Reference ■ How Midnight works ■ Building blocks

Building blocks

Midnight's transaction structure is unique and may not be immediately intuitive. This section covers the structure of transactions, their effects, and what makes them *tick*.

Transactions

In Midnight, transactions consist of:

- a 'guaranteed' Zswap offer
- an optional 'fallible' Zswap offer
- an optional contract calls segment, consisting of:
  - a sequence of contract calls or contract deploys
  - a cryptographic binding commitment (see: transaction integrity)
- a binding randomness (see transaction integrity).

Contract deployments

A contract deployment creates a new contract if it does not already exist and fails otherwise. It is executed entirely as part of the 'fallible' execution step.

Ask AI

Feedback

Contract deployment transaction parts consist of a contract state and a nonce, creating a new contract at the address that is a hash of the deploy part.

Contract calls

A contract call invokes a specific contract address and entry point at this address. Entry points are keys into the contracts' operation map. Combined, the two select the verifier key that a contract call will be validated against.

A contract call declares a guaranteed and fallible *transcript*, which declares the visible effects of this call. It further contains a *communication commitment*, which may be used for cross-contract interaction.

> INFO
>
> Cross-contract interaction is still under development and is not available for use at this time. The team is keen to hear what kinds of interactions you would like to be able to do.

Finally, a contract call includes a zero-knowledge proof that the transcripts are valid for this contract and binding to other transaction elements.

Merging

Zswap permits atomic swaps by allowing transactions to be merged. Currently, contract call sections cannot be merged, but two transactions can be merged if at least one of them has an empty contract call section. This outputs a new, composite transaction and has the effect of both input transactions combined.

Feedback

Transaction integrity

Midnight inherits the basic transaction integrity mechanism from Zswap, which, due to the ability to merge, uses Pedersen commitments for transaction integrity. These commitments commit to the value of each input and output of a transaction and are homomorphically summed before the whole transaction is checked for integrity by opening the composite commitment. Only people who created the individual components of the transaction know the opening randomnesses summed to decompose the transaction. This ensures a form of binding that guarantees that the user's funds are spent as they originally intended.

This binding is extended to contract calls by the contract call section contributing to the overall Pedersen commitment. This contribution is further restricted to carry no value vector, by requiring knowledge of an exponent of the generator, in the form of a Fiat-Shamir transformed Schnorr proof.

Feedback