# Enhancing DeFi Security with TokenHook and LeverEdge: Improving ERC-20 Token Protection and Addressing Leveraged Token Shortcomings

**Mohammadreza Rahimian**

**Concordia University, 2025**

ERC-20 tokens have become widely adopted as tools for representing real-world assets on the blockchain. They function as code, running through smart contracts. However, the development of smart contracts has proven to be error-prone, often leading to security vulnerabilities. This study addresses these issues by systematizing 82 known vulnerabilities and best practices. We then introduce a new ERC-20 implementation, TokenHook, which considers all these security aspects. This improved model outperforms widely used ERC-20 templates in terms of security and reliability.

As the blockchain ecosystem evolves, the rise of leveraged tokens (LVTs) presents additional challenges. They extend the features of ERC-20 by adding decentralized finance (DeFi) functionality. Users can buy and sell LVTs like cryptocurrencies but with amplified returns. However, an analysis of over 1,600 LVTs from 10 issuers reveals critical deficiencies due to the absence of a standardized framework, compromising their return on investment. To protect investors, we introduce LeverEdge, a fully decentralized model designed for deploying LVTs on the blockchain. Unlike existing implementations, LeverEdge operates entirely on-chain, overcoming limitations such as transparency, latency, and gas fees through a hybrid L1-L2 approach. With its security carefully tested, LeverEdge provides a potential reference framework for future decentralized LVT deployments.

This progression, from enhancing the security of ERC-20 with TokenHook to developing LeverEdge as a decentralized LVT, contributes to a more secure, transparent, and decentralized approach to DeFi ecosystem.