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 node operator network, to enable efficient and regulated financial activities.

1 INTRODUCTION

Blockchain technology has the potential to revolutionize the financial industry by facilitating decentralized, atomic, and trustless transaction execution. Decentralized finance (DeFi) further enhances this potential by offering transparent and automated mechanisms for activities such as trading, lending, and asset management [5, 8, 15, 16]. These capabilities could be transformative for traditional finance (TradFi), particularly in high-value markets like repurchase agreements with $3 trillion in daily transactions and foreign exchange with $7.5 trillion traded daily. Despite this promise, the integration of tokenized real-world assets (RWAs) into DeFi remains limited, hindered by challenges related to scalability, security, and interoperability.

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.
- **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 from Ethereum, and cross-chain communication protocols utilization of assets from private Layer-1 (L1) blockchains.

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

- **RWA Hooks for DeFi:** Customized DeFi protocols and hooks - external smart contracts - designed for tokenized RWAs, enabling the handling of corporate actions and end-to-end value chain management directly on-chain by DeFi smart contracts.
- **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 that operates the DeFiAM Chain ensures fair transaction execution, access to MEV (arbitrage, liquidation) opportunities 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 and DeFi protocols on both public L1 and L2 networks, promoting innovation and collaboration throughout the ecosystem.

2 PRIOR WORK AND CURRENT CHALLENGES

Ethereum established the foundation for programmable blockchains; however, the application of DeFi protocols to tokenized Real-World Assets (RWAs) is hindered by several challenges:

- **Interoperability Barriers:** While DeFi protocols primarily operate on Ethereum and its public rollups, tokenized RWAs are often deployed on private L1 networks that lack EVM compatibility. This disconnect limits the trading volume of tokenized RWAs.
- **Privacy and Compliance Requirements:** Institutional adoption of DeFi requires privacy-preserving features and regulatory compliance, which are not natively supported by public blockchains or DeFi protocols.
- **Composability Issues for RWAs:** RWAs, such as financial instruments, bonds, involve unique corporate actions like coupon payments, which significantly complicate their integration with DeFi protocols.

Despite these obstacles, various projects led by the Bank for International Settlements (BIS) and central banks have demonstrated the transformative potential of DeFi in institutional finance. For example, Project Guardian applied lending protocols and automated market makers (AMMs) for FX market operations [2]. Similarly, Project Mariana utilized a Crypto-Swap-Invariant AMM for cross-currency trading of EUR, CHF, and SGD, further enhanced through a L2 blockchain approach [1, 9]. Most recently, Project Mandala explored programmable compliance using zero-knowledge proofs to validate regulatory requirements [3]. These initiatives highlight the potential of DeFi and RWAs to bridge blockchain technologies to TradFi.

3 RWA INTEGRATION IN DEFI

Integrating tokenized RWAs into DeFi protocols poses significant challenges, even on EVM-compatible blockchain. These challenges, if left unaddressed, can disrupt TradFi processes on-chain, resulting in impermanent loss [6, 11–13] or loss-versus-rebalancing (LVR) [14]

for liquidity providers (LPs) and adverse price impacts for DeFi users [4]. This section introduces external hooks—smart contracts essential for enabling RWAs in decentralized lending and AMMs.

RWA Wrappers. Tokenized financial assets, such as corporate or government bonds, require specialized wrappers to accommodate their unique features, including coupon payments and other corporate actions. These wrappers represent the dirty price of bonds, including accrued interest, making them analogous to reward tokens in liquid staking protocols. Wrappers ensure compatibility with DeFi platforms while maintaining the functionality of RWAs, and are similar to reward-based liquid staking tokens [7].

Repurchase Agreements. On-chain cross-bank lending (repurchase agreements) involves borrowing stablecoins or wholesale CBDCs using tokenized bonds as collateral. Effective integration of RWA wrappers and external hooks into defli lending protocols is critical for [10]:

- **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 interest rates with TradFi markets while providing incentives for financial institutions serving as LPs.
- **Fixed Maturity Handling:** Support of fixed-term loans, which require external hooks to complement DeFi's predominantly perpetual lending models.

These mechanisms enhance competitiveness with TradFi, while arbitrageurs and liquidators maintain price parity through MEV opportunities. Governance by a consortium of financial institutions provides legal counterparty support for transactions executed by smart contracts, and equals the basis for interest rate mechanisms with TradFi.

Automated Market Makers. AMMs are essential for trading and price discovery of tokenized RWAs, especially illiquid assets. Although there exists a multitude of AMMa [17], AMMs are not compatible with RWAs. Wrappers are required for a seamless integration when complex corporate actions are involved,, and external hooks are needed to optimize capital efficiency:

- **Dynamic Liquidity Provisioning:** Automatically adjusting LP positions based on predicted price trajectories, such as dirty bond prices relative to stablecoins.
- **Maturity Handling:** Converting expiring bonds into stablecoins upon maturity, ensuring smooth transitions.

Proper LP strategies and hooks minimize impermanent loss and LVR, encouraging participation from liquidity providers. Arbitrageurs ensure efficient price adjustments. Additionally, the total value locked (TVL) for each RWA pool must be dynamically adjusted to provide adequate liquidity for DeFi lending protocols while compensating LPs for coupon payments on the underlying RWAs.

4 PRIVACY-PRESERVING ZK ROLLUP

DeFiAM operates as a validium, a type of ZK rollup that submits only ZK validity proofs of the blockchain state to Ethereum. This ensures that transactions on the DeFiAM Chain remain invisible to Ethereum users, unlike optimistic rollups where transaction data is publicly accessible via Ethereum.

Additionally, to enhance transaction privacy within the DeFiAM Chain, an additional layer of ZK proofs is implemented. This ensures that transaction details are visible exclusively to the involved parties and (sequencer) operators, while enabling regulatory audits to maintain compliance. This level of transaction privacy is not possible to achieve on the optimistic rollups due to their fraud verification mechanisms that requirs posting full transaction details to Ethereum.

5 INTEROPERABILITY

The DeFiAM Chain employs the canonical bridge (with transaction ZK proves) to integrate tokens from Ethereum and hyper-chains to communication with other L2 networks. Cross-chain communication ensures the utilization of assets and information from private L1 networks of financial institutions.

6 DEFIAM NODE OPERATORS

Rollups, a Layer-2 scaling solution, leverage the security and decentralization of their Layer-1 blockchain. However, single-sequencer setups can affect liveness, MEV dynamics, and transaction finality. Unlike optimistic rollups, ZK rollups are resistant to tampering with historical data and invalid blocks. The primary risks in ZK rollups include delayed finality and unfair MEV extraction, such as arbitrage.

To mitigate these risks, the DeFiAM Chain introduces DeFiAM Node Operators, a decentralized network of financial institutions that earn rewards based on their stake. Operators run their own client nodes that verify the validity proves of the state transitions, without access to the transaction details. This decentralization ensures fair transaction finality while reducing reliance on single sequencers.

7 POTENTIAL FUTURE WORK

The DeFiAM Chain is designed for extensibility, enabling future enhancements to address emerging challenges and optimize functionality. Planned and potential extensions include:

- **MEV Re-distributions:** Integrate MEV mechanisms into the sequencer that permit only back-running MEV activities, such as arbitrage and liquidations, while preventing front-running ones, including sandwich attacks. The revenues generated from MEV should be redistributed to users through DeFi protocols.
- **Improved Latency:** Optimize block production to achieve 200–250ms latency, enhancing transaction throughput.
- **Decentralized Identity (DID):** Integrate DID systems to ensure KYC/AML compliance for tokens and DeFi protocol users.

8 CONCLUSION

The DeFiAM Chain accelerates institutional DeFi adoption by integrating privacy-preserving zk-rollups with tokenized RWAs and DeFi protocols. By addressing compliance, security, and interoperability challenges, it offers a robust platform for regulated financial

activities. Its RWA-hooks to DeFi protocols enable financial institutions and their clients to create new use cases, driving increased trading volumes for tokenized financial instruments.

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] Austin Adams, Benjamin Y Chan, Sarit Markovich, and Xin Wan. 2024. Don't Let MEV Slip: The Costs of Swapping on the Uniswap Protocol. In *Financial Cryptography and Data Security (FC)*.
[5] Raphael Auer, Bernhard Haslhofer, Stefan Kitzler, Pietro Saggese, and Friedhelm Victor. 2023. The Technology of Decentralized Finance (DeFi). (2023).
[6] Robin Fritsch. 2021. Concentrated Liquidity in Automated Market Makers. In *the ACM CCS Workshop on Decentralized Finance and Security (FC-DeFi)*.
[7] Krzysztof Gogol, Robin Fritsch, Malte Schlosser, Johnnatan Messias, Benjamin Kraner, and Claudio Tessone. 2024. Liquid Staking Tokens in Automated Market Makers. (2024). arXiv:cs.CR/2403.10226
[8] Krzysztof Gogol, Christian Killer, Malte Schlosser, Thomas Boeck, and Burkhard Stiller. 2023. SoK: Decentralized Finance (DeFi) - Fundamentals, Taxonomy and Risks.
[9] 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
[10] Lewis Gudgeon, Sam M. Werner, Daniel Perez, and William J. Knottenbelt. 2020. DeFi Protocols for Loanable Funds: Interest Rates, Liquidity and Market Efficiency. arXiv:2006.13922
[11] Lioba Heimbach, Eric Schertenleib, and Roger Wattenhofer. 2022. Risks and Returns of Uniswap V3 Liquidity Providers. In *the 4th ACM Conference on Advances in Financial Technologies (AFT)*.
[12] Lioba Heimbach, Ye Wang, and Roger Wattenhofer. 2021. Behavior of Liquidity Providers in Decentralized Exchanges. In *2021 Crypto Valley Conference on Blockchain Technology (CVCBT), Rotkreuz, Switzerland*.
[13] Stefan Loesch, Nate Hindman, Nicholas Welch, and Mark B Richardson. 2021. Impermanent Loss in Uniswap v3. *arXiv preprint arXiv:2111.09192* (2021).
[14] Jason Milionis, Ciamac C. Moallemi, Tim Roughgarden, and Anthony Lee Zhang. 2022. Automated Market Making and Loss-Versus-Rebalancing. *arXiv preprint arXiv:2208.06046v5* (2022).
[15] 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
[16] 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
[17] Jiahua Xu, Krzysztof Paruch, Simon Cousaert, and Yebo Feng. 2021. SoK: Decentralized Exchanges (DEX) with Automated Market Maker (AMM) Protocols. *ACM Computing Surveys, Vol. 55, No. 11* (2021).