Lifecycle of a CAPE Transaction

CAPE transactions consist of:

- A transaction specification in which the user designates:
-
    - A recipient address and encryption key
-
    - An asset type and amount being transferred
- *
- User private keys that enable consuming input records
- Auxiliary information about input records obtained from the CAPE smart contract
- A testnet CAPE “fee” asset record: As a technicality, CAPE transactions require an asset record of a specific asset type (called the “CAPE fee asset type”) to be included. During the testnet phase, transaction fee amounts are set to 0. Despite the fee amount being zero, an asset record with the CAPE fee asset type is still required. This can be retrieved from the CAPE faucet. Fee payment does not expose transaction details.
-

Please note that this is a testnet “fee” token for demonstration only, not for value transfer or exchange. There is no CAPE token sale or other distribution happening or currently planned.

With this information the transaction can be built containing:

- The nullifiers of the input records
- The record commitments of the outputs
- A memo consistent with the asset policy
- A zero-knowledge proof that ensures all the data of the transaction is correctly computed
-

Owner memos, which encrypt information corresponding to the output records necessary for the recipient to spend them, and binds them to the transaction. The resulting transaction can safely be submitted to the CAPE system and the owner memos can be published.

The CAPE system meets the following requirements:

- The transaction cannot be linked to the sender or recipient without a designated viewing key
- Transaction details including amount and asset type are encrypted
- Transaction validation is performed by verifying a zero-knowledge proof, and checking the nullifiers are all distinct and have not been published before, and thus cannot be spent multiple times
-

The computation required to construct a transaction must be performed by the user or an entity the user trusts. The transaction itself, on the other hand, is a cryptographic object that may be verified by anyone without the underlying transaction data being revealed, with the exception of the CAPE fee amount.

CAPE currently supportswrapping ERC-20 tokens, with support for ERC-721 tokens planned. In order to transform an ERC-20 token into a CAPE asset record (wrapping), the user calls thedepositErc20 function of the CAPE contract. The contract validates the parameters of the call and updates the CAPE contract state with a new asset record corresponding to the ERC-20 token transfer.

The reverse operation (unwrapping), converting some wrapped asset records back to ERC-20 tokens, is done by submitting a “burn” transaction to the CAPE contract. This transaction is processed in such a way that the asset records are burned (made unspendable) and the equivalent in ERC-20 tokens are unlocked to a specified Ethereum address.

Previous Asset Creation + Definition Next CAPE System Components Last updated1 year ago On this page