how-to-capture-it
8. A big future for small payments? Micropayments and their impact on the payment ecosystem - European Central Bank, accessed March 3, 2026, https://www.ecb.europa.eu/pub/pdf/other/ecb.micropaymentsimpactonnpaymentsecosystem202308~bb92cda8ce.en.pdf
9. Why REST APIs Aren't Built for Agentic Workflows: Introducing the Model Context Protocol (MCP) - Xano, accessed March 3, 2026, https://www.xano.com/blog/why-rest-apis-arent-built-for-agentic-workflows-introducing-mcp/
10. AI Agentic workflows and Enterprise APIs: Adapting API ... - arXiv.org, accessed March 3, 2026, https://arxiv.org/abs/2502.17443
11. Agent-to-Agent Is the New API: A Guide to the Protocols That Matter | by Will Gathright, PhD, accessed March 3, 2026, https://medium.com/@gathright/agent-to-agent-is-the-new-api-a-guide-to-the-protocols-that-matter-eda321a08d15
12. The Protocol Comparison That I Wish I Knew Earlier for AI Agents | by Zakariae Essaiydy, accessed March 3, 2026, https://medium.com/@zakaressaiydy/the-protocol-comparison-that-i-wish-i-knew-earlier-for-ai-agents-d105816ea0bd

13. A2A vs MCP vs AP2: Different Between AI Communication Protocols - Analytics Vidhya, accessed March 3, 2026, https://www.analyticsvidhya.com/blog/2025/10/a2a-vs-mcp-vs-ap2/
14. Announcing Agent Payments Protocol (AP2) | Google Cloud Blog, accessed March 3, 2026, https://cloud.google.com/blog/products/ai-machine-learning/announcing-agents-to-payments-ap2-protocol
15. AP2 - Agent Payments Protocol Documentation, accessed March 3, 2026, https://ap2-protocol.org/
16. Secure Use of the Agent Payments Protocol (AP2) | CSA, accessed March 3, 2026, https://cloudsecurityalliance.org/blog/2025/10/06/secure-use-of-the-agent-payments-protocol-ap2-a-framework-for-trustworthy-ai-driven-transactions
17. AP2 specification - AP2 - Agent Payments Protocol Documentation, accessed March 3, 2026, https://ap2-protocol.org/specification/
18. PayPal Community Blog | Agent Payments Protocol: Building Verifiable Trust for Agentic Commerce, accessed March 3, 2026, https://developer.paypal.com/community/blog/PayPal-Agent-Payments-Protocol/
19. Solving AI Agent Payment Authentication: A Technical Guide to AP2 Mandates, accessed March 3, 2026, https://sonnetandprose.com/blog/solving-ai-agent-payment-authentication-a-technical-guide-to-ap2-mandates/
20. Agent Payments Protocol (AP2): Complete Guide with Java Implementation - Medium, accessed March 3, 2026, https://medium.com/@visrow/agent-payments-protocol-ap2-complete-guide-with-java-implementation-aec56400d360
21. Performance Analysis of NIST Standardized Post-Quantum Cryptography Algorithms in Resource-Constrained IoT Environments - ResearchGate, accessed March 3, 2026, https://www.researchgate.net/publication/401137400_Performance_Analysis_of_NIST_Standardized_Post-Quantum_Cryptography_Algorithms_in_Resource-Constrained_IoT_Environments
22. A Practical Performance Benchmark of Post-Quantum Cryptography Across Heterogeneous Computing Environments - MDPI, accessed March 3, 2026, https://www.mdpi.com/2410-387X/9/2/32
23. Post-Quantum Cryptography and Quantum-Safe Security: A Comprehensive Survey - arXiv.org, accessed March 3, 2026, https://arxiv.org/html/2510.10436v1
24. Are Enterprises Ready for Quantum-Safe Cybersecurity? - arXiv, accessed March 3, 2026, https://arxiv.org/html/2509.01731v1
25. Design and implementation of an authenticated post-quantum session protocol using ML-KEM (Kyber), ML-DSA (Dilithium), and AES-256-GCM - Frontiers, accessed March 3, 2026, https://www.frontiersin.org/journals/physics/articles/10.3389/fphy.2025.1723966/full
26. Post-quantum cryptography | NIST - National Institute of Standards and Technology, accessed March 3, 2026, https://www.nist.gov/pqc

27. What Is Post-Quantum Cryptography? - NIST, accessed March 3, 2026, https://www.nist.gov/cybersecurity-and-privacy/what-post-quantum-cryptography
28. Implementing CRYSTALS Kyber and Dilithium in Intel SGX Secure Enclaves, accessed March 3, 2026, https://www.semanticscholar.org/paper/Implementing-CRYSTALS-Kyber-and-Dilithium-in-Intel-Pratiwi-Firmansyah/d6a6c0ab6b675c970a67237ac14a0fca31b94dd8
29. Trusted execution environments for quantum computers - Frontiers, accessed March 3, 2026, https://www.frontiersin.org/journals/computer-science/articles/10.3389/fcomp.2025.1521059/full
30. NIST's post-quantum cryptography standards are here - IBM Research, accessed March 3, 2026, https://research.ibm.com/blog/nist-pqc-standards
31. NIST Releases First 3 Finalized Post-Quantum Encryption Standards, accessed March 3, 2026, https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards
32. SGXoMeter: Open and Modular Benchmarking for Intel SGX, accessed March 3, 2026, https://www.ibr.cs.tu-bs.de/users/mahhouk/papers/eurosec2021.pdf
33. Performance and Storage Analysis of CRYSTALS-Kyber (ML-KEM) as a Post-Quantum Replacement for RSA and ECC - arXiv, accessed March 3, 2026, https://arxiv.org/html/2508.01694v3
34. The impact of data-heavy, post-quantum TLS 1.3 on the Time-To-Last-Byte of real-world connections - CSRC, accessed March 3, 2026, https://csrc.nist.gov/csrc/media/Events/2024/fifth-pqc-standardization-conference/documents/papers/the-impact-of-data-heavy-post-quantum.pdf
35. Canton Network vs. EVM-Compatible Blockchains: A Technical Reckoning - DeFi Prime, accessed March 3, 2026, https://defiprime.com/canton-vs-evm
36. Beyond Public Versus Private: Connectivity and Control Within ..., accessed March 3, 2026, https://www.digitalasset.com/hubfs/Canton_Connectivity%20and%20Control%20Within%20Regulatory%20Guardrails_FINAL.pdf?hsLang=en
37. A Regulatory Perspective - The Canton Network, accessed March 3, 2026, https://www.canton.network/blog/the-canton-network-a-regulatory-perspective-1
38. Canton Network: Most Realistic Blockchain - by Ryan Yoon - Tiger Research Reports, accessed March 3, 2026, https://reports.tiger-research.com/p/canton-network-most-realistic-blockchain-eng
39. Canton First Look: Bringing Traditional Finance Onchain - Figment, accessed March 3, 2026, https://www.figment.io/insights/canton-first-look-bringing-traditional-finance-onchain/
40. DAML Development for Business: A Practical Guide to Building Multi-Party

Applications, accessed March 3, 2026, https://pixelplex.io/blog/daml-development-guide/
41. The structure and flow of Daml smart contracts: Part 1 - Digital Asset Blog, accessed March 3, 2026, https://blog.digitalasset.com/blog/-daml-smart-contract-structure-part-1
42. UCC Article 12: How States are Regulating Digital Asset Transactions | Paul Hastings LLP, accessed March 3, 2026, https://www.paulhastings.com/insights/crypto-policy-tracker/ucc-article-12-how-states-are-regulating-digital-asset-transactions
43. UCC Article 12: New Protections for Crypto Creditors | Ave Maria School of Law, accessed March 3, 2026, https://www.avemarialaw.edu/ucc_article12/
44. THE NEW UCC ARTICLE 12: WHAT YOU NEED TO KNOW NOW - American College of Bankruptcy, accessed March 3, 2026, https://www.americancollegeofbankruptcy.com/file.cfm/19/docs/panel%205-cryptocurrency.pdf
45. UCC Articles 9 and 12: A Modern Legal Framework for Secured Transactions and Digital Assets | Lowenstein Sandler LLP, accessed March 3, 2026, https://www.lowenstein.com/news-insights/publications/articles/ucc-articles-9-and-12-a-modern-legal-framework-for-secured-transactions-and-digital-assets-citron-caporale-podolnyy
46. EMERGING TECHNOLOGIES AND LAGGING LAWS: ARTICLE 12 AND THE UCC™S ATTEMPT TO COMMERCIALLY INCORPORATE THE RAPIDLY CHANGING WORL, accessed March 3, 2026, https://mckinneylaw.iu.edu/practice/law-reviews/ilr/pdf/vol56p417.pdf
47. Settlement finality - Finance - European Commission, accessed March 3, 2026, https://finance.ec.europa.eu/capital-markets-union-and-financial-markets/financial-markets/post-trade-services/settlement-finality_en
48. EU Launches Review of the Settlement Finality Directive - A&O Shearman | FinReg, accessed March 3, 2026, https://finreg.aoshearman.com/EU-Launches-Review-of-the-Settlement-Finality-Dir
49. On Settlement Finality and Distributed Ledger Technology, by Nancy Liao, accessed March 3, 2026, https://www.yalejreg.com/nc/on-settlement-finality-and-distributed-ledger-technology-by-nancy-liao/
50. The Impact of Distributed Ledger Technology in Capital Markets, accessed March 3, 2026, https://www.gfma.org/wp-content/uploads/2025/08/1.-full-report-impact-of-dlt-in-cap-mkts-final-1.pdf
51. Markets in Crypto-Assets Regulation (MiCA) - ESMA - European Union, accessed March 3, 2026, https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica
52. Distributed Ledger Technology (DLT) - Monetary Authority of Singapore, accessed March 3, 2026,

https://www.mas.gov.sg/development/fintech/technologies---blockchain-and-dlt
53. Fixed Income Framework - Monetary Authority of Singapore, accessed March 3, 2026, https://www.mas.gov.sg/-/media/mas-media-library/development/fintech/guardian/guardian-fixed-income-framework-v1_1.pdf
54. MAS Announces Successful Live Trial of Settlement of Interbank Overnight Lending Using Wholesale Central Bank Digital Currency - Monetary Authority of Singapore, accessed March 3, 2026, https://www.mas.gov.sg/news/media-releases/2025/mas-announces-successful-live-trial-of-settlement-of-interbank-overnight-lending
55. GUARDIAN - Monetary Authority of Singapore, accessed March 3, 2026, https://www.mas.gov.sg/schemes-and-initiatives/project-guardian
56. III. Blueprint for the future monetary system: improving the old ..., accessed March 3, 2026, https://www.bis.org/publ/arpdf/ar2023e3.htm
57. ESMA74-2119945925-1969 Report on ESMA assessment of the shortening of the settlement cycle in the European Union, accessed March 3, 2026, https://www.esma.europa.eu/sites/default/files/2024-11/ESMA74-2119945925-1969_Report_on_shortening_settlement_cycle.pdf
58. The Benefits of Shortening the Securities Settlement Cycle - SEC.gov, accessed March 3, 2026, https://www.sec.gov/newsroom/speeches-statements/benefits-shortening-securities-settlement-cycle
59. T+0? More Risk, Fewer Benefits - SIFMA, accessed March 3, 2026, https://www.sifma.org/news/blog/t0-more-risk-fewer-benefits
60. Shorter settlement cycles: global alignment or fragmented markets? | PwC UK, accessed March 3, 2026, https://www.pwc.co.uk/financial-services/assets/pdf/shorter-settlement-cycles-global-alignment-or-fragmented-markets.pdf
61. What is T2? - European Central Bank, accessed March 3, 2026, https://www.ecb.europa.eu/paym/target/t2/html/index.en.html
62. Economizing on Liquidity with Deferred Settlement Mechanisms - FEDERAL RESERVE BANK of NEW YORK, accessed March 3, 2026, https://www.newyorkfed.org/research/epr/04v10n3/0412mcan/0412mcan.html
63. Liquidity usage in TARGET2 - European Central Bank, accessed March 3, 2026, https://www.ecb.europa.eu/press/economic-bulletin/articles/2021/html/ecb.ebart202103_03~2e159cbd38.en.html
64. Distributed Ledger Technology Experiments in Payments and Settlements in - IMF eLibrary, accessed March 3, 2026, https://www.elibrary.imf.org/view/journals/063/2020/001/article-A001-en.xml
65. Settlement compression – where next? - flow – Deutsche Bank, accessed March 3, 2026, https://flow.db.com/topics/trust-and-securities-services/settlement-compression-where-next
66. What Is Atomic Settlement? - Liberty Street Economics, accessed March 3, 2026, https://libertystreeteconomics.newyorkfed.org/2022/11/what-is-atomic-settleme

nt/
67. The Impact of Distributed Ledger Technology in Capital Markets - ASIFMA, accessed March 3, 2026, https://www.asifma.org/wp-content/uploads/2025/09/full-report-dlt-report-final3.pdf
68. AetherNet_API Design_ Secure AI Agent Network Communication(1).pdf