PRCY Exchange integration

What is it?

PRCY uses integrated addresses with payment id's in order to uniquely identify transactions sent to an exchange privacy account. The implementation of this is operationally similar to Monero.

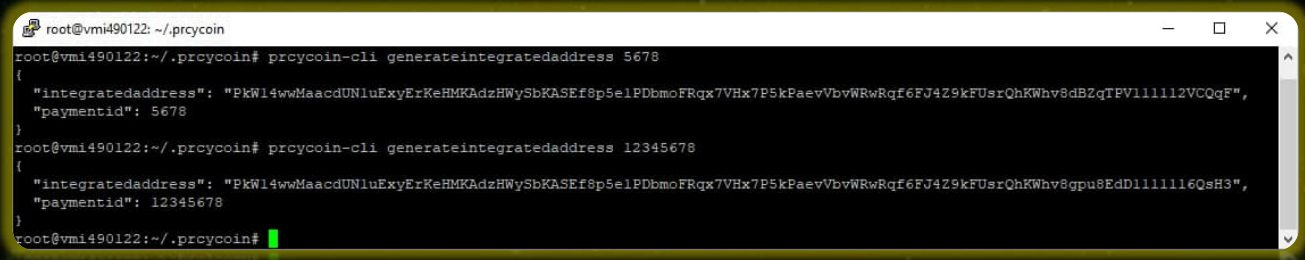
How does it work?

PRCY has 2 different address types:

1. Master Privacy Account - single account per daemon
2. Integrated addresses - multiple per Master Privacy Account

When a user creates an account on an exchange, their user id (payment id) is added to the address creation in order to generate a unique sub-address within the exchange privacy account.

Here is an example:



All transactions that are sent to the same integrated address will have the same payment Id data in the transactions.

- Please note that all PaymentID's must be positive numbers.

All PRCY Integrated addresses are created under the single Master Privacy Account.

In order to see what transactions the privacy account has recently received the exchange can use ListSinceLastblock.
The exchange can then iterate through each of the transactions and use GetRawTransaction in order to determine whether the transaction was indeed intended for them or not and if so, what the direction was and what the different vins and vouts were.

Here is an example:

Suppose your exchange master privacy account is:

PakdxgDtXqiDUc7VbV34sGiMNey69gcU3AHz2UmzykAa8EvPwZP6g2nF5PAAMEHMnja2AEVYk
PeJ14VEZ5zGjeYu12gYCPiZz5N

You generate an integrated address using GenerateIntegratedAddress with a payment ID (unique id) of 5555 for a user:

PkTJyV3P97EDUc7VbV34sGiMNey69gcU3AHz2UmzykAa8EvPwZP6g2nF5PAAMEHMnja2AEVY
kPeJ14VEZ5zGjeYu8RWhLL18X1H111111jaVPj

If the user wants to deposit to the exchange, they will send [x] PRCY to the **integrated address**
The transaction will have:

1. The payment ID 5555
2. A transaction output destined to the exchange payment id
3. A transaction output destined to the user (change)

The exchange checks that:

1. Payment ID: 5555 => transaction depositing to the users exchange account
2. Transaction output 1 destined to the exchange wallet => the depositing amount

If the payment ID in a transaction does not match with any one of your users' payment IDs, but one of the outputs belong to the exchange wallet then this can be considered a non-depositing transaction and hence can be considered as a donation.

What fields are there to indicate relevant data for an exchange?

The following are the main fields that exchanges should focus on:

1. The user is never inputting the payment id into the transaction, the payment id is included in the address details and is displayed in the transaction output.
   Users can never manually create a payment id and add it to a transaction.
2. isMine is a bool flag that indicates to the caller whether or not they can decode the transaction.
3. If the direction = deposit then the vout[decoded_amount] field is the total amount deposited.
4. If the direction=withdrawal
   Then the amount sent needs to be computed as
   Sum(vins[IsMine=true][decoded_amount]) - vout[decoded_amount] - fees.

PRCY uses Stealth Addresses. Therefore no address data can be used to identify the sending or receiving address in any transaction. If the exchange desires to use only addresses in order to identify users then the exchange must call GenerateIntegratedAddress <paymentid> again in order for the system to regenerate the address based upon the given payment ID in the transaction.
The generated address will not differ from the original integrated address as the 2 keys used for the generation - private key and payment id - are still the same.
This is however not the recommended path to take.
We suggest that the exchange uses user id's and payment id's as the linking method.

General information

1. GetRawTransaction is the RPC call used to get the raw hex transaction details that includes the payment id.
2. DecodeRawTransaction is then called and passed the output from the Getratransaction as a parameter.
3. **Payment id's and other transaction details can only be read by the owner of the integrated address - in this case, the exchange - or the intended receiver and calling GetRawTransaction on any transaction that is not owned by either the sender or receiver will not disclose the transaction details.**

Please see the attached files for withdrawal examples.

Relevant Links:

Github: https://github.com/PRCYCoin
Email: admin@prcycoin.com
Website: https://prcycoin.com
Telegram Support channel:
Private Telegram / Discord chats will be set up at integration time for support purposes.

Team PRCY