Your keys. Your crypto. Your trade.

Self-custodial crypto trading
powered by 100% distributed liquidity.

swopblock

WHITE PAPER

MORE INFO:
swopblock.org
info@swopblock.org
github.com/swopblock
@swopblock

LIQUIDITY STREAM SPECIFICATION:
TRANSFER PROTOCOL

ABSTRACT

The SWOBL Exchange Protocol is a protocol used for storing and transferring SWOBL as a non-native digital cash on multiple blockchains. SWOBL is represented by sums of unsigned integers that sum to 52,800,000 in aggregate.

Swopblock will survey and record SWOBL investment perks and implement a sub-ledger with genesis entries that associate the perk SWOBL with one or more cryptos at one or more native addresses of the cryptos that then can be transferred using exchange transactions that preserve the quantity of the SWOBL perks and preserve self-custody even while changing custody of the crypto.

INTRODUCTION

In blockchain transaction implementations, outputs represent a quantity of native crypto. With the SWOBL Exchange Protocol, these outputs can encapsulate a quantity of SWOBL comingled with a native crypto amount for multiple blockchains to enable cross-blockchain exchange.

APPLICATIONS

Swopblock is developing software applications that will provide an infrastructure to facilitate autonomous trade and exchange between peers.

A bank could back SWOBL by a cash reserve, then people could withdraw and deposit money in SWOBL, or use it to pay for goods and services. This would allow a system for transaction not only in SWOBL, but in any currency.

Equity could be associated with SWOBL on a new blockchain. Capital fundraising and future dividends and interest could be traded among companies by shareholders to start new companies or expand existing ones.

OVERVIEW

Inputs using the SWOBL Exchange Protocol to store SWOBL have elements that are explicit (present in output meta-data) or implicit (not present in output meta-data), the elements as follows:

Asset Id is an identifying hash of a particular block in a particular blockchain.

Asset is an unsigned integer that represents the number of units of native blockchain crypto that are stored on Inputs

Cash Id is a hash of the output referenced by the first input of a Swopblock LLC launch transaction that initially issued SWOBL Cash on a particular blockchain as the blockchain genesis of SWOBL for that blockchain. There after any user will be enabled to issue by protocol onto the launched block-chain the SWOBL they own. Swopblock will retain the private key for the Cash Id to issue SWOBL but after the launch transaction the absolute power to issue SWOBL will be disabled permanently by protocol and only the power to issue that all users have by protocol will be retained in Swopblock's private key. This launch protocol will serve as a performance bond to guarantee the initial value of SWOBL on the launch blockchain. Each blockchain will have at least one Cash Id.

Cash is an unsigned integer that represents the number of units of SWOBL that are stored on Inputs.

Uncirculated Cash is an unsigned integer that represents the number of units of SWOBL that are uncirculated and are available to become circulated.

OVERVIEW

(continued)

Circulated Asset is an unsigned integer that represents the number of units of native blockchain crypto that are circulated and have storage on an input.

Cash Volume is an unsigned integer that represents the number of units of native blockchain crypto that have been circulated or uncirculated in transfers from one input to another.

TRANSACTIONS

Transactions relevant to the Liquidity Stream Protocol must have meta data payloads for the explicit elements of the protocol. This allows clients to recognize such transactions. Transactions can then be used to issue remaining SWOBL Cash on new blockchains, or transfer ownership of Cash and Assets.

Transactions that are not recognized as Liquidity Stream transactions are considered as having all their outputs uncirculated and all their inputs remain unchanged with respect to Cash storage.

PAYLOADS

Outputs are either circulated and have encapsulated SWOBL and have sub elements defined, or uncirculated and have no encapsulated SWOBL and have no sub elements.

Protocol outputs can have a zero or non-zero native crypto value. Protocol outputs are circulated and contain a parsable meta data payload. If multiple valid protocol outputs exist in the same transaction, they are parsed according to output order, and the other outputs are considered as regular uncirculated outputs. If no valid protocol output exists in the transaction, all outputs are considered uncirculated.

The payload is defined by field names and descriptions as follows:

NAME: DESCRIPTION

Mark: Tag indicating transaction is a Liquidity Stream transaction.

Version: Major revision number of the Liquidity Stream Protocol.

PAYLOADS

(continued)

Output: Represents the outputs of a protocol transaction

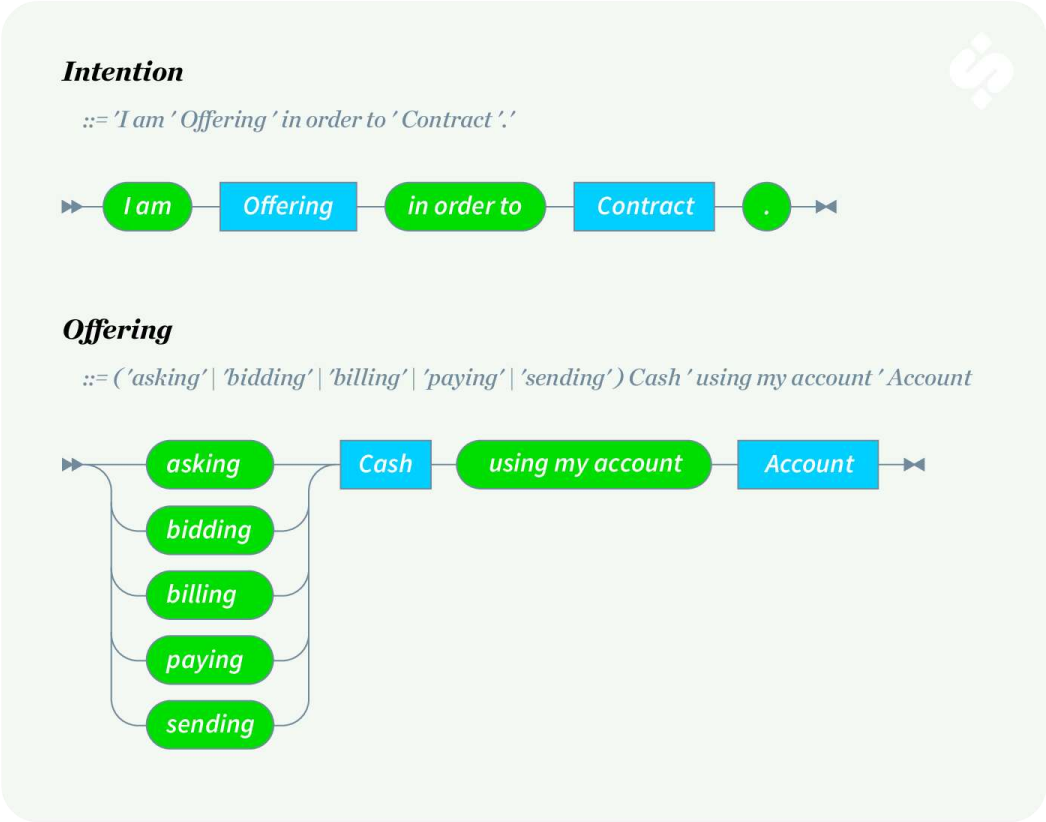
Output Count: Represents the number of outputs in the Output List field.

Output List: A list of zero or more outputs representing either a Circulated Output or an Uncirculated Output of the transaction outputs in their order.

The Output List is used to determine the quality and quantity of each output of the protocol transaction. If the protocol output is malformed, it is considered non-parsable. Coinbase transactions and transactions with zero inputs cannot have a valid protocol output, even if it would be otherwise considered valid.

Circulated Output: Represents an intention of a user to place an order involving the circulation of SWOBL cash. If there are less items in the Output List than the number of Outputs, the outputs in excess receive a Cash quantity of zero. If there are more items in the Cash List than the number of circulated outputs, the protocol output is deemed invalid.

The User Intention is defined by fields that have binary and text renderings as follows:

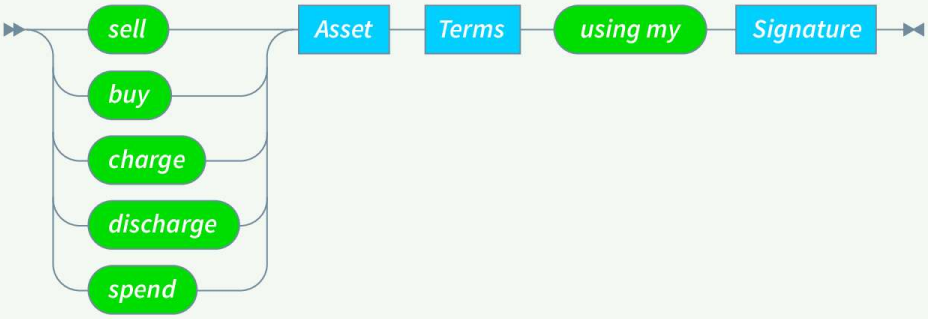


PAYLOADS

(continued)

Contract

::= ('sell' | 'buy' | 'charge' | 'discharge' | 'spend') Asset Terms 'using my ' Signature



Terms

::= 'and the order is good while the market volume is ' Amount

Cash

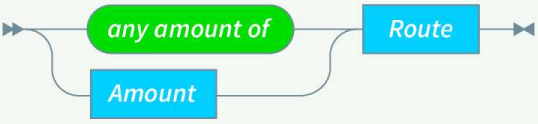
::= Amount 'SWOBL'

Account

::= Route Number

Asset

::= ('any amount of' | Amount) Route



PAYLOADS

(continued)

Amount

::= ('exactly' Number | AtLeast | AtMost | Range)

Route

::= ('BTC' | 'ETH')

AtLeast

::= 'at least' Number

AtMost

::= 'at most' Number

Range

::= AtLeast 'and' AtMost

PAYLOADS

(continued)

The Asset transfer quantity of an output is consistent with the exchange equilibrium equation as follows:

Let ***H*** denote the amount of the Uncirculated Cash.
Let ***increase(H)*** denote an increase to the Uncirculated Cash (Offering).
Let ***decrease(H)*** denote a decrease to the Uncirculated Cash (Contract).

Let ***A*** denote the amount of the Circulated Asset.
Let ***increase(A)*** denote an increase to the Circulated Asset (Contract).
Let ***decrease(A)*** denote a decrease to the Circulated Asset (Offering).

Let ***net(A)*** be the net Asset transfer quantity ***(increase(A) – decrease(A))*** of a circulated output.
Let ***net(A)*** be the net Cash transfer quantity ***(increase(H) – decrease(H))*** of a circulated output.

Then the exchange equilibrium equation is as follows:

$$(H + increase(H)) * (A - decrease(A)) = (H - decrease(H)) * (A + increase(A))$$

ISSUANCE

All the outputs marked for SWOBL issuance and with a non-zero asset quantity get assigned the Cash ID defined as a hash of the output referenced by the first input of the transaction.

TRANSFER

All the output orders must be valid before transfers can be valid. This includes Cash and Asset availability for the order in sufficient quantity before the expiration of the order determined by the Terms of the order by comparing the Terms Cash Volume thresholds to the actual Cash Volume needed to lock-in the order as valid for execution.

Inputs are seen as a sequenced flow of both Cash and Asset that is serialized into the Outputs where the Inputs are emptied in order of their index and Outputs are filled in order of their index and any unfilled Outputs are invalid and any left-over Inputs are still available to another transaction of the same account.

CHARACTERISTICS

The whole cryptographic infrastructure of the blockchains provided for securing the spending of outputs is reused for securing the ability to trade assets. There is a symmetry between "an address + private key" as a way to spend on the blockchains, and "an address + private key" as a way to trade assets.

Issuance is based on the invocation of the exchange equilibrium equation which makes it impossible to issue more than the 52,800,000 SWOBL that is defined in the genesis transactions.

HAVE QUESTIONS?

Contact ***jeff@swopblock.org*** for further inquiries and questions.

swopblock.org
info@swopblock.org
github.com/swopblock
@swopblock