FRANKLIN TEMPLETON

Perspective from Franklin Templeton Digital Assets

Agentic AI and Blockchain Infrastructure

Decentralization, concentration risk, and value capture across trust, payments, execution, and interoperability layers

May 2026 | White Paper

Executive Summary

For analytical purposes, we group blockchain infrastructure into eight functional categories: (1) base protocol and settlement, (2) access, (3) execution and ordering, (4) data and oracles, (5) interoperability, (6) trust and attestation, (7) payments, and (8) governance and control.

Agentic AI is likely to increase demand across this infrastructure by enabling autonomous software agents to transact, coordinate, verify information, and execute workflows with limited human involvement. In our view, the resulting opportunity is less likely to sit in applications alone and more likely to develop across the systems that make agent activity reliable, verifiable, and repeatable at scale. Early examples already point in that direction: ERC-8004[1] illustrates how identity, reputation, and validation could strengthen the trust and attestation category for autonomous agents, while x402[2] shows how machine-native payments may become embedded directly in API-driven workflows.



Priti Kumari
Research Analyst
Franklin Templeton
Digital Assets



Lou Mohn
Portfolio Manager
Franklin Templeton
Digital Assets



Christopher Jensen
Head of Research
Franklin Templeton
Digital Assets

Key Takeaways

- **Early trust-layer adoption is already concentrated.**
  BNB, Ethereum, and Base account for ~74% of ERC-8004 Registrations, indicating that agent-related trust infrastructure is clustering in a small number of ecosystems rather than diffusing broadly.
- **Machine-native payments are moving from concept to measurable usage.**
  By December 11, 2025, the official x402 V2 launch post said x402 had processed over 100 million payments across APIs, apps, and AI agents after launching in May 2025, suggesting early evidence of repeatable machine-to-machine transaction flows.
- **Infrastructure dependency can override protocol-level decentralization.**
  The March 2025 Infura outage shows that user access can fail even when the underlying blockchain remains live, underscoring the importance of resilient access infrastructure.
- **Economic control is more concentrated than surface-level metrics suggest**.
  On Ethereum, three entities (Lido, Binance, ether.fi) control >33% of staked ETH, This shows that a high number of validators does not necessarily mean control is widely distributed.
- **Agent-driven activity may increase reliance on a narrow set of providers.**
  As agents optimize latency, reliability, and cost, usage may converge default infrastructure providers across Remote Procedure Call (RPC)[3], execution, data, and payments.
- **Low-cost automation increases the economic importance of identity and validation.**
  As the number of agents grows, Sybil risk—the risk that one actor can create or control many fake identities—rises at the application layer, increasing demand for identity, attestation, and reputation infrastructure.
- **Value capture is likely to emerge at workflow bottlenecks, not at the application layer.**
  Infrastructure that controls access, execution, trust, payments, or interoperability is better positioned to capture durable economic rents than layers exposed only to increased usage.

Specific securities and companies mentioned are for illustrative purposes and are not investment recommendations or discussions about any current Franklin Templeton holdings.

1. ERC-8004 – a proposed Ethereum standard that enables AI agents to carry verifiable identity and reputation across platforms, allowing systems to assess trust and interact with them reliably.
2. x402 – an open payment protocol that enables APIs, apps, and AI agents to make machine-native payments directly within online workflows, using HTTP payment requests instead of traditional checkout flows.
3. RPC (Remote Procedure Call) – a way for apps or AI agents to connect to a blockchain to read data or submit transactions.

Not FDIC Insured | No Bank Guarantee | May Lose Value

Table of Contents

Executive Summary

Key Takeaways

1. Why Now?

2. Market-Structure Thesis

3. Where Value May Accrue
   - Access / RPC
   - Execution / Ordering
   - Trust Infrastructure
   - Payments

4. Key Risks
   - Business Continuity Risk
   - Concentration Risk
   - Governance and Policy Risk
   - Identity and Authorization Risk

5. Assessment Framework: What to Check and Track

6. Trust Infrastructure: Identity, Validation, and Agent-Native Payments
   - Why Trust Infrastructure Matters
   - ERC-8004: Identity, Reputation, and Validation Registries
   - Solana's Trust Stack
   - Agent-native Payments: Payment Rails as a Complementary Layer
   - Assessment Takeaways

7. Blockchain Readiness for Agentic Workloads

8. Decentralized AI Infrastructure

9. Conclusion

10. Appendices
    - Appendix A. Nakamoto Coefficient (NC): Definition and "Which NC Is This?"
    - Appendix B. Ethereum NC Calculation (9 March 2026) — Entity-Level Stake NC (33%)
    - Appendix C. Technical Overview of Fetch.ai and Bittensor

11. References

1. Why Now?

As defined in the Executive Summary, we assess blockchain infrastructure across eight functional layers: base protocol and settlement, access, execution and ordering, data and oracles, interoperability, trust and attestation, payments, and governance and control.[4] These layers are not new. What has changed is that autonomous software is beginning to use them in more practical and repeatable ways. In 2026, the key question is no longer whether blockchain can support software agents in theory, but which infrastructure layers are already showing live usage.

The clearest current signal is payments. x402 is one of the strongest public examples of machine-native payment infrastructure moving into real use. The draft notes that x402 launched in May 2025, reported more than 100 million payments by December 2025, and by April 2026 was associated with 165M+ transactions, more than $50M in volume, and more than 480K transacting agents. That does not prove long-term adoption, but it does show that blockchain payment rails are becoming operational rather than conceptual. This matters because payments have long been a missing piece in autonomous digital systems: Once software can discover a service, pay for it directly, and complete a transaction without manual billing or approval, blockchain infrastructure becomes more relevant to real economic activity.

Trust infrastructure is also beginning to show visible traction. The draft presents ERC-8004 as a framework for identity, reputation, and validation registries, and it points to early activity across Ethereum-compatible environments alongside parallel trust architecture on Solana. Tempo and MPP also suggest that dedicated payment infrastructure is beginning to form around machine-native commerce. Taken together, these developments make 2026 a more meaningful point of analysis than 2023–2024: The issue is no longer whether blockchain may eventually support autonomous software, but which infrastructure layers are already becoming embedded in live activity.

Infrastructure layer	Current signal	Why it matters now
Payments	x402 has reported substantial payment activity, while Tempo and MPP point to emerging machine-payment rails	Machine-native payments are moving from concept toward live use
Trust and attestation	ERC-8004 is showing early activity in EVM environments, while Solana has live registry and attestation components	Identity, validation, and reputation are becoming reusable infrastructure

Beyond crypto-native efforts, NIST's AI Agent Standards Initiative and related work on agent identity and authorization suggest that these issues are moving into a broader institutional standards agenda.

4. Oracles – services that bring real-world data, such as prices, events, or outcomes, onto a blockchain so smart contracts can use it.

2. Market-Structure Thesis

The key question is not simply which protocols see higher usage, but which layers have the pricing power and durability to monetize rising agent-driven activity. Value is most likely to accrue at infrastructure bottlenecks that are difficult to bypass. Agentic AI may expand demand for blockchain-based trust, payment, data, execution, and interoperability infrastructure more than for application layers alone. As agents operate continuously and at scale, economic upside may shift toward the infrastructure layers that enable settlement, routing, verification, and reliable access.

We evaluate blockchain infrastructure through three lenses: value capture (pricing power, monetization, durability), control (bottlenecks, routing power, switching costs, dependency), and resilience (failure domains and concentration-adjusted resilience).

Our core thesis is that agent-driven activity could increase utilization across the blockchain infrastructure while creating more selective revenue opportunities across infrastructure providers. RPC providers, which give applications and agents access to blockchain nodes for reading data and submitting transactions, along with oracle networks, execution venues, bridge infrastructure, and emerging trust/payment rails may become disproportionate beneficiaries if autonomous workflows scale. The same dynamic may also increase concentration risk, because a network can appear decentralized at the protocol layer while remaining dependent on a small number of providers across access, execution, governance, or data layers.

The key distinction is between infrastructure that is merely exposed to higher activity and infrastructure that is structurally positioned to capture durable economic rents from that activity (De Rossi et al., 2025; Infura, 2025). This makes subsystem-level concentration analysis as important as headline network activity. By subsystem-level, we mean concentration within a specific functional layer of the blockchain layer—such as RPC access, sequencing,[5] oracle delivery, bridge operations,[6] or governance—rather than across the network in aggregate. The paper's framework supports this directly: the Nakamoto Coefficient (NC) should be assessed according to the control threshold of the subsystem that actually matters. As Appendix B indicates, validator count in Ethereum is therefore a less informative measure than entity-level dependency or entity-level influence. By entity-level dependency, we mean the degree to which a given subsystem relies on a small number of firms, operators, or affiliated organizations to function; by entity-level influence, we mean the degree to which those entities can shape outcomes, route activity, impose bottlenecks, or extract rents within that subsystem.

Investment Implications:

- Infrastructure layers with embedded workflow control (RPC, execution, trust, payments) appear favorable
- Prioritize systems with high switching costs and developer integration depth
- Be cautious of high-usage layers without monetization power
- Treat protocol decentralization as insufficient—underwrite subsystem concentration
- Key question: Is this layer a bottleneck, or is it easily replaceable?

3. Where May Value Accrue?

Value is most likely to accrue where agent activity creates measurable dependence on infrastructure that is hard to bypass and repeatedly used in live workflows. In practice, the relevant evidence is concentration, usage, and control: who handles access, who determines execution quality, where trust-layer activity is clustering, and whether payment rails are moving from concept to repeatable use.

Access / RPC

The March 2025 Infura Ethereum Mainnet JSON-RPC partial outage illustrates the core economic point: chain uptime and user uptime can diverge when access depends on concentrated providers. Chain uptime refers to the blockchain itself remaining live, with blocks still being produced, transactions still able to settle, and the protocol continuing to function at the network level. User uptime refers to whether users, applications, and agents can actually reach and use the chain in practice through the access layer, including RPC endpoints and wallet defaults. The most useful indicators for this layer are top-3 RPC provider share, outage frequency at default endpoints, and the presence or absence of credible failover routing. If agent workflows depend on a small number of default endpoints, access becomes both a bottleneck and a potential value-capture layer.

5. Sequencing – the process of ordering transactions before they are added to a blockchain or rollup.
6. Bridge operations – the infrastructure and processes that move assets or data between different blockchains.

Execution / ordering

This category should be assessed using practical performance indicators, not validator counts alone. The key question is not only how decentralized the blockchain is, but who controls the ordering and successful processing of transactions. Useful indicators include the share of transaction ordering handled by the largest builders, relays, or sequencers; transaction speed; time to final settlement; and failed transaction rates. As AI agents prioritize speed, reliability, and execution certainty, these measures become more useful for identifying where control and economic value may concentrate.

Trust infrastructure. Early trust-layer activity is already showing concentration in Ethereum-compatible environments: Figure 3 shows ERC-8004 registrations led by BNB, Ethereum, and Base, indicating that trust-related identity, reputation, and validation infrastructure is beginning to cluster in a small number of EVM ecosystems. At the same time, Solana's Agent Registry and Solana Attestation Service suggest that comparable trust architecture is also emerging outside the EVM stack.[7] Taken together, these signals suggest that trust infrastructure is becoming a reusable layer across ecosystems rather than a chain-specific feature.

Payments

Payments are the clearest live signal in the draft. x402 launched on May 6, 2025, the x402 V2 launch post said by December 11, 2025 that it had processed more than 100 million payments, and by April 20, 2026 the draft records 165M+ transactions, more than $50M in volume, and more than 480K transacting agents; the public site also showed 75.41M transactions and $24.24M in volume over the preceding 30 days. Tempo adds a second signal: as of March 18, 2026, its mainnet was live and MPP had launched alongside a payments directory for machine-compatible services. Taken together, these data suggest that machine-native payments are moving from design concept toward usable production infrastructure.

4. Key Risks

Decentralized systems often present a surface appearance of resilience and distributed control, yet critical dependencies can introduce hidden points of fragility. Understanding how risks emerge across infrastructure, economic concentration, governance, and identity layers is essential to assessing the true robustness of these networks.

- Business continuity risk chain uptime and user uptime can diverge. Chain uptime refers to the blockchain itself remaining live, with blocks still being produced, transactions still able to settle, and the protocol continuing to function at the network level. User uptime refers to whether users, applications, and agents can actually reach and use the chain in practice through the access layer, including RPC endpoints and wallet defaults. When access depends on a concentrated provider, disruptions at that layer can impair practical usability even if the underlying chain remains live. The March 2025 Infura Ethereum Mainnet JSON-RPC partial outage illustrates this distinction: The chain remained live, but intermittent endpoint unavailability disrupted access during investigation and remediation.
- **Concentration risk:** control can concentrate in a small number of operators across the blockchain infrastructure layers —staking entities, builders/relays, sequencers, bridges, and oracle providers—making headline validator counts an incomplete proxy for resilience. Ethereum illustrates the distinction between protocol decentralization and economic concentration. Headline validator counts can suggest broad participation, but the economically relevant question is how much stake is controlled by independent entities rather than how many validator instances exist. This distinction also appears in early trust infrastructure adoption. Figure 3 shows ERC-8004 events led by BNB, Ethereum, and Base, which together account for roughly three-quarters of the displayed activity. Likewise, Appendix B shows that Ethereum's entity-level stake NC (Nakamoto Coefficient) is 3 at the 33% threshold, meaning that only three independent entities are needed to reach that level of stake concentration.

A network can appear decentralized at the protocol layer while remaining economically concentrated at the access, execution, governance, or data layer.

7. EVM stack – the group of blockchain networks and tools that are compatible with Ethereum's smart contract system, allowing apps and infrastructure to work across Ethereum-like chains.

- **Governance and policy risk**: In many systems, especially Layer 2, control is embedded in upgrade and administrative mechanisms (security councils, multisigs). On Optimism, a Security Council multisig can authorize protocol upgrades and certain emergency actions, illustrating how upgrade authority can be concentrated even in widely used systems (Optimism Collective, 2023).
- **Identity and authorization risk:** As the number of low-cost agents rises, application-layer systems that treat wallets or agent instances as distinct participants may become more vulnerable to Sybil-style behavior. This is most relevant in airdrops, wallet-based governance, faucets—services that distribute small amounts of tokens, often for testing, onboarding, or promotional use—agent marketplaces, social layers, and reputation systems, particularly in low-fee environments. The issue is distinct from consensus-layer security and should be assessed at the application layer and in the identity, attestation, and reputation systems that support it.

5. Assessment Framework: What to Check and Track

Assessment should be done at the subsystem level rather than at the protocol level alone. The relevant question is not simply whether a blockchain appears decentralized, but whether the layers most exposed to agent-driven activity are diversified enough to avoid chokepoint risk while still positioned to capture value. The matrix below identifies the main control surfaces in agent-driven blockchain infrastructure, the questions that matter most, and the indicators that are most useful to track over time.

Assessment Matrix: What to Check and Track by Layer

Layer	What to check	Metrics to track	Why it matters
Access / RPC	Whether access depends on a small number of default providers, and whether credible failover routing exists	Top-3 RPC provider share; outage frequency at default endpoints; failover coverage	A chain can remain live while agent workflows fail if access is concentrated and redundancy is weak
Execution / Ordering	Whether builders, relays, or sequencers control execution quality and inclusion certainty	Share of ordering handled by top builders, relays, or sequencers; latency / time-to-finality; failed execution rate	Agents optimize for speed and certainty, so value and control may shift toward execution layers rather than consensus alone
Data / Oracles	Whether agents rely on a narrow set of machine-readable data providers	Share of updates or integrations concentrated in top oracle or data-feed providers; stale-feed incidents	Agent workflows depend on timely, trusted data, making oracle concentration a potential chokepoint
Bridges / Interoperability	Whether cross-chain workflows depend on a small number of bridges or interoperability layers	Cross-chain volume concentration; signer-set concentration; bridge outages or security incidents	As agents operate across chains, interoperability layers can become both value-capture points and failure domains
Governance / Upgrade Control	Who can upgrade, pause, or override the system, and whether emergency powers are concentrated	Multisig or council concentration; timelock length; scope of upgrade authority	A system may appear decentralized at the protocol layer while remaining centrally controlled through governance mechanisms
Trust Infrastructure	Whether identity, reputation, attestation, and validation layers are becoming portable, auditable, and interoperable	Registered agents; attestations or validation events; reputation entries; proof-of-personhood adoption	As low-cost automation scales, trusted participation becomes harder to establish without dedicated identity and validation infrastructure
Payments	Whether agent-native payment rails are moving from concept toward repeatable usage and integration	Payment count; payment volume; average transaction cost; repeat-use or session-based payment flows; developer integrations	Real adoption requires payment rails that are not only technically possible, but cheap, repeatable, and embedded in live workflows

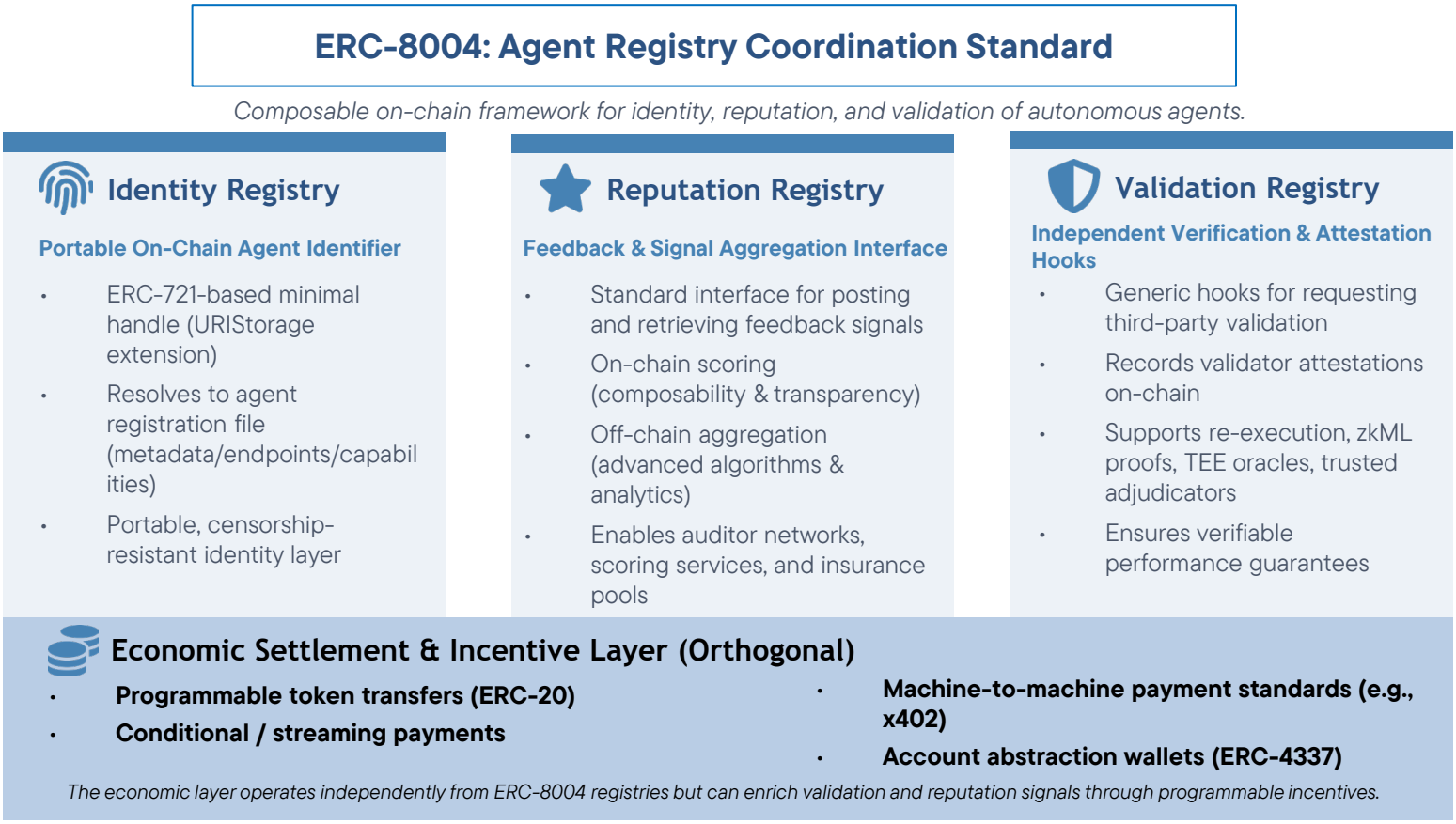
6. Trust Infrastructure: Identity, Validation, and Agent-Native Payments

Why Trust Infrastructure Matters

As agent workflows move from experimentation to production, the key constraint shifts from capability to credibility. The relevant question is not only whether an agent can act, but whether its identity can be verified, its performance tracked, and its outputs independently validated. In that context, trust infrastructure may become a distinct layer of blockchain market structure.

As the number of low-cost AI agents increases, the feasible scale of Sybil-style behaviours—the ability of one actor to create or control many fake or coordinated identities—also rises. The relevant risk sits primarily at the application layer rather than at the consensus layer: systems that rely on wallet count, agent count, or shallow reputation signals can become easier to game, particularly in airdrops—token distributions based on wallet activity or other eligibility rules—wallet-based voting, faucets, agent marketplaces, social and reputation layers, and low-fee chains and L2s. This increases the economic importance of identity, proof-of-personhood, authorization, attestation, and validation infrastructure. In the near term, the clearest market may be anti-Sybil, proof-of-personhood, and agent-trust infrastructure for airdrops, governance, reputation, and emerging agent platforms, especially in higher-value workflows that need to distinguish trusted from low-cost automated participation.

ERC-8004: Identity, Reputation, and Validation Registries



For Illustrative Purposes Only. Not an investment recommendation.

Figure 2. ERC-8004 proposes a composable trust layer for autonomous agents, centered on identity, reputation, and validation registries, with payments operating as an orthogonal economic layer.

- **Identity Registry:** portable on-chain agent identifier linked to metadata, endpoints, and capabilities.
- **Reputation Registry:** standard interface for posting and retrieving feedback signals.
- **Validation Registry:** records independent verification, including re-execution, zkML[8] (zero-knowledge machine learning) proofs, TEE attestations, or trusted adjudication.
- **Strategic relevance:** if adopted, this type of standard could support monetizable identity, compliance, and verification infrastructure

8. zkML (zero-knowledge machine learning) – a method that proves an AI model produced a result correctly without revealing the model's private data or full internal details.

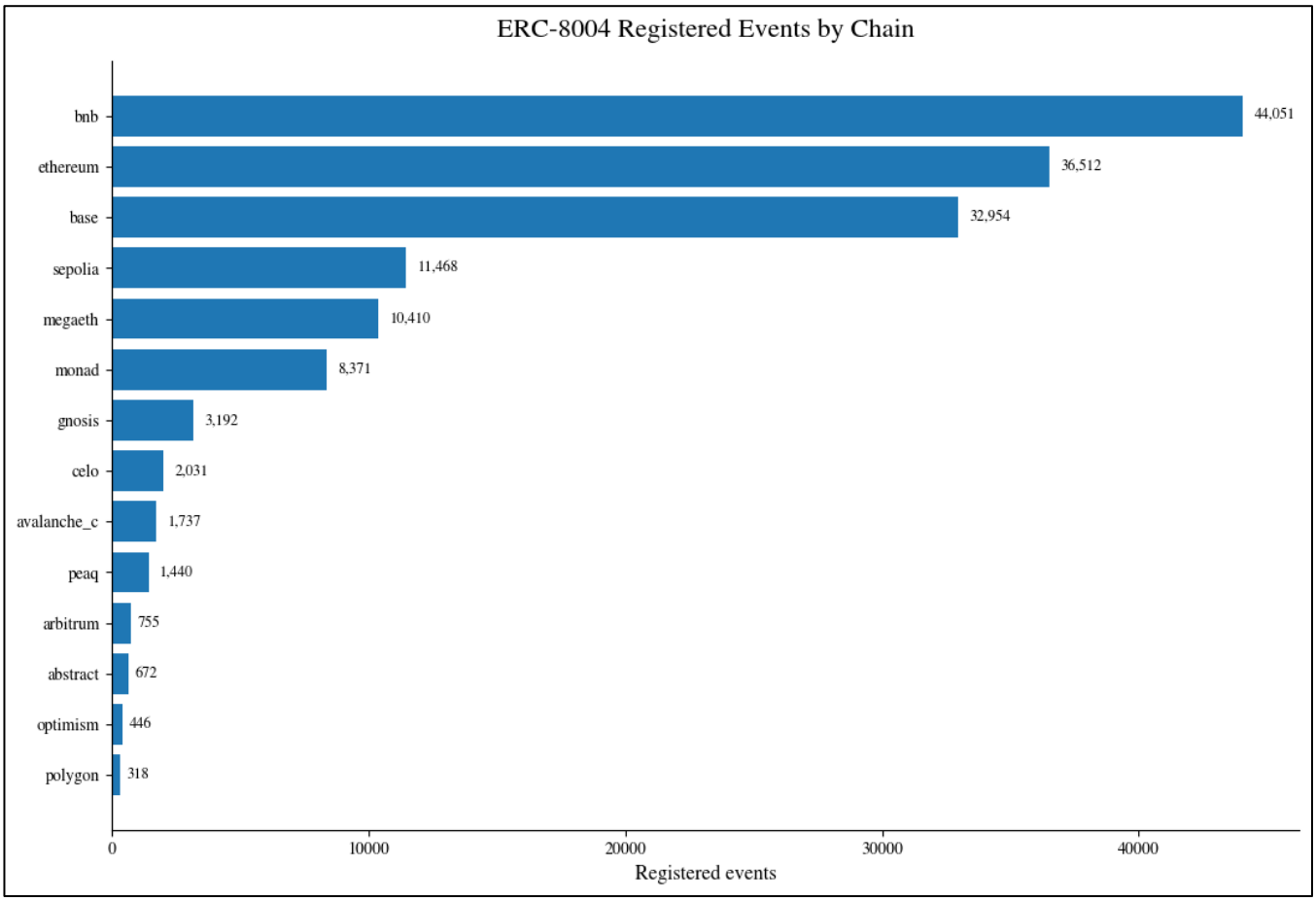


Figure 3: ERC-8004 registered events by chain. Source: Dune Analytics, ERC-8004 dashboard, data accessed March 21, 2026.

This chart shows that ERC-8004 is seeing early uptake across multiple Ethereum-compatible environments, with activity concentrated in the chains where agent experimentation and on-chain coordination are already most active. In the context of this paper, the signal is not "blockchain adoption" in the abstract, but growing use of trust infrastructure—identity, reputation, and validation registries—as a functional layer for autonomous agent workflows.

Solana's Trust Stack

Solana presents a parallel trust architecture through its Agent Registry and Solana Attestation Service. The stack combines verifiable identity, portable reputation, and attestation-based credibility, allowing trust signals to strengthen without placing sensitive data directly on-chain. This suggests trust infrastructure may develop as a reusable layer across ecosystems rather than as a one-off design choice.

Agent-native Payments: Payment Rails as a Complementary Layer

Payments should be viewed as complementary to trust registries, rather than embedded within them. Identity, reputation, and validation determine whether an agent can be trusted; payment infrastructure determines how that agent transacts, settles, and sustains repeat economic activity. This distinction matters because trust and payments may emerge as separate infrastructure layers, each with its own standards, control points, and value-capture dynamics.

x402

x402 is one of the clearest early examples of agent-native payment infrastructure at the API layer. By extending the HTTP 402 flow to machine-to-machine payments, it allows software and autonomous agents to pay for digital resources programmatically and in real time. Its importance is not just technical. It signals a potential shift in market structure: as agent-driven activity scales, payment functionality may move out of embedded application logic and into dedicated rails for machine-native commerce. If that happens, value may accrue to the infrastructure that standardizes transaction flows across agents, APIs, and services.

Machine Payments Protocol (MPP) and Tempo

MPP points to a broader coordination layer for autonomous payments, including recurring, session-based, and multi-step machine transactions. Tempo, a payments-focused blockchain that is compatible with the Ethereum Virtual Machine (EVM), can be viewed as an infrastructure expression of that thesis. EVM-compatible means it can support Ethereum-style smart contracts and tooling. Alongside mainnet, Tempo is introducing the Machine Payments Protocol (MPP), an open standard for machine payments co-authored with Stripe, a major global payments platform. Stripe's participation is notable because it suggests that machine-native commerce may require dedicated payment standards and infrastructure, rather than relying entirely on existing payment abstractions.

Assessment Takeaway

If autonomous agents become meaningful economic actors, trust and payments may develop as distinct infrastructure layers. Trust systems determine whether an agent is credible; payment rails determine whether it can transact efficiently and at scale. That separation expands the investable surface area of the stack. The key question is not only which applications gain adoption, but which infrastructure layers control transaction flows, settlement logic, and developer integration. Those control points are where durable pricing power and long-term value capture are most likely to emerge.

7. Blockchain Readiness for Agentic Workloads

Blockchain readiness for agentic workloads should be assessed by function rather than by general activity. Identity and trust, validation and attestation, machine-native payments, discovery and coordination, execution quality, and developer tooling do not mature evenly across ecosystems. As a result, early activity metrics should be read as experimentation signals rather than as a ranking of which chains are most agent-ready by design. The examples below are illustrative rather than exhaustive. They are selected not to rank ecosystems comprehensively, but to show how different infrastructure functions relevant to agentic workloads—trust and attestation, payments, coordination, and execution—are maturing unevenly across ecosystems.

- **Solana** is one of the clearest trust-stack examples. Its Agent Registry is positioned as onchain infrastructure for agent identity, reputation, and validation, and Solana says it is interoperable with **ERC-8004** on Ethereum. Solana Attestation Service adds a live credential layer for verifiable attestations, making trust primitives available in production rather than only in theory.
- **Ethereum** is also increasingly relevant as an agent-ready trust environment. **ERC-8004** defines a standard for trustless agents centered on identity, reputation, and validation registries, while **ERC-8126** defines a standard interface for AI agent registration and verification on Ethereum. Ethereum now has both emerging standards and visible activity around agent registration, making it more than just a general-purpose settlement layer in this context.
- **peaq** is best understood as a machine-economy stack with agent infrastructure built into the core design. Its materials position the chain around machine identity, trust, and payments, making it one of the more explicitly agent-oriented ecosystems by design.
- **Fetch.ai / ASI** is closer to a coordination-first agent environment than to a generic execution chain. In the uAgents stack, agents register on the Almanac smart contract on the Fetch.ai blockchain, while Agentverse is used for hosting, registration, discovery, and deployment. That makes the ecosystem stronger on coordination and agent networking than on trust or payments alone.
- **Base** and **Tempo** are highly relevant, but in narrower roles. Base is increasingly an agent-enabled execution and payments environment, while Tempo is better understood as a payments-first chain built around machine-native transaction flows and payment infrastructure.

The practical implication is that agent readiness should not be treated as a binary label. Some ecosystems are strongest in trust and attestation, some in payments, and some in coordination. The relevant assessment is therefore not which chain is "the AI-agent chain" in the abstract, but which infrastructure functions are already live, reusable, and positioned to become control points as agent-driven activity scales.

Blockchains listed above are examples to illustrate recent innovations regarding agentic infrastructure, and are not intended as investment recommendations or indications of trading intent.

8. Decentralized AI Infrastructure

Decentralized AI infrastructure should be treated as a related but separate category from blockchain readiness for agentic workloads. Some networks are designed primarily to support autonomous agent coordination, while others are designed to create crypto-economic markets for AI capability. In **decentralized AI**, the goal is to decentralize who provides AI compute, hosts models, serves inference, verifies outputs, controls access, and captures value. That distinction matters because these systems may contribute to the broader agentic AI theme without serving the same role as trust, payment, or execution infrastructure in the blockchain layers.

The examples below are illustrative rather than exhaustive. We focus on Fetch.ai / ASI and Bittensor because they represent two analytically distinct decentralized-AI models. Fetch.ai / ASI is best understood as an agent-coordination network, where the key question is whether decentralized discovery, coordination, and transactions between autonomous agents become a useful infrastructure layer. Bittensor is better understood as a crypto-economic market for AI capability, where subnet-based competition, evaluation, and reward allocation determine which AI outputs earn value. Both belong to the broader decentralized AI theme, but neither should be treated as interchangeable with trust-, payments-, or execution-oriented blockchain infrastructure. See Appendix C for the technical comparison of Fetch.ai and Bittensor.

Blockchains listed above are examples to illustrate recent innovations regarding agentic infrastructure, and are not intended as investment recommendations or indications of trading intent.

9. Conclusion

Agentic AI is unlikely to reward all blockchain layers equally. The most durable value is more likely to accrue to infrastructure that becomes embedded in agent trust, payments, access, execution, and interoperability workflows, rather than to application activity alone. Early evidence also suggests that readiness is not uniform across chains: Solana and Ethereum are emerging as trust-stack environments through live or developing identity, validation, and registration layers, peaq is oriented around machine identity, trust, and payments, Fetch.ai / ASI appears stronger in agent coordination, and Base and Tempo are increasingly relevant as execution- and payments-oriented environments. Some blockchains are becoming more ready by design to support AI agents, while others are better understood as general-purpose environments where agent activity is still experimental. The key question, therefore, is not simply whether agentic AI increases blockchain usage, but which infrastructure functions become reusable control points as agent-driven activity scales. That same shift may also intensify concentration in economically critical middleware, widening the gap between apparent protocol decentralization and the true location of operational control. Assessing this theme therefore requires tracking both growth in agent-driven demand and concentration across the subsystems that monetize it.

10. Appendices

Appendix A. Nakamoto Coefficient (NC): definition and "which NC is this?"

The Nakamoto Coefficient is a simple way to quantify a blockchain's decentralization. It measures the minimum number of independent entities that would need to coordinate in order to control a meaningful share of the network.

In this paper, we use the NC-PoS-33% (entity-level), which refers to the minimum number of independent entities needed to reach 33% of total stake or voting power in a proof-of-stake system. This threshold matters because, in many PoS networks, control of roughly one-third of stake can be enough to block finalization or exercise significant influence over network outcomes.

When we compute NC from "staking entities" (e.g., Lido, Binance, ether.fi), we are computing **Entity-level Stake NC at 33%,** not validator-count NC. This is the NC most relevant to economic control in PoS systems.

Appendix B. Ethereum NC calculation (9 March 2026) — Entity-level Stake NC (33%)

Source: Beaconcha.in validators chart (Total validators on 9 March 2026: 948,583).

Key point: many validators are not independent because large entities run many validators.

Entity shares (example snapshot):

- Lido = 20.89%
- Binance = 8.86%
- ether.fi = 6.04%

Cumulative sum:

- Lido: 20.89%
- Lido + Binance: 20.89% + 8.86% = 29.75%
- ether.fi: 29.75% + 6.04% = 35.79% crosses 33%

Result: Ethereum Entity-level Stake NC (33%) = 3 (Lido, Binance, ether.fi)

Interpretation: Validator count is not the decentralization metric; control aggregation by entity is.

Appendix C. Technical Overview of Fetch.ai and Bittensor

Fetch.ai and Bittensor are both part of the decentralized AI theme, but they differ materially in architecture, coordination logic, and incentive design.

Feature	Fetch.ai	Bittensor
Core function	Agent coordination network	Crypto-economic market for machine intelligence
Primary unit	Autonomous software agents	AI outputs and subnet participants
What the system does	Enables agents to discover counterparties, exchange information, coordinate actions, and execute transactions	Enables participants to provide AI services, have outputs evaluated, and earn rewards based on performance
Economic logic	Value depends on agent activity, workflow density, and coordination utility	Value depends on competition, evaluation, and reward allocation for useful AI outputs
Role of blockchain	Coordination, identity, and settlement layer around agent-based activity	Incentive and reward layer governing participation and emissions
How incentives work	Tied to usage of the agent network and coordination infrastructure	Participants produce outputs, validators assess them, and rewards are distributed in TAO
Technical structure	Agent-based architecture focused on discovery, coordination, and transactions	Subnet-based architecture with task-specific evaluation and incentive rules
Key design feature	Decentralized coordination between autonomous agents	Subnets allow different AI task domains to operate under different scoring and reward rules
Recent evolution	Continued development of agent tooling and coordination infrastructure	dTAO further links emissions and incentives to subnet-level market dynamics
Best interpretation	Decentralized AI agents and coordination	Decentralized AI markets and incentives

Technical takeaway

- **Fetch.ai** is closer to an agent platform, where the core question is whether decentralized agent coordination becomes a useful infrastructure layer.
- **Bittensor** is closer to a tokenized marketplace for AI capability, where the core question is whether subnet-based competition and evaluation can sustain a durable market for machine intelligence.
- In both cases, decentralization is strongest in coordination, participation, and incentive design, rather than in fully on-chain AI execution. Model inference, software environments, and adoption still depend heavily on off-chain systems.

11. References

- Bittensor. (n.d.). *Bittensor: A peer-to-peer intelligence market* [Whitepaper].
- De Rossi, M., Crapis, D., Ellis, J., & Reppel, E. (2025, August 13). *ERC-8004: Trustless agents* (Ethereum Improvement Proposal No. 8004). *Ethereum Improvement Proposals*.
- Fetch.ai. (n.d.). *Fetch.ai developer platform documentation*.
- Infura. (2025, March 14). *Ethereum Mainnet JSON-RPC API partial outage* [Incident report].
- L2BEAT, "The state of the layer two ecosystem" and "Stages."
- OpenAI, "New tools for building agents," 2025.
- Optimism Collective. (2023, September 28). *Security Council Charter v0.1* [Forum post]. *Optimism Governance Forum*.
- Solana. (n.d.-a). *Agent Registry documentation*.
- Solana. (2025). *Solana Attestation Service (SAS) documentation*.
- x402. (2025). x402 documentation / project materials.

WHAT ARE THE RISKS?

All investments involve risk, including the loss of principal.

Digital assets are subject to risks relating to immature and rapidly developing technology, security vulnerabilities of this technology (such as theft, loss or destruction of cryptographic keys), conflicting intellectual property claims, credit risk of digital asset exchanges, regulatory uncertainty, high volatility in their value/price, unclear acceptance by users and global marketplaces, and manipulation or fraud. Portfolio managers, service providers to the portfolios and other market participants increasingly depend on complex information technology and communications systems to conduct business functions. These systems are subject to a number of different threats or risks that could adversely affect the portfolio and their investors, despite the efforts of the portfolio managers and service providers to adopt technologies, processes and practices intended to mitigate these risks and protect the security of their computer systems, software, networks and other technology assets, as well as the confidentiality, integrity and availability of information belonging to the portfolios and their investors.

Any companies and/or case studies referenced herein are used solely for illustrative purposes; any investment may or may not be currently held by any portfolio advised by Franklin Templeton. The information provided is not a recommendation or individual investment advice for any particular security, strategy or investment product and is not an indication of the trading intent of any Franklin Templeton managed portfolio.

IMPORTANT LEGAL INFORMATION

This material is intended to be of general interest only and should not be construed as individual investment advice or a recommendation or solicitation to buy, sell or hold any security or to adopt any investment strategy. It does not constitute legal or tax advice. This material may not be reproduced, distributed or published without prior written permission from Franklin Templeton.

The views expressed are those of the investment manager and the comments, opinions and analyses are rendered as at publication date and may change without notice. The underlying assumptions and these views are subject to change based on market and other conditions and may differ from other portfolio managers or of the firm as a whole. The information provided in this material is not intended as a complete analysis of every material fact regarding any country, region or market. There is no assurance that any prediction, projection or forecast on the economy, stock market, bond market or the economic trends of the markets will be realized. The value of investments and the income from them can go down as well as up and you may not get back the full amount that you invested. **Past performance is not necessarily indicative nor a guarantee of future performance.**

Any research and analysis contained in this material has been procured by Franklin Templeton for its own purposes and may be acted upon in that connection and, as such, is provided to you incidentally. Data from third-party sources may have been used in the preparation of this material and Franklin Templeton ("FT") has not independently verified, validated or audited such data. Although information has been obtained from sources that Franklin Templeton believes to be reliable, no guarantee can be given as to its accuracy and such information may be incomplete or condensed and may be subject to change at any time without notice. The mention of any individual securities should neither constitute nor be construed as a recommendation to purchase, hold or sell any securities, and the information provided regarding such individual securities (if any) is not a sufficient basis upon which to make an investment decision. FT accepts no liability whatsoever for any loss arising from use of this information and reliance upon the comments, opinions and analyses in the material is at the sole discretion of the user.

Products, services and information may not be available in all jurisdictions and are offered outside the US by other Franklin Templeton affiliates and/or their distributors as local laws and regulation permits. Please consult your own financial professional or Franklin Templeton institutional contact for further information on availability of products and services in your jurisdiction.

Brazil: Issued by Franklin Templeton Investimentos (Brasil) Ltda., authorized to render investment management services by CVM per Declaratory Act n. 6.534, issued on October 1, 2001.

Canada: Issued by Franklin Templeton Investments Corp., 200 King Street West, Suite 1500 Toronto, ON, M5H3T4, Fax: (416) 364-1163, (800) 387-0830, www.franklintempleton.ca. **Offshore Americas:** In the US, this publication is made available by Franklin Templeton, One Franklin Parkway, San Mateo, California 94403-1906. Tel: (800) 239-3894 (USA Toll-Free), (877) 389-0076 (Canada Toll-Free), and Fax: (727) 299-8736. **US:** by Franklin Templeton, One Franklin Parkway, San Mateo, California 94403-1906, (800) DIAL BEN/342-5236, www.franklintempleton.com. Investments are not FDIC insured; may lose value; and are not bank guaranteed.

Issued in **Europe** by: Franklin Templeton International Services S.à r.l.—Supervised by the Commission de Surveillance du Secteur Financier–8A, rue Albert Borschette, L-1246 Luxembourg. Tel: +352-46 66 67-1, Fax: +352-46 66 76. **Poland:** Issued by Templeton Asset Management (Poland) TFI S.A.; Rondo ONZ 1; 00-124 Warsaw. **South Africa:** Issued by Franklin Templeton Investments SA (PTY) Ltd, which is an authorised Financial Services Provider. Tel: +27 (21) 831 7400, Fax: +27 (21) 831 7422. **Switzerland:** Issued by Franklin Templeton Switzerland Ltd, Stockerstrasse 38, CH-8002 Zurich. **United Arab Emirates:** Issued by Franklin Templeton Investments (ME) Limited, authorized and regulated by the Dubai Financial Services Authority. Dubai office: Franklin Templeton, The Gate, East Wing, Level 2, Dubai International Financial Centre, P.O. Box 506613, Dubai, U.A.E. Tel: +9714-4284100, Fax: +9714-4284140. **UK:** Issued by Franklin Templeton Investment Management Limited (FTIML), registered office: Cannon Place, 78 Cannon Street, London EC4N 6HL. Tel: +44 (0)20 7073 8500. Authorized and regulated in the United Kingdom by the Financial Conduct Authority. **Saudi Arabia:** Franklin Templeton Financial Company, Unit 209, Rubeen Plaza, Northern Ring Rd, Hittin District 13512, Riyadh, Saudi Arabia. Regulated by CMA. License no. 23265-22. Tel: +966-112542570. All investments entail risks including loss of principal investment amount.

Australia: Issued by Franklin Templeton Australia Limited (ABN 76 004 835 849) (Australian Financial Services License Holder No. 240827), Level 47, 120 Collins Street, Melbourne, Victoria 3000. **Hong Kong:** Issued by Franklin Templeton Investments (Asia) Limited, 62/F, Two IFC, 8 Finance Street, Central, Hong Kong. **Japan:** Issued by Franklin Templeton Investments Japan Limited. **Korea:** Franklin Templeton Investment Advisors Korea Co., Ltd., 3rd fl., CCMM Building, 101 Yeouigongwon-ro, Yeongdeungpo-gu, Seoul, Korea 07241. **Malaysia:** Issued by Franklin Templeton Asset Management (Malaysia) Sdn. Bhd. & Franklin Templeton GSC Asset Management Sdn. Bhd. This document has not been reviewed by Securities Commission Malaysia. **Singapore:** Issued by Templeton Asset Management Ltd. Registration No. (UEN) 199205211E, 7 Temasek Boulevard, #38-03 Suntec Tower One, 038987, Singapore.

Please visit www.franklinresources.com to be directed to your local Franklin Templeton website.



FRANKLIN TEMPLETON

franklintempleton.com

© 2026 Franklin Distributors, LLC. Member FINRA/SIPC. All rights reserved.

AIBC-FL-0526