DeFiAM Chain:
A Privacy-Preserving ZK Rollup for Institutional DeFi [Draft]

ABSTRACT

DeFiAM Chain is a permissioned ZK rollup designed for financial and interbank operations, offering complete transaction privacy and seamless integration of decentralized finance (DeFi) protocols with tokenized real-world assets (RWAs). The platform addresses scalability, privacy, and compliance challenges in institutional finance. This paper introduces key innovations, including RWA-hooks - external smart contracts - to DeFi protocols, transaction privacy mechanisms, and a validation network, to enable efficient and regulated financial activities.

1 INTRODUCTION

Blockchain technology has the potential to transform the financial industry by enabling decentralized, atomic, and trustless transaction execution. In addition, decentralized finance (DeFi) offers transparent mechanisms for on-chain financial activities such as trading, lending, and asset management [5, 6, 9, 11] that could be applied in traditional fiance (TradFi), for example, in repurchase agreements ($3 trillion daily) and foreign exchange markets ($7.5 trillion daily). However, the integration of tokenized real-world assets (RWAs) in DeFi remains limited due to scalability, security and interoperability challenges.

This paper introduces the DeFiAM Chain, a ZK-rollup leveraging ZKsync's Elastic Chain to address these challenges, offering the following key properties:

- **EVM Compatibility:** Seamless deployment of DeFi protocols is ensured through Ethereum Virtual Machine (EVM) compatibility, facilitating integration with existing ecosystems.
- **Gated Access:** Access to DeFiAM Chain is restricted to clients of financial institutions and compliant liquidity providers. The deployment of DeFi protocols remains permissionless, promoting flexibility and openness for developers.
- **Interoperability:** The canonical bridge of the ZK Chain enables secure integration of tokens originating from Ethereum, and cross-chain communication protocols transfer of assets from private Layer-1 blockchains.

To meet the specific requirements of institutional DeFi and tokenized RWAs, the following innovations are introduced:

- **RWA Hooks for DeFi:** Customized DeFi protocols tailored for tokenized RWAs, enabling the handling of corporate actions and end-to-end value chain management directly on-chain.
- **Transaction Privacy Mechanisms:** Zero-knowledge (ZK) proofs ensure complete transaction privacy while maintaining full regulatory compliance.
- **Node Operator Network:** A decentralized network of financial institutions ensures data integrity, fair transaction execution, and fast settlement times.

The development of the DeFiAM Chain follows an iterative approach, with its codebase and features made accessible for other ZK chains or DeFi protocols on public L1 and L2 chains, fostering innovation and collaboration across the ecosystem.

2 PRIOR WORK AND CURRENT CHALLENGES

Ethereum established the foundation for programmable blockchains; however, the application of DeFi protocols to

- **Interoperability Barriers:** Current DeFi protocols operate on Ethereum and its public rollups, whereas tokenized RWAs are deployed to private L1 networks that does not support EVM capable to operate DeFi smart contracts. Consequently, the trading volume of tokenized RWA remains low.
- **Privacy and Compliance Requirements:** Institutions require privacy-preserving features and regulatory compliance that public blockchains and consequently DeFi protocols do not provide natively.
- **Composability Issues for RWAs:** RWAs, especially financial instruments face challenges when integrating with DeFi due to special corporate actions, e.g. coupon payments by bonds.

Despite these challenges, various projects initiated by the Bank for International Settlements (BIS) and central banks have pioneered the application of DeFi protocols for wholesale Central Bank Digital Currencies (CBDCs) [4, 10], demonstrating the transformative potential of blockchain in institutional finance [8]. For instance, Project Guardian [2] applied both lending protocols and automated market makers (AMMs) for operations in the FX market, Project Mariana [1] utilized a Crypto-Swap-Invariant AMM to facilitate cross-country trading of EUR, CHF, and SGD. This concept was further enhanced through the L2 blockchain approach [7]. Most recently, Project Mandala [3] explored programmable compliance with zero-knowledge proofs to validate regulatory requirements.

3 RWA INTEGRATION IN DEFI

Integrating tokenized Real-World Assets (RWAs) into DeFi protocols presents significant challenges, even with EVM compatibility. If unaddressed, these issues could disrupt the TradFi processes on-chain, leading to potential losses for LPs (impermanent loss, loss-verus-rebalancing) and DeFi users (price impact). This section introduces hooks—external smart contracts—necessary for the effective operation of RWAs in decentralized lending and automated market makers (AMMs).

RWA Wrappers. Due to features like coupon payments and other corporate actions, tokenized financial assets, such as corporate or government bonds, require specialized wrappers to be compatible with DeFi protocols. For instance, tokenized debt wrappers represent the dirty price of bonds, including accrued interest, making them similar to reward tokens in liquid staking protocols.

Repurchase Agreements. On-chain cross-bank lending (repurchase agreements) involves borrowing stablecoins or wholesale CBDCs, with tokenized bond as collateral. Proper integration of RWA-wrappers and external hooks is essential for:

- **Risk Management:** Configuring loan-to-value (LTV) ratios, liquidation thresholds, penalties, and reserve factors with real-time collateral management using oracle-provided bond ratings.
- **Interest Rate Optimization:** Aligning on-chain rates with TradFi markets, including incentives for financial institutions acting as LPs.
- **Fixed Maturity Bonds:** Supporting fixed-term lending requires external hook development, as most of DeFi loans are perpetual by design.

These mechanisms ensure competitiveness with TradFi, with arbitrageurs and liquidators maintaining price parity via MEV opportunities. Governance by a consortium of financial institutions provides legal counterparity for operations executed automatically by smart contracts.

Automated Market Makers. AMMs can be used to facilitate trading and price discovery for tokenized RWAs, especially illiquid assets. Wrappers integrate these tokens seamlessly into AMMs, even if complex corporate actions are involved, while hooks enable:

- **Dynamic Liquidity Provisioning:** Adjusting LP positions based on price trajectories, e.g., dirty bond prices relative to stablecoin.
- **Maturity Handling:** Automatically convert expiring bonds on maturity dates into stablecoins.

Proper LP-hooks are essential to minimize impermanent loss and LVR to attract LP, while arbitrageurs ensure efficient price transitions. Total value locked (TVL) requirements for each RWA pool must also be adjusted to provide sufficient liquidity for DeFi lending protocols and compensate LP for coupon payments of the underlying RWA.

4 PRIVACY-PRESERVING ZK ROLLUP

DeFiAM Chain leverages ZK proofs for transaction privacy without compromising compliance. Decentralized identity (DID) solutions ensure KYC/AML adherence of tokens and DeFi protocols for each user.

Transaction Privacy. DeFiAM provides a privacy-preserving architecture that operates with Ethereum as its base layer, ensuring security, availability, and compliance across user interactions. This approach ensures that user transaction details are visible only for involved parties while allowing for regulatory audits.

- Zero-knowledge proofs ensure transaction confidentiality.
- Decentralized identity (DID) solutions support KYC/AML compliance.

*4.0.1 *Interoperability.* The DeFiAM Chain employs the canonical bridge (with transaction ZK proves) to integrate tokens from Ethereum and hyper-chains to communication with other layer-2 networks. Cross-chain communication ensures the effective transfer of digital assets and information across DeFiAM Chain and private layer-1 networks of financial institutions.

5 DEFIAM NODE OPERATORS

While rollups, a form of layer-2 blockchain scaling, benefit from the strong security and decentralization of the underlying blockchain, single-sequencer setups can impact the chain's liveness, MEV dynamics, and transaction finality. ZK rollups, such as DeFiAM Chain, unlike optymisic rollups, are resistant by design to tampering with historical transaction data and invalid block productions. The risks associated with single-sequencer architectures in case of ZK rollups are limited to delayed transaction finality and unfair extraction of MEV (e.g. arbitrage) opportunities. By introducing the DeFiAM Node Operators, a decentralized network of operators, the DeFiAM Chain mitigates these risks. Node operators - financial institutions - stake assets to participate in the network maintenance, earning rewards based on their stake weight when producing blocks by the sequencer. This decentralized system ensures fair transaction finality. It also enables the consortium of financial institutions to govern the platform, especially, smart contacts for DeFi protocols, and actz as a legal counter-party to the platform's clients.

6 POTENTIAL FUTURE WORK

The DeFiAM Chain is designed to support future enhancements; some of planned and potential future extensions include:

- **MEV Auctions:** Minimize MEV risks in permissioned networks through sequencer-run auctions.
- **Improved Latency:** Reduce block production times to 200-250ms for enhanced transaction throughput.

7 CONCLUSION

DeFiAM Chain accelerates institutional DeFi adoption by merging privacy-preserving zk-rollups with tokenized RWAs. By addressing compliance, scalability, and interoperability challenges, it offers a robust platform for regulated financial activities. The innovations presented here enable financial institutions and their clients to seamlessly create new use-case for tokenized RWAs with DeFi protocols while maintaining privacy and regulatory adherence.

ACKNOWLEDGMENTS

This research article is a work of scholarship and reflects the authors' own views and opinions. It does not necessarily reflect the views or opinions of any other person or organization, including the authors' employers. Readers should not rely on this article for making strategic or commercial decisions, and the authors are not responsible for any losses that may result from such use.

REFERENCES

[1] 2023. Cross-border exchange of wholesale CBDCs using automated market-makers. (2023). https://www.bis.org/about/bisih/topics/cbdc/mariana.htm

[2] 2023. Project Guardian - Open and Interoperable Networks. (2023). https://www.mas.gov.sg/publications/monographs-or-information-paper/2023/project-guardian-open-interoperable-networks

[3] 2024. Project Mandala: shaping the future of cross-border payments compliance. (2024). https://www.bis.org/about/bisih/topics/cbdc/mandala.htm

[4] Raphael Auer, Jon Frost, Leonardo Gambacorta, Cyril Monnet, Tara Rice, and Hyun Song Shin. 2021. Central bank digital currencies: motives, economic implications and the research frontier. (2021). https://www.bis.org/publ/work976.pdf

[5] Raphael Auer, Bernhard Haslhofer, Stefan Kitzler, Pietro Saggese, and Friedhelm Victor. 2023. The Technology of Decentralized Finance (DeFi). (2023).

[6] Krzysztof Gogol, Christian Killer, Malte Schlosser, Thomas Boeck, and Burkhard Stiller. 2023. SoK: Decentralized Finance (DeFi) - Fundamentals, Taxonomy and Risks.

[7] Krzysztof Gogol, Johnnatan Messias, Malte Schlosser, Benjamin Kraner, and Claudio Tessone. 2024. Cross-border Exchange of CBDCs using Layer-2 Blockchain. (2024). arXiv:cs.CR/2312.16193

[8] Sky Guo, Joseph Kreitem, and Thomas Moser. 2022. DLT options for CBDC. *Journal of Central Banking Theory and Practice* 13, 1 (2022), 57–88.

[9] Fabian Schär. 2020. Decentralized Finance: On Blockchain- and Smart Contract-based Financial Markets. (2020). https://ssrn.com/abstract=3571335orhttp://dx.doi.org/10.2139/ssrn.3571335

[10] Orla Ward and Sabrina Rochemont. 2019. Understanding central bank digital currencies (CBDC). *Institute and Faculty of Actuaries* (2019).

[11] Sam M. Werner, Daniel Perez, Lewis Gudgeon, Ariah Klages-Mundt, Dominik Harz, and William J. Knottenbelt. 2022. SoK: Decentralized Finance (DeFi). (2022). arXiv:cs.CR/2101.08778