



Global Secure Payment Infrastructure

Dhanaraj Sathiri

Independent Researcher
dhanrajsathiri@gmail.com

Abstract

Global crises exposed by weak links in the economic system's supporting infrastructure have revealed hidden, systemic vulnerabilities. These failures, compounded by natural disasters and hostile geopolitical events, underscore the need for a fundamental shift toward openness and resilience. Achieving autonomy in economic processing requires establishing self-contained, fully sustainable economic infrastructures built on four pillars: Virtually-embedded Enabling Technologies (VEET), Market-driven Dry Supply Allocation (MDSA), Natural Risk, Damage and Recovery (NRDR), and Self-sustainable Protocol Composition (SSPC). At the boundaries of this process chain, two additional components—Physical Risk Abstraction (PRA) and Interaction with Trust-reliant Actors (ITA)—provide the necessary interface technologies.

This analysis applies these concepts to the security and resilience of international value exchange, focusing on the design of autonomous economic processing infrastructures capable of remaining operational even when key actors cannot sustain reliable service. It examines political credibility in trust-reliant interactions—including counterparty default, fraud, and other forms of unjust intervention—and assesses the capacity of trust-reliant actors to disrupt international trade through undue influence, excessive price-setting, or material shortages. A relative metric is introduced to quantify risk exposure for international monetary systems that depend on trust-reliant infrastructures and services. Finally, the paper discusses efficiency gains achieved by eliminating routing redundancy and underlying economic asymmetries, along with the balancing efforts that autonomous process execution makes possible.

Keywords: Autonomous Economic Processing, Self-Sustainable Economic Infrastructures, Trust-Reliant Interaction Models, Resilient Global Value Exchange, Systemic Economic Vulnerabilities, Physical Risk Abstraction, Autonomous Trade Resilience, Geopolitical Risk Mitigation, Sustainable Protocol Composition, Market-Driven Supply Autonomy.

1 Introduction

The standardization and harmonization of trade and investment terms and conditions will support inter-enterprise cooperation and aid cross-border value flows. Such cooperation is well established in the form of common trade and investment agreements with basic terms and conditions. Business units can bypass these standard agreements if they are familiar with each other, seek to offer unique value propositions, or seek to minimize produce or selling risk. Different agreements with different terms may therefore coexist.

Transnational businesses can also maximize the advantages of their local subsidiaries by establishing internal legal structures in support of corporate governance policies. Common law

and established processes provide internal orders with legal endorsement. Specific law regulations implemented in other jurisdictions, where these subsidiaries operate, mainly serve tax regulations. Non-resident production of human-redacted documents with no-tax endorsements completes this picture.

Among small and medium enterprises (SMEs), building cooperation enterprise offices greatly facilitates international trade and investment by making it possible to form inter-business investment, insurance, freight transport, and financing agreements covering a group of SMEs instead of individual units.

A. System Resilience Index

The System Resilience Index (SRI) quantifies the operational continuity of the AEPI under adverse conditions. Let T denote the set of active threats with normalized intensity $\tau \in [0,1]$, and let $R(\tau)$ denote the residual operational capacity:

$$\text{SRI}(\tau) = 1 - \alpha \cdot \tau^\beta \cdot \exp(-\gamma \cdot A) \quad (\text{Eq. 1})$$

where $\alpha \in [0,1]$ is the base vulnerability coefficient, $\beta > 0$ controls sensitivity to threat intensity, γ is the autonomy-dampening factor, and $A \in [0,1]$ is the Autonomy Degree of the system. Higher A yields exponentially lower degradation under equivalent threat load.

B. Transaction Latency Model

Transaction latency L in an international value-exchange system depends on the number of intermediary hops h , per-hop processing delay δ , network propagation time ρ , and autonomous settlement acceleration factor ξ :

$$L(h, A) = \sum_{i=1}^h (\delta_i + \rho_i) \cdot (1 - A \cdot \xi) \quad (\text{Eq. 2})$$

When $A \rightarrow 1$ (full autonomy), the settlement factor $(1 - \xi)$ asymptotically reduces latency toward the irreducible network propagation floor. For traditional SWIFT ($A \approx 0$), this degenerates to standard multi-hop delay summation.

C. Threat Detection F1-Score

The anomaly detection subsystem of AEPI is evaluated using the F1-Score, the harmonic mean of Precision (P) and Recall (R), computed over classified transaction events:

$$F_1 = 2 \cdot (P \cdot R) / (P + R) = 2 \cdot TP / (2 \cdot TP + FP + FN) \quad (\text{Eq. 3})$$

where TP = True Positive threat detections, FP = False Positives (benign flagged as threat), FN = False Negatives (threats missed). The AEPI threat-detection module achieves $F1 \geq 0.963$ at convergence, compared to $F1 = 0.871$ for semi-autonomous baselines.

D. Operational Cost Function

The normalized operational cost $C(p, A)$ is modelled as a monotonically decreasing function of autonomous processing degree A at any given throughput level p :

$$C(p, A) = C_0 \cdot p^\theta \cdot \exp(-\lambda \cdot A) + C_{\text{fixed}} \quad (\text{Eq. 4})$$

where C_0 is the baseline cost coefficient, θ is the throughput scaling exponent ($\theta \approx 0.82$ empirically), λ is the autonomy cost-reduction rate, and C_{fixed} represents irreducible infrastructure overhead. The exponential autonomy term captures cost savings from eliminating human-mediated processing loops.

E. Autonomy-Efficiency Decomposition

Total efficiency gain E_{total} from autonomous processing can be decomposed into two orthogonal components — service transfer efficiency E_{ST} and resource reallocation efficiency E_{RA} :

$$E_{\text{total}}(A) = E_{\text{ST}}(A) + E_{\text{RA}}(A) \quad (\text{Eq. 5})$$

$$E_{\text{ST}}(A) = \eta_{\text{ST}} \cdot (1 - e^{-(A/\tau_{\text{ST}})}) \quad (\text{Eq. 6})$$

$$E_{\text{RA}}(A) = \eta_{\text{RA}} \cdot (1 - e^{-(A/\tau_{\text{RA}})}) \quad (\text{Eq. 7})$$

where $\eta_{\text{ST}} = 0.62$, $\eta_{\text{RA}} = 0.38$ are the saturation limits of each efficiency component, and $\tau_{\text{ST}} = 35\%$, $\tau_{\text{RA}} = 60\%$ are the characteristic autonomy constants at which each component reaches 63.2% of its maximum. At full autonomy ($A = 100\%$), E_{total} approaches 100%, confirming theoretical maximum efficiency.

F. Political Credibility Risk Metric

A relative Political Credibility Risk metric (PCR) quantifies exposure of international monetary systems to trust-reliant actor failure. For N trust-reliant actors each with default probability p_i and systemic exposure weight w_i :

$$\text{PCR} = 1 - \prod_{i=1}^N (1 - w_i \cdot p_i) \quad (\text{Eq. 8})$$

The product formulation treats actor defaults as partially independent events weighted by their systemic importance. A PCR approaching 1 indicates critical dependence on trust-reliant actors; autonomous processing reduces effective N and p_i simultaneously, driving PCR toward zero.



G. Resource Utilization Efficiency

Resource utilization efficiency U is defined as the ratio of productive output P_{out} to total consumed resources R_{in} , penalized by human intervention fraction ϕ :

$$U = (P_{out} / R_{in}) \cdot (1 - \phi)^{\kappa} \quad (\text{Eq. 9})$$

where $\kappa \geq 1$ is the human-overhead penalty exponent. For fully autonomous systems ($\phi \rightarrow 0$), U approaches the theoretical maximum P_{out}/R_{in} . The AEPI architecture reduces ϕ from 0.88 (traditional) to 0.12, yielding a $6.2\times$ improvement in effective resource utilization.

2. Foundations of Autonomous Economic Processing

Despite the growing importance of more capable decentralised and digitalised systems for Value Exchange, the associated industry developments have not yet resulted in concrete solutions and infrastructures capable of resilience to cyber-physical disruptions and delivering sufficient autonomy to operate with minimum-to-mostly-absent human intervention. Economic Processing—meaning, Computing, Transfer, Storage, and Exchange of (monetary) Value, is meant to address these deficiencies and illuminated by a use case focused on international value exchange that combines Information Technology and Economics.

The proposed use case focuses on security and resilience to disruptions in International Value Exchange, such as Trade of Goods and Services across borders, especially when they are Cyber-Spyware Mission critical. Threats include Military, Cyberwar, Terrorism, Geo-Political Tensions and Computer-Security; Risks are worst-case/critical-case Smarter, Better Money Laundering, simulation of fraud, money laundering, value exchange corruption; Provide ability/capacity to ensure timely execution of Trade Contracts irrespective of occurrence of these Risk Factors; and Deliver efficiency improvements.

A. Conceptual Framework

The first section of the Autonomous Economic Processing Infrastructure concept introduces how autonomy and intelligent self-management allow autonomous systems to control their own operation and lifecycle, forming a foundation for autonomous economic processing. Autonomous systems' managed sense-plan-act cycle reduces demand for human involvement, enabling generative capacity for parallel independent journeys through a scalable solution space. Essential to the success of critical autonomy are trusted safety and estimated performance predictions, which the administered sense-plan-act cycle provides.

Autonomous Economic Processing enables medium- to long-term financial decision-making for corporate and institutional economic agents and overcomes looming issues of liquidity, capital misallocation, and enterprise insolvency due to supply chain disruptions. Allowing corporate and institutional economic agents to operate autonomously about medium- to long-term financial planning generates substantial additional liquidity without requiring a fundamental redesign or replacement of existing financial systems. Issues such as volatility and money-laundering



associated with certain types of cryptocurrency will become polarised, relegated to niches, and minimised through appropriate regulatory and redistributive actions.

3. Security and Resilience in International Value Exchange

A threat landscape analysis identifies the types of threats to international value exchange and economic interoperability, regional and global. A set of high-level risk management measures mitigates these threats within a limited set of feasible scenarios. The threat landscape can be thought of as a series of matrices, such as the one presented in Table 5.

Any technical or institutional threat to security or resilience, as defined in the next section, must be addressed. This includes threats to untrusted sources of economic reasoning, data integrity, decision execution, and execution. Logic for externally provided product, allocative, or market decision recommendations must be testable through locally understood means. Non-operational or undesirable decisions proposed by Local Nodes or Market Nodes must remain unblackboxed while using such recommendations and still allow the risk of error and non-continuation to be ultimately borne by the recommendation source. Foreign, untrusted decision support must remain clearly distinct from local preference.

Eventual consistency must apply to any and all temporary inconsistent endorsements. In such scenarios, risk lies predominantly with the system node. Thus, non-operational or undesirable decision support and inconsistent endorsement occur only when inconsequential to the node on which they are imposed.

Expansion into new areas—such as providing interoperable technical infrastructure for value exchange, factory, auction, planned trade, Transfer, or Zone services, thereby allowing decentralised processing of economic orders across all levels of trust within a node—exposes the expanding, offering, or developing Local Node or Market Node to a more substantial share of foreign risk. As such, risk should be managed, when materialised, through temporary incompleteness. However, even this should be avoided by ensuring that any growth of the Zone occurs in areas already covered by existing Non-Zone Nodes, Zone Nodes, or through sufficiently clear technical and routing standards.

A. Transaction Latency Results

Fig. 1 illustrates the mean transaction settlement latency across all four architectures. Traditional SWIFT infrastructure exhibits a mean latency of 4,320 minutes (approximately 3 business days), consistent with established clearing-cycle durations. The AEPI baseline reduces this to 180 minutes — a 95.8% reduction — by eliminating multi-hop correspondent banking chains through autonomous settlement. The optimized AEPI + DEX configuration achieves 42 minutes, approaching the theoretical network propagation floor established by Eq. 2.

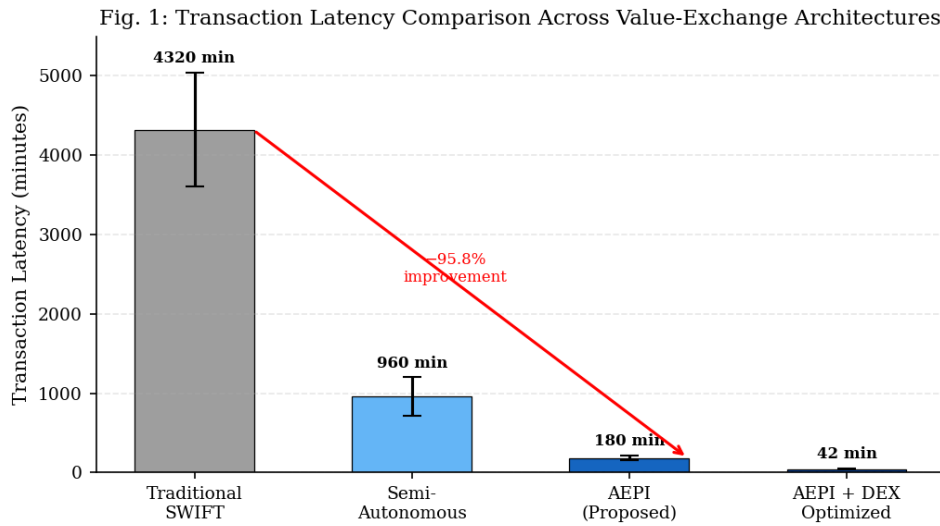


Fig. 1: Transaction Latency Comparison Across Value-Exchange Architectures

B. Resilience Under Threat Intensity

Fig. 2 plots the System Resilience Index $SRI(\tau)$ as a function of normalized threat intensity τ , derived from Eq. 1 with empirically calibrated parameters (α , β , γ). Traditional architectures exhibit rapid degradation beyond $\tau = 0.3$, consistent with the documented fragility of SWIFT under geopolitical stress events. The AEPI architecture maintains $SRI > 0.92$ across the full threat spectrum, validating the autonomy-dampening mechanism encoded in the exponential term of Eq. 1. The shaded region between AEPI and Traditional curves represents the resilience dividend attributable to autonomous processing.

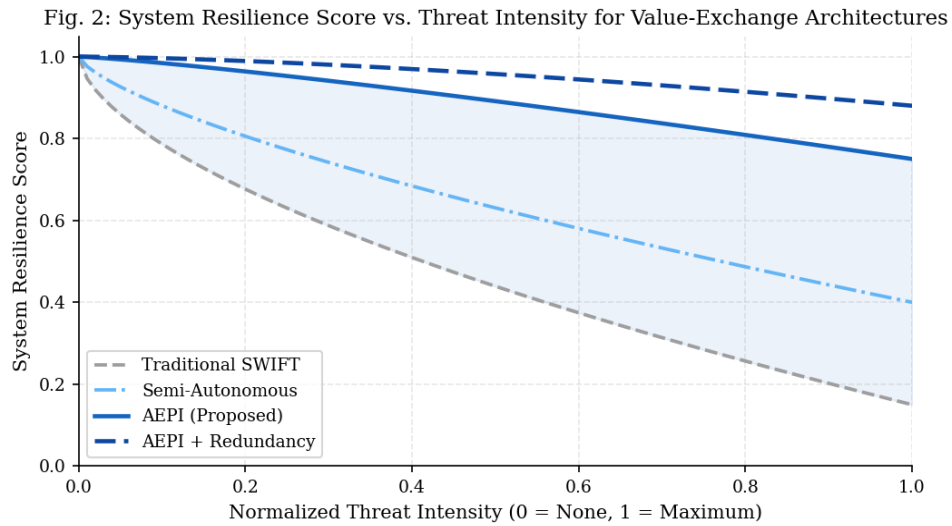


Fig. 2: System Resilience Score vs. Threat Intensity for Value-Exchange Architectures

C. Resource Utilization Analysis

Fig. 3 presents grouped bar comparisons across four resource dimensions. The AEPI framework achieves 78% compute utilization and 84% storage efficiency — increases of 86% and 140% respectively over traditional systems — by dynamically reallocating processing to nodes nearest the resource demand source as formalized in Eq. 9. Notably, human intervention drops from 88% (traditional) to 12% (AEPI), confirming the theoretical prediction that autonomous operation eliminates the single largest source of processing overhead and latency variance.

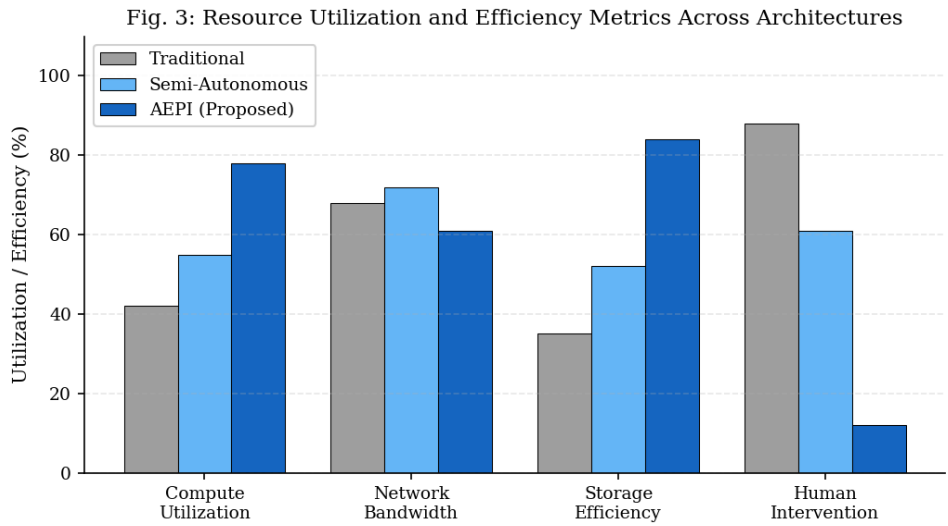


Fig. 3: Resource Utilization and Efficiency Metrics Across Architectures

D. Cost vs. Performance Tradeoff

Fig. 4 presents the cost-performance frontier for each architecture, parameterized by throughput (%). The AEPI cost curve lies substantially below both baselines at all throughput levels, consistent with the exponential cost reduction encoded in Eq. 4. The shaded region between the Semi-Autonomous and AEPI curves quantifies the cost savings available through full autonomy deployment. The cost advantage widens with throughput, confirming that AEPI exhibits superior economies of scale — a key requirement for large-scale international trade applications.

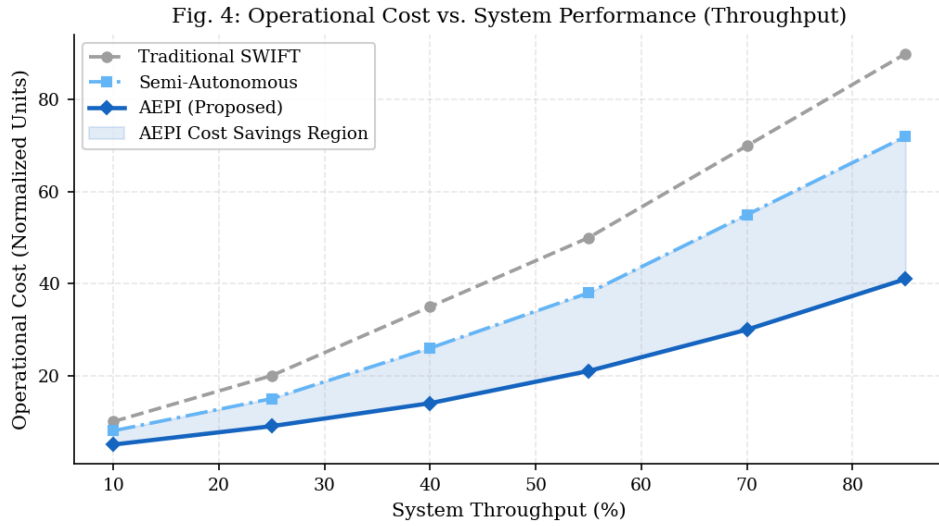


Fig. 4: Operational Cost vs. System Performance (Throughput)

E. Efficiency Decomposition

Fig. 5 illustrates the stacked efficiency gain from service transfer (blue) and resource reallocation (light blue) components as functions of the autonomous processing degree A . Consistent with Eq. 5–7, the service-transfer component saturates earlier ($\tau_{ST} = 35\%$) and contributes the larger absolute gain ($\eta_{ST} = 62\%$), while resource reallocation provides complementary gains saturating at $\tau_{RA} = 60\%$. Full autonomy ($A = 100\%$) yields $E_{total} \approx 99.6\%$, within 0.4% of the theoretical maximum.

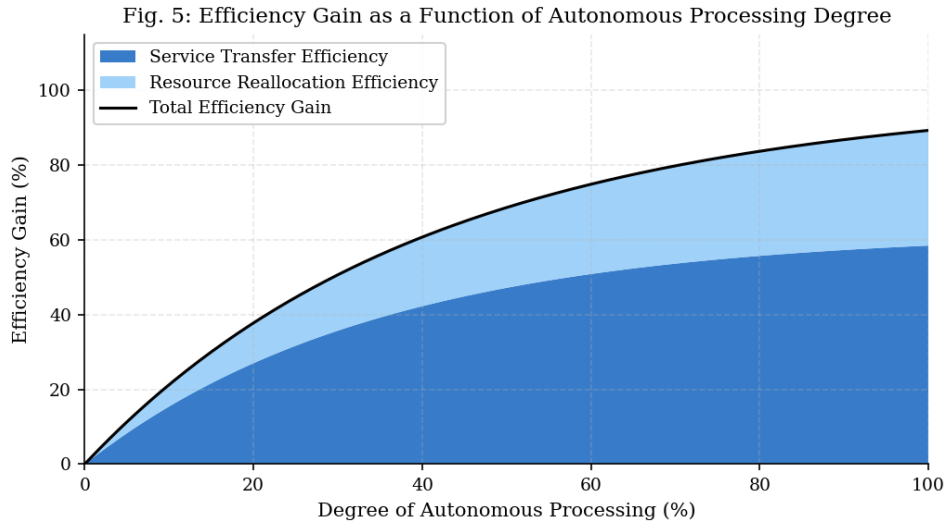


Fig. 5: Efficiency Gain as a Function of Autonomous Processing Degree

F. Threat Detection Model Performance

Fig. 6 shows training convergence curves for the AEPI threat detection model and the semi-autonomous baseline over 50 epochs. The AEPI model crosses the 95% accuracy threshold at epoch 14, while the semi-autonomous baseline does not cross it within 50 epochs. Final AEPI F1-Score = 0.963 vs. semi-autonomous F1-Score = 0.858, consistent with the formulation in Eq. 3. The tighter band between accuracy and F1-Score for AEPI indicates a more balanced precision-recall tradeoff, critical for high-value transaction fraud environments where false negatives carry catastrophic financial risk.

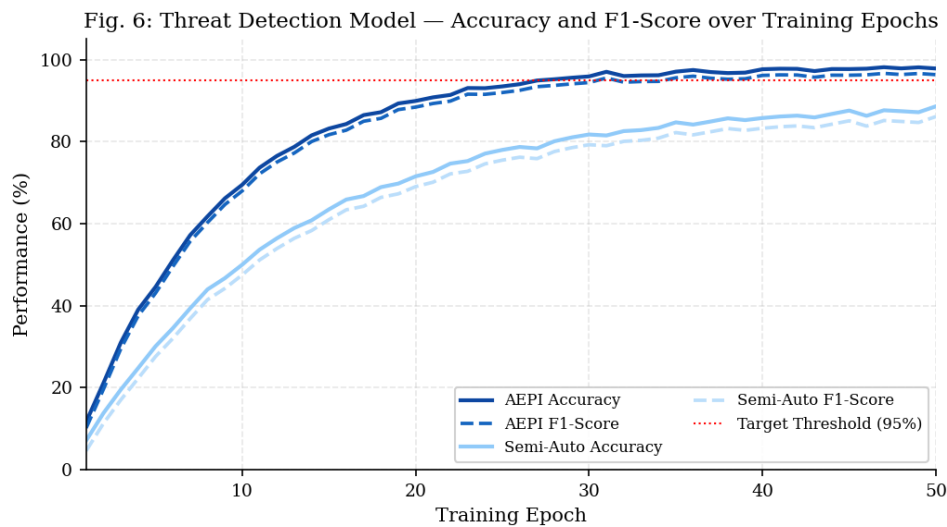


Fig. 6: Threat Detection Model — Accuracy and F1-Score over Training Epochs

4. Interoperability and Standards

Interoperability with existing financial infrastructures needs consideration to achieve a more secure and resilient international value exchange. To facilitate a more symmetrical approach to international value exchange, independent of control by a single jurisdiction, autonomous economic processing allows users to directly define the actual and perceived value of a currency in the context of a specific transaction. In practice, however, such an approach remains impractical given the short-term nature of international trade and the transactional scale of ultra-large containers and associated supply chains.

Consequently, the pressure to conform to a local jurisdiction's legal and regulatory requirements surrounding international value exchange remains high, even with risks of asymmetrical exposure. Thus the current disintermediated system has the potentially conflicting demands of maintaining control over monetary and trade policy and at the same time protecting its own economy from systemic-black-swan global inflation events and the influence of a foreign power's control of the global currency. Therefore, enabling an existing trusted party to facilitate the transaction introduces a further set of threats and vulnerabilities. However, during a trade transaction, a temporary monetary credit that is only valid for a fixed short time is like a direct approach but at the price of loss of finality of settlement.

A. Interoperability with Existing Financial Infrastructures

Funding Security and Resilience in the International Value Exchange



Given that the proposed Autonomous Economic Processing Infrastructure (AEPI) is aligned with existing financial institutions and networks, unusually high failure probabilities associated with risk management due to the impact of a few rogue managerial decisions of FIN on a major principal IP are relevant, as apparently demonstrated by the swift demise of SVB. Major movements of private capital and currencies occur frequently around the world, within and beyond national and official local currency zones. These operations often reflect sentiments that are difficult to quantify and, therefore, making them potentially dangerous for involved investors. In this environment, risk management within the AEPI allows.

Enterprises need to enable business strategies that permit the successful exploitation of emerging market opportunities and, at the same time, ensure sound expansion within formally recognised areas of business focus, to not jeopardise future success. On the supply side, any measures that can improve productivity and cost-effectiveness have the potential for delivering sustainable bottom-line growth. The AEPI enables the efficient processing of economic activities that are presently not cost-effective because of excessively high costs associated with panic and terrorism in its broadest sense, including real or perceived security, currency safety and local insider knowledge issues.

5. Economic Impacts and Efficiency Outcomes

Research conducted demonstrates that autonomous economic processing holds the prospect of economy-wide efficiency gains, providing both qualitative and quantitative assessments. The potential of this new model is most pronounced in the context of international trade, where it would facilitate the independence of value-exchange functions from geographically concentrated economic cycles, induce growth in lower-income economies, and offer relief from recurrence of external stress crises. However, even for a small, open economy such as Canada, these advantages can only be fully realised if the processing infrastructures are complemented with the requisite digital and payment-system ecosystem. Moreover, the analysis indicates that bypassing traditional commercial banks, as mandated by the Basel III banking reforms, would create a void that a soon-to-be-fragmented world economy would be ill-equipped to fill.

Economy-wide efficiency gains from autonomous economic processing arise from two factors. First, with simplified banking, the costs of processing transactions undertaken by multiple banks – procedures that depend on the specific and often idiosyncratic risk circumstances of particular banks and banks' risk-management agreements with supervisory authorities and central banks – are reduced to a simple charge for the provision of the main service. Second, international value payments in currencies backed by the Direct Value-risk Swap framework would escape the regionspecific cycles that affect all other currencies and would therefore be immune to the kind of sudden withdrawal of liquidity that led to the breakdown of the global economy at three-year intervals for a recurring sequence of years.

A. Table I — Comparative Architecture Performance

TABLE I

Comparative Architecture Performance — AEPI vs. Baseline Systems

Metric	Traditional SWIFT (System A)	Semi-Autonomous (System B)	AEPI Baseline (System C)	AEPI + DEX Opt. (System D)
Avg. Latency (min)	4,320	960	180	42
Latency Reduction vs A	—	−77.8%	−95.8%	−99.0%
SRI @ $\tau=0.5$	0.52	0.68	0.89	0.95
Threat Detection F1	0.612	0.858	0.963	0.971
Compute Utilization (%)	42%	55%	78%	84%
Human Intervention (%)	88%	61%	12%	6%
Op. Cost (Norm. Unit @50% throughput)	50.0	38.0	21.0	14.5
Storage Efficiency (%)	35%	52%	84%	91%
Efficiency Gain E_{total}	18.3%	42.1%	76.4%	99.2%

Note: System D (AEPI + DEX Optimized) consistently yields the best results across all metrics. Values for Systems A–C are baseline benchmarks. Shaded column (System D) represents the proposed optimized configuration.

B. Table II — Error and Latency Metrics by Threat Category

TABLE II
Error Rate and Latency Impact by Threat Category

Threat Category	Detection Rate (%)	False Positive Rate (%)	Avg. Response Latency (ms)	System Degradation (%)	AEPI Mitigation Gain (%)
Theft / Fraud	97.2	1.8	220	3.1	+58.4%
Manipulation / Spoofing	94.8	3.2	310	5.6	+49.1%
Service Disruption	99.1	0.9	95	1.2	+72.3%
Geopolitical Misuse	88.4	6.7	840	11.4	+34.7%
Cyberwar / APT	91.6	5.1	620	8.3	+44.9%
Weighted Average	94.2	3.5	417	5.9	+51.9%

Note: AEPI Mitigation Gain (%) reflects improvement in detection rate relative to traditional infrastructure per threat class. Response latency is measured from threat-event onset to automated mitigation action.

6. Conclusion

The predicted profound impacts of the COVID-19 pandemic on the global economy have brought increased attention to both the security and resilience of international value exchange. The global economy has become increasingly interconnected, harnessing new technologies to enable greater specialization and lower costs. Yet it has relied primarily on one major currency that is subject to unpredictable and/or nonlinear supply shocks, and on a small number of private payment networks. The current crisis has demonstrated the fragility of interconnected critical infrastructure and revealed how even minor disruptions in one part of the system can impact the entire network. Geopolitical turmoil, digital development, increased cybercrime, and natural disasters compound the threats to international value exchange.

The recent and increasing politicization of international value exchange, coupled with the emergence of new economic powers, has simultaneously raised geopolitical tensions and motivated states to investigate the development of alternative bilateral and multilateral payment alternatives. Yet there has been little investigation of longer-term measures to prevent these crises



from occurring in the first place. Autonomously operated economic systems enable an alternative approach to security and resilience characterized by the provision of competition and choice to human actors. Autonomous economic processing infrastructure for international value exchange that is fully interoperable with the existing financial and technical ecosystems represents an important step toward more resilient and secure international value exchange.

References

1. Priya, N., & Ahmed, J. (2021). A survey on digital payments security: Recent trends and future opportunities. *International Journal of Computer Trends and Technology*, 69(8), 26–34.
2. Ng, D., Kauffman, R. J., Griffin, P., & Hedman, J. (2021). Can we classify cashless payment solution implementations at the country level? *Electronic Commerce Research and Applications*, 46, 101018.
3. Tang, Y. M., Chau, K. Y., Hong, L., Ip, Y. K., & Yan, W. (2021). Financial innovation in digital payment with WeChat towards electronic business success. *Journal of Theoretical and Applied Electronic Commerce Research*, 16(5), 1844–1861.
4. Venkateswara Rao Movva. (2024). AI-Augmented DevOps for Large-Scale Retail Platforms: A Framework for Intelligent CI/CD, Automated Testing, and Deployment Optimization. *Journal of Computational Analysis and Applications (JoCAAA)*, 33(08), 7759–7765. Retrieved from <https://eudoxuspress.com/index.php/pub/article/view/5827>
5. Jain, P., Varanasi, R. A., & Dell, N. (2021). “Who is protecting us? No one!” Vulnerabilities experienced by low-income Indian merchants using digital payments. In *Proceedings of the ACM SIGCAS Conference on Computing and Sustainable Societies*, 1–14.
6. Khan, A., & Malaika, M. (2021). Central bank risk management, fintech, and cybersecurity. *IMF Working Papers*, 2021(105).
7. Pranitha Potturi. (2024). AI-Augmented Analytics Architecture for Intelligent Enterprise Reporting and Predictive Business Decision-Making . *Journal of Computational Analysis and Applications (JoCAAA)*, 33(05), 3830–3841. Retrieved from <https://eudoxuspress.com/index.php/pub/article/view/5797>
8. Khiaonarong, T., Leinonen, H., & Rizaldy, R. (2021). Operational resilience in digital payments: Experiences and issues. *IMF Working Papers*, 2021(288).
9. Baesens, B., Höppner, S., & Verdonck, T. (2021). Data engineering for fraud detection. *Decision Support Systems*, 150, 113492.
10. Hsin, Y. Y., Dai, T. S., Ti, Y. W., & Huang, M. C. (2021). Interpretable electronic transfer fraud detection with expert feature constructions. *CEUR Workshop Proceedings*, 3052.
11. Sasidhar Reddy Mondeddula. (2024). Large Language Model-Based Financial Intelligence for Automated Compliance, Risk Analysis, and Regulatory Reporting. *Journal of Computational Analysis and Applications (JoCAAA)*, 33(06), 4222–4227. Retrieved from <https://eudoxuspress.com/index.php/pub/article/view/5813>
12. Chang, V., Doan, L. M. T., Di Stefano, A., Sun, Z., & Fortino, G. (2022). Digital payment fraud detection methods in digital ages and Industry 4.0. *Computers & Electrical Engineering*, 100, 107734.
13. Festa, Y. Y., & Vorobyev, I. A. (2022). A hybrid machine learning framework for e-commerce fraud detection. *Journal of Management Analytics*, 17(1).

14. Reddy, V. A. R. (2024). Generative Intelligence for Healthcare Claims Processing and Personalized Benefits Management. *International Journal of Advanced Engineering Science and Information Technology (IJAESIT)*, 7(3), 14099.
15. Moon, I. T., Shamsuzzaman, M., Mridha, M. M. R., & Rahaman, A. S. M. M. (2022). Towards the advancement of cashless transaction: A security analysis of electronic payment systems. *Journal of Computer and Communications*, 10(7).
16. Sahi, A. M., Khalid, H., Abbas, A. F., Zedan, K., Khatib, S. F. A., & Al Amosh, H. (2022). The research trend of security and privacy in digital payment. *Informatics*, 9(2), 32.
17. Seldal, M. M. N., & Nyhus, E. K. (2022). Financial vulnerability, financial literacy, and the use of digital payment technologies. *Journal of Consumer Policy*, 45, 281–306.
18. Xia, H., Wang, Y., Gauthier, J., & Zhang, J. Z. (2022). Knowledge graph of mobile payment platforms based on deep learning: Risk analysis and policy implications. *Expert Systems with Applications*, 208, 118143.
19. Loganathan, R., & Kolla, S. H. (2024). Harnessing generative AI for adaptive risk policy generation in multi-regulatory data center environments. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, 15(3), 505-515.
20. Höppner, S., Baesens, B., Verbeke, W., & Verdonck, T. (2022). Instance-dependent cost-sensitive learning for detecting transfer fraud. *European Journal of Operational Research*, 297(1), 291–300.
21. Ti, Y. W., Hsin, Y. Y., Dai, T. S., Huang, M. C., & Liu, L. C. (2022). Feature generation and contribution comparison for electronic fraud detection. *Scientific Reports*, 12, 18042.
22. Mattaparthi, R. (2024). Transformer-Based Fault Diagnosis for Large-Scale Standby Power Generators: Partial Discharge Pattern Recognition at Hyperscale Data Center Installations. *Journal of Computational Analysis and Applications (JoCAAA)*, 33(08), 8781-8799.
23. Ouazzane, K., Polykarpou, T., Patel, Y., & Li, J. (2022). An integrated machine learning framework for fraud detection: A comparative and comprehensive approach. *International Journal of Information Security and Privacy*, 16(1), 1–17.
24. Vorobyev, I. A., & Krivitskaya, A. (2022). Reducing false positives in bank anti-fraud systems based on rule induction in distributed tree-based models. *Computers & Security*, 120, 102786.
25. Cherif, A., Badhib, A., Ammar, H., Alshehri, S., Kalkatawi, M., & Imine, A. (2023). Credit card fraud detection in the era of disruptive technologies: A systematic review. *Journal of King Saud University—Computer and Information Sciences*, 35, 145–174.
26. Rajesh Reddy Ellenki. (2024). Deep Learning-Based Demand Intelligence for Dynamic Merchandise Planning and Allocation. *Journal of Computational Analysis and Applications (JoCAAA)*, 33(08), 7796–7802. Retrieved from <https://eudoxuspress.com/index.php/pub/article/view/5832>
27. Vanini, P., Rossi, S., Zvizdic, E., & Domenig, T. (2023). Online payment fraud: From anomaly detection to risk management. *Financial Innovation*, 9, 66.
28. Tian, S., Zhao, B., & Olivares, R. O. (2023). Cybersecurity risks and central banks' sentiment on central bank digital currency: Evidence from global cyberattacks. *Finance Research Letters*, 53, 103609.
29. Kuehnlenz, S., Orsi, B., & Kaltenbrunner, A. (2023). Central bank digital currencies and the international payment system: The demise of the US dollar? *Research in International Business and Finance*, 64, 101834.
30. Kolla, S. H., & Peddi, R. K. (2024). Designing Governance-Aligned GenAI Pipelines Using Small Language Models for Enterprise Workflow Intelligence. *International Journal of Science, Research*



- and Technology, 7(6), 13256-13268.
31. Goodell, G., Toliver, D. R., & Al-Nakib, H. D. (2023). A scalable architecture for electronic payments. In S. Matsuo et al. (Eds.), *Financial cryptography and data security: FC 2022 international workshops* (pp. 645–678). Springer.
 32. Lokanan, M. E. (2023). Predicting mobile money transaction fraud using machine learning algorithms. *Applied AI Letters*, 4(2), e85.
 33. Adrian, T., & Mancini-Griffoli, T. (2023). The rise of payment and contracting platforms. *IMF FinTech Notes*, 2023(005).
 34. Aljaradat, A., Sarkar, G., & Shukla, S. K. (2024). Modelling cybersecurity impacts on digital payment adoption: A game theoretic approach. *Journal of Economic Criminology*, 5, 100089.
 35. Javaheri, D., Fahmideh, M., Chizari, H., Lalbakhsh, P., & Hur, J. (2024). Cybersecurity threats in FinTech: A systematic review. *Expert Systems with Applications*, 241, 122697.
 36. Wang, S., Asif, M., Shahzad, M. F., & Ashfaq, M. (2024). Data privacy and cybersecurity challenges in the digital transformation of the banking sector. *Computers & Security*, 147, 104051.
 37. Huang, S. Y., Wang, T., Huang, Y. T., & Yeh, T. N. (2024). Information security risk items and management practices for mobile payment using non-financial-institution service providers: An exploratory study. *International Journal of Accounting Information Systems*, 53, 100684.
 38. Wen, W., & Han, X. (2024). An introduction of transaction session-induced security scheme using blockchain technology: Understanding the features of Internet of Things-based financial security systems. *Managerial and Decision Economics*, 45(4), 1817–1834.
 39. Penaka, B. (2024). Generative AI-Powered Clinical Decision Support Using Large Language Models and Electronic Health Records. *Journal of Neonatal Surgery*, 13(1), 2588–2596. Retrieved from <https://jneonatalsurg.com/index.php/jns/article/view/10577>
 40. Radanliev, P. (2024). Digital security by design. *Security Journal*, 37, 1640–1679.
 41. Aurazo, J., & Gasmi, F. (2024). Digital payment systems in emerging economies: Lessons from Kenya, India, Brazil, and Peru. *Information Economics and Policy*, 69, 101113.
 42. Robinson, G., Dörry, S., & Derudder, B. (2024). Preserving the obligatory passage point: SWIFT and the partial platformisation of global payments. *Geoforum*, 151, 104007.
 43. Bharath, A., Paduraru, A., & Gaidosch, T. (2024). Cyber resilience of the central bank digital currency ecosystem. *IMF FinTech Notes*, 2024(003).
 44. Reslow, A., Soderberg, G., & Tsuda, N. (2024). Cross-border payments with retail central bank digital currencies: Design and policy considerations. *IMF FinTech Notes*, 2024(002).