One-Shot Markets: Redefine Liquidity on the UTXO Ledger

Hai Nguyen Quang
hai@meld.com

Tuan Tran Quoc
tuan@meld.com

September 2021

Abstract

This paper presents One-Shot Markets, a new type of economics model explicitly designed for the eUTXO[1] ledger model of Cardano. The key is to create new markets, loans, and other economic components after consuming one market UTXO instead of maintaining on-chain shared states. This way, different markets can be processed in parallel, while multiple can be consumed together for more liquidity per transaction. This generalized market also allows a single UTXO to act as lending, liquidity, stake, or insurance pool, to be interacted differently to create different outputs per redeemer. While the remaining text is written with the Plutus scripting language and Cardano Native Tokens, the model should adapt to any UTXO ledger that supports scripting and custom tokens.

1 Introduction

Since its inception, DeFi has grown mainly on account-based ledger models. With smart contracts coming to Cardano, there have been numerous attempts to bring those battle-tested designs to the UTXO world. This approach usually leads to unnatural design hacks or poor performance due to the apparent differences at the ledger level. For example, a UTXO can only be spent once creating race conditions for traders swapping on the same liquidity pool UTXO. Workarounds have been proposed, but most sacrifice decentralization, are prone to performance attacks or are capital-inefficient.

This paper proposes a new economics model explicitly designed for the UTXO ledger. We call it One-Shot Markets as each UTXO is a local market with a lifetime of a single transaction. Each time a UTXO is spent, its market is closed to open more markets, loans, and other economic components. The whole economics picture can still be drawn and analyzed by bringing all UTXO markets together. Another fundamental design choice is to move price discovery off-chain, with a well-thought incentive structure for liquidity providers to stay close to the market price. This simplification of on-chain validators usually leads to fewer edge cases, better security, transaction size, and fees.