OpenBridge: A Hybrid Blockchain Protocol for Scalable Cross-Border Payments

Group 3
Warwick Business School

April 2025

Submitted in partial fulfilment of the requirements for
IB9YW0 – Fintech: Digital Currencies and Decentralised Finance

Abstract

Despite the rapid globalization of commerce and finance, cross-border payments continue to rely on legacy infrastructure that is slow, expensive, and opaque. OpenBridge presents a new architecture designed to overcome these challenges by combining the strengths of blockchain technology with the practical requirements of regulated financial systems. The protocol operates on a permissioned Proof-of-Authority (PoA) Layer-1, coupled with Layer-2 scalability through rollups, enabling fast and cost-effective settlements without compromising compliance or security. Integrated zero-knowledge proofs preserve transaction confidentiality without compromising regulatory oversight, while oracle-powered smart contracts facilitate transparent and programmable foreign exchange settlement. Rather than idealizing total decentralization, OpenBridge prioritizes institutional interoperability—delivering a resilient, compliance-ready framework for modern cross-border payments.

Contents

1 Introduction and Motivation

Cross-border payments remain one of the most costly and inefficient components of the global financial system. Despite facilitating over $150 trillion in annual flows—including remittances, trade settlements, and capital transfers—the underlying infrastructure remains slow, opaque, and expensive. According to the World Bank, the average remittance cost globally still exceeds 6%, with many low-income corridors experiencing even higher fees.[1] These payments often traverse multiple correspondent banks, introducing delays, foreign exchange markups, and opacity in tracking and delivery. Legacy systems like SWIFT were not designed for retail payments or real-time settlement, leading to operational bottlenecks for individuals and SMEs alike. Settlement often takes 1–5 days. These inefficiencies disproportionately impact remittance-dependent economies and financially underserved populations, highlighting a critical need for rethinking existing infrastructure.

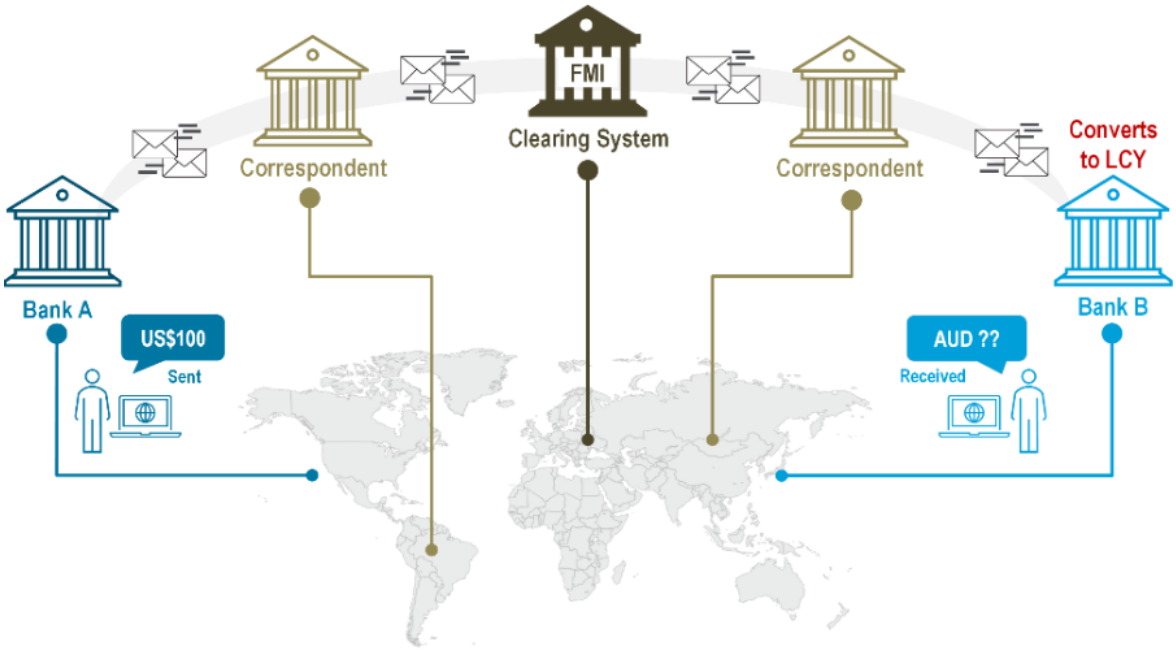

Figure 1: Cross-Border Payments Using a Correspondent Bank, Transaction Settled in Beneficiaries' Currency. Source: Bank of England, Citi Research.

Against this backdrop, blockchain technology is emerging as a viable alternative to streamline international payments. By enabling peer-to-peer transactions secured by cryptographic consensus, blockchain reduces reliance on intermediaries while ensuring transparency and auditability. Distributed ledger platforms allow programmable asset transfer, fast settlement, and integration of compliance logic through smart contracts. Projects such as BIS's mBridge[2] and the IMF's Multi-Currency Contracting Platform[3] highlight a growing institutional recognition of blockchain's potential for FX execution and settlement. Meanwhile, platforms like Ripple and Stellar are already facilitating

[1] World Bank Remittance Prices Worldwide, Q4 2023.

[2] BIS Innovation Hub (2023). *mBridge: Exploring Multilateral Platforms for Cross-Border Payments.*

[3] Adrian, T. et al. (2022). *A Multi-Currency Exchange and Contracting Platform.* IMF Working Paper 217.

low-cost transfers using stablecoins and tokenized assets in regions such as Africa, Latin America, and Southeast Asia.

1.1 The Cross-Border Payments Problem

Cross-border payments are the financial lifeline of international trade, remittances, and global investment flows. Yet the infrastructure that supports them remains largely outdated. With over $150 trillion transacted annually, these payments continue to rely on legacy systems such as SWIFT and correspondent banking chains, which were never designed to accommodate real-time, high-frequency, or small-value transactions. Instead of a single integrated rail, the process involves a relay of intermediaries, each introducing settlement delays, opaque foreign exchange markups, and service fees. Compounding these inefficiencies is the reliance on pre-funded nostro accounts and fragmented reconciliation procedures—factors that limit liquidity and introduce operational risk. These structural constraints contribute to high costs, unpredictable timelines, and poor transparency for both institutions and end-users.

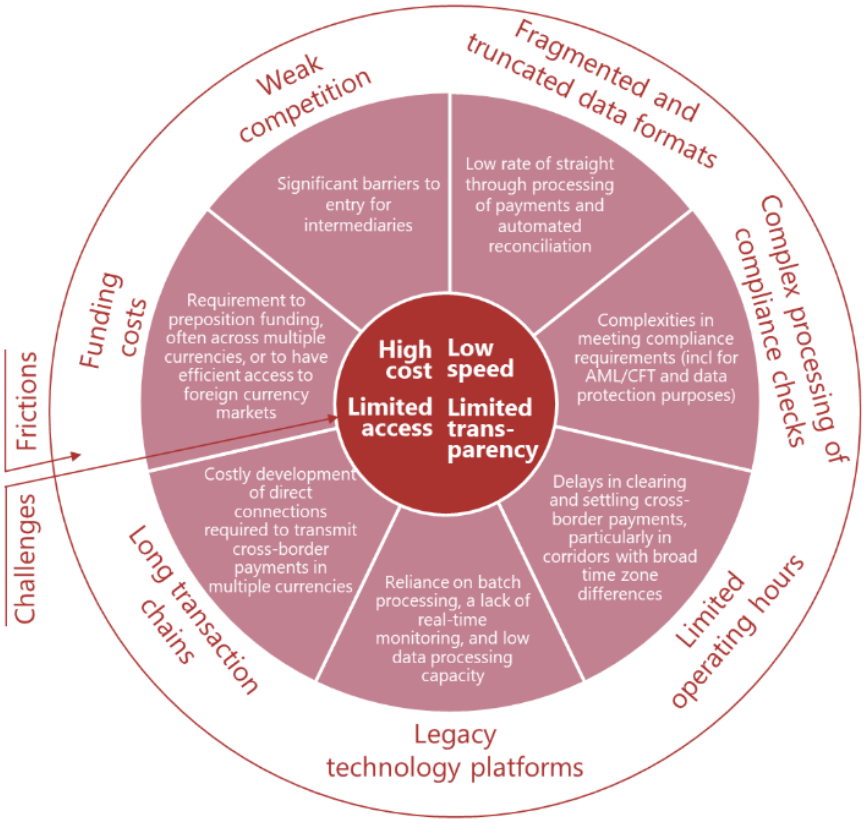

Figure 2: Cross-border payment frictions and their underlying causes. Source: Bank for International Settlements (2020).

A 2020 report by the Bank for International Settlements (BIS) identifies four key pain points in the cross-border payments landscape: high cost, low speed, limited access, and limited transparency. These outcomes are underpinned by deeper structural frictions—such as fragmented data formats, reliance on batch processing, and complex AML/CFT compliance requirements. For example, intermediaries must often maintain pre-funded accounts in foreign currencies to facilitate settlement, locking up capital and

reducing liquidity efficiency. Time zone mismatches and limited operating hours further delay processing, while the absence of end-to-end transaction visibility prevents users from tracking payments in real time. For small and medium enterprises (SMEs) and low-income migrant workers, these inefficiencies translate into disproportionately high fees and uncertainty.

The impact of these flaws is especially acute in low-income and emerging markets where financial infrastructure is weakest, and dependence on remittances is highest. For example, average remittance fees to sub-Saharan Africa still exceed 8%, among the highest in the world. Meanwhile, new entrants such as fintech platforms and mobile money operators face substantial barriers to entry due to interoperability gaps, compliance burdens, and fragmented regulatory oversight. These dynamics entrench the dominance of large financial institutions and prevent more inclusive and cost-effective models from scaling. To move beyond incremental fixes, there is a growing recognition of the need for architectural transformation—one that marries digital efficiency with regulatory safeguards, enabling a more inclusive, transparent, and resilient cross-border payment ecosystem.

1.2 Why Blockchain, Why Now?

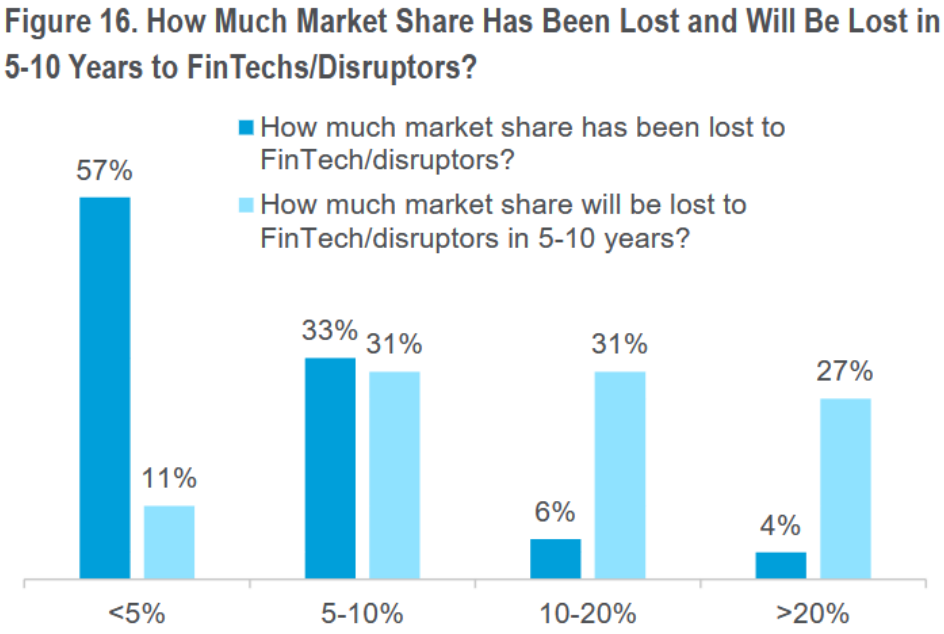

Figure 3: How much market share has been and will be lost to FinTechs. **Source:** Citi Research, 2023.

Over the past decade, blockchain technology has evolved from a niche experiment into a serious contender for solving deep-rooted inefficiencies in global financial infrastructure. Nowhere is this transformation more relevant than in the domain of cross-border payments. Unlike legacy networks built around intermediaries and proprietary protocols, blockchain offers a decentralized, programmable, and cryptographically secure alternative. Distributed ledgers allow real-time value transfer, immutable record-keeping, and automated compliance checks, all within a single framework. These advantages directly address the major pain points outlined by the G20 and BIS—namely, high fees, low speed,

and lack of transparency. Moreover, smart contract functionality introduces programmability into payments, allowing compliance logic, FX execution, and settlement rules to be enforced automatically at the protocol level.

This momentum is already reshaping market expectations. As shown in Figure 3, financial institutions acknowledge the growing threat posed by digital disruptors, with over 50% of surveyed incumbents expecting to lose 10–20% or more of their market share to FinTechs within the next decade. These trends reflect both consumer demand for faster, cheaper, and more transparent financial services, and institutional pressure to modernize aging infrastructure. In this context, blockchain is no longer a fringe innovation but a strategic imperative—one capable of delivering programmable money, real-time FX, and cross-border interoperability at a fraction of today's costs. The case for blockchain is not just technological—it's structural, economic, and increasingly, unavoidable.

1.3 Case for a New Design Paradigm

Despite the transformative potential of blockchain technology, its broad adoption in cross-border payments remains constrained by several critical limitations. Scalability remains a persistent challenge—particularly for networks that must handle high transaction volumes without sacrificing speed or cost-efficiency. Energy consumption is another concern, especially for protocols reliant on Proof-of-Work, such as Bitcoin, which consume significant computational resources. Volatility in native crypto assets also introduces exchange rate risk for end-users, undermining trust and stability in payment flows. In addition, fragmented regulatory frameworks, lack of international standards, and limited interoperability with legacy infrastructure continue to restrict seamless integration of blockchain-based systems into the global financial architecture.

Modernising cross-border payments is now an economic necessity, as global trade digitizes and financial inclusion becomes a policy priority. To meet these demands, a new design paradigm is emerging—one that blends the programmability and transparency of blockchain with the trust frameworks of traditional finance. Platforms like OpenBridge exemplify this shift: combining permissioned consensus, zero-knowledge proofs, and multi-currency smart contracts to enable compliant, privacy-preserving, and cost-efficient transfers across jurisdictions. Achieving this vision will require coordinated innovation among all key stakeholders. When done right, such systems can lay the foundation for a truly global, inclusive and twenty-first-century payment ecosystem.

2 Case Study: Stellar Protocol for Cross-Border Payments

2.1 Overview and Design of the Stellar Network

Cross-border payments for individuals and small businesses remain inefficient and expensive. As we have already highlighted, traditional networks like SWIFT operate through a chain of correspondent banks, each adding layers of fees, foreign exchange markups, and settlement delays. In many cases, a single international payment can take several days, with limited transparency on pricing and delivery status. These inefficiencies not only increase transaction costs but also disproportionately affect remittance corridors and low-income users who can least afford them.

Against this backdrop, the global financial system is undergoing a profound shift with the rise of digital currencies and blockchain infrastructure. Traditional cross-border

payment systems, primarily reliant on SWIFT and correspondent banking relationships, are increasingly being challenged by more efficient, decentralized alternatives. Among the most prominent of these solutions is Stellar: an open-source, decentralized network designed specifically for low-cost, real-time value transfers across borders.

Launched in 2014 by Jed McCaleb, a co-founder of Ripple, Stellar was designed not to replace the existing financial system but to complement and interoperate with it. Its core vision revolves around bridging the gap between traditional finance and the emerging world of digital assets. Rather than creating an isolated ecosystem, Stellar connects regulated financial institutions - termed 'anchors' - to a global blockchain-based settlement layer. These anchors act as on- and off-ramps for fiat currencies, enabling users to deposit money locally and send it across borders almost instantly. This hybrid model has proven especially effective in facilitating financial access in emerging markets, where banking infrastructure is often fragmented or underdeveloped.

What sets Stellar apart is its explicit commitment to financial inclusion. Its lightweight, energy-efficient consensus protocol (the Stellar Consensus Protocol, or SCP) enables participation by a wide range of actors, including those in regions with limited technological infrastructure. With its focus on accessibility, transparency, and affordability, Stellar has become an enabling layer for NGOs, development agencies, and cross-border payment firms operating in underserved and frontier markets.

2.2 Key Features and Core Architecture of Stellar

2.2.1 Anchors and Asset Tokens

Anchors are central to Stellar's interoperability model. These are regulated financial institutions or fintech companies that issue fiat-pegged digital tokens on the network and serve as trusted bridges between the traditional banking system and the Stellar blockchain. When a user deposits a local currency with an anchor, they receive a corresponding digital asset (e.g., USD token, NGN token) on Stellar. This digitized form of money can then be transferred, exchanged, or stored across the network with ease.

The use of anchors allows Stellar to maintain regulatory compatibility while offering the efficiencies of a blockchain network. Anchors act as bridges between the physical financial system and the digital Stellar network. They also handle important responsibilities like KYC/AML compliance and user onboarding. By 2021, major stablecoins like USD Coin (USDC) joined Stellar through such anchors, meaning Stellar users can hold and transfer digital USD that is fully backed by real dollars

2.2.2 Smart Contracts and Compliance Mechanisms

Unlike Ethereum-style Turing-complete smart contracts, Stellar opts for a more constrained model based on multi-operation transactions and pre-defined logic flows. This design choice prioritizes safety, auditability, and low computation costs, making it ideal for high-volume payment use cases. Through tools like pre-authorized transactions and multi-signature requirements, users and institutions can construct payment logic such as escrow services, recurring transfers, and conditional payouts.

Compliance is also integrated into Stellar's protocol-level operations. Anchors can implement KYC, AML, and sanction screening protocols as part of their onboarding process. Features like claimable balances also support compliance workflows by allowing regulated parties to hold transfers until recipients complete identity verification. These

mechanisms make Stellar highly adaptable for financial institutions seeking blockchain utility without compromising regulatory obligations.

2.2.3 Fast, Low-Cost Transactions

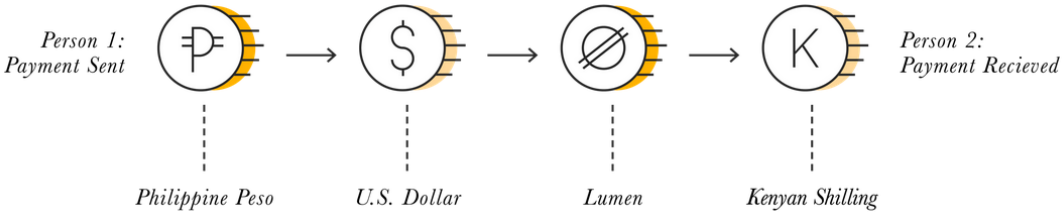

Figure 4: Cross-border payment process using Stellar. **Source:** Official Stellar.

Transactions on Stellar settle in just 3 to 5 seconds and carry a nominal fee (0.00001 XLM) to deter spam. In real terms, this translates to a cost of less than a fraction of a cent. This efficiency stems from Stellar's streamlined transaction model, low on-chain complexity, and a consensus protocol purpose-built for speed. As a result, the network is especially well-suited for emerging markets, remittance corridors, and payment providers looking to bypass the delays and high costs of traditional financial rails.

2.2.4 Stellar Consensus Protocol (SCP)

At the heart of Stellar's performance is the Stellar Consensus Protocol (SCP), a federated Byzantine agreement (FBA) system. Unlike traditional consensus mechanisms such as Proof of Work (PoW) or Proof of Stake (PoS), SCP achieves a unique balance across four critical dimensions: *decentralized control*, *low latency*, *flexible trust*, and *asymptotic security*. As summarized in Table 1, this makes SCP one of the few consensus models capable of combining operational efficiency with strong decentralization and resilience.

Mechanism	**Decentralized Control**	**Low Latency**	**Flexible Trust**	**Asymptotic Security**
Proof of Work	✓			maybe
Proof of Stake	✓	maybe	✓	✓
Byzantine Agreement		✓		✓
Tendermint	✓	✓		✓
SCP	✓	✓	✓	✓

Table 1: Properties of different consensus mechanisms, adapted from the SCP whitepaper by Mazieres (2016).

Rather than requiring a globally agreed set of validators, SCP allows each node to select its own trusted subset of participants, called *quorum slices*. Consensus is reached when enough of these slices intersect, forming a quorum across the network. This structure enables Stellar to finalize transactions in seconds without relying on energy-intensive computation or centralized authorities.

2.2.5 Path Payments, Liquidity Pools, and On-Chain FX

Stellar's path payment feature is a powerful tool for global remittances and FX execution. It allows users to send one asset while the recipient receives another, with the protocol finding the most efficient conversion path through available order books and liquidity pools. For instance, if a user wants to send EUR to someone who wants to receive NGN (Nigerian Naira), Stellar can convert the funds via USD or XLM if those paths offer better exchange rates or liquidity.

Liquidity is maintained through decentralized order books and automated market-making (AMM) pools introduced in Stellar Protocol 18. These AMMs allow liquidity providers to deposit pairs of assets and earn fees from facilitating swaps.

2.3 Stellar's Comparison with Ripple

One of the closest counterparts to Stellar in the blockchain-based cross-border payments space is Ripple. At first glance, the two networks appear strikingly similar—both were created to facilitate real-time, low-cost international transactions and rely on native digital assets (XLM for Stellar and XRP for Ripple) to bridge currencies. However, beneath the surface, they diverge significantly in their design philosophies and operational models. Ripple, structured as a private company, focuses on serving large financial institutions and central banks through enterprise-grade solutions. Stellar, on the other hand, is managed by a nonprofit foundation focused on financial inclusion and open access, particularly in underserved markets. These differences are further reflected in their approach to governance, compliance, and developer ecosystems. As such, while both aim to modernize global payments, they cater to complementary user bases rather than competing head-on.

Table 2: Comparison of Stellar and Ripple

Criteria	Stellar	Ripple
Philosophy	Focused on financial inclusion and open access, particularly in underserved markets.	Targeted at large financial institutions and central banks with a focus on enterprise adoption.
Governance	Managed by a nonprofit foundation (Stellar Development Foundation) with open-source governance and a public permissionless network.	Operated by a private company (Ripple Labs), with a more centralized validator and governance model.
Monetary Policy	Operates on a fixed-supply model, having launched with 100 billion XLM and later reducing the total supply to approximately 50 billion following a 2019 community vote, with no additional issuance planned.	XRP was pre-mined with 100 billion tokens; Ripple Labs controls a majority share, releasing them programmatically from escrow.

In an evolving financial world, the coexistence of both platforms could lead to a

bifurcated market where Ripple addresses the needs of banks and institutional clients, and Stellar serves the Fintechs and the unbanked. The two are not necessarily competitors in function, but rather complementary players in the broader digital finance ecosystem.

2.4 Cross-Border Transaction Flow in Stellar

To understand Stellar's real-world utility, here is an illustration through a sample transaction involving two users—**Alice in Brazil** and **Bob in Nigeria**. The following steps outline how Stellar facilitates this transfer efficiently, securely, and with full currency conversion:

1. **Transfer Initiation**
   Alice wishes to send 100 BRL to Bob. She opens her Stellar-based mobile wallet and inputs Bob's wallet address or phone number, specifying the payout currency as Nigerian Naira (NGN).

2. **Onboarding via Local Anchor (Brazil)**
   Alice's wallet connects to a regulated Brazilian anchor that performs KYC and accepts the 100 BRL deposit. The anchor then tokenizes this value on-chain—either issuing BRL tokens or converting the funds into a widely accepted stablecoin like USDC. Alice now holds $100 worth of USDC on the Stellar network.

3. **Path Payment and Asset Routing**
   Stellar's path payment mechanism activates, seeking the most efficient conversion route from USDC to NGN. If no direct liquidity is available, the protocol may route through intermediate assets like XLM or USD tokens. The routing logic ensures minimal slippage and real-time quoting.

4. **Transaction Execution and Finality**
   Once a viable path is confirmed, Stellar executes the transaction in 3–5 seconds using the Stellar Consensus Protocol (SCP). Funds are atomically debited from Alice's wallet and credited to the Nigerian anchor in NGN equivalent.

5. **Payout via Local Anchor (Nigeria)**
   The Nigerian anchor receives the NGN tokens and disburses the fiat equivalent to Bob via a mobile money wallet, bank transfer, or card credit—depending on local infrastructure. All compliance and regulatory checks are enforced before settlement.

6. **Confirmation and Audit Trail**
   Both Alice and Bob receive instant confirmations. The entire transaction, including FX rates, routing path, and fees is verifiable via Stellar's public ledger.

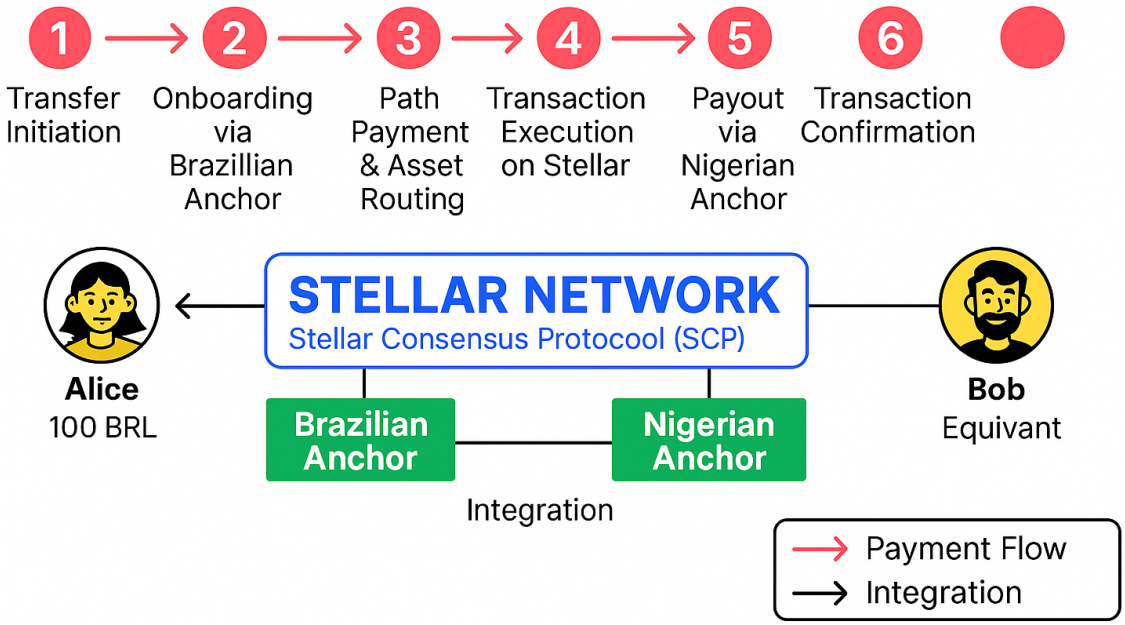

Figure 5: Cross-Border Payment Flow from Brazil (BRL) to Nigeria (NGN) via Stellar Anchors.

While Stellar has demonstrated considerable promise as a low-cost, high-speed payment network, several limitations restrict its broader applicability in highly regulated, institutional-grade environments. Its anchor-based model, though effective in theory, places the burden of regulatory compliance on local partners—leading to inconsistencies in KYC/AML enforcement across jurisdictions. Additionally, the network's limited support for smart contracts constrains its ability to accommodate complex settlement logic, such as conditional disbursements or programmable compliance. Liquidity is another concern, particularly for less commonly traded currency pairs, where transaction paths may depend heavily on third-party market makers. These structural gaps underscore the need for next-generation solutions like OpenBridge, which aim to integrate deeper regulatory alignment, richer programmability, and institutional-grade liquidity within a permissioned blockchain framework.

3 OpenBridge Protocol: Architecture and Design

3.1 Overview of the OpenBridge Architecture

As we have seen so far, cross-border payment solutions today face multiple inefficiencies, such as high fees, slow processing times, limited scalability, privacy concerns, and regulatory complexity. While traditional systems like SWIFT rely heavily on intermediaries, resulting in delays and increased costs, even blockchain-based systems like Ripple or Stellar encounter scalability constraints and fluctuating liquidity challenges during market volatility (BIS Innovation Hub, 2022).

OpenBridge addresses these challenges by carefully combining multiple innovative blockchain elements into a unified solution. The protocol operates using a Proof-of-Authority (PoA) model, where transactions are quickly validated by trusted financial institutions, thus ensuring security and regulatory compliance. To resolve scalability bottlenecks, Layer-2 scaling solutions such as Optimistic and Zero-Knowledge (ZK) Rollups

are utilised, allowing the protocol to efficiently handle high transaction volumes at significantly reduced costs. OpenBridge's privacy is strengthened through the seamless integration of Zero-Knowledge Proofs (ZKPs), allowing transactions to remain confidential while still verifiable. Lastly, the deployment of oracle-based smart contracts guarantees transparent and predictable FX pricing (Adrian et al., 2022), reinforcing consumer trust in the prototype. This architecture allows OpenBridge to function as both a technical platform and policy-aligned bridge between DeFi and traditional finance.

3.2 Hybrid Blockchain Consortium Model

OpenBridge is built on a hybrid consortium blockchain model that reflects the practical demands of cross-border retail payments. Rather than relying on fully decentralized networks, this model brings together a select group of trusted institutions, such as central banks and regulated payment providers, to serve as validators. This approach directly responds to the well-known trade-off between scalability, decentralization, and security - sometimes referred to as the blockchain trilemma (Buterin, 2017). Given the system's objective to integrate with traditional financial markets, certain priorities become clear: transactions must be fast, compliant, and secure. A fully open validator set may offer greater decentralization in theory, but at the cost of auditability, operational efficiency, and governance clarity. By adopting a consortium framework, OpenBridge ensures regulatory alignment, reduces operational risks, and provides the technical flexibility required to support both institutional and retail use cases. To achieve this, the protocol is structured around a two-layer mechanism:

3.2.1 Layer-1: Permissioned Settlement Layer

The first layer (Layer-1) of the OpenBridge architecture consists of a permissioned blockchain employing a Proof-of-Authority (PoA) consensus mechanism. In this framework, validator nodes are exclusively operated by a consortium of pre-approved, regulated financial institutions such as central banks, commercial banks, and licensed payment service providers. They validate transactions and ensure settlement. Unlike Proof-of-Work (PoW), which depends on computational power, or Proof-of-Stake (PoS), which allocates influence based on token holdings, PoA grants validation authority based on institutional identity, regulatory vetting, and reputational accountability.

Table 3: Comparison of Blockchain Consensus Mechanisms

Criteria	**Proof-of-Authority (PoA)**	**Proof-of-Stake (PoS)**	**Proof-of-Work (PoW)**
Validator Identity	Known and verified (institutions)	Pseudonymous (any token holder)	Anonymous (miners)
Selection Criteria	Regulatory approval and reputation	Amount of staked cryptocurrency	Computational power (hashrate)
Energy Consumption	Very low	Moderate to low	Very high
Transaction Finality	Near-instant	Probabilistic	Probabilistic
Regulatory Compliance	Strong (built-in AML/KYC)	Variable (depends on implementation)	Weak to none
Security Basis	Institutional accountability	Economic stake	Computational difficulty
Best Use Case	Regulated finance, enterprise blockchains	DeFi, staking ecosystems	Public cryptocurrencies (e.g., Bitcoin)

This model offers several advantages that align closely with the needs of cross-border financial systems. It reduces latency, avoids the inefficiencies of energy-intensive validation methods, and supports near-instant transaction finality. The use of trusted validators ensures compliance with AML/KYC frameworks while maintaining high security standards. Critically, PoA also allows for deterministic block times and consistent network throughput—features that are difficult to guarantee in fully open or pseudonymous networks.

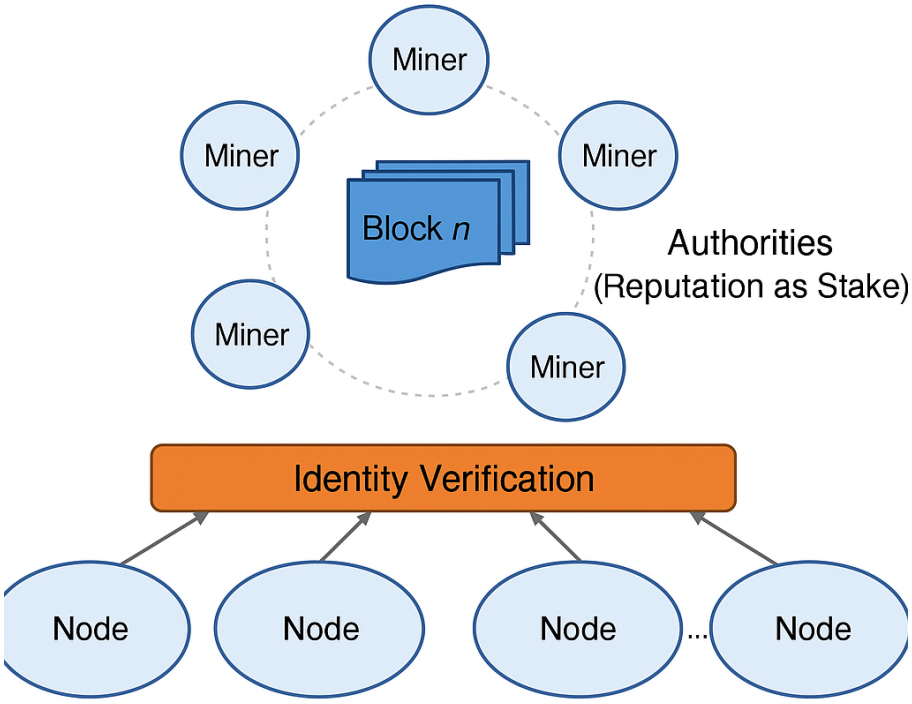

Figure 6: Architecture of the Proof-of-Authority (PoA) consensus mechanism, where validators must verify their identity before participating in block production. Source: Kim et al. (2019).

3.2.2 Layer-2: Scalability and Transaction Processing Layer

To handle high transaction volumes and maintain efficient performance, OpenBridge incorporates Layer-2 scalability solutions, specifically Optimistic and Zero-Knowledge (ZK) Rollups. This decision reflects the distinct operational profiles of both models. Optimistic Rollups assume transaction validity by default and only require proof in the event of a dispute, which allows them to process large volumes of transactions efficiently with minimal computational overhead (Buterin, 2021). In contrast, ZK-Rollups generate complex cryptographic proofs for every transaction bundle, though more private and fast, require more computational resources and are more expensive to deploy at scale, particularly for general-purpose transactions (Chainalysis Team, 2024).

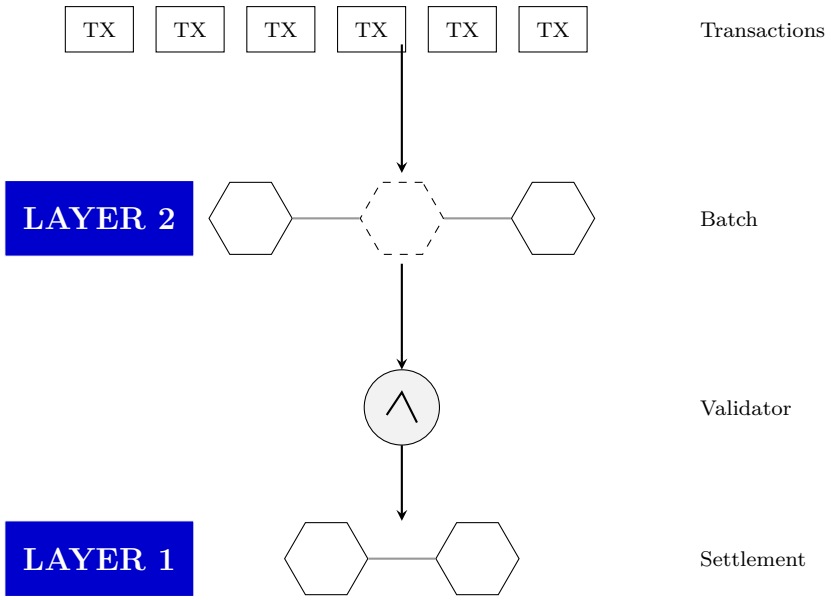

Figure 7: Layer-2 rollup architecture: Transactions are generated by users (TX), batched off-chain in Layer 2, validated, and finally committed to Layer 1 for secure settlement.

By enabling Optimistic Rollups by default, OpenBridge ensures maximum scalability and cost-efficiency for everyday retail cross-border payments. Meanwhile, ZK-Rollups are made available for users who require enhanced privacy, such as in corporate settlements or jurisdictions with heightened data protection requirements. Both rollup types ultimately anchor their final states to the permissioned Layer-1 blockchain, maintaining the protocol's integrity, security, and compliance posture.

3.3 Zero-Knowledge Proof (ZKP) Integration

In traditional payment networks, users often trade privacy for access. Transaction data is visible to either centralized intermediaries or, in the case of public ledgers, to anyone with a block explorer. For a protocol like OpenBridge, which seeks to bridge consumer-level usability with institutional-grade compliance, confidentiality cannot be an afterthought. This is why we have integrated Zero-Knowledge Proofs in our prototype.

Zero-Knowledge Proofs (ZKPs) are cryptographic techniques that allow one party (the prover) to prove to another (the verifier) that a specific statement is true without revealing the underlying data. In practical terms, it's like proving a transaction meets compliance rules without exposing the actual transaction. ZKPs function by encoding rules (e.g. AML/KYC checks, value ranges, sanctioned lists) into a mathematical circuit. The prover generates a proof showing that the transaction satisfies those rules. The verifier checks the proof, without ever seeing the transaction data itself. This balance of privacy and verifiability is what makes ZKPs powerful for cross-border payments where trust, regulation, and confidentiality must coexist.

While zk-SNARKs are widely used in blockchain protocols (e.g., Zcash, Polygon Hermez), *OpenBridge* instead adopts the zk-STARKs variant. The rationale for this choice is twofold:

- **Scalability:** STARK-based proofs are highly parallelizable and optimized for larger data sets—ideal for OpenBridge's rollup architecture, which must handle thousands of transactions per batch (StarkNet Foundation, 2024).

- **Speed and Simplicity:** zk-STARKs are non-interactive and do not rely on elliptic curve cryptography, making them faster, quantum-resistant, and easier to implement securely in real-world applications (Cyfrin Team, 2023).

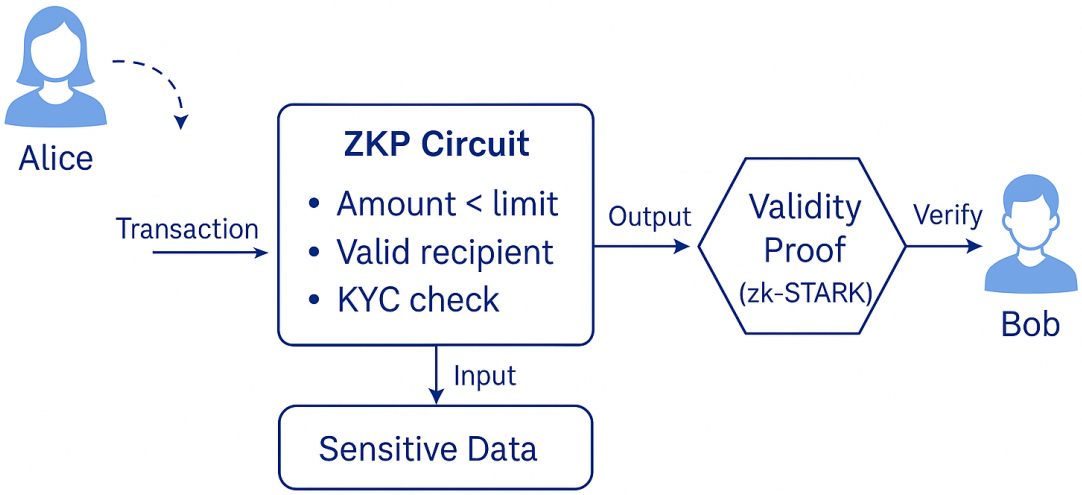

Figure 8: ZKP circuit logic for validating a payment transaction using zk-STARKs

Figure 8 illustrates the privacy-preserving validation flow in OpenBridge using Zero-Knowledge Proofs (ZKPs). In this architecture, Alice initiates a transaction to Bob. Instead of submitting raw transaction data, Alice passes the transaction through a predefined ZKP circuit, which verifies key conditions such as ensuring the transfer amount is within prescribed limits, that the recipient is valid, and that appropriate KYC checks are met.

Sensitive data such as Alice's identity or transaction metadata is processed internally as input to the circuit but is never revealed externally. The circuit then outputs a zk-STARK-based *validity proof*, which confirms that all conditions were met without disclosing the underlying data. This proof is then submitted to a validator node, which verifies the cryptographic integrity and authorizes the transaction. If valid, Bob receives the funds instantly.

At no point do Bob or the validators gain access to Alice's sensitive information. They only receive a cryptographic proof confirming that all compliance checks have been met. This approach preserves user privacy while maintaining institutional trust, regulatory compliance, and overall system integrity.

3.4 Multi-Currency Smart Contract and FX Mechanism

In the context of cross-border payments, exchange rate execution and settlement is one of the most complex and cost-intensive layers. OpenBridge addresses this by integrating a Multi-Currency Smart Contract Layer, drawing conceptual inspiration from the IMF's *Multi-Currency Exchange and Contracting Platform* (Adrian et al. (2022)) and the BIS's *Project Dunbar* (BIS Innovation Hub (2022)). These initiatives outline programmable frameworks for FX settlement, where smart contracts govern the rules for how and when currencies are exchanged between parties. This programmable structure enables condi-

tional settlements, compliance automation, and consistent FX execution[4] [5], all of which are critical to the retail remittance corridors OpenBridge is designed to serve.

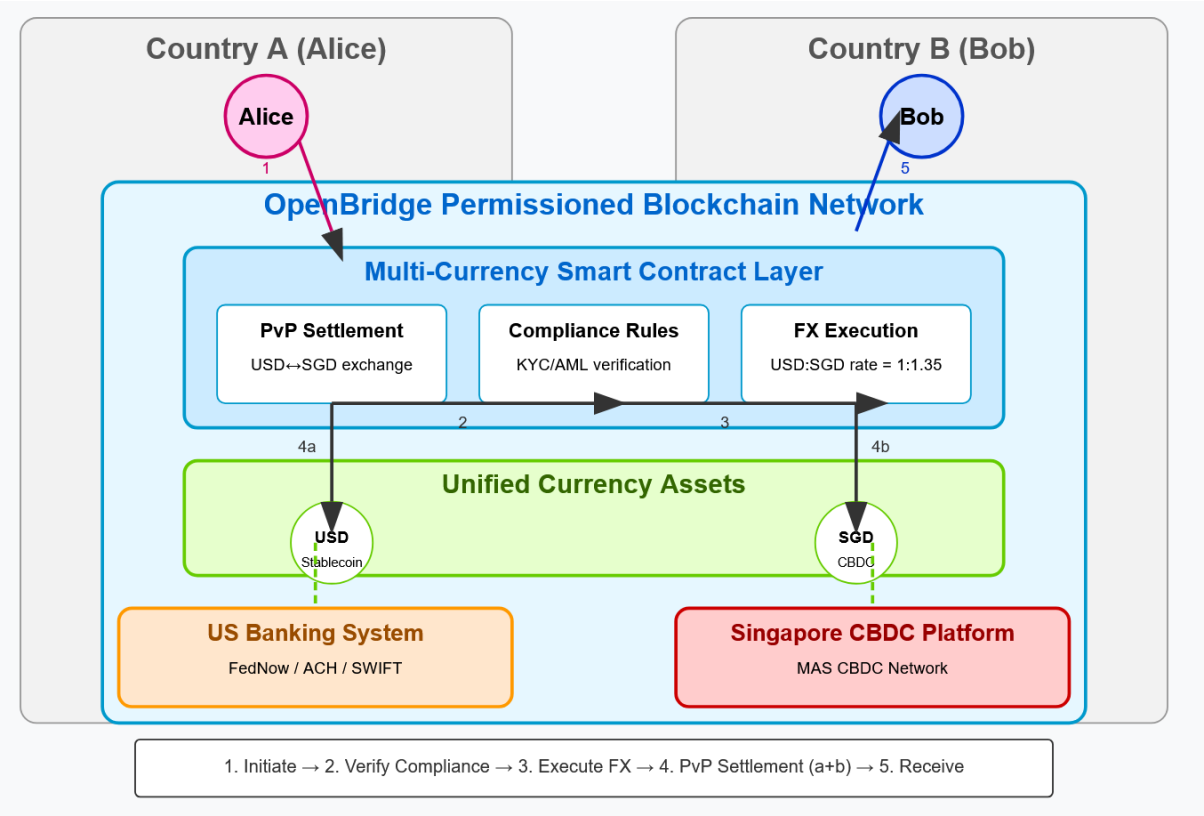

Figure 9: OpenBridge Multi-Currency Smart Contract Workflow. This diagram illustrates how OpenBridge facilitates a cross-border payment from Alice (Country A) to Bob (Country B) via its permissioned blockchain network. The Multi-Currency Smart Contract Layer handles compliance checks, FX rate execution, and atomic PvP settlement between USD and SGD.

In the OpenBridge architecture, all fiat-pegged stablecoins and CBDCs used for cross-border payments are issued and maintained on a shared, permissioned blockchain network. This unified infrastructure allows smart contracts to manage the exchange and settlement of currencies directly, without relying on intermediaries or coordinating across separate platforms. For instance, Payment-versus-Payment (PvP) conditions can be programmed into the contract to ensure both sides of a currency exchange are settled at the same time. This reduces the risk of one party defaulting or a partial settlement occurring. When assets are bridged in from external networks—such as legacy blockchains or national CBDC platforms—OpenBridge can still enforce FX settlement through smart contracts. However, these interactions involve more technical complexity. In such cases, the contracts use tools like timelocks and hashlocks to coordinate the process and protect against disputes, timeouts, or failed delivery (BIS Innovation Hub (2022)).

[4]Project Dunbar by the BIS demonstrates how CBDCs and tokenised assets can be settled atomically across borders via smart contracts operating on a common ledger.

[5]The IMF's proposal outlines an architecture for multi-currency contract execution that leverages programmable logic for real-time FX conversion and settlement.

3.5 Fee Mechanism and Exchange Rate Architecture

3.5.1 Foreign Exchange Mechanism

In most DeFi environments, foreign exchange rates are determined either through automated market makers (AMMs) or decentralized oracle networks. OpenBridge takes a different route rather than defaulting to these models. While AMMs are algorithmically elegant, they often suffer from slippage, price volatility, and impermanent loss, which don't suit predictable, low-cost cross-border payments like OpenBridge.

To address this, OpenBridge uses a limited centralized oracle model. FX rates are sourced in real time from a consortium of regulated liquidity providers, central banks, and institutional FX markets. This design draws justification from BIS's analysis of the oracle problem in DeFi (Duley et al. (2023)), which highlights how attempts to decentralize oracle design often degrade system efficiency, increase cost, and expose users to manipulation. In fact, Garratt and Monnet (2022) argue that ensuring honest reporting in a decentralized setting may be logically impossible when there's no single source of authoritative truth.

Within OpenBridge, the FX oracle layer is managed by the same consortium of regulated financial institutions that validate transactions on the Layer-1 blockchain. These oracles are subject to compliance, auditability, and reputational accountability—features that make them well-suited for providing institutional-grade FX pricing. Real-time exchange rates are fetched from interbank FX data feeds and published to the blockchain through signed, timestamped messages verified by multiple oracle nodes.

3.5.2 Fee Calculation and Distribution

Each FX rate applied to a transaction includes a transparent markup (e.g., 0.25–0.50%) which is explicitly displayed to users prior to confirming a transfer. This markup is embedded within the smart contract logic at the point of execution, ensuring full visibility and eliminating the risk of hidden fees. For retail users navigating remittance corridors or small business payments, this pricing transparency builds long-term trust and supports regulatory compliance—particularly important during periods of high volatility or currency stress.

OpenBridge applies a dual-fee model designed to ensure the platform's sustainability while aligning incentives across all participants involved in the payment lifecycle:

- **Base Transaction Fee:** A minimal Layer-1 fee for validating and confirming transactions on the permissioned blockchain. This fee compensates validator nodes for their role in maintaining network compliance, integrity, and security.
- **FX Spread Fee:** A programmable markup on the exchange rate, typically 25–50 basis points. This spread dynamically adjusts based on market volatility, liquidity, and transaction volume, and is computed using data provided by the oracle consortium.

The total fees collected are distributed among the following stakeholders:

- **Validators:** Receive a portion of the base transaction fee as compensation for processing and confirming transactions.

- **Liquidity Providers:** Earn a share of the FX spread in return for offering consistent, low-slippage exchange execution.
- **Protocol Treasury:** Retains approximately 5–10% of total fees to fund ongoing development, operational costs, or serve as an insurance buffer to absorb rare but severe FX slippage events.

3.6 Interoperability Standards

OpenBridge is built to integrate smoothly with both existing financial infrastructure and emerging digital networks. Its architecture aligns with ISO 20022 messaging standards, enabling direct compatibility with SWIFT and other legacy banking systems. At the same time, it supports interaction with digital assets like stablecoins and central bank digital currencies (CBDCs), ensuring operational flexibility as the financial landscape evolves. Drawing conceptual influence from BIS's mBridge project, OpenBridge is designed to support cross-border value transfer between jurisdictions without forcing institutions to overhaul their existing systems.

4 Transaction Flow Using OpenBridge

To demonstrate OpenBridge's end-to-end process in a real-world remittance use case, we present a cross-border transaction involving Alice in Brazil and Bob in Nigeria. The protocol leverages a permissioned blockchain with Proof-of-Authority consensus, Layer-2 rollups, zero-knowledge proofs, and a multi-currency smart contract system to ensure privacy, compliance, and cost-efficiency.

4.1 Alice-to-Bob: Brazil to Nigeria Case

1. **Transaction Initiation**
   - Alice initiates a cross-border payment to Bob, specifying the amount in BRL (Brazilian Real) to be converted into NGN (Nigerian Naira).
   - Alice selects either:
     - *Default Rollup Mode* (Optimistic Rollup) for low-cost and fast retail transfer, or
     - *Privacy Mode* (zk-Rollup) if enhanced confidentiality is required.
2. **KYC/AML Verification via ZKP**
   - Alice's wallet submits her identity and transaction details to a ZKP circuit.
   - The circuit checks:
     - KYC/AML compliance.
     - Sanction lists.
     - Transfer limits or thresholds.
   - A zk-STARK proof confirms compliance without revealing details.
3. **FX Rate Request and Locking**

- The system queries the centralized FX oracle layer, which fetches real-time USD/BRL and USD/NGN rates from institutional data feeds.
- The best available rate is published on-chain with a 0.25–0.50% markup, verifiable via a signed, timestamped oracle message.
- The smart contract locks in the FX rate and displays it to Alice for approval.

4. **Transaction Batching (Layer-2 Rollup)**
   - Alice's transaction is added to a batch:
     - In *Optimistic Rollup*, assumed valid unless challenged.
     - In *zk-Rollup*, a validity proof is pre-generated.
   - The batch is aggregated off-chain along with other user transactions.
5. **Batch Submission to Layer-1**
   - The batched transactions are committed to the permissioned Layer-1 blockchain.
   - Validator nodes (regulated banks, PSPs, etc.) verify:
     - zk-STARK compliance proof (if applicable).
     - Valid FX rate lock and fees.
   - Upon validation, the transaction gains final settlement status.
6. **PvP Smart Contract Execution**
   - The multi-currency smart contract executes a *Payment-versus-Payment (PvP)* exchange:
     - BRL is tokenized or withdrawn from Alice's wallet (via fiat stablecoin or CBDC).
     - NGN is credited to Bob's wallet.
     - Both transfers are atomic and conditional, preventing partial settlement.

4.2 Transaction Cost Breakdown

In this hypothetical transaction, Alice initiates a cross-border payment of 100 BRL to Bob via the OpenBridge protocol. The BRL is exchanged into USD at a base rate of 1 BRL = 0.20 USD, resulting in a nominal amount of 20 USD. An FX spread fee of 0.50% is applied, adding a 0.10 USD markup to the exchange rate. Additionally, a base Layer-1 transaction fee of 0.50 USD is charged to cover validation, compliance, and settlement costs. Thus, the total fees amount to 0.60 USD, and Bob ultimately receives the equivalent of 19.40 USD in NGN. The collected fees are then distributed among stakeholders.

Table 4: Hypothetical Fee Distribution for a 100 BRL Transaction

Stakeholder	**Amount (USD)**	**Purpose / Notes**
Validators	0.40	For verifying compliance, executing smart contracts, and maintaining the integrity of the network.
Liquidity Providers	0.08	For offering real-time exchange execution with low slippage across currency pairs.
Protocol Treasury	0.12	Reserved for development, operational sustainability, and as an insurance buffer during FX volatility.
Total Fees Collected	**0.60**	—

5 Conclusion

We have proposed a cross-border framework minimizing trust reliance without sacrificing regulatory integrity. Designed to be low-cost, globally accessible, and free from unnecessary intermediaries, OpenBridge reimagines how value moves across borders. By combining zero-knowledge proofs, a multi-currency smart contract layer, and programmable execution within a permissioned Proof-of-Authority network, the protocol ensures compliance, privacy, and finality in a single architecture. Validators do not compete for block rewards, nor are they anonymous; instead, they earn legitimacy through regulatory accountability and reputational risk. In this design, rules are enforced not by faith, but by embedded cryptographic logic, offering a robust alternative to the inefficiencies of both traditional rails and unconstrained DeFi systems.

References

Adrian, T., Grinberg, F., Mancini Griffoli, T., Townsend, R. M., and Zhang, N. (2022). A multi-currency exchange and contracting platform. *IMF Working Paper*, 2022(217):1–57. [Online]. Available at: `https://www.elibrary.imf.org/view/journals/001/2022/217/article-A001-en.xml` (Accessed: 5 April 2025).

Bank for International Settlements (2023). Project mbridge: connecting economies through cbdc. Technical report, BIS Innovation Hub. [Online]. Available at: `https://www.bis.org/publ/othp59.pdf` (Accessed: 5 April 2025).

BIS Innovation Hub (2022). Project dunbar: International settlements using multi-cbdcs. [Online]. Available at: `https://www.bis.org/about/bisih/topics/cbdc/dunbar.htm` (Accessed: 4 April 2025).

Buterin, V. (2017). On the blockchain scalability trilemma. [Online]. Available at: `https://vitalik.eth.limo/general/2017/12/31/sharding_faq.html` (Accessed: 5 April 2025).

Buterin, V. (2021). A rollup-centric ethereum roadmap. [Online]. Available at: `https://ethereum-magicians.org/t/a-rollup-centric-ethereum-roadmap/4698` (Accessed: 4 April 2025).

Chainalysis Team (2024). Zk vs optimistic rollups: A developer's overview. [Online]. Available at: `https://www.chainalysis.com/blog/zero-knowledge-rollups-optimistic-rollups-overview/` (Accessed: 4 April 2025).

Citi Research (n.d.). Digital money: Tokenisation, payments and the future of financial infrastructure. Technical report, Citi Research. [Online]. Available at: `https://www.citifirst.com.hk/home/upload/citi_research/rsch_pdf_30185684.pdf` (Accessed: 5 April 2025).

Committee on Payments and Market Infrastructures (2020). Enhancing cross-border payments: Building blocks of a global roadmap. Technical report, Bank for International Settlements. [Online]. Available at: `https://www.bis.org/cpmi/publ/d193.pdf` (Accessed: 5 April 2025).

Committee on Payments and Market Infrastructures (2023). Exploring multilateral platforms for cross-border payments. Technical report, Bank for International Settlements. [Online]. Available at: `https://www.bis.org/cpmi/publ/d213.pdf` (Accessed: 5 April 2025).

Cyfrin Team (2023). A full comparison: What are zk-snarks and zk-starks? [Online]. Available at: `https://www.cyfrin.io/blog/a-full-comparison-what-are-zk-snarks-and-zk-starks` (Accessed: 5 April 2025).

Duley, C., Gambacorta, L., Garratt, R., and Koo Wilkens, P. (2023). The oracle problem and the future of defi. Technical Report 76, Bank for International Settlements. [Online]. Available at: `https://www.bis.org/publ/bisbull76.htm` (Accessed: 5 April 2025).

Garratt, R. and Monnet, C. (2022). An impossibility theorem on truthful reporting in fully decentralized systems. [Online]. Available at: https://ssrn.com/abstract=4017963 (Accessed: 6 April 2025).

Kim, S., Deka, G. C., and Zhang, P. (2019). Role of blockchain technology in iot applications. In *Advances in Computers*, volume 115, pages 181–209. Academic Press, United States. [Online]. Available at: https://www.oreilly.com/library/view/role-of-blockchain/9780128171929/ (Accessed: 5 April 2025).

Kraken (n.d.). Stellar vs. ripple: What's the difference? [Online]. Available at: https://www.kraken.com/compare/stellar-vs-ripple (Accessed: 6 April 2025).

MIT Digital Currency Initiative (2022). Opencbdc: Building an open source platform for central bank digital currency (cbdc). [Online]. Available at: https://dci.mit.edu/opencbdc (Accessed: 3 April 2025).

Montelibero (2024). Stellar blockchain: A comprehensive overview. [Online]. Available at: https://montelibero.org/2025/04/02/stellar-blockchain-a-comprehensive-overview-eng/ (Accessed: 5 April 2025).

StarkNet Foundation (2024). Recursive starks and their role in scaling ethereum. [Online]. Available at: https://www.starknet.io/blog/recursive-starks (Accessed: 5 April 2025).

Stellar Development Foundation (2021). The story of 2021: Stellar's year in review. [Online]. Available at: https://stellar.org/blog/foundation-news/the-story-of-2021 (Accessed: 6 April 2025).

Stellar.org (2016). Stellar consensus protocol explained. [Online]. Available at: https://stellar.org/learn/stellar-consensus-protocol (Accessed: 6 April 2025).

Stellar.org (n.d.). What is lumen (xlm)? [Online]. Available at: https://stellar.org/learn/lumens (Accessed: 5 April 2025).

World Bank (2023). Remittance prices worldwide: Quarterly report q4 2023. Technical report, World Bank. [Online]. Available at: https://remittanceprices.worldbank.org/sites/default/files/rpw_main_report_and_annex_q423_final.pdf (Accessed: 3 April 2025).