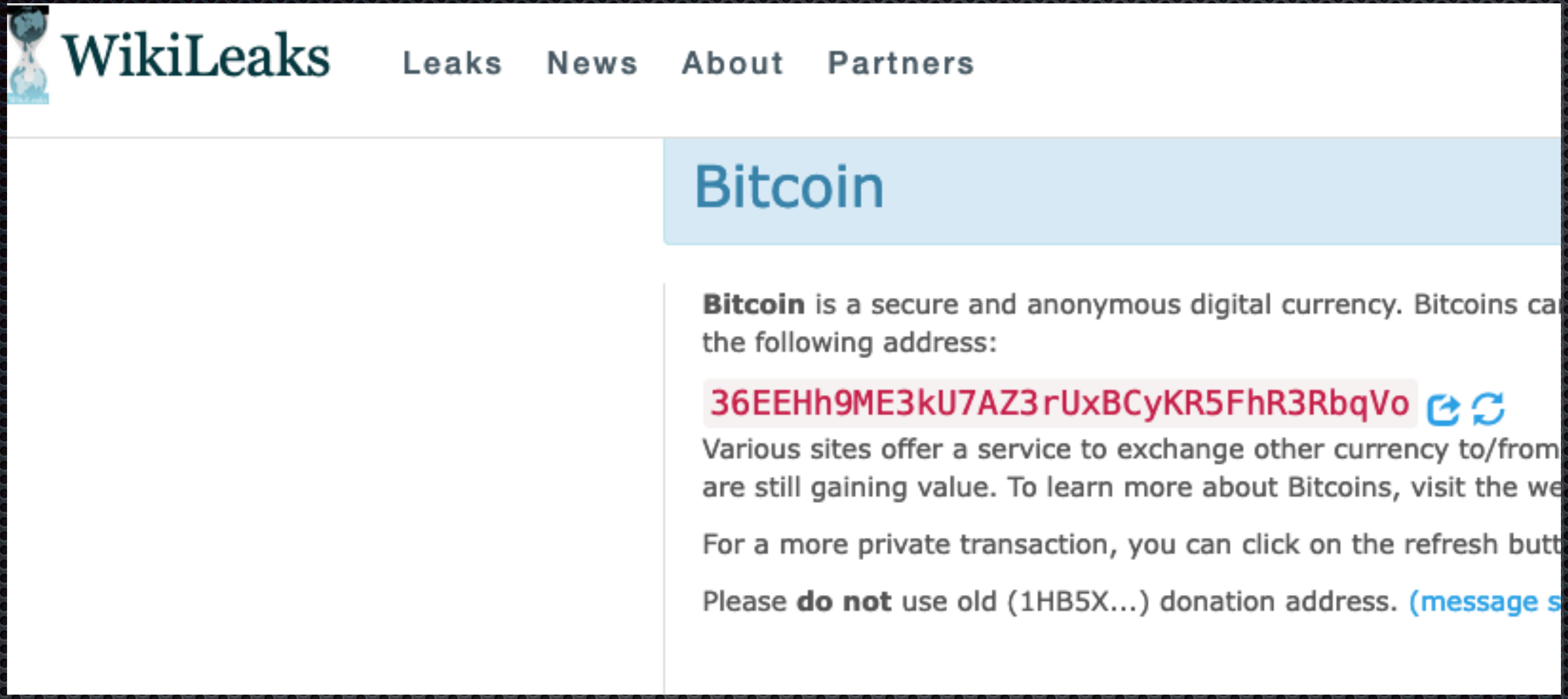
[XTX]

PayNyms

Dublin Bitcoiners Meet Up

Options for receiving Bitcoin payments or donations

- Post a static address (which is **terrible** for privacy).



WikiLeaks Leaks News About Partners

Bitcoin

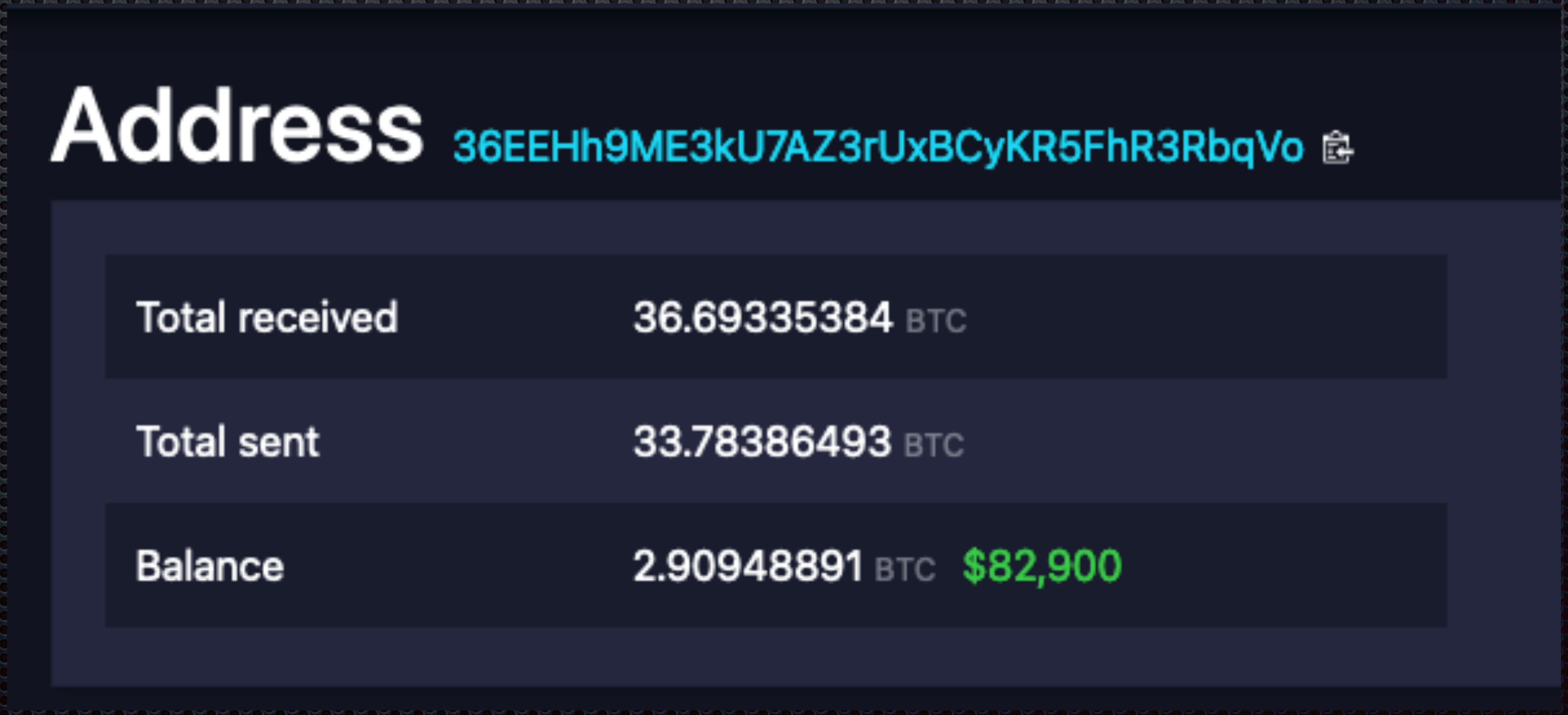
Bitcoin is a secure and anonymous digital currency. Bitcoins ca the following address:

36EEHh9ME3kU7AZ3rUxBCyKR5FhR3RbqVo

Various sites offer a service to exchange other currency to/from are still gaining value. To learn more about Bitcoins, visit the we

For a more private transaction, you can click on the refresh butt

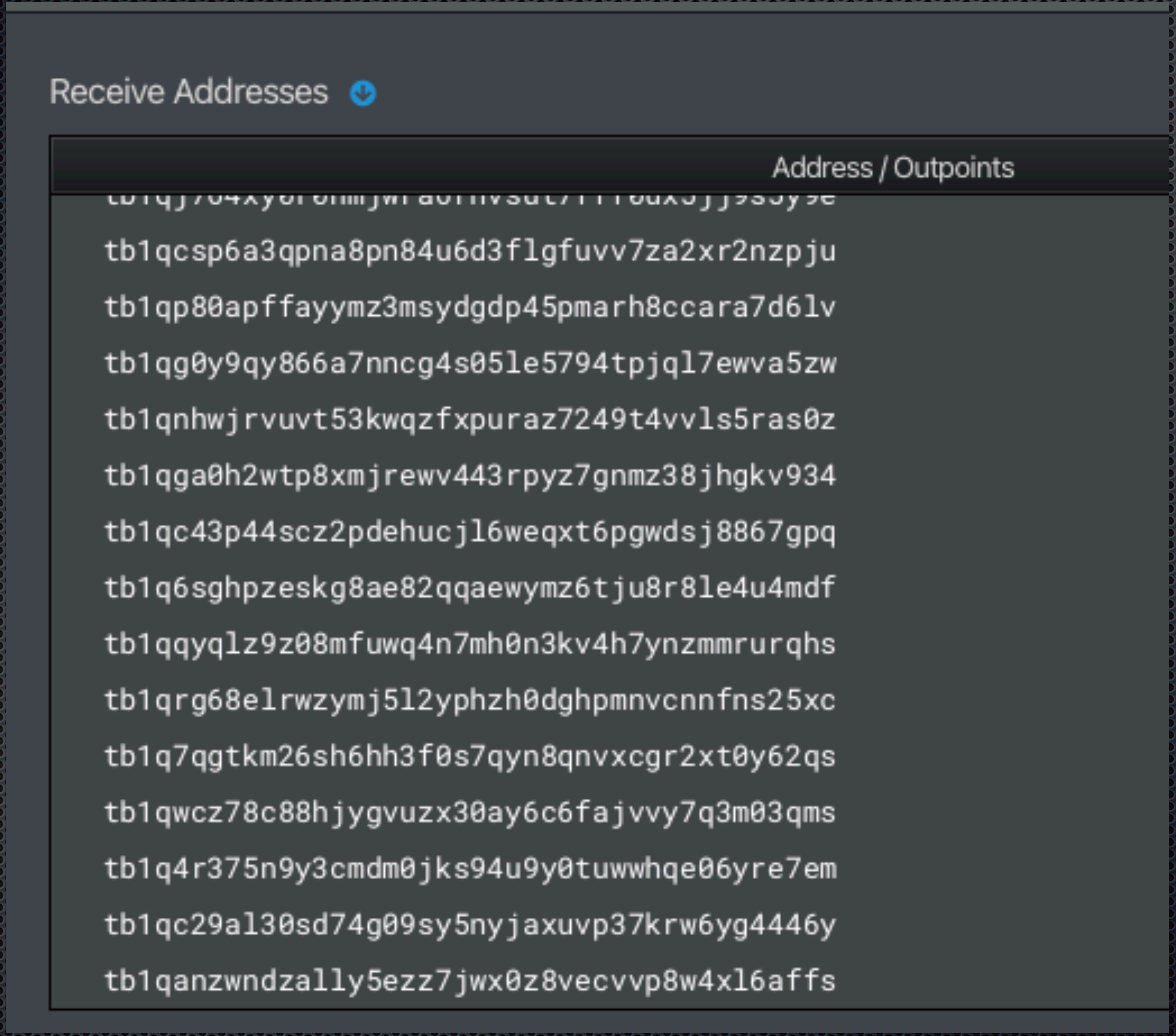
Please **do not** use old (1HB5X...) donation address. (message s



Address 36EEHh9ME3kU7AZ3rUxBCyKR5FhR3RbqVo

Total received	36.69335384 BTC
Total sent	33.78386493 BTC
Balance	2.90948891 BTC $82,900

- Manually generate a new address for each transaction (not scalable).

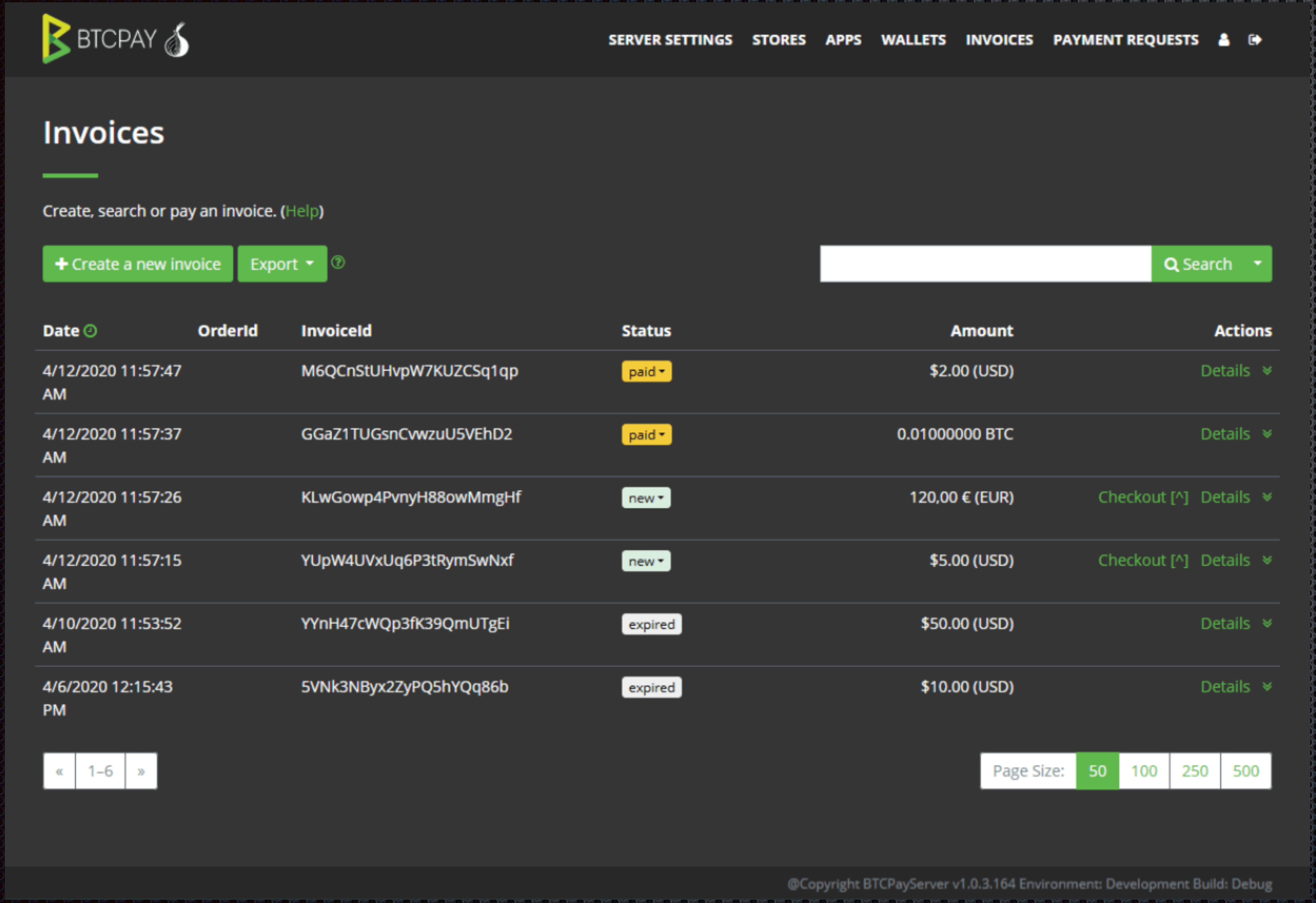


Receive Addresses

Address / Outpoints

```
tb1qcsp6a3qpna8pn84u6d3flgfuvv7za2xr2nzpju
tb1qp80apffayymz3msydgdp45pmarh8ccara7d6lv
tb1qg0y9qy866a7nncg4s05le5794tpjql7ewva5zw
tb1qnhwjrvuvt53kwqzfxpuraz7249t4vvls5ras0z
tb1qga0h2wtp8xmjrewv443rpyz7gnmz38jhgkv934
tb1qc43p44scz2pdehucjl6weqxt6pgwdsj8867gpq
tb1q6sghpzeskg8ae82qqaewymz6tju8r8le4u4mdf
tb1qqyqlz9z08mfuwq4n7mh0n3kv4h7ynzmmrurqhs
tb1qrg68elrwzymj5l2yphzh0dghpmnvcnnfns25xc
tb1q7qgtkm26sh6hh3f0s7qyn8qnvxcgr2xt0y62qs
tb1qwcz78c88hjygvuzx30ay6c6fajvvy7q3m03qms
tb1q4r375n9y3cmdm0jks94u9y0tuwwhqe06yre7em
tb1qc29al30sd74g09sy5nyjaxuvp37krw6yg4446y
tb1qanzwndzally5ezz7jwx0z8vecvvp8w4xl6affs
```

- Running a BTCPay server or zaprite

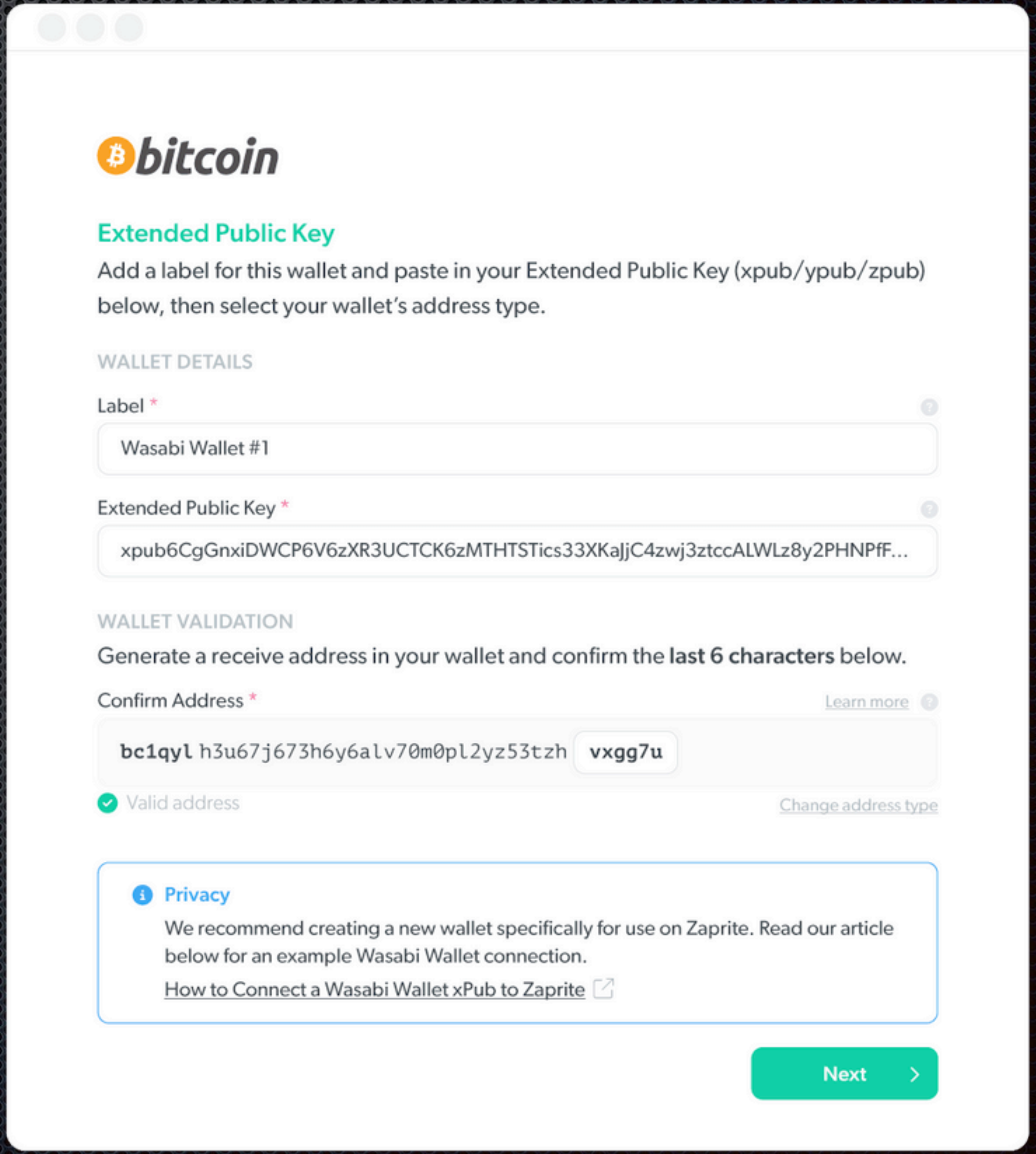


Invoices

Create, search or pay an invoice. (Help)

Date	OrderId	InvoiceId	Status	Amount	Actions
4/12/2020 11:57:47 AM		M6QCnStUHvpW7KUZCSq1qp	paid	$2.00 (USD)	Details
4/12/2020 11:57:37 AM		GGaZ1TUGsnCvwzuU5VEhD2	paid	0.01000000 BTC	Details
4/12/2020 11:57:26 AM		KLwGowp4PvnyH88owMmgHf	new	120,00 € (EUR)	Checkout [^] Details
4/12/2020 11:57:15 AM		YUpW4UVxUq6P3tRymSwNxf	new	$5.00 (USD)	Checkout [^] Details
4/10/2020 11:53:52 AM		YYnH47cWQp3fK39QmUTgEi	expired	$50.00 (USD)	Details
4/6/2020 12:15:43 PM		5VNk3NByx2ZyPQ5hYQq86b	expired	$10.00 (USD)	Details

@Copyright BTCPayServer v1.0.3.164 Environment: Development Build: Debug



Extended Public Key

Add a label for this wallet and paste in your Extended Public Key (xpub/ypub/zpub) below, then select your wallet's address type.

WALLET DETAILS

Label *

Wasabi Wallet #1

Extended Public Key *

xpub6CgGnxiDWCP6V6zXR3UCTCK6zMTHTSTics33XKaJjC4zwj3ztccALWLz8y2PHNPfF...

WALLET VALIDATION

Generate a receive address in your wallet and confirm the **last 6 characters** below.

Confirm Address * Learn more

`bc1qyl h3u67j673h6y6alv70m0pl2yz53tzh vxgg7u`

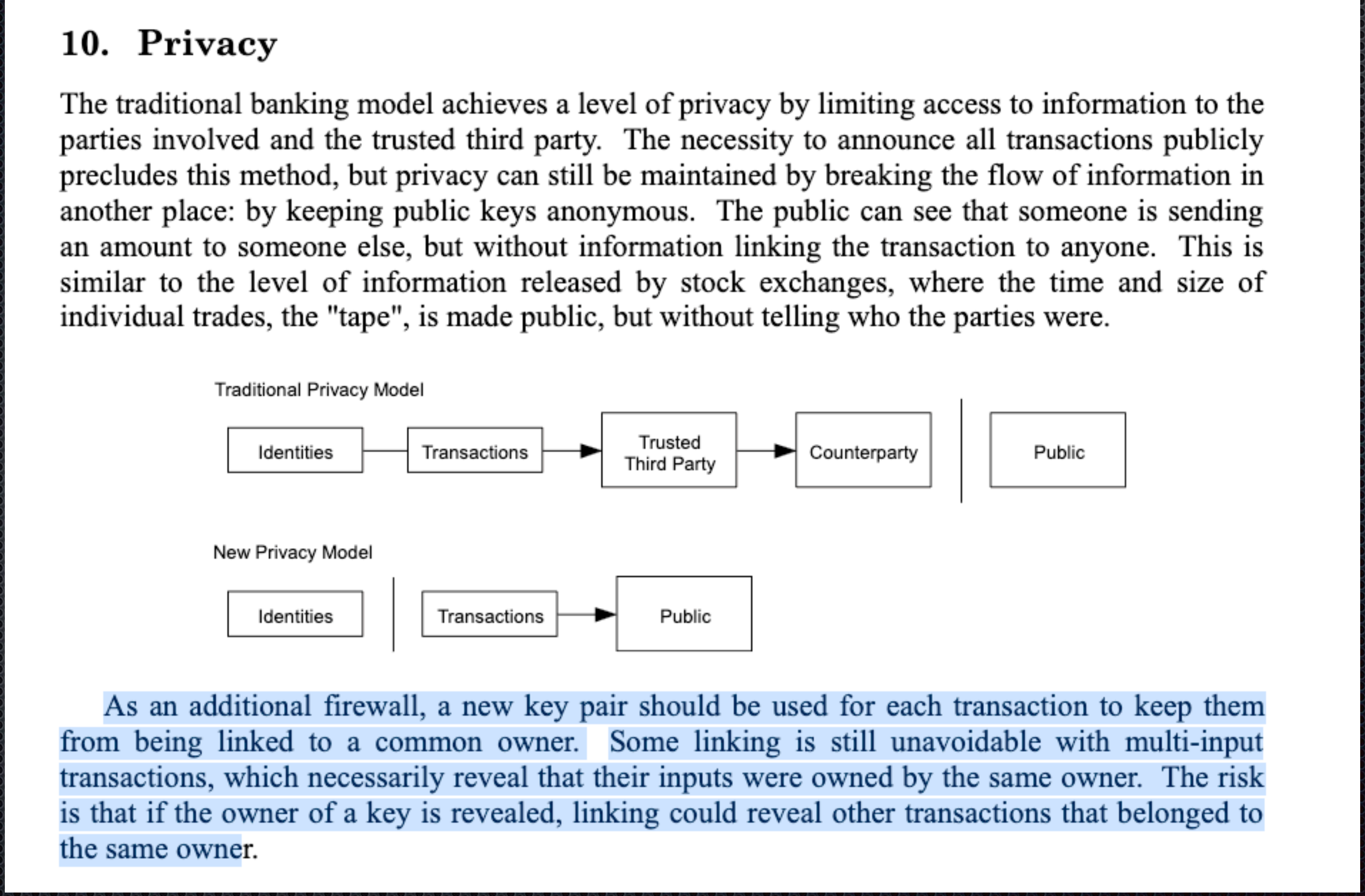
✓ Valid address Change address type

Privacy

We recommend creating a new wallet specifically for use on Zaprite. Read our article below for an example Wasabi Wallet connection.

How to Connect a Wasabi Wallet xPub to Zaprite

- This concern regarding the reissuing of addresses was already addressed in the 2008 whitepaper.



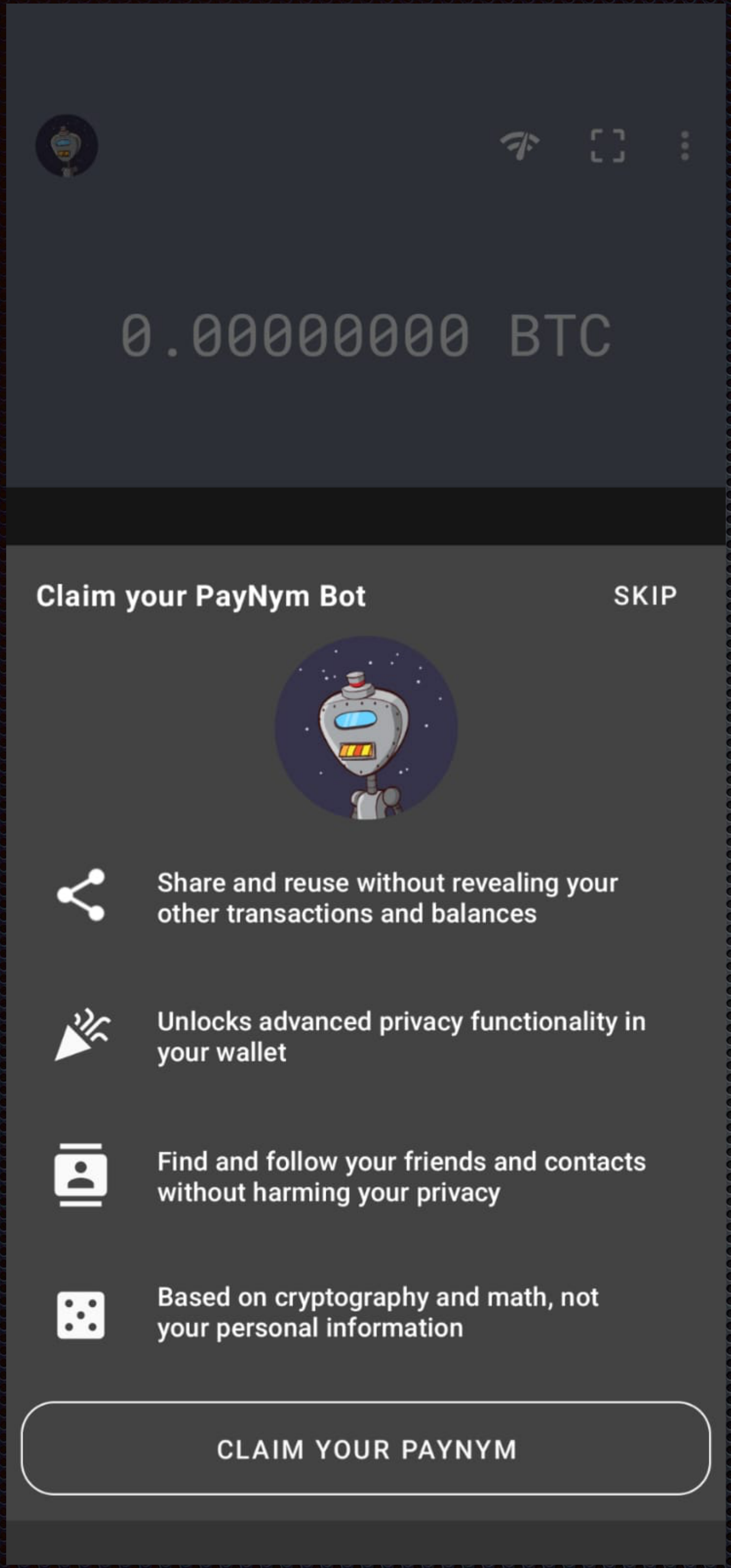
10. Privacy

The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone. This is similar to the level of information released by stock exchanges, where the time and size of individual trades, the "tape", is made public, but without telling who the parties were.

As an additional firewall, a new key pair should be used for each transaction to keep them from being linked to a common owner. Some linking is still unavoidable with multi-input transactions, which necessarily reveal that their inputs were owned by the same owner. The risk is that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner.

What are PayNyms?

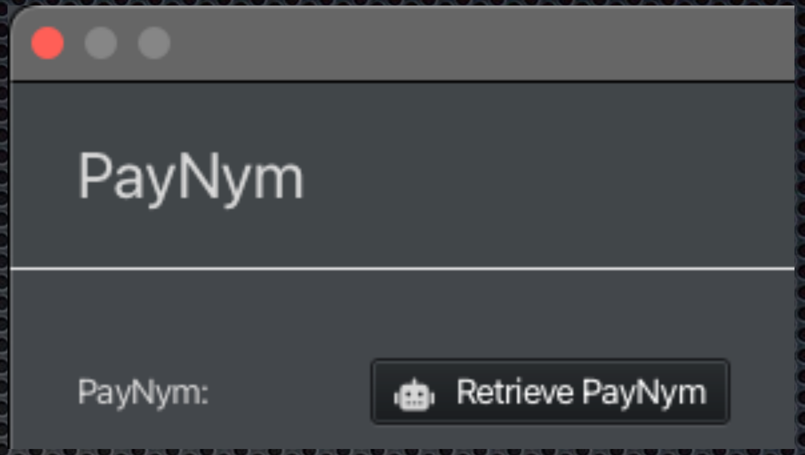
- ‘PayNym’ is the Samourai Wallet implementation of BIP47: ‘Reusable Payment Codes’.
- A publicly shareable ID, derived from your private key.
- Anyone else using a BIP47 compatible wallet can combine their own unique code with yours to generate bitcoin addresses for the two of you to transact.



0.00000000 BTC

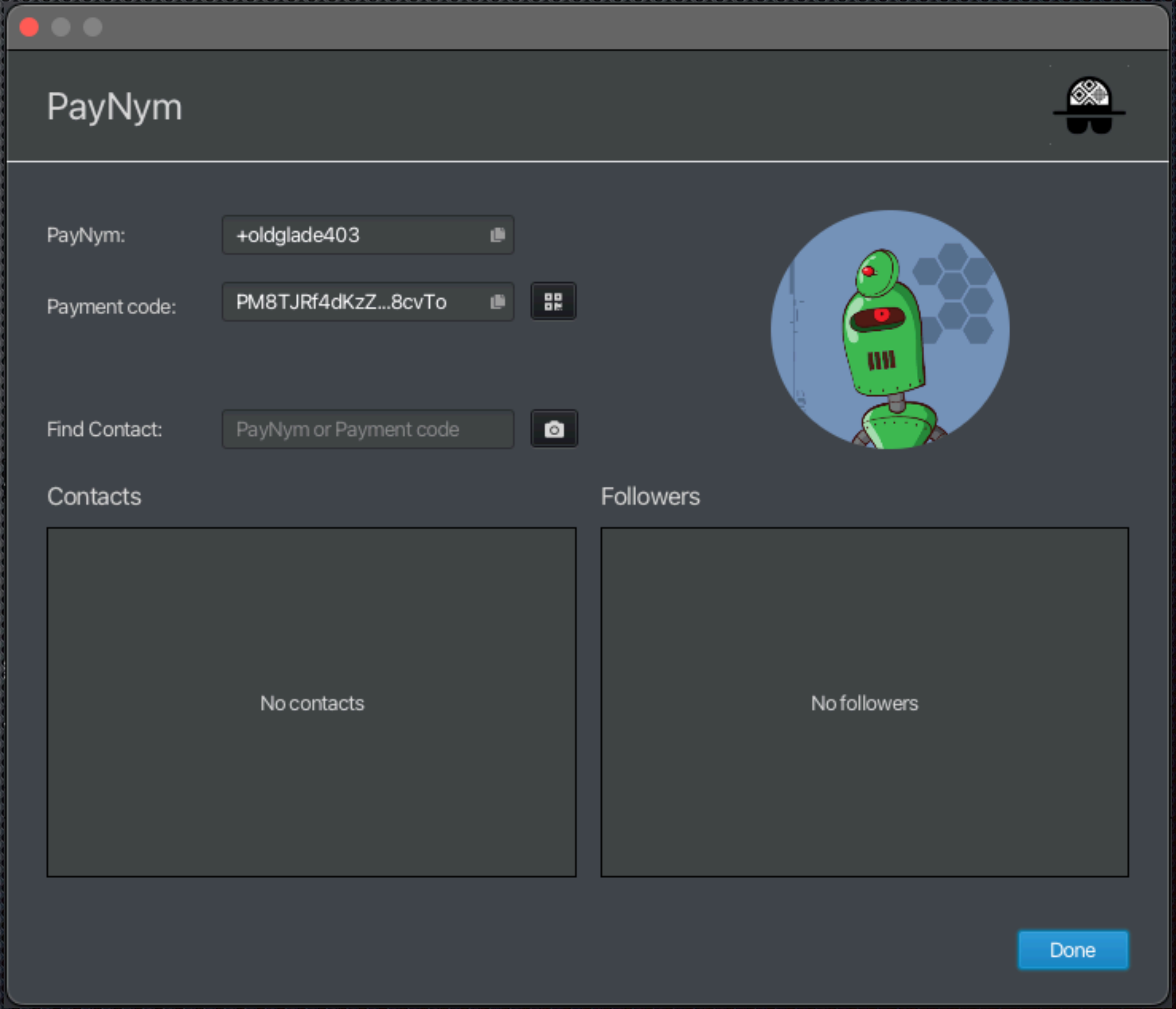
Claim your PayNym Bot

- Share and reuse without revealing your other transactions and balances
- Unlocks advanced privacy functionality in your wallet
- Find and follow your friends and contacts without harming your privacy
- Based on cryptography and math, not your personal information



PayNym

PayNym:



PayNym

PayNym: +oldglade403

Payment code: PM8TJRf4dKzZ...8cvTo

Find Contact: PayNym or Payment code

Contacts

No contacts

Followers

No followers

- PayNyms provide a secure and private way to send and receive bitcoin using BIP47 Reusable Payment Codes.

- PayNyms allow you to add friends to your wallet contact list without revealing your balance or transaction history, for secure sending and receiving.

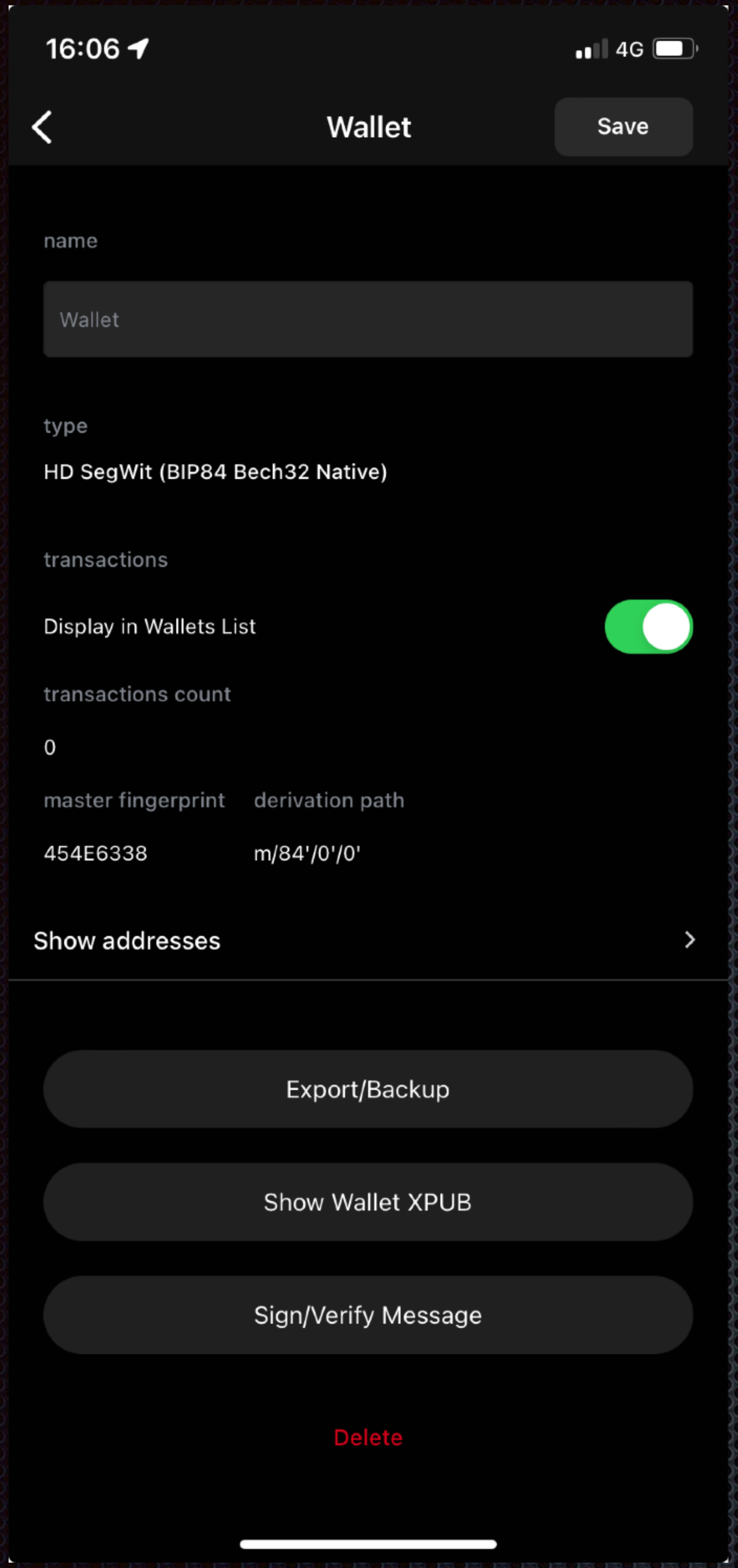
How do PayNym's work?

https://github.com/bitcoin/bips/blob/master/bip-0047.mediawiki#protocol

BORING!

- The wallet needs your private keys to derive addresses for connected PayNyms.
- Currently, this functionality is only available in Samourai, Sparrow Wallet, Bluewallet, and Stack Wallet.
- Samourai manages Paynym directory and provides Custom PayNyms at its discretion.
- The only other alternative to BIP 47 is "silent payments”, but no wallet has implemented them yet.

[XTX]



16:06 4G

Wallet

name

Wallet

type

HD SegWit (BIP84 Bech32 Native)

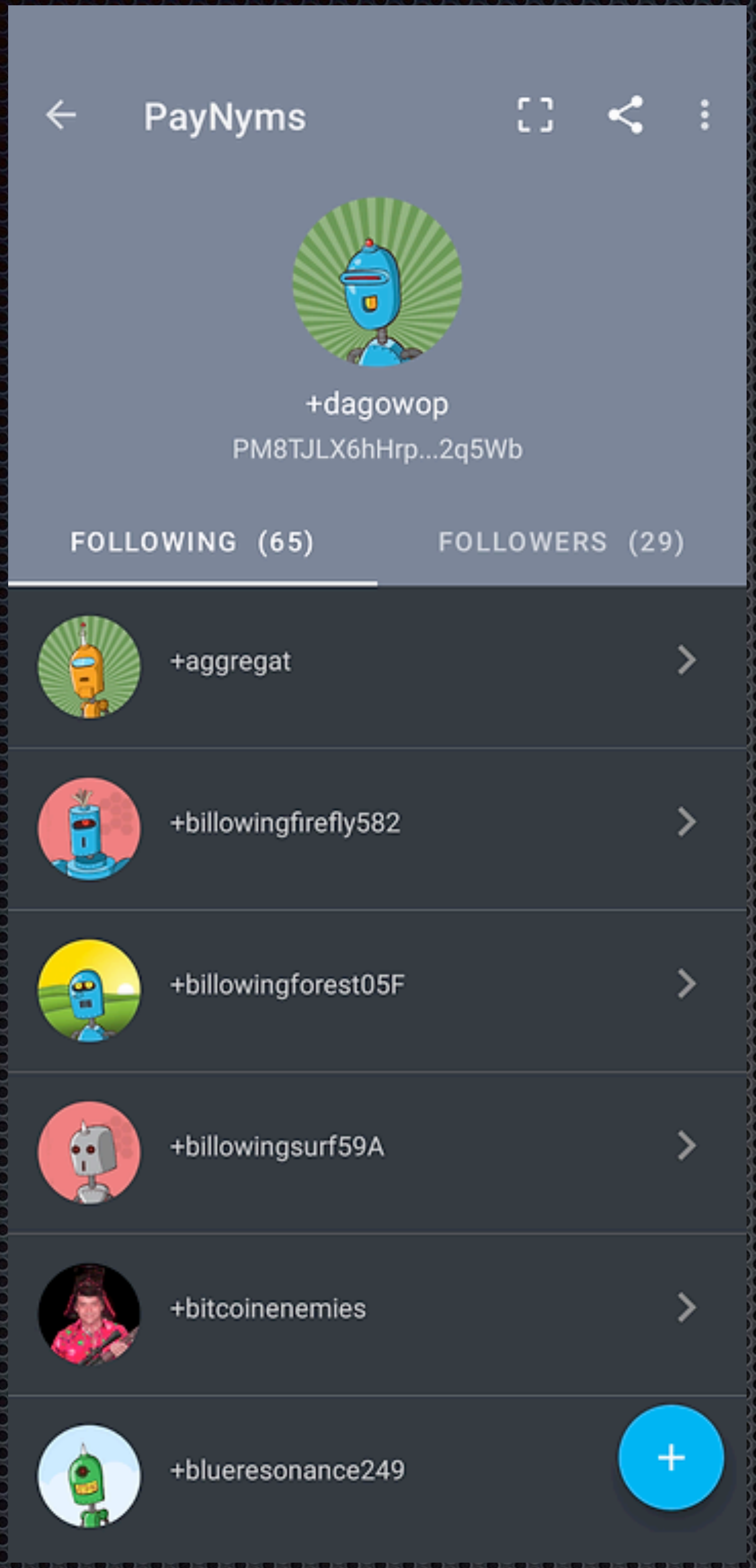
transactions

Display in Wallets List

transactions count

0

master fingerprint	derivation path
454E6338	m/84'/0'/0'



PayNyms

+dagowop

PM8TJLX6hHrp...2q5Wb

FOLLOWING (65) FOLLOWERS (29)

+aggregat

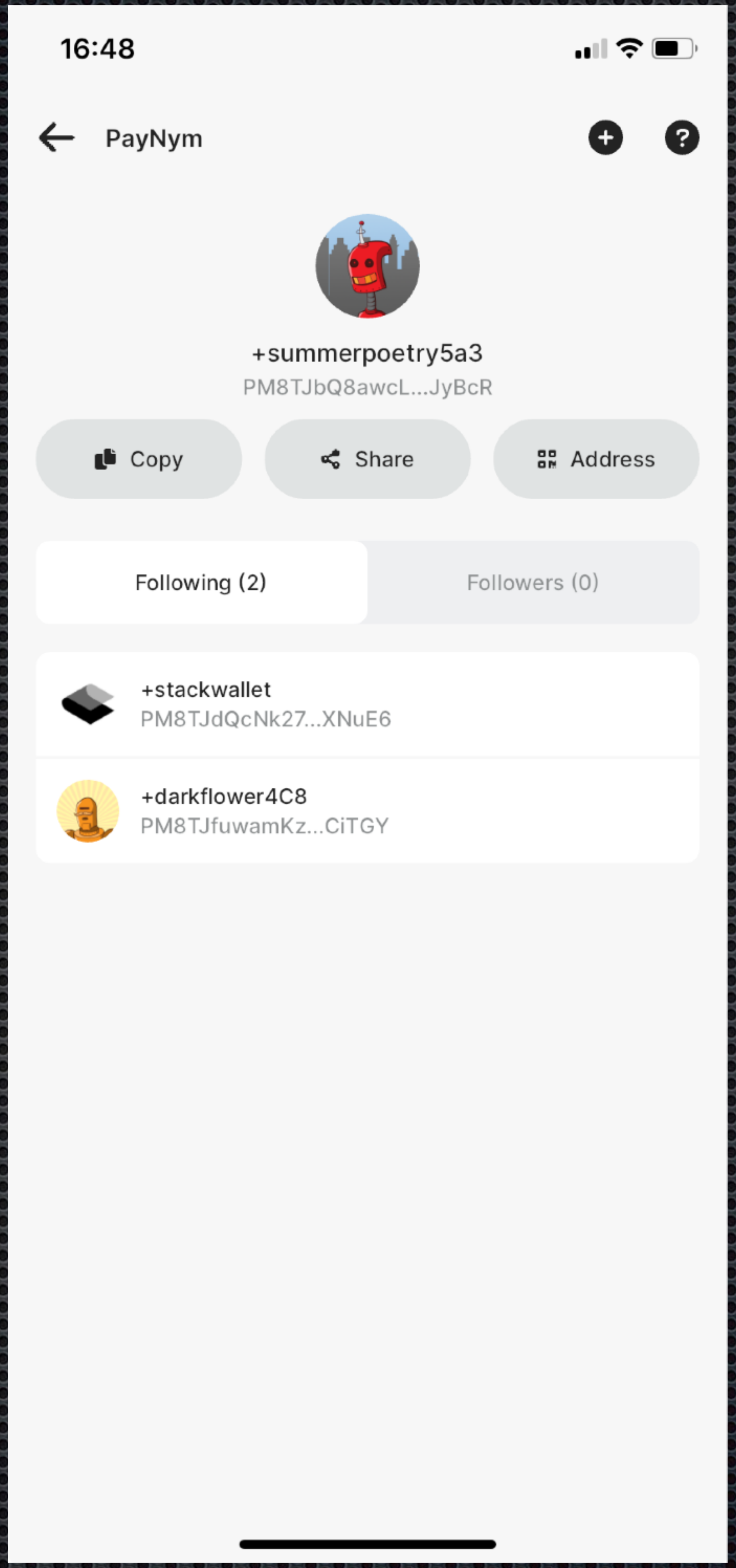
+billowingfirefly582

+billowingforest05F

+billowingsurf59A

+bitcoinenemies

+blueresonance249



16:48

PayNym

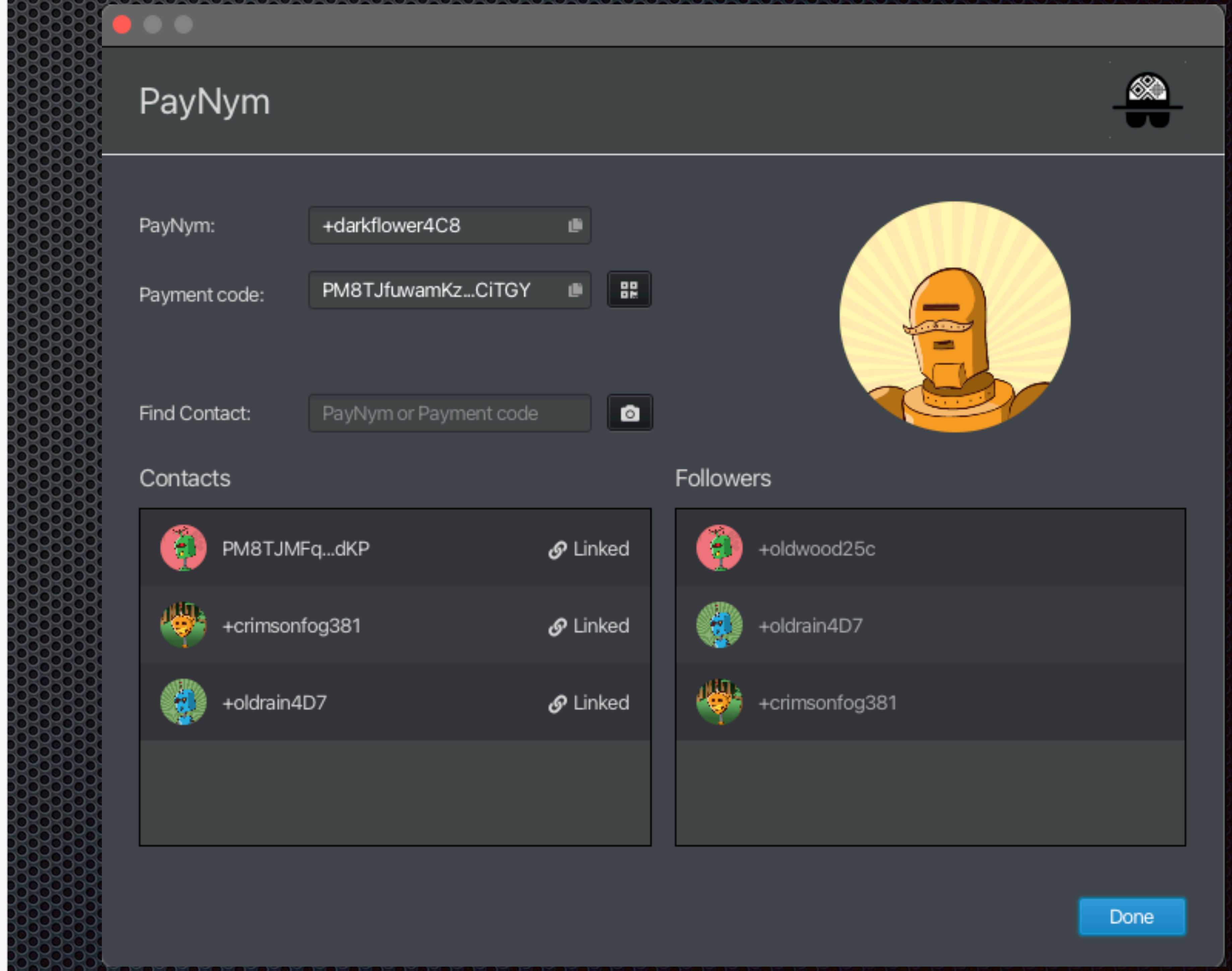
+summerpoetry5a3

PM8TJbQ8awcL...JyBcR

Following (2) Followers (0)

+stackwallet
PM8TJdQcNk27...XNuE6

+darkflower4C8
PM8TJfuwamKz...CiTGY



PayNym

PayNym: +darkflower4C8

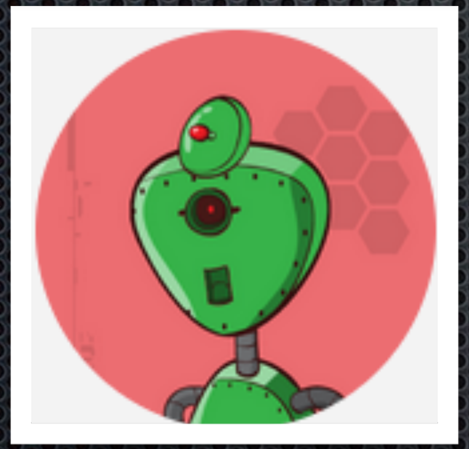
Payment code: PM8TJfuwamKz...CiTGY

Find Contact: PayNym or Payment code

Contacts	
PM8TJMFq...dKP	Linked
+crimsonfog381	Linked
+oldrain4D7	Linked

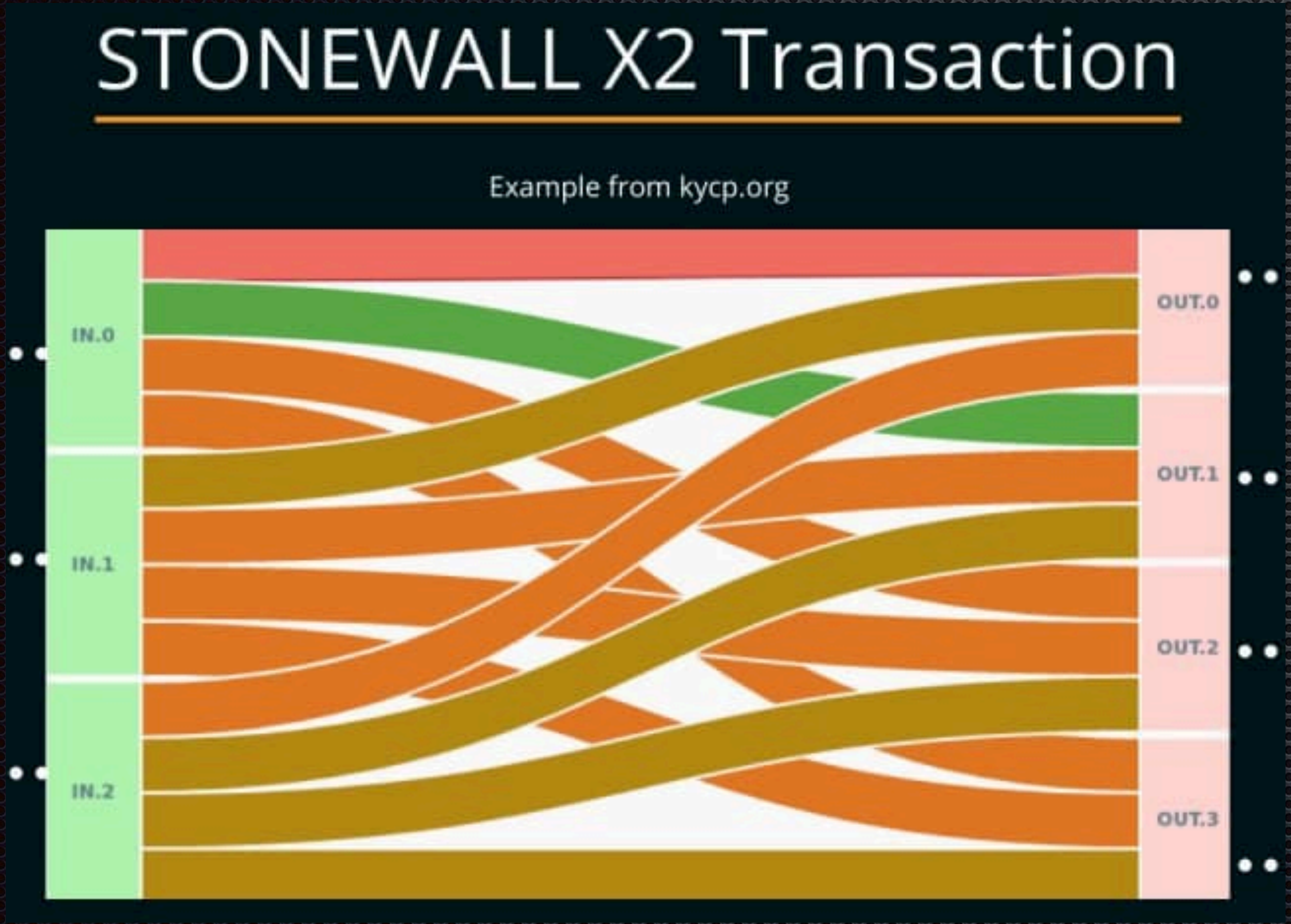
Followers
+oldwood25c
+oldrain4D7
+crimsonfog381

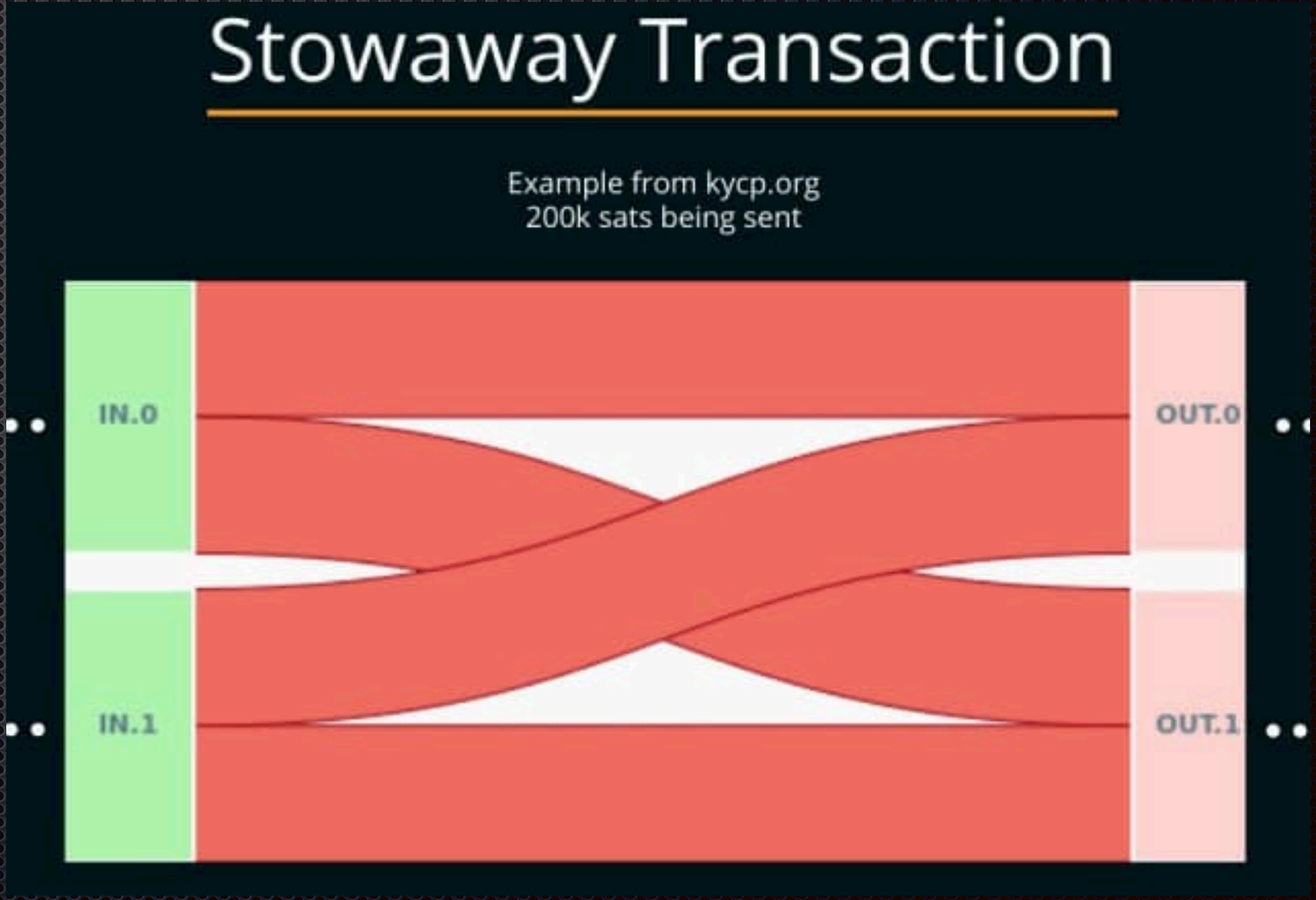
Payment code or PayNym?

- The ‘PayNym’ ID you see within is simply a visual layer built on top to improve user experience and is not integral to the underlying operation of the BIP.
- Here is my payment code:
  - PM8TJf24x11fQXTBXGHvYSQjs9bPsNcnfKkXKdsdWNiaGGcomo4kaq5TGpuBpHw294AngwnFsKqT9dWeVuCukJgeqiDpr8f9egaiUsa1f78e8smTKmCV
  - 

Collaborative Payments (Following)

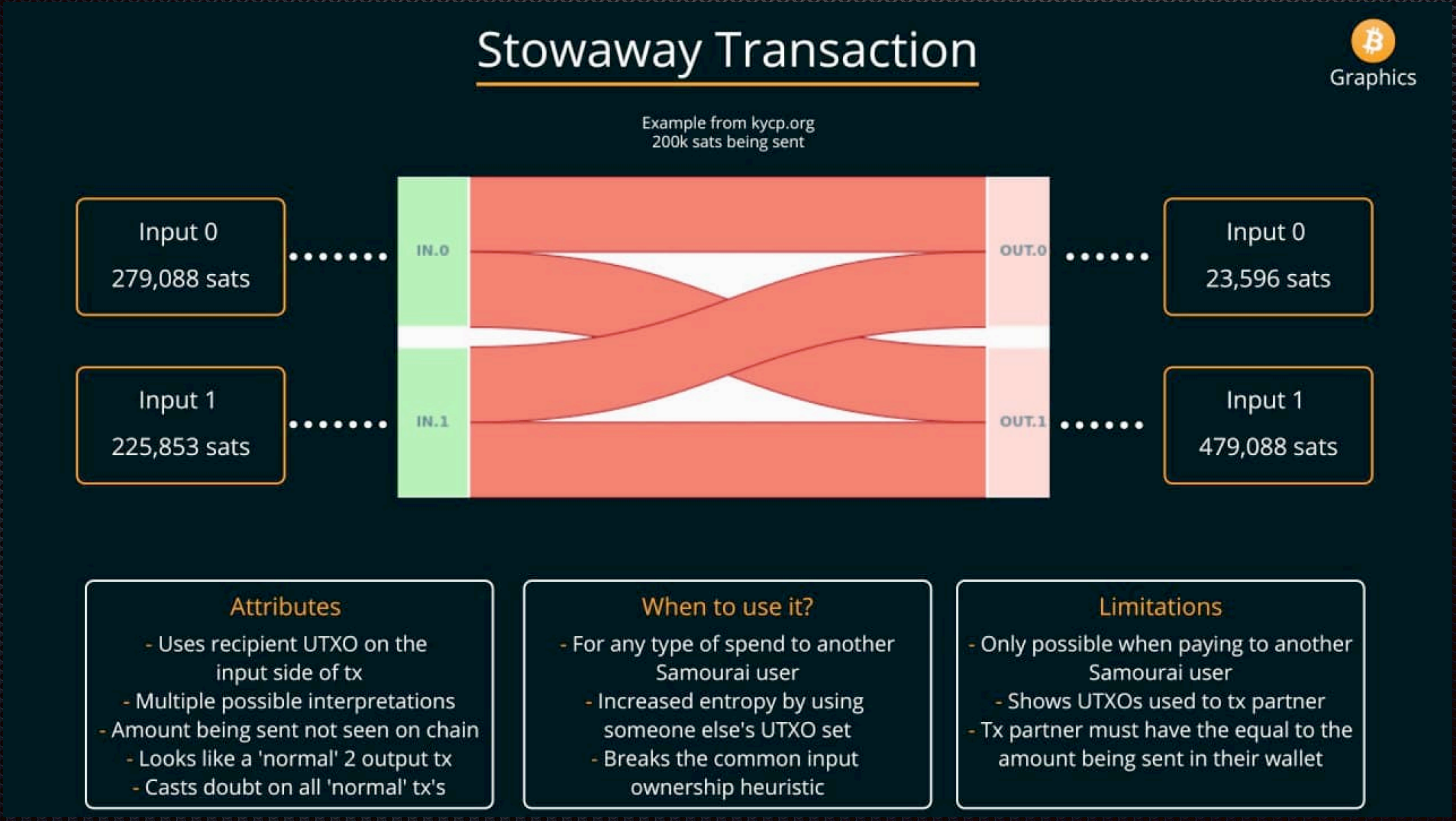
This free option, built by the Samourai team, allows you and any other PayNym you follow to collaborate using Cahoots (Stowaway, Stonewall x2).





Stowaway

A 2-Person CoinJoin that simulates a "simple" bitcoin payment



Stowaway Transaction

Graphics

Example from kycp.org
200k sats being sent

Input 0
279,088 sats

Input 1
225,853 sats

Input 0
23,596 sats

Input 1
479,088 sats

Attributes

- Uses recipient UTXO on the input side of tx
- Multiple possible interpretations
- Amount being sent not seen on chain
- Looks like a 'normal' 2 output tx
- Casts doubt on all 'normal' tx's

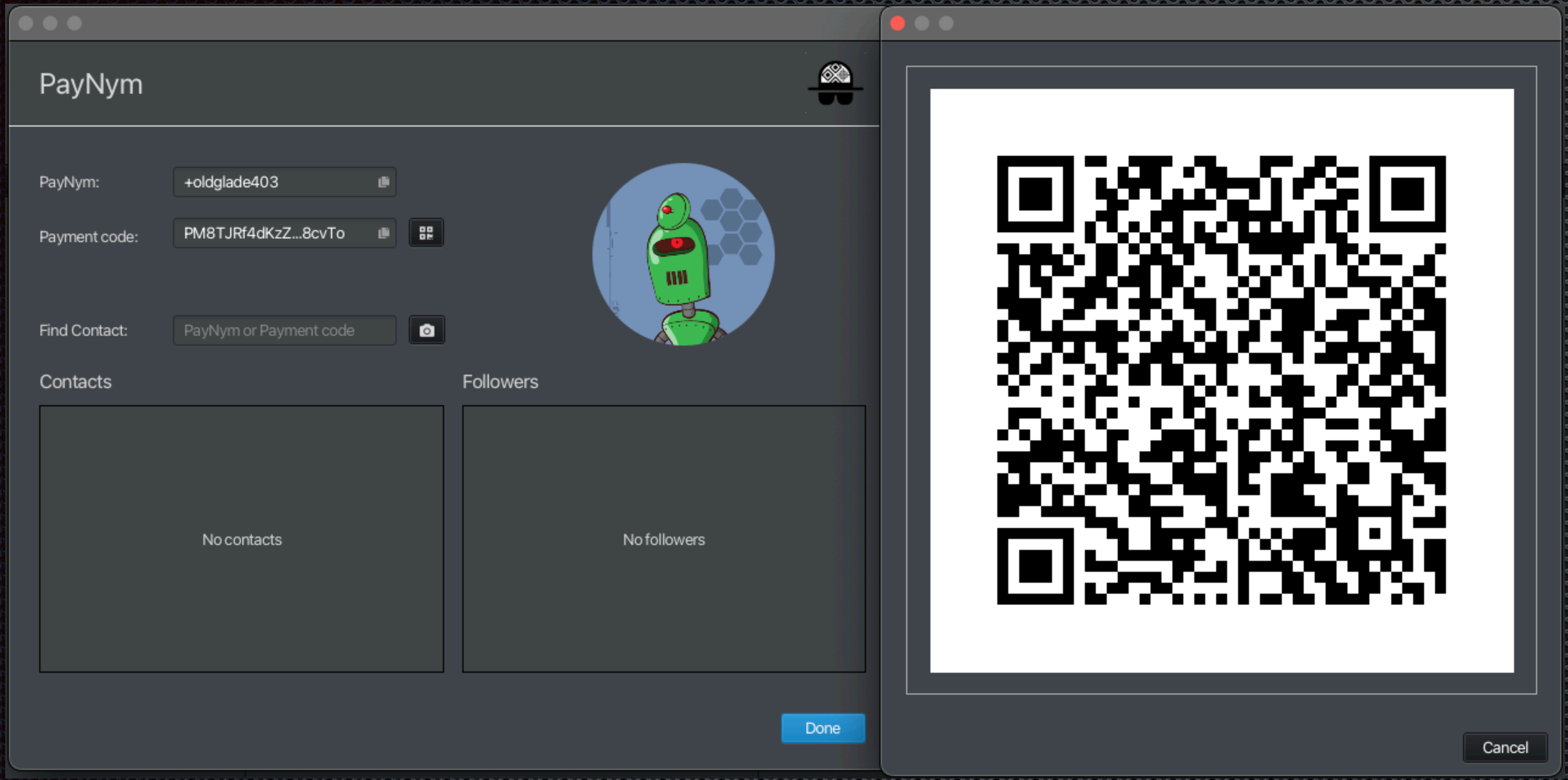
When to use it?

- For any type of spend to another Samourai user
- Increased entropy by using someone else's UTXO set
- Breaks the common input ownership heuristic

Limitations

- Only possible when paying to another Samourai user
- Shows UTXOs used to tx partner
- Tx partner must have the equal to the amount being sent in their wallet

[XTX]



PayNym

PayNym: +oldglade403

Payment code: PM8TJRf4dKzZ...8cvTo

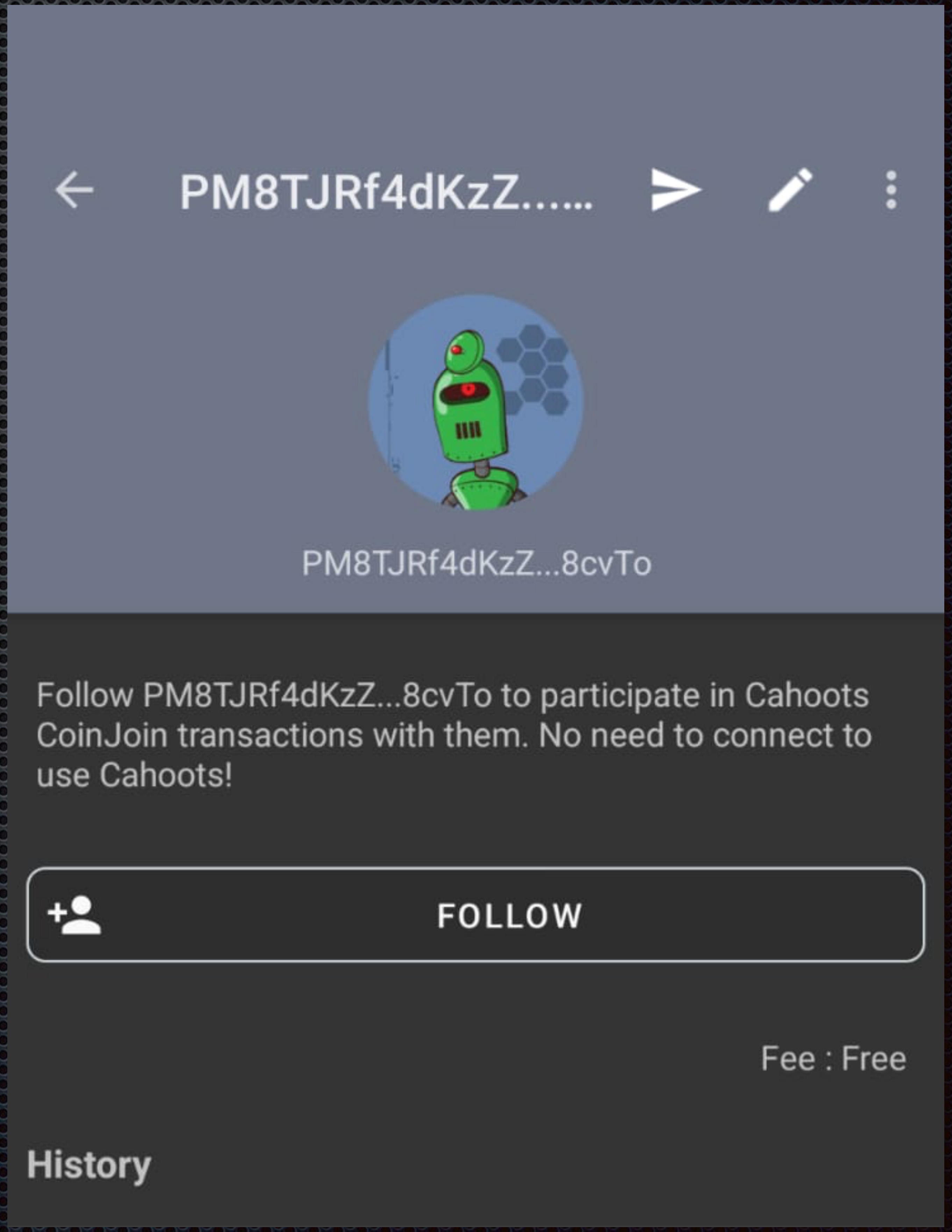
Find Contact: PayNym or Payment code

Contacts

No contacts

Followers

No followers



PM8TJRf4dKzZ......

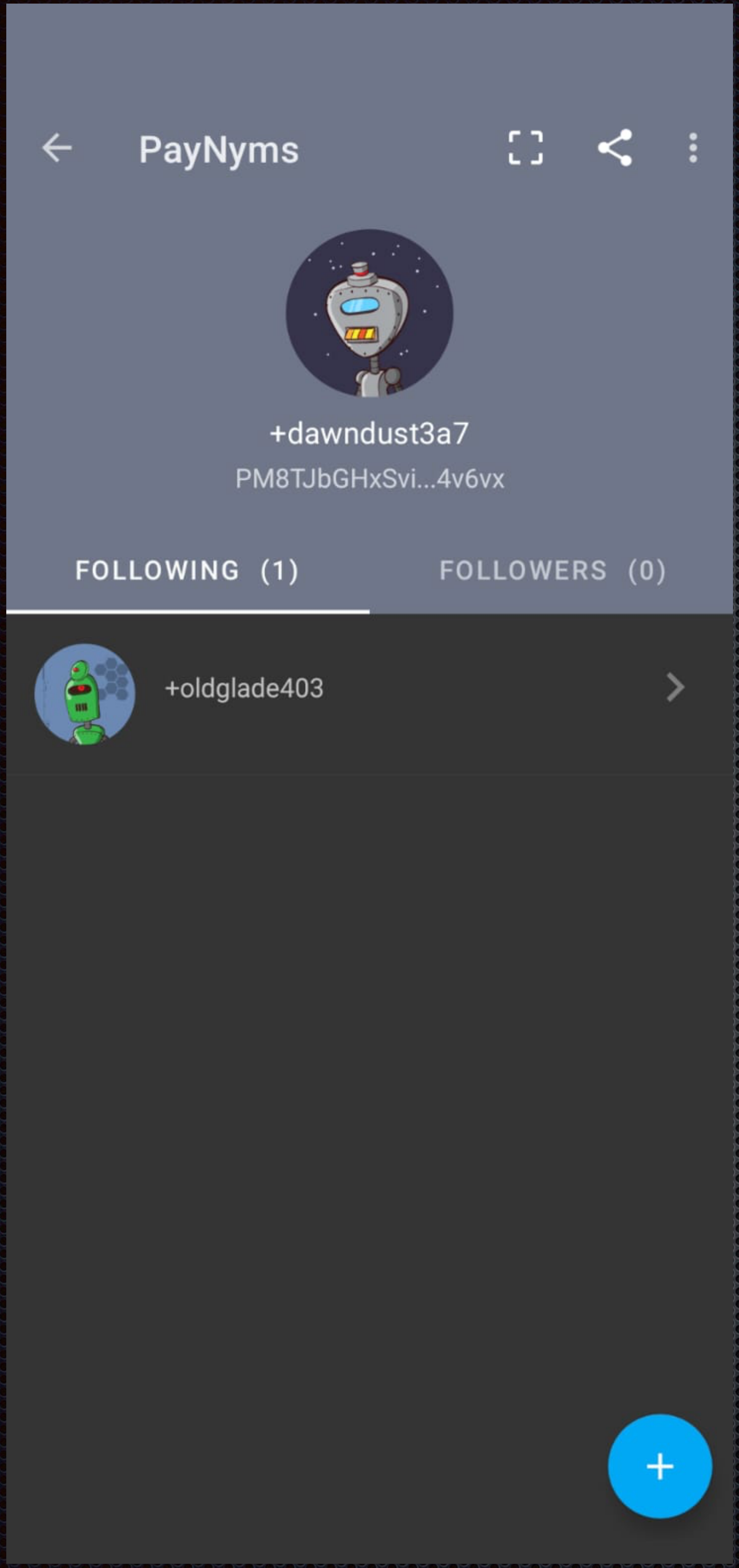
PM8TJRf4dKzZ...8cvTo

Follow PM8TJRf4dKzZ...8cvTo to participate in Cahoots CoinJoin transactions with them. No need to connect to use Cahoots!

Fee : Free

History

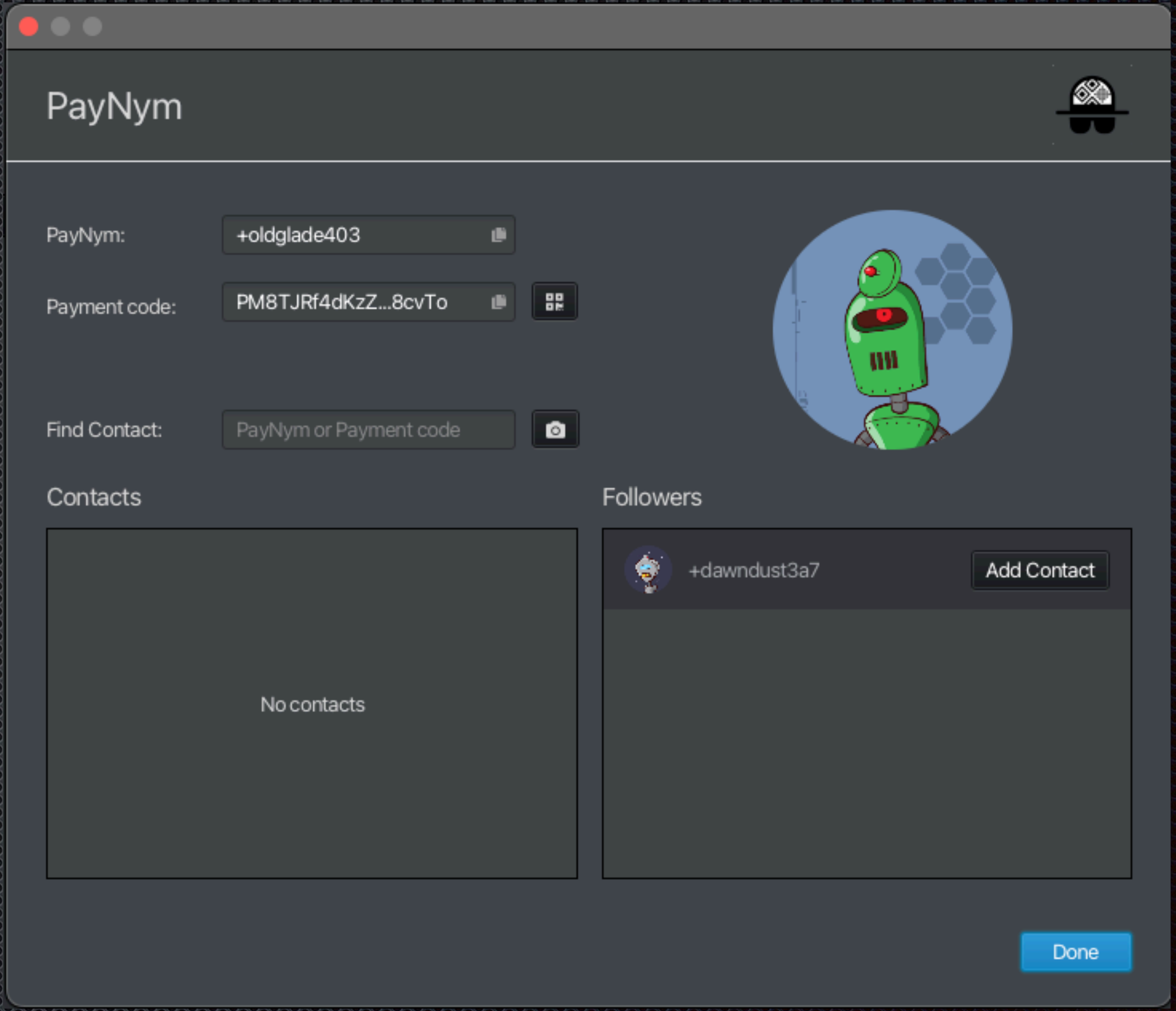
[XTX]



+dawndust3a7

PM8TJbGHxSvi...4v6vx

+oldglade403



PayNym: +oldglade403

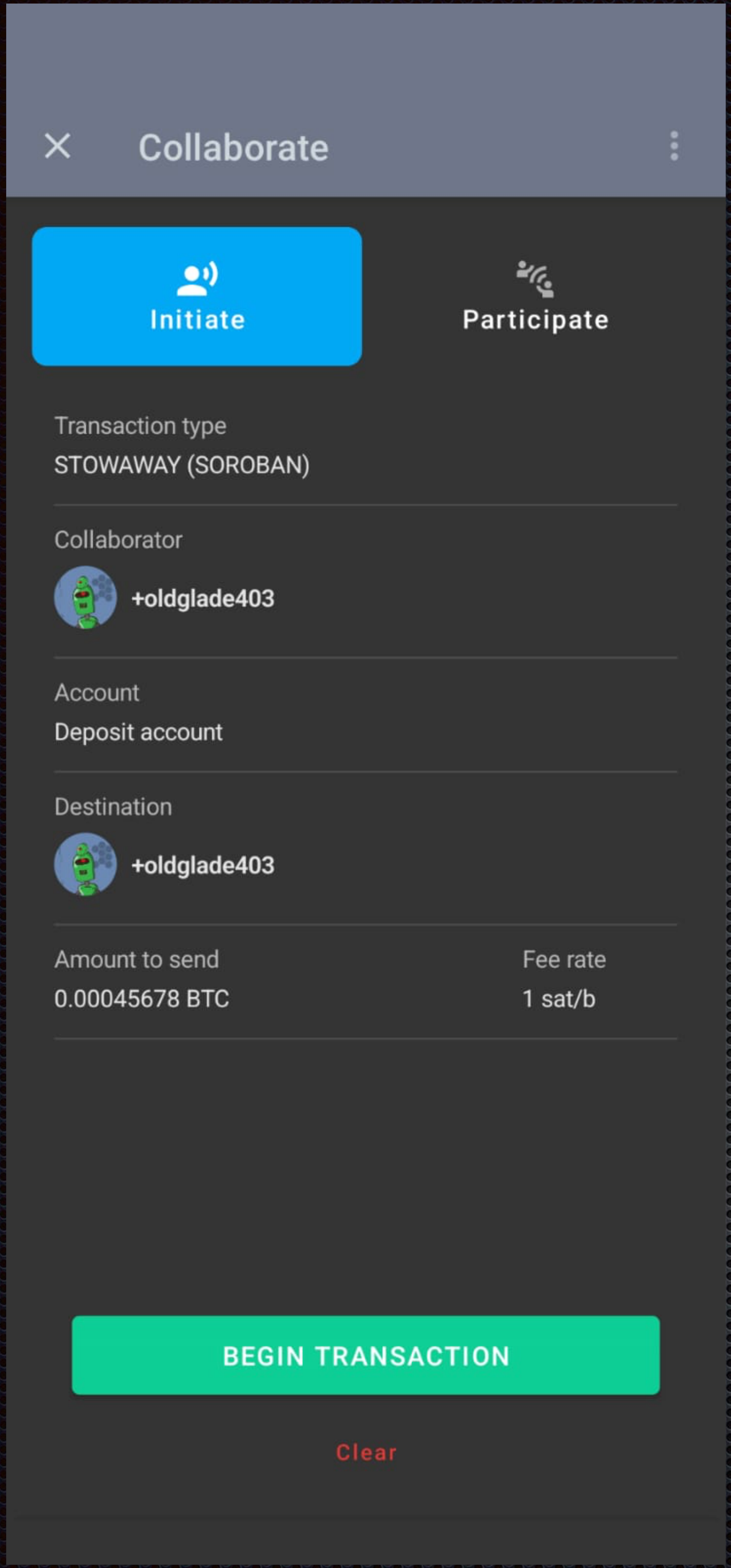
Payment code: PM8TJRf4dKzZ...8cvTo

Find Contact: PayNym or Payment code

No contacts

+dawndust3a7

[XTX]



Transaction type
STOWAWAY (SOROBAN)

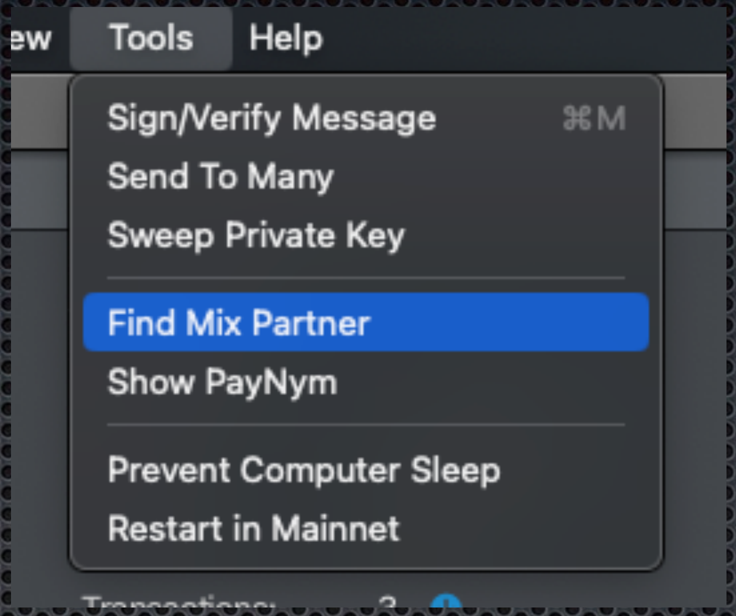
Collaborator
+oldglade403

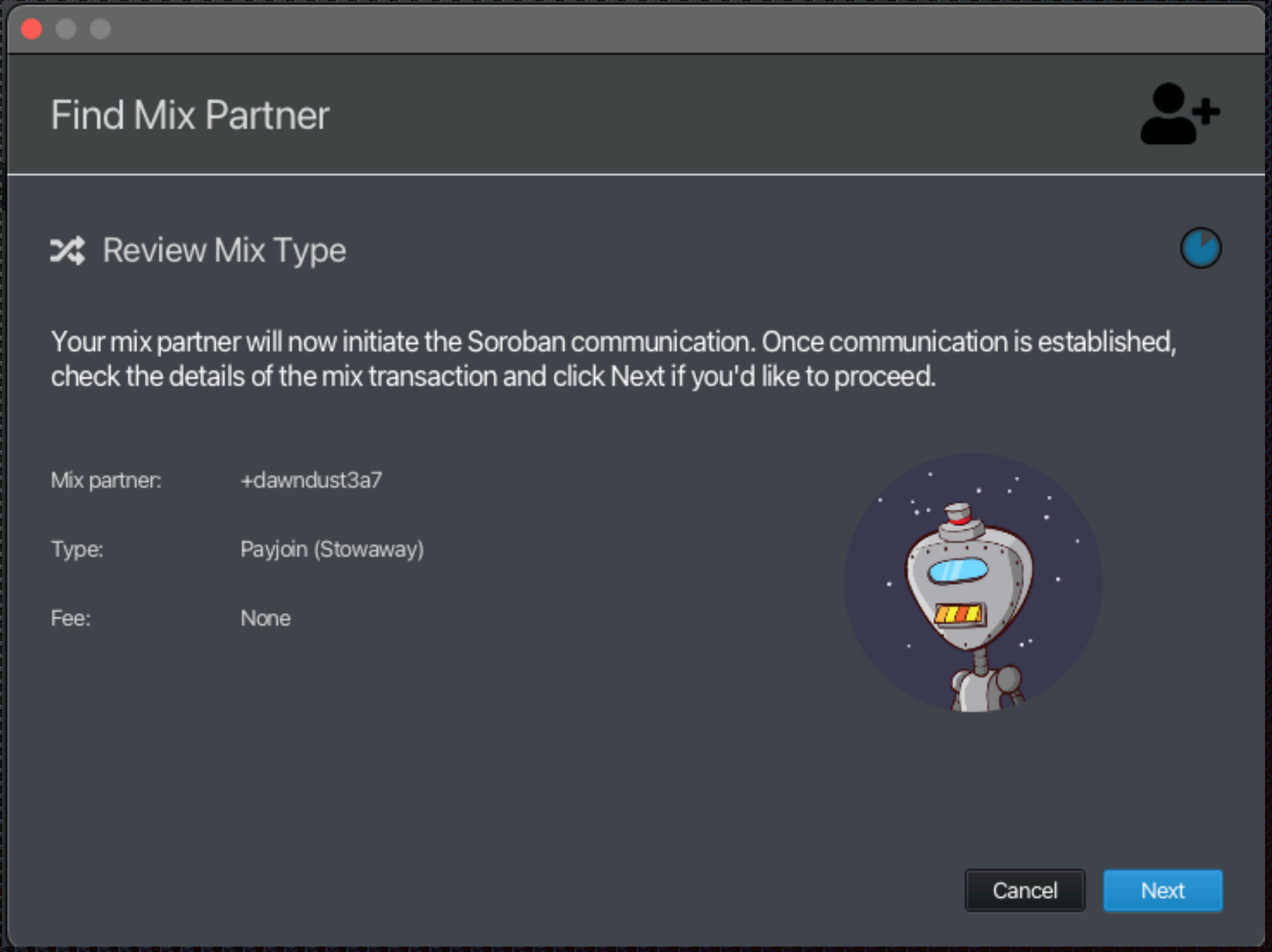
Account
Deposit account

Destination
+oldglade403

Amount to send
0.00045678 BTC

Fee rate
1 sat/b





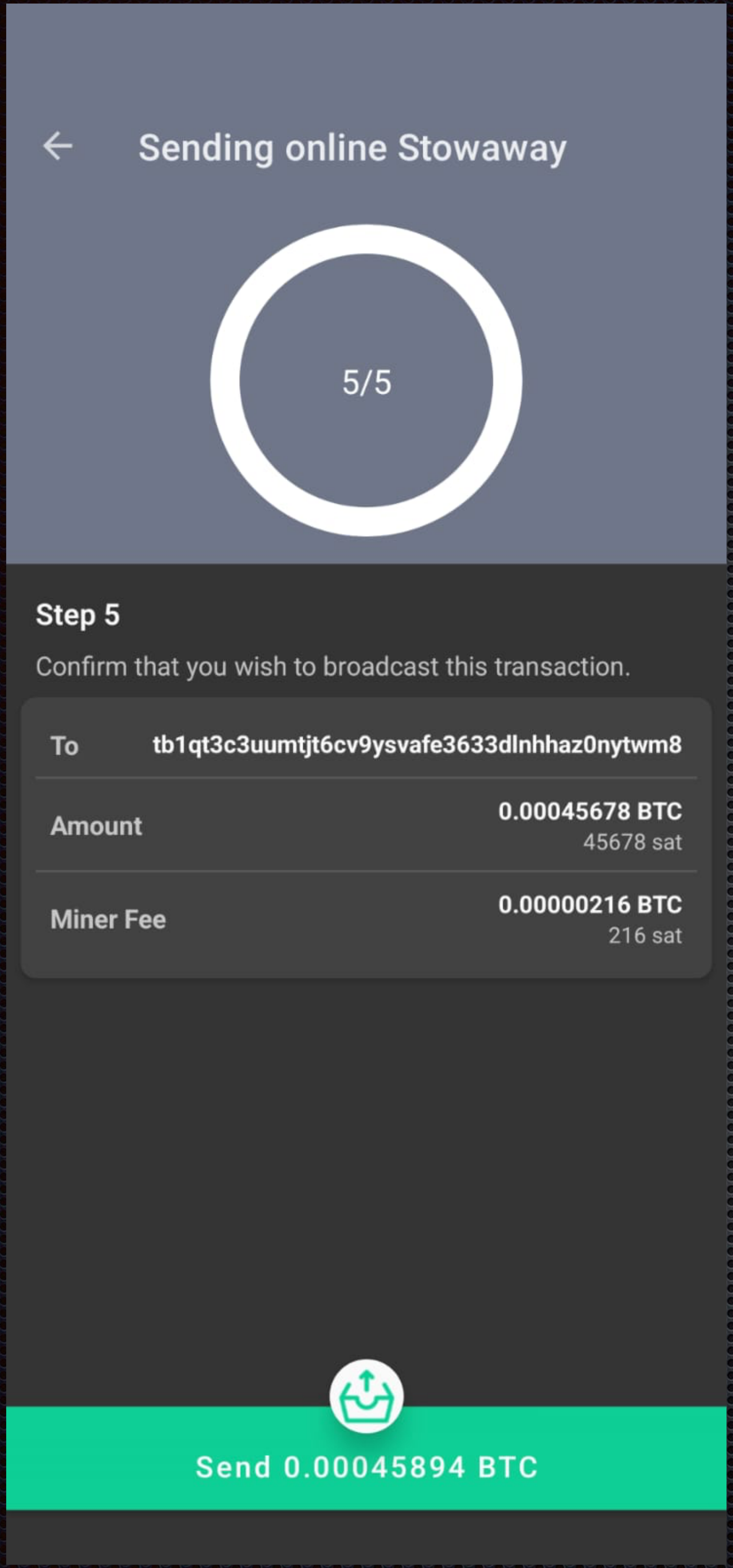
Your mix partner will now initiate the Soroban communication. Once communication is established, check the details of the mix transaction and click Next if you'd like to proceed.

Mix partner: +dawndust3a7

Type: Payjoin (Stowaway)

Fee: None

[XTX]

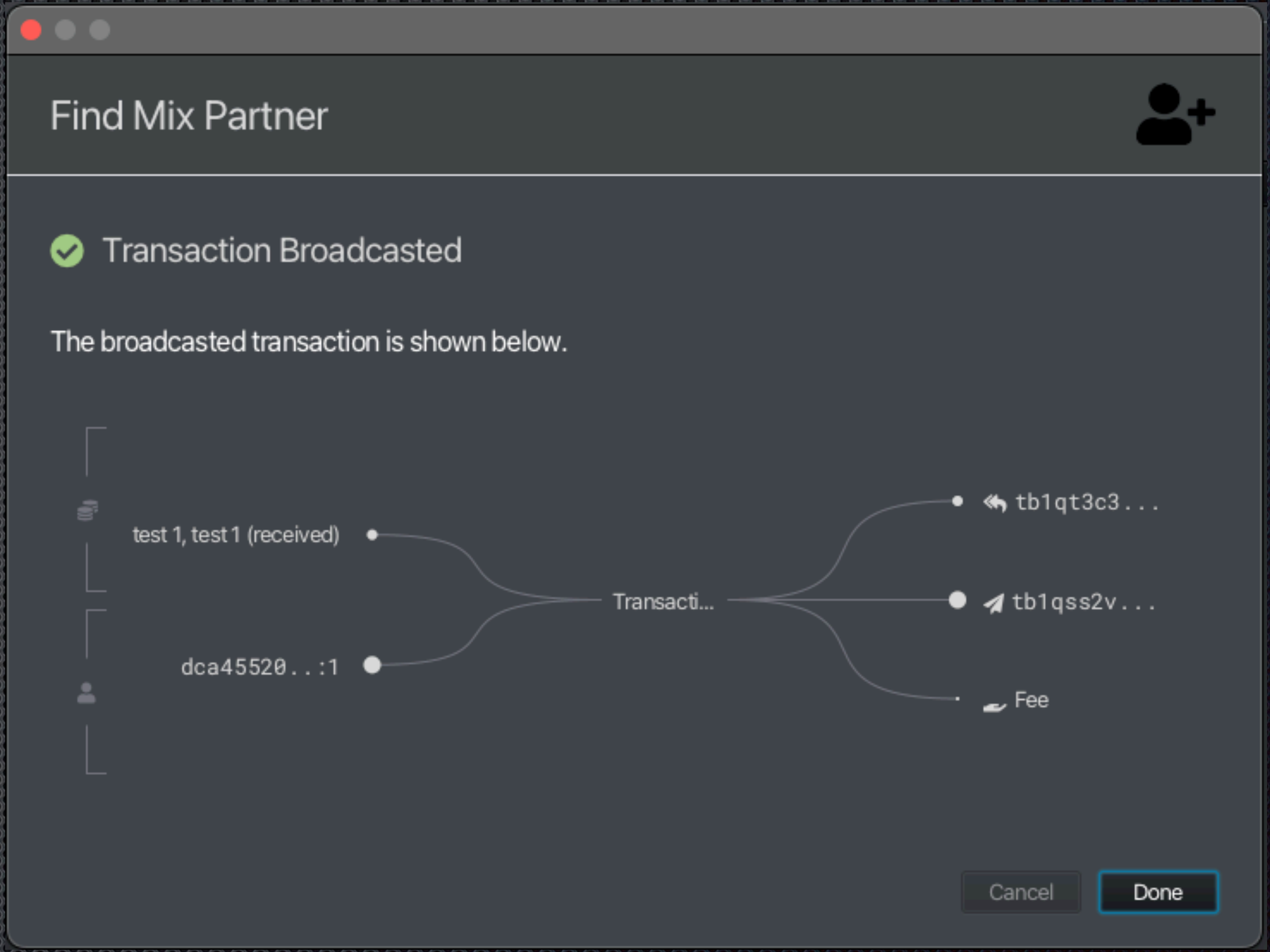


Sending online Stowaway

Step 5

Confirm that you wish to broadcast this transaction.

To	tb1qt3c3uumtjt6cv9ysvafe3633dlnhhaz0nytwm8
Amount	0.00045678 BTC 45678 sat
Miner Fee	0.00000216 BTC 216 sat

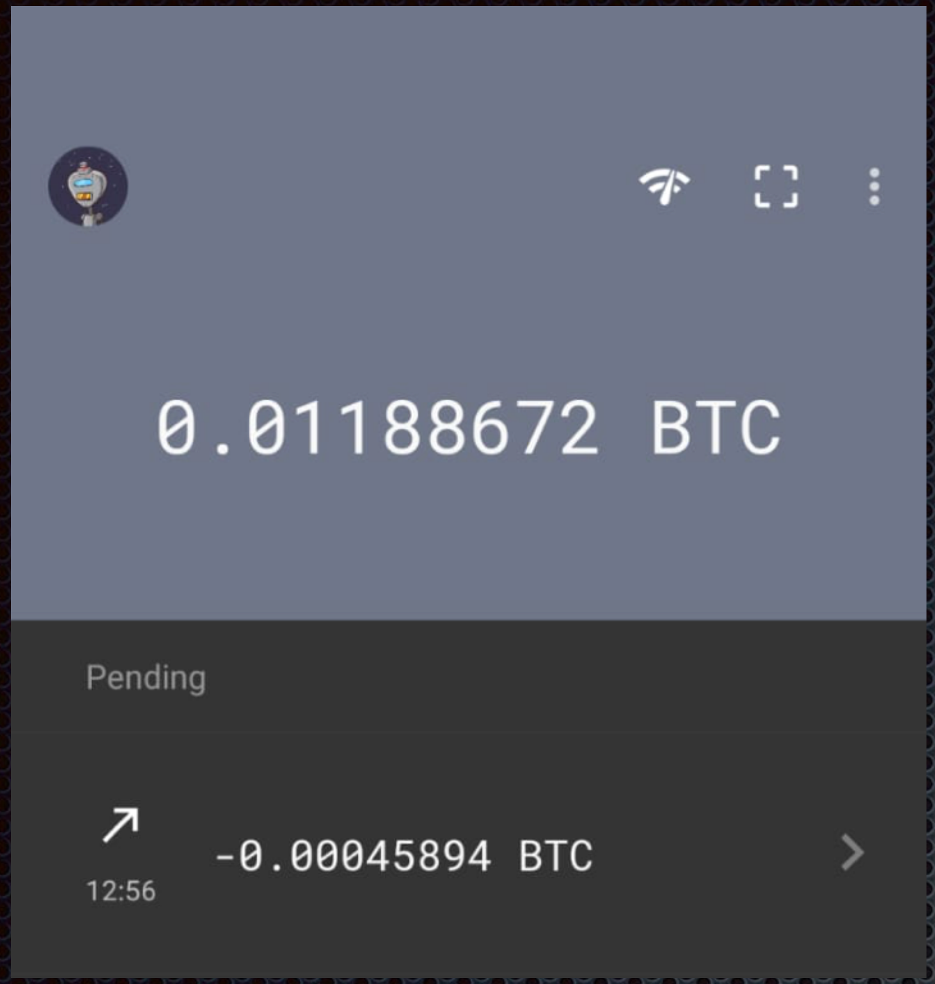


Find Mix Partner

✓ Transaction Broadcasted

The broadcasted transaction is shown below.

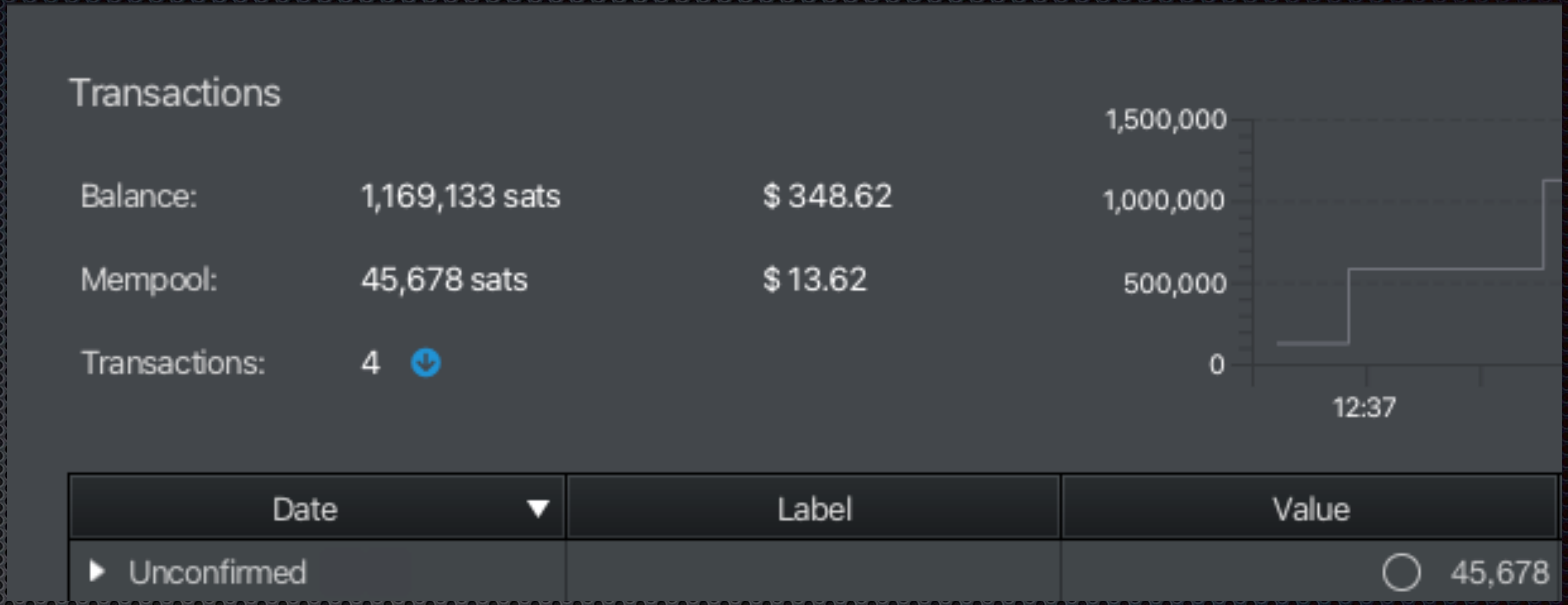
[XTX]



0.01188672 BTC

Pending

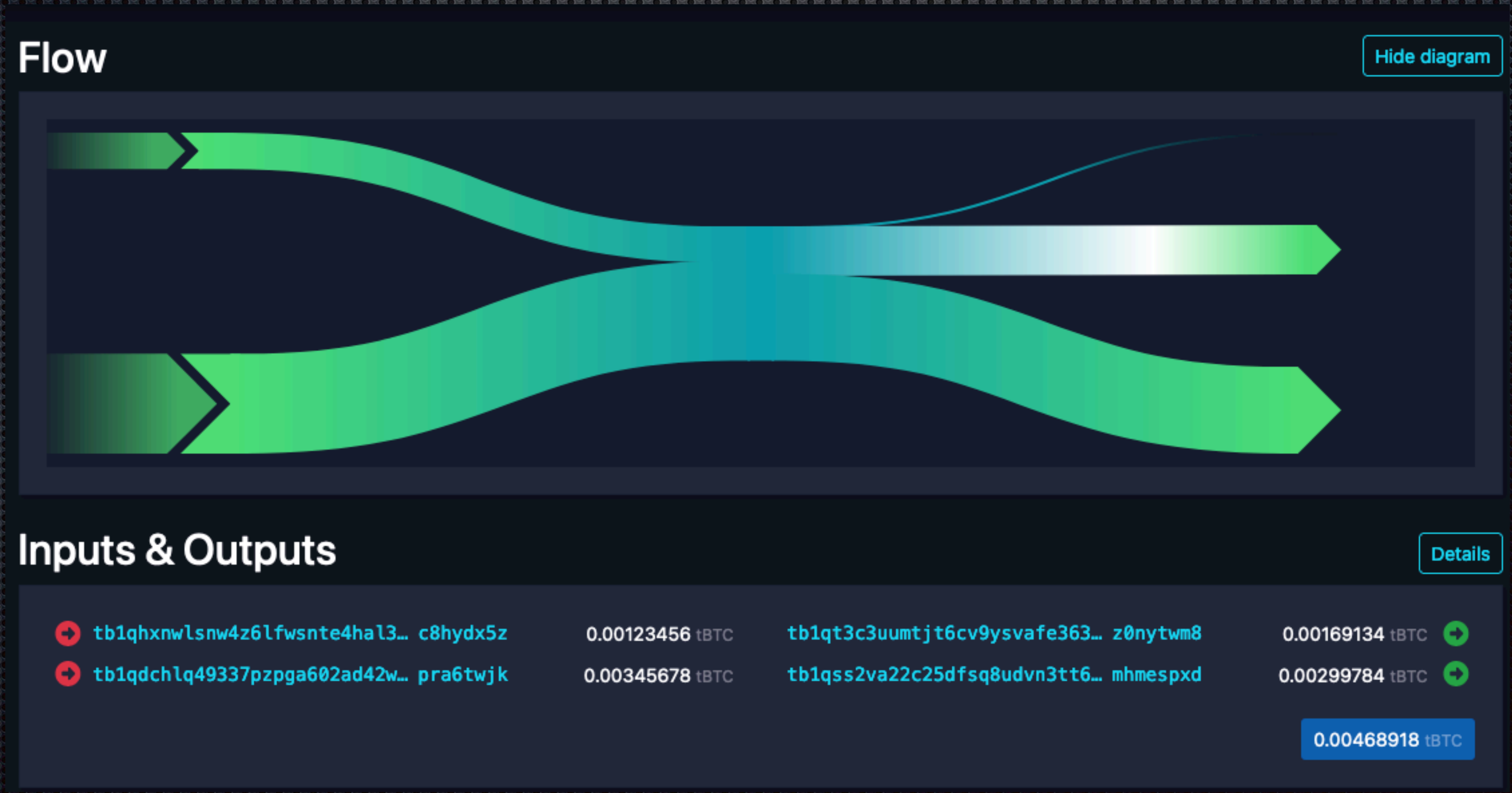
↗ 12:56 -0.00045894 BTC



Transactions

Balance:	1,169,133 sats	$ 348.62
Mempool:	45,678 sats	$ 13.62
Transactions:	4	

Date ▼	Label	Value
▸ Unconfirmed		○ 45,678



Flow

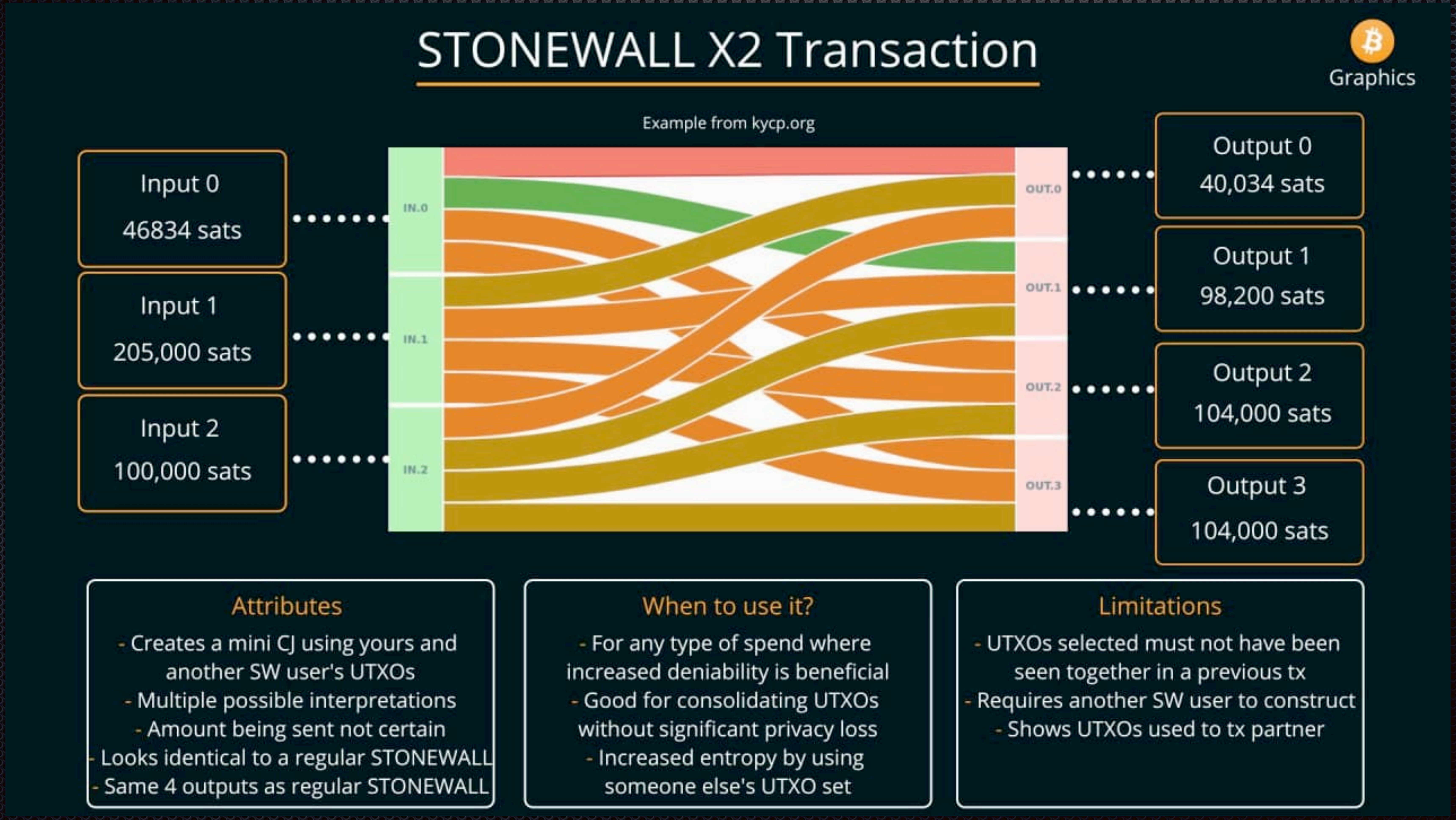
Inputs & Outputs

tb1qhxnwlsnw4z6lfwsnte4hal3… c8hydx5z	0.00123456 tBTC	tb1qt3c3uumtjt6cv9ysvafe363… z0nytwm8	0.00169134 tBTC
tb1qdchlq49337pzpga602ad42w… pra6twjk	0.00345678 tBTC	tb1qss2va22c25dfsq8udvn3tt6… mhmespxd	0.00299784 tBTC

0.00468918 tBTC

Stonewallx2

A 2-Person CoinJoin.



STONEWALL X2 Transaction

Graphics

Example from kycp.org

Input 0
46834 sats

Input 1
205,000 sats

Input 2
100,000 sats

Output 0
40,034 sats

Output 1
98,200 sats

Output 2
104,000 sats

Output 3
104,000 sats

Attributes

- Creates a mini CJ using yours and another SW user's UTXOs
- Multiple possible interpretations
- Amount being sent not certain
- Looks identical to a regular STONEWALL
- Same 4 outputs as regular STONEWALL

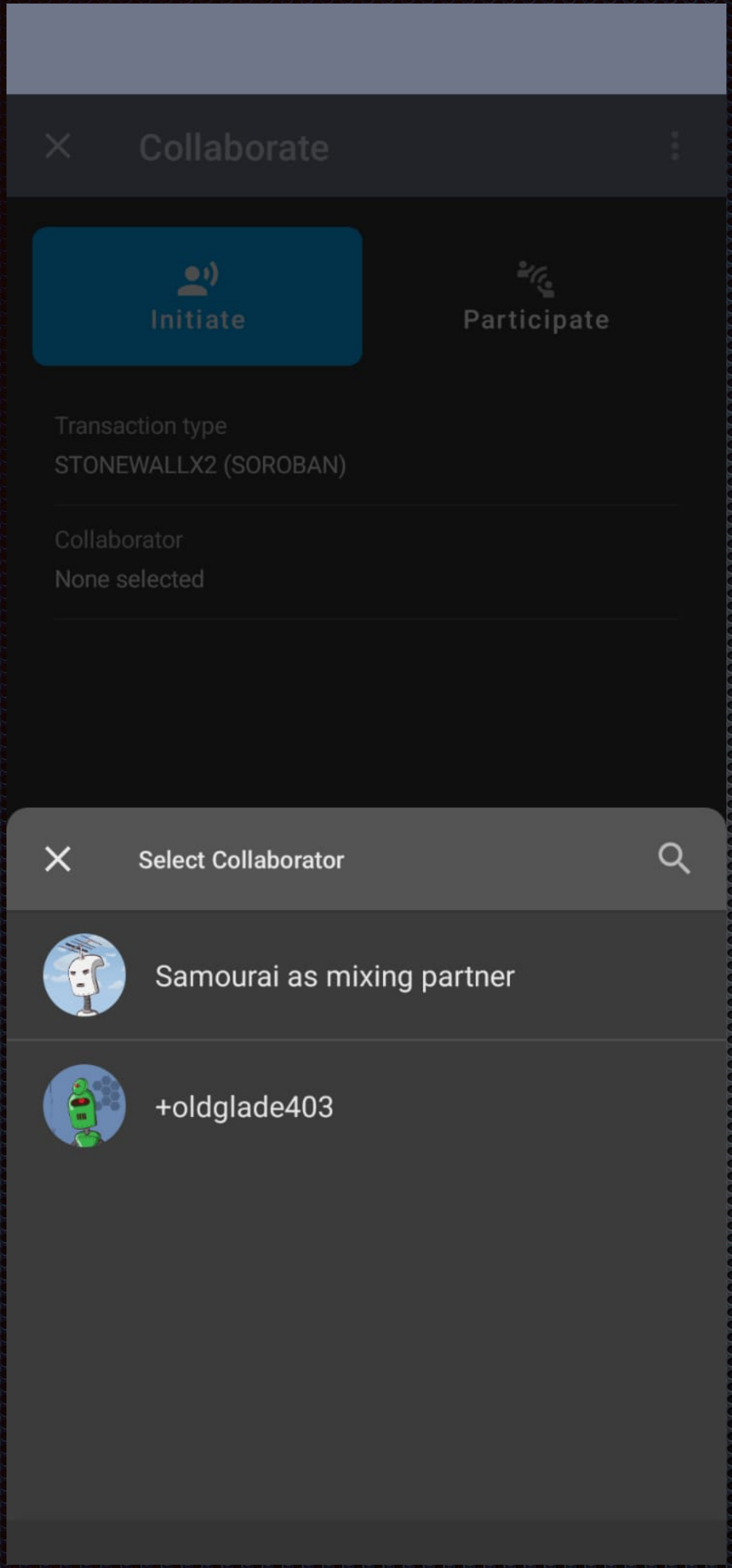
When to use it?

- For any type of spend where increased deniability is beneficial
- Good for consolidating UTXOs without significant privacy loss
- Increased entropy by using someone else's UTXO set

Limitations

- UTXOs selected must not have been seen together in a previous tx
- Requires another SW user to construct
- Shows UTXOs used to tx partner

[XTX]



Collaborate

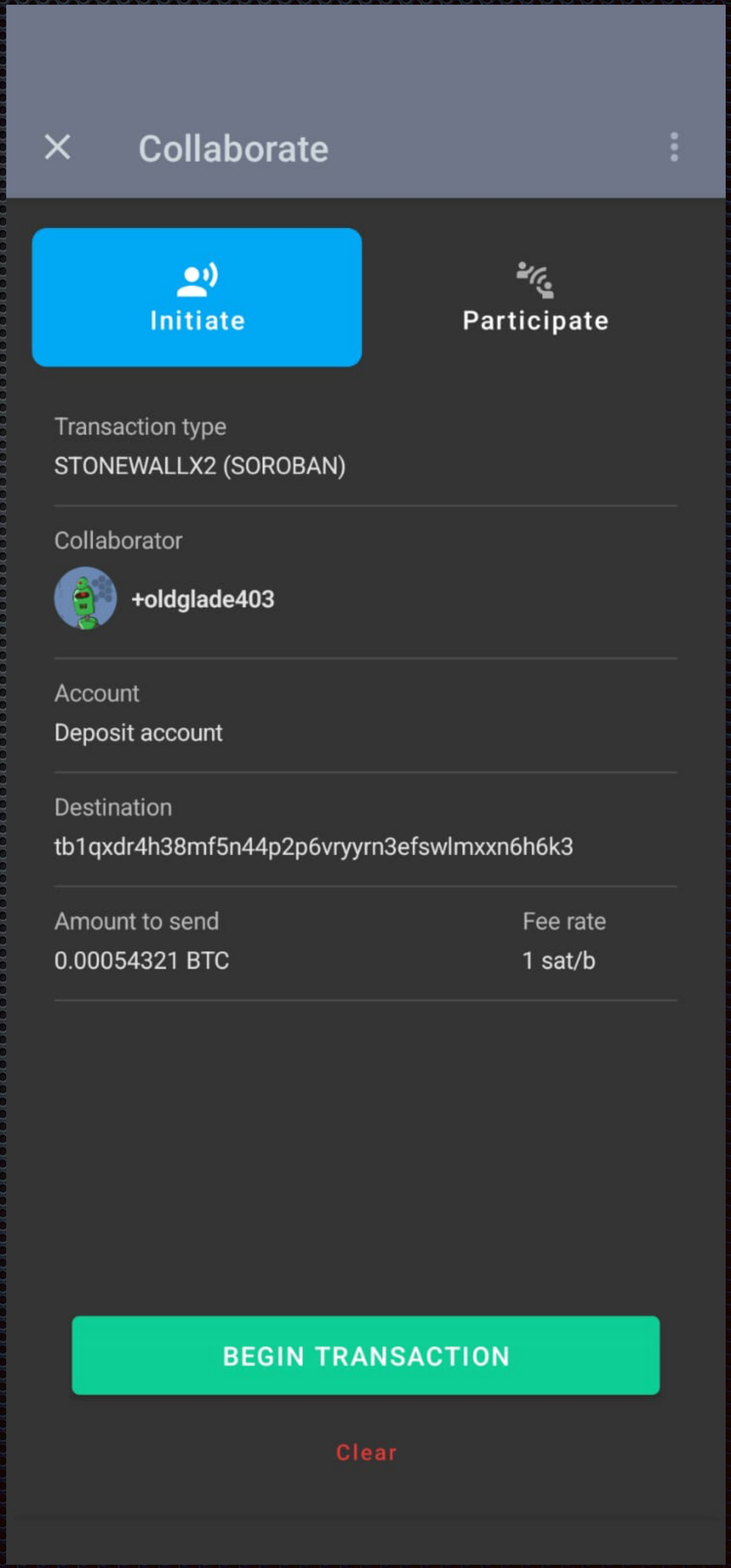
Transaction type
STONEWALLX2 (SOROBAN)

Collaborator
None selected

Select Collaborator

Samourai as mixing partner

+oldglade403



Collaborate

Transaction type
STONEWALLX2 (SOROBAN)

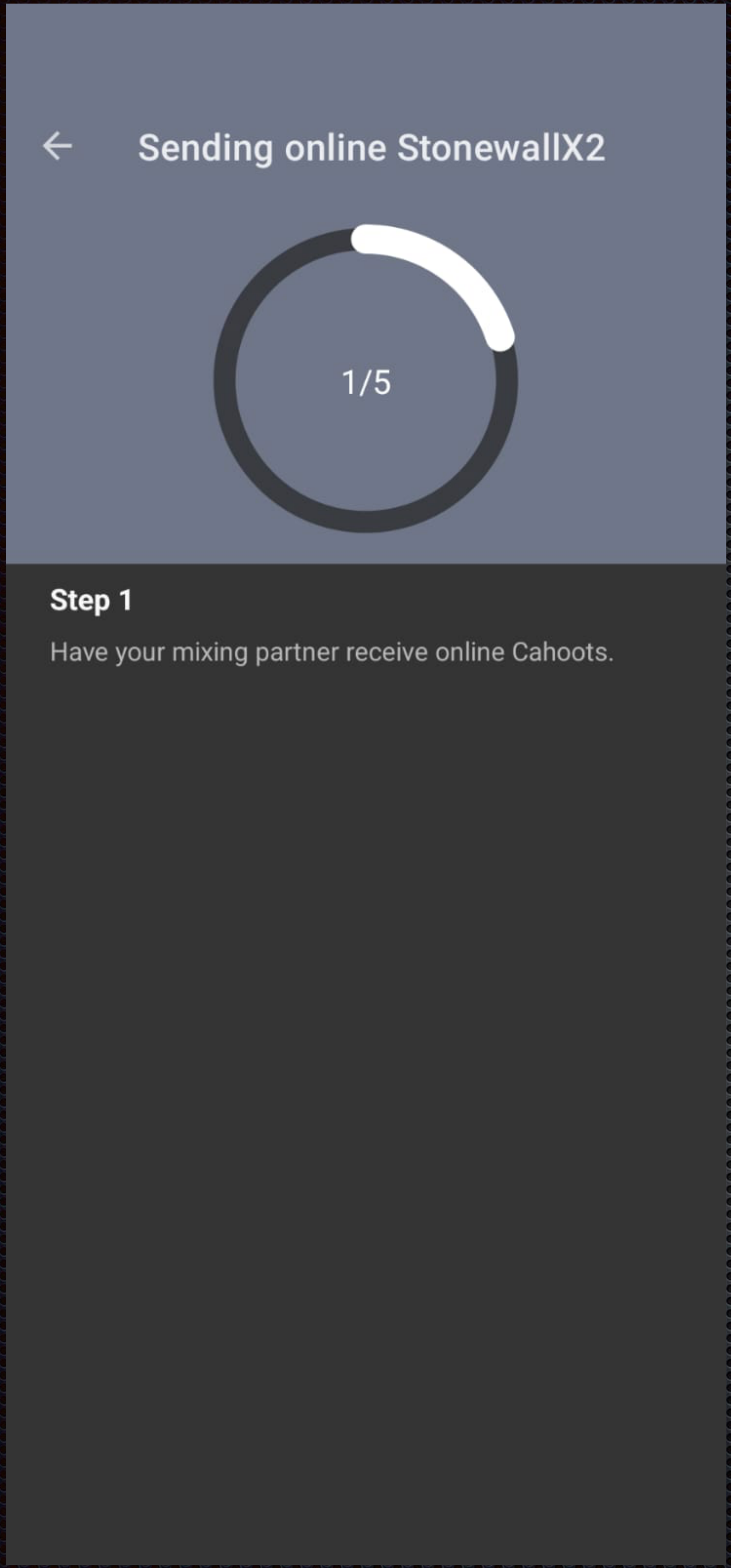
Collaborator
+oldglade403

Account
Deposit account

Destination
tb1qxdr4h38mf5n44p2p6vryyrn3efswlmxxn6h6k3

Amount to send
0.00054321 BTC

Fee rate
1 sat/b

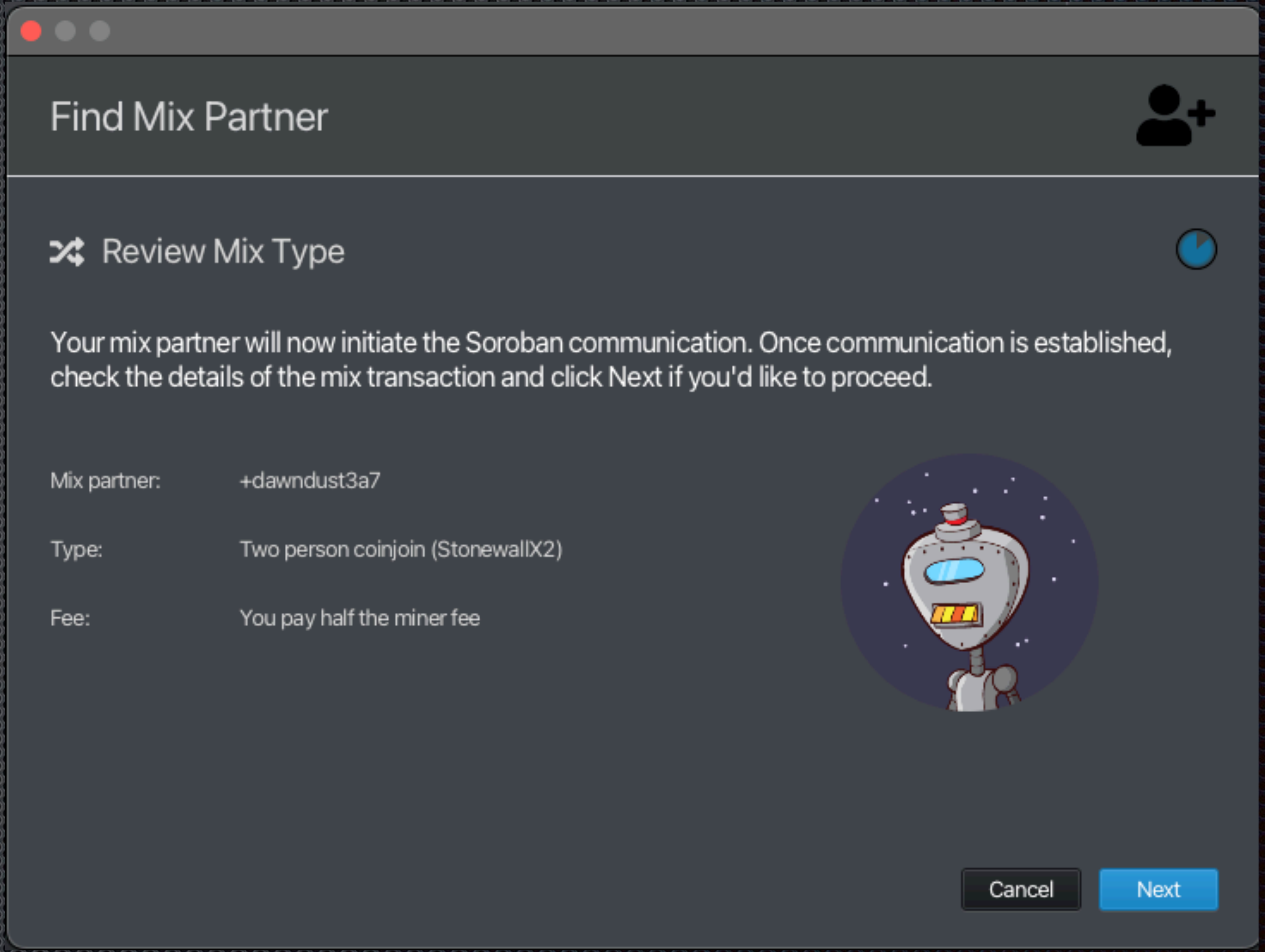


Sending online StonewallX2

1/5

Step 1

Have your mixing partner receive online Cahoots.

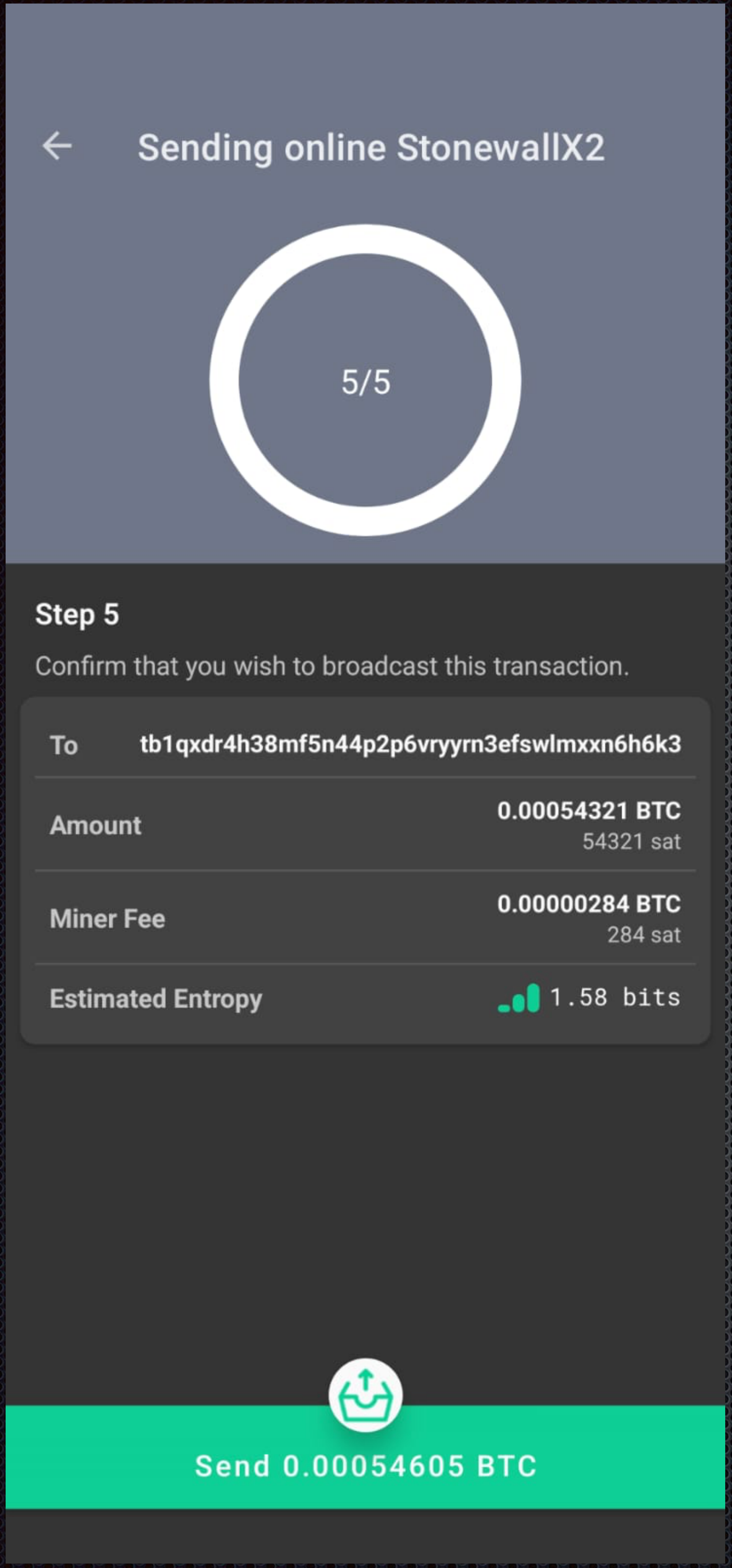


Find Mix Partner

Review Mix Type

Your mix partner will now initiate the Soroban communication. Once communication is established, check the details of the mix transaction and click Next if you'd like to proceed.

Mix partner:	+dawndust3a7
Type:	Two person coinjoin (StonewallX2)
Fee:	You pay half the miner fee



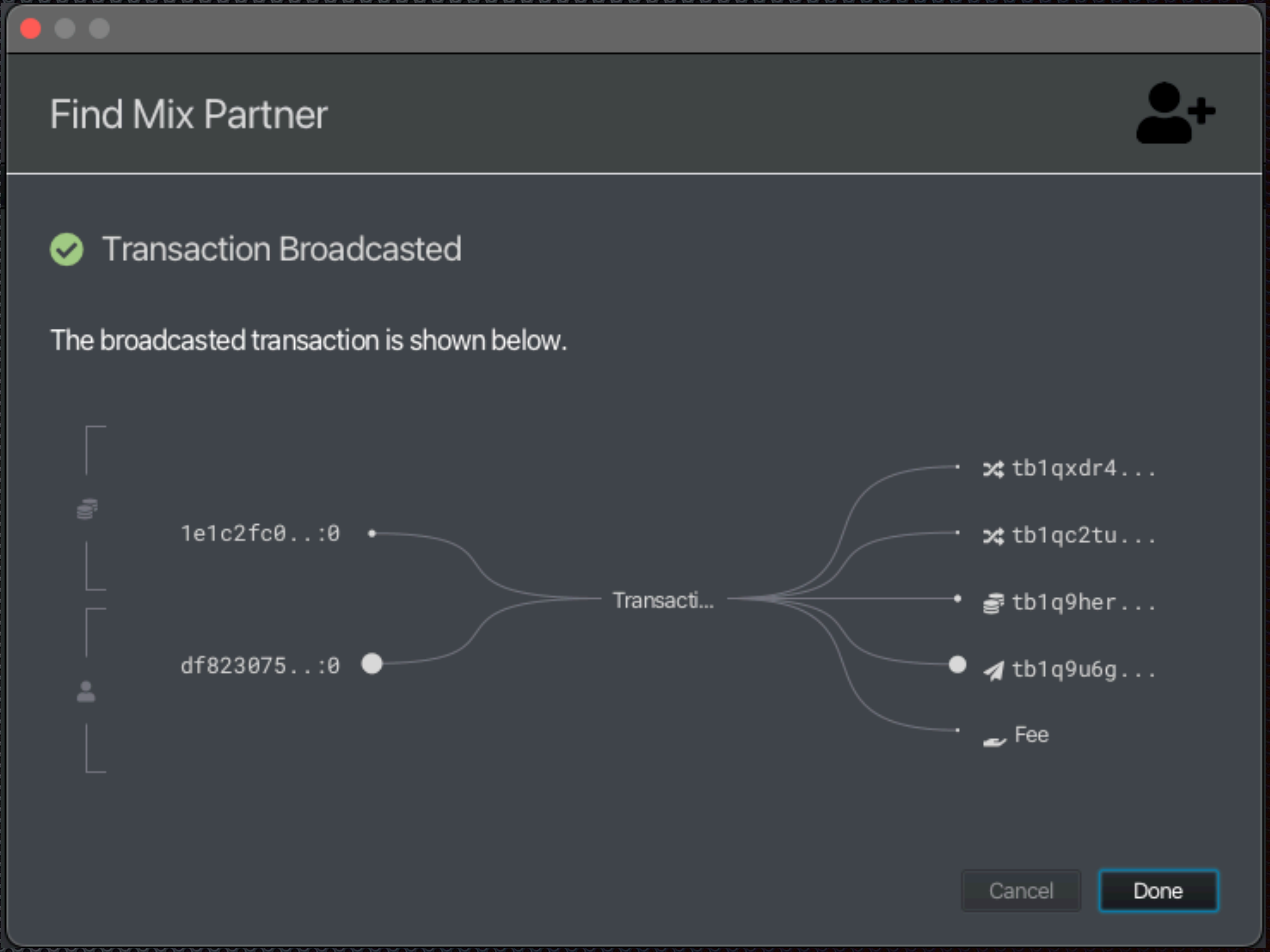
Sending online StonewallX2

5/5

Step 5

Confirm that you wish to broadcast this transaction.

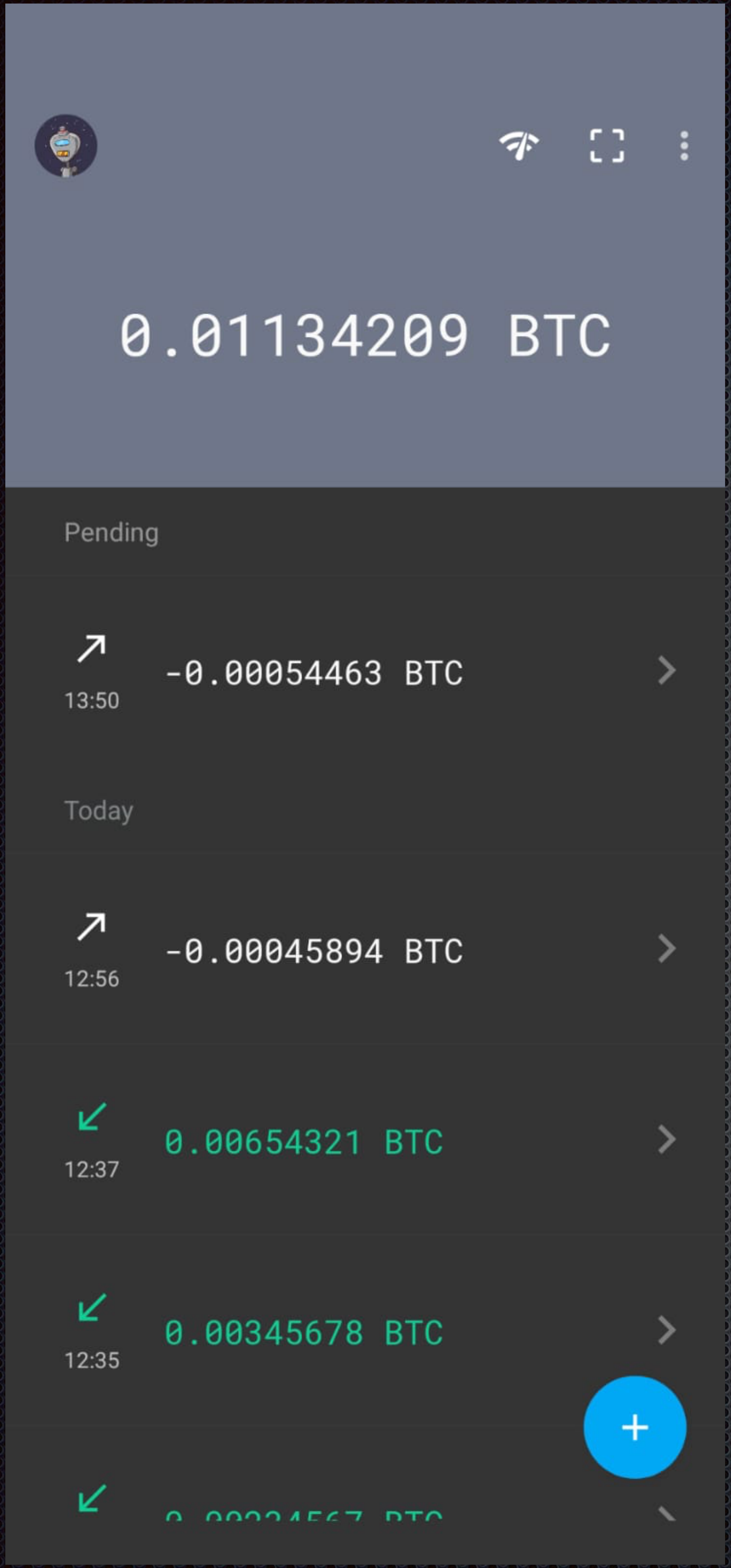
To	tb1qxdr4h38mf5n44p2p6vryyrn3efswlmxxn6h6k3
Amount	0.00054321 BTC 54321 sat
Miner Fee	0.00000284 BTC 284 sat
Estimated Entropy	1.58 bits



Find Mix Partner

Transaction Broadcasted

The broadcasted transaction is shown below.



0.01134209 BTC

Pending

-0.00054463 BTC
13:50

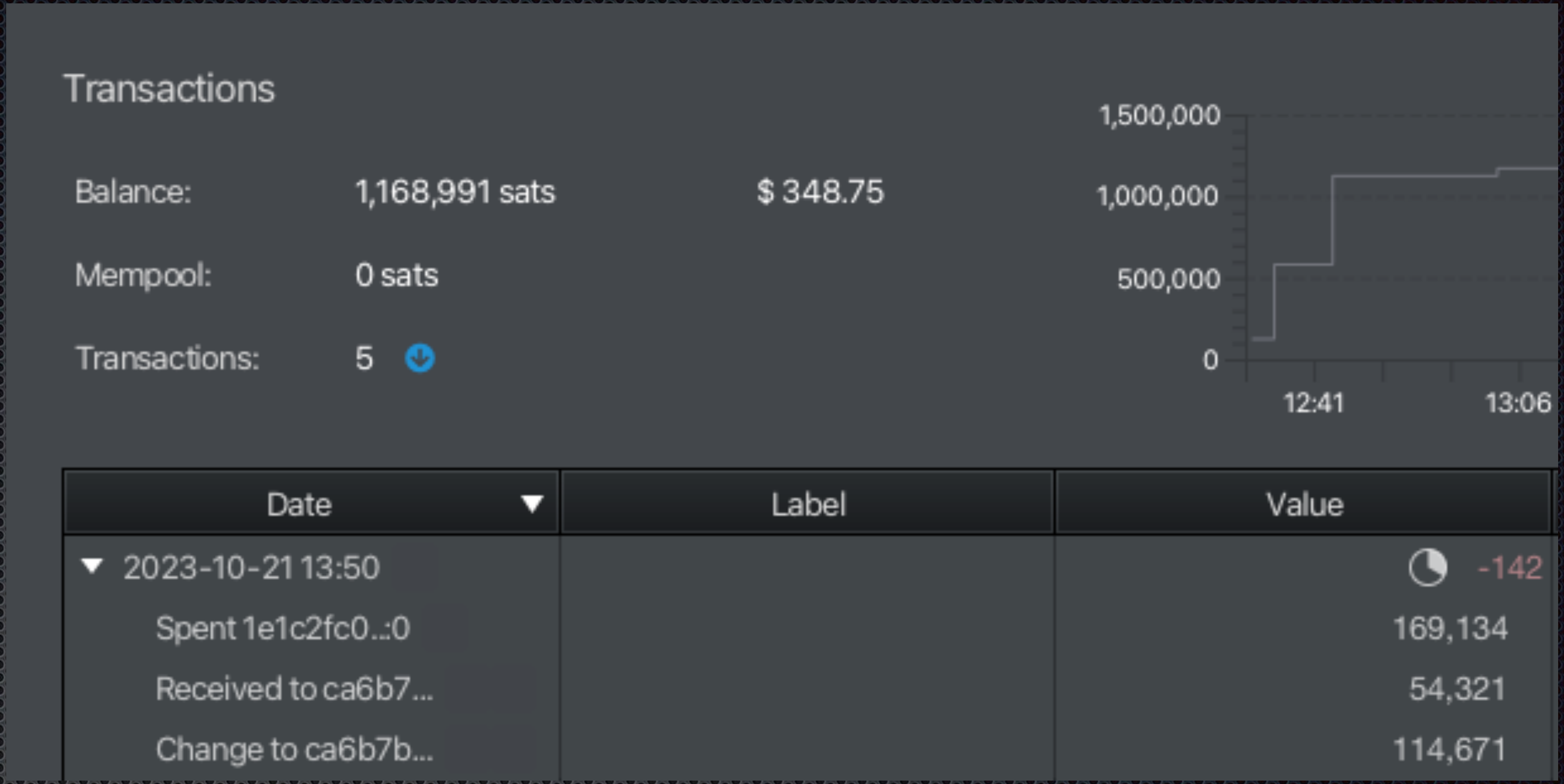
Today

-0.00045894 BTC
12:56

0.00654321 BTC
12:37

0.00345678 BTC
12:35

0.00234567 BTC



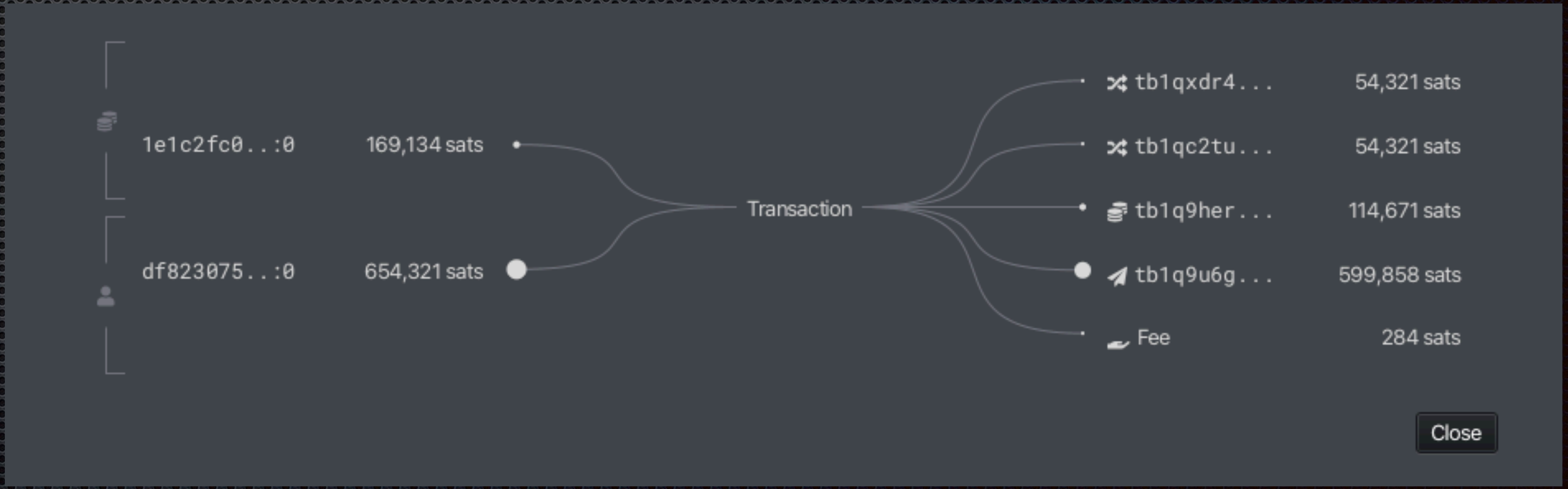
Transactions

Balance: 1,168,991 sats $ 348.75

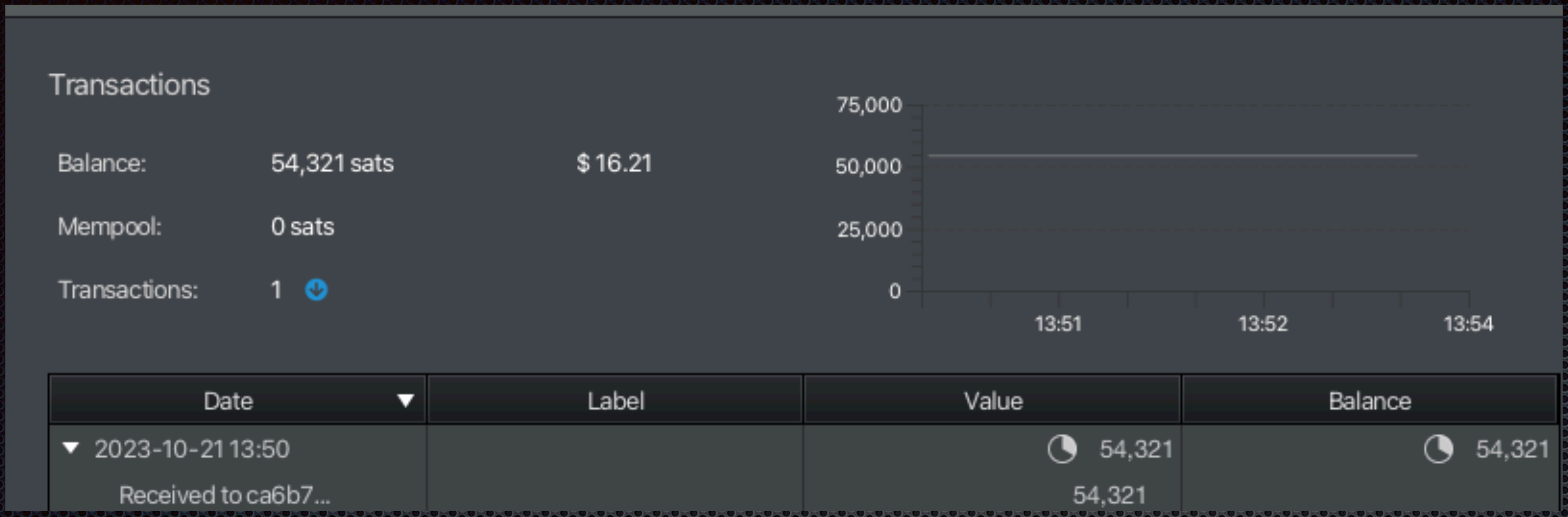
Mempool: 0 sats

Transactions: 5

Date ▼	Label	Value
2023-10-21 13:50		-142
Spent 1e1c2fc0..:0		169,134
Received to ca6b7...		54,321
Change to ca6b7b...		114,671



1e1c2fc0..:0	169,134 sats	Transaction	tb1qxdr4...	54,321 sats
df823075..:0	654,321 sats		tb1qc2tu...	54,321 sats
			tb1q9her...	114,671 sats
			tb1q9u6g...	599,858 sats
			Fee	284 sats



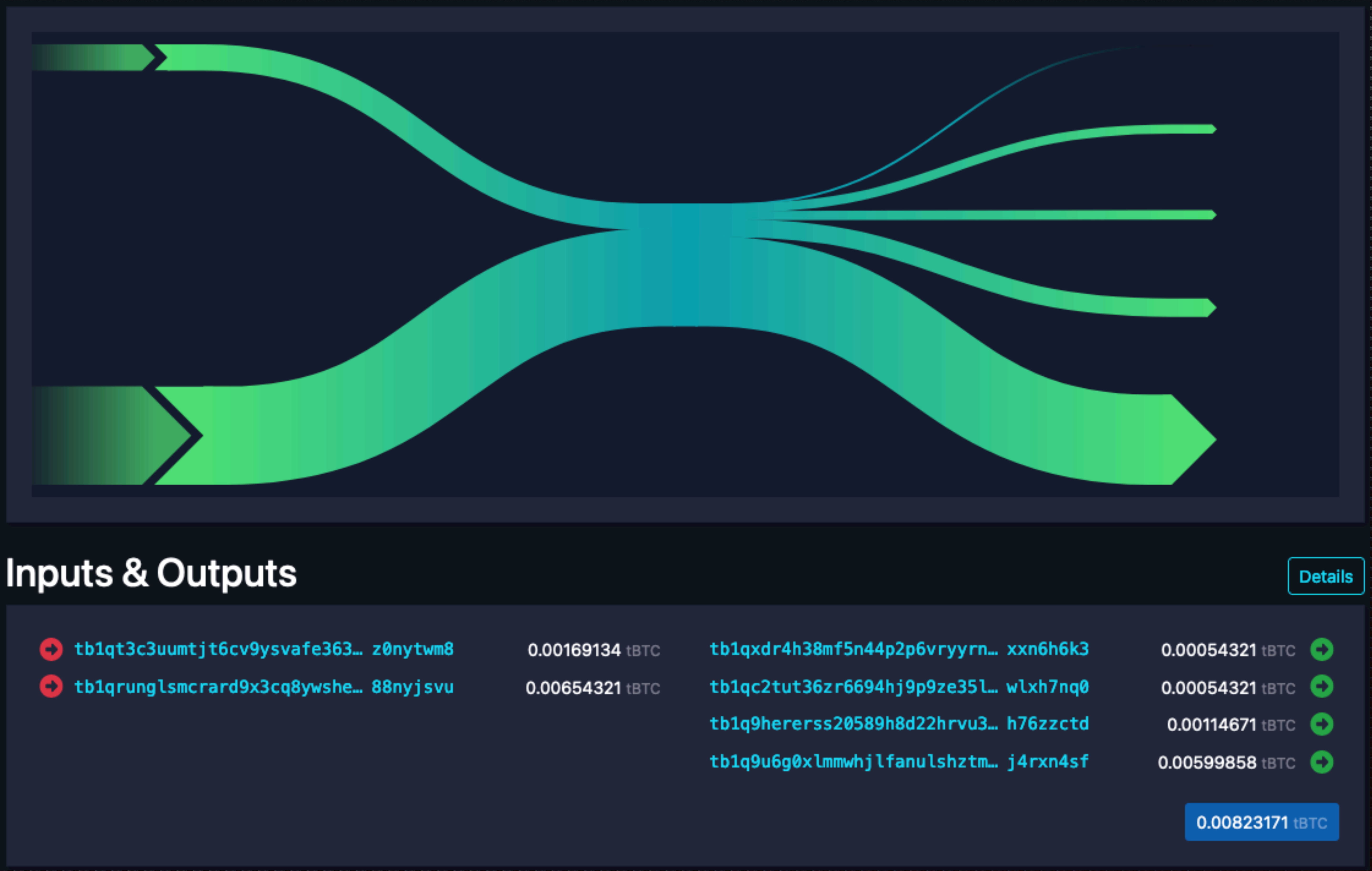
Transactions

Balance: 54,321 sats $ 16.21

Mempool: 0 sats

Transactions: 1

Date	Label	Value	Balance
▼ 2023-10-21 13:50		54,321	54,321
Received to ca6b7...		54,321	



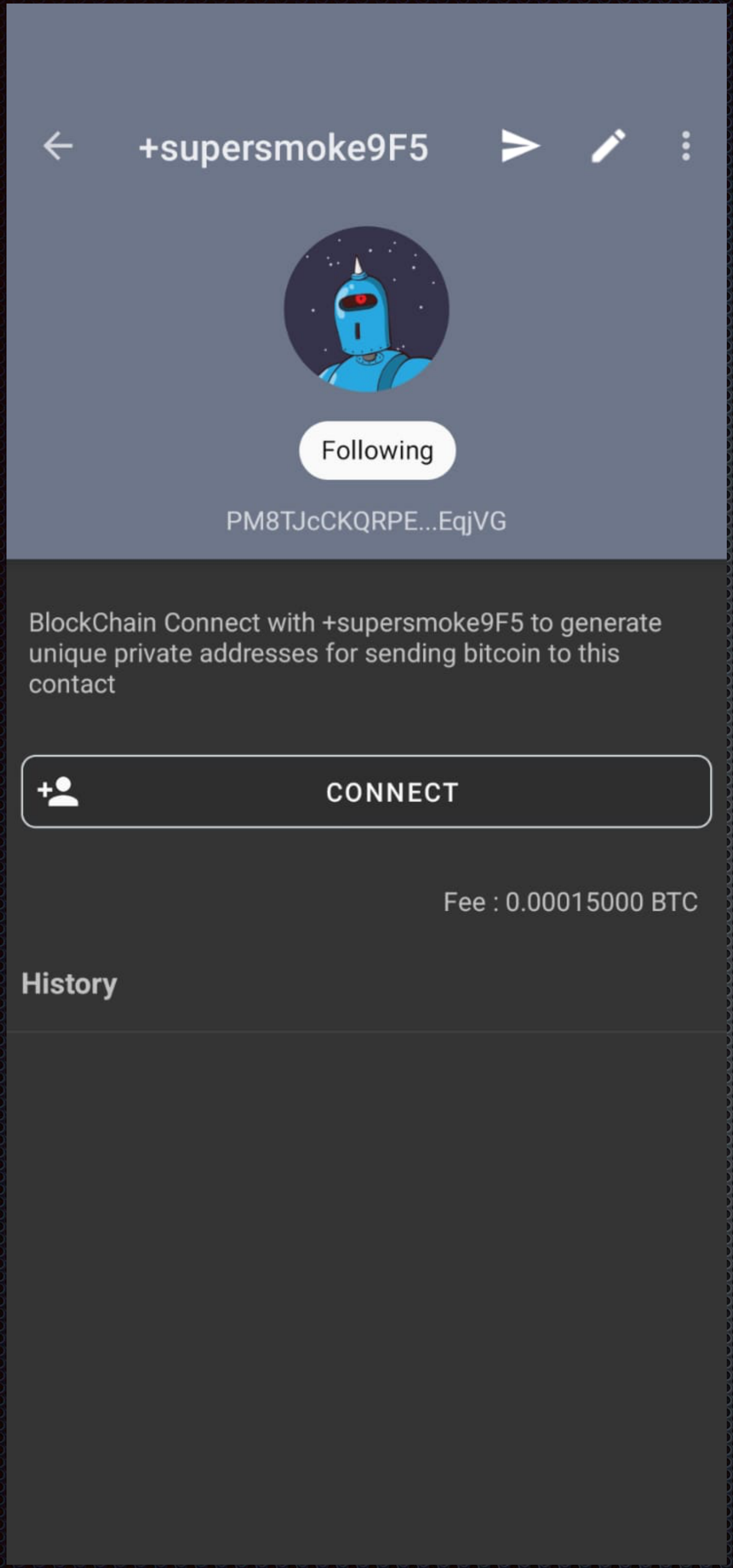
Inputs & Outputs

tb1qt3c3uumtjt6cv9ysvafe363… z0nytwm8	0.00169134 tBTC	tb1qxdr4h38mf5n44p2p6vryyrn… xxn6h6k3	0.00054321 tBTC
tb1qrunglsmcrard9x3cq8ywshe… 88nyjsvu	0.00654321 tBTC	tb1qc2tut36zr6694hj9p9ze35l… wlxh7nq0	0.00054321 tBTC
		tb1q9hererss20589h8d22hrvu3… h76zzctd	0.00114671 tBTC
		tb1q9u6g0xlmmwhjlfanulshztm… j4rxn4sf	0.00599858 tBTC
			0.00823171 tBTC

No collaborative (Connected)

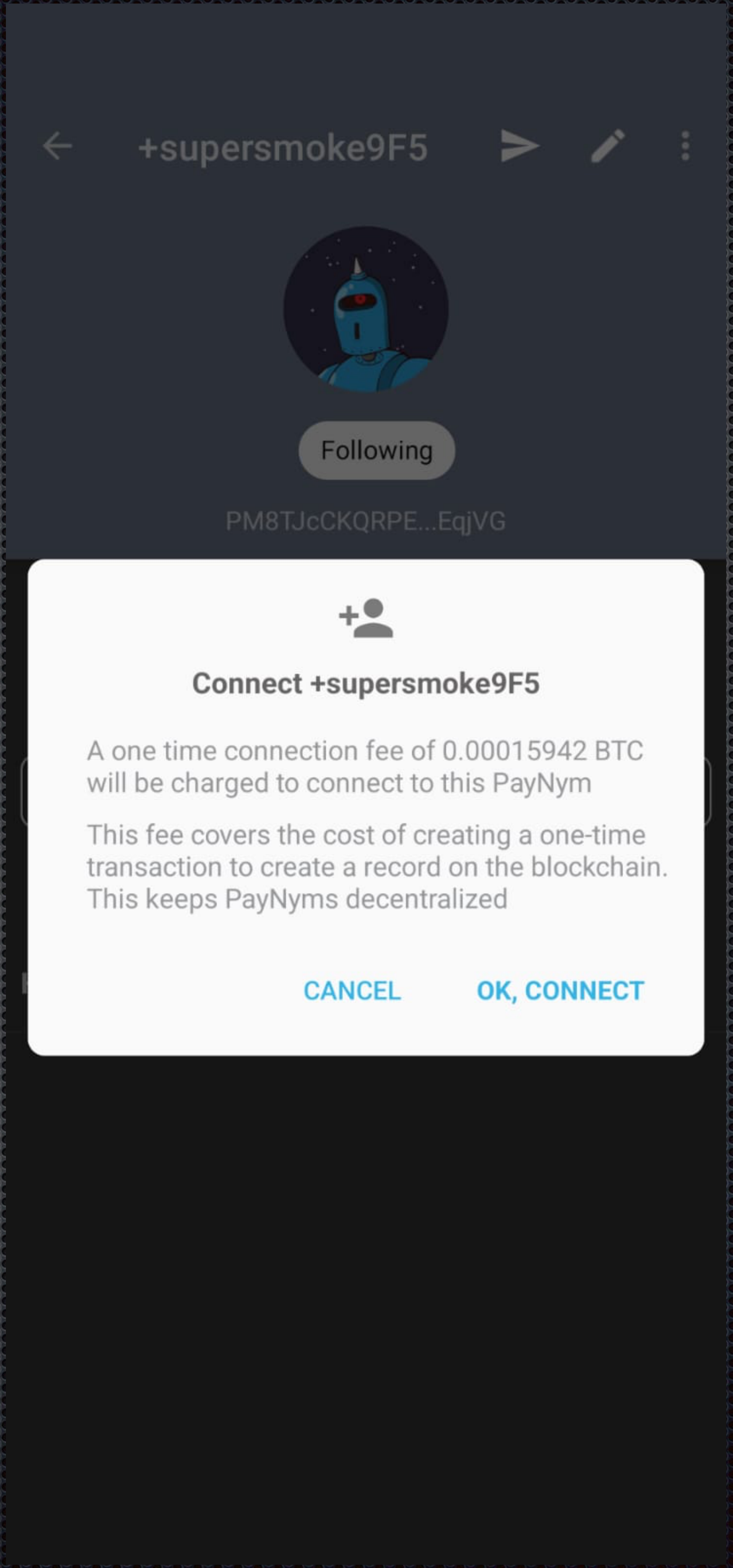
If we are connected, we can send funds without the interaction of the other side.

[XTX]



BlockChain Connect with +supersmoke9F5 to generate unique private addresses for sending bitcoin to this contact

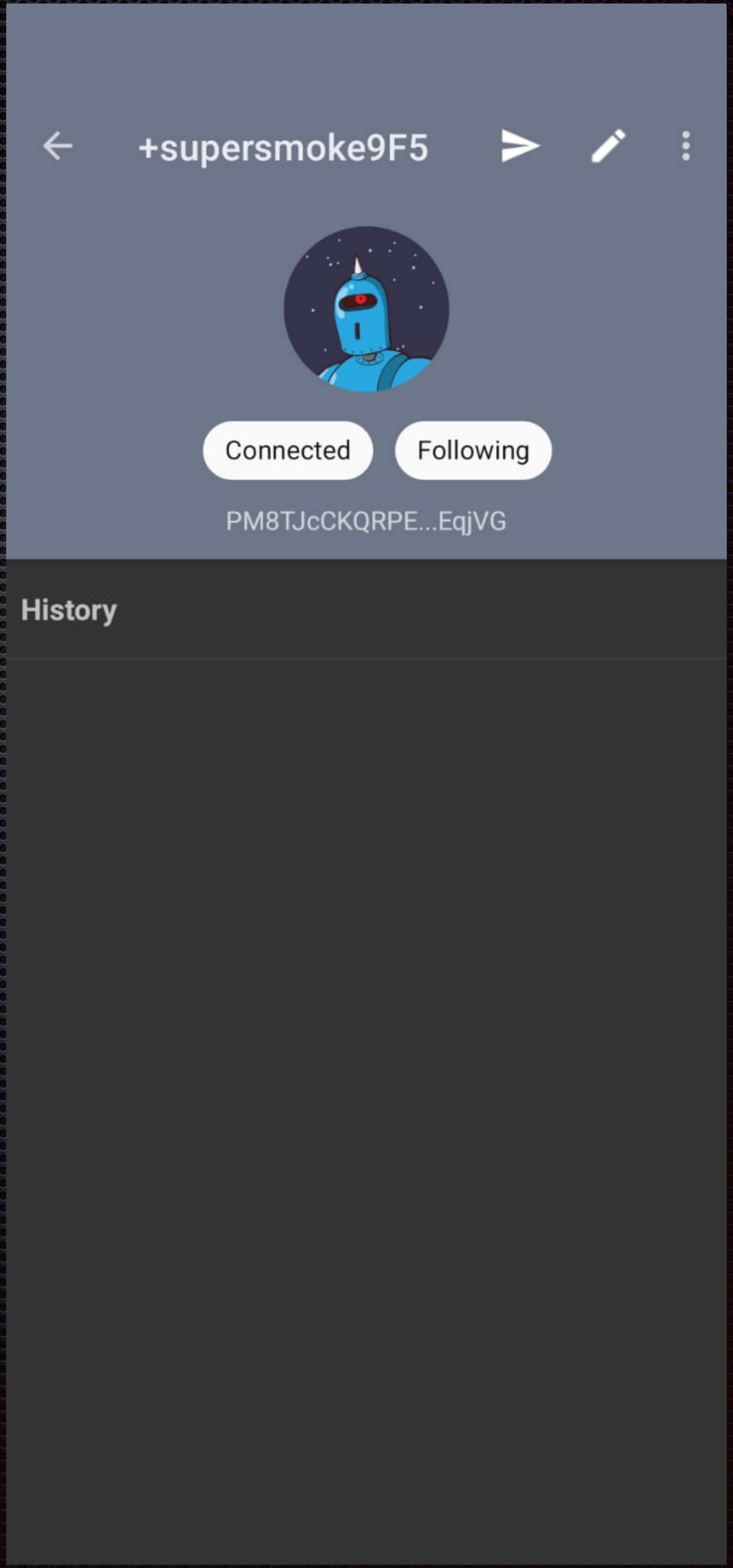
Fee : 0.00015000 BTC



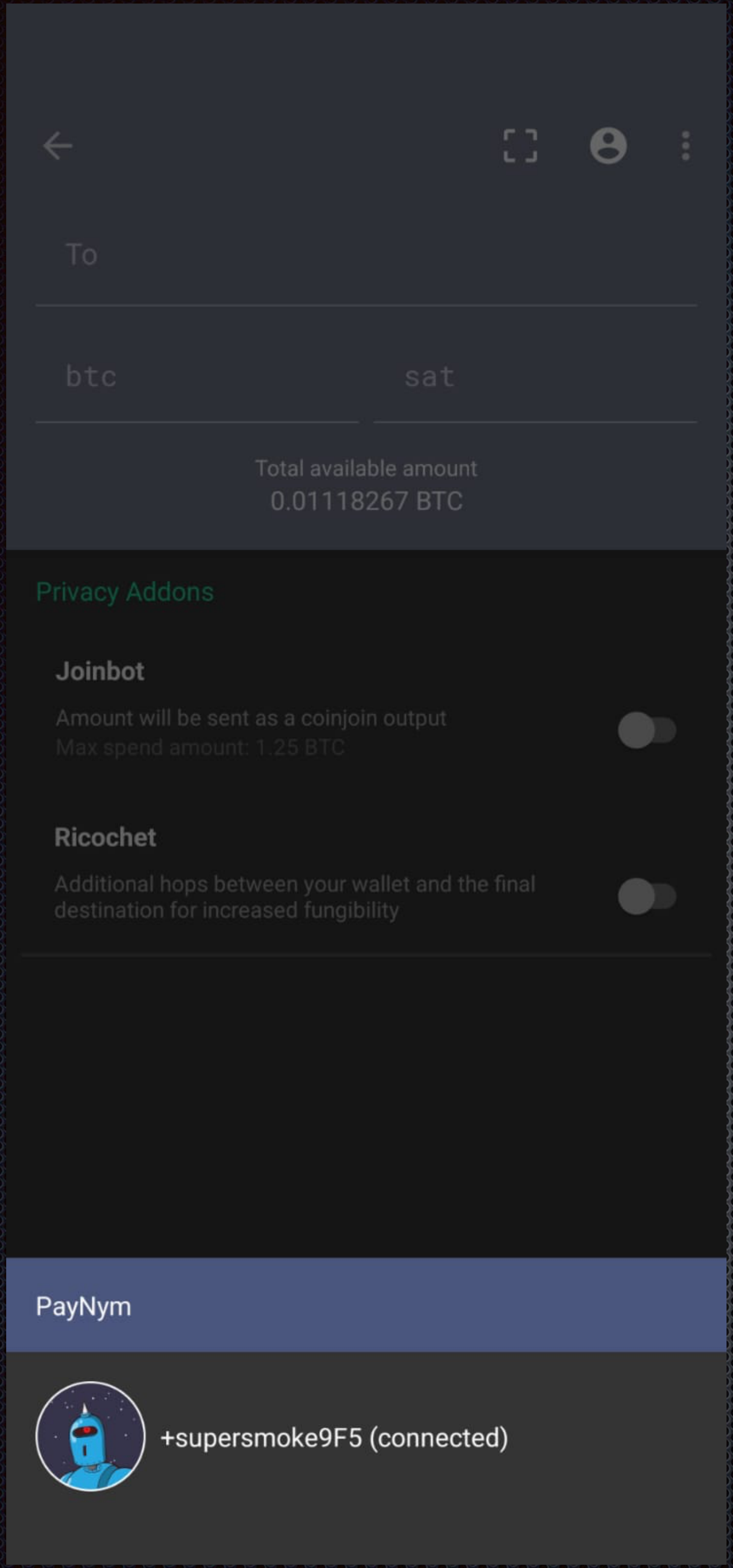
Connect +supersmoke9F5

A one time connection fee of 0.00015942 BTC will be charged to connect to this PayNym

This fee covers the cost of creating a one-time transaction to create a record on the blockchain. This keeps PayNyms decentralized



[XTX]



To

btc

sat

Total available amount
0.01118267 BTC

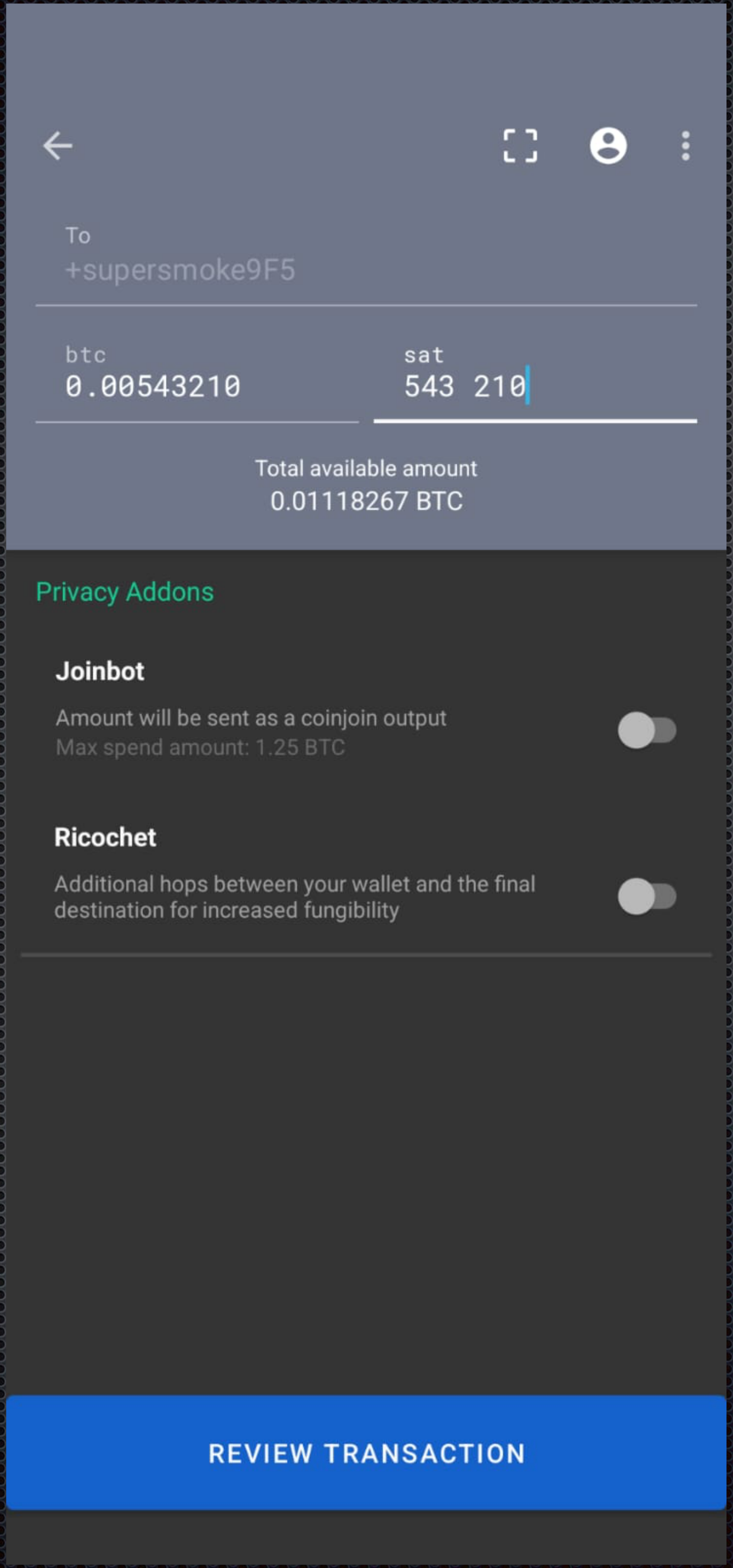
Privacy Addons

Joinbot
Amount will be sent as a coinjoin output
Max spend amount: 1.25 BTC

Ricochet
Additional hops between your wallet and the final destination for increased fungibility

PayNym

+supersmoke9F5 (connected)



To
+supersmoke9F5

btc
0.00543210

sat
543 210

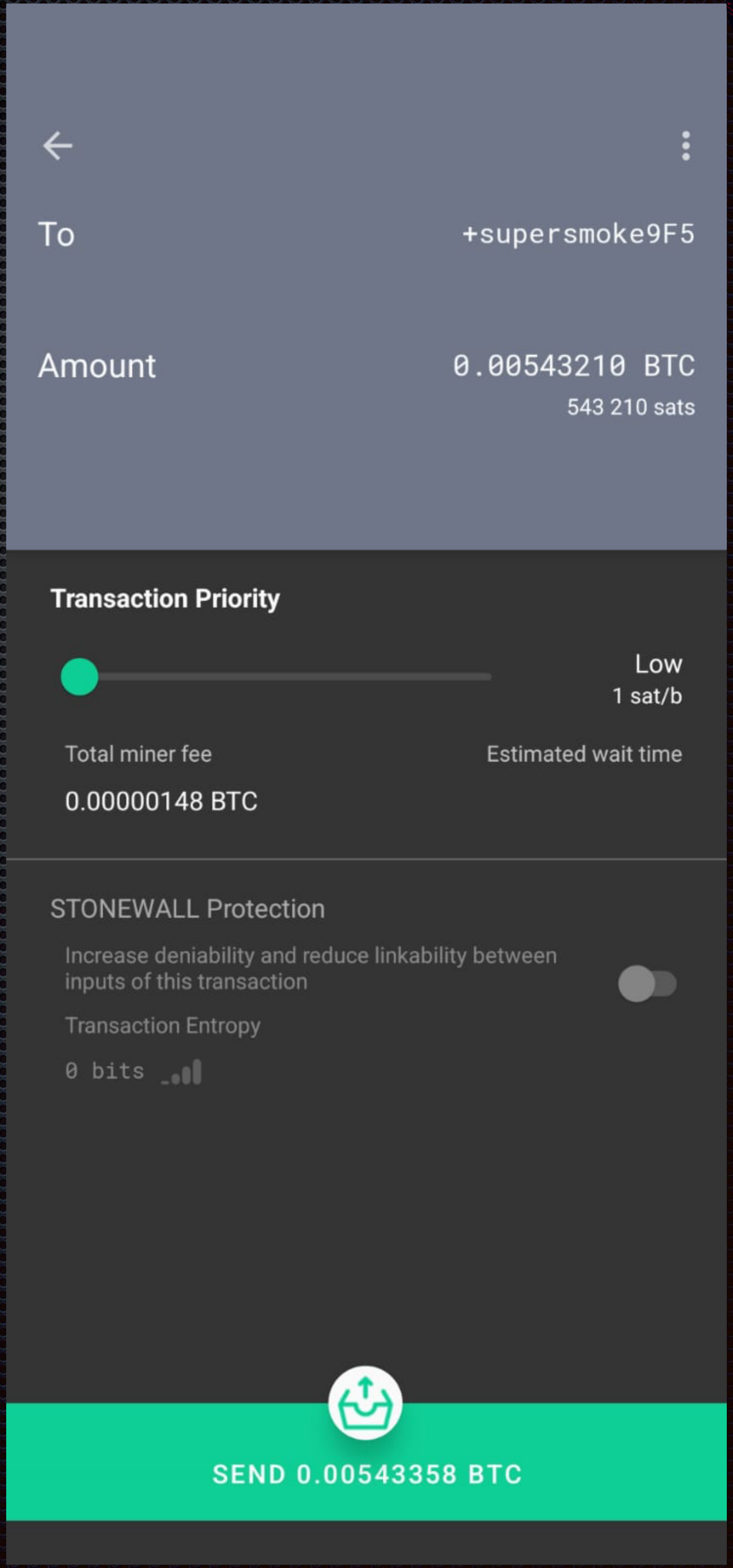
Total available amount
0.01118267 BTC

Privacy Addons

Joinbot
Amount will be sent as a coinjoin output
Max spend amount: 1.25 BTC

Ricochet
Additional hops between your wallet and the final destination for increased fungibility

REVIEW TRANSACTION



To +supersmoke9F5

Amount 0.00543210 BTC
543 210 sats

Transaction Priority

Low
1 sat/b

Total miner fee
0.00000148 BTC

Estimated wait time

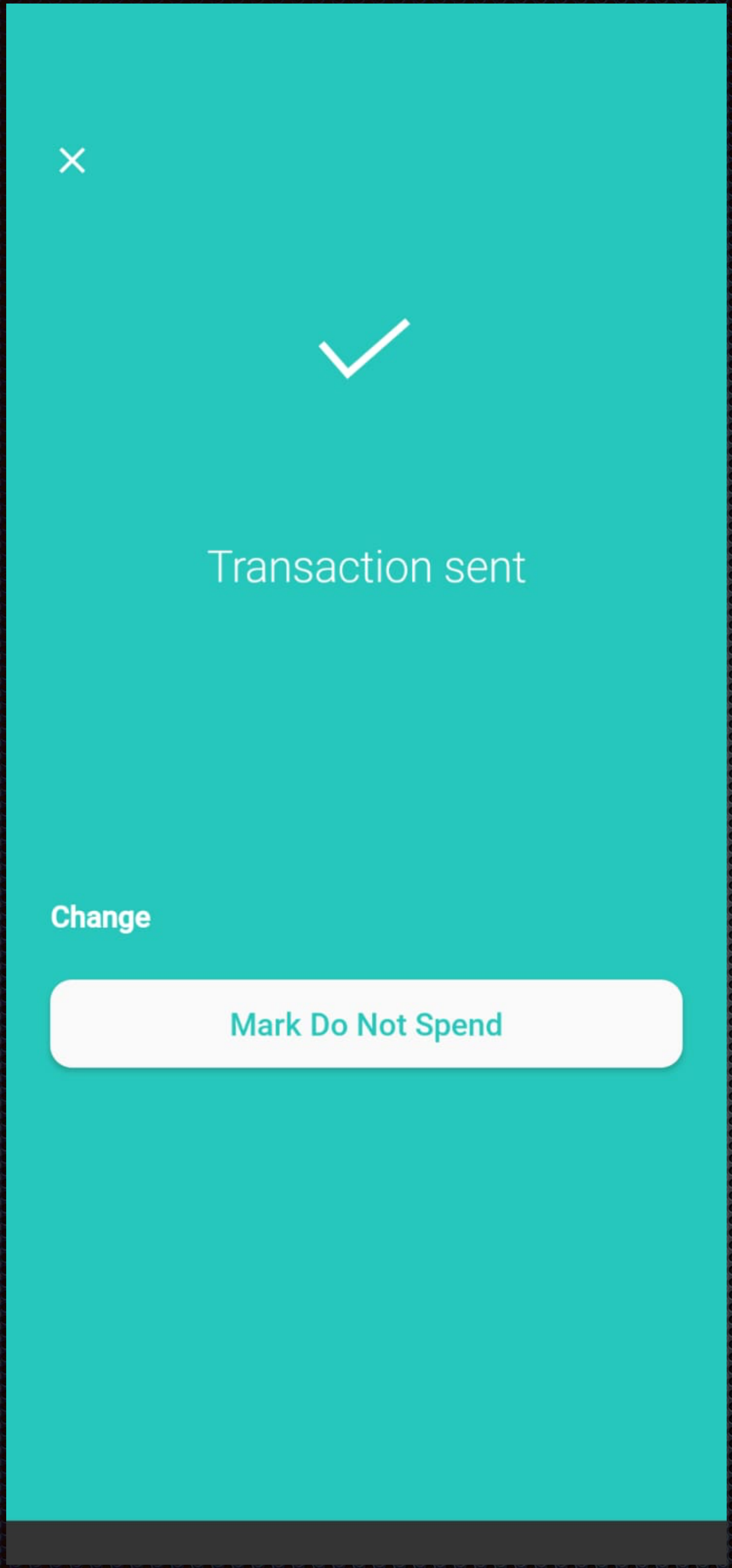
STONEWALL Protection

Increase deniability and reduce linkability between inputs of this transaction

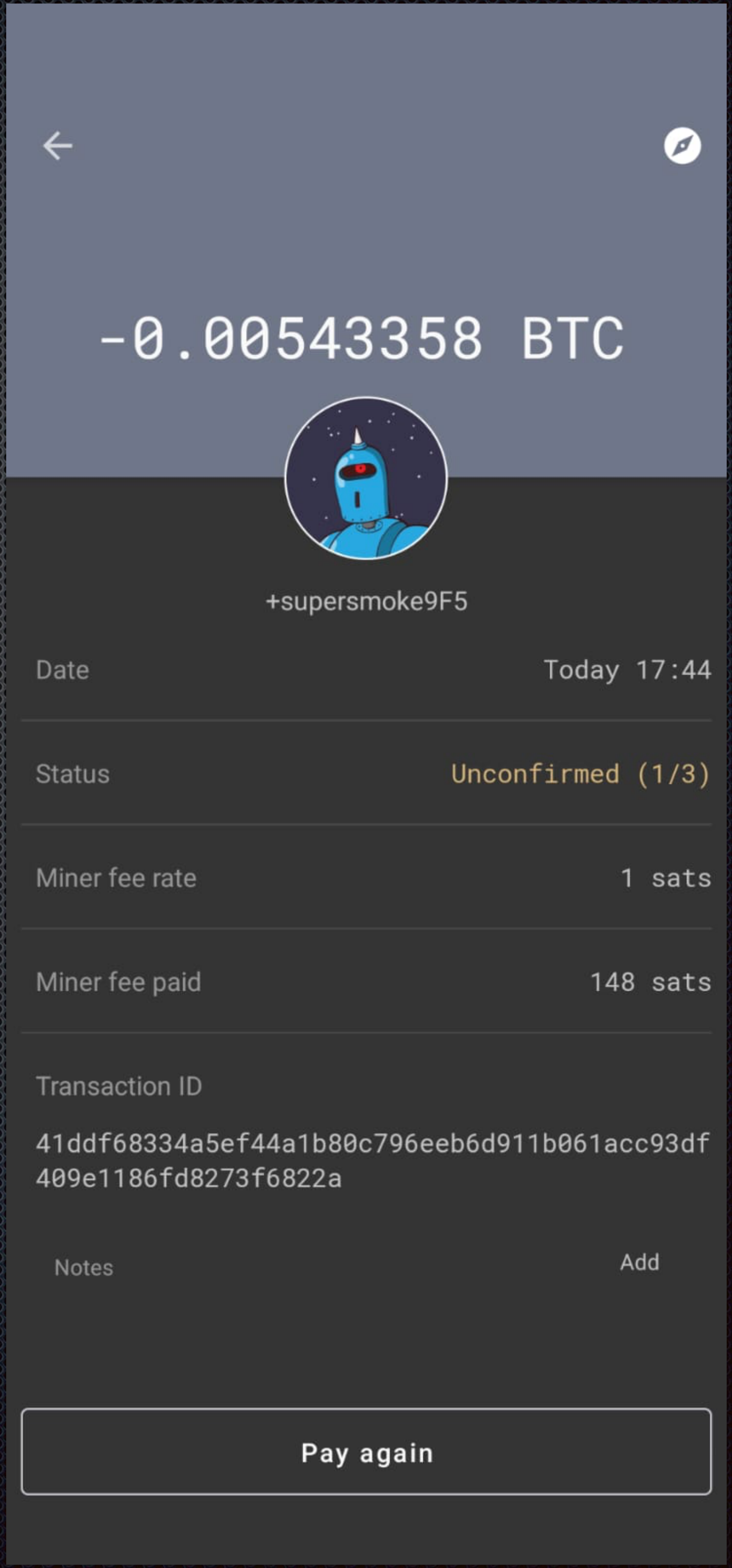
Transaction Entropy

0 bits

SEND 0.00543358 BTC



Transaction sent



-0.00543358 BTC

+supersmoke9F5

Date Today 17:44

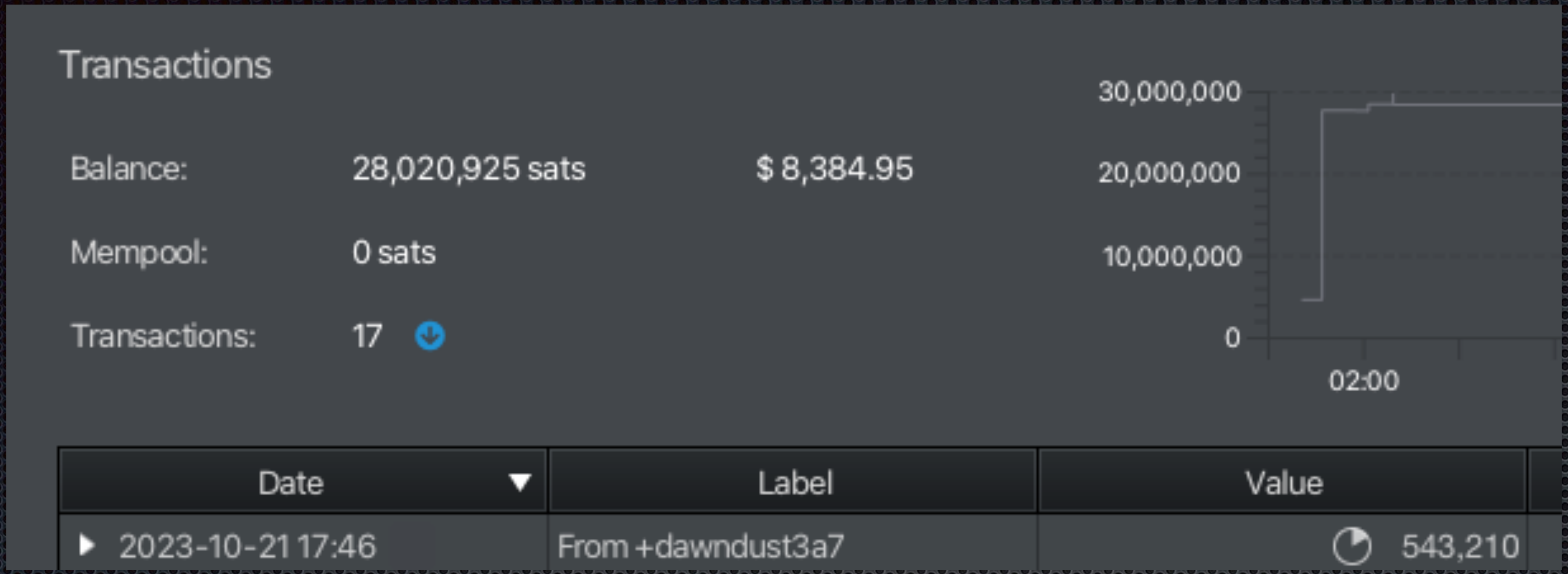
Status Unconfirmed (1/3)

Miner fee rate 1 sats

Miner fee paid 148 sats

Transaction ID

41ddf68334a5ef44a1b80c796eeb6d911b061acc93df409e1186fd8273f6822a



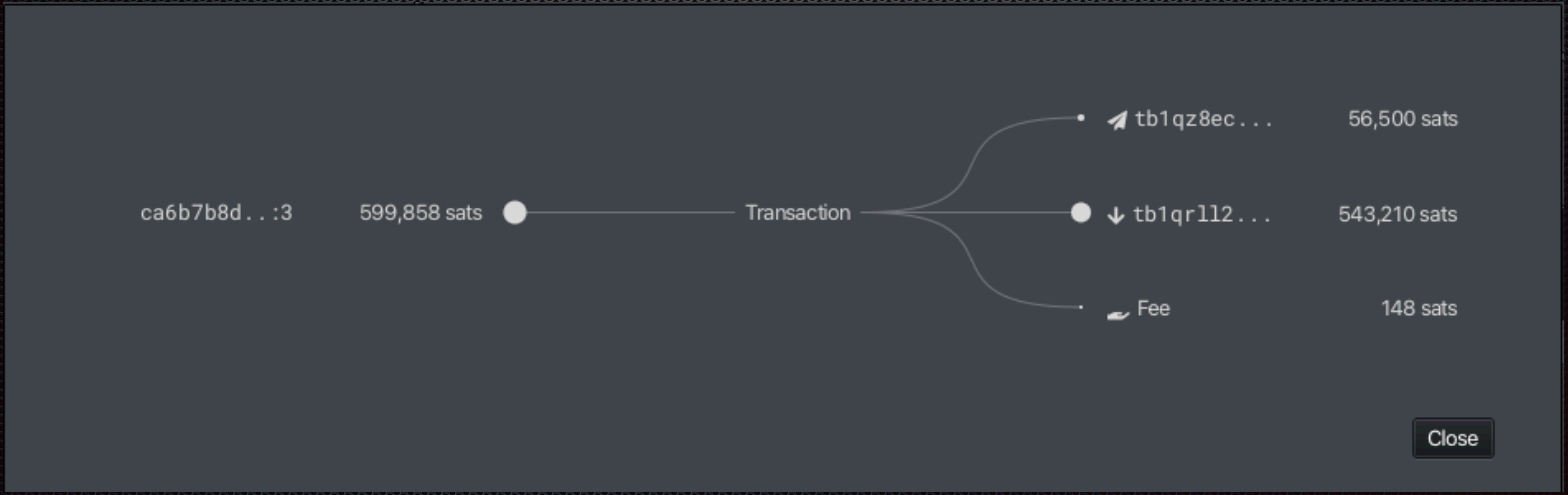
Transactions

Balance: 28,020,925 sats $ 8,384.95

Mempool: 0 sats

Transactions: 17

Date	Label	Value
▶ 2023-10-21 17:46	From +dawndust3a7	543,210



ca6b7b8d..:3 599,858 sats

Transaction

tb1qz8ec... 56,500 sats

tb1qrl12... 543,210 sats

Fee 148 sats

> *“Further, even though collaborative transactions require more effort, the value they provide not only to you but to other users is significant. Consider using these techniques for every transaction you send. It is never too late to start.”*

–Craig Raw–

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main

Credits:

- https://github.com/bitcoin/bips/blob/master/bip-0047.mediawiki#protocol
- https://gist.github.com/RubenSomsen/c43b79517e7cb701ebf77eec6dbb46b8
- https://bitcoiner.guide/paynym/
- https://www.paynym.is/
- https://docs.samourai.io/en/wallet/features/paynym
- https://sparrowwallet.com/
- https://foundationdevices.com/