Finternet - Approach for Interoperability across Unified Ledgers

October 2024

Authors
Sriram Venkateswaran, CTPO - rootPe
Jay Prakash, Co-Founder & CEO - Silence Laboratories
Prabal Banerjee, Co-Founder - Avail

This is a draft concept paper, inspired by Agustín Carstens and Nandan Nilekani's Finternet: The Financial System of the Future. We welcome any feedback to help strengthen and refine the concepts presented in the paper. Please feel free to share your feedback at sriram@rootpe.com.

We extend our gratitude to the volunteers of Finternet and the team members of Rootpe, Avail, and Silence Laboratories for their valuable contributions to this paper.

Contents

1 Abstract **2**

2 Introduction **2**

3 The Problem Statement – Seamless and Trusted Interoperability across Unified Ledgers **3**

4 System Design **4**

4.1 Trust-minimized Blockchain-based Interoperability 4

4.2 Interchain Messaging Solution - Forex Transfer as an usecase 6

4.3 Privacy Preserving Compliance Verification Messaging in Forex 10

5 Conclusion **12**

Abbreviations

Abbreviation	Definition
AML	Anti Money Laundering
DeFi	Decentralized Finance Institute
EVM	Ethereum Virtual Machine
Forex	Foreign Exchange
ID	Identification
KYC	Know Your Customer
MPC	Multi Party Computation
NFT	Non-Fungible Token
NIN	Nigeria's National Identification Number
OLE	Oblivious Linear Evaluation
P2M	Person-to-Merchant
P2P	Peer-to-Peer
PSI	Private Set Intersection
QR Code	Quick Response Code
SGD	Singapore Dollar
SIM	Subscriber Identity Module
SWIFT	Society for Worldwide Interbank Financial Telecommunication
UL	Unified Ledger
UPI	Unified Payments Interface
USD	United States Dollar
Web3	Web 3.0 (Third Generation of the World Wide Web, often associated with decentralized internet)
ZK	Zero Knowledge

1 Abstract

This paper presents a novel architectural approach for achieving interoperability across unified ledgers (ULs) in the Finternet ecosystem, addressing the critical challenge of seamless communication between isolated financial systems. The proposed solution leverages public blockchain technology as a base layer, combined with zero-knowledge cryptography and secure multi-party computation (MPC) to enable trust-minimized interactions while preserving privacy.

The architecture introduces a comprehensive framework comprising four key components: (1) independent unified ledgers capable of handling multiple tokenized assets, (2) proof generators with adapters for state validation, (3) a centralized proof aggregator hub for consolidating state updates, and (4) a message relayer system for cross-ledger communication. The paper demonstrates the framework's efficacy through a foreign exchange (Forex) transfer use case, illustrating how two distinct unified ledgers can securely exchange tokenized currencies while maintaining regulatory compliance.

Privacy preservation is achieved through advanced cryptographic methods, including Zero-Knowledge Proofs for state validation and Multi-Party Computation for sensitive operations such as sanctions list checking. The system enables financial institutions to verify transactions against sanctions lists without exposing sensitive payment information, while ensuring compliance with anti-money laundering (AML) regulations across jurisdictions.

This architecture represents a significant advancement in financial system interoperability, offering enhanced transaction speed, configurable flexibility, and robust security measures while maintaining the privacy requirements essential for global financial operations.

2 Introduction

The concept of Finternet, as introduced in the April 2024 white paper by Augustin Carstens and Nandan Nilekani, represents the next stage in the evolution of financial systems. It envisions a digital-first, tokenized

financial ecosystem, designed to put individuals and businesses at the heart of their financial activities. Built on unified ledgers, Finternet aims to enable new types of financial products and facilitate seamless transactions, driving inclusivity and efficiency across global markets. For this vision to be realized, seamless interoperability between various unified ledgers is essential. Independent and isolated financial networks are insufficient. The true potential of Finternet lies in the ability of these systems to communicate, transact, and share information with one another in a trusted, efficient, and secure manner. At the same time, in today's digital age, where transactions often expose individuals to potential risks, ensuring privacy and data protection is of utmost importance.

This paper proposes an approach for achieving interoperability across these unified ledgers, leveraging advanced cryptographic technologies such as zero-knowledge proofs and secure multi-party computation. These technologies enable seamless communication between ledgers while ensuring privacy by design. The goal is not only to safeguard sensitive information but also to allow transactions to be verified without revealing underlying details, fostering a trusted and transparent environment for financial interactions.

In this paper, we use tokenized currencies as an asset class and illustrate the approach with a Forex usecase between a Singapore Dollar (SGD) and a US Dollar (USD). However, the proposed approach can be applied to any tokenized asset class by incorporating the relevant regulations and compliance requirements of the respective jurisdiction at the unified ledger or wallet level.

This is an early exploration and a draft version of this approach. We seek feedback from the readers on their thoughts and any improvement to this approach.

3 The Problem Statement – Seamless and Trusted Interoperability across Unified Ledgers

In today's digital landscape, financial systems primarily operate on isolated ledgers or databases, often limited in their ability to communicate and scale efficiently. This isolation presents several key challenges that restrict innovation and prevent seamless storage / transfer of assets within financial services. Finternet addresses this fragmentation by creating an ecosystem that enhances accessibility, efficiency, and ease of use, building a financial services framework that is both scalable and adaptable to the diverse needs of individuals, businesses, and organizations worldwide.

Finternet aims to establish a universal approach to finance by focusing on unification across asset classes, sectors, and geographies. Inspired by how the internet connects different systems, networks, and applications, Finternet envisions a similar interoperable framework for financial ecosystems, allowing various financial services to communicate and collaborate seamlessly, irrespective of their underlying technology. This universal system supports both retail and wholesale financial transactions across different platforms while adhering to regulatory requirements.

At the heart of Finternet's vision is interoperability—ensuring, much like the internet, that financial systems can work together regardless of their design or infrastructure. To achieve this objective, we identify three essential elements needed to create an interconnected financial ecosystem:

. **Seamless and Scalable Communication:** Financial systems need the capacity to exchange information and assets across diverse infrastructures. This challenge requires the development of standardized, interoperable protocols that enable different financial platforms to interact seamlessly, ensuring frictionless communication across systems. Additionally, this communication framework must be scalable, supporting high transaction volumes and efficient cross-platform interactions.

. **Trust-Minimized Interactions:** Reducing reliance on intermediary trust structures is essential for increasing efficiency and minimizing friction in financial interactions. Finternet emphasizes trust-minimized communication, enabling systems to interact with minimal reliance on intermediaries or centralized controls. This approach reduces systemic risk and increases transaction speed, enhancing the overall resilience and efficiency of the financial ecosystem.

. **Privacy Preservation:** In an interconnected ecosystem, preserving user privacy is critical. Finternet aims to implement privacy-preserving protocols that allow secure exchanges of information and assets between systems without exposing sensitive user data, ensuring that privacy remains intact throughout these interactions.

This paper presents a strategic approach to addressing these core elements—scalable communication, trust-minimized interactions, and privacy preservation—proposing a structure capable of handling a broad range of transactions while maintaining regulatory compliance. By focusing on these components, Finternet is positioned to revolutionize the future of global finance, unlocking new opportunities for innovation, inclusivity, and growth.

4 System Design

Interoperable systems have proven to be a key driver of scalability and success across various industries, from digital payments to identity verification. Numerous success stories highlight the transformative impact of such systems. For instance, the Unified Payments Interface (UPI) in India enables instant money transfers between different banks on a single platform. Regardless of the bank or payment app a user selects, UPI facilitates seamless peer-to-peer (P2P) and person-to-merchant (P2M) transactions across various platforms. By allowing banks and payment service providers to operate on a common network, UPI has created a frictionless experience, propelling India into the global digital payment landscape, processing over 15 billion[1] transactions monthly as of September 2024.

Other examples include Nigeria's verifiable digital identity system (NIN), which has enrolled over 100 million[2] people and is used at scale for low-cost SIM card registration, bank account opening, travel authorization, and more. Thailand's fast payments scheme, PromptPay, has deployed an interoperable QR code infrastructure that has scaled to 3.7 million merchants, compared to just 140,000 merchants accepting debit/credit cards[3]. Singapore is implementing a digital ID and credentials infrastructure called Singpass, which drives efficiency using digital ID[4].

Similarly, in the Web3 world, interoperability is the backbone of scalability, enabling the seamless movement of funds, assets, and NFTs across different blockchains. By facilitating cross-chain communication and asset transfers, interoperable systems are allowing the Web3 ecosystem to grow exponentially. Whether through cross-chain DeFi platforms, NFT marketplaces, or decentralized applications, interoperability ensures that Web3 can scale efficiently, making it more accessible to users, developers, and businesses alike.

This paper presents an approach by examining various large-scale interoperability models within regulated environments, exploring recent advancements in the Web3 ecosystem, and leveraging the latest cryptographic technologies to ensure privacy and security.

4.1 Trust-minimized Blockchain-based Interoperability

The proposed architecture enables connectivity between multiple independent Unified Ledgers (ULs) using cryptographic proofs (including but not limited to aggregated Zero Knowledge Proofs) of their state updates. The paper demonstrates this interoperability through a Foreign Exchange transfer use case between two accounts on distinct currency ULs. An independent entity provides liquidity and exchange rates (the detailed operation of this Forex transfer entity is beyond the scope of this paper).

Messaging Architecture

The ULs communicate with each other in a trust-minimized manner using a Messaging Protocol (MP). The protocol relies on verification of cryptographic proofs, such as validity proofs and zero-knowledge proofs (ZKPs), to ensure mathematical security of transmitted messages. This section describes the various components of the architecture, their roles, and the sequence of actions that enable message passing.

[1] https://www.npci.org.in/what-we-do/upi/product-statistics
[2] https://nimc.gov.ng/enrolment-dashboard-december-2023/
[3] https://www.bot.or.th/en/statistics/payment.html
[4] https://www.developer.tech.gov.sg/products/categories/digital-identity/singpass/overview.html

Components

Unified Ledger

- A Unified Ledger can be implemented either as a standalone system or based on established blockchain technologies such as Ethereum, Solana, Cord Protocol, etc., and can utilize any execution environment like EVM, SVM, or an application-specific runtime.
- A Unified Ledger can maintain various tokens representing assets and currencies, including fungible, non-fungible, or other token representations.
- The state of an active Unified Ledger can be represented and updated as a Rollup (a condensed state change of a Unified Ledger over time) to a Data Availability layer (a blockchain network dedicated to storing data published by Rollups) to ensure Rollup safety, liveness, and verifiability.

Proof Generator and Adapter

- The Proof Generator is responsible for generating a validity proof of the Unified Ledger's state change over a period. These proofs are generated based on the UL's State Transition Function (STF), which defines the runtime of the UL.
- The Adapter transforms these proofs into a format that the Proof Aggregator Hub can interpret and aggregate. This ensures that despite different ULs potentially using different proof systems, the Hub receives homogeneous proofs for efficient verification and aggregation.

Proof Aggregator Hub

- The Proof Aggregator Hub serves as a central repository where all Unified Ledgers post their current state and valid proofs of state changes.
- The Proof Aggregator Hub generates a Unified State Update Proof by combining the State Update Proofs from various Unified Ledgers.
- Any entity can verify the correctness of a Unified Ledger by verifying the proofs and the data available in the Data Availability layer against the state of the Proof Aggregator Hub.

Message Relayer

- The Message Relayer leverages the verified state information of Unified Ledgers in the Proof Aggregator Hub to transfer and prove messages across different Unified Ledgers.
- A message from one entity on a source Unified Ledger addressed to another entity on a destination Unified Ledger can be propagated with a valid state proof, enabling action execution in the destination UL.
- Financial settlements can be modeled as a series of verifiable messages and acknowledgments transported by the Messaging Protocol.

The Sequence of Actions

- A batch of transactions are processed in UL A which results in change of state. Some of these transactions can result in messages being sent as data from a source entity to a different entity on another UL B. These messages can be stored in an Outbox application as part of UL A's state.
- The batch of transactions are sent to the Data Availability layer for ordering and publishing.
- The Proof Generator registers this batch of transactions and generates a proof against the new state. The Adapter propagates this proof to the Hub. This is repeated by the Adapters of all the Unified Ledgers.

- The Proof Aggregator Hub verifies each UL's State Update Proof against the Data Availability layer and creates a consolidated state of all verified ULs.
- The Message Relayer listens to all the data sent as Messages in the updated state of different ULs and forwards them to the destination ULs as verified Message transactions.
- The receiving entity verifies the message against the Unified State and takes the appropriate action based on the content. It may optionally send a acknowledgment message to the source.

A visual representation of the above flow is shown in Fig. 1

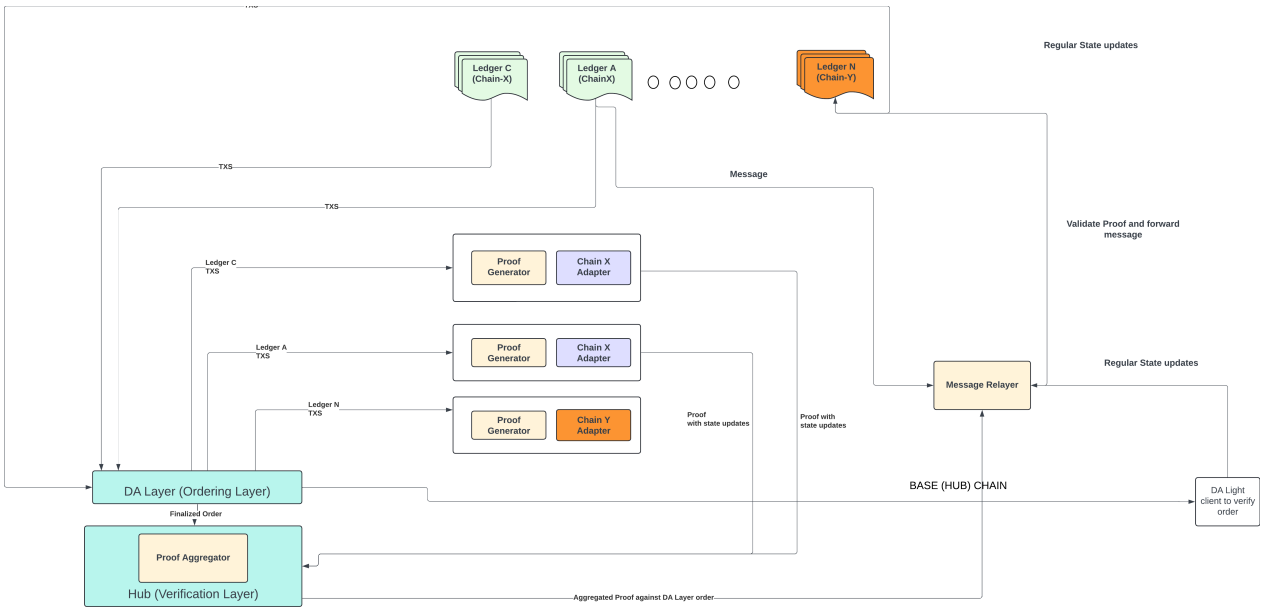

Figure 1: Propagation of State Proofs and Messages across Unified Ledgers

Proof Systems

The proofs used to verify the state updates of Unified Ledgers are validity proofs or Zero Knowledge Proofs. A succinct proof of execution of a Unified Ledger is generated by the Adapter depending on the Virtual Machine or Execution Environment and the State Tree representation of the UL. A typical state representation could be a Merkle-Patricia Trie which is a Merkelized Trie of all the keys and values used to represent the State data as used in Ethereum Node implementations. When given an ordered set of state changing operations and the State Tree Roots before and after the change, the cryptographic proof is able to mathematically prove that the state change is accurate. This proof is further aggregated with proofs of other ULs to generate a consolidated proof of all state updates.

The updated State Root in earlier paragraph holds the key to verify any structured data on the ULs. A Merkle proof of inclusion of any message object existing in the Storage Tree can be generated by the Message Realyer client with access to the UL's data. The message object thus encoded in the state storage format, the Merkle root of the State Tree and the Merkle proof linking the two, is enough for any other UL to verify that the Message is accurate and executed on the source UL. The Merkle verification can be performed efficiently quickly as a part of message relay within the destination UL's Virtual Machine or execution environment.

4.2 Interchain Messaging Solution - Forex Transfer as an usecase

In this paper the suggested architecture extends to enable interoperability across various token types on two or more Unified Ledgers (ULs), regardless of their underlying blockchain. Here, we illustrate a foreign

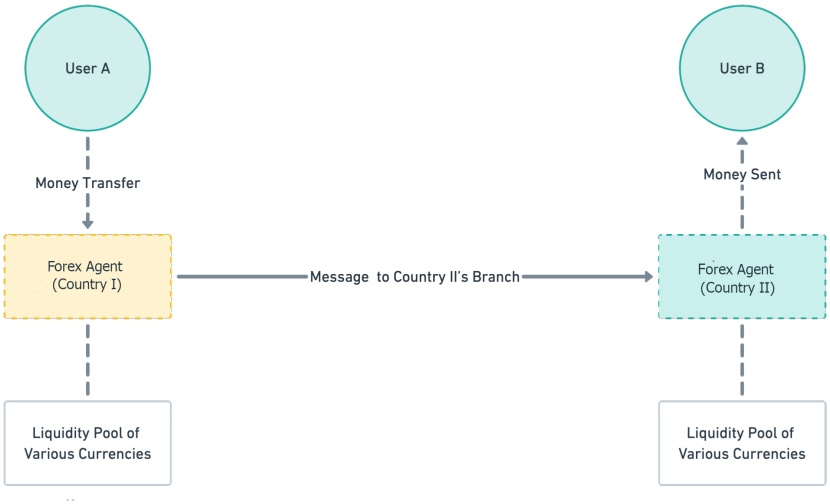

Figure 2: Foreign Exchange Transfers

exchange (Forex) transfer as a model for communication and settlement between two interoperable ULs, each holding distinct tokenized currencies.

Typically, Forex transfers are facilitated by banks and financial institutions holding liquidity reserves across regions, setting exchange rates for conversions. Transfers occur as interbank messages relayed through protocols like SWIFT. In this model, we propose emulating this process as a direct token exchange between assets on different Unified Ledgers, with configurable exchange rates that adjust to market conditions.

Forex Transfer - Interchain Messaging Solution

The proposed solution involves a tokenized Forex exchange across Unified Ledgers, facilitated by an Interchain Messaging Protocol (IMP), enhancing the efficiency and security of cross-border currency transfers.

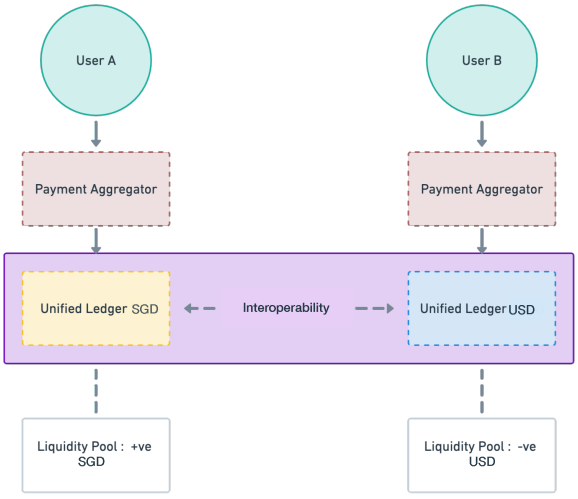

Figure 3: Forex Transfer with Interchain Messaging

Stakeholders

The proposed framework incorporates the following key stakeholders to enable secure and efficient currency transfers across the Finternet network:

- **User A:** An individual or institution aiming to transfer a specified amount in SGD to User B in USD.
- **User B:** An individual or institution designated to receive an equivalent amount in USD from User A.
- **Ledger A:** A Unified Ledger based in the EU, holding SGD and managed by a local financial institution.
- **Ledger B:** A Unified Ledger in India that holds USD, administered by a local financial institution.
- **Entity A:** An institution holding SGD on Ledger A, capable of initiating inter-ledger communications to Ledger B.
- **Entity B:** A subsidiary or partner of Entity A, authorized to receive messages from Entity A and facilitate the transfer to User B in USD.
- **Oracle B:** An on-chain price oracle on Unified Ledger B, managed by Entity B, which provides real-time SGD to USD conversion rates.

Flow

The Forex conversion process unfolds through the following steps, involving secure messaging and verification to ensure reliable and swift settlement:

1. **Initiation:** User A, holding SGD, decides to send 100 SGD to User B in USD.
2. **Deposit:** User A deposits SGD on Ledger A within the Unified Ledger network.
3. **Conversion Request:** User A requests Forex conversion from SGD to USD based on the rate provided by Oracle B, specifying User B as the recipient.
4. **Locking of Funds:** Entity A locks the specified SGD amount on behalf of User A.
5. **Message Dispatch:** Entity A sends a message to Entity B, requesting conversion and transfer of the equivalent USD to User B.
6. **Validation:** The hub verifies the State Update of Ledger A containing the conversion message.
7. **Message Relay:** The Interchain Messaging Protocol relays the message to Entity B with proof of the State Update.
8. **Proof Verification:** Entity B verifies the proof, ensuring it is addressed to them from Entity A.
9. **Execution:** Entity B calculates the equivalent USD based on Oracle B's rate and initiates the transfer to User B.
10. **Acknowledgment:** Entity B sends an acknowledgment message back to Entity A, confirming the transfer completion.
11. **Final Settlement:** The acknowledgment is relayed back to Entity A, releasing the locked SGD to complete the Forex conversion.

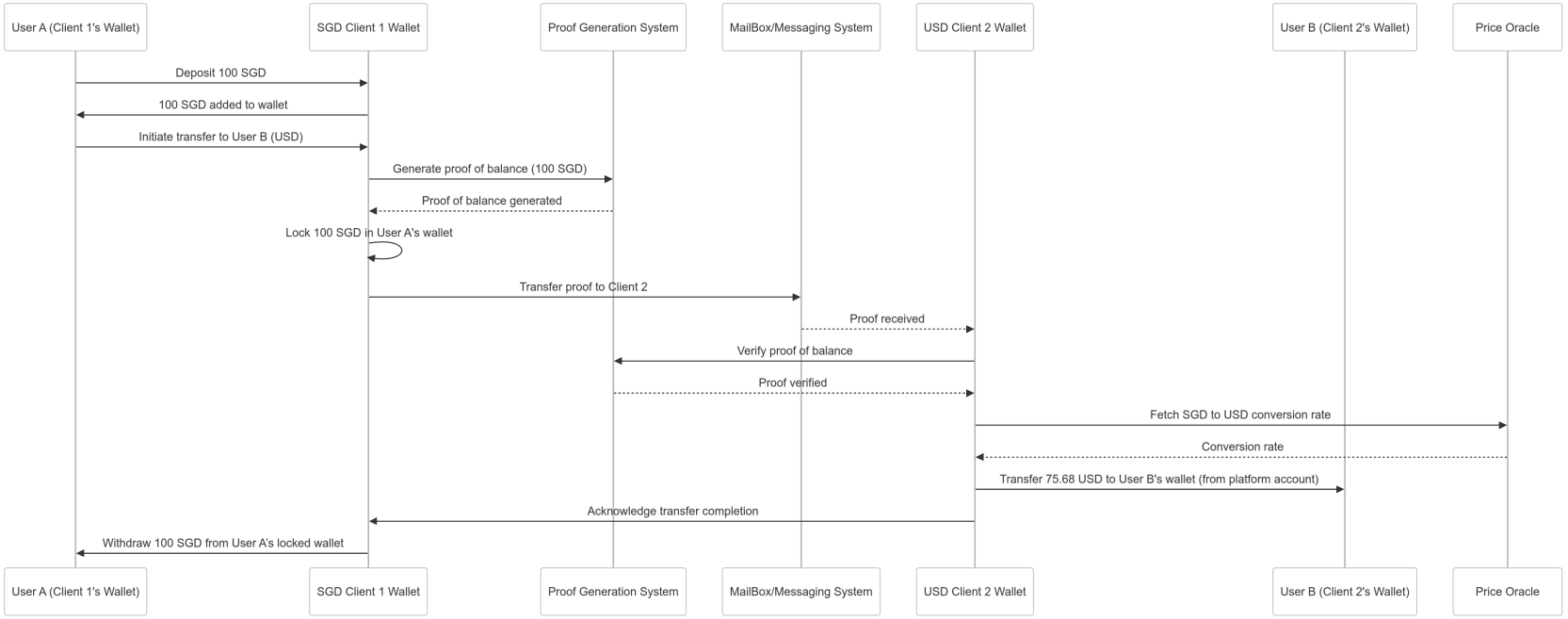

Figure 4: Forex Transfer Sequence Diagram

4.3 Privacy Preserving Compliance Verification Messaging in Forex

Cross-border foreign exchange transactions face heightened scrutiny due to concerns about money laundering, terrorism financing, and compliance with international sanctions. Financial institutions are required to screen payments against sanctions lists—governmental and international databases that identify individuals, organizations, or countries prohibited from accessing financial services. Although essential for compliance, sanctions screening presents serious privacy and data security issues. Cross-border payment systems require financial institutions to disclose sensitive details—such as sender, receiver, and transaction information—to multiple intermediaries, increasing the risk of data leaks and unauthorized access. Ensuring compliance without exposing personal information, particularly for those not on sanctions lists, remains a significant challenge.

Privacy-preserving technologies offer a secure way for institutions to conduct sanctions checks without disclosing sensitive payment information or violating data privacy. Techniques like Multi-Party Computation (MPC) and Zero-Knowledge Proofs (ZKP) allow multiple data owners to collaboratively compute results without revealing their private inputs, ensuring data confidentiality. These methods protect against data breaches, enhance compliance with AML and sanctions regulations, and build trust by limiting information access to authorized parties only. Furthermore, they facilitate cross-border compliance by enabling institutions to meet regulatory standards securely and efficiently across jurisdictions.

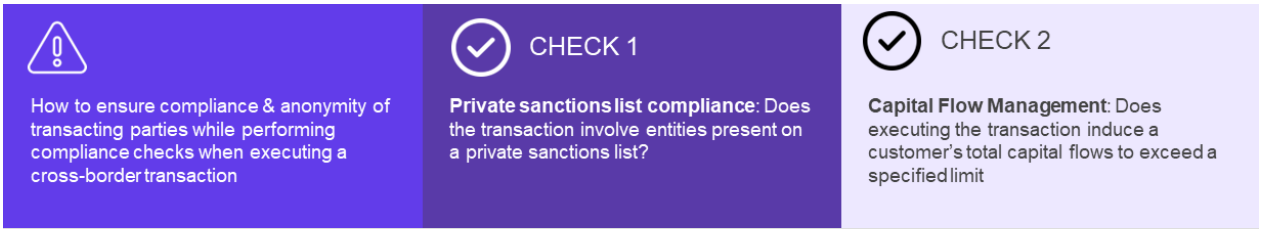

Figure 5: Defining the Problem Statement for Compliance check

As represented in Fig.5, jurisdiction-specific regulatory requirements, like sanctions screening and capital flow management (CFM), are key compliance measures. Finternet's FX module aims to enhance cross-border FX by increasing efficiency, transparency, and speed for large-value transactions, while adhering to strict regulatory standards. Using Privacy-Enhancing Technologies (PETs), Finternet automates compliance and clarifies country-specific policies, enabling each party in a transaction to conduct necessary checks seamlessly before funds are released. [Silence Laboratories(2024)] white paper gives details on the multi-party computation based privacy compliance verification algorithms as adopted in Finternet. It defines the protocols required for conducting Private Sanctions List checks, ensuring security against malicious adversaries who may attempt to deviate from the protocol. This protection follows the standard real-ideal model for MPC protocols [Canetti(2000), Canetti(2001)]. This paradigm assumes each protocol emulates an ideal oracle, accepting private inputs, performing the specified computation on the combined data, and returning only the final result without leaking intermediate states.

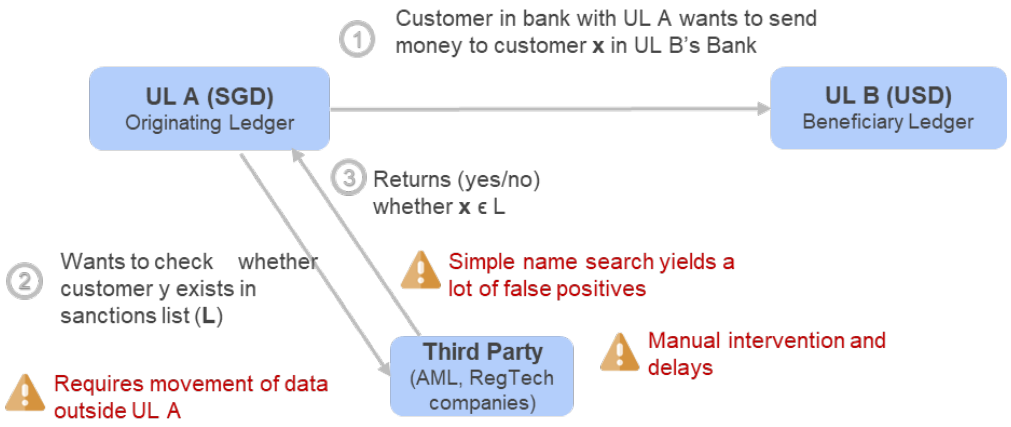

Figure 6: Existing flow of sanction list check and challenges there in

Privacy Preserving Sanction List Verification and Capital Flow Management

The Private Sanctions List check allows the originating bank or financial institution to confirm that the beneficiary does not appear on a sanctions list maintained by the beneficiary bank or institution. This protocol preserves the privacy of each party's inputs: the beneficiary bank receives no information about the transaction, and the originating bank learns only whether the beneficiary is on the sanctions list. For instance, if the beneficiary is listed, other names on the sanctions list remain obscured, appearing as random pseudonyms to the originating bank. The Capital Flow Management protocol allows an originating bank to confirm that a transaction will not cause the beneficiary's balance to surpass a predetermined limit. Each protocol is equipped with measures to identify and defend against active deviations. A dishonest party can only attempt a denial of service by withholding communication or causing an abort with an invalid message.

The secure computation for the Private Sanctions List check is based on Private Set Intersection (PSI), a well-explored problem in MPC. We implement this using a Diffie-Hellman-based PSI approach, which requires only elliptic curves and a hash function. In contrast, the Capital Flow Management check is more intricate, utilizing general-purpose MPC techniques. Central to this protocol is the secure comparison of private values, achieved by constructing the comparison circuit within an MPC framework. Implementing general MPC, especially with protections against active deviations, necessitates combining several advanced cryptographic methods.

[Silence Laboratories(2024)] gives details on the algorithms which enables both checks, as mentioned in this paper and as implemented for Finternet. It outlines multi-party computation based privacy compliance verification algorithms as adopted in Finternet. It outlines the protocols to be used for the Private Sanctions List check and CFM, offering security against malicious adversaries who may deviate from the protocol. This security is ensured within the standard real-ideal paradigm for MPC protocols. We follow a standard recipe for designing such protocols laid out in works such as BDOZ [Bendlin et al.(2011)], SPDZ [Damgård et al.(2012)], and MASCOT [Keller et al.(2016)]: an Oblivious Linear Evaluation (OLE) is used to generate so-called Beaver Triples along with corresponding Message Authentication Codes, which are then used to securely evaluate an arithmetic circuit in topological order. We make use of the arithmetic recurrence relation formulated by Garay et al. [Garay et al.(2007)] to implement a comparison circuit. Informed by efficiency tradeoffs established in the context of a widely deployed MPC-based tool—ECDSA signing—we utilize Oblivious Linear Evaluation (OLE) based on Oblivious Transfer (and its Extension [Ishai et al.(2003), Keller et al.(2015), Roy(2022)]), due to its relatively low computational footprint.

Key Benefits

- **Enhanced Speed:** Message delivery is significantly faster compared to current interbank transfer protocols.
- **Configurable Flexibility:** Tailored messaging protocols enable the design of advanced financial systems with high adaptability and security.
- **Privacy by Design:** Usage of PETs such as MPC for sensitive messages ensures privacy by design which would help in amplification of participation to Finternet, due to higher accuracy and faster settlements (as more inferences and messages could be shared now).

5 Conclusion

In this paper, we have introduced a robust methodology to unify states across multiple ledgers using Data Availability Layers and Zero-Knowledge Proof Adapters. This unified state forms the backbone of a Messaging Protocol capable of seamless data exchange between applications on different ledgers. Together, these technologies, augmented by Privacy Preservation techniques can help enable the Finternet vision for seamless connections and interchange of assets between multiple Unified Ledgers (ULs)

The Forex transfer scenario illustrates how interoperability within Finternet's framework can streamline foreign exchange operations across jurisdictions, enhancing efficiency and reducing systemic risk. By leveraging a Pricing Oracle, this model also highlights opportunities for dynamic pricing based on liquidity. The proposed messaging protocol can extend to additional financial applications, supporting transactions with speed, security, and reliability that meet the evolving demands of the global financial ecosystem.

References

[Bendlin et al.(2011)] Rikke Bendlin, Ivan Damgård, Claudio Orlandi, and Sarah Zakarias. 2011. Semi-homomorphic Encryption and Multiparty Computation. In *EUROCRYPT 2011 (LNCS, Vol. 6632)*, Kenneth G. Paterson (Ed.). Springer, Heidelberg, 169–188. https://doi.org/10.1007/978-3-642-20465-$4_1$1

[Canetti(2000)] Ran Canetti. 2000. Security and Composition of Multiparty Cryptographic Protocols. *Journal of Cryptology* 13, 1 (Jan. 2000), 143–202. https://doi.org/10.1007/s001459910006

[Canetti(2001)] Ran Canetti. 2001. Universally Composable Security: A New Paradigm for Cryptographic Protocols. In *42nd FOCS*. IEEE Computer Society Press, 136–145. https://doi.org/10.1109/SFCS.2001.959888

[Damgård et al.(2012)] Ivan Damgård, Valerio Pastro, Nigel P. Smart, and Sarah Zakarias. 2012. Multiparty Computation from Somewhat Homomorphic Encryption. In *CRYPTO 2012 (LNCS, Vol. 7417)*, Reihaneh Safavi-Naini and Ran Canetti (Eds.). Springer, Heidelberg, 643–662. https://doi.org/10.1007/978-3-642-32009-$5_3$8

[Garay et al.(2007)] Juan A. Garay, Berry Schoenmakers, and José Villegas. 2007. Practical and Secure Solutions for Integer Comparison. In *PKC 2007 (LNCS, Vol. 4450)*, Tatsuaki Okamoto and Xiaoyun Wang (Eds.). Springer, Heidelberg, 330–342. https://doi.org/10.1007/978-3-540-71677-$8_2$2

[Ishai et al.(2003)] Yuval Ishai, Joe Kilian, Kobbi Nissim, and Erez Petrank. 2003. Extending Oblivious Transfers Efficiently. In *CRYPTO 2003 (LNCS, Vol. 2729)*, Dan Boneh (Ed.). Springer, Heidelberg, 145–161. https://doi.org/10.1007/978-3-540-45146-4_9

[Keller et al.(2015)] Marcel Keller, Emmanuela Orsini, and Peter Scholl. 2015. Actively Secure OT Extension with Optimal Overhead. In *CRYPTO 2015, Part I (LNCS, Vol. 9215)*, Rosario Gennaro and Matthew J. B. Robshaw (Eds.). Springer, Heidelberg, 724–741. https://doi.org/10.1007/978-3-662-47989-$6_3$5

[Keller et al.(2016)] Marcel Keller, Emmanuela Orsini, and Peter Scholl. 2016. MASCOT: Faster Malicious Arithmetic Secure Computation with Oblivious Transfer. In *ACM CCS 2016*, Edgar R. Weippl, Stefan Katzenbeisser, Christopher Kruegel, Andrew C. Myers, and Shai Halevi (Eds.). ACM Press, 830–842. https://doi.org/10.1145/2976749.2978357

[Roy(2022)] Lawrence Roy. 2022. SoftSpokenOT: Quieter OT Extension from Small-Field Silent VOLE in the Minicrypt Model. In *CRYPTO 2022, Part I (LNCS, Vol. 13507)*, Yevgeniy Dodis and Thomas Shrimpton (Eds.). Springer, Heidelberg, 657–687. https://doi.org/10.1007/978-3-031-15802-$5_2$3

[Silence Laboratories(2024)] Silence Laboratories. 2024. Multiparty Computation Protocols for Private Compliance Checks. https://www.silencelaboratories.com/silent-compute/cross-borader-tx-privacy.