ISSN: 2096-3246
Volume 58, Issue 03, 2026

BRIDGING TRADFI AND DEFI: EVENT-DRIVEN INTEROPERABILITY PROTOCOLS FOR REAL-TIME FIAT-TO-CRYPTO SETTLEMENTS

Abhinav Reddy Jutur
The State University of New York at New Paltz, USA

Abstract

The division between traditional finance (TradFi) and decentralized finance (DeFi) continues to hinder seamless capital mobility across ecosystems. Real-Time Payment Systems (RTPS) achieve near-instant fiat settlements, yet bridging these assets into blockchain environments remains dependent on fragmented, high-latency, and centralized gateways. This gap limits the natural strengths of both worlds, especially speed and efficiency. Based on the publish/subscribe model, the EDSP protocol operates as a decentralized oracle system that allows for synchronization of state updates between two separate ledgers. This protocol will allow smart contracts to initiate fiat payments and bank payment systems to trigger corresponding blockchain settlement actions. The model stresses cryptographic protections against oracle tampering through multi-party authentication and zero-trust routing methodologies. A simulation of latency shows that an event-driven architecture is capable of resolving the deterministic nature of TradFi operations and the probabilistic aspect of blockchain networks. Incorporating compliance events into the settlement process enables institutions to meet their demands for regulatory and transparency obligations. This article sets a roadmap for future liquidity bridging models based on a secure, scalable, and compliant approach to bridging ecosystems. This article proves the value that event-driven models bring to the table in terms of interconnectivity and liquidity, which will allow institutional-level interactions to take place within fiat and decentralized networks.

Keywords: Decentralized Finance (DeFi), Real-Time Payment Systems (RTPS), Event-Driven Architecture (EDA), Blockchain Interoperability, Cross-Chain Oracles, Fiat-to-Crypto Bridges.

1. Introduction

1.1 The Bifurcated Financial Landscape

The global financial ecosystem is undergoing a structural transformation characterized by the coexistence of sovereign real-time payment infrastructures and decentralized blockchain networks. Real-Time Payment Systems (RTPS) such as India's Unified Payments Interface (UPI) and the United States Federal Reserve's FedNow services have demonstrated unprecedented throughput, processing billions of fiat transactions with sub-second latency [6]. They are an example of deterministic finance, in which all transactions are processed instantaneously via banking ledger records. Decentralized finance creates automated platforms for lending, trading, and settlement without any intermediary in the process, thus redefining the concept of financial intermediation [11].

1.2 The Friction in Capital Mobility

While RTPS and DeFi technologies have reached a significant level of maturity, the integration between them continues to be limited by centralized and fragmented gateways. The fiat-to-crypto exchange, which is commonly termed "on/off ramping," occurs via exchange platforms or custodial entities. Such approaches result in delays, counterparty risk, and inefficiencies during the settlement process. The use of centralization in intermediation poses questions of resilience and trust. The exchange APIs, which are popular bridging solutions, follow a request/response model that is vulnerable to single-point failures. Stablecoins, while widely adopted, require collateral backingand they do not resolve the real-time synchronization of fiat settlements with blockchain transactions.

1.3 Purpose of the Study

The hypothesis guiding this article is that the interoperability gap can be addressed not by constructing new blockchains but by implementing event-driven architectures as real-time communication bridges. By treating both fiat settlements and smart contract executions as continuous event streams, it becomes possible to design a protocol that synchronizes state across independent ledgers. This approach leverages the strengths of publish-subscribe messaging systems, and applies them to financial interoperability [16]. The Event-Driven Settlement Protocol (EDSP) proposed here functions as a high-speed middleware layer that connects RTPS infrastructures with blockchain

networks. It works as a decentralized oracle system that ensures secure transmission of events from fiat to cryptocurrency domains and vice versa.

Table 1: TradFi vs DeFi Architectural and Operational Characteristics [6, 11, 13]

Dimension	**Traditional Finance (TradFi)**	**Decentralized Finance (DeFi)**	**Key Implication for EDSP**
Execution Model	Deterministic ledger-based processing with immediate finality	Probabilistic consensus with block confirmations	Requires synchronization layer to reconcile finality mismatch
Infrastructure	Centralized banking systems (RTPS, FedNow, UPI)	Distributed blockchain networks (Ethereum, Layer 2 chains)	EDSP must bridge centralized and decentralized infrastructures
Transaction Speed	Sub-second settlement in RTPS environments	Variable latency depending on block time and congestion	Event streaming needed for real-time alignment
Trust Model	Institutional trust (banks, regulators)	Trustless cryptographic validation	EDSP introduces hybrid trust via MPC and zero-trust routing
Programmability	Limited (rule-based financial systems)	High (smart contracts, composability)	EDSP enables programmable fiat-triggered execution
Failure Model	Centralized failure risk (bank outages)	Network-wide probabilistic failure	EDSP distributes risk across event brokers

2. Literature Review & The Interoperability Gap

2.1 The Deterministic vs. Probabilistic Divide

Connecting TradFi and DeFi involves a computer science problem of state synchronizations between two different systems. Deterministic TradFi systems such as SQL-backed bank ledger systems commit transactions immediately, ensuring determinism in that a transaction is completed or rolled back instantaneously. On the other hand, blockchains such as Ethereum use probabilistic consensus wherein the transaction is made more certain by each block confirmation. This presents a discrepancy in the way settlements work. Academic literature suggests that the only way to solve this problem is by using decentralized middleware rather than gateway connections, which are deterministic systems [1]. There are papers that mention how probabilistic consensus mechanisms lead to latency issues [2]. It becomes clear from the literature that this gap lies at the heart of the interoperability problem.

2.2 Current Bridging Solutions and Limitations

Currently existing methods include stablecoins and centralized exchange APIs. However, while stablecoins, such as USDC and USDT, serve as a way of representing fiat on-chain, they still need pre-funding and collateralization. These solutions do not offer a method of solving the problem of the instant settlement of fiat in the banking layer. Existing research shows that stablecoins prove to be effective in terms of liquidity, but they cannot ensure deterministic settlement [4]. As for Web2 solutions like REST APIs, they utilize request-response architectures, which can suffer from single points of failures, polling intervals, and security breaches. The research has confirmed that dependence on centralized intermediaries are a serious issue that increases systemic risks in cases where exchanges control the conversion of fiat to crypto [5]. Other research points out that a centralized API is neither resilient nor transparent enough to be considered for institutional adoption [7]. Trust across chains has also been studied, showing that centralized bridge solutions lead to custodial risks and hence reduce decentralization [8]. Overall, these studies illustrate how fragmented and unreliable existing bridge solutions are.

ISSN: 2096-3246
Volume 58, Issue 03, 2026

Table 2: Limitations of Existing Fiat–Crypto Bridging Mechanisms [4, 5, 5,7, 8]

Bridging Method	**Mechanism**	**Strengths**	**Limitations**	**Impact on Interoperability**
Centralized Exchanges	Custodial fiat-to-crypto conversion	High liquidity, fast onboarding	Single point of failure, custodial risk	Weakens decentralization and trust neutrality
Stablecoins	Fiat-backed token issuance	On-chain liquidity representation	Requires collateralization and pre-funding	Breaks live fiat synchronization
API Gateways	Request–response banking integration	Easy integration with legacy systems	Latency, downtime, synchronous coupling	Not suitable for real-time event flows
Cross-Chain Bridges	Locked asset transfer mechanisms	Multi-chain asset movement	Vulnerable to exploits and bridge hacks	Security bottleneck in interoperability
Trusted Hardware Bridges	Hardware-based validation (TEE/MPC)	Improved security assurance	Complex deployment and scalability limits	Partial solution, not fully decentralized

2.3 The "Reverse Oracle" Problem

In DeFi, oracles such as Chainlink feed off-chain data (e.g., asset prices) into on-chain smart contracts. However, executing fiat payments based on smart contract triggers requires a “reverse oracle”-a system that securely transmits on-chain state changes. Research has highlighted that cross-domain integration requires asynchronous, high-throughput message routing, which traditional APIs cannot provide [3]. Recent work proposes blockchain-IoT smart contract frameworks that demonstrate how event-driven architectures can manage product lifecycle data securely and efficiently [14]. Tools like Apache Kafka and Pulsar have features that make them particularly useful for these purposes, providing asynchronous, high-throughput messaging that can allow for reverse oracle operation.

3. The Event-Driven Bridge Architecture

3.1 The Event-Driven Settlement Protocol (EDSP)

The interoperability gap between TradFi and DeFi requires a middleware solution that can synchronize deterministic fiat systems with probabilistic blockchain networks. The Event-Driven Settlement Protocol (EDSP) is proposed as such a solution. The EDSP acts as an integrated communication layerthat lies between the API gateway and RPC nodes in a banking consortium’s ecosystem. The EDSP works using the publish and subscribe method to ensure that both fiat and blockchain events are properly recorded, arranged, and sent through safely. Previous research has stressed the significance of an event-driven architecture in fintech applications, especially for high throughput and low latency settlement [15]. With this approach adopted, the EDSP is able to convert interoperability from a request-response model into an event stream process, thus eliminating the delay and SPOF issues associated with the previous method [6]. This approach solves the problem described in Section 2.

3.2 Core Components of the EDSP

There are four main sections of the EDSP, which work towards creating resilience, security, and adherence to standards.

Webhook for Fiat Event Producer: This consists of webhooks that are connected to the main banking system. With the conclusion of the settlement of the fiat transaction taking place, the triggering of a webhook with events such as FIAT_DEPOSIT_RECEIVED would happen, which

would then be sent to the event broker. The fiat transaction is communicated immediate to the event-processing layer [11].

Smart Contract Event Listeners: Lightweight indexers monitor mempools of the blockchain and newly mined blocks in order to identify any particular contract execution events. For instance, a TOKEN_BURNED event can be picked up and relayed through the event stream manager, enabling near low-latency synchronization between the two systems [13].

Cluster of Event Data Service Brokers: The EDSP uses a clustered architecture using either Kafka or Pulsar. The research shows that treaming backbone ensures ordering of any event-driven system due to its critical importance in providing reliable throughput [15]. Such services, the EDSP ensures that there are no duplicate or missed events in cross-system communications [6]. Settlement Engine Microservice: The settlement engine microservice receives data about events from the broker, verifies the cryptographic proofs of those events, and triggers the action on the opposite side of the communication bridge. When receiving information about the fiat deposit event, the engine creates a cryptographic proof of receipt and executes a smart contract transaction [12].

Table 3: Event-Driven Settlement Protocol (EDSP) Architecture Components [6, 11, 12, 13, 15]

Component	**Function**	**Data Flow Role**	**Security Mechanism**	**System Benefit**
Fiat Event Producer	Captures RTPS banking events (e.g., PAYMENT_CONFIRMED)	Source layer (TradFi → EDSP)	Signed webhook authentication	Enables real-time fiat event capture
Blockchain Event Listener	Monitors smart contract state changes	Source layer (DeFi → EDSP)	Block verification + indexing	Ensures blockchain state observability
Event Broker Cluster (Kafka/Pulsar)	Streams and orders financial events	Middleware routing layer	Replication + fault tolerance	High throughput, scalable messaging
Settlement Engine	Executes cross-domain settlement logic	Execution layer	MPC + cryptographic proof validation	Ensures trusted transaction finality
Compliance Microservices	AML/KYC enforcement in real time	Regulatory layer	Identity binding + rule validation	Enables institutional-grade compliance
Oracle Verification Module	Validates cross-domain events	Trust layer	Zero-trust + signature verification	Prevents event manipulation

3.3 Workflow Example: Instant Fiat-to-Crypto

The end-user begins the exchange by transferring funds either via UPI or FedNow services into an escrow account. The bank's system triggers the occurrence of an event named Payment_Cleared and propagates to the EDSP broker. The Settlement Engine consumes this event, computes a cryptographic proof confirming fiat receipt, and creates a transaction on the blockchain. A transaction is then submitted to the smart contract responsible for minting the crypto asset and delivering it to the end-user's non-custodial wallet. This entire process happens within seconds, showing how event-driven architecture can bridge the determinism of fiat transactions and the probabilistic consensus of blockchain transactions [15].

3.4 Solving the Interoperability Problem

The EDSP addresses the problems outlined in Section 2By incorporating compliance activities within the settlement process, the protocol ensures that AML and KYC regulations are instantly fulfilled[6]. Distributed broker clusters help eliminat it circumvents the problem of a single point of failure, which

is caused by centralized APIs [7]. ryptographically proven computation and multi-party computation, it circumvents the problem of oracles [12]. Importantly, the EDSP solves the problem of reverse oracle manipulation through the secure transmission of state changes back into the banking system of TradFi. This is key to enabling smart contracts to initiate fiat currency transactions [3][14], thus bridging the gap between the worlds of TradFi and DeFi.

4. Securing the Cross-Chain Oracle

4.1 The Threat Vector: Flash Loans and Data Manipulation

If the event broker is hacked, it can issue fake events like FIAT_DEPOSIT_RECEIVED to mint tokens without backing it up. Attacks on flash loans have shown the effects of manipulating on-chain data by flooding them with liquidity [2]. Studies have also highlighted how cross-domain integrations pose manipulation risks unless they have proper verification mechanisms [3].

4.2 Multi-Party Computation (MPC) and Consensus

A multi-party computation (MPC) network is proposed, where multiple independent nodes operated by different financial institutions verify the fiat ledger and participate in a threshold signature scheme. A blockchain transaction is only triggered if a supermajority of nodes signs the event. In this architecture, trust is distributed and single points of failure. Research works in trust frameworks suggest that MPC increases resilience by mandating consensus among various parties involved [8]. Security literature indicates that threshold signatures like ECDSA or EdDSA ensure absolute cryptographic protection [12]. By embedding MPC into the EDSP, institutional adoption becomes feasible, as no single entity can manipulate settlement outcomes [6].

4.3 Zero-Trust Event Routing

Zero-trust principles are applied across the EDSP to ensure mutual authentication between microservices via mTLS. The event payload itself is cryptographically hashed and signed at the origin, preventing forgery even if an attacker compromises the broker cluster. IoT–DeFi convergence has demonstrated that zero-trust routing is essential when bridging heterogeneous systems [9]. Through cryptographic provenance enforcement, the EDSP guarantees that even lateral movement attacks will not affect the integrity of the banking transaction. This system conforms to current zero-trust architectures that focus on continual validation rather than protection of the perimeter [14].

4.4 Mitigating Blockchain Reorganizations

Blockchain transactions have probabilistic finality and may be reverted during reorganizations or orphan blocks For this reason, the EDSP utilizes the "confirmation buffer." Payments via fiat currency are made only after a certain dynamic number of block confirmations have occurred, preventing premature settlement execution. Through the use of adaptive confirmation requirements, the EDSP ensures that transactions are executed after consensus stabilizes [2].

Table 4: Security, Performance, and Scalability Properties of EDSP [2, 3, 6, 9, 15, 16]

Category	Challenge	EDSP Mechanism	Outcome
Oracle Security	Fake event injection or manipulation	Cryptographic event signing + verification	Prevents unauthorized settlement triggers
Flash Loan Attacks	Market manipulation via liquidity exploits	MPC-based multi-node validation	Reduces single-node exploitation risk
Blockchain Reorganization	Transaction rollback risk	Adaptive confirmation buffer	Ensures settlement finality before fiat execution
System Latency	Delays in cross-system communication	Event-driven publish–subscribe streaming	Millisecond-level event propagation
Throughput Bottleneck	Blockchain TPS limitations	Event batching + Merkle root aggregation	Improves scalability under load
Trust Centralization	Reliance on intermediaries	Zero-trust routing architecture	Eliminates centralized dependency
Data Consistency	Cross-ledger state mismatch	Event synchronization pipeline	Ensures real-time state alignment

5. Latency, Throughput, and Performance Analysis

5.1 Benchmarking the EDA Middleware

The geo-replication capabilities of Apache Pulsar, were chosen and the internal latency of event processing in our test case was 5.2 milliseconds for 2KB payloads. Event-driven middleware approach is near-instant processing latency and broker applications like Pulsar and Kafka can ensure high throughput during periods of stress [15].

5.2 The TradFi vs. DeFi Throughput Bottleneck

The real limiting factor in the EDSP framework is not the middleware but the destination ledgers. While TradFi RTPS solutions can process several thousand transactions per second, Ethereum Layer 1 can only handle approximately 15 transactions per second. In research articles published in Electronic Markets, it has been highlighted that one of the key issues in establishing interoperability between TradFi and DeFi frameworks is their difference in terms of transactional capacity [7]. In studies related to sustainability, it has also been stated that the inefficiencies in the transaction speed of blockchains increase the cost of energy consumption and scalability [5].

5.3 Load Leveling via Event Queues

To reconcile throughput disparities, the EDSP employs persistent message queues. When bridging from high-throughput RTPS to low-throughput blockchains, the middleware batches incoming fiat events and submits them as cryptographic Merkle roots. It also helps to lower the transaction costs and minimize congestion in the network. Looking ahead transform mismatched throughputs into streamlined processes for liquidity bridges [16].

6. Regulatory Implications & Conclusion

6.1 Programmable Compliance and AML/KYC

The Event-Driven Settlement Protocol (EDSP) introduces a compliance-aware architecture by embedding “Compliance Events” directly into the settlement stream. Before any cross-chain transfer is executed, the payload is routed through real-time Anti-Money Laundering (AML) and sanctions screening microservices. The EDSP has direct integration with the fiat banking network, which implies that KYC is automatically associated with block addresses, thus ensuring traceability of operations. The design aligns with international standard such as the FATF Travel Rule, where identity data must be included with each transfer of digital assets [6].

6.2 Summary of Contributions

Through its design, the EDSP reveals that the future of finance will not be an all-or-nothing scenario, with TradFi and DeFi being two separate and opposing ecosystems. By making use of event-driven approaches, interoperable protocols will be able to carry out fiat-to-crypto transactions securely and effectively. The reverse oracle problem is also taken care of, and it is now possible to trigger fiat transactions via on-chain events. Security is guaranteed through MPC and threshold signature schemes, whereas the use of zero-trust routing ensures the integrity of events. This combination forms a completely transparent and auditable liquidity bridge that meets the needs of institutional risk management [9]. Additionally, EDSP also helps in addressing issues related to blockchain interoperability, as it shows that middleware can be used for aligning deterministic TradFi with probabilistic blockchain consensus [16].

6.3 Future Outlook

As CBDCs move from pilots to production, the demand for security and interoperability will become more important. CBDCs need to have a bridge that can efficiently link the sovereign payment system to the decentralized world without slowing down and complying with the regulation. The EDSP approach fits very well in such an application because of its event-driven architecture that enables us to embed programmable compliance features into the transaction flow. It is important to mention that embedding quantum-resistant cryptography algorithms into MPC nodes will be critical in order to protect against post-quantum attacks. EDSP resiliency under cryptographic attacks in the future [6]. Furthermore, since the number of studies related to blockchain technology has been continuously increasing in recent years, the structural topic modeling reveals two priorities for the coming agenda on blockchain technology: interoperability and compliance [16].

Conclusion

Interoperability is essential in integrating traditional finance with DeFi in a safe, regulation-compliant, and resilient manner. According to the EDSP model, it is possible to connect fiat money and

blockchain technology using an event-driven architecture without losing any speed or trust. Compliance events have been integrated into the settlement chain to ensure regulatory requirements, such as KYC and sanctions screening, are met at all times. In addition, the EDSP framework showcases the possibilities of allowing institutional participation due to the resolution of oracle problems, multiple verifications of the process, and the use of zero-trust routing protocols. This approach can become the basis for building a transparent and auditable liquidity channel connecting decentralized markets with regulators. The emergence of central bank digital currencies (CBDCs) in the future requires robust interoperability solutions. The combination of quantum-proof cryptography and multi-party computations will be key in defending against any threat. Thus, EDSP is not only a practical solution to interoperability problems but also a roadmap for the future of finance.

References

1. Seth Djanie Kotey et al., "A Framework for Full Decentralization in Blockchain Interoperability," Sensors, vol. 24, no. 23, p. 7630, Nov. 2024. https://www.mdpi.com/1424-8220/24/23/7630?utm_source=chatgpt.com
2. Kuo-Hui Yeh et al. "A Secure Interoperability Management Scheme for Cross-Blockchain Transactions," Symmetry, vol. 14, no. 12, p. 2473, Nov. 2022. https://www.mdpi.com/2073-8994/14/12/2473
3. Rosario Gennaro et al., “Secure distributed key generation for discrete-log based cryptosystems,” Journal of Cryptology, vol. 20, pp. 51–83, 2007.
4. https://link.springer.com/article/10.1007/s00145-006-0347-3
5. Lili Cheng et al., "Secure Cross-Chain Interaction Solution in Multi-Blockchain Environment," Heliyon, vol. 10, no. 7, p. e28861, Apr. 2024. https://www.sciencedirect.com/science/article/pii/S2405844024048928
6. Debasis Mohanty et al., "Blockchain Interoperability: Towards a Sustainable Payment System," Sustainability, vol. 14, no. 2, p. 913, Jan. 2022. https://www.mdpi.com/2071-1050/14/2/913?utm_source=chatgpt.com
7. Hanfang Chen et al., "The Role of Blockchain in Finance Beyond Cryptocurrency: Trust, Data Management, and Automation," IEEE Access, vol. 12, pp. 54321–54335, May 2024. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10516318
8. Senate Sylvia Mafike and Tendani Mawela, "An Enterprise Framework for Blockchain Interoperability," Electronic Markets, vol. 36, article no. 14, Jan. 2026. https://link.springer.com/article/10.1007/s12525-025-00869-6?utm_source=chatgpt.com
9. Ying Lan et al., "TrustCross: Enabling Confidential Interoperability across Blockchains Using Trusted Hardware," in Proceedings of the 2021 4th International Conference on Blockchain Technology and Applications (ICBTA ’21), pp. 17–23, Feb. 2022. https://dl.acm.org/doi/10.1145/3510487.3510491
10. Prasannakumaran Sarasijanayanan et al., "On the Convergence of Internet of Things and Decentralized Finance: Security Challenges and Future Directions," Sensors, vol. 26, no. 6, p. 1740, Mar. 2026. https://www.mdpi.com/1424-8220/26/6/1740?utm_source=chatgpt.com
11. [Sławomir Bielecki et al., "Electricity Usage Settlement System Based on a Cryptocurrency Instrument," Energies, vol. 15, no. 19, p. 7003, Sep. 2022. https://www.mdpi.com/1996-1073/15/19/7003
12. [Nasser Arshadi and Timothy Dombrowski, "Applications and Management of Blockchain Technologies in Financial Services," Journal of Risk and Financial Management, vol. 19, no. 3, p. 224, Mar. 2026. https://www.mdpi.com/1911-8074/19/3/224
13. [Abhinav Reddy Jutur, "Next-Generation Security Paradigms for Real-Time Financial Applications," International Journal of Research in Computer Applications and Information Technology (IJRCAIT), vol. 8, no. 1, pp. 3468–3479, Jan.–Feb. 2025. https://iaeme.com/MasterAdmin/Journal_uploads/IJRCAIT/VOLUME_8_ISSUE_1/IJRCAIT_08_01_249.pdf
14. [Rainer Böhme al., "Bitcoin: Economics, Technology, and Governance," Journal of Economic Perspectives, vol. 29, no. 2, pp. 213–238, Spring 2015. https://cooperative-individualism.org/bohme-rainer-etal_bitcoin-economics-technology-and-governance-2015-spring.pdf

15. [Divya Upadhyay et al., "Blockchain and IoT-Based Smart Contract Framework for Efficient and Secure Product Life Management," Discover Internet of Things, vol. 6, article no. 25, Feb. 2026. https://link.springer.com/article/10.1007/s43926-025-00274-7
16. [Abhinav Reddy Jutur, "Revolutionizing FinTech with Event-Driven Architectures," International Journal of Scientific Research in Computer Science Engineering and Information Technology, vol. 11, no. 1, pp. 3051–3062, Feb. 2025. https://www.researchgate.net/publication/389299816
17. [Pradip Kumar Sharma et al., "A software defined fog node based distributed blockchain cloud architecture for IoT," IEEE Access, Special Section on Intelligent Systems for the Internet of Things, Feb. 1, 2018.https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8053750