Intention Is All You Need

Kasey White
byword-hitters.9h@icloud.com
Cardano Foundation

Lucas Rosa
todo
Input Output Global

Abstract

This paper introduces a novel approach to account abstraction on UTxO ledger based blockchains. We present a system where users sign intentions—fragments of desired transaction elements—rather than complete transactions. Our smart contracts abstract ownership of an address to a quorum of keys stored in a UTxO while validating that user intentions are fulfilled in the final transaction. This approach provides increased security through multi-signature capabilities, simplifies user interaction with blockchain assets, and enables new wallet features for more efficient DeFi applications including orderbook exchanges, atomic swaps, and sequencer services for interactions with global state.

Keywords Cardano · UTxO · Account Abstraction · Blockchain

1 Introduction

Blockchain users often tie airdrops, protocol rewards, stake control, asset ownership, and user identity to a single address. In traditional UTxO-based blockchains like Cardano and Bitcoin, these addresses are typically formed from a single key, creating potential for significant security vulnerabilities. If that key is lost or stolen, all associated funds are compromised. Additionally, interacting with malicious sites can lead to complete fund drainage through deceptive transaction signing requests.

This paper introduces Bullet, a novel approach to account abstraction on UTxO-based blockchains that fundamentally transforms how users interact with their assets. Rather than managing individual UTxOs and signing complete transactions, Bullet enables users to focus solely on the value leaving their account and the specific actions they want to execute.

At the core of our approach is the concept of intention validation. Instead of signing entire transactions with specific inputs and outputs, users sign intention messages that specify only fragments of what they want included in a transaction and the fee they're willing to pay. Smart contracts then validate that these intentions are properly fulfilled when the transaction is executed, regardless of who builds the final transaction.

Bullet provides several key advantages over traditional UTxO management:

- Enhanced security through multi-signature support with customizable quorum requirements
- Flexible key management with different types of signing keys (cold, hot, and wallet-specific)
- Improved user experience by abstracting away the complexity of UTxO management
- An account-centered approach that simplifies both wallet interfaces and DApp interactions
- Protection mechanisms that shield assets from potential DeFi vulnerabilities

Our work represents a significant step toward combining the security benefits of UTxO-based systems with the usability advantages typically associated with account-based blockchains like Ethereum, all while introducing new capabilities through the intention validation mechanism.

2 Background

Account abstraction seeks to enhance blockchain usability by separating ownership validation from transaction logic, simplifying user interactions while maintaining security. While account-based blockchains have established standards for account abstraction, UTxO-based blockchains lack comparable solutions despite their widespread adoption.

2.1 UTxO Model

Cardano, Bitcoin, and other blockchains use a ledger model called UTxO (Unspent Transaction Output). Value transfers are written as a series of inputs (spent outputs) and outputs, each with a unique identifier. In this model, users sign complete transactions, verifying they control the inputs being spent.

This design creates specific challenges for user experience and application development:

1. Contention issues arise when multiple users attempt to interact with a UTxO representing global state. Since a UTxO must be unspent before inclusion in a transaction, users race to consume it, with only one succeeding while others' transactions fail.
2. Failed transactions require users to sign entirely new transactions, creating poor user experiences in high-contention scenarios like decentralized exchanges (DEXs) where a liquidity pool might be represented by a single UTxO.
3. Complex operations require careful construction of transaction inputs and outputs, placing significant burden on wallet implementations.

However, the UTxO model offers security advantages as transaction outcomes are explicitly defined in the transaction itself, rather than computed during execution as in account-based models.

2.2 Intentions

An intention is a signed message that contains a user's authorization to perform a specific action within a transaction. Unlike traditional UTxO transactions where users sign complete transactions with predetermined inputs and outputs, intentions specify only fragments of desired transaction elements.

The structure of an intention typically includes:

- The specific action to be performed
- The fee the user is willing to pay for this action
- The address responsible for paying the fee
- The signature(s) of the address owner validating the intention

This approach allows users to authorize specific actions without needing to construct or sign complete transactions. By validating intentions rather than complete transactions, we can maintain the security properties of UTxO models while addressing their usability limitations.

We have developed a series of smart contracts that offers hot and cold multisignature schemes that are stored in an onchain state managed by the user. In addition, our solution introduces a vault mechanism to shield assets from usage in DeFi applications and from malicious wallet drainers."

3 Bullet

Bullet is a comprehensive system for account abstraction on UTxO-based blockchains implemented as a series of micro-validators. These validators are linked via a proxy contract to minimize execution costs for users. The architecture employs both direct validator parameterization (using validator hashes) and indirect linkage through global state in datums or token names, creating a flexible yet secure validation framework.

The system addresses key challenges of UTxO-based blockchains by allowing users to interact with their assets through intention signatures rather than complete transaction signing. This approach significantly improves user experience, particularly in high-contention scenarios like DeFi applications, while maintaining the security benefits of the UTxO model.

3.1 Hot and Cold Multisig Credentials

Bullet implements a sophisticated key management system through hot and cold multisignature credentials:

Hot Keys provide flexibility for day-to-day operations:
- Normal spend transactions (e.g., sending assets to friends)
- Signing intentions for DeFi interactions
- Actions related to staking or voting in blockchain governance
- Limited access to Vault UTxOs (requiring a higher quorum threshold of signatures)

Cold Keys offer enhanced security for critical operations:
- Access to spending when hot keys are unavailable (e.g., offline servers) or lost
- Authority to modify credential state, including updating both hot and cold key sets

This dual-key approach allows users to balance convenience with security, implementing appropriate protection levels for different transaction types. The system supports multiple signature schemes including Schnorr, ECDSA, and Ed25519, providing compatibility across various wallet implementations and key management practices.

3.1.1 Signing a Transaction

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim aeque doleamus animo, cum corpore dolemus, fieri tamen permagna accessio potest, si aliquod aeternum et infinitum impendere malum nobis opinemur. Quod idem.

3.2 Fund Management

Bullet introduces advanced fund management capabilities through its Vault mechanism. This feature allows users to designate specific UTxOs that require elevated security for spending:

- Vault UTxOs require either a greater quorum of hot key signatures or cold key authorization
- This creates a clear separation between freely available funds and secured assets

- Users can maintain a small portion of funds for normal spending or DeFi interactions while protecting the majority of their holdings
- The mechanism helps protect against draining attacks or misuse by DApps

As an additional benefit, this structure enables off-chain indexers to track how much value Bullet users allocate to DeFi applications versus secured storage, potentially serving as an indicator of DeFi ecosystem health.

For a user to specify a UTxO as a Vault UTxO, they simply need to create that UTxO with a Vault type datum from the Bullet Datum types.

3.3 Intentions in Bullet

Intentions form the core innovation of Bullet, representing a paradigm shift in how transactions are authorized in UTxO-based systems. Unlike traditional transactions where users sign complete input-output structures, an intention is a signed message specifying:

1. A fragment of desired transaction elements (constraints)
2. The fee the user is willing to pay
3. The address paying the fee
4. Authentication signatures

Bullet implements intentions through a sophisticated validation engine with several components:

Validation Flow:
- Analysis of redeemer data containing intention lists
- Per-user intention processing including signature validation
- Constraint system validation against transaction structure
- Value movement tracking and verification
- Final verification of intention completion

Constraint System:
- Output constraints: specifying address, value, datum, and reference requirements
- Input constraints: validating existing UTxOs being consumed
- Signature requirements: ensuring proper authorization
- Minting policies: controlling token creation
- Time bounds: enforcing valid time ranges
- Contract Execution: enforcing the presence of contract executions in the transaction

Execution Models:
- Sequential execution: using incrementing nonce values
- Parallel processing: using UTXO references as nonces
- Combined models supporting multiple users with different execution patterns

This flexible constraint system enables complex transaction patterns while maintaining security and predictability. The approach allows transaction builders (who may not be the original signers) to include user intentions in their transactions, opening possibilities for third-party transaction construction and fee markets.

3.3.1 Temporary Value System

The temporary value system is a simple yet powerful mechanism in Bullet's intention validation that passes data between constraints. It works as follows:

- Starts as `None` and can be set by certain constraints (input, reference input, redeemer validation)
- Subsequent constraints can use this value for validation decisions or output construction
- Once used, each constraint typically updates the temp_val for the next constraint
- Enables data extraction from one part of a transaction to influence validation in another

This creates a validation flow where information can be chained through multiple constraints, allowing for dynamic transaction structures without compromising security.

3.3.2 Signing an intention

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim aeque doleamus animo, cum corpore dolemus, fieri.

4 Applications in DeFi

Bullet's intention-based approach solves key challenges in DeFi applications on UTxO-based blockchains, enabling more efficient and user-friendly experiences across multiple use cases.

4.1 Orderbook DEX

Traditional orderbook DEXs on UTxO blockchains face significant limitations:
- Users pay transaction fees for placing orders even if they're never executed
- Order contention requires signing new transactions when targeted orders are already taken
- Market responsiveness is limited by blockchain confirmation times

Bullet addresses these issues through its intention mechanism:
- Users create orders via intentions but only pay when orders execute ("pay-on-execution")
- Multiple orders can be created rapidly to follow market movements
- A single signed intention remains valid regardless of UTxO contention
- The fee is satisfied from any available UTxOs, eliminating the need for re-signing when transactions fail

This approach creates a more efficient orderbook experience with reduced costs and improved market responsiveness for traders.

4.2 Atomic Swap

Bullet enhances atomic swap capabilities by allowing multiple intentions to be combined in a single transaction with flexible user conditions. Key benefits include:

- Multiple parties can participate in complex exchanges without requiring direct coordination
- All-or-nothing execution ensures transactions either complete fully or fail completely
- New use cases like atomic flash loans become possible, where borrowed value must be returned within the same transaction
- Risk is minimized as failure results in no value movement

This creates more robust peer-to-peer trading possibilities while maintaining the security guarantees of atomic execution.

4.3 Sequencer Ordering

When accessing global state in UTxO blockchains, contention creates significant user experience challenges. Bullet transforms this model:

- Users sign intentions to utilize global state without directly handling contention
- Transaction builders (sequencers) combine multiple user intentions into single transactions
- Sequencers, better equipped for rapid signing, handle contention for global state UTxOs
- Users experience reliable interaction regardless of underlying contention

This approach is particularly valuable for high-demand protocols where global state access (like liquidity pools or lending markets) creates bottlenecks in traditional UTxO designs.

5 Interoperability

Bullet supports cross-chain key compatibility through multiple signature schemes to create a more accessible user experience.

To enable a “drop-in experience” for users with existing blockchain wallets, Bullet allows for Secp256k1 and Schnorr signature schemes alongside the native Ed25519 keys used in Cardano. This allows private keys commonly derived for either Secp256k1 (used in Bitcoin, Ethereum, and many EVM chains) or Schnorr to be used in Bullet without requiring users to generate new keys.

The implementation uses an alternative message signing approach necessitated by the constraints of the UTxO model. Since providing external signatures to a transaction would alter the transaction hash itself, Bullet derives the message to be signed from the script context available during on-chain execution:

1. The on-chain Plutus script accesses its execution context
2. Inputs and outputs from this context are serialized
3. This serialized data is hashed to create a consistent message
4. The resulting message can be signed by any supported key type
5. The signature can be provided to the transaction without changing the message hash

This technical approach is the only viable method for supporting these additional signature schemes within the constraints of the system. While broader protocol-level interoperability features are not currently implemented, wallet integrations are in development to provide seamless experiences across different blockchain ecosystems.

6 Conclusion

This paper has introduced Bullet, a novel approach to account abstraction on UTxO-based blockchains that fundamentally transforms how users interact with digital assets. By implementing an intention-based validation system, we have demonstrated that the traditional limitations of UTxO models can be overcome while preserving their security benefits.

The most significant contribution of our work is the paradigm shift from transaction building to intention building. Rather than requiring users to construct and sign complete transactions with precise input-output relationships, Bullet enables users to express only what they intend to accomplish, delegating transaction construction to builders who can optimize execution. This approach dramatically improves user experience, particularly in high-contention scenarios like DeFi applications.

Additionally, by separating keys from addresses and implementing user-controlled state, Bullet provides enhanced security through multisignature schemes and enables key rotation capabilities not previously available in UTxO systems. The vault mechanism further protects user assets from potential vulnerabilities, creating a more robust security model.

The applications in DeFi demonstrate that this approach addresses critical pain points in existing implementations, from reducing costs in orderbook exchanges to eliminating contention issues when accessing global state. The ability to combine multiple intentions into atomic transactions opens new possibilities for complex financial operations while maintaining deterministic execution guarantees.

Integrations with existing ecosystem applications like DexHunter are currently in progress, which will provide real-world validation of these concepts. As adoption grows, we anticipate that the intention-based model will become a standard approach for blockchain interactions, bridging the usability gap between UTxO and account-based systems while introducing new capabilities that neither could achieve independently.

By focusing on what users intend to accomplish rather than how transactions are structured, Bullet represents a significant step toward more intuitive, secure, and efficient blockchain systems that can better serve both individual users and decentralized applications.