Enabling a Secure and Resilient Internet of Everything: A Multi-Layer Non-Cryptocurrency Blockchain Approach

Porya Elahi Kheibary
Independent Researcher
Iran
porya.elahi@versatilechain.com

Navidreza Asadi
Technical University of Munich
Munich, Germany
navidreza.asadi@tum.de

Wolfgang Kellerer
Technical University of Munich
Munich, Germany
wolfgang.kellerer@tum.de

***Abstract*—The Internet of Everything (IoE) remains fragmented by vendor-specific stacks, centralized bottlenecks, and the economic friction of transaction-fee-based blockchains. We present Versatile Network, a multi-layer, non-cryptocurrency blockchain architecture that separates high-volume peer-to-peer (P2P) data streams from global state validation. An intent-based communication model enables seamless interoperability among heterogeneous devices, while a resource-sharing framework lets constrained endpoints leverage network-wide compute and storage. Resource-based Sybil resistance and adaptive validation provide robust security without fees. Compared with Ethereum, Solana, and IPFS, Versatile Network achieves better suitability for IoE through cost-free operation, scalability, and seamless off-chain integration—positioning it as a pragmatic foundation for Web 4.0.**

I. Problem and Motivation

Billions of heterogeneous devices must exchange data and coordinate actions with low latency, privacy, and resilience. Today's approaches are limited by (i) centralized control planes, resulting in privacy concerns, single points of failure, and data silos; (ii) incompatible protocols and custom integrations, and (iii) fee-based blockchains that are impractical for high-frequency, low-value IoE interactions [1], [2]. A new substrate is needed that preserves decentralization and security yet remains efficient and economically frictionless at IoE scale.

A. Context and Gaps

Across consumer, industrial, and civic domains, device ecosystems evolved in isolation with proprietary middleware and cloud backends. This fragmentation inflates integration costs and prevents seamless cross-vendor coordination. Meanwhile, generalized blockchains improved integrity but coupled every interaction to a transaction, introducing fees and latency mismatched to continuous telemetry and control. Storage-focused systems like IPFS simplify distribution but omit active validation and real-time coordination. The IoE demands a fabric that keeps fast, local data movement separate from slow-changing global state, while enabling devices to interact based on intent rather than brittle API couplings.

TABLE I
Mapping requirements to design elements

Req.	Design element
R1	Fee-free streams; validators audit only consequential state
R2	Local P2P data paths; global aggregation of hashes/policies only
R3	Intent-based discovery and negotiation; standardized schemas
R4	Resource sharing framework for storage/bandwidth
R5	Resource-based Sybil resistance; redundant encryption/attestations
R6	Native HTTP/TCP/UDP hooks; no oracles required

B. Design Requirements

We distill six practical requirements for an IoE substrate:
R1: **Zero per-interaction fees** to support high-frequency, low-value telemetry/events.
R2: **Local-first data motion** with global audit of consequential state only.
R3: **Interoperability across vendors** via protocol-agnostic, intent-driven discovery.
R4: **Support for constrained devices** with offload of compute/storage/bandwidth.
R5: **Robust security without token economics**, resisting Sybil and tampering.
R6: **Seamless off-chain integration** using standard transports and stacks.

C. Contributions

We present Versatile Network, a multi-layer blockchain architecture designed to meet the above requirements (Table I). Key innovations include:
Multi-layer non-cryptocurrency architecture: Separates P2P streams from validator-managed state, avoiding the TPS and fee constraints of transaction-centric chains.
Intent-based communication: Protocol-agnostic discovery and interaction enable plug-and-play interoperability across vendors and device classes [3].

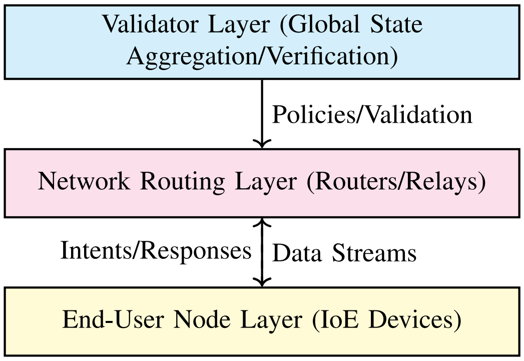
Validator Layer (Global State Aggregation/Verification)
Policies/Validation
Network Routing Layer (Routers/Relays)
Intents/Responses
Data Streams
End-User Node Layer (IoE Devices)

Fig. 1. VERSATILE NETWORK separates data motion (streams) from state validation to optimize IoE efficiency and scalability.

Resource-based Sybil resistance: Progressive limits and adaptive synchronization ensure secure participation without token economics; compatible with lightweight consensus [4].
Seamless off-chain integration: Direct interaction with existing stacks (e.g., HTTP/TCP/UDP) without oracles bridges on-chain trust with real-world systems.

II. Architecture Overview

VERSATILE NETWORK is organized into three layers that decouple high-volume data motion from global state validation:
End-User Node Layer: Endpoints (sensors, mobiles, microcontrollers) initiate intents and data streams, offloading heavy tasks when needed.
Network Routing Layer: Routers/relays provide locality-aware P2P streaming and per-route integrity checks, preventing ledger bloat by keeping most data off-chain.
Validator Layer: Validators aggregate and validate essential state changes, enforcing protocol rules and network integrity without per-interaction fees.

Figure 1 illustrates this three-layer separation between end-user devices, the routing mesh, and the validator tier.

A. Terminology and Roles

- **User–Router Connection Layer (routing):** The operational mesh of relays that forms local data paths and enforces lightweight integrity and QoS.
- **Validator Layer:** The state-protection tier that consolidates only important state (e.g., service bindings, access policies) for audit and recovery.
- **End-User Nodes:** Sensors, actuators, mobiles, and servers that issue intents, consume services, and initiate streams.

B. Layer Responsibilities and Data Path

Data-plane flow: Endpoints negotiate intents, then bind P2P streams via the routing layer; routers enforce local integrity checks (sequence numbers, lightweight MACs) and QoS. Only consequential state (e.g., service binding hashes, access policies) is aggregated by validators.

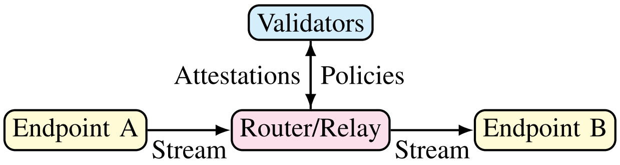

Fig. 2. Local streams with validator-backed control. Only essential state is globally aggregated; bulk data remains local.

Control-plane flow: Validators publish policies and attestations; routers subscribe to enforce admission control and rate/-fairness policies. Endpoints fetch validated service directories for discovery.

Figure 2 depicts the local streaming path between endpoints with validator-backed policy and attestation exchange.

C. Security and Validation

- **Resource-based Sybil resistance:** Progressive per-account quotas and mandatory cross-storage/validation among routers discourage mass account abuse without token fees.
- **Redundant encryption and distribution:** Critical metadata is redundantly encrypted with validator keys and distributed to resist tampering.
- **Adaptive synchronization:** Validators aggregate only critical state, reducing bandwidth while preserving auditability [1], [2].

Threat model. (i) *Sybil/adversarial endpoints:* Limited by per-identity quotas and cross-validation duties. (ii) *Byzantine routers:* Detectable via path diversity, redundant attestations, and end-to-end integrity checks. (iii) *Eavesdroppers:* Mitigated by stream encryption and validator-key-backed metadata encryption. (iv) *DoS via bursty telemetry:* Rate caps and priority scheduling at routers; validators unaffected by bulk traffic.

III. Programming and Interaction Model

An intent-driven model replaces rigid API coupling. Applications broadcast intents to discover services and negotiate capabilities, then bind to P2P streams or simple request/response calls. This model supports: (i) *dynamic discovery:* Services discover each other on the fly, reducing vendor lock-in; (ii) *flexible patterns:* RPC-like calls, bi-directional streams, and event notifications over a unified interface; and (iii) *interoperability:* Standardized intent definitions enable multi-vendor ecosystems and integration with existing IT systems [3]. Implementations auto-derive encoding/validation helpers, minimizing boilerplate and enabling safe, network-aware types.
VARP and off-chain integration: VERSATILE NETWORK applications interact with external stacks (e.g., C#, Python, Java) using standard transports (HTTP/JSON, TCP, UDP). This avoids oracles and keeps business logic close to where data is produced and consumed.

A. Compact Intent Schema Example

```
protocol SensorData {
    sensorId: u32;    // Sensor identifier
    temp: i16;        // Temperature reading
    timestamp: u64;   // Unix timestamp
}

intent SensorService {
    api fetchSensorData(req: SimpleReq): SensorData;
    stream sensorStream<SensorData, Void>;
    event CriticalEvent(id: u32, alertMsg: String);
}
```

IV. IoE Fit and Comparative Notes

Why streams + aggregated state? For IoE, most traffic is high-frequency telemetry best kept local; only consequential state needs global consensus. Thus, bandwidth and latency improve dramatically versus transaction-broadcast blockchains.

Table II summarizes Versatile Network's positioning against transaction-centric blockchains along key IoE concerns.

Context with existing work: Rollups increase throughput for tx-centric chains [5] but still impose costs and latency unsuitable for many IoE streams. Intent-Based Networking principles [3] align with our protocol design. Lightweight consensus directions [4] inform validator efficiency. Foundational surveys [1], [2] motivate our non-transactional, layered approach.

TABLE II
Positioning of Versatile Network for IoE

Feature	Tx-centric Chains	Versatile Network
Per-interaction fees	Yes	**No**
Off-chain integration	Oracles	**Native**
IoT/microcontrollers	Challenging	**Native**
Data motion model	Broadcast Tx	**P2P Streams**
Scalability focus	TPS	**Bandwidth/Locality**

V. Operational Considerations

Deployment. Routers run on commodity gateways and edge servers; validators run in cloud or on-prem clusters. Discovery relies on signed directories and intent catalogs.

Policy and slicing. IBN-inspired policies [3] define per-intent QoS, admission, and isolation, and routers enforce these slices end-to-end without a central broker.

Fault tolerance. Endpoints maintain alternate relays, and validators use quorum-based attestation to preserve liveness under partial failures.

Interoperability. Native hooks for HTTP/TCP/UDP remove the need for oracles, and legacy devices attach via lightweight shims.

Privacy and governance. Only essential metadata is aggregated by validators; stream contents remain local and encrypted, enabling privacy-preserving oversight and domain-specific governance.

VI. Discussion

Limitations. Global queries over raw telemetry are intentionally out-of-scope (streams remain local); auditability focuses on consequential state. Strong identity bootstrapping is delegated to compatible PKI/attestation systems. As the future work, standardized intent schemas for major verticals, large-scale pilots, and formal analysis of resource-based Sybil defenses are planned.

Illustrative use cases. Versatile Network 's architecture suits diverse IoE scenarios: (i) *Smart living:* Appliances coordinate procurement and delivery via intents; drones receive real-time routes from city sensors without centralized brokers. Distributed machine learning on shared edge resources enables smart environments [6]–[9]; (ii) *Industrial telemetry:* High-rate sensor streams stay local; only alerts and state changes reach validators, cutting WAN costs and latency; and (iii) *Healthcare/IoMT:* Devices interoperate under strict privacy budgets; compute-heavy analytics are offloaded, preserving battery life.

VII. Conclusion and Next Steps

Versatile Network provides a pragmatic path to a fee-free, scalable, and interoperable IoE by decoupling fast, local data streams from validator-managed global state, enabling intent-driven interactions, and supporting resource sharing across heterogeneous devices. By aligning architecture with IoE realities—continuous telemetry, constrained endpoints, and cross-vendor interoperability we aim to address the core limitations of both centralized platforms and fee-centric blockchains. Ongoing work focuses on large-scale pilots across smart living and industrial settings, standard intent schemas for major verticals, and formal modeling and verification of the resource-based Sybil defense.

References

[1] A. Pinna, S. Ibba, G. Baralla, R. Tonelli, and M. Marchesi, "A survey on blockchain for the internet of things," *arXiv preprint arXiv:1801.03528*, 2018.

[2] K. Salah, M. H. U. Rehman, N. Nizamuddin, and A. Al-Fuqaha, "A survey on consensus protocols in blockchain for iot networks," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2040–2059, 2019.

[3] T. Szigeti, D. Zacks, M. Falkner, and S. Arena, *Cisco digital network architecture: intent-based networking for the enterprise*. Cisco Press, 2018.

[4] J. Gai *et al.*, "A fair and lightweight hybrid consensus algorithm for iot," *arXiv preprint arXiv:2503.08607*, 2025.

[5] T. Lavaur, J. Lacan, and C. P. Chanel, "Enabling blockchain services for ioe with zk-rollups," *Sensors*, vol. 22, no. 17, p. 6493, 2022.

[6] N. Asadi and M. Goudarzi, "Variant parallelism: lightweight deep convolutional models for distributed inference on iot devices," *IEEE Internet of Things Journal*, vol. 11, no. 1, pp. 345–352, 2023.

[7] L. Wulfert, N. Asadi, W.-Y. Chung, C. Wiede, and A. Grabmaier, "Adaptive decentralized federated gossip learning for resource-constrained iot devices," in *Proceedings of the 4th International Workshop on Distributed Machine Learning*, 2023, pp. 27–33.

[8] N. Asadi, H. I. Bengü, L. Wulfert, H. Wöhrle, and W. Kellerer, "Road to tiny reality: Digital twins for decentralized ai on microcontrollers," in *The 31st Annual International Conference on Mobile Computing and Networking*, ser. MobiCom '25. New York, NY, USA: Association for Computing Machinery, 2025, p. 1–3.

[9] N. Asadi, H. I. Bengü, L. Wulfert, H. Wöhrle, and W. Kellerer, "Gist - Optimizing Segmentation for Decentralized Federated Learning on Tiny Devices," in *Federated Learning and Edge AI for Privacy and Mobility (FLEdge-AI '25)*, ser. FLEdge-AI '25. New York, NY, USA: Association for Computing Machinery, 2025.