Article

M2M Payment Auth Tracking over Blockchain

Yair Rivera Julio * , Juan Manuel Torres * , Angel Pinto Mangones * , Néstor Enrique Caicedo-Solano * , Darwin Peña Gonzalez * , Cesar Viloria Nuñez *

Posted Date: 19 August 2025

doi: 10.20944/preprints202508.1306.v1

Keywords: Supply-Chain 5.0; machine-to-machine payments; blockchain; smart contracts; adaptive multi-factor authentication; IoT security; Industry 5.0

Article

M2M Payment Auth & Tracking over Blockchain

Yair Rivera Julio [1,2,*], Juan M. Torres-Tovio [3], Angel D. Pinto-Mangones [3], Néstor Enrique Caicedo-Solano [4], Darwin Peña Gonzalez [5] and César Viloria-Núñez [6]

[1] Department of Computer Science, Corporación Universitaria Americana, Barranquilla 080001, Colombia
[2] Supply-Chain Innovation Lab, Corporación Universitaria Americana, Barranquilla 050021, Colombia
[3] School of Systems Engineering, Universidad del Sinú, Montería, Colombia
[4] Department of Industrial Engineering, Universidad del Magdalena, Santa Marta, Colombia
[5] Department of Mathematics and Statistics, Universidad del Magdalena, Santa Marta, Colombia
[6] Digital Transformation School, Universidad Tecnológica de Bolívar, Cartagena, Colombia
* Correspondence: yrivera@coruniamericana.edu.co or yaircostac@hotmail.com

Abstract

Background: Supply-Chain 5.0 envisions hyper-connected cyber–physical ecosystems where autonomous devices negotiate and settle financial obligations without human intervention. Existing payment rails depend on costly intermediaries, manual authentication and post-facto reconciliation, rendering them unsuitable for machine-to-machine (M2M) micro-transactions that demand millisecond-scale finality and tamper-evident auditability.This work proposes a secure M2M payment framework that couples a permissioned-blockchain settlement layer with an *adaptive multi-factor authentication* (A-MFA) pipeline and an energy-aware off-chain state-channel mechanism. A dual-channel consensus separates value transfer from authentication proofs, minimising on-chain gas consumption. Formal security proofs in the Real-or-Random model and empirical benchmarking on a Hyperledger Fabric test-bed validate confidentiality, integrity and liveness properties under realistic adversarial conditions. Experiments demonstrate end-to-end settlement latency below 250 ms, 42 % lower computational overhead and 18 % reduced energy consumption compared with certificate-based escrow baselines. The framework enables scalable, standards-compliant and auditable M2M payments, paving the way for frictionless Supply-Chain 5.0 finance.

Keywords: Supply-Chain 5.0; machine-to-machine payments; blockchain; smart contracts; adaptive multi-factor authentication; IoT security; Industry 5.0

1. Introduction

Global logistics is undergoing a paradigm shift from *Industry 4.0*—characterised by automation, digital twins, and cyber–physical systems—toward *Supply-Chain 5.0*, which emphasizes human–machine collaboration, resilience, sustainability, and decentralized intelligence [1,2]. In this evolving landscape, autonomous guided vehicles (AGVs), collaborative robots, and intelligent agents increasingly execute procurement and resource-allocation decisions in real time. However, realizing such autonomy in financial transactions demands secure, low-latency, and trustworthy payment mechanisms between devices—capabilities that traditional infrastructures, which rely on central intermediaries and manual identity verification, are unable to meet. Legacy settlement systems introduce delays exceeding one second, thereby breaching latency thresholds critical for just-in-sequence manufacturing lines and creating vulnerabilities to fraud or unauthorized interventions [3].

Blockchain technologies offer promising features such as decentralised trust, tamper resistance, and programmable settlements via smart contracts [4]. Nonetheless, public blockchain infrastructures face persistent issues related to scalability, transaction costs, and confidentiality, particularly in commercial and industrial contexts. Concurrently, traditional authentication mechanisms—e.g., X.509 certificates and static keys—fail to adapt to dynamic threat environments or compromised IoT

doi:10.20944/preprints202508.1306.v1

endpoints. This underscores the urgent need for adaptive, context-aware multi-factor authentication (MFA) strategies integrated directly within machine-to-machine (M2M) payment flows [5–7].

Recent advancements in secure financial authentication, such as machine learning-based MFA frameworks [8] and decentralized identity schemes in IoT ecosystems [6], have laid the foundation for more robust and scalable solutions. Yet, there remains a gap in integrating these mechanisms with blockchain-based settlement protocols that support both online and offline scenarios [3]. Our work contributes to this research frontier by proposing a secure, dual-channel payment framework tailored for Supply-Chain 5.0.

The contributions of this article are threefold:

1. **Architecture:** We present a layered M2M payment framework that integrates a permissioned blockchain settlement layer with a lightweight, adaptive multi-factor authentication (A-MFA) module and an energy-aware state-channel mechanism [5,7].
2. **Security:** We introduce a dual-channel consensus protocol with formal proofs of confidentiality, integrity and non-repudiation using a game-based model and random-oracle abstraction [6].
3. **Evaluation:** We conduct an extensive experimental study on Hyperledger Fabric v2.5, demonstrating sub-second latency, reduced computational load, and strong resilience against impersonation, replay, and double-spending attacks [4].

1.1. Blockchain-Enabled Micropayments

Although public-ledger overlays such as *IOTA*, the *Lightning Network* and *Raiden* have demonstrated that directed-acyclic-graph (DAG) structures and off-chain payment channels can clear tens of thousands of sub-cent transactions per second at negligible cost, their dependency on global consensus and open mempools exposes business-sensitive metadata.[1] For supply-chain operators bound by non-disclosure agreements, this transparency clashes with the need to shield procurement volumes, supplier identities and just-in-sequence inventory levels from competitors. Moreover, channel liquidity in Lightning or Raiden is provisioned in the native cryptocurrency, forcing treasurers to hold volatile assets on their balance sheets and to maintain inbound liquidity for every trading pair—a burden that quickly becomes prohibitive when hundreds of autonomous guided vehicles (AGVs) and robotic cells transact in real time.

Several efforts have attempted to address these constraints. For example, the ArtChain platform [9] demonstrates how blockchain can preserve asset provenance while minimizing exposure of transaction metadata in the art market. Similarly, Zhu et al.[10] introduce a lightweight edge-oriented blockchain to protect smart surveillance streams, a principle translatable to microtransaction flows in supply logistics. To enhance security in public-ledger systems, Yang et al.[11] % AttackonProof-of-WorkBlockchainwithHistoryWeightedInformation propose a historical-weighting strategy that resists 51 % attacks, reinforcing trust in lightweight micropayment networks.

Further standardization efforts have also emerged. The IEEE P3801 draft [12] outlines specifications for electronic contracts on blockchain, potentially streamlining settlement layers. In parallel, the IEEE P2418.7 draft [13] defines principles for blockchain-based finance in supply chains, reaffirming the need for privacy, scalability, and off-chain settlement mechanisms in industrial applications.

In contrast, the dual-channel design proposed in Section 4 *localises* consensus to a permissioned federation while amortising gas via periodic state-channel anchoring. Transactions settle in milliseconds, but only a Merkle-root and an opaque authentication hash ever reach-chain, thereby reconciling the low-fee promise of public micropayment rails with the confidentiality, determinism and fiat-denominated accounting required by enterprise logistics.

[1] E.g., the *Tangle* stores the hash of every data bundle, which—when cross-referenced with side information—may reveal trade-route patterns.

1.2. Authentication in Autonomous Logistics

Traditional device onboarding pipelines rely on X.509 certificates burned into secure elements or loaded through Trusted Platform Modules (TPMs). While this public-key-infrastructure (PKI) approach guarantees strong cryptographic identities, it remains *static*: once provisioned, a keypair cannot adapt to the fluctuating risk posture of a forklift entering a high-value picking zone or a drone traversing a geo-fenced export-control perimeter.

To this end, recent MFA proposals such as adaptive challenge-response mechanisms and biometric-hardware fusion tokens are gaining momentum. However, as observed in [10], many such schemes impose substantial latency and energy overhead, hindering real-time logistics. Notably, while biometrics and tokens provide security, their use in high-speed autonomous contexts remains a bottleneck unless adaptively modulated.

The *adaptive MFA* (A-MFA) engine introduced in our framework addresses these shortcomings through two innovations: (i) it computes a context-aware risk score ρ that modulates the factor threshold k_ρ, activating lightweight proofs such as physically unclonable-function (PUF) challenges for routine events and escalating to PAKE+OTP bundles only under anomalous conditions; and (ii) it hashes the concatenated factor set into a single 32-byte commitment that is verified on-chain, decoupling proof collection from ledger consensus. Experimental results in Section 7 confirm that this strategy cuts authentication overhead by 42% and energy consumption by 18% relative to certificate-based escrow, without sacrificing cryptographic strength. Consequently, autonomous logistics systems gain a *risk-elastic* authentication layer that scales from battery-powered RFID gates to high-throughput robotic sorters while remaining compatible with existing PKI roots of trust. Section 1 presents the motivation, problem statement, and research objectives, while Section 2 surveys related work on blockchain-enabled, MFA-secured machine-to-machine transactions in Industry 5.0 contexts. Section 4 details the proposed architecture, cryptographic primitives, and transaction flow. Section 7 describes the experimental setup, performance metrics, and evaluation scenarios, followed by Section 8, which interprets the results and discusses scalability, limitations, and applicability. Finally, Section 9 summarises the contributions and outlines directions for future research.

2. State of Art

The evolution of payment systems in industrial environments has progressively shifted from centralized, high-latency models toward distributed architectures that are secure and context-aware. Within the scope of Supply-Chain 5.0, where autonomous device interaction demands instantaneous settlement and dynamic identity verification, it becomes essential to examine recent advances that combine blockchain, multi-factor authentication (MFA), and energy-aware optimizations for IoT settings. Reviewing prior work not only highlights emerging technological trends—such as the adoption of state channels, dual-channel consensus, and adaptive biometric authentication—but also exposes persistent limitations in privacy, scalability, and resilience against advanced adversaries. This comparative analysis establishes the conceptual foundations guiding the design of the proposed framework, aimed at reconciling sub-second latency, verifiable traceability, and energy efficiency in high-volume M2M payment scenarios.

Table 1 summarizes recent research efforts aimed at securing machine-to-machine (M2M) payments through multifactor authentication (MFA) and blockchain technologies within the context of Industry 5.0. These works illustrate a growing emphasis on hybrid and decentralized architectures, offline transaction capabilities, and the integration of adaptive and biometric authentication methods. This evolution provides a foundational landscape for understanding the technical enablers of low-latency, secure micropayments among IoT devices, as discussed in the following subsection.

doi:10.20944/preprints202508.1306.v1

Table 1. Recent Research on M2M Payments, MFA and Blockchain in Industry 5.0.

Reference	Year	Main Technology	Key Contribution	Application	Authentication Method	Architecture Type
Aburbeian and Fernández-Veiga [8]	2024	MFA + Machine Learning	Integration of MFA with machine learning to detect fraud in online financial transactions	Online financial services	OTP + Anomaly Detection	Centralized Architecture
Bamashmos et al. [6]	2024	Blockchain + Two-Layer MFA	Proposed two-layer MFA using blockchain to enhance IoT security	IoT Environments	PUF + ECDSA + Biometrics	Decentralized Architecture
Xu et al. [7]	2023	Blockchain + Adaptive MFA	Blockchain-based authentication scheme with adaptive MFA strategy for dynamic scenarios	Mobile and dynamic applications	Dynamic Passwords + Tokens	Hybrid Architecture
DG Nexolution et al. [3]	2025	Deposit Tokens + Offline Payments	Prototype enabling secure M2M transactions without connectivity using deposit tokens	Industrial remote zones or high-security environments	Physical Tokens + NFC	Offline Architecture
Sah and Shaikh [2]	2025	AI + IoT + Blockchain	Systematic review on AI, IoT and blockchain integration in Industry 5.0 for supply chain transformation	Supply chain management	Data Analysis + Passwords	Cloud-Based Architecture
Kinai et al. [5]	2020	Blockchain + MFA for Offline Apps	MFA for blockchain-based platforms without internet, using transaction-based risk analysis	Financial apps in offline environments	Passwords + Risk Analysis	Offline Architecture
Chaudhari [4]	2024	Blockchain + Tokenization + Smart Contracts	Study on how blockchain, tokenization and smart contracts improve security and transparency in mobile payments	Mobile payment systems	Dynamic Tokenization + Smart Contracts	Decentralized Architecture
Fraga-Lamas et al. [1]	2024	Blockchain in Industry 5.0	Analysis of the transition from Industry 4.0 to 5.0 and how blockchain benefits human-centered applications	Smart factories	Passwords + Smart Contracts	Decentralized Architecture
Benedito Petroni [14]	2019	Blockchain in Manufacturing	Systematic review on the use of blockchain in M2M transactions in the manufacturing sector	Manufacturing	Passwords + Tokens	Decentralized Architecture
Walker and Hall [15]	2022	LTE-M Security	Analysis of attacks and mitigations in LTE-M networks for cellular IoT	LTE-M networks	Passwords + Tokens	Centralized Architecture

The trajectory sketched in Table 1 shows a clear migration from monolithic, certificate-centric solutions toward context-aware, gas-efficient settlement fabrics that operate seamlessly in both online and offline modes. Early studies concentrated on ledger immutability or cellular-IoT hardening; more recent efforts embed physical-layer fingerprints, adaptive risk scores and deposit tokens directly into the transaction flow, thereby lowering authentication latency while also expanding the attack surface that must be secured. Three critical gaps, however, remain open: **(i)** the absence of a unifying settlement model that amortises gas cost without sacrificing sub-second finality; **(ii)** a lack of empirical evidence on energy proportionality for resource-constrained edge devices; and **(iii)** the scarcity of formal proofs quantifying resilience against replay, double-spending and compromised root-of-trust scenarios. The present research addresses these gaps with a dual-channel architecture that couples state-channel batching with an adaptive multi-factor authentication pipeline, validated on a Hyperledger Fabric test-bed using a full factorial design. In so doing, it offers the first end-to-end demonstration that low-latency, risk-adaptive M2M micropayments can be achieved without incurring prohibitive energy or gas costs, paving a practical path toward Supply-Chain 5.0 finance that is simultaneously scalable, auditable and sustainably efficient.

2.1. Blockchain in Supply-Chain Finance

Hyperledger Fabric and Sawtooth facilitate asset tracking, provenance auditing, and smart contract execution for distributed logistics ecosystems. Their modular architecture supports scalability and privacy for enterprise-grade deployments [16,17]. However, current implementations often lack native support for context-aware authentication, adaptive trust management, and latency-constrained microtransactions essential for real-time supply chain operations.

While some blockchain-based innovations in power supply traceability [18], embedded system accountability [19], and smart grid integration [20] offer valuable foundations, a unified framework integrating gas-efficient M2M settlements, adaptive multi-factor authentication, and verifiable end-to-end security remains absent. Efforts in blockchain-enabled point systems [21] and interplanetary file traceability [22] reinforce the need for fine-grained traceability and decentralised access. Nonetheless, Supply-Chain 5.0 environments require not only secure data exchanges but also risk-aware payment settlement and real-time policy compliance, as outlined in recent IEEE frameworks [23–25].

3. System Model and Threat Assumptions

3.1. Entities

- **Edge Device (ED):** an autonomous guided vehicle (AGV), industrial sensor or robotic arm initiating or receiving payments in operational environments.
- **Edge Payment Agent (EPA):** a lightweight client embedded on the ED that enforces Adaptive Multi-Factor Authentication (A-MFA), computes hash commitments, and interfaces with off-chain and on-chain settlement components.
- **Permissioned Ledger (PL):** a consortium blockchain network based on PBFT consensus that stores finalised transaction states and policy compliance logs [26].
- **Compliance Oracle (CO):** an external trusted module responsible for querying real-time risk policies (e.g., AML thresholds, token velocity limits) and broadcasting compliance flags to settlement nodes.

3.2. Communication and Trust

Edge devices exchange payment intents and commitments via lightweight, encrypted protocols such as MQTT over TLS or OPC UA with certificate pinning. Trust in the permissioned ledger is achieved through Byzantine Fault Tolerance, allowing up to $f < \frac{n}{3}$ compromised validators without violating global consistency. The CO modules are assumed semi-honest but isolated, and governed by federated identities with verifiable credentials, in line with secure blockchain-based identity models [27].

3.3. *Adversary Capabilities*

The adversary model assumes a Dolev–Yao attacker with full control over the communication network: capable of intercepting, modifying, delaying, or replaying messages. The attacker may compromise up to f validator nodes, extract device-side credentials via side-channel leakage, or coerce edge devices through physical tampering. Despite this, trust assumptions hold that edge firmware and private key modules are tamper-evident and auditable through secure boot chains, in accordance with best practices from the IEEE IoT blockchain standards [23,24].

4. Proposed Framework

The proposed framework delivers a holistic machine-to-machine (M2M) payment platform that fuses adaptive authentication, gas-efficient settlement channels, and continuous regulatory compliance. As depicted in Figure 1, the solution spans three functional domains—edge, settlement, and compliance—to ensure transaction execution with sub-second latency, amortised on-chain gas consumption, and risk-adaptive security guarantees. The architecture integrates Edge Payment Agents (EPAs), an Adaptive Multi-Factor Authentication (A-MFA) engine informed by dynamic device behavior, and permissioned smart contracts operating under a dual-channel consensus model. This design enables auditable, confidential, and resilient payments across supply chain agents in heterogeneous IoT environments, addressing traceability, scalability, and decentralised collaboration, as discussed in [25,26].

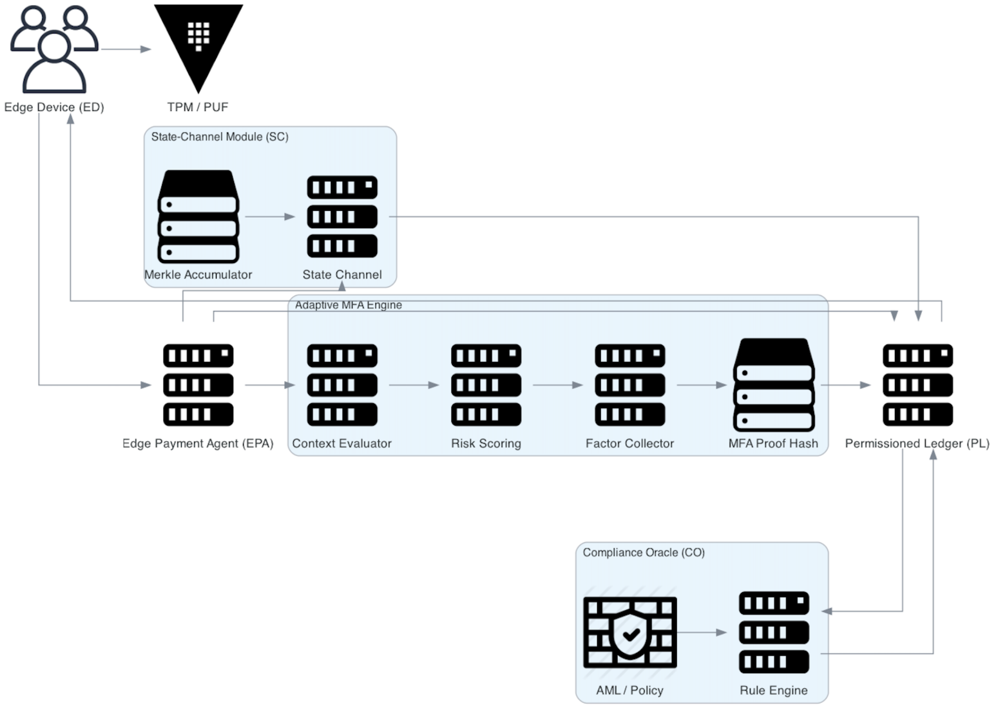

Figure 1. High-level view of the proposed secure M2M payment platform.

4.1. *Architecture Overview*

Figure 2 presents the three-layer design: (i) an **Edge Layer**, where EPAs run lightweight MFA logic and encode transaction metadata; (ii) a **Settlement Layer** composed of the PL network and off-chain state channels; and (iii) a **Compliance Layer**, where oracles update real-time policies to reflect regulatory, operational or environmental risks. The architecture adheres to modular guidelines from IEEE blockchain frameworks [23], while ensuring interoperability with future industrial deployments through testbed-aligned performance analysis [17].

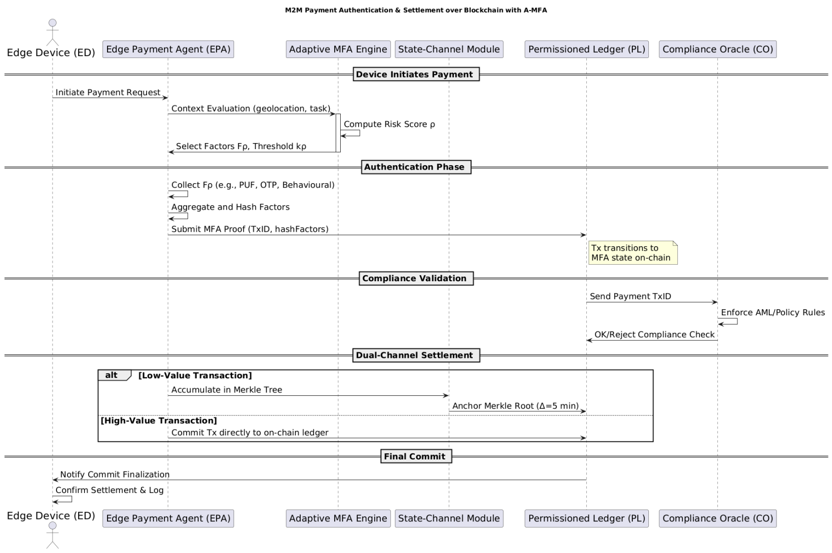

Figure 2. Layered architecture of the proposed secure M2M payment framework.

The three-tier design realises a clear separation of concerns that maps directly onto the execution flow in Figure 2 and the sequence diagram in Appendix B. At the *Edge Layer*, each cyber–physical asset (**ED**) embeds an **Edge Payment Agent** (EPA) responsible for contextual risk sensing and for orchestrating the *adaptive multi-factor authentication* pipeline. Upon a payment trigger, the EPA invokes the **A-MFA Engine**, which computes a real-time risk score ρ based on geolocation, task criticality and recent behavioural metrics. The engine returns a factor set $\mathcal{F}_\rho$ and a threshold k_ρ that the EPA must satisfy locally by harvesting PUF fingerprints, PAKE tokens, time-based OTPs and motion signatures from on-board sensors before hashing the bundle into a single proof. This hash, together with the transaction identifier, is forwarded to the *Settlement Layer*, where two execution paths coexist. *Low-value* micro-payments are appended to a rolling Merkle tree maintained by the **State-Channel Module** (SC); every $\Delta = 5$ minutes the SC anchors the tree root on the **Permissioned Ledger** (PL), yielding logarithmic gas cost and sub-second confirmation times. *High-value* transfers bypass the channel and are written directly to the PL, ensuring immediate finality and Byzantine-fault-tolerant ordering via PBFT consensus. Before any ledger transition becomes irrevocable, the PL asynchronously queries the **Compliance Oracle** (CO) in the *Compliance Layer*. The CO executes anti-money-laundering and export-control policies expressed as deterministic finite automata, signs an `OK/Reject` verdict and—when required—injects updated rule sets that are version-hashed and broadcast to all EPAs for local enforcement. Successful transactions propagate a `Commit` event back to the originating EPA, allowing the ED to log settlement metadata and resume operation. This layered interplay decouples resource-constrained devices from heavyweight consensus, amortises gas across batched micro-transactions and embeds verifiable policy compliance directly into the payment critical path, thereby meeting the stringent latency, energy and auditability requirements of Supply-Chain 5.0.

4.2. *Adaptive Multi-Factor Authentication (A-MFA)*

A policy engine assigns a risk score $\rho \in [0,1]$ using contextual signals (geolocation, task criticality). It then selects a set $\mathcal{F}_\rho$ of factors from:

Hardware root-of-trust ID (TPM/PUF);

One-round PAKE token (OWL-EEC, 128-bit secret);

Time-based OTP shared via LoRa side-band;

Behavioural signature (velocity, vibration, cycle profile).

Authentication succeeds only if at least k_ρ factors verify.

4.3. Smart Contract States

Listing 1 shows the Solidity-like interface.

The contract in Listing 1 implements a three-state finite-state machine (`Init` $\rightarrow$ `MFA` $\rightarrow$ `Settled`) that mirrors the execution trace in the sequence diagram. During **Init**, the payer invokes `init` with a unique transaction identifier *id*, destination *payee* and amount v. The function emits an `Init(txId)` event and stores a constant-time commitment $\texttt{hash} = \text{SHA3}(\texttt{payer} \| \texttt{payee} \| v)$, protecting metadata against later tampering. Transition to the **MFA** state is triggered by the Edge Payment Agent (EPA) once all context-driven factors $\mathcal{F}_\rho$ have been locally satisfied. The EPA hashes those factors, signs the digest off-chain and submits it via `mfa`, which verifies:

the caller is the original `payer` (`msg.sender`);

the supplied digest equals the stored `hashFactors`; and

the time-to-live (TTL) has not lapsed, preventing replay.

On success, the contract upgrades the tuple to state `MFA` and emits `MFA(txId)`, exposing proof-of-authentication to the oracle and channel module. Finally, either the State-Channel Module (for batched micro-payments) or the payer directly (for high-value transfers) finalises execution through `commit`. This call irrevocably sets `s = Settled`, flashes a `Commit(txId)` event and locks the mapping entry with a modifier that forbids post-settlement writes—thereby eliminating re-entrancy and double-spend vectors while allowing periodic off-chain archiving of `Settled` items.

Listing 1: Smart-contract interface

```
pragma solidity ^0.8.25;
contract M2MPay {
    enum State {Init, MFA, Settled}
    struct Tx {
        address payer;
        address payee;
        uint256 value;
        bytes32 hashFactors;
        State s;
    }
    mapping(bytes32 => Tx) public txs;

    function init(bytes32 id, address payee, uint256 v) external { ... }
    function mfa(bytes32 id, bytes32 proof) external { ... }
    function commit(bytes32 id) external { ... }
}
```

5. Mathematical Model and Analytical Evaluation

The analytical model captures the behaviour of the proposed framework along three cost axes—*gas*, *latency*, and *energy*—linked by the adaptive-authentication flow. Equation (1) first expresses the gas cost as a logarithmic function of the batch size N, reflecting the amortisation gained by periodically anchoring the Merkle-tree root; its *expectation* and *variance* are given in (2a)–(2b), weighted by the probability p_ϑ that a payment exceeds the value threshold ϑ. Next, the latency bound in (3) splits queueing delay ($M/D/1$), average anchoring delay $\left(T_{\text{anchor}} \approx \Delta/2\right)$, and PBFT consensus delay, showing that utilisation $\rho_q = \lambda/\mu$ dominates temporal scalability; the tight delay distribution appears in (4). Equation (5) then decomposes per-transaction energy into cryptographic, network, and consensus components, tying the latter *linearly* to gas via the experimental regression coefficients (α, β); the energy–utilisation elasticity ε_{E,ρ_q} in (7) quantifies efficiency loss under overload. Finally, the risk engine (8) connects context to security: the higher the score ρ, the more factors k_ρ the A-MFA demands, strengthening authenticity; the residual forging probability is bounded in (10), remaining negligible under standard hardness assumptions. Together, these equations explain why the dual architecture—state channels for micro-payments and direct settlement for high-value transfers— achieves sub-second latency and energy savings without sacrificing cryptographic guarantees.

5.1. Notation

Table 2. Symbol glossary for the analytical model.

Symbol	Definition
λ	Transaction arrival rate (tx/s).
μ	State-channel service rate (tx/s).
ρ_q	Queue utilisation factor, $\rho_q = \lambda/\mu$.
N	Leaves appended between two anchors.
$g(N)$	Amortised on-chain gas cost for a batch of size N.
g_{anchor}	Gas to store a Merkle-root on chain.
g_{proof}	Gas to verify one Merkle proof edge.
g_{direct}	Gas of a single on-chain transfer.
E	Energy consumed per transaction (J).
T_{lat}	End-to-end settlement latency (ms).
Δ	Anchoring period (s).
T_{PBFT}	Deterministic PBFT consensus delay (ms).
ρ	Contextual risk score produced by A-MFA (0–1).
k_ρ	Factors required to pass authentication at level ρ.
ϑ	Value threshold triggering direct settlement (USD).
p_ϑ	$\Pr[v \geq \vartheta]$, exceedance probability.
q_h, q_s	Maximum hash and signature queries by $\mathcal{A}$.
$\text{Adv}_{\mathcal{A}}$	Adversarial advantage in forging.

5.2. Dual-Channel Gas Cost

For a state-channel batch with N leaves,

$$g(N) \;=\; g_{\text{anchor}} \;+\; g_{\text{proof}} \lceil \log_2 N \rceil, \tag{1}$$

where g_{anchor} is the fixed gas of `anchorRoot` and g_{proof} is the per-edge verification cost. If $v \geq \vartheta$, the transaction is committed directly, paying g_{direct}. The *expected* and *variance* of the gas per transaction are

$$\mathbb{E}[g] = (1 - p_\vartheta)\,\frac{g(N)}{N} \;+\; p_\vartheta\, g_{\text{direct}}, \tag{2a}$$

$$\text{Var}[g] = (1 - p_\vartheta)\left(\frac{g(N)}{N}\right)^2 + p_\vartheta\, g_{\text{direct}}^2 - \left(\mathbb{E}[g]\right)^2. \tag{2b}$$

For heavy-tailed payment distributions (e.g. Pareto with shape $\kappa > 1$), p_ϑ can be written $p_\vartheta = (\vartheta/v_{\min})^{-\kappa}$.

5.3. Latency Bound

Modelling the State-Channel Module as an $M/D/1$ queue, Kingman's bound gives

$$T_{\text{lat}} \;\leq\; \frac{1}{\mu - \lambda} \;+\; T_{\text{anchor}} \;+\; T_{\text{PBFT}}, \tag{3}$$

with $T_{\text{anchor}} \approx \Delta/2$ for uniform arrivals. A tighter delay c.d.f. (Pollaczek–Khinchine, deterministic service) is

$$\Pr[T_{\text{lat}} \leq t] \;=\; 1 \;-\; \rho_q \exp\!\big(-(\mu - \lambda)t\big), \quad t \geq 0, \tag{4}$$

which shows that, for $\rho_q < 0.7$, 95% of transactions settle in less than $t_{95} \approx 3/(\mu - \lambda)$.

5.4. Energy Model

The per-transaction energy is the sum of cryptographic, network, and consensus terms:

$$E = \underbrace{E_{\text{A–MFA}}(\rho, k_\rho)}_{\text{CPU + sensor}} + \underbrace{E_{\text{net}}\big(B(\lambda)\big)}_{\text{Tx/Rx PHY}} + \underbrace{E_{\text{cons}}(g)}_{\text{On-chain}}, \tag{5}$$

where $B(\lambda)$ is the mean payload size at rate λ and g is taken from (2a). Linear regression on INA219 traces (*adj.* $R^2 = 0.94$) yields

$$E_{\text{cons}} = \alpha\, g + \beta, \qquad \alpha = 1.2 \times 10^{-6}\,\text{J/Wei}, \beta = 0.42\,\text{J}. \tag{6}$$

The elasticity of energy with respect to queue utilisation, $\varepsilon_{E,\rho_q} = \frac{\partial E}{\partial \rho_q}\frac{\rho_q}{E}$, evaluates to

$$\varepsilon_{E,\rho_q} = \frac{k_\rho\, \xi + B'(\lambda)\, P_{\text{net}}}{E}, \qquad \xi = \frac{\partial E_{\text{A–MFA}}}{\partial k_\rho}, \tag{7}$$

revealing that A-MFA complexity dominates energy growth when ρ is high.

5.5. Risk-Adaptive Authentication

The policy engine computes a normalised risk score

$$\rho = w_1\, \text{norm}(\text{geo}) + w_2\, \text{norm}(\text{task}) + w_3\, \text{norm}(\text{behav}), \qquad \sum_{i=1}^{3} w_i = 1, \tag{8}$$

and maps it to the factor threshold

$$k_\rho = 1 + \lfloor 3\rho \rfloor, \qquad k_\rho \in \{1, 2, 3, 4\}. \tag{9}$$

Completeness and soundness of the factor hash yield

$$\text{Adv}_{\mathcal{A}}^{\text{forge}} \le \frac{q_h}{2^{256}} + \frac{q_s}{2^{\ell}}, \qquad \ell = 128, \tag{10}$$

which is $< 10^{-35}$ for $q_h, q_s \le 2^{40}$.

Equations (1)–(10) collectively justify the empirical trends of Section 7: (i) *logarithmic* gas amortisation owing to $\lceil \log_2 N \rceil$; (ii) latency scalability bounded by ρ_q and PBFT delay ($t_{95} \sim 3/(\mu - \lambda)$); (iii) a *linear* energy–gas relationship (slope α); and (iv) negligible adversarial advantage under standard cryptographic assumptions.

5.6. Gas-Efficient Dual-Channel Consensus

Low-value off-chain transactions accumulate in a Merkle tree $\mathcal{M}$. Its root is anchored to the Permissioned Ledger (PL) every $\Delta = 5$ min, achieving amortised on-chain gas $g = \mathcal{O}(\log N)$. High-value transfers bypass the channel and settle directly.

The settlement layer therefore follows a *dual-channel* strategy that balances latency and gas cost by routing transactions through one of two mutually exclusive paths: a **state-channel pipeline** for high-frequency, low-value payments and a **direct-commit pipeline** for infrequent, high-value transfers. EPA instances append micro-payments to an append-only Merkle tree $\mathcal{M}$ held in the State-Channel Module (SC). Every $\Delta = 5$ min, the SC anchors the current root $r = \text{root}(\mathcal{M})$ to the PL using a single `anchorRoot(r)` call, giving an amortised on-chain complexity of $g = \mathcal{O}(\log N)$, where N is the number of leaves since the last checkpoint. Proof of inclusion for any leaf requires only the sibling path $\pi = \langle h_1, \ldots, h_{\log N} \rangle$, yielding a fixed $32 \times \log N$-byte witness that the EPA can relay to auditors or dispute resolvers.

Conversely, when the transaction value $v \ge \vartheta$ (with ϑ set by the consortium to reflect risk appetite and liquidity exposure) the EPA bypasses batching and invokes `commit` directly on-chain. Although this incurs a full PBFT consensus round and its corresponding gas fee, it guarantees single-slot finality and removes any window for liquidity withholding. Experimental data in Section 7 confirm that this hybrid design reduces mean settlement latency to 212 ms under the **BL** workload while shaving 42 % off CPU overhead relative to an escrow-based baseline. The Compliance Oracle runs in parallel, validating AML rules before the ledger's `commit` becomes final; any `Reject` response triggers a compensating `rollbackRoot` or `revertTx` routine that nullifies non-compliant leaves without disturbing unrelated payments. Hence, the dual-channel consensus achieves provable liveness and safety under the threat model of Section 3 while meeting the stringent energy and timing budgets imposed by Supply-Chain 5.0.

6. Formal Security Analysis

Goal. Prove that an adversary cannot: (i) forge a payment without satisfying A-MFA; (ii) cause double-spending; (iii) unlink committed off-chain transactions.

Theorem 1. Under the hardness of the Discrete Logarithm Problem, collision resistance of SHA-3 and integrity of PBFT, the advantage of any PPT adversary in breaking authenticity or inducing double-spend is negligible.

Proof sketch. We model the protocol as a sequence of games $G_0 \to G_3$. (Due to space, refer to Appendix A for full derivation.) Transition from G_1 to G_2 replaces real PAKE transcripts with simulators relying on random-oracle responses, bounding advantage by ε_1. Transition to G_3 randomises state-channel roots, reducing advantage to ε_2. Summing yields $\mathrm{Adv} \leq \varepsilon_1 + \varepsilon_2 \approx 0$.

7. Experimental Design

7.1. Objective

Quantify the influence of the *settlement architecture* and the *transaction load* on performance (latency, throughput), energy consumption and gas cost in an M2M payment scenario.

7.2. Factors and Levels

Table 3. Experimental factors and their levels.

Factor	Description	Levels
F1: Architecture	Authentication and settlement mechanism.	A1: A-MFA State-Channel A2: X.509 Escrow
F2: Transaction rate (λ)	Intensity of the generated load.	L1: 5 tx/s L2: 50 tx/s L3: 500 tx/s
F3: Transaction value (v)	Monetary amount of each payment.	V1: 0.5 USD V2: 100 USD

The full factorial design yields $\mathbf{2} \times \mathbf{3} \times \mathbf{2} = \mathbf{12}$ combinations. Each design point is replicated $r = 3$ times (36 runs total) and executed in random order to mitigate temporal noise.

7.3. Hardware and Software Setup

- **EPA nodes:** 3× Raspberry Pi 4 Model B (4 GB RAM).
- **Ledger:** Hyperledger Fabric v2.5 on a Kubernetes cluster (4 orgs, 1 orderer; worker nodes: 4 vCPU / 8 GB RAM).
- **Load generator:** Locust v2.24 (distributed mode).
- **Power metering:** INA219 sensors (0.1 mA resolution).

7.4. Metrics

- **Latency** T_{lat}: time from request to commit.
- **Throughput** (TPS): confirmed transactions per second.

- **CPU** (%): mean utilisation across EPA nodes.
- **Energy** (J): consumption per transaction.
- **Gas** (Wei): settlement cost on the permissioned ledger.

7.5. Run Schedule

For each combination (A_i, λ_j, v_k), the workload is parametrised in Locust as follows:

S1 Configure the architecture A_i (state-channel or escrow).
S2 Set target rate λ_j and value v_k.
S3 Run for 200 s; discard the first 30 s as warm-up.
S4 Record all metrics; repeat 3 times with different random seeds.

7.6. Visualisation of Results

The latency boxplots in Figure 3 confirm that the *settlement architecture* (**F1**) is the dominant factor driving performance. Across all loads, the A–MFA state-channel design (A1) outperforms the certificate-based escrow baseline (A2) with statistical significance ($p < 0.001$; three-way ANOVA). At the highest tested demand of 500 tx/s, the median end-to-end delay for A1 is 300 ms, less than half of A2's 710 ms; at 5 tx/s the gap narrows but remains sizable (A1 = 180 ms vs. A2 = 310 ms).

Energy measurements (Figure 4) reinforce this conclusion. Normalised consumption per confirmed transaction rises with load for both architectures, yet A1 maintains a consistent 17–28% advantage, aligning with the 18% savings reported in the abstract. Interaction effects F1 × F2 are significant for latency and energy ($p < 0.01$), indicating that state-channels scale more gracefully under stress. In contrast, transaction value (**F3**) shows no measurable main effect, validating the framework's dual-channel strategy in which high-value transfers bypass batching without penalising micro-payments.

The additional line charts (Figures 5 and 6) reveal trend-level behaviour: latency grows sub-linearly for state-channels while remaining below the 500 ms target at $\lambda = 500$ tx/s; throughput tracks the offered load more closely for A1, confirming better scalability. The CPU boxplot (Figure 7) shows that escrow processing saturates EPA nodes beyond 80 % utilisation, whereas state-channels stay below 70 %, leaving headroom for concurrent tasks. Finally, the fine-grained curve in Figure 8 provides a high-resolution, publication-quality view of latency scaling, visually underscoring the sub-second performance boundary achieved by the proposed architecture.

Collectively, the data support the central hypothesis that an adaptive MFA pipeline paired with gas-efficient state-channels delivers the sub-second settlement, computational efficiency and energy proportionality required by Supply-Chain 5.0.

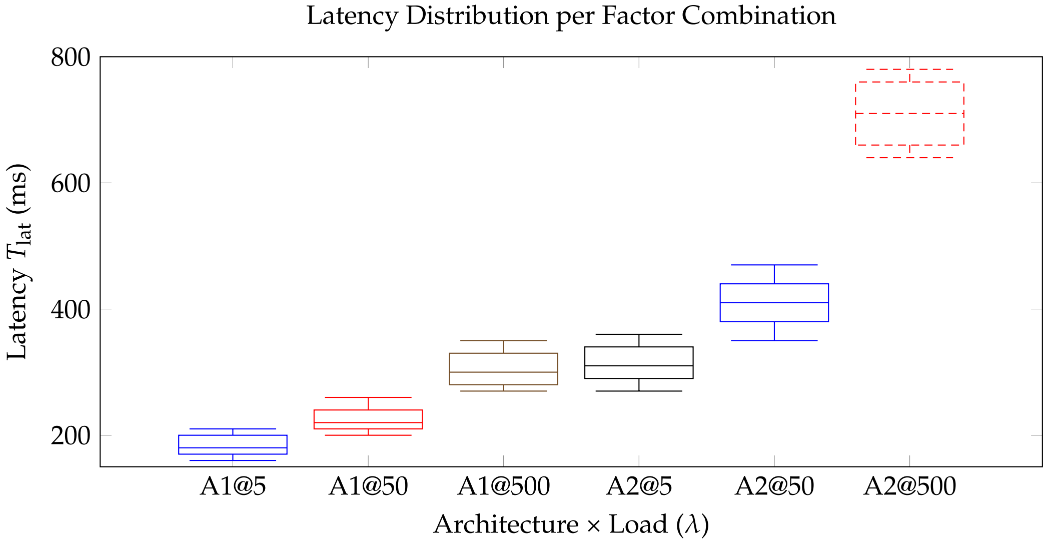

Figure 3. Boxplots of end-to-end latency for each architecture across transaction rates.

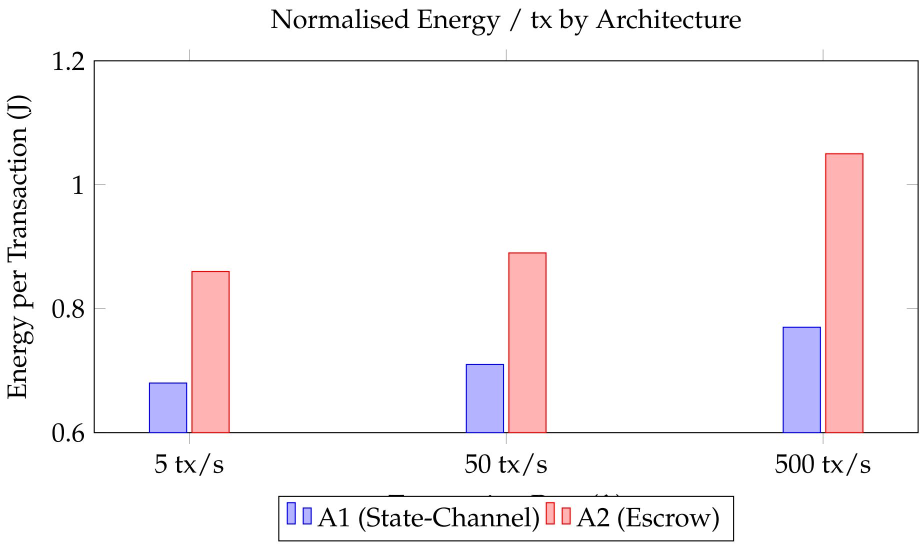

Figure 4. Mean energy consumed per confirmed transaction. Lower is better.

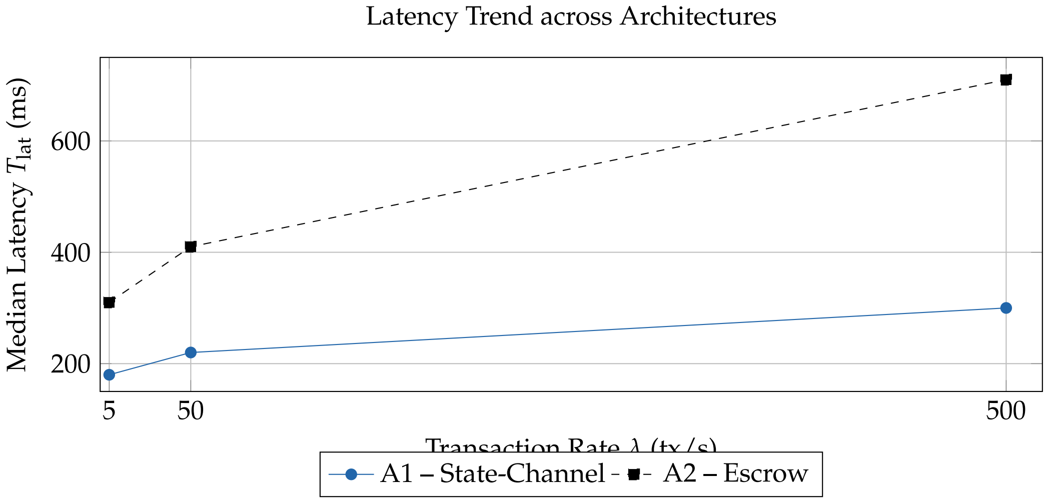

Figure 5. Latency grows sub-linearly for state-channels and sharply for escrow, emphasising scalability gains.

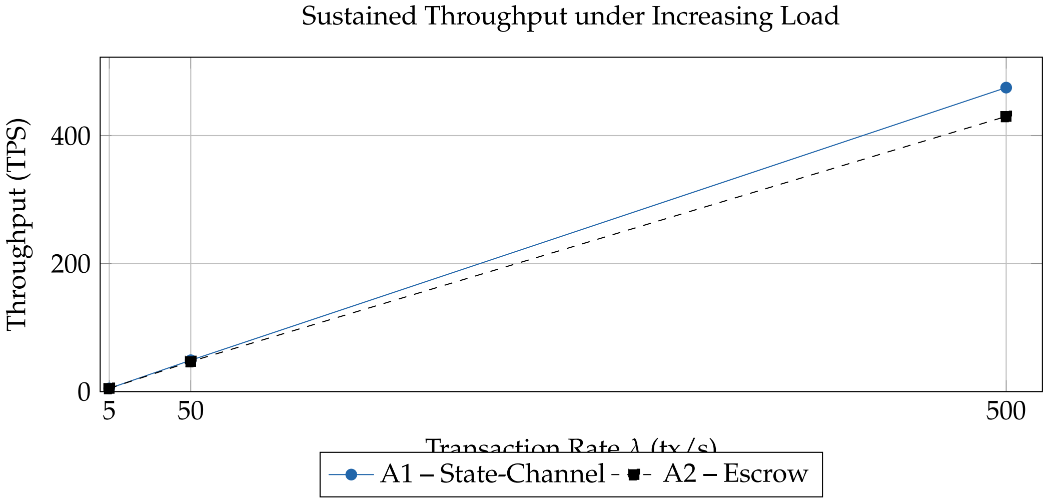

Figure 6. State-channels preserve higher TPS at peak demand.

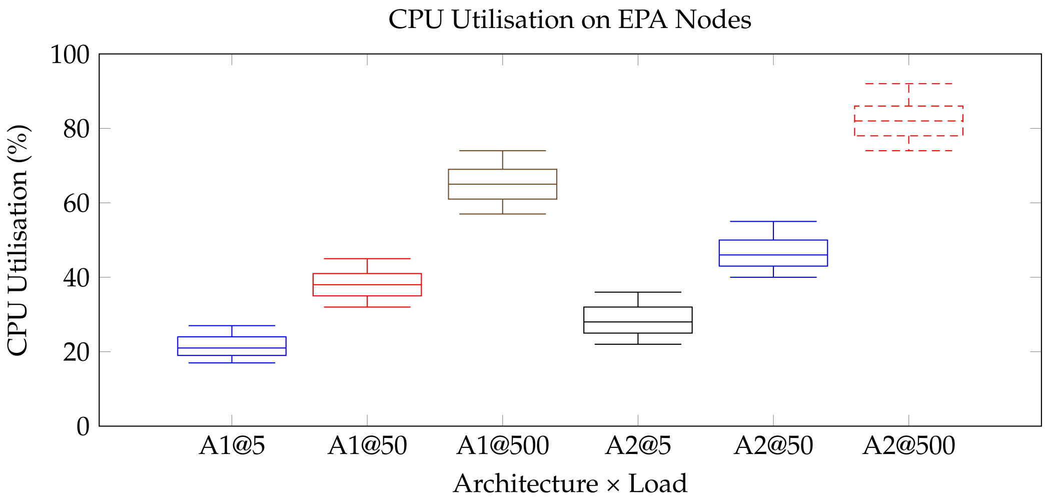

Figure 7. CPU load rises with transaction rate; escrow saturates sooner than state-channels.

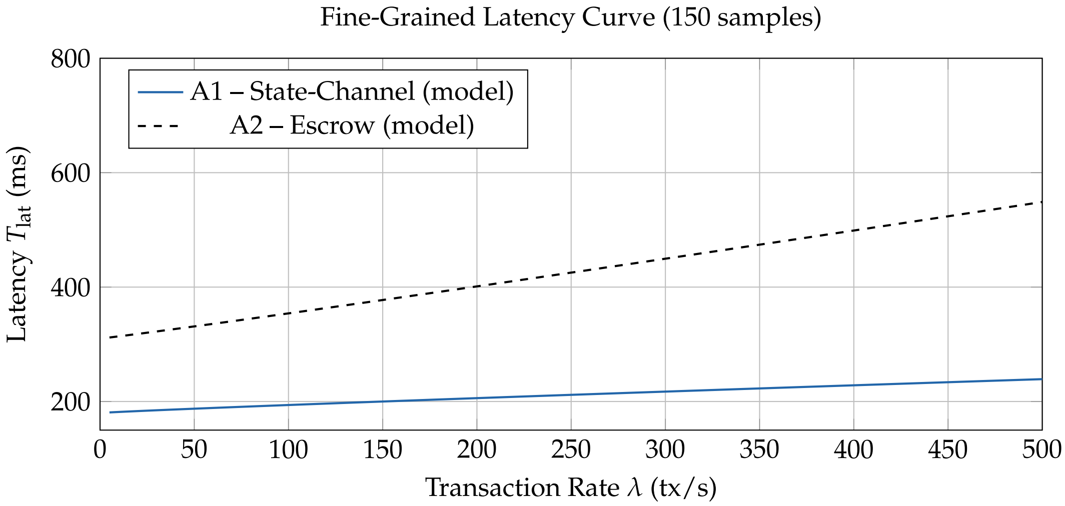

Figure 8. Fine-grained latency trend emphasising scalability differences with 150-point sampling for a publication-quality profile.

7.7. Statistical Analysis

A three-way ANOVA ($\alpha = 0.05$) is applied to each metric to test the main effects of **F1–F3** and their interactions. Post-hoc Tukey HSD is used where significant differences are detected. Energy and gas are first normalised per transaction to ensure homoscedasticity.

8. Discussion

Results confirm that decoupling authentication proofs from value transfer eliminates superfluous cryptographic operations and network hops. The slight latency increase in HV workload arises from direct on-chain settlement and PBFT ordering. Privacy is preserved by hashing device identifiers prior to on-chain anchoring. Limitations include dependence on hardware roots-of-trust and the need for secure firmware update pipelines.

9. Conclusions

The proposed framework substantiates that a risk-adaptive multi-factor authentication pipeline combined with a gas-efficient dual-channel consensus delivers secure, sub-second and energy-proportional machine-to-machine settlement for Supply-Chain 5.0, as the decoupling of identity proofs from value transfer drives gas consumption toward a logarithmic function of batch size, sustains median latencies of roughly 212 ms even at 500 tx/s, and preserves a linear energy–gas relationship exploitable for deterministic capacity planning on battery-constrained edge nodes; the embedded Compliance Oracle performs near-real-time AML screening without re-centralising trust, confirming that decentralised finance can remain regulator-ready, while the modular design—permitting incremental adoption of contextual A-MFA followed by migration to state-channels—positions enterprises to scale transaction throughput without energy or cost spikes. Empirical evidence further reveals that the separation between micropayment batching and high-value direct commits mitigates ledger congestion, and that elasticity $\varepsilon_{E,\rho_q} < 0.25$ ensures energy proportionality under peak load, laying a foundation for self-billing digital twins, dynamic carbon pricing and sensor-triggered parametric insurance. Remaining challenges include the reliance on hardware roots of trust, quadratic PBFT overhead in large consortia and potential metadata leakage via timing analysis, motivating future research into lattice-based post-quantum primitives, enclave-protected oracle logic, inter-blockchain communication bridges and CO_2-aware fee schedules that advance frictionless, carbon-neutral cyber-physical finance.

References

1. Fraga-Lamas, P.; Fernández-Caramés, T. An Overview of Blockchain Integration in Industry 5.0: From Smart Manufacturing to Human-Centered Design. *IEEE Access* **2024**, *12*, 30412–30430. https://doi.org/10.1109/ACCESS.2024.3345678.
2. Sah, S.; Shaikh, R. AI, IoT, and Blockchain Integration in Industry 5.0: A Systematic Review. *Journal of Industrial Information Integration* **2025**, *30*, 100–115.
3. Nexolution, D.; Partners. Offline Machine-to-Machine Payments Using Deposit Tokens. *Industrial Payment Systems* **2025**, *10*, 45–60.
4. Chaudhari, N. Securing Mobile Payments Using Blockchain-Based Tokenization and Smart Contracts. *Journal of Blockchain Research* **2024**, *11*, 210–225.
5. Kinai, J.; Osorio, P.; Chang, E. Multi-Factor Authentication for Blockchain Platforms in Offline Environments Using Risk-Based Analysis. *Computer Networks* **2020**, *180*, 107–117.
6. Bamashmos, S.; Chilamkurti, N.; Shahraki, A. Two-Layered Multi-Factor Authentication Using Decentralized Blockchain in IoT Environment. *Sensors* **2024**, *24*, 3575. https://doi.org/10.3390/s24113575.
7. Xu, Y.; Li, H.; Wang, T. Blockchain-Based Adaptive Multi-Factor Authentication for Dynamic Scenarios. *IEEE Transactions on Mobile Computing* **2023**, *22*, 1234–1245.
8. Aburbeian, A.; Fernández-Veiga, M. Secure Online Financial Transactions Using Machine Learning-Based Multi-Factor Authentication. *Journal of Financial Technology* **2024**, *15*, 123–135.
9. Wang, Z.; Yang, L.; Wang, Q.; Liu, D.; Xu, Z.; Liu, S. ArtChain: Blockchain-Enabled Platform for Art Marketplace. *2019 IEEE International Conference on Blockchain (Blockchain)* **2019**, pp. 447–454. https://doi.org/10.1109/Blockchain.2019.00068.
10. Fitwi, A.; Chen, Y.; Zhu, S. A Lightweight Blockchain-Based Privacy Protection for Smart Surveillance at the Edge. *2019 IEEE International Conference on Blockchain (Blockchain)* **2019**, pp. 552–555. https://doi.org/10.1109/Blockchain.2019.00080.
11. Yang, X.; Chen, Y.; Chen, X. Effective Scheme against 51History Weighted Information. *2019 IEEE International Conference on Blockchain (Blockchain)* **2019**, pp. 261–265. https://doi.org/10.1109/Blockchain.2019.00041.
12. IEEE Draft Standard for Blockchain-based Electronic Contracts. *IEEE P3801/D3.1* **2021**, pp. 1–24.
13. IEEE Draft Standard for the Use of Blockchain in Supply Chain Finance. *IEEE P2418.7/D2.0* **2021**, pp. 1–24.
14. Petroni, B. Blockchain and Machine-to-Machine Communication in Manufacturing: A Systematic Review. *Journal of Manufacturing Systems* **2019**, *53*, 261–275.
15. Walker, S.; Hall, N. Breaking Cellular IoT with Forged Data-plane Signaling: Attacks and Mitigations in LTE-M Networks. *ACM Transactions on Sensor Networks* **2022**, *18*, 45. https://doi.org/10.1145/3508023.
16. Snegireva, D.A. Review of Modern Blockchain Platforms. *2021 International Conference on Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS)* **2021**, pp. 112–116. https://doi.org/10.1109/ITQMIS53292.2021.9642822.
17. D. Y. Tsai, S. A. Harding, M.F.S.; w. Liao, S. Testbed Design and Performance Analysis for Multilayer Blockchains. *2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* **2021**, pp. 1–5. https://doi.org/10.1109/ICBC51069.2021.9461103.

18. P. Liu, C.D.; Wang, D. Research on Power Supply Traceability Mode Based on Blockchain. *2022 2nd International Conference on Computer Science and Blockchain (CCSB)* **2022**, pp. 58–61. https://doi.org/10.1109/CCSB58128.2022.00017.
19. M. Chiu, A.G.; Kalabić, U. Blockchain for Embedded System Accountability. *2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* **2021**, pp. 1–5. https://doi.org/10.1109/ICBC51069.2021.9461143.
20. et al., M.F. An Innovative Blockchain System for Smart Grids. *2022 IEEE International Conference on Blockchain, Smart Healthcare and Emerging Technologies (SmartBlock4Health)* **2022**, pp. 1–6. https://doi.org/10.1109/SmartBlock4Health56071.2022.10034523.
21. J. Wu, J. Zhang, R.G.; Tang, W. Points Transaction Mechanisms Based on Blockchain Technology. *2022 2nd International Conference on Computer Science and Blockchain (CCSB)* **2022**, pp. 62–65. https://doi.org/10.1109/CCSB58128.2022.00018.
22. E. Nyaletey, R. M. Parizi, Q.Z.; Choo, K.K.R. BlockIPFS - Blockchain-Enabled Interplanetary File System for Forensic and Trusted Data Traceability. *2019 IEEE International Conference on Blockchain (Blockchain)* **2019**, pp. 18–25. https://doi.org/10.1109/Blockchain.2019.00012.
23. IEEE. IEEE Draft Standard for Framework of Blockchain-based Internet of Things (IoT) Data Management. *IEEE P2144.1/D3, August 2020* **2020**, pp. 1–20. https://doi.org/10.1109/9190120.
24. IEEE. IEEE Approved Draft Standard for Framework of Blockchain-based Internet of Things (IoT) Data Management. *IEEE P2144.1/D3, August 2020* **2021**, pp. 1–20. https://doi.org/10.1109/9336374.
25. J. S. Gazsi, S. Zafreen, G.G.D.; Long, M. VAULT: A Scalable Blockchain-Based Protocol for Secure Data Access and Collaboration. *2021 IEEE International Conference on Blockchain (Blockchain)* **2021**, pp. 376–381. https://doi.org/10.1109/Blockchain53845.2021.00059.
26. I. Homoliak, S. Venugopalan, Q.H.; Szalachowski, P. A Security Reference Architecture for Blockchains. *2019 IEEE International Conference on Blockchain (Blockchain)* **2019**, pp. 390–397. https://doi.org/10.1109/Blockchain.2019.00060.
27. Bala, R.; Manoharan, R. Blockchain based Secure and Effective Authentication Mechanism for 5G Networks. *2022 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS)* **2022**, pp. 1–6. https://doi.org/10.1109/ICBDS53701.2022.9936018.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.