A Privacy-Preserving ZK Rollup Framework for Institutional DeFi: Use-Case of Repurchase Agreement [Draft]

Krzysztof Gogol[1,2]

[1] DeFiAM Labs
[2] University of Zurich

Abstract. The integration of tokenized real-world-assets (RWAs) and regulatory-compliant stablecoins into decentralized finance (DeFi) has transformative potential for financial markets. This study presents the proof-of-concept (PoC) conducted by ING, Raiffeisen, and Commerzbank on the DeFiAM L2, a permissioned layer-2 blockchain on Ethereum. In this PoC, tokenized bonds were used as collateral to borrow stablecoins, and DeFi smart contracts acted as a lender, automating borrowing and repayment, and as an automated market maker, pricing the tokenized bonds. For the purpose of the PoC, Aave and Uniswap, the leading DeFi protocols for lending and trading, respectively, were forked, calibrated, and extended with hooks, external smart contracts, to support efficient integration of tokenized RWAs. Regulatory-compliant stablecoins were bridged from Ethereum via native bridge of the DeFiAM layer-2 blockchain.
Keywords: Institutional DeFi, Lending, Repurchase Agreements, Layer-2

1 Introduction

Blockchain technology has the potential to revolutionize the financial industry, addressing longstanding inefficiencies and risks [11]. One of its key advantages is the atomicity of transactions, which directly addresses the delivery-versus-payment challenge in traditional finance (TradFi). The first generation of blockchains, initiated by Bitcoin [15] in 2008, introduced decentralized networks secured by consensus mechanisms to prevent double-spending. These public blockchains enable open participation and pseudonymous transactions, where wallet addresses and their transaction histories are publicly visible.

In response to the transparency of public blockchains, private (permissioned) blockchains such as Hyperledger and Corda R3 emerged. These networks restrict participation to authorized entities, offering enhanced privacy and control. However, their reduced decentralization introduces risks related to concentration and vulnerability. Private networks, often operating with fewer nodes, lack the resilience of public networks, which are supported by millions of miners or validators.

Nevertheless, private blockchains have gained traction among financial institutions, particularly for tokenizing real-world assets (RWAs) such as financial products. Tokenization facilitates atomic settlements, as demonstrated by pilots like Project Helvetia [1] in Switzerland and others across Europe. These projects highlight the potential of blockchain for domestic and cross-border settlements, often leveraging wholesale Central Bank Digital Currencies (wCBDCs) [5,18]. However, a significant challenge for tokenized RWAs on private networks is their limited use cases, resulting in low trading volumes.

The launch of Ethereum [7] in 2015 marked the advent of second-generation blockchains. Unlike their predecessors, these blockchains introduced virtual machines capable of executing *smart contracts*, self-executing programs that enable automated financial services collectively referred to as decentralized finance (DeFi) [10,12,19,16,6,9]. In 2018, Uniswap [4], a DeFi protocol for token exchange, pioneered this space. Today, over $100 billion in Total Value Locked (TVL) [2] is deposited across DeFi platforms, driven by innovations in trading, lending, and asset management on Ethereum and other EVM-compatible blockchains.

To address Ethereum's limitations, such as high gas fees and low throughput, Layer 2 (L2) scaling solutions, including rollups, were proposed [8,17,14]. These solutions rely on Ethereum for data availability and security while achieving greater scalability. Public L2 chains like Arbitrum, Base, and ZKsync have seen significant adoption, with increasing activity migrating from Ethereum to these platforms [13].

More recently, specialized L2 chains (appchain) tailored to specific applications, or group of applications have emerged. For example, Unichain [3] is a DeFi-specific rollup offering faster block production, compared to other L2s, and built-in interoperability. However, the use of L2 technology for institutional applications remained largely unexplored. DeFiAM L2, built on ZKsync's elastic chain framework, is the permissioned, privacy-preserving zk-rollup on Ethereum, designed for institutional DeFi. This work presents the new use-cases for tokenized RWA and regulatory-compliant stabecloins in DeFi lending and automated market makers (AMMs) on DeFiAM L2.

Related Work. Several initiatives have explored the application of DeFi in institutional settings. Projects like Project Mariana and Project Guardian by central banks and the Bank for International Settlements (BIS) tested DeFi mechanisms in foreign exchange (FX) markets. However, these efforts were limited in scope, primarily addressing FX transactions. Our work extends these applications to stablecoins and RWAs within DeFi lending ecosystems, addressing markets such as cross-bank repos.

Existing platforms such as AaveArc and Ondo Finance have attempted to whitelist participants and tokens within DeFi protocols on Ethereum. However, these approaches often face challenges related to composability with other DeFi protocols, such as Uniswap.

Contribution. This paper presents the outcomes of a technical feasibility study conducted with financial institutions on DeFiAM L2, involving ING, Raiffeisen, and Commerzbank. The study demonstrates the successful execution of cross-bank operations using stablecoins and tokenized bonds as collateral within DeFi lending protocols.

- We propose a framework for integrating RWAs and other digital assets from both Ethereum and private blockchains into DeFiAM L2 and demonstrate how protocols like Aave and Uniswap must be calibrated and adjusted for seamless RWA integration with hooks, external smart contracts.
- We present the DeFiAM Repo Platform and its proof-of-concept (PoC) executed with three leading European banks, showcasing how cross-bank repo agreements can be executed using DeFi protocols.
- We introduce DeFiAM L2, a permissioned and privacy-preserving zk-rollup, capable of supporting institutional DeFi use-cases with tokens bridged from public and private blockchains.

Paper Organization. Section 2 provides an overview of DeFi lending protocols and decentralized exchanges. Section 3 introduces the DeFiAM L2 blockchain, Section 4 outlines its Repo platform parameterization and adjustments to integrate RWAs. Section 5 details the proof-of-concept conducted on the DeFiAM Repo Platform. The final section discusses various approaches for cross-bank on-chain lending as well as challenges of integrating RWAs in DeFi, including regulatory compliance requirements.

2 Background

Decentralized Finance (DeFi) seeks to revolutionize the financial system by automating processes and eliminating unnecessary intermediaries. It is powered by smart contracts, self-executing programs hosted on the blockchain. This section introduces two core categories of DeFi protocols: decentralized lending, which facilitates token borrowing, and decentralized exchanges (DEXs), which enable token trading.

2.1 Decentralized Lending

Decentralized lending protocols, such as Aave, Compound, Curve Lend, and Morpho, operate via liquidity pools. Liquidity providers (LPs) deposit tokens into these pools, while smart contracts act as intermediaries, lending tokens to borrowers. Borrowers are required to deposit sufficient collateral along with an additional safety margin. The protocols determine interest rates based on the pool's current utilization rate.

Stable Utilization. A primary objective of lending protocols is to manage the pool's supply-demand balance, referred to as "utilization." The goal is to maintain utilization near an optimal level. Low utilization typically results in lower interest rates to encourage borrowing, while higher utilization triggers increased rates to balance supply and demand. This mechanism prevents excessive utilization, ensuring that lenders can withdraw funds and maintain the protocol's attractiveness.

Collateral Factor. The collateral factor, or over-collateralization ratio, plays a critical role in managing risks and returns. Protocols mitigate the risk of default and liquidation by requiring borrowers to provide substantial collateral. However, excessively high collateral requirements can render the lending market inefficient and unattractive, particularly for borrowers using stable-priced assets. Determining the optimal collateral factor requires analyzing historical price trends and assessing lenders' risk tolerance.

Shortcomings of Existing Approaches. Most current DeFi platforms calculate interest rates using fixed functions that rely solely on utilization. This simplistic approach may not account for the dynamic complexities of lending markets.

2.2 Decentralized Exchanges

Decentralized exchanges (DEXs) introduce innovative methods for token trading and price discovery directly on the blockchain. Unlike traditional finance and centralized exchanges (CEXs), which rely on order-book-based systems, DEXs use automated market makers (AMMs).

AMMs employ liquidity pools, pricing algorithms, and smart contracts to facilitate trading. Liquidity providers (LPs) deposit tokens into pools, which traders can interact with to execute orders. The AMM's algorithm automatically manages prices, eliminating the need for LPs to manually set quotes. This approach simplifies trading, enhances liquidity provision, and removes the necessity for order matching.

Traders interact directly with liquidity pools, and the pricing algorithm adjusts token prices based on the pool's reserves. This model represents a significant shift in trading dynamics, offering decentralized, permissionless, and transparent alternatives to traditional systems.

3 DeFiAM Layer-2 Blockchain

DeFiAM L2 is a permissioned, DeFi-specific rollup designed to operate as a fully privacy-preserving zk-rollup on Ethereum. This blockchain ensures transaction privacy and maintains gated access for participants and liquidity providers.

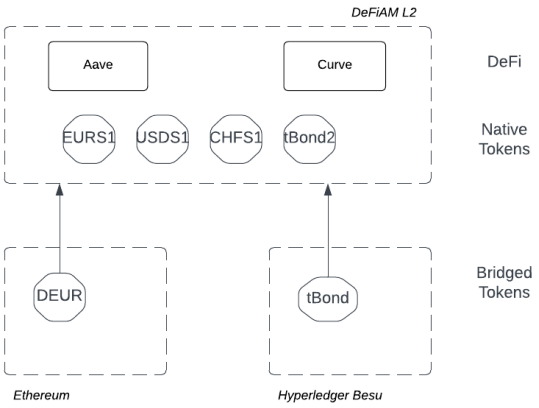

Fig. 1: High-level architecture of the DeFiAM L2 blockchain.

However, despite its permissioned nature, DeFiAM L2 remains open for the deployment of EVM-compatible DeFi protocols. The primary components of its architecture are as follows:

- **ZK Rollup.** DeFiAM L2 utilizes zk-rollup technology, a layer-2 scaling solution for Ethereum. This ensures that data availability and integrity are secured by Ethereum, preventing malicious blockchain operators from tampering with historical data.
- **Validium Approach.** The zk-rollup employs a validium model, wherein zero-knowledge proofs (ZK proofs) of transaction states are stored on Ethereum. This design ensures that Ethereum users cannot access transaction details from DeFiAM L2, maintaining privacy.
- **Permissioned Access.** Access to the network is restricted to accredited participants, who are authorized to interact with protocols, create, or bridge tokens. However, the deployment of DeFi protocols remains permissionless.
- **Privacy-Preserving Design.** Transaction details are accessible only to the participants involved. ZK proofs enable regulators to verify compliance with blockchain transactions without revealing specific participant details.
- **Cross-Chain Token Bridging.** Tokens can be bridged from public or permissioned chains or natively deployed on DeFiAM L2. Ethereum token integration is facilitated via the native bridge.
- **EVM-Equivalence.** DeFiAM L2 achieves EVM compatibility, allowing seamless deployment of Ethereum-based DeFi protocols such as Aave, Uniswap, and Curve.

The architecture of DeFiAM L2 is depicted in figures 1 and 2. Node operators, known as sequencers, are responsible for batching transactions and generating zero-knowledge proofs, which are submitted to Ethereum to validate transaction integrity. This design ensures that L2 node operators cannot tamper with

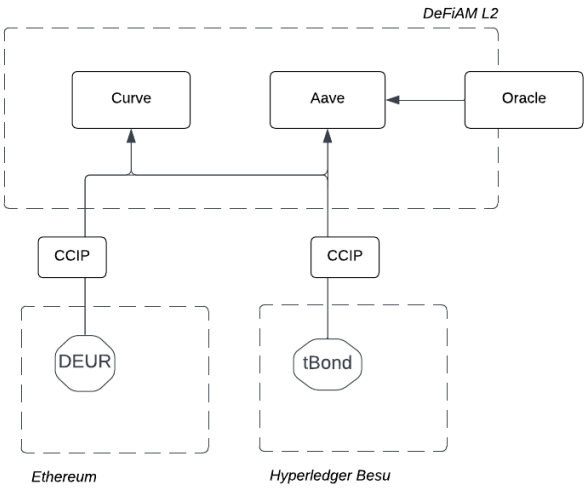

Fig. 2: Token bridging and protocol deployment on DeFiAM L2.

blockchain data, providing a secure and decentralized environment for institutional DeFi applications. DeFi protocols are deployed directly on the rollup, while tokens are either natively deployed or transferred via aggregation protocols from Ethereum or other public and private blockchains. Token integration from Ethereum is performed through the native bridge.

4 DeFiAM Repo Platform

The DeFiAM Repo Platform leverages DeFi protocols to automate cross-bank repurchase agreements (repos). This section outlines the platform's architecture.

4.1 Platform Architecture

The DeFiAM Repo Platform is an application built on the DeFiAM blockchain, specifically designed to facilitate cross-bank lending. It utilizes DeFi smart contracts to cover the entire value chain of cross-bank repurchase agreements. The platform integrates official forks of two leading Ethereum-based DeFi protocols:

- **Aave (v3):** For decentralized lending.
- **Uniswap (v2):** For decentralized token exchange.

Further enhancements include support for Uniswap v3 and custom hooks tailored for tokenized real-world assets (RWAs). Figure 2 illustrates the high-level architecture of the DeFiAM Repo Platform.

4.2 DeFi Parametrization

The core components of the DeFiAM Repo Platform involve the parametrization of Aave and Uniswap smart contracts to accommodate the specific requirements of cross-bank repos. Key adjustments include:

- **Coupon Payments.** The platform adopts an approach similar to stETH, allowing for seamless handling of periodic coupon payments during the lending period.
- **Bond Maturity.** In the PoC, it is assumed that the bonds used as collateral do not expire during the lending period, ensuring continuity of the repo agreements.
- **Loan Repayment.** The lending mechanism assumes timely repayment of loans, enabling the automatic release of collateral upon fulfillment of obligations.

This architecture and its parametrization address key challenges in implementing cross-bank repos, ensuring efficient and compliant execution of financial agreements using DeFi protocols.

5 Proof-of-Concept

The proof-of-concept (PoC) on the DeFiAM blockchain explores innovative applications of stablecoins and tokenized RWAs in conjunction with DeFi protocols. As part of this pilot, Aave (for decentralized lending) and Uniswap (for decentralized token exchange) were deployed on DeFiAM.

The digital assets utilized in the PoC included two tokenized bonds, labeled *tB1* and *tB2*, both denominated in EUR, and a EUR-denominated stablecoin, *dEUR*, issued by a consortium of European central banks. The *dEUR* tokens were bridged from Ethereum to DeFiAM using the native canonical bridge, while the tokenized bonds *tB1* and *tB2* were issued directly on DeFiAM. The participants included three leading European banks, referred to as *Bank1*, *Bank2*, and *Bank3*.

In the scenario:

Bank1 and *Bank2* acted as liquidity providers (LPs) to the *dEUR* pool on Aave, as well as to the *dEUR-tB1* and *dEUR-tB2* pools on Uniswap (v3). *Bank3* deposited tokenized bond *tB1* into Aave as collateral and borrowed *dEUR*, maintaining a health factor of 1.25The loan was repaid 24 hours later, after which *Bank3* automatically reclaimed its bond from the Aave pool. The *tB1-dEUR* pool on Uniswap acted as a liquidation mechanism in case the loan was not repaid or if the value of the collateral dropped.

- **Stablecoin:** *dEUR* issued by a consortium of European banks, bridged from Ethereum to DeFiAM via a canonical bridge.
- **Collateral:** Two tokenized digital bonds, *tB1* and *tB2*.
- **DeFi Protocols:** Aave (v3) for lending and Uniswap (v3) for trading.
- **Participants:** Three leading European banks—*Bank1*, *Bank2*, and *Bank3*.

Phases of the PoC

Phase 0: Initial Setup

- *Bank1* provides 100 million *dEUR* to the Aave *dEUR* pool.
- *Bank2* provides 400 million *dEUR* to the Aave *dEUR* pool.
- *Bank1* provides 300 million *dEUR* to the Uniswap *tB1-dEUR* pool.

Phase 1: Repo Transaction

- *Bank3* deposits 50 million *tB1* tokens into the Aave *tB1* pool as collateral.
- *Bank3* borrows 45 million *dEUR* from the Aave *dEUR* pool, with the Aave smart contract determining the maximum borrowable amount based on the total value of collateral provided by *Bank3*.

Phase 2: Repayment

- *Bank3* repays the borrowed 45 million *dEUR*, along with accrued interest, to the Aave *dEUR* pool.
- Upon full repayment, *Bank3* withdraws its collateral—50 million *tB1* tokens—from the Aave *tB1* pool.
- In cases of partial or non-repayment, the Aave smart contract determines the maximum amount of *tB1* tokens that can be withdrawn from the collateral pool.

6 Discussion

Repo in DeFi. This work focuses on executing repo agreements using DeFi lending pools; however, alternative approaches are feasible and could further enhance efficiency and flexibility.

- **Stablecoin Protocols.** Repo agreements could also be facilitated using decentralized stablecoin protocols. In this approach, stablecoins are minted by the protocol when collateral (e.g., tokenized bonds) is deposited by the borrower and are subsequently burned upon loan repayment. This mechanism resembles the operation of lending-based decentralized stablecoin protocols such as DAI (MakerDAO), lUSD (Liquity), and USDe (Ethena).
- **Auctions.** Another potential approach involves implementing on-chain auctions, similar to traditional order-book mechanisms. While such mechanisms may face scalability challenges on Ethereum, zero-knowledge proofs (ZKP) and rollups make them viable on DeFiAM L2. An example includes the auction-based design used by Neptun on Cosmos.

Challenges. Several challenges remain in adapting DeFi protocols to institutional applications:

- **Corporate Actions in DeFi.** Managing tokenized deposits and coupon payments on the blockchain presents operational complexities for DeFi protocols, both lending protocols and automated market makers. Tokenized bonds, type of tokenized RWAs usied in the PoC, can pay coupons. In order to assure the correct behavior of Uniswap and Aave the dirty price of bonds should be used. This approach is similar to liquid staking tokens (LSTs) thay pay thier holder staking rewards. The reward-based LSTs, such as wstETH or rETH, are generally more compatible with DeFi protocols than rebase tokens such as stETH.
- **Liquidation Mechanisms.** The system assumes that arbitrageurs will equal the prices of tokenized bond in Uniswap pools with off-chain systems. However, the temporary price deviations could affect liquidation processes and led to the liqudiators losses.
- **Legal Counterparties to Smart Contracts.** Establishing legal frameworks for interactions with DeFi smart contracts remains critical, particularly in the governance of L2 rollups operated by sequencers.
- **Regulatory Compliance.** Ensuring compliance for public blockchains like Ethereum is challenging, especially when selecting validators to operate transactions in a manner that aligns with institutional requirements.

7 Conclusions

This study demonstrates the feasibility of combining tokenized RWA, stablecoins, and DeFi protocols on DeFiAM, a permissioned layer-2 blockchain - an approach with the potential to significantly disrupt and transform existing financial systems. The evaluated example, cross-bank repurchase agreements (repos), was successfully executed on-chain using tokenized bonds and regulatory-compliant stablecoin, bridged from Ethereum. DeFi smart contracts, Aave and Uniswap, acted as lenders and automated market makers, respectively, showcasing the capability of DeFi to streamline operations, enhance transparency, and reduce reliance on intermediaries in institutional finance.

References

1. Project helvetia (2023), `https://www.bis.org/about/bisih/topics/cbdc/helvetia.htm`
2. DeFi Llama (12 2024), `https://defillama.com/`
3. Adams, H., Toda, M., Karys, A., Wan, X., Gretzke, D., Zhong, E., Wong, Z., Marzec, D., Miller, R., Floersch, K., Robinson, D.: Unichain (2024)
4. Adams, H., Zinsmeister, N., Robinson, D.: Uniswap v2 Core (2020)
5. Auer, R., Frost, J., Gambacorta, L., Monnet, C., Rice, T., Shin, H.S.: Central bank digital currencies: motives, economic implications and the research frontier (2021), `https://www.bis.org/publ/work976.pdf`
6. Auer, R., Haslhofer, B., Kitzler, S., Saggese, P., Victor, F.: The technology of decentralized finance (defi) (2023)

7. Buterin, V.: Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform. (2014)
8. Gangwal, A., Gangavalli, H.R., Thirupathi, A.: A Survey of Layer-Two Blockchain Protocols. Journal of Network and Computer Applications, Vol 209 (2022)
9. Gogol, K., Killer, C., Schlosser, M., Bocek, T., Stiller, B., Tessone, C.: SoK: Decentralized Finance (DeFi) – Fundamentals, Taxonomy and Risks (2024)
10. Gudgeon, L., Werner, S.M., Perez, D., Knottenbelt, W.J.: DeFi Protocols for Loanable Funds: Interest Rates, Liquidity and Market Efficiency. In: the 2nd ACM Conference on Advances in Financial Technologies (AFT) (2020)
11. Guo, S., Kreitem, J., Moser, T.: DLT options for CBDC. Journal of Central Banking Theory and Practice (2022)
12. Jensen, J., von Wachter, V., Ross, O.: An Introduction to Decentralized Finance (DeFi). Complex Systems Informatics and Modeling Quarterly (2021)
13. L2Beat: Value Locked (2024), `https://l2beat.com/`, accessed on June 10, 2024
14. Motepalli, S., Freitas, L., Livshits, B.: SoK: Decentralized Sequencers for Rollups. arXiv preprint arXiv:2310.03616 (2023)
15. Nakamoto, S.: Bitcoin: A Peer-to-Peer Electronic Cash System. www.bitcoin.org (2008)
16. Schär, F.: Decentralized finance: On blockchain- and smart contract-based financial markets (2020)
17. Thibault, L.T., Sarry, T., Hafid, A.S.: Blockchain Scaling Using Rollups: A Comprehensive Survey. IEEE Access, Vol. 10 (2022)
18. Ward, O., Rochemont, S.: Understanding central bank digital currencies (cbdc). Institute and Faculty of Actuaries (2019)
19. Werner, S.M., Perez, D., Gudgeon, L., Klages-Mundt, A., Harz, D., Knottenbelt, W.J.: Sok: Decentralized finance (defi) (2022)