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 stablecoins into decentralized finance (DeFi) has the potential to transform financial markets. This paper presents a framework for a multi-bank proof-of-concept (PoC) demonstrating the application of tokenized bonds in decentralized lending protocols on a permissioned Layer-2 (L2) blockchain. In this PoC, tokenized bonds serve as collateral for borrowing regulatory-compliant stablecoins, with DeFi smart contracts acting as lenders to automate interest rate calculations, collateral management, and liquidation processes. Additionally, automated market maker (AMM) functions as trading venues to facilitate price discovery for tokenized bonds. For the purposes of the PoC, Aave ledning protocol and Uniswap AMM are forked on the DeFiAM L2 blockchain to meet regulatory requirements. These protocols are calibrated and extended with hooks—external smart contracts—designed to maximize capital efficiency and minimize borrowing fees whereas stablecoins are bridged from Ethereum via a native bridge, ensuring seamless interoperability.
Keywords: DeFi, Lending, Repurchase Agreements, Layer-2

1 Introduction

Blockchain technology has the potential to revolutionize the financial industry, addressing longstanding inefficiencies and risks [19]. One of its key advantages is the atomicity of transactions that solves delivery-versus-payment (DvP) challenges of traditional finance (TradFi). The first generation of blockchains, initiated by Bitcoin [23] in 2008, introduced decentralized networks secured by consensus mechanisms to prevent double-spending. These public blockchains enabled open participation and pseudonymous transactions, where wallet addresses and their transaction history 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, these networks often suffer from the lack of decentralization that introduces concentration and governance risks and related vulnerabilities. Private networks, often operating with fewer nodes, lack the resilience of public networks, maintained by millions of miners or validators.

Nevertheless, private blockchains have gained traction among financial institutions, particularly for tokenizing real-world assets (RWAs), especially financial instruments. Tokenization facilitates atomic settlements, as demonstrated by central bank pilots like Project Helvetia [4] 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) [10,28]. However, a significant challenge for tokenized RWAs on private networks is their limited use cases, resulting in low trading volumes.

The launch of Ethereum [12] 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) [18]. In 2018, Uniswap [8], a DeFi protocol for token exchange, pioneered this space. Today, over $100 billion in Total Value Locked (TVL) [5] is deposited across DeFi protocols, driven by innovations in trading, lending, and asset management on Ethereum and other EVM-compatible blockchains [29,26,11,15].

To address Ethereum's limitations, such as high gas fees and low throughput, Layer 2 (L2) scaling solutions, including rollups, were proposed [14,27,22]. 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 [20]. Recently, specialized Layer-2 (L2) chains, or appchains, tailored for specific applications or groups of applications, have gained prominence. For example, Unichain [7], a DeFi-specific rollup, offers faster block production and built-in interoperability compared to other L2s. However, the application of L2 technology for institutional use cases remains largely unexplored.

DeFiAM L2 addresses this gap as a permissioned, privacy-preserving ZK-rollup on Ethereum, specifically designed for institutional DeFi. This work introduces new use cases for tokenized RWAs and regulatory-compliant stablecoins in DeFi lending and automated market makers (AMMs) deployed on DeFiAM L2. Unlike public rollups, permissioned L2s meet regulatory requirements such as KYC compliance while preserving privacy. Additionally, unlike private L1 chains, DeFiAM L2 offers EVM compatibility, enabling the seamless integration of DeFi protocols. This combination facilitates the integration of RWAs into DeFi in a compliant manner, unlocking new business opportunities and use cases in institutional finance such as repurchase agreements, proposed in this work.

Related Work. Several initiatives, led by the Bank for International Settlements (BIS) and central banks, have explored the application of DeFi in institutional settings. Project Guardian applied lending protocols and AMMs for FX market operations [3]. Mariana Project explored the cross-border exchange of wCBDCs, further enhanced through an L2 blockchain approach [2,16]. However, these efforts were limited in scope and focused primarily on FX transactions.

Initiatives such as Broadridge, HQLAx, and Finality employ private Layer 1 blockchains to facilitate the settlement of transactions involved in cross-bank re-

purchase agreements (repos). In these platforms, one financial institution transfers collateral while the other transfers cash, with the blockchain consensus mechanism ensuring that the transaction is atomic. This implies that either both parties receive the agreed-upon assets, or neither does. However, these solutions do not employ smart contracts, and essential operations, such as the settlement of business terms, calculation of interest rates, and management of collateral, still occur off-chain through triparty intermediaries.

Full-circle collateralized lending for institutions via smart contracts was pioneered by AaveArc and Ondo Finance. These platforms forked the DeFi lending protocols Aave and Compound, respectively, on Ethereum to whitelist participants and liquidity. However, this approach was hindered by the lack of composability with other DeFi protocols, such as AMMs. This work presents the novel framework for integrating stablecoins and RWAs within the DeFi lending and AMM ecosystem on the permissioned L2 blockchain, efficiently addressing interoperability, scalability, and regulatory challenges.

Contribution. This paper presents a framework for a technical feasibility study with three leading European banks. The study demonstrates how stablecoins and tokenized bonds can be utilized within DeFi protocols operating on a permissioned L2 blockchain to efficiently and compliantly execute cross-bank repurchase agreements.

- We demonstrate the necessary calibration and adjustments for DeFi protocols like Aave and Uniswap, including the use of hooks-external smart contracts-for seamless integration of tokenized bonds.
- We propose a framework for integrating RWAs, regulatory-compliant stablecoins, and other digital assets from Ethereum and private blockchains into DeFiAM Chain-permissioned L2s on Ethereum-operating DeFi protocols.
- We present the DeFiAM Repo platform and its PoC, showcasing the execution of cross-bank repurchase agreements using DeFi protocols, with defined roles, namely, the borrower, the liquidity provider (LP) and the liquidator, assigned to three banks.

Paper Organization. Section 2 introduces the DeFi fundamentals, focusing on lending protocols and AMMs. Section 3 presents the Layer-2 scaling approach and the permissioned network of DeFiAM L2 on Ethereum. Section 4 describes the DeFiAM Repo Platform, including the Aave and Uniswap forks, and their adjustments for tokenized bonds integration. Section 5 details the PoC conduct, outlining the roles and responsibilities for participating banks. The final section explores the alternative approaches for cross-bank on-chain lending and discusses the regulatory challenges related to integrating RWAs into DeFi.

2 DeFi Preliminaries

Decentralized finance (DeFi) refers to financial applications that employ blockchain and smart contracts to deliver customer services without relying on

intermediaries. DeFi originated on Ethereum, the first blockchain to introduce smart contracts, and consequently most of the DeFi applications are developed for Ethereum Virtual Machine (EVM). These applications, often referred to as DeFi protocols to emphasize that their core logic resides on the blockchain as smart contracts, provide a wide range of services, including trading, lending, and asset management [15,29,26,11]. Unlike traditional finance, DeFi protocols do not depend on intermediaries to facilitate their operations, but fully automate the processes with smart contracts. Contrary to popular belief, DeFi is not peer-to-peer finance, but smart contracts, called liquidity pools, facilitate the interactions between DeFi participants. The logic of smart contracts is immutably stored on the blockchain, ensuring transparency and fairness, and adhering to the principle often summarized as *code is law*. This section introduces two key categories of DeFi protocols: decentralized lending and decentralized exchanges (DEXs).

2.1 Decentralized Lending

Decentralized lending protocols, such as Aave, Compound, Curve Lend, and Morpho, facilitate the borrowing of digital assets [13,25,21]. Liquidity providers (LPs) deposit tokens into the liquidity pools - smart contracts that act as intermediaries, lending tokens to borrowers. Unlike traditional money markets, where intermediaries such as banks facilitate transactions, decentralized lending protocols allow borrowers interact directly with smart contracts that calculates interest rates dynamically based on the supply and demand of assets in its liquidity pools. LPs earn interest on the tokens they deposited in the pool. Borrowing positions are over-collateralized to mitigate risks, with collateral values monitored and adjusted to reflect market fluctuations.

Interest Rate Curve. A primary goal of decentralized lending protocols is to manage the pool's utilization, which represents the ratio of borrowed funds to the total available liquidity in a pool. Maintaining utilization near an optimal level ensures the protocol's efficiency and attractiveness to both LPs and borrowers. The utilization rate U_t at time t can be expressed as:

$$U_t = \frac{B_t}{L_t},$$

where B_t is the amount borrowed, and L_t is the total liquidity in the pool at time t. Interest rates are adjusted dynamically based on utilization, with a sharp increase in rates when utilization exceeds the optimal threshold, as per the kinked interest rate model [17,1]:

$$i_{b,t} = \begin{cases} \alpha + \beta U_t & \text{if } U_t \leq U_{opt}, \\ \alpha + \beta U_{opt} + \gamma(U_t - U_{opt}) & \text{if } U_t > U_{opt}, \end{cases}$$

where α represents the base rate, β the slope below the optimal utilization, and γ (where $\gamma > \beta$) the slope beyond U_{opt}.

Collateral Factor and Liquidation. The collateral factor, or over-collateralization ratio, is critical for managing risks. Borrowers must lock collateral that exceeds the value of the borrowed assets, ensuring the protocol's solvency even in volatile markets. The collateral factor is determined based on historical price trends and risk tolerance, balancing the protocol's security and the market's efficiency. Liquidation mechanisms are triggered if the collateral's value falls below a predefined liquidation threshold, protecting lenders and maintaining the protocol's stability [24]. Key parameters in liquidation mechanism include:

- **Loan-to-Value (LTV):** The maximum borrowable amount relative to the collateral's value. For example, an LTV of 0.7 means borrowers can borrow up to 70% of the collateral's value.
- **Liquidation Threshold (LT):** The point at which a position is eligible for liquidation. A higher LT implies more tolerance for price fluctuations.
- **Health Factor (HF):** A measure of a position's risk, calculated as:

$$HF = \frac{\sum_{i \in A}(\text{Collateral}_i \times LT_i)}{\text{Total Borrows}},$$

  where A is the set of all collateral assets. An HF below 1 indicates liquidation risk.
- **Liquidation Penalty (LP):** A fee charged for liquidating a position, distributed to the protocol.

Shortcomings of Existing Approaches. Current DeFi platforms often rely on static functions for interest rate calculations, which depend solely on utilization rates. This approach fails to account for the dynamic complexities of lending markets. Moreover, loans generally have indefinite maturities, with variable interest rates recalculated continuously. This variability introduces uncertainty, making the lending experience less predictable for users [17]

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 set the exchange price between two tokens based on the current reserves of tokens in the liquidity pool:

- Liquidity providers (LPs) deposit tokens into liquidity pools.
- Traders interact directly with liquidity pools, and the pricing algorithm adjusts token prices based on the pool's reserves.
- The AMM smart contract automatically manages prices, eliminating the need for LPs to manually set quotes. This approach eliminates the necessity for order matching.

– Arbitrageurs are a special group of traders who identify and exploit price discrepancies across different trading platforms to achieve equilibrium.

The first AMM was introduced by Uniswap on the Ethereum blockchain in 2018, followed by Curve, Balance and more. The most common AMMs are Constant Function Market Makers (CFMM) that use a trading (reserve) function that assigns token reserves to a constant real number L (invariant), which remains the same for every swap transaction. Typically, the liquidity pool consists of two tokens, and x_1, x_2 represents the token reserves. Numerous CFMM variants have been proposed and implemented [30] to reduce the price impact for traders and increase the capital efficiency for LPs. Brief descriptions of the main AMM types follows.

Uniswap v2. Constant product market maker is the first AMM. It was introduced by Uniswap and employs a straightforward invariant [8]. This AMM is currently used in pools with tokens with substantial volatility or newly issued tokens whose prices have not yet reached equilibrium.

$$x_1 x_2 = L^2$$

Uniswap v3. Constant product with concentrated liquidity was introduced with Uniswap v3 [9] in order to increase the efficiency of liquidity in the pool. It allows LPs to specify price range $[p_a, p_b]$ within which liquidity is supplied. Consequently, the trade invariant applicable to this specified interval is

$$\left(x_1 + \frac{L}{\sqrt{p_b}}\right)(x_2 + L \cdot \sqrt{p_a}) = L^2$$

Uniswap v4. Uniswap v4 [6] builds on the capital efficiency mechanism of Uniswap v3, introducing enhanced flexibility through *hooks*—external smart contracts that can be attached to the swap lifecycle. Hooks enable customization by allowing arbitrary code execution before or after predetermined liquidity pool actions. Hooks can introduce entirely new capabilities that would otherwise require independent AMM implementations, offering flexibility and adaptability. In this studies we develop the hooks for listing tokenized RWAs such as tokenized bonds, on Uniswap v4, and automatically handle corporate actions such as coupon payments.

3 DeFiAM Layer-2 Blockchain

While most corporate blockchains today utilize Layer-1 networks such as Hyperledger and Corda, the emergence of Layer-2 scaling solutions—particularly rollups—has proven highly effective in scaling Ethereum and offers significant potential for corporate blockchain applications. This section introduces the concept of Layer-2 scaling with a focus on rollups and subsequently presents DeFiAM Chain, a permissioned ZK-rollup built on Ethereum, tailored for institutional use cases.

3.1 Layer-1 and Layer-2 Blockchain

Blockchain scalability can be addressed through two approaches: Layer-1 (L1) scaling and Layer-2 (L2) scaling. In L1 scaling, a new blockchain is developed with its own consensus mechanism and validator network to ensure security and operations. However, establishing a decentralized validator network for each new L1 is a significant challenge. Insufficient decentralization increases the risk of centralization, potentially allowing a small group of validators to collude and tamper with the blockchain's historical data.

L2 scaling takes a different approach, with rollups being the most popular form. *Rollups* act like a blockchain, but they are non-custodial, meaning they do not store data outside of the underlying L1 blockchain. Unlike L1s, rollups do not rely on their own consensus mechanisms or validator networks. Instead, they use cryptographic proofs to store transaction states on the underlying L1. As a result, tampering with rollup data requires compromising the security of the L1 blockchain. Most rollups use Ethereum as their L1, though there are efforts to integrate Bitcoin in similar architectures. Rollups rely on *sequencers*, which are collateralized operators responsible for batching transactions and submitting them to the L1 blockchain. Based on how data validity is ensured, rollups are divided into two types:

- *Optimistic Rollups:* Data is submitted to the L1 under the assumption of correctness. A predefined challenge period allows anyone to dispute invalid transactions, ensuring security. Optimism and Arbitrum are the most prominent examples of pubic optymisctic rollups.
- *Zero-Knowledge (ZK) Rollups:* Data validity is guaranteed by cryptographic proofs generated by provers. These proofs are submitted to the L1 along with or without the transaction data. However, ZK rollups incur additional computational costs for proof generation. ZKsync and StarkNet are the most known public ZK rollups.

Optimistic rollups provide easier EVM compatibility, whereas ZK rollups are preferred for faster finality and better security, though they involve higher costs for ZK-proves generation and overall complexity.

3.2 DeFiAM - Permissioned Layer-2

DeFiAM L2 is a permissioned ZK rollup on Ethereum that is (institutional) DeFi-specific with fully privacy-preserving. It ensures transaction privacy and maintains gated access for participants and liquidity providers. However, DeFiAM L2 remains open for the deployment of EVM-based DeFi protocols. The primary components of its architecture follows.

- **ZK Rollup.** DeFiAM L2 is ZK rollup on Ethereum. This ensures that data availability and integrity are secured by Ethereum, preventing malicious operators from tampering with historical data.

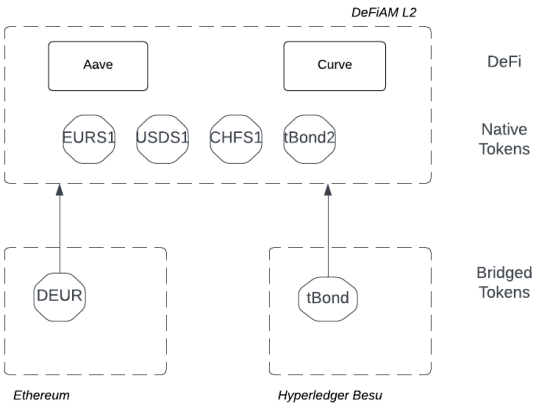

Fig. 1: High-level architecture of the DeFiAM L2 blockchain.

- **Validium Approach.** DeFiAM L2 employs a validium model of ZK rollups, wherein only ZK proofs of transaction states are stored on Ethereum. This design ensures that Ethereum users cannot access transaction details from DeFiAM L2, maintaining privacy.
- **Gated Access.** Access to the network is restricted to accredited participants and liquidity. However, the deployment of DeFi protocols remains permissionless.
- **Privacy-Preserving.** Transaction details are accessible only to the participants involved. ZK proofs enable regulators to verify compliance of blockchain transactions without revealing specific participant details.
- **Cross-Chain Token Integration.** Tokens can be bridged from public or permissioned blockchains or natively deployed on DeFiAM L2. The integration of Ethereum tokens is facilitated through the native bridge that is responsible for posting ZK proves.
- **EVM.** DeFiAM L2 is an EVM compatible network, allowing the seamless deployment of Ethereum-based DeFi protocols such as Aave, Uniswap, and Curve.

The architecture of DeFiAM L2 is shown in Figures 1 and 2. Node operators 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 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.

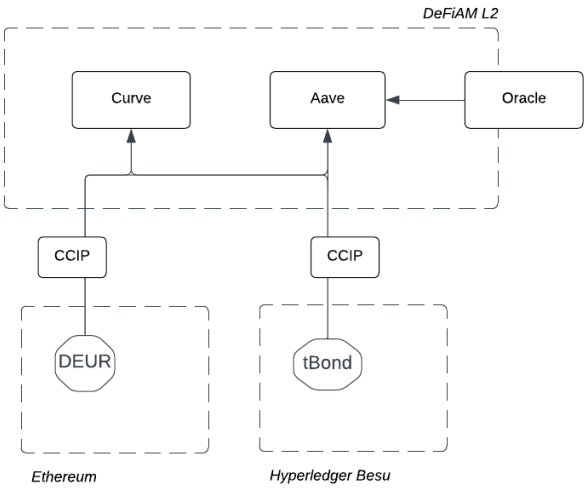

Fig. 2: Token bridging and protocol deployment on DeFiAM L2.

4 DeFiAM Repo Platform

The DeFiAM Repo Platform is an application built on the DeFiAM blockchain, specifically designed to facilitate cross-bank lending. Using DeFi smart contracts, it covers the entire value chain of cross-bank repurchase agreements without any triparty. This section outlines the platform architecture and how the underlying DeFi protocols need to be adjusted in order to correctly support liquidity pools involving tokenized RWAs.

4.1 Platform Architecture

Figure 2 illustrates the high-level architecture of the DeFiAM Repo Platform. The platform integrates official forks of two DeFi protocols:

- **Aave (v3):** This protocol acts as a lender and facilitates on-chain borrowing, including the interest rate mechanism, haircuts, and liquidations.
- **Uniswap (v2), (v3), (v4):** AMMs are used for the price discovery of tokenized RWAs as well as as a trading venue to buy or sell tokenized RWAs. AMMs are essential in the the loan liquidation process, as AMMs are counterparties that buy liquidated collateral.

The correct parametrization of DeFi protocols for tokenized RWAs is essential for the initial adoption, as it increases the capital efficiently in the pool and minimizes costs for the DeFi users. The parameterization of Aave and Uniswap is done for the liquidity pools involving the tokens:

– EUR-stablecoin,
– EUR-denominated government bond,
– EUR-denominated corporate bond.

The major challenge for the DeFi protocols is posed by the corporate actions related to the tokenized bonds, especially coupon payments and the bond expiration date. This section further explains how Aave and Uniswap need to be calibrated or extended with hooks, external smart contracts, in order to correctly support the liquidity pools with tokenized bonds correctly.

4.2 Parametrization of Aave

There are three liquidity pools created at Aave for each token: EUR-stablecoins, tokenized government, and corporate bonds. The tokenized government and corporate bonds can act as collateral to borrow the stablecoins. The parameterization of each pool is presented in Table 1.

Table 1: Key parameters of liquidity pools in Aave with EUR-stablecoin, EUR-denominated government and corporate bonds.

Parameter	**Stablecoin**	**Government Bond**	**Corporate Bond**
Collateral Enabled	No	Yes	Yes
LTV (Loan-to-Value)	-	98%	98%
Liquidation Threshold	-	99%	99%
Liquidation Bonus	-	4%	8%
Reserve Factor	10%	4%	12%
Borrowing Enabled	Yes	No	No

Nevertheless, some adjustments in the Aave smart contracts require the development of hooks, external smart contracts that integrate with Aave. These adjustments include:

– **Coupon Payments.** This adjustment is necessary for seamless handling of periodic coupon payments during the lending period. The tokenized bonds that pay coupon are similar to liquid staking tokens (LSTs). In order to ensure the proper functioning of the Aave and Uniswap protocols, the tokens must represent the dirty price of tokenized bonds.
– **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.
– **Fixed Maturity** The lending mechanism assumes timely repayment of loans, enabling the automatic release of collateral upon fulfillment of obligations.

4.3 Parametrization of Uniswap

The Repo Platfrom support three AMMs, each with distinct objectives: Uniswap (v2), (v3) and (v4). Uniswap (v2) is used for the discovery of the price of newly issued tokens with high price volatility. Uniswap (v3) allows LP to specify price ranges for which liquidity is provided; however, it required the manual adjustments of the LP-position when the price changes. Hooks - external smart contracts - to Uniswap (v4) allow to automate the LP-adjustments. Currently, there are two liquidity pools created in Uniswap (v3):

- stablecoin - government bond,
- stablecoin - corporate bond.

Further enhancements include support for Uniswap (v4) and custom hooks tailored for tokenized real-world assets (RWAs) such as tokenized bonds. As the dirty pice of tokenized bonds accrue coupon payment, its price trajectory against stablecoins is known and can be used as a basis to automatically optimize LP-position.

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 integrating tokenized Real-World Assets (RWAs) and stablecoins into DeFi protocols on a permissioned Layer-2 (L2) blockchain—an approach with the potential to transform the financial system and unlock new use cases for tokenized assets. It presents a framework for a proof-of-concept (PoC) focused on executing repurchase agreements (repos) using DeFi protocols on the permissioned L2 blockchain on Ethereum - DeFiAM.

In this PoC, tokenized bonds serve as collateral for borrowing regulatory-compliant stablecoins, with DeFi smart contracts automating interest rate calculations, collateral management, and liquidation processes and automated market makers (AMMs) facilitate price discovery for tokenized bonds. The study defined PoC roles—borrower, liquidity provider (LP), and liquidator—assigned to three banks. For the DeFiAM Repo Platform, the Aave lending protocol and Uniswap AMM are forked on the DeFiAM L2 blockchain. This paper details the calibration and extensions required in DeFi protocols to effectively manage tokenized bonds and stablecoins, demonstrating DeFi's capability to streamline operations, enhance transparency, and reduce reliance on intermediaries in institutional finance. The L2 blockchain approach ensures KYC compliance for participants, seamless liquidity management, and integration of tokenized RWAs and regulatory-compliant stablecoins from Ethereum and private Layer-1 blockchains operated by banks.

References

1. Aave - Protocol Whitepaper V1.0. Tech. rep. (2020)

2. Cross-border exchange of wholesale cbdcs using automated market-makers (2023), https://www.bis.org/about/bisih/topics/cbdc/mariana.htm
3. Project guardian - open and interoperable networks (2023), https://www.mas.gov.sg/publications/monographs-or-information-paper/2023/project-guardian-open-interoperable-networks
4. Project helvetia (2023), https://www.bis.org/about/bisih/topics/cbdc/helvetia.htm
5. DeFi Llama (12 2024), https://defillama.com/
6. Adams, H., Salem, M., Zinsmeister, N., Reynolds, S., Adams, A., Pote, W., Toda, M., Henshaw, A., Williams, E., Robinson, D.: Uniswap v4 Core (2024)
7. Adams, H., Toda, M., Karys, A., Wan, X., Gretzke, D., Zhong, E., Wong, Z., Marzec, D., Miller, R., Floersch, K., Robinson, D.: Unichain (2024)
8. Adams, H., Zinsmeister, N., Robinson, D.: Uniswap v2 Core (2020)
9. Adams, H., Zinsmeister, N., Salem, M., River, K., Robinson, D.: Uniswap v3 Core (2021)
10. 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
11. Auer, R., Haslhofer, B., Kitzler, S., Saggese, P., Victor, F.: The technology of decentralized finance (defi) (2023)
12. Buterin, V.: Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform. (2014)
13. Chiu, J., Ozdenoren, E., Yuan, K., Zhang, S.: On the Fragility of DeFi Lending (2022), https://g20.org/wp-content/uploads/2022/02/FSB-Report-on-Assessment-of-Risks-to-Financial-
14. Gangwal, A., Gangavalli, H.R., Thirupathi, A.: A Survey of Layer-Two Blockchain Protocols. Journal of Network and Computer Applications, Vol 209 (2022)
15. Gogol, K., Killer, C., Schlosser, M., Bocek, T., Stiller, B., Tessone, C.: SoK: Decentralized Finance (DeFi) – Fundamentals, Taxonomy and Risks (2024)
16. Gogol, K., Messias, J., Schlosser, M., Kraner, B., Tessone, C.: Cross-border Exchange of CBDCs using Layer-2 Blockchain. In: Crypto Finance Conference(CfC) (2024)
17. Gudgeon, L., Werner, S., Perez, D., Knottenbelt, W.J.: DeFi Protocols for Loanable Funds: Interest Rates, Liquidity and Market Efficiency (2020). https://doi.org/10.1145/3419614.3423254
18. 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)
19. Guo, S., Kreitem, J., Moser, T.: DLT options for CBDC. Journal of Central Banking Theory and Practice (2022)
20. L2Beat: Value Locked (2024), https://l2beat.com/, accessed on June 10, 2024
21. Lehar, A., Parlour, C.A.: Systemic Fragility in Decentralized Markets (2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4164833
22. Motepalli, S., Freitas, L., Livshits, B.: SoK: Decentralized Sequencers for Rollups. arXiv preprint arXiv:2310.03616 (2023)
23. Nakamoto, S.: Bitcoin: A Peer-to-Peer Electronic Cash System. www.bitcoin.org (2008)
24. Perez, D., Werner, S.M., Xu, J., Livshits, B.: Liquidations: DeFi on a Knife-edge (2020). https://doi.org/10.1007/978-3-662-64331-0{_}24
25. Saengchote, K.: Decentralized lending and its users: Insights from Compound (2022), https://ssrn.com/abstract=3925344

26. Schär, F.: Decentralized finance: On blockchain- and smart contract-based financial markets (2020)
27. Thibault, L.T., Sarry, T., Hafid, A.S.: Blockchain Scaling Using Rollups: A Comprehensive Survey. IEEE Access, Vol. 10 (2022)
28. Ward, O., Rochemont, S.: Understanding central bank digital currencies (cbdc). Institute and Faculty of Actuaries (2019)
29. Werner, S.M., Perez, D., Gudgeon, L., Klages-Mundt, A., Harz, D., Knottenbelt, W.J.: Sok: Decentralized finance (defi) (2022)
30. Xu, J., Paruch, K., Cousaert, S., Feng, Y.: SoK: Decentralized Exchanges (DEX) with Automated Market Maker (AMM) Protocols. ACM Computing Surveys, Vol. 55, No. 11 (2021)