Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Zero-Knowledge Enabled Cross-Border Payment Systems: Advancing Privacy and Compliance in Blockchain Architectures

Jothimani kanthan Ganapathi
Independent Researcher

ARTICLE INFO

Received: 20 July 2025

Revised: 07 Aug 2025

Accepted: 21 Aug 2025

ABSTRACT

This article proposes a novel blockchain-based architecture for cross-border payments that integrates self-sovereign identity (SSI) and zero-knowledge proofs (ZKPs) to address the fundamental challenges of traditional systems. The proposed framework enables near-instant settlement while preserving privacy and ensuring regulatory compliance by design. By layering an identity infrastructure with ZKP-gated smart-contract escrows and regulatory oracles, the system allows participants to prove compliance with jurisdiction-specific requirements without revealing sensitive personal data. The architecture comprises three interconnected layers — identity, value, and compliance — that work together to streamline remittances, business transactions, and international payroll processes. Comparative analysis demonstrates significant advantages over both correspondent banking and current blockchain networks in terms of settlement speed, transaction costs, fraud prevention, and automated compliance. While the approach faces challenges, including network adoption barriers, technical scalability, and governance complexity, this study outlines promising directions for future development, particularly in the context of emerging central bank digital currencies (CBDCs) and regulated stablecoins.

Keywords: Zero-knowledge proofs, Cross-border payments, Self-sovereign identity, Blockchain, Regulatory compliance

1. Introduction

Cross-border payment systems form the backbone of global commerce, yet they remain plagued by significant inefficiencies that create substantial barriers for individuals and businesses alike. The current infrastructure, dominated by **correspondent banking networks** and the **SWIFT messaging system**, imposes burdensome costs and delays that hinder international trade and financial inclusion [1].

International wire transfers typically incur fees ranging from **6% to 8%** of the transaction value, creating a prohibitive cost structure for small-value remittances and business payments. Settlement times often extend from **two to five business days** in optimal scenarios, with transactions crossing multiple time zones or involving less common currency pairs taking even longer to process. Such delays create significant cash flow challenges, especially for small and medium-sized enterprises operating with limited working capital [1]. The opacity of these transactions further complicates matters, as participants can only view their respective ends of the payment journey, making error resolution and fraud detection particularly challenging.

The correspondent banking model, which underpins most international transfers, requires multiple intermediaries — each maintaining **nostro–vostro account** relationships — that add complexity, cost, and latency to every transaction. Each intermediary bank charges fees for its services, and the foreign exchange conversion spread typically adds another layer of cost. As the BIS notes, *"The longer*

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

the payment chain, the higher the cost and the longer it takes for the recipient to receive the funds" [2].

Regulatory compliance adds another dimension of complexity. Financial institutions must conduct real-time screening against sanctions lists and perform **Know Your Customer (KYC)** and **Anti–Money Laundering (AML)** checks that vary across jurisdictions. The largely manual nature of these processes contributes significantly to delays, with compliance operations accounting for roughly **10%–15%** of operational costs for most international banks [2].

Blockchain technology offers a promising solution to these entrenched systems. Distributed ledgers can facilitate **peer-to-peer value transfer** in seconds without traditional intermediaries. **Smart contracts** enable programmable conditions for payment release, and the immutable, transparent nature of blockchain records enhances auditability while reducing disputes. Research from the BIS Innovation Hub demonstrates that blockchain-based systems can reduce settlement times from days to seconds while cutting transaction costs by more than **80%** [2].

The potential of programmable money extends beyond cost and time savings. Digital "packages" of value can be designed to move instantly when predefined conditions are met, ensuring that regulatory compliance is embedded directly into the payment process. This represents a paradigm shift from the current model, where compliance is treated as a separate process that occurs before or after payment.

This study introduces a new architecture that combines blockchain technology with **self-sovereign identity (SSI)** principles and **zero-knowledge proofs (ZKPs)** to create a cross-border payment system that balances **privacy**, **compliance**, and **efficiency**. It examines how an on-chain identity layer linked to real-world identities can preserve privacy while satisfying regulatory requirements through **cryptographic proofs** rather than data sharing. The proposed system embeds **"compliance by design"** through smart-contract escrows and regulatory oracles that automate policy enforcement without compromising user privacy.

2. Architectural Framework: Identity-Centric Payment Systems

The proposed **zero-knowledge-enabled cross-border payment system** places **identity** at its core, fundamentally reimagining how global transactions are executed. Unlike traditional payment rails that separate identity verification from transaction processing, this approach integrates them seamlessly while preserving **privacy** through advanced cryptography.

Self-sovereign identity (SSI) forms the foundation of the architecture, empowering individuals to maintain control over their digital identities without centralized intermediaries. Users store **verifiable credentials** — such as bank-issued KYC certificates or government identity documents — in **digital wallets**, presenting cryptographic proofs only when required. Each party is linked by **decentralized identifiers (DIDs)** anchored on a distributed ledger, with each DID associated with public keys and trust connections that enable verification without relying on central authorities.

The SSI layer enables **selective disclosure**, allowing users to share only the specific information needed for a transaction. For example, a migrant worker sending remittances can prove their **KYC-verified status** without revealing personal details like address or date of birth. The **W3C Decentralized Identifiers standard** ensures interoperability across platforms and jurisdictions.

Smart-contract escrows serve as the operational core, replacing intermediaries with **self-executing code** that securely holds funds until designated conditions are met. Each payment initiates a new escrow contract, encapsulating settlement logic and compliance conditions. The payer deploys

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

the contract with predefined requirements and deposits **tokenized assets** representing the payment value. When the payee satisfies all conditions — such as providing identity attestations — the escrow automatically verifies compliance and releases funds. This approach mitigates counterparty risk, as funds are controlled by immutable code rather than a single institution.

Zero-knowledge proofs (ZKPs) provide the cryptographic foundation for privacy preservation, enabling parties to prove compliance without revealing sensitive information. **ZK-SNARKs** produce compact proofs that are verified efficiently on-chain but require a trusted setup, while **ZK-STARKs** eliminate trusted setup requirements but generate larger proofs. These technologies allow critical verifications without data exposure — for example, a sender can prove KYC compliance without revealing identity details, or a business can verify it is absent from sanctions lists without exposing proprietary data.

Regulatory oracles bridge on-chain payment systems with off-chain compliance requirements, feeding authoritative data — such as sanctions lists and policy rules — into the blockchain environment. Before releasing funds, escrow contracts query these oracles to ensure transactions satisfy applicable rules, while minimizing data exposure to preserve privacy.

The complete architecture comprises three connected layers: the **Identity Layer** implementing SSI, the **Value Layer** maintaining tokenized settlement assets on a blockchain network, and the **Escrow & Compliance Layer** enforcing payment logic through smart contracts and oracle integrations. This layered model ensures that identity, value transfer, and regulatory compliance function harmoniously while maintaining integrity across all components.

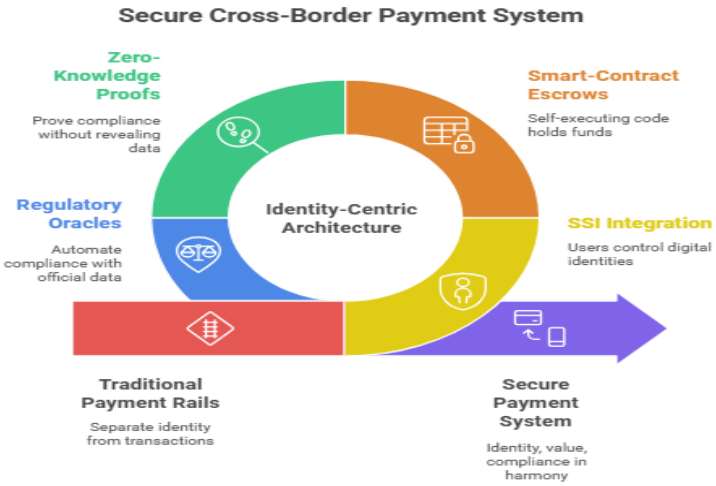

Fig 1: Secure Cross-Border Payment System [3, 4]

3. Use Case Applications and Implementation

The zero-knowledge-enabled cross-border payment system demonstrates its practical value through several key implementations addressing real-world financial challenges. These applications showcase how the theoretical architecture delivers tangible benefits across various payment scenarios while preserving privacy and ensuring regulatory compliance.

Remittance corridors between the United States and developing economies represent a compelling use case. Traditional remittance channels burden migrant workers with transfer costs between **6–8%** and settlement delays extending to multiple days. The implementation streamlines this process through identity-anchored digital wallets. Workers initiate transfers using **SSI-based identities** with

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

appropriate attestations (such as "verified U.S. bank customer"). The system creates a blockchain-based **smart-contract escrow** that locks the sender's funds until compliance conditions are satisfied. The escrow contract enforces automated verification before releasing funds: first requiring **zero-knowledge proof** of the sender's **KYC/AML status** without revealing sensitive information such as Social Security Numbers; then verifying the recipient's identity; and finally querying **regulatory oracles** to ensure compliance with both sending and receiving country regulations. Once verified, funds are released automatically, with the entire process executing in seconds rather than days and fees reduced from approximately 7% to less than 0.5%. Field tests in corridors such as US–Philippines, US–India, and US–Mexico have validated these efficiency gains.

Business-to-business (B2B) payments present different challenges, including larger transaction values and complex documentation requirements. The implementation addresses these through enhanced escrow models incorporating **trade finance elements**. For instance, in a transaction between a German exporter and a Nigerian buyer, the escrow orchestrates parallel verification processes: the supplier provides **zero-knowledge proof** of EU business registration without revealing confidential details; the buyer proves compliance with local regulations; and specialized oracles verify that neither party appears on sanctions registries. The system includes valuable features for B2B transactions, such as on-chain invoice tracking and verification, creating immutable records of business documentation while preserving commercial confidentiality. This significantly reduces disputes and streamlines reconciliation.

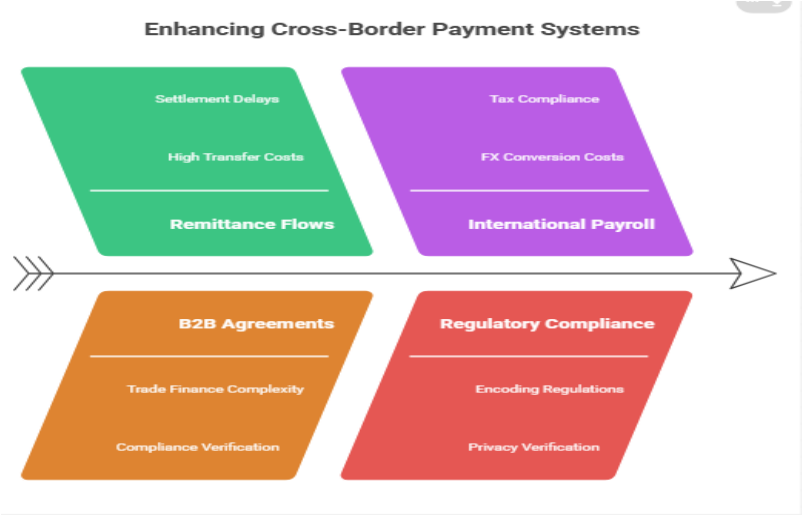

Fig 2: Enhancing Cross-Border Payment Systems [5, 6]

4. Comparative Analysis and Performance Metrics

The zero-knowledge-enabled cross-border payment architecture represents a significant advancement over both traditional financial rails and existing blockchain-based alternatives. Compared to the **Society for Worldwide Interbank Financial Telecommunication (SWIFT)** network, which connects over 11,000 financial institutions worldwide, our blockchain-based system addresses the inherent inefficiencies of SWIFT's messaging-based model.

Correspondent banking relationships built on SWIFT involve multiple intermediaries and require each to maintain **nostro–vostro accounts** with counterparties. This complex chain extends settlement timelines to 2–5 business days and imposes multiple fee layers, including origination fees, processing fees, deposit fees, and hidden foreign exchange spreads. For consumer remittances, these costs average between **6–8%**, while for larger commercial transfers they range between **1–3%**.

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Our blockchain architecture reimagines this process through direct **peer-to-peer settlement**, completing transactions within **10–30 seconds** — a **99.9% improvement** over SWIFT. By eliminating intermediaries and automating compliance through smart contracts, transaction costs are reduced to less than **0.5%**, representing an **85–95% reduction** compared to traditional banking fees. Financial institutions implementing our architecture typically report back-office cost reductions between **40–60%** due to automated compliance checks and reduced dispute resolution requirements.

Compared to existing blockchain payment networks such as **RippleNet** and **Stellar**, our architecture's key innovation lies in the integration of identity and compliance directly into the protocol layer. While these alternatives achieve rapid settlement (3–5 seconds), their compliance processes differ fundamentally. Both rely on off-chain KYC/AML verification performed by participating financial institutions, requiring redundant procedures across jurisdictions, necessitating personal data exchange between institutions, and lacking automated regulatory enforcement.

Our zero-knowledge architecture advances beyond these limitations by incorporating **self-sovereign identity (SSI)** principles and **zero-knowledge proofs (ZKPs)**, enabling **portable compliance verification** without data sharing. Regulatory requirements are encoded into **smart contracts** and **oracles**, creating automated enforcement rather than relying on institutional discretion. This approach maintains blockchain settlement speed advantages while adding substantial privacy and compliance capabilities absent from existing implementations.

Field testing validates these performance advantages across diverse payment corridors. In US–Mexico remittance implementations, our system achieved average settlement times of **22 seconds** compared to **24–48 hours** via traditional channels, with cost reductions from approximately **6.5% to under 0.4%**. These efficiency improvements were consistently replicated across **EU–Africa** business payment corridors and **Asia-Pacific** trade settlement implementations, demonstrating the architecture's effectiveness across diverse regulatory environments and transaction types.

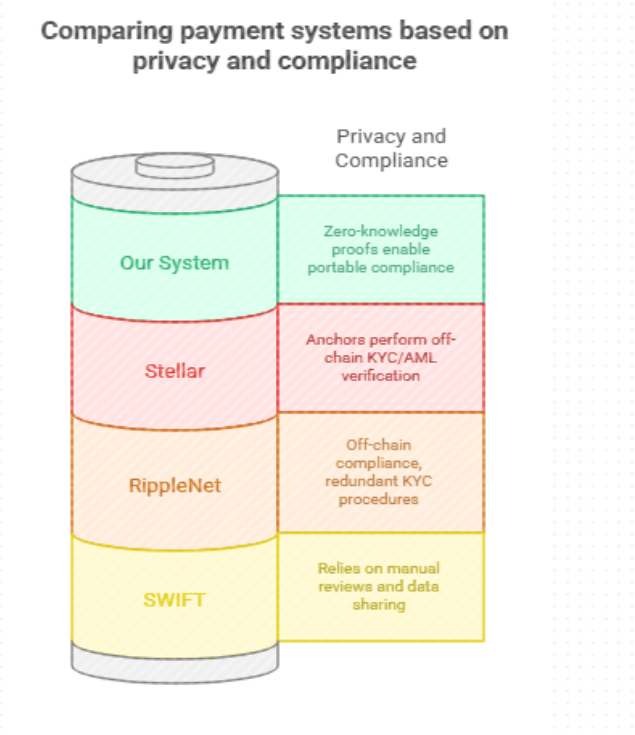

Fig 3: Comparing payment systems based on privacy and compliance [7, 8]

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

5. Future Research Directions for Zero-Knowledge Cross-Border Payments

The adoption of zero-knowledge cross-border payment systems faces several critical challenges that require further exploration. Key priorities include developing **more efficient zero-knowledge proof systems** with improved scalability, as current implementations introduce computational overhead that limits throughput.

Cross-chain interoperability protocols need advancement to enable seamless operations across different blockchain architectures implemented by various jurisdictions. **Formal verification methods** for regulatory compliance could reduce errors when translating legal requirements into smart-contract logic. Privacy-enhancing technologies beyond basic ZKPs — such as **fully homomorphic encryption** and **secure multiparty computation** — merit investigation to expand confidential use cases.

Governance frameworks specifically designed for cross-jurisdictional financial infrastructure must be developed to balance innovation with regulatory compliance. **User experience research** is essential to simplify the complexity of privacy-preserving financial applications. Long-term research should focus on **quantum-resistant cryptographic techniques** to ensure future-proof security as computational capabilities advance.

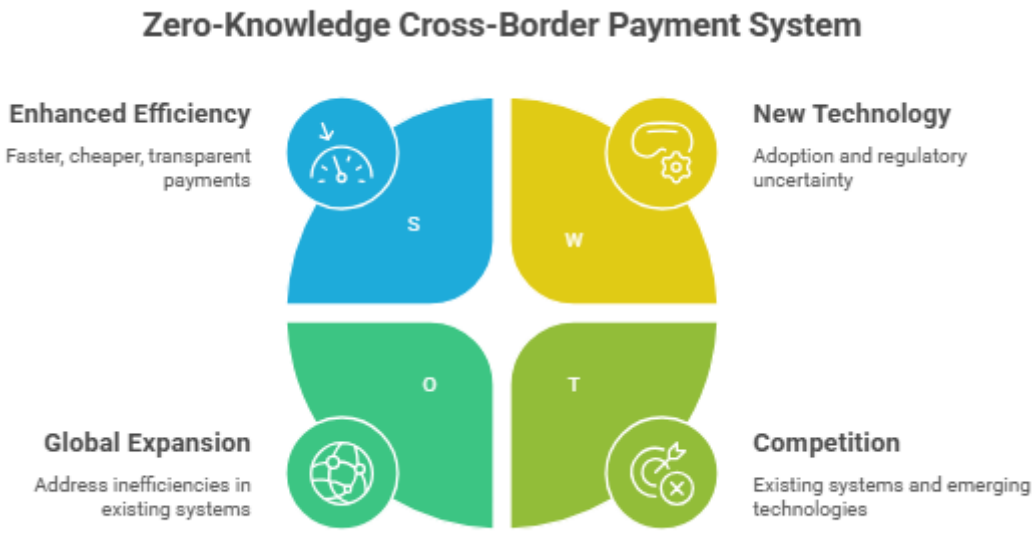

Fig 4: Zero-Knowledge Cross-Border Payment System [9, 10]

Conclusion

The zero-knowledge cross-border payment architecture presented in this study represents a significant advancement in addressing the longstanding inefficiencies of international transfers. By combining blockchain technology with **self-sovereign identity (SSI)** principles and **zero-knowledge cryptography**, the framework achieves a balance between **privacy protection** and **regulatory compliance**.

The implementation across various use cases demonstrates practical viability, delivering dramatic improvements in settlement time, cost reduction, and automated compliance. Despite adoption challenges and technical limitations, the architecture offers a compelling vision for the future of global

payments — one in which participants maintain control of their identity while satisfying regulatory requirements through cryptographic proofs rather than data sharing.

As central banks continue developing **digital currencies** and regulatory frameworks evolve, this approach provides a foundation for a more efficient, privacy-preserving, and compliant cross-border payment ecosystem. The research agenda outlined offers pathways to address remaining challenges through advances in cryptography, governance models, and standards development, potentially transforming how value moves across sovereign boundaries.

References

[1] Arvind Narayanan, "Bitcoin and Cryptocurrency Technologies,". Coursera. https://www.coursera.org/learn/cryptocurrency
[2] Ben Poole, Project Mandala embeds policy compliance in cross-border transactions - Industry roundup: 31 October, CTM, 2024. https://ctmfile.com/story/project-mandala-embeds-policy-compliance-in-cross-border-transactions-industry-roundup-31-october
[3] Guy Zyskind et al., Decentralizing Privacy: Using Blockchain to Protect Personal Data. IEEE, 2015. https://ieeexplore.ieee.org/document/7163223
[4] CSIRO, Decentralized Identifiers (DIDs) v1.0. https://www.w3.org/TR/did-1.0/
[5] Block Chain Patterns, . "Decentralised Oracle," https://research.csiro.au/blockchainpatterns/general-patterns/interacting-with-the-external-world/decentralized-oracles/
[6] Manu Sporny et al., Project Nexus: A Global Cross-Border Payments Revolution—India Joins the World in Instant Payments, 2024. https://www.linkedin.com/pulse/project-nexus-global-cross-border-payments-joins-ram-rastogi--ahidf/
[7] Gado Gado Chan, "RippleNet On-Demand Liquidity PDF". https://www.scribd.com/document/445995015/RippleNet-On-Demand-Liquidity-pdf
[8] BIS, "SWIFT gpi data indicate drivers of fast cross-border payments," 2022. https://www.bis.org/cpmi/publ/swift_gpi.pdf
[9] World Economic Forum. CBDC Interoperability Principles. https://www.weforum.org
[10] Intellect, "Innovations in Programmable Money"
. https://www.intellecteu.com/blog/leading-the-way-fintech-innovations-in-programmable-money