





## Mempool & RBF - CPFP Dublin Bitcoiners Meet Up





# Mynatis the memoral







### Steps from the moment we broadcast a tx.

- The node contacts another node, and so we propagate the transaction
- So until it reaches a miner
- The miners place the tx based on the fees they are willing to pay. Miners are rational and want to maximize their efforts.\*
- There's an auction every 10 minutes for space.
- It is a dynamic market.





#### Broadcast directly into the main mempools to avoid purging

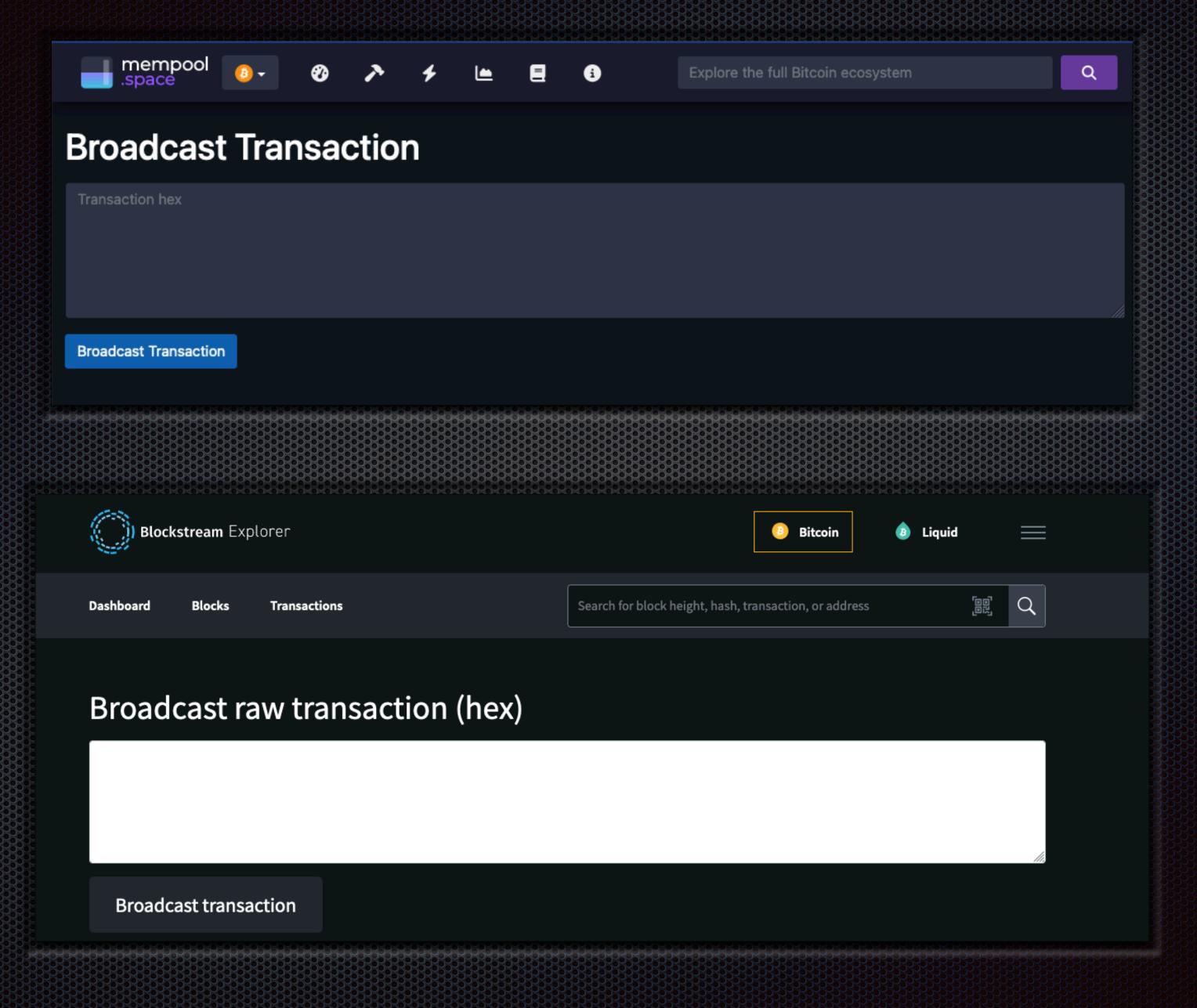


















Select the perfect fee for your transaction and check the current status of the mempool.

mempoolhqx4isw62xs7abwphsq7ldayuidyx2v2oethdhhj6mlo2r6ad.onion https://mempool.space



Get a transaction summary with fundamental technical and privacy analysis.

oxtmblv4v7q5rotqtbbmtbcc5aa5vehr72eiebyamclfo3rco5zm3did.onion https://light.oxt.me/



Check the details of your transaction and basic privacy analysis.

explorerzydxu5ecjrkwceayqybizmpjjznk5izmitf2modhcusuqlid.onion <a href="https://blockstream.info/">https://blockstream.info/</a>



~15 sat/vB

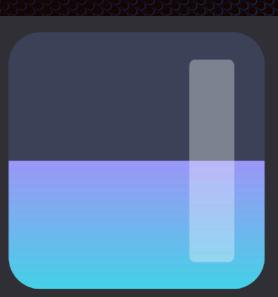
345.68 MB

(177 blocks)

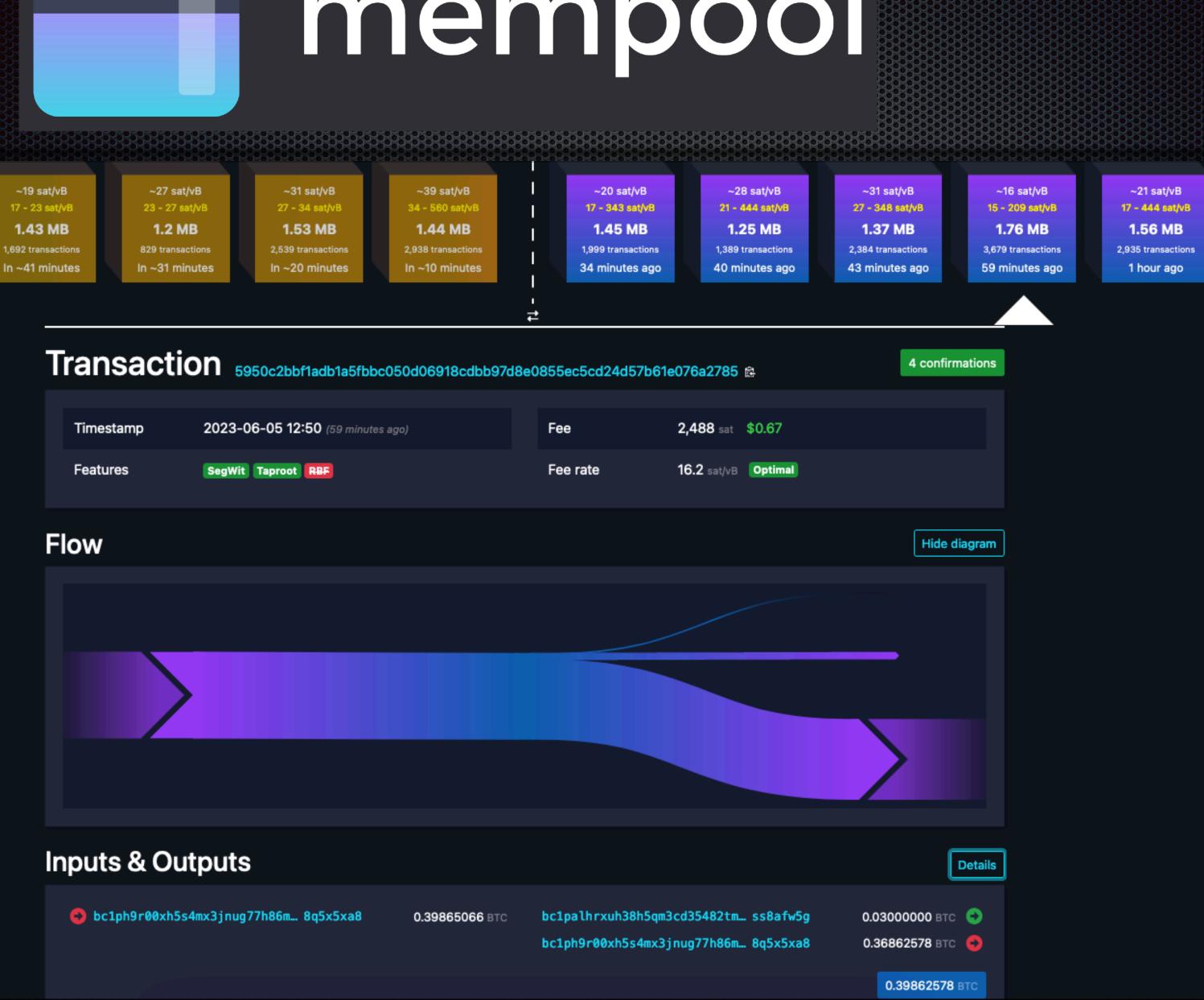
~15 sat/vB

2.04 MB

In ~51 minutes



## mempool











#### TRANSACTION Segwit taproot

5950c2bbf1adb1a5fbbc050d06918cdbb97d8e0855ec5cd24d57b61e076a2785

MONDAY, JUNE 5, 2023 11:50 AM [BLOCK 792960]

SUMMARY INPUTS & OUTPUTS TECHNICAL NOTES (0)

#### FINANCIAL

BDD

VOLUME FEES FEES/VBYTE FEES/BYTE

0.39862578 B 0.00002488 B

16.16 SAT/VB

12.14 SAT/B

0.00 B.DAYS

INPUTS

UTXOS CONSUMED ADDRESSES

#### OUTPUTS

UTXOS CREATED ADDRESSES

#### PRIVACY

NEW ADDRESSES

PREVIOUSLY USED ADDRESSES

TX ENTROPY

50% 0 BITS

#### TRANSACTION Segwit (taproot)



5950c2bbf1adb1a5fbbc050d06918cdbb97d8e0855ec5cd24d57b61e076a2785

MONDAY, JUNE 5, 2023 11:50 AM [BLOCK 792960]

INPUTS & OUTPUTS TECHNICAL NOTES (0)

< bc1ph9r00xh5s4mx3jnug77h86m52j59g0879wm... -0.39865066 B

bc1palhrxuh38h5qm3cd35482tmq4s7fs5f5xne... 0.03000000 B

bc1ph9r00xh5s4mx3jnug77h86m52j59g0879wm... 0.36862578 B >

VOLUME OUT 0.39862578 B

FEES 0.00002488 B

TOTAL 0.39865066 B









#### (B) Transaction

5950c2bbf1adb1a5fbbc050d06918cdbb97d8e0855ec5cd24d57b61e076a2785



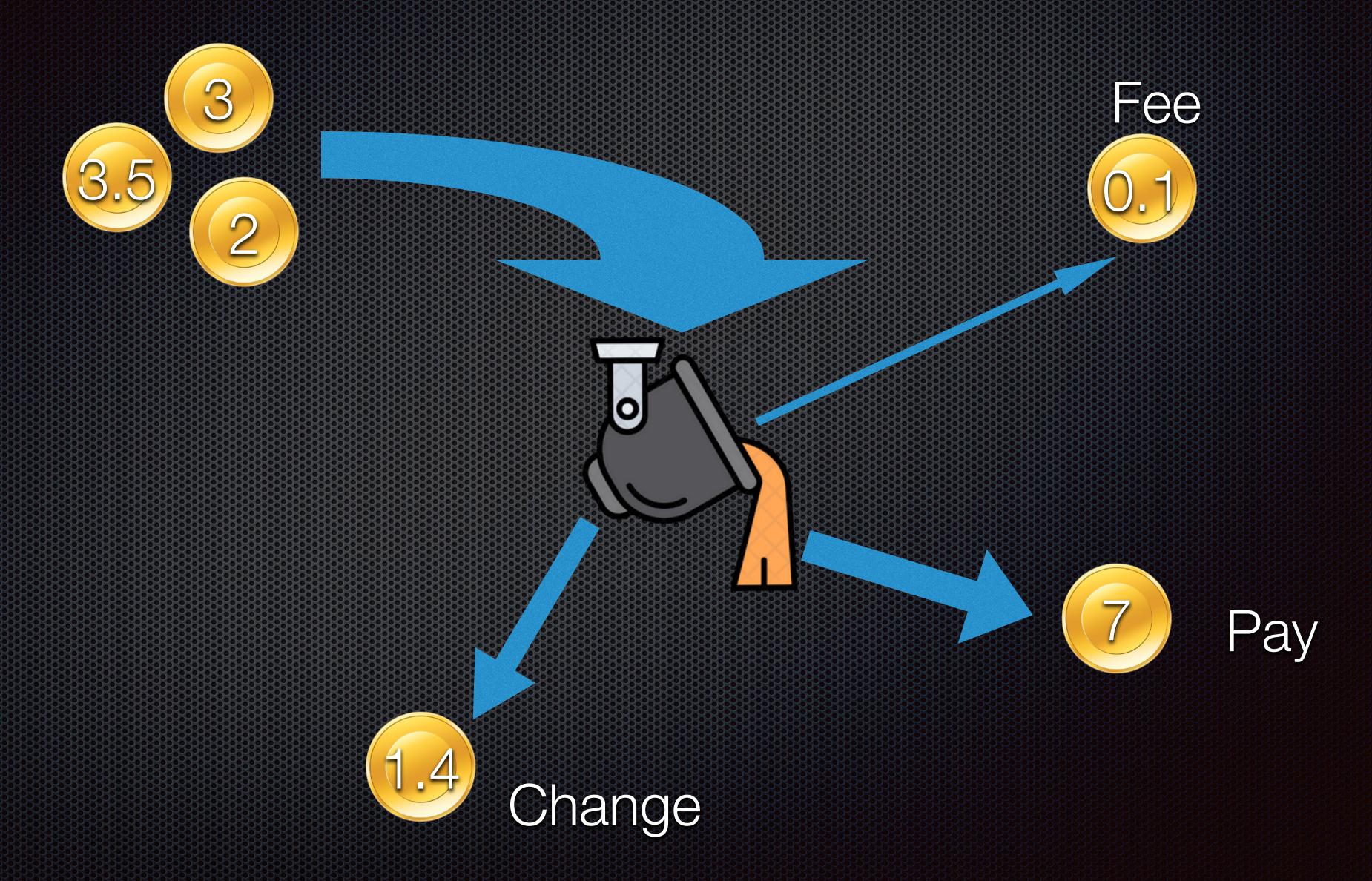
4 Confirmations	STATUS
K 000000000000000000000000000000000000	INCLUDED IN BLOCK
792960	BLOCK HEIGHT
2023-06-05 12:50:20 GMT +1	BLOCK TIMESTAMP
0.00002488 BTC (16.2 sat/vB)	TRANSACTION FEES
205 B	SIZE
154 vB	VIRTUAL SIZE
616 WU	WEIGHT UNITS
2	VERSION
0	LOCK TIME
Address reuse ₹ Round payment amount ₹	PRIVACY ANALYSIS





## Transactions/payments

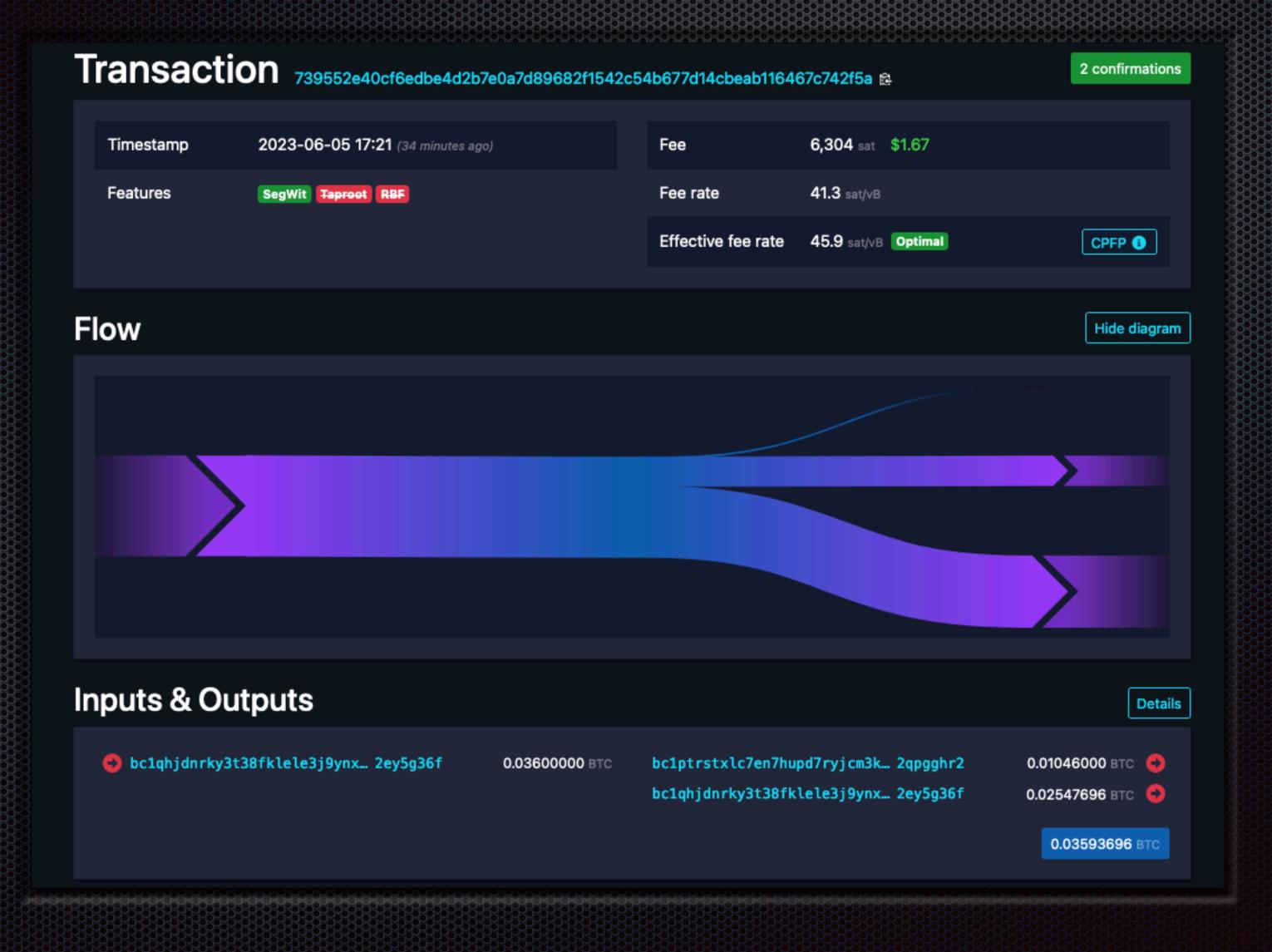






## Standard payment

One input - two outputs (payment and change)





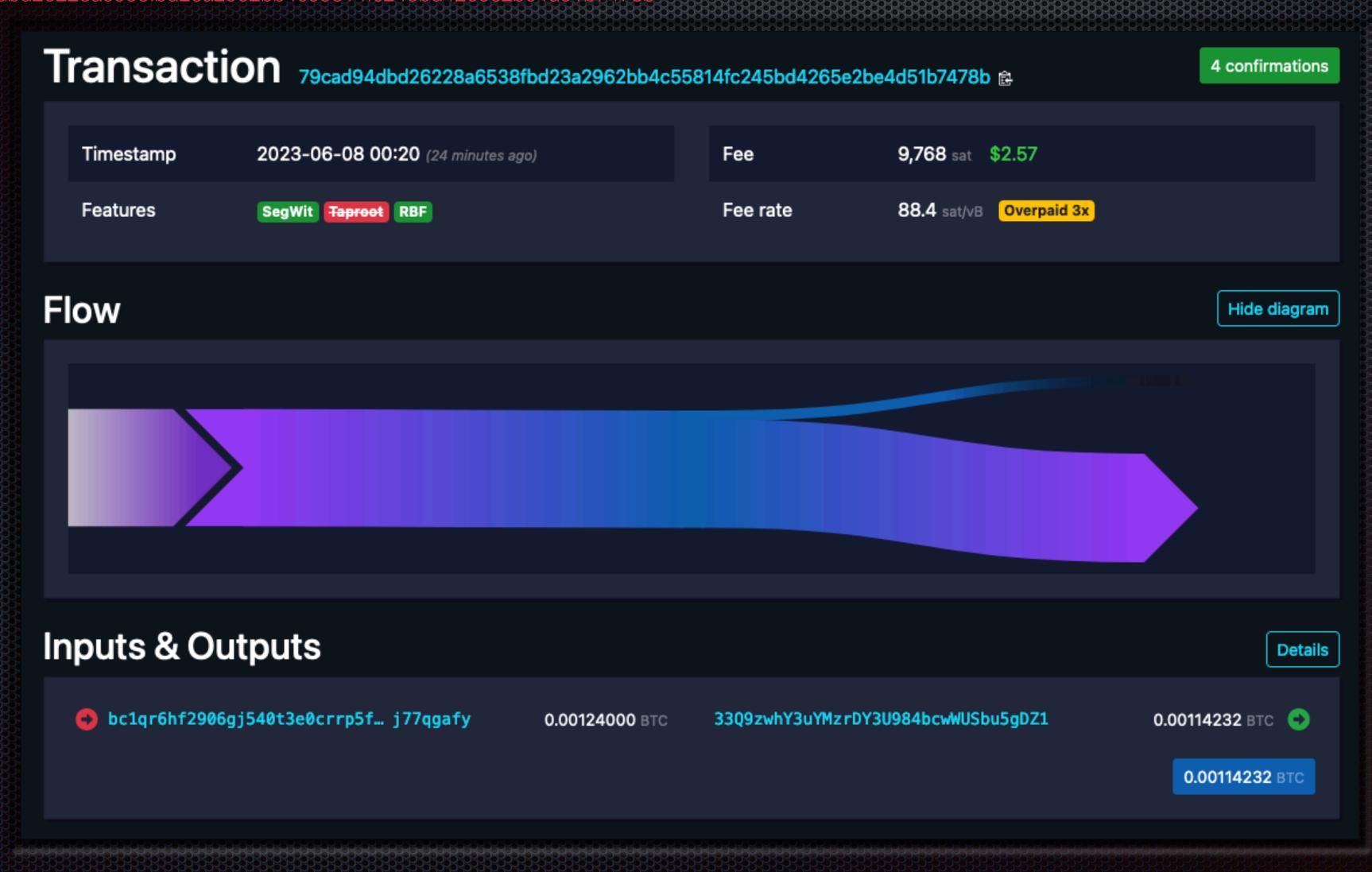


## Sweep payment



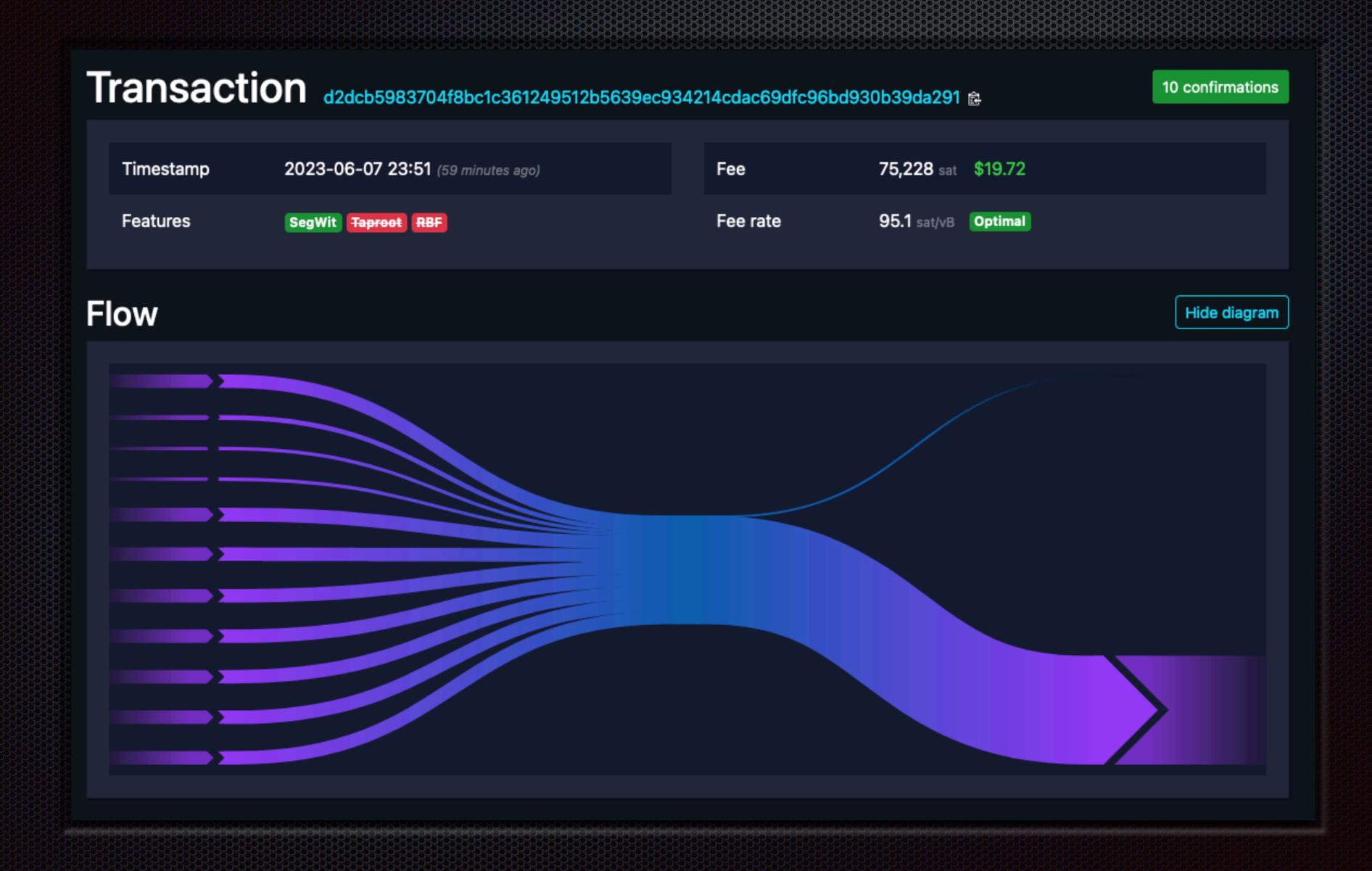
Self transfer. One input - One output

79cad94dbd26228a6538fbd23a2962bb4c55814fc245bd4265e2be4d51b7478b



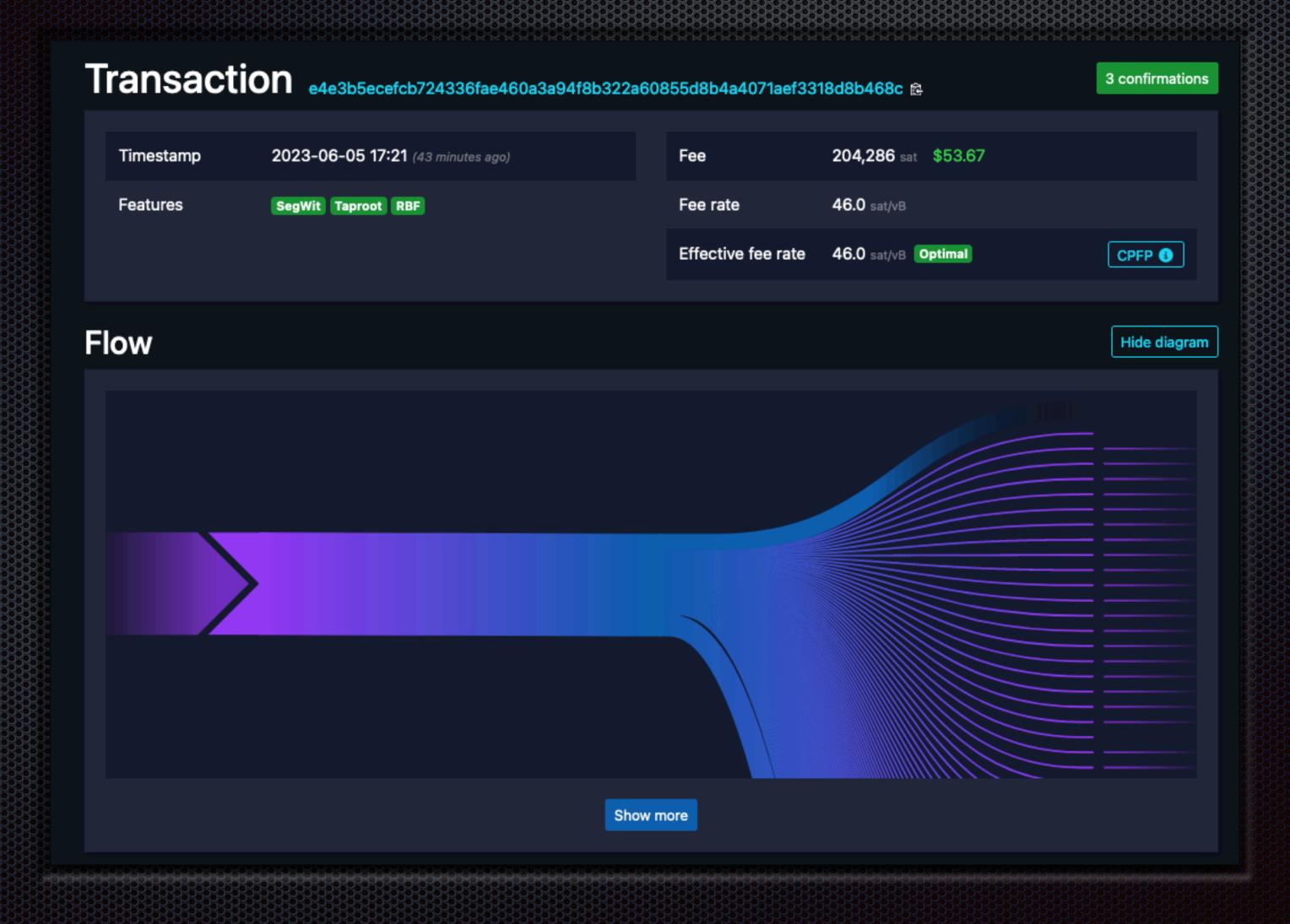












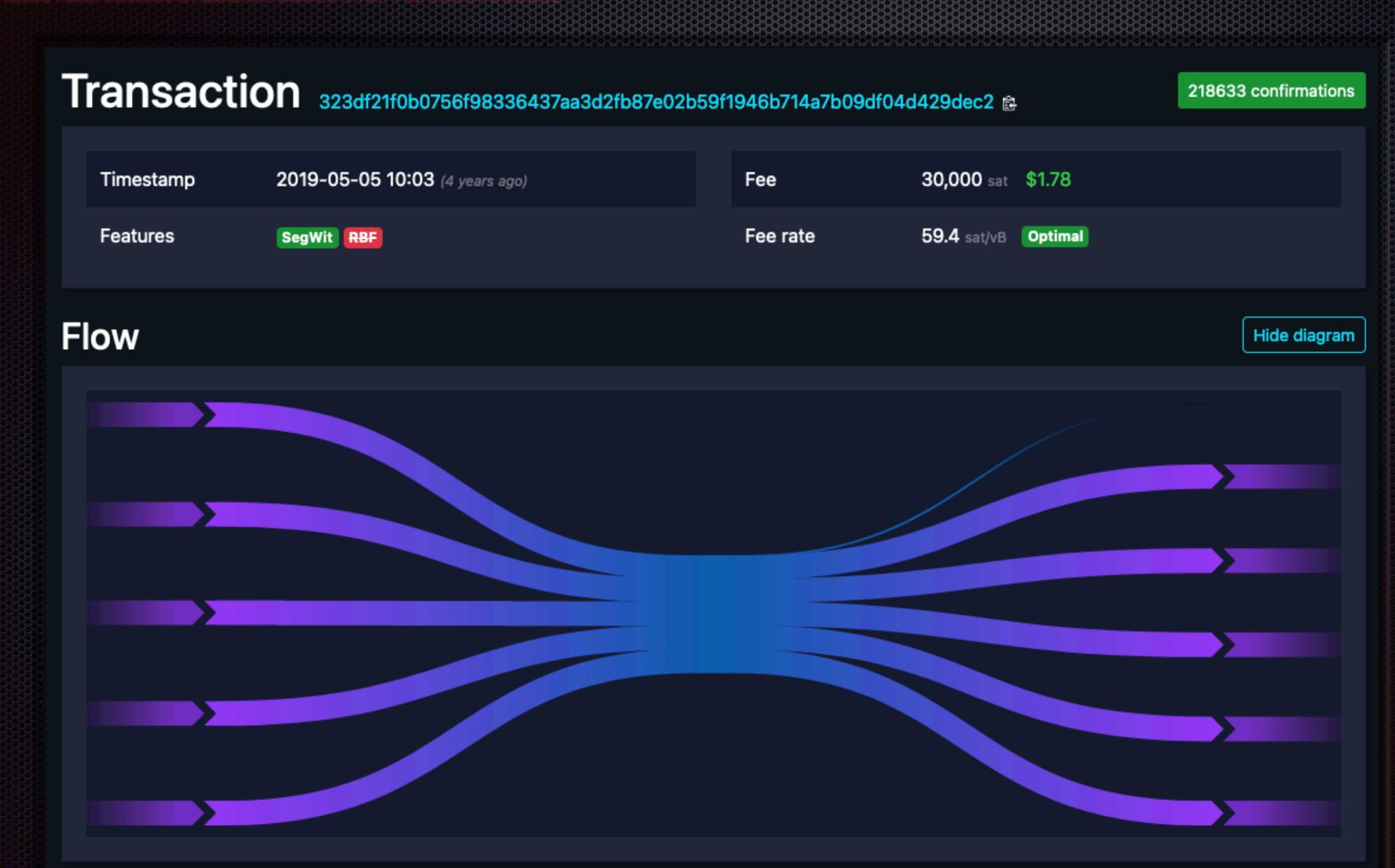
### [XTX]

## Coinjoin



Several inputs and outputs. Few partners.

323df21f0b0756f98336437aa3d2fb87e02b59f1946b714a7b09df04d429dec2







## REDE: Loy Fee



#### [XTX]



**Replace-by-fee** allows the sender to replace this transaction with another similar transaction which pays a higher fee.

RBF only works while the transaction is in the mempool and soon as a transaction enters a block, it cannot be replaced by fee.

The original transaction that was first sent, it must specify that it is available to be replaced by fee in the future.

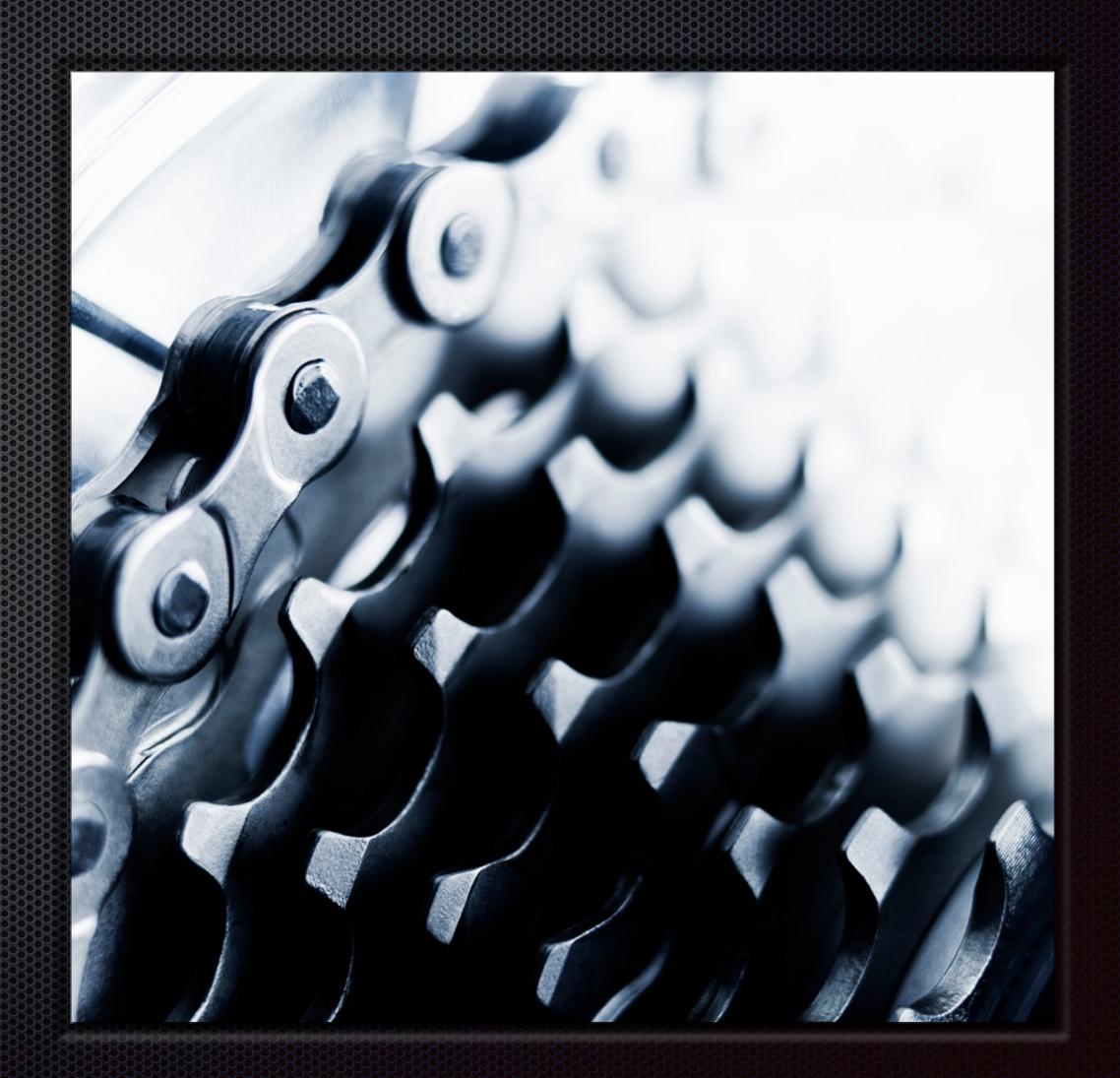
You can also replace the entire transaction, there is the option to reverse a transaction within a short period.





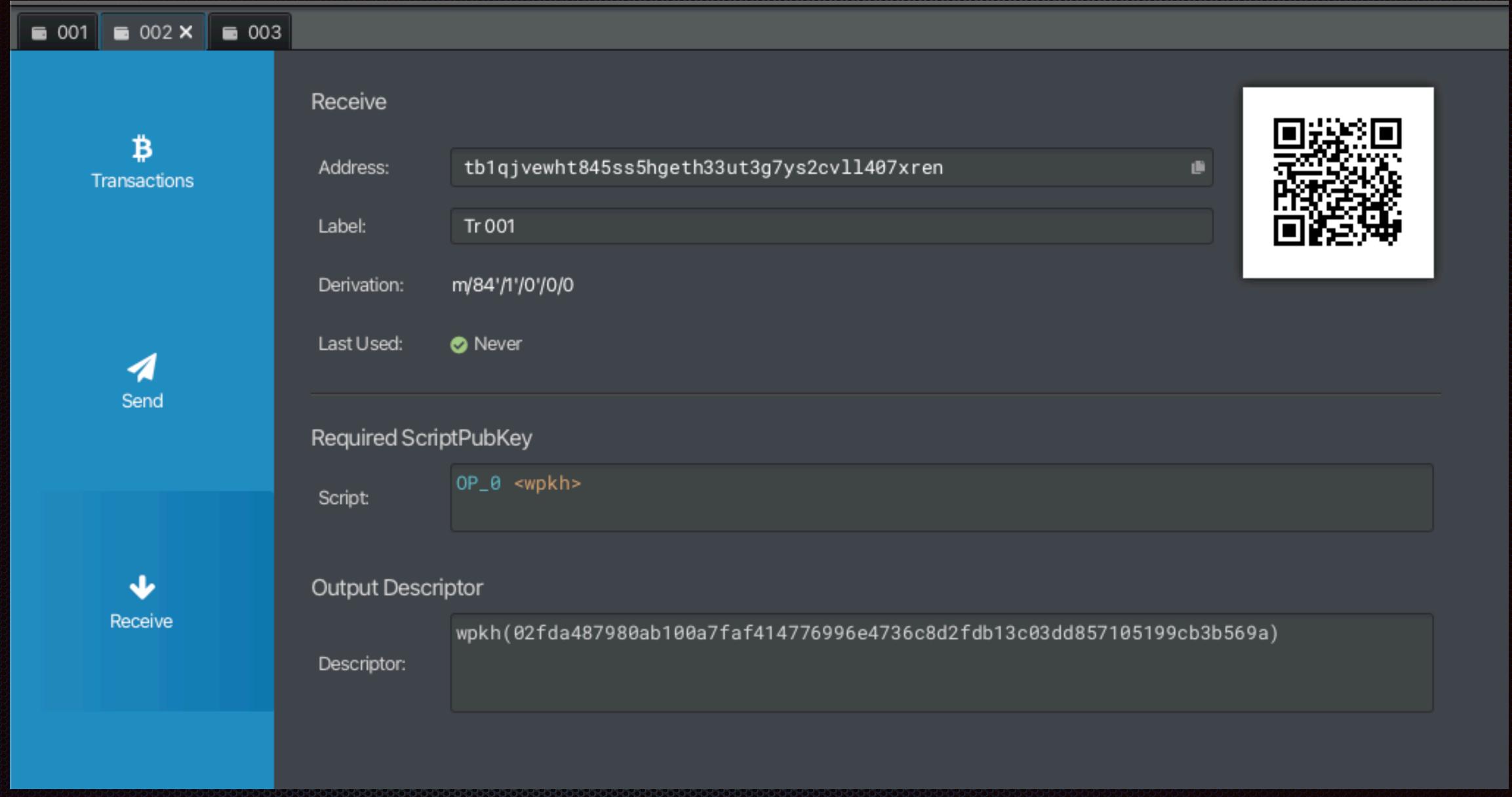
## RPF in Sparrow

- Be in the mempool (not yet confirmed)
- Have all inputs enabled for RBF (this is the default for transactions sent by Sparrow)
- Have all inputs from your wallet



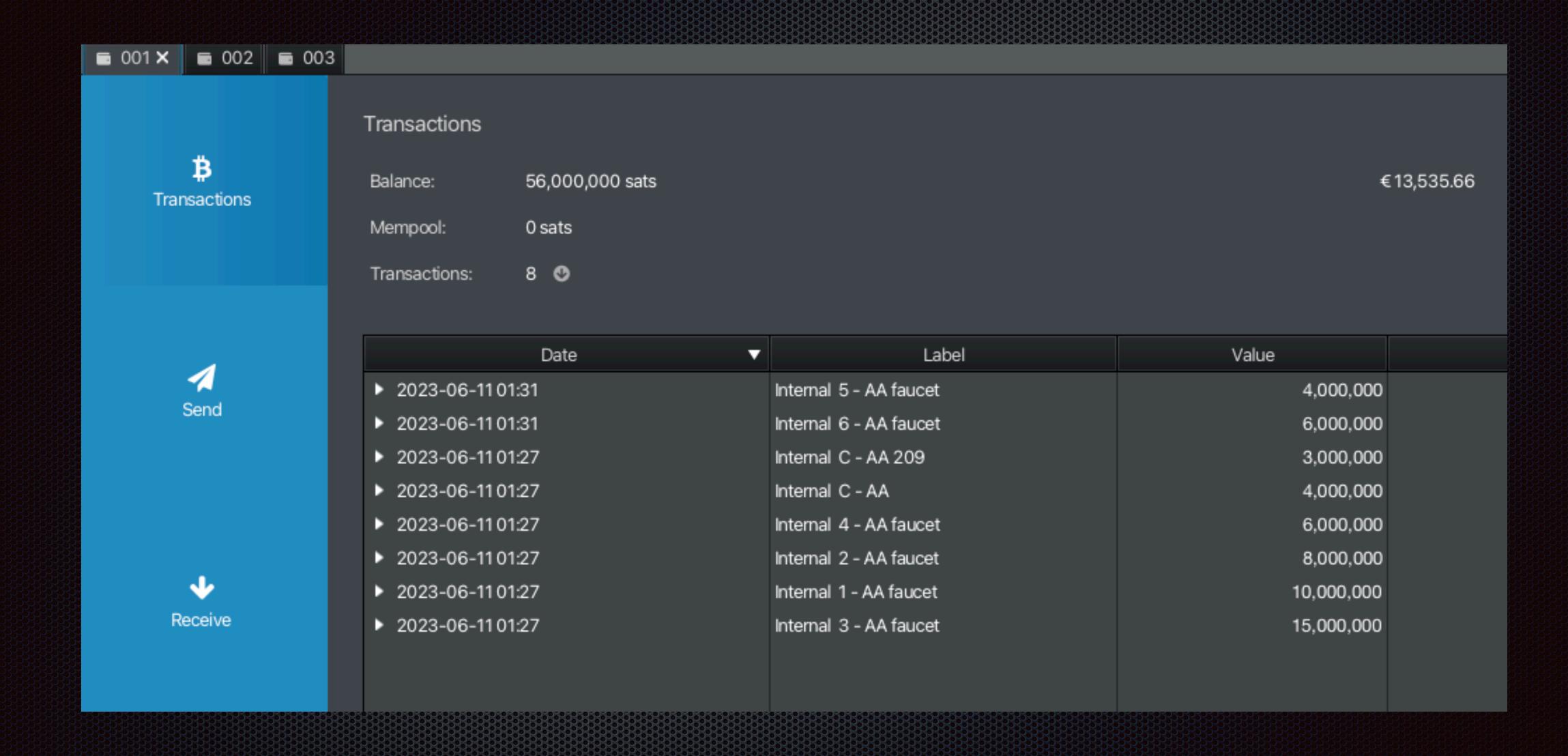






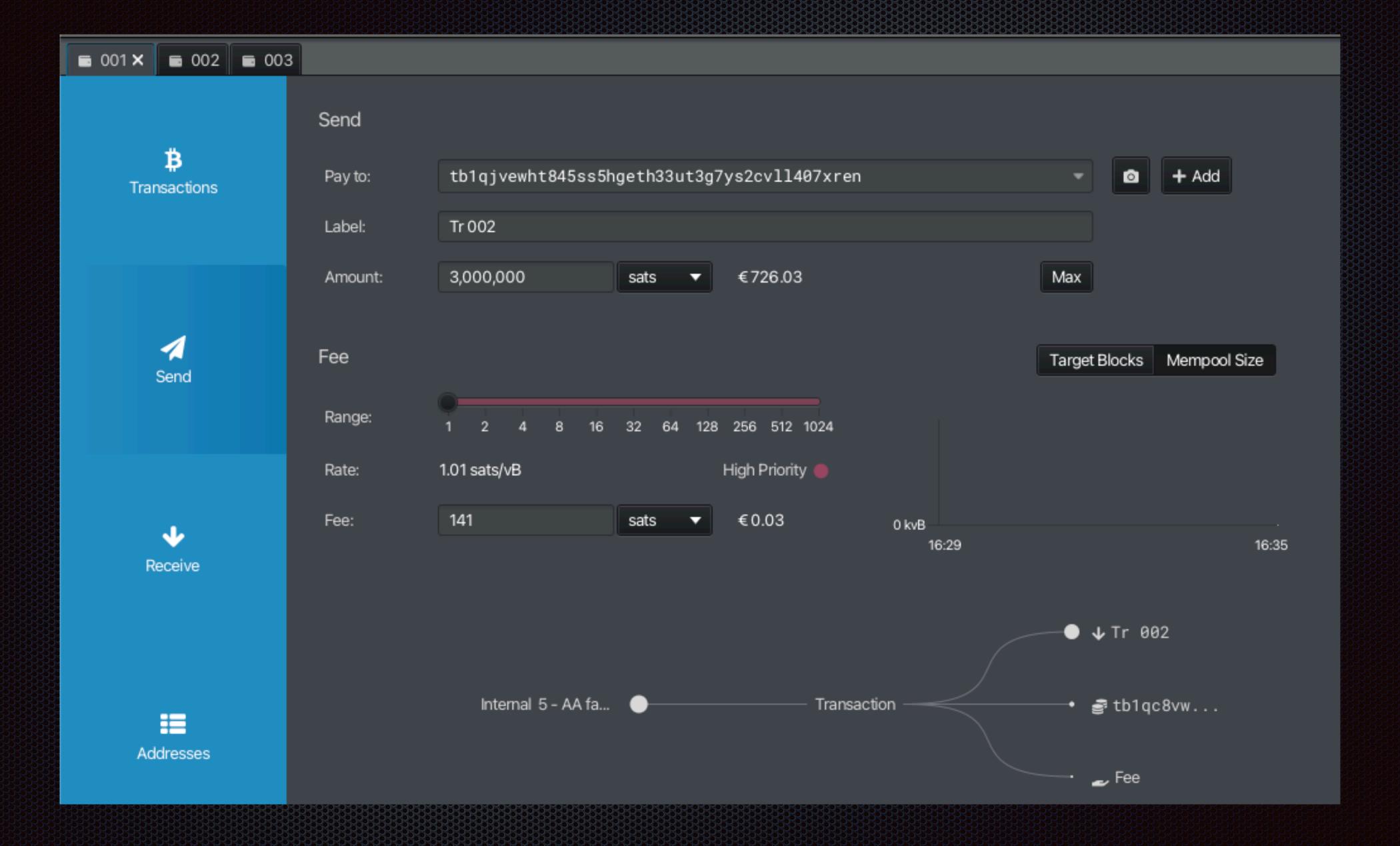






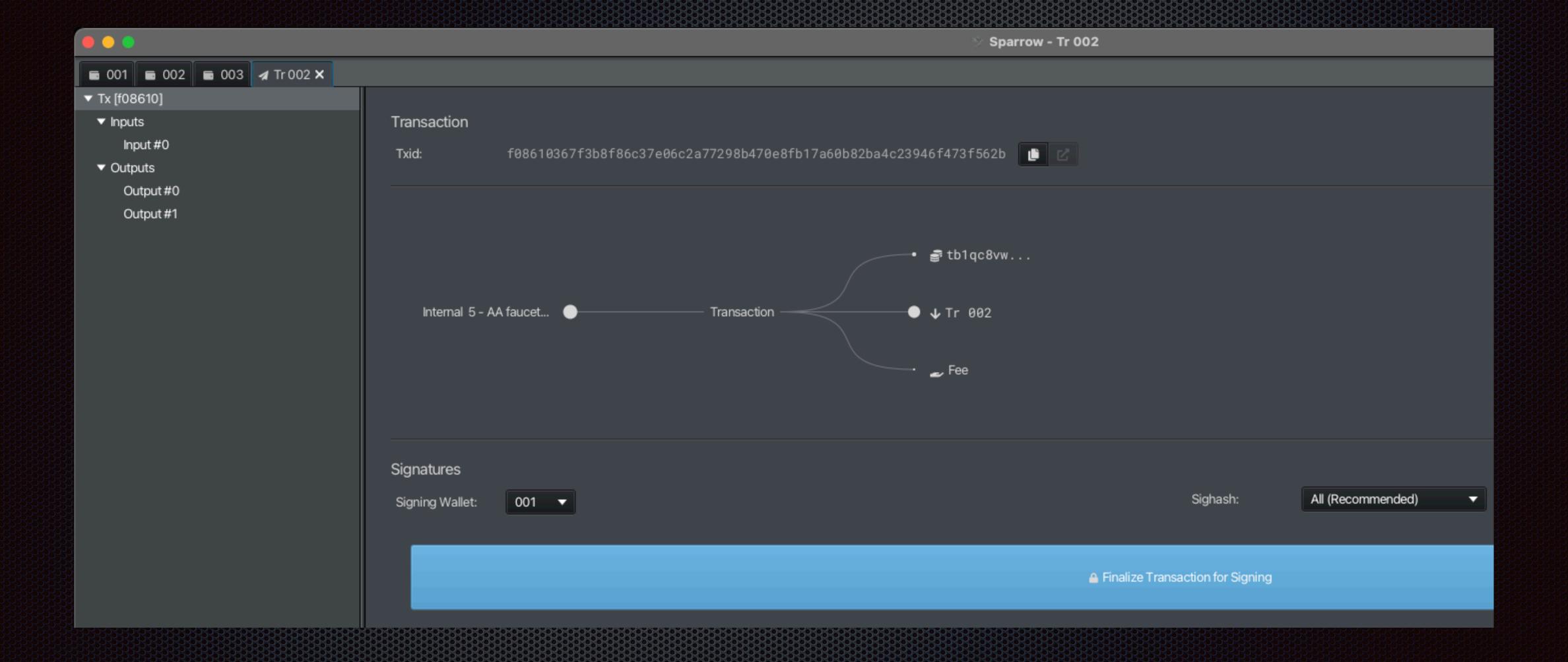












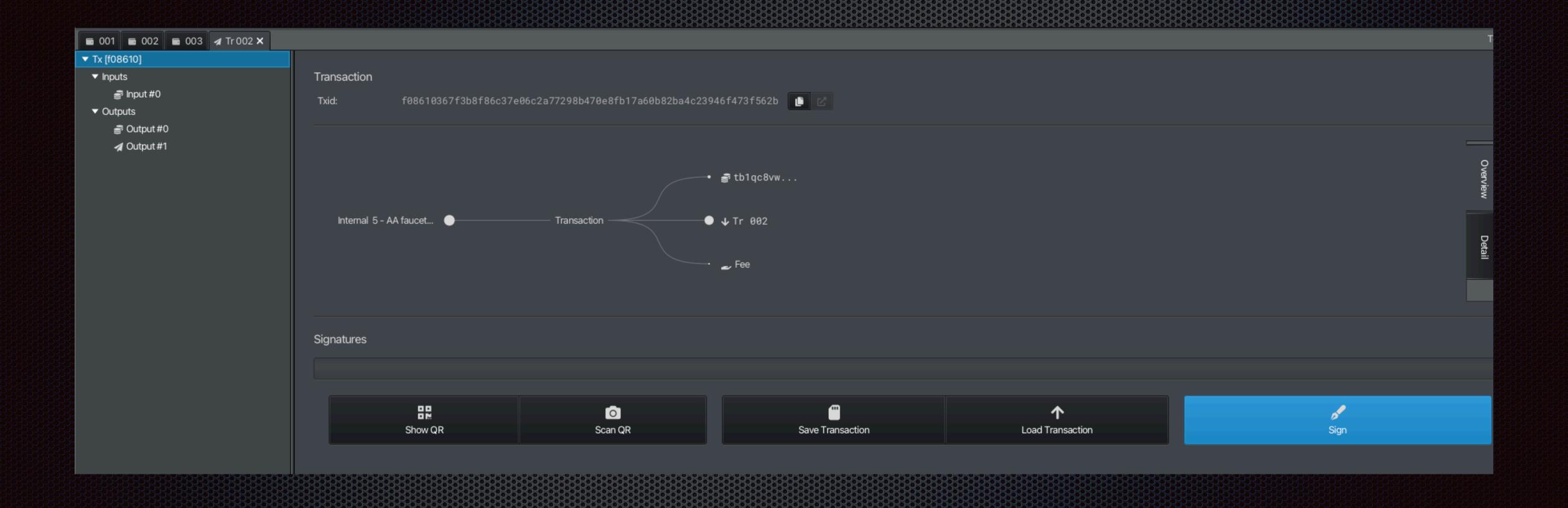




■ 001 ■ 002 ■ 003 🖈 Tr 002 🗙						
▼ Tx [f08610]						
▼ Inputs	Input #0					
Input #0	Outpoint:	d38db8473242da020fdac5b058a423ba2ad84116456c493bd489db09f7bbd551:1				
▼ Outputs	Spends:	4,000,000 sats from tb1qx7w9gd88qg32pf38p897qptrj8dn7smr5hvst7				
Output #0	Sperius.	4,000,000 sats iloiti turqx/wagaooqgazpraopoa/qptraoui/siiiraiivat/				
Output #1						
	Script					
	ScriptSig:					
	RedeemScript:					
	Witnesses:					
	WitnessScript:					
	Status		Locktime (nSequence)			
	Signatures:	0/1	Туре:	Disabled	Absolute	Relative
	RBF:		Block:	2438057		
52525252525252525252525252525252525252				Sporovorovorov	RSPSRSRS	

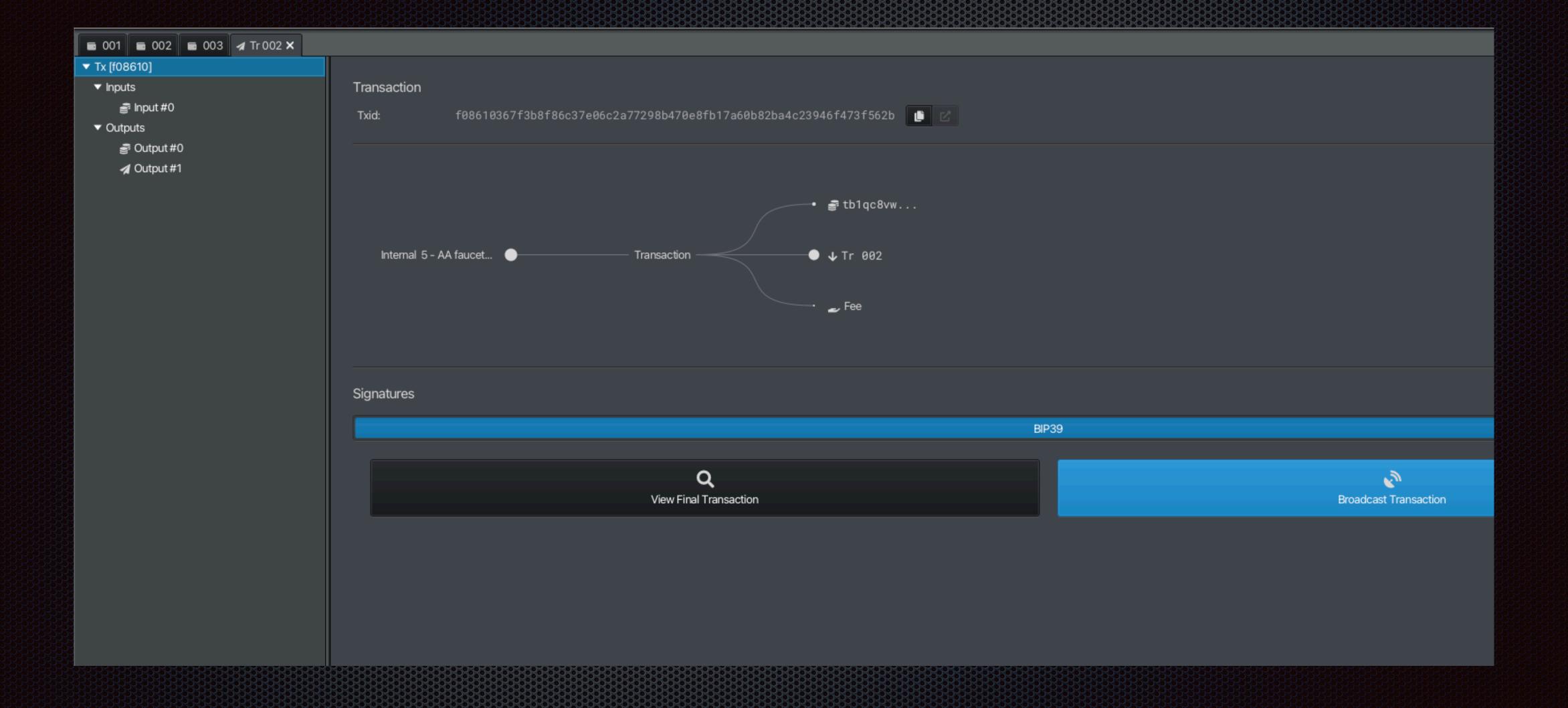






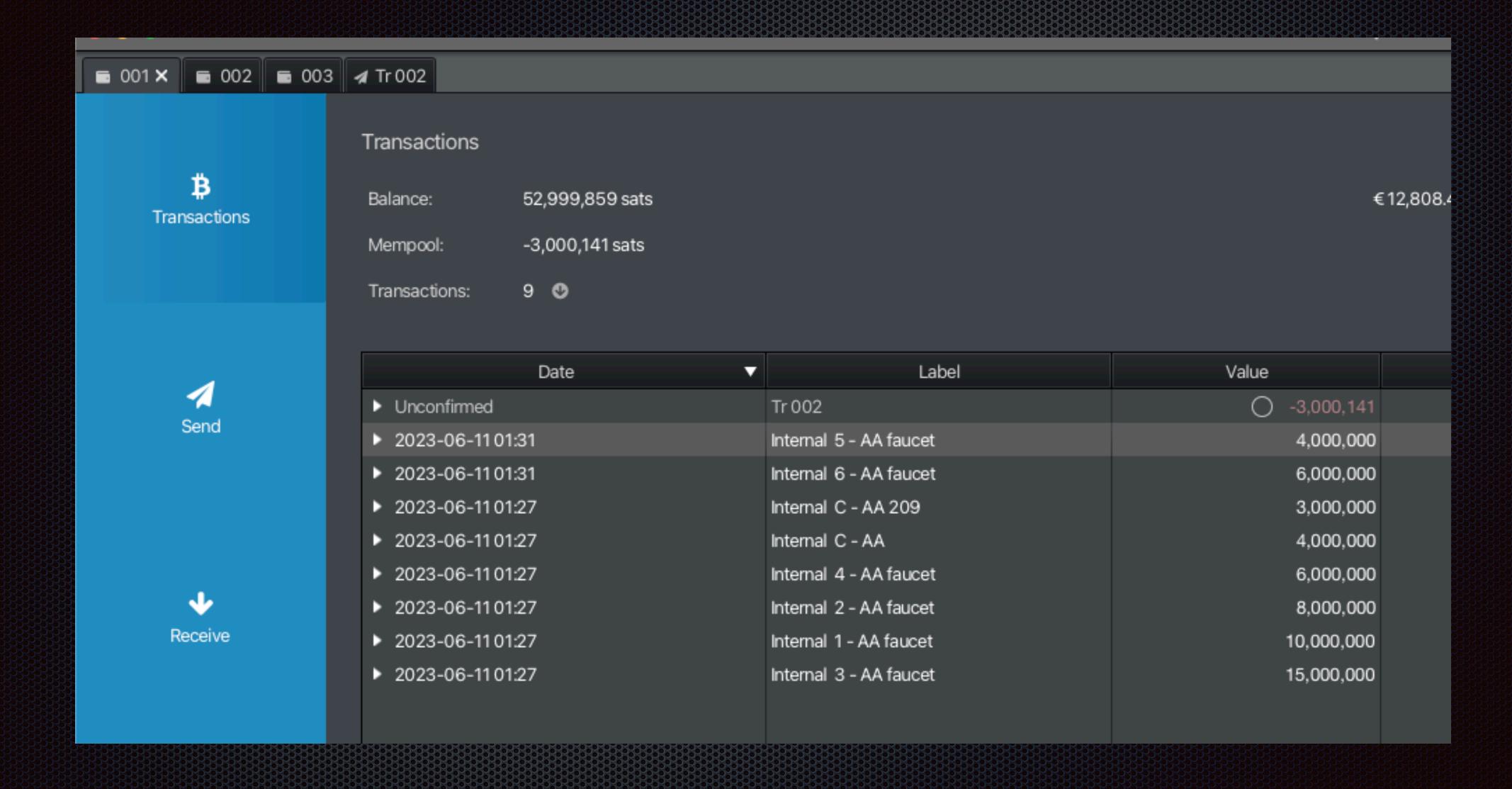






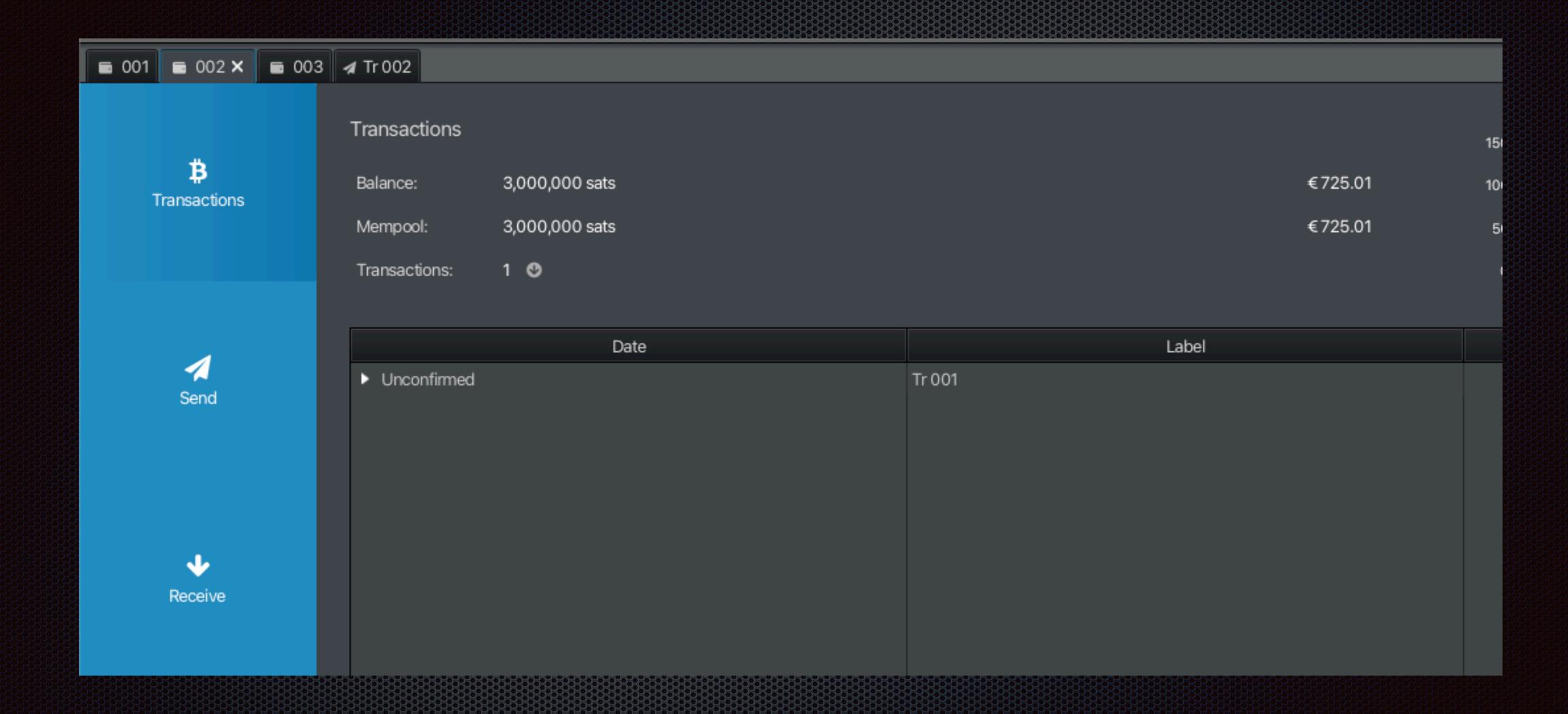






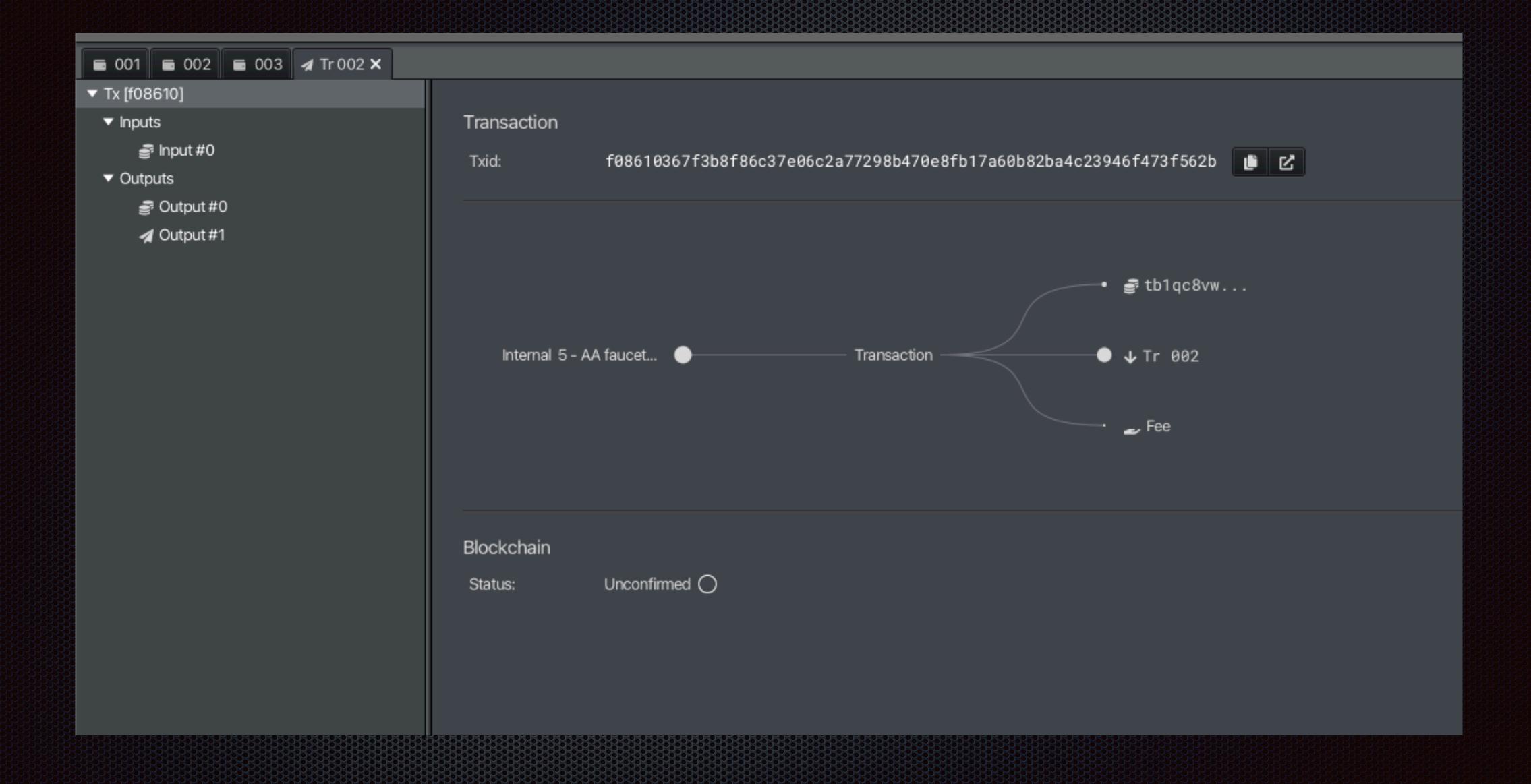




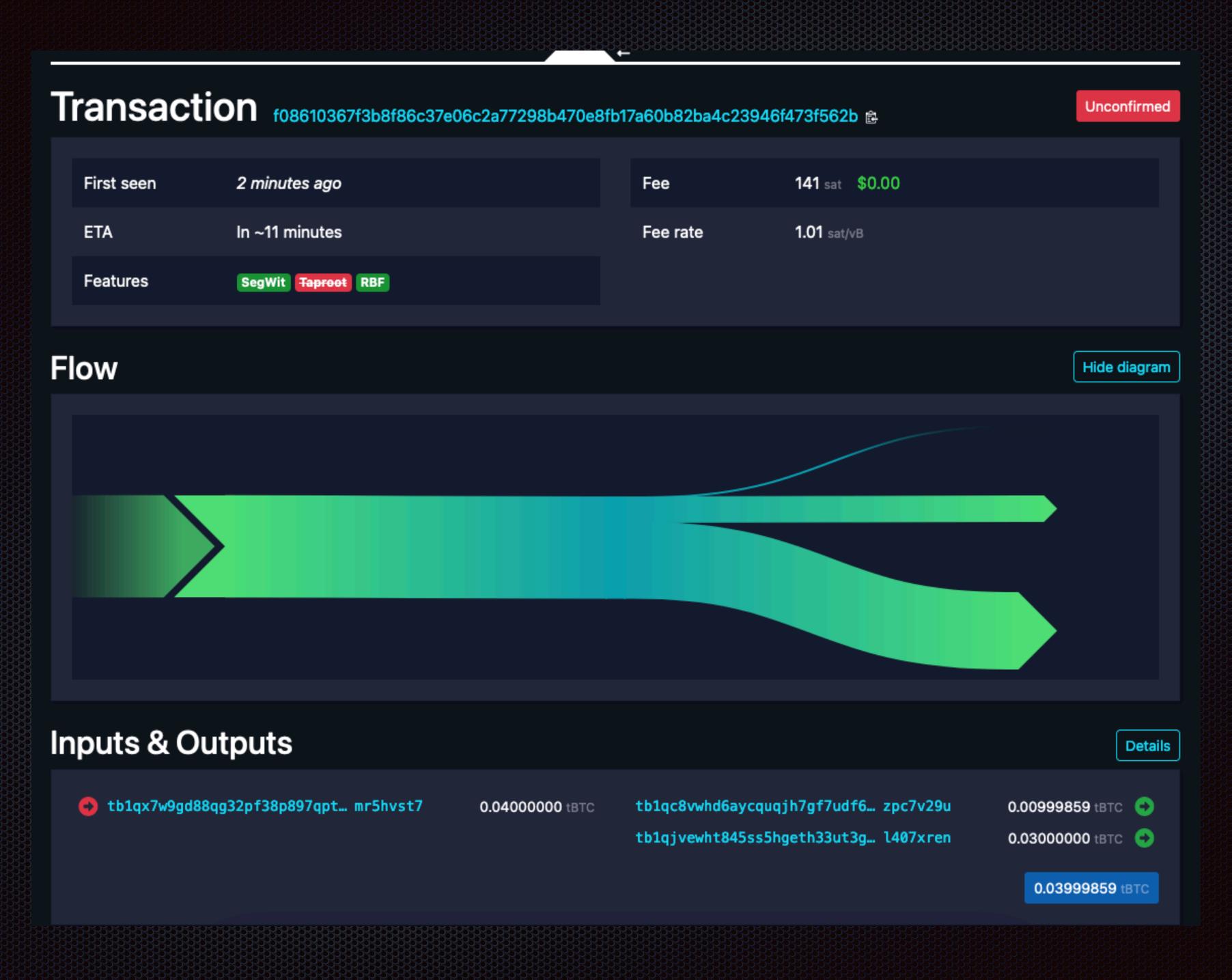








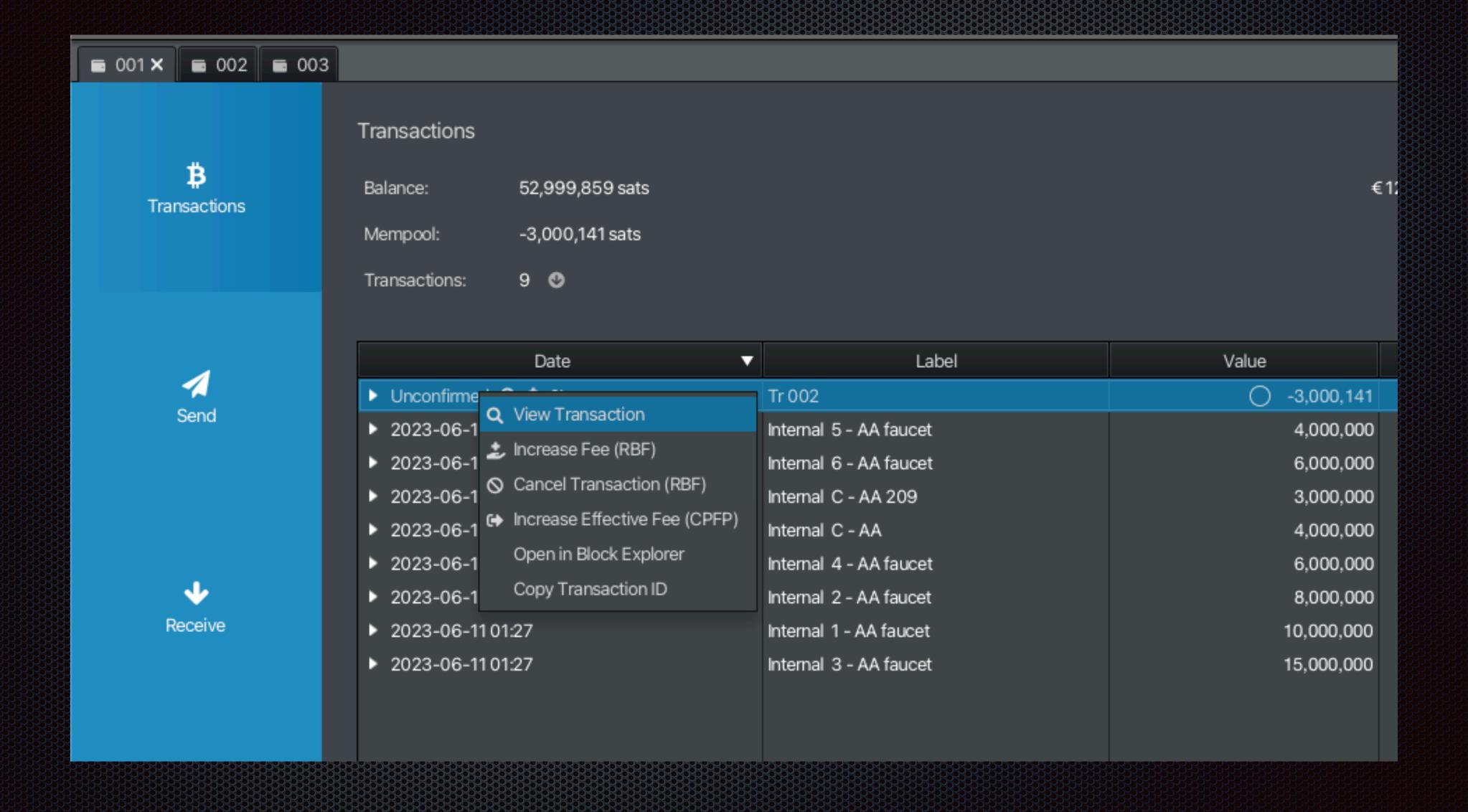






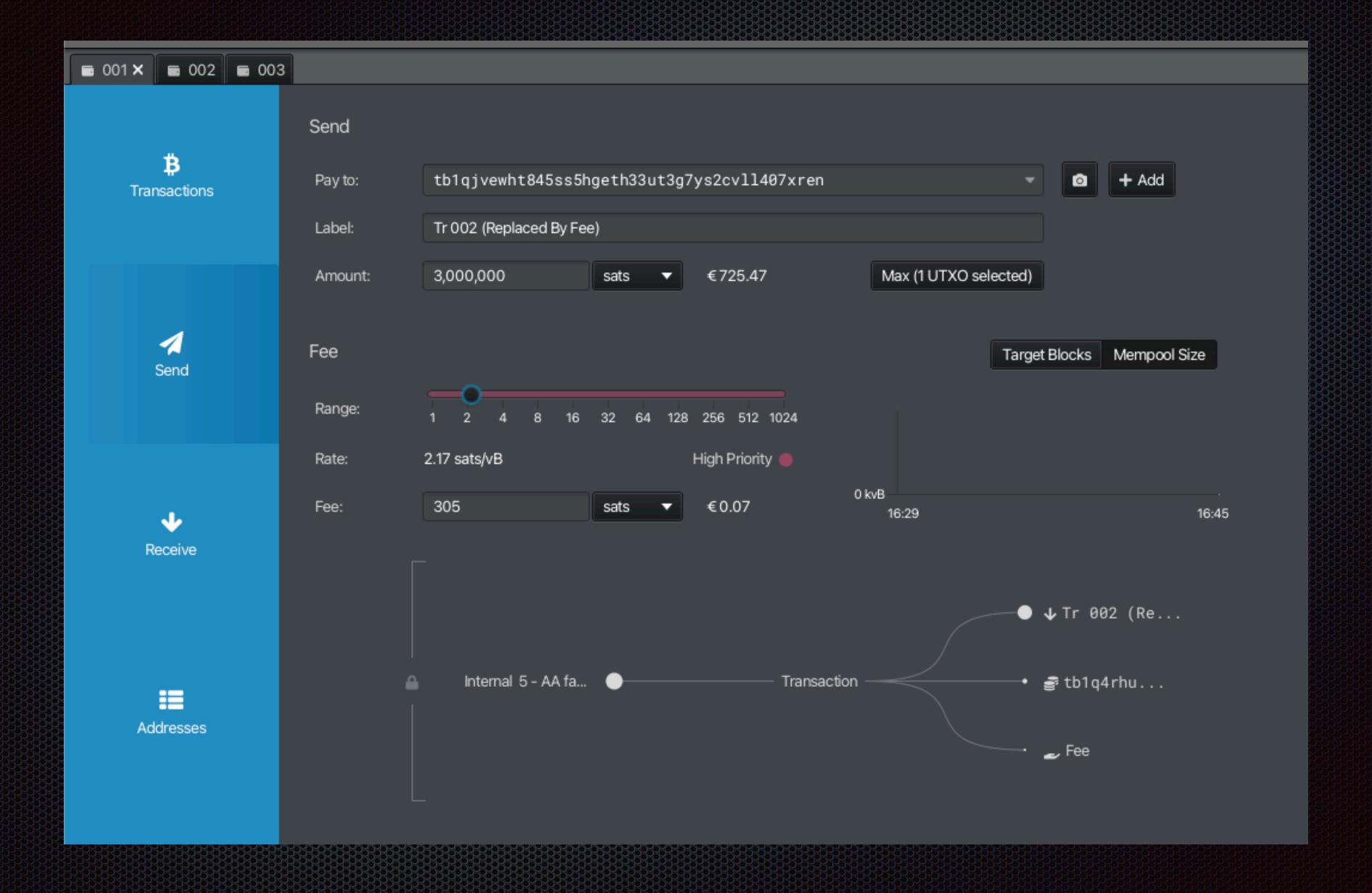






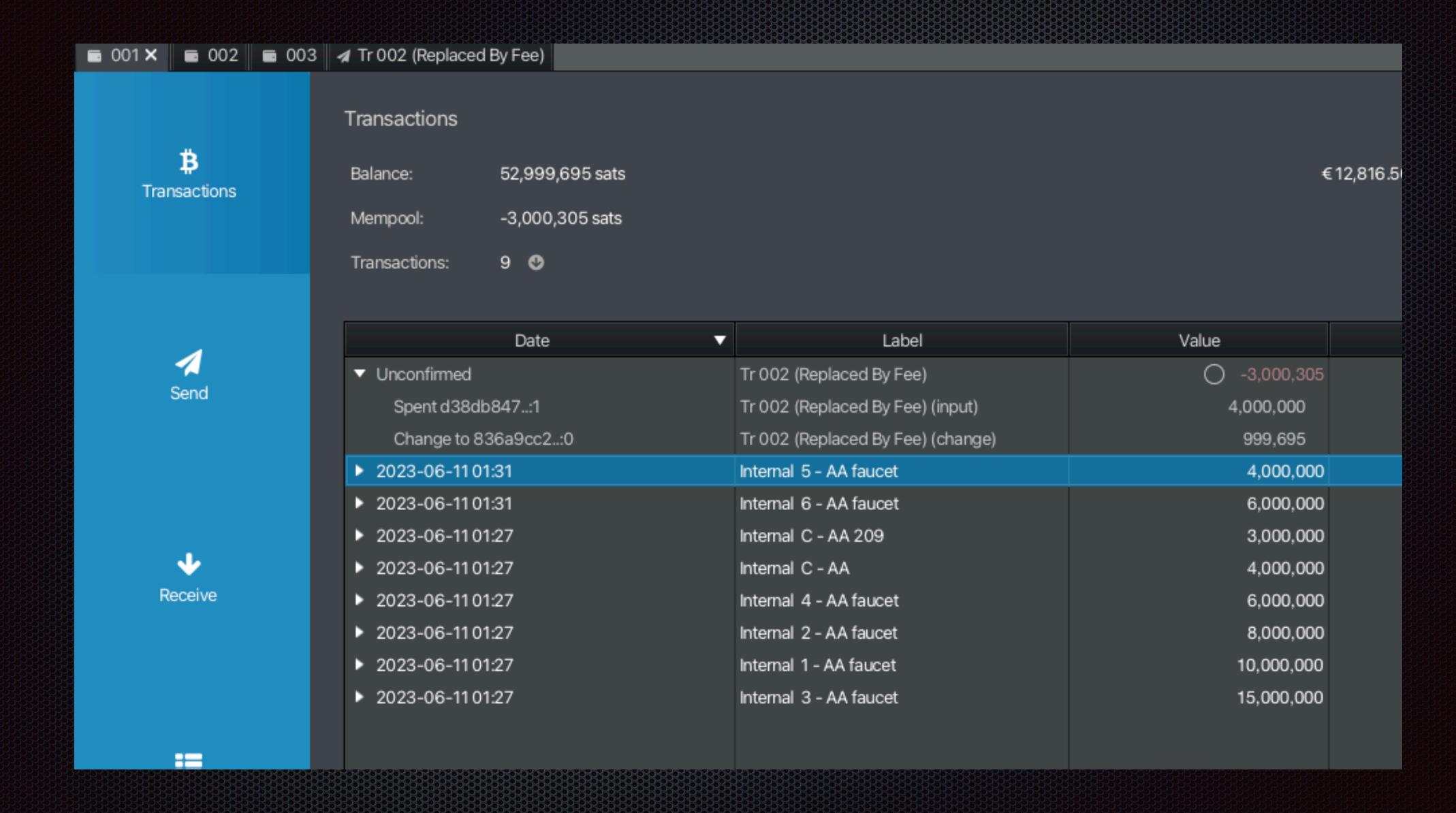




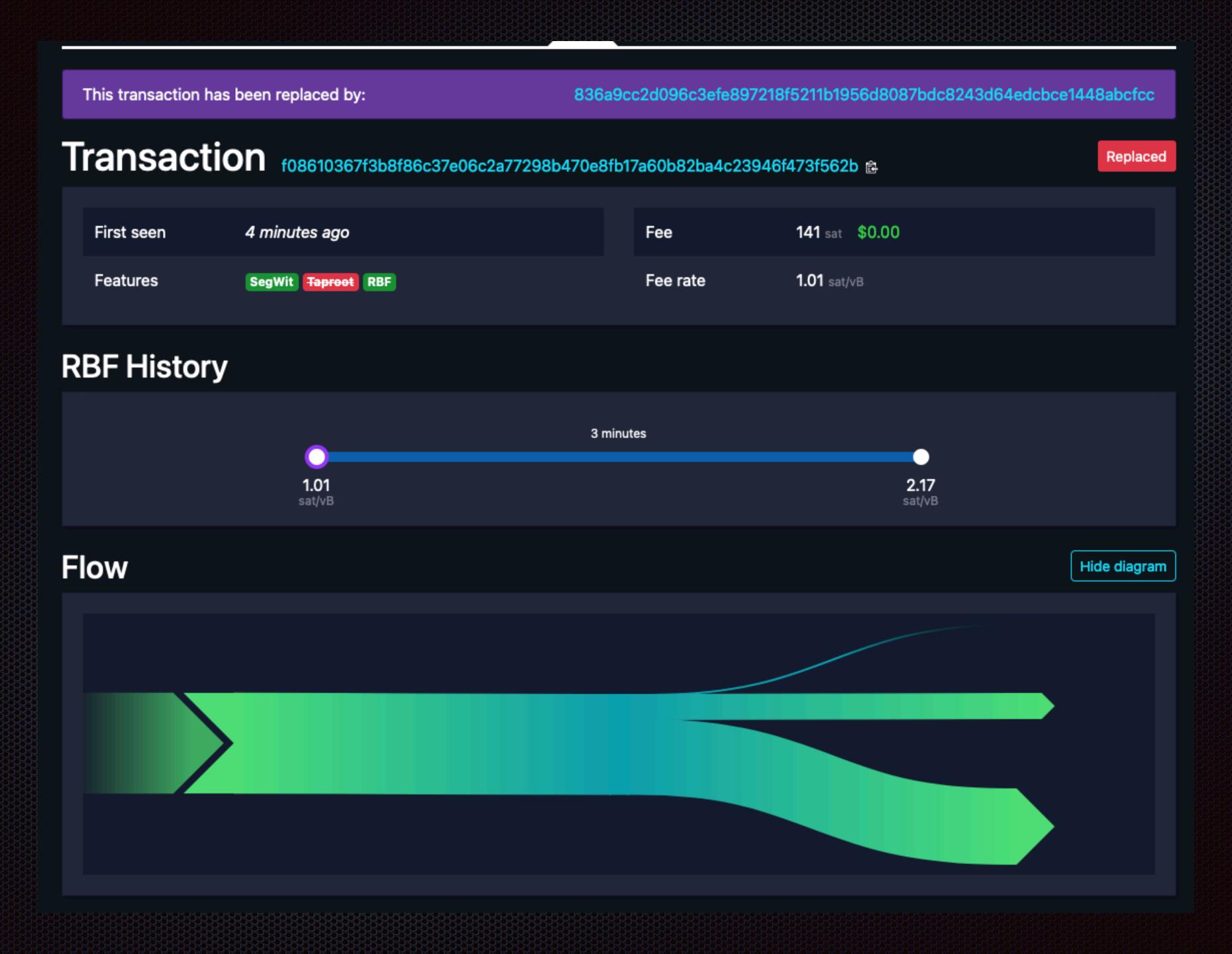








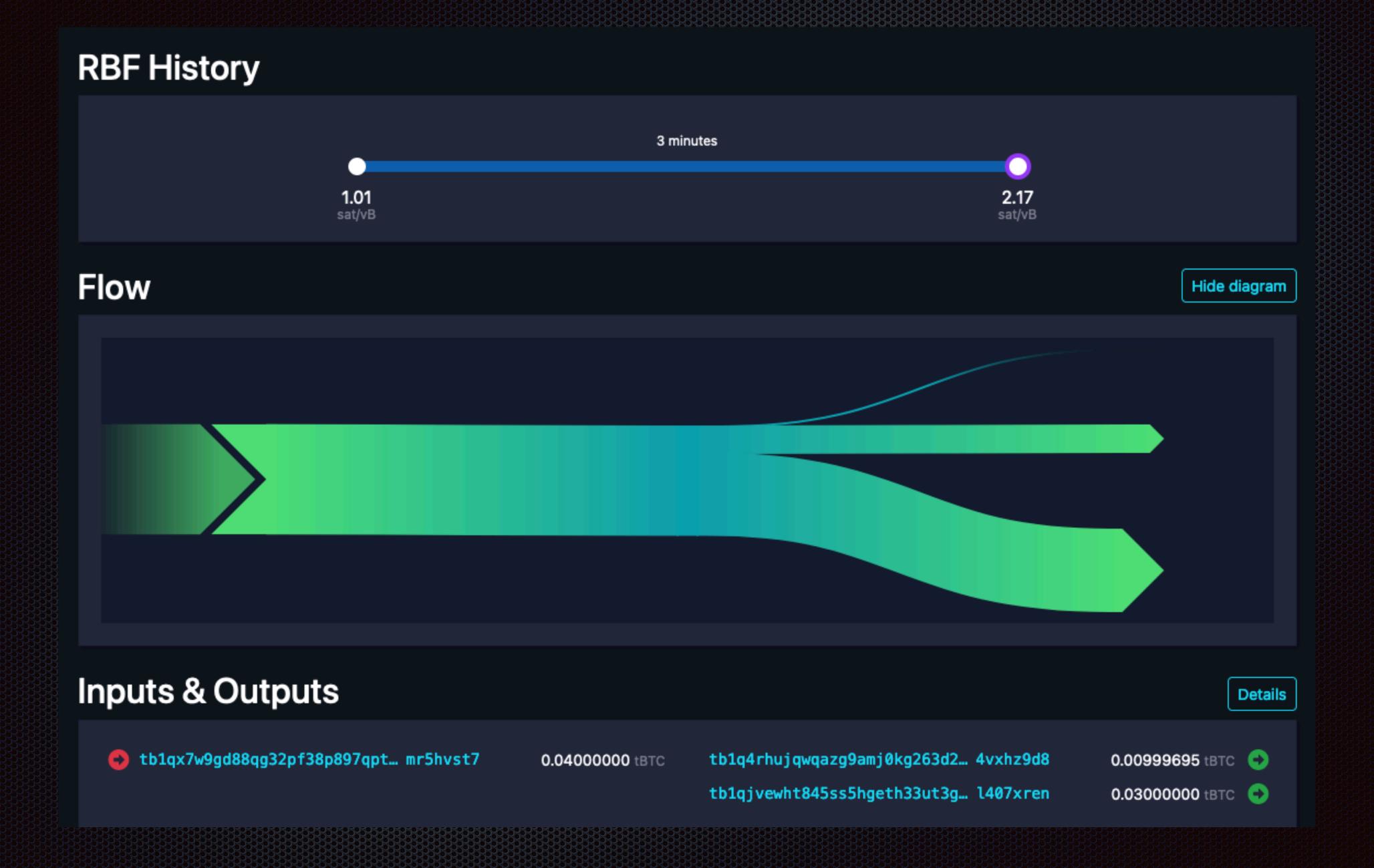
















CPFP:
Child Pays For Parent



#### IXTX



Child Pays for Parent: you're creating a new transaction (Child) using the funds of the delayed one (parent) and then resending it with a much higher fee.

It will cause miners to consider confirming the parent transaction, it is rational for miners to implement it (they make more money).

It is not a change in the protocol, but in miner strategy.





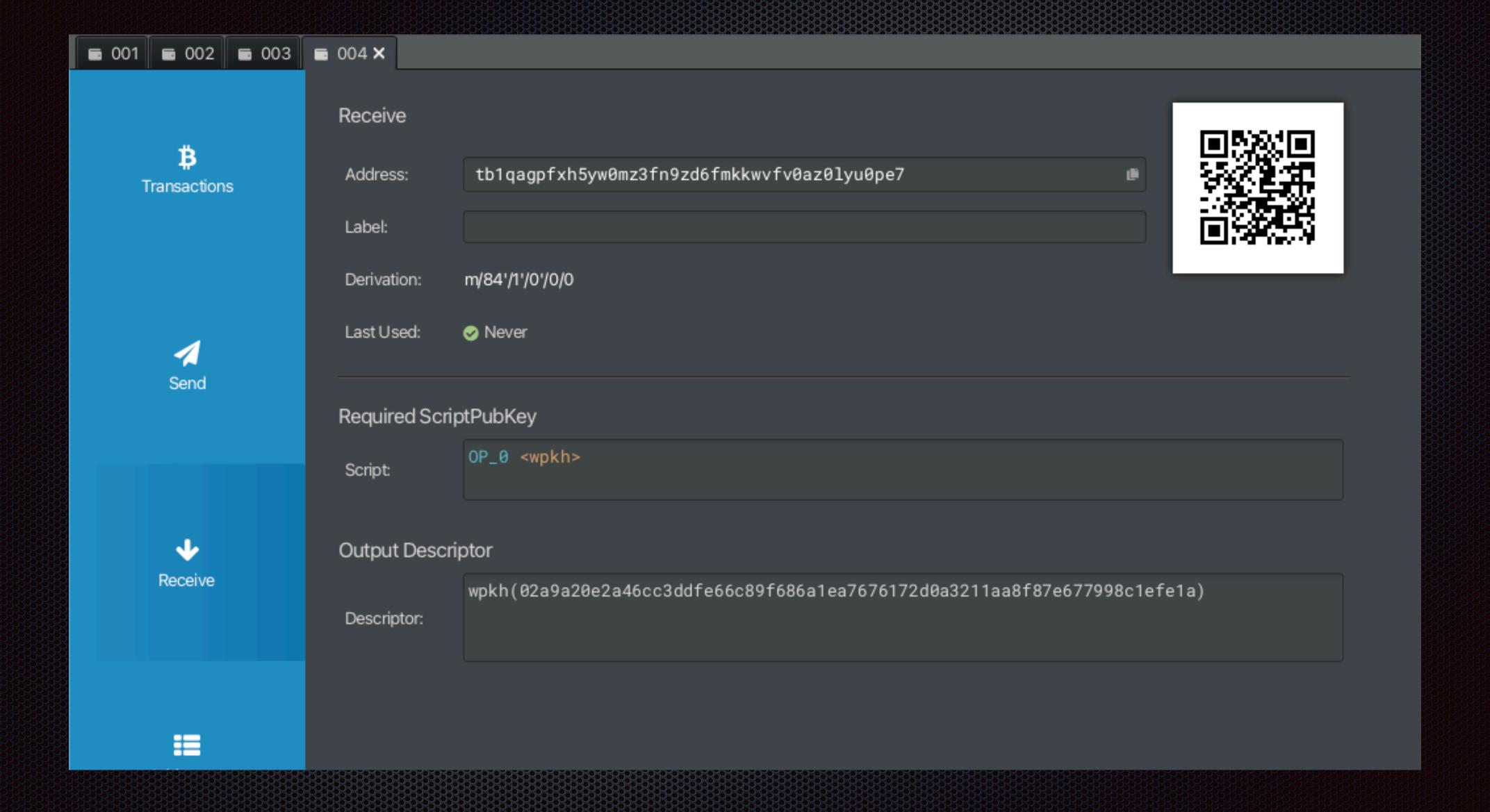
## CPP in Sparrow

- Be in the mempool (not yet confirmed)
- Have rights over the outputs.



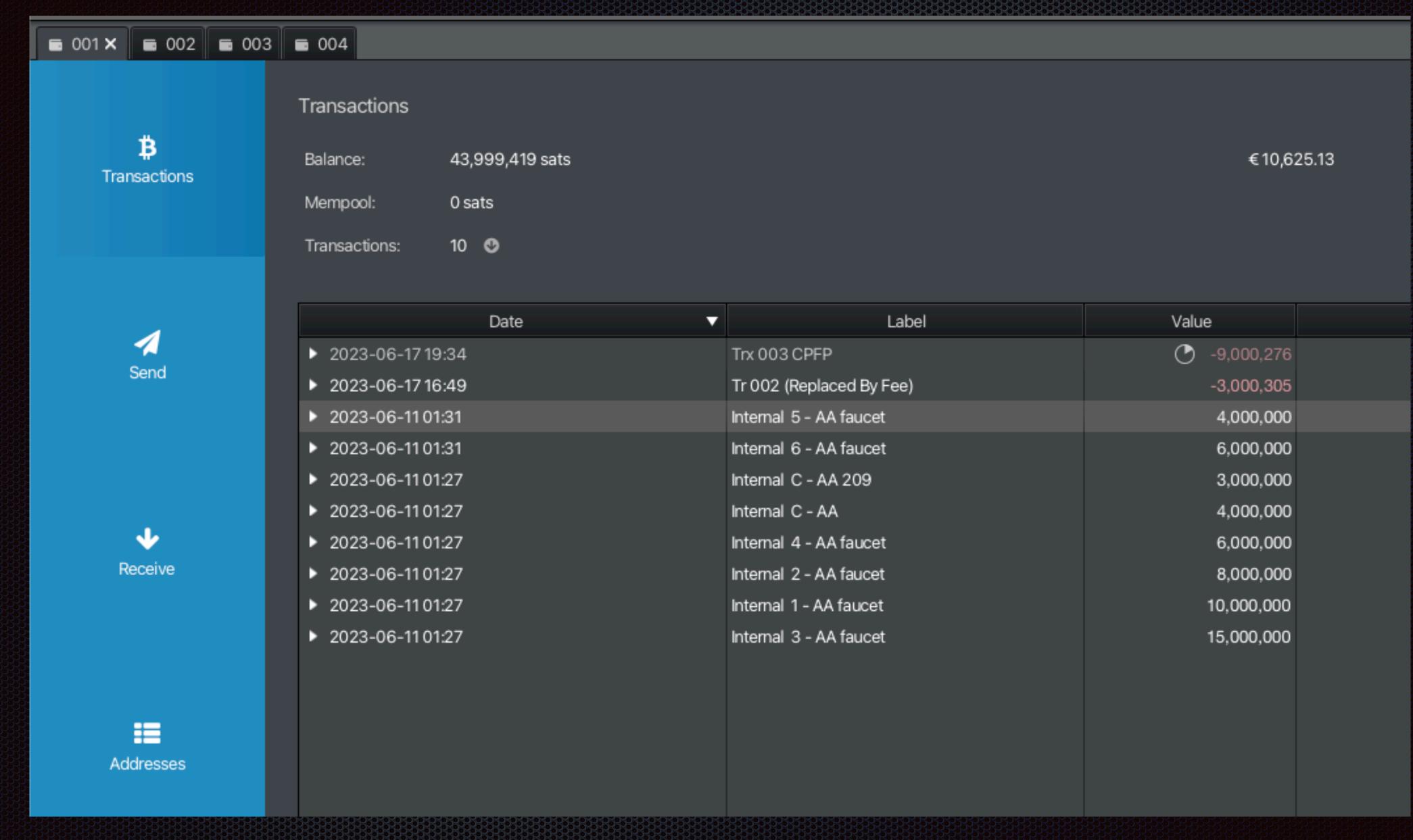




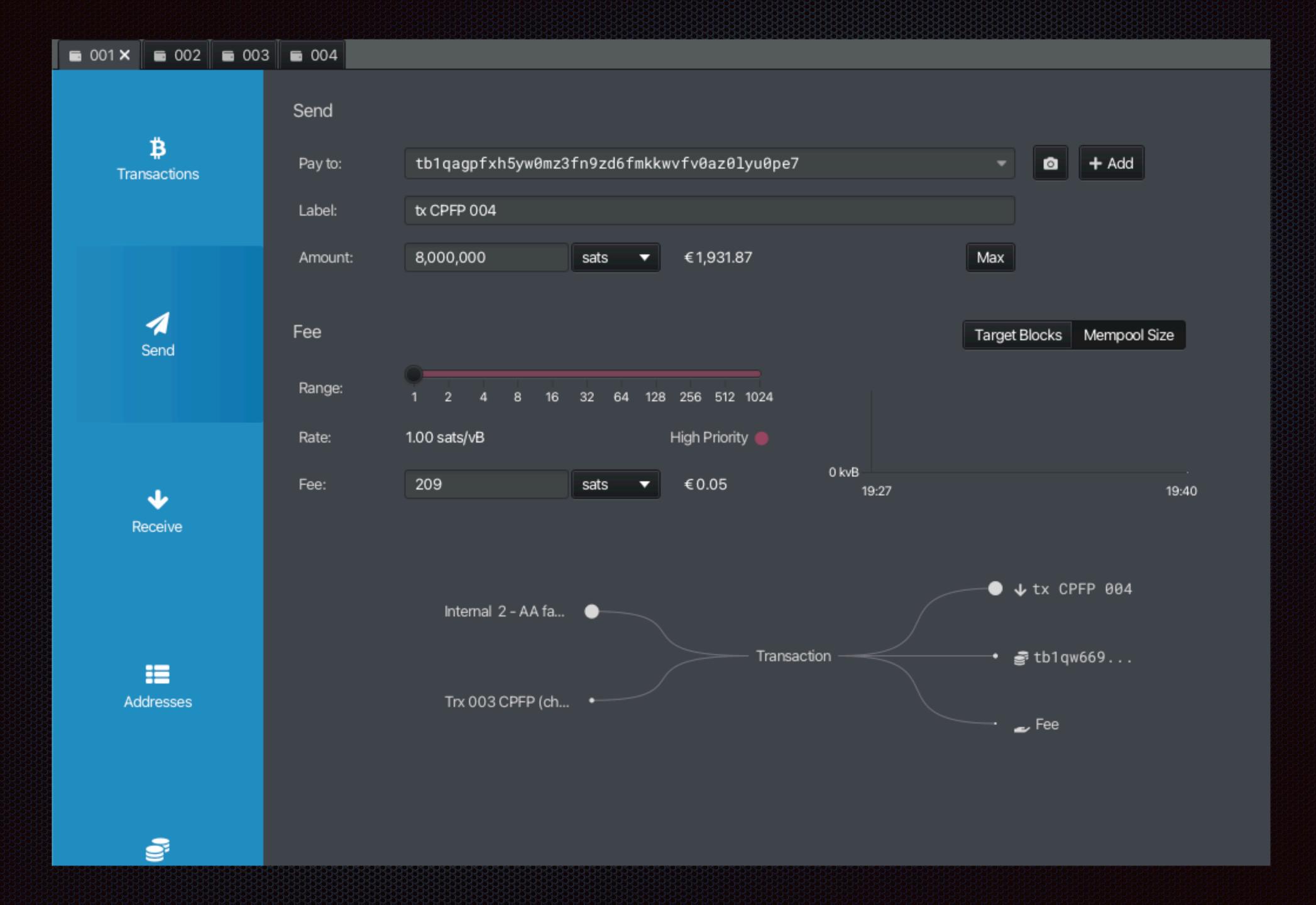






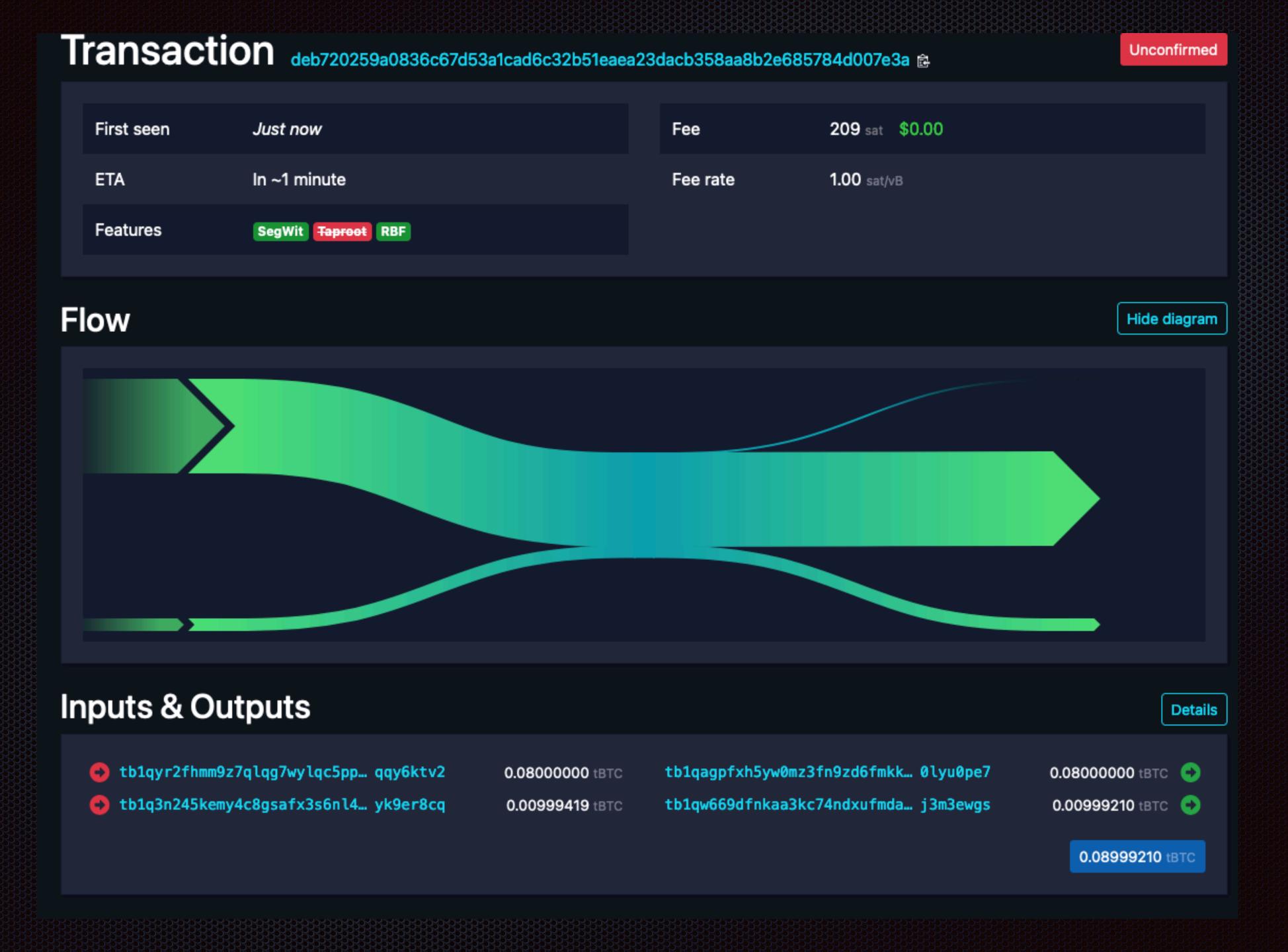








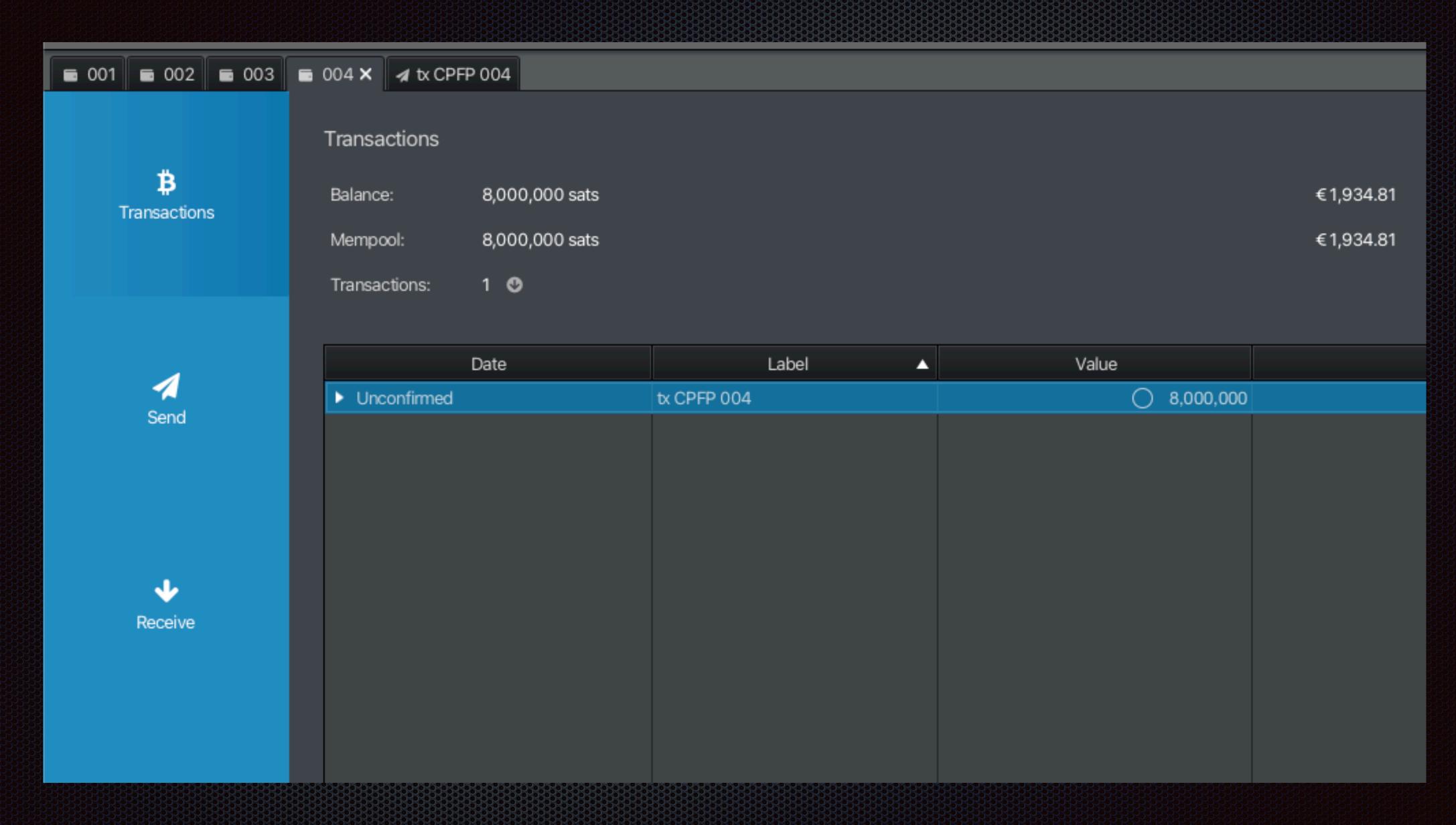






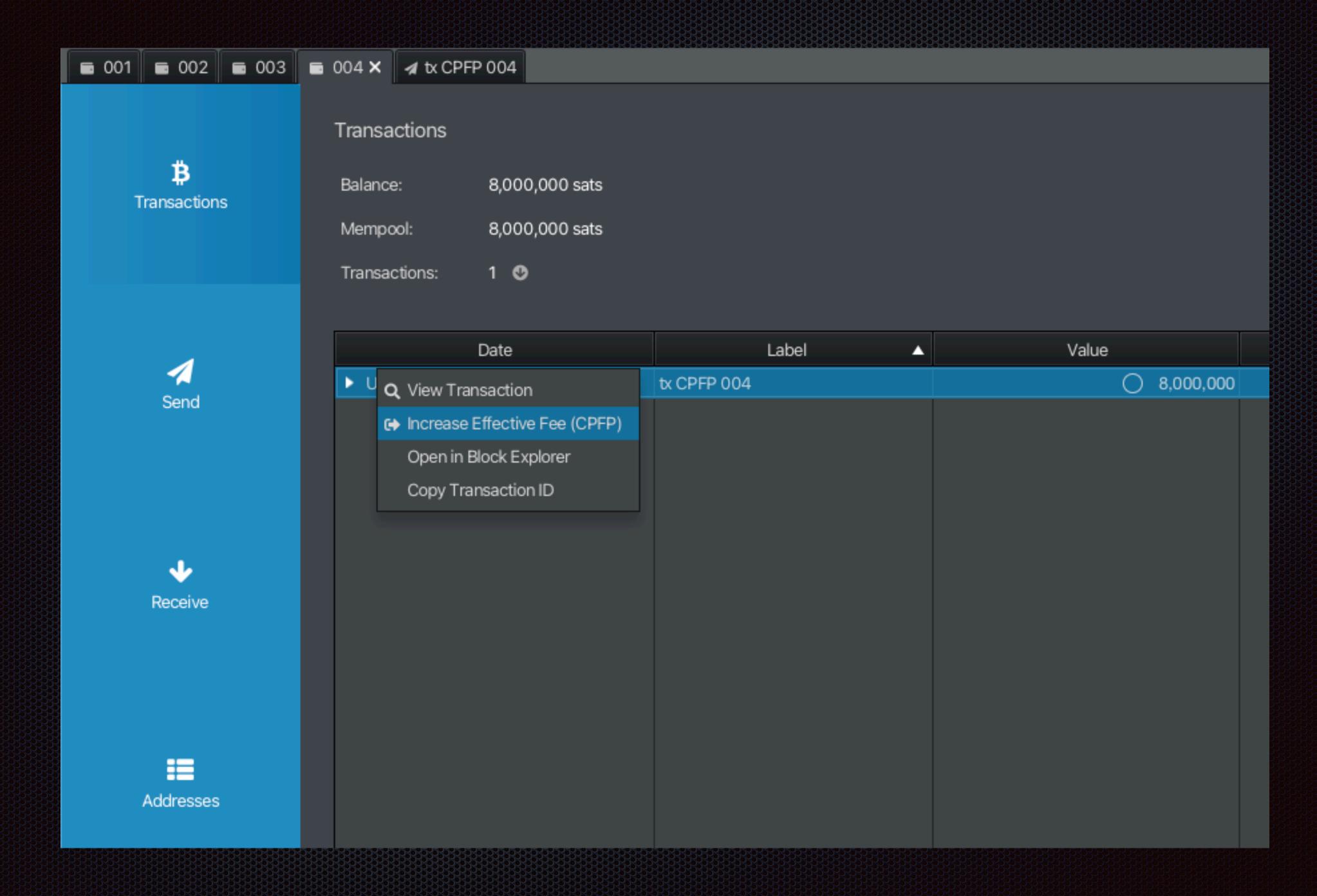






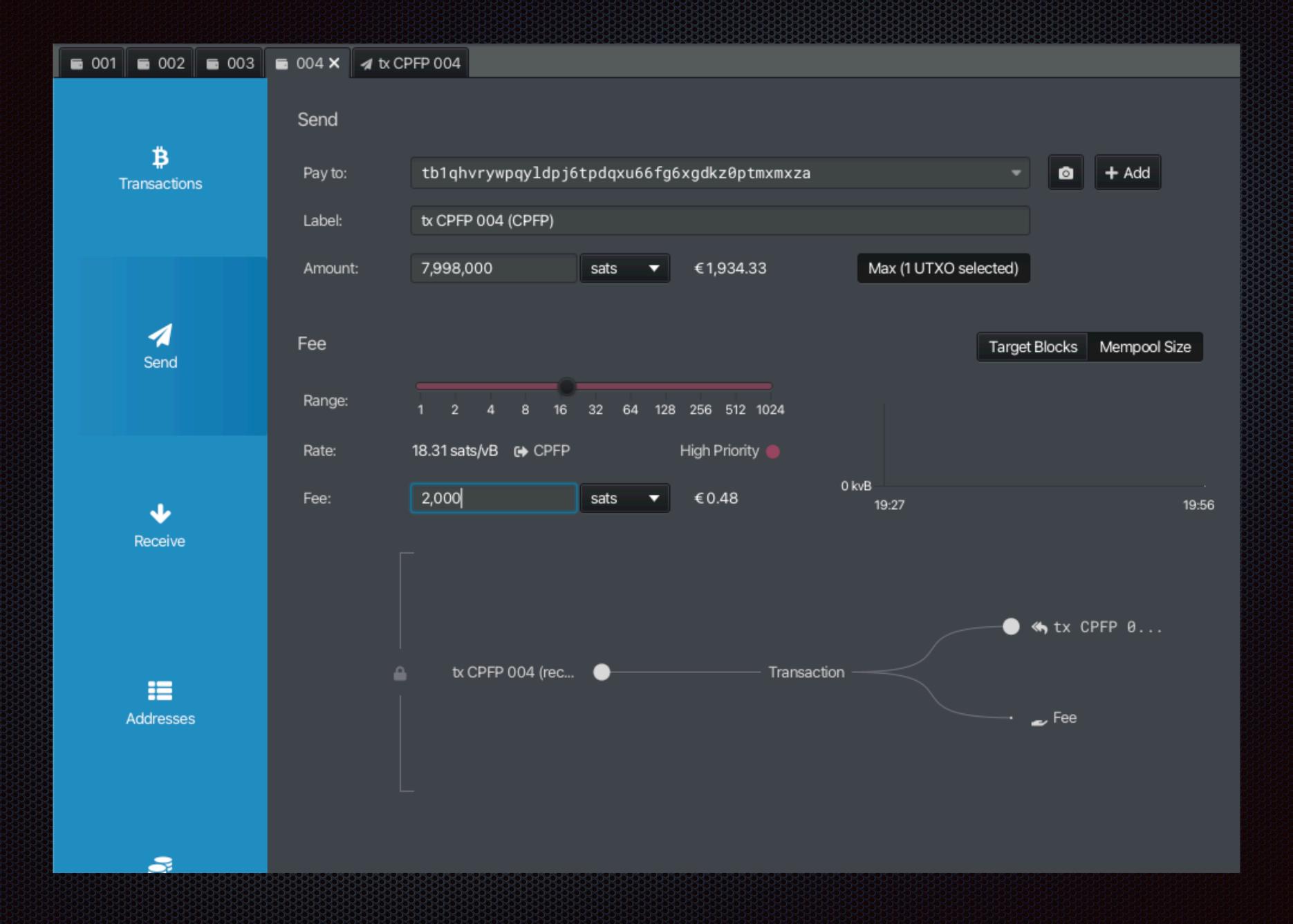






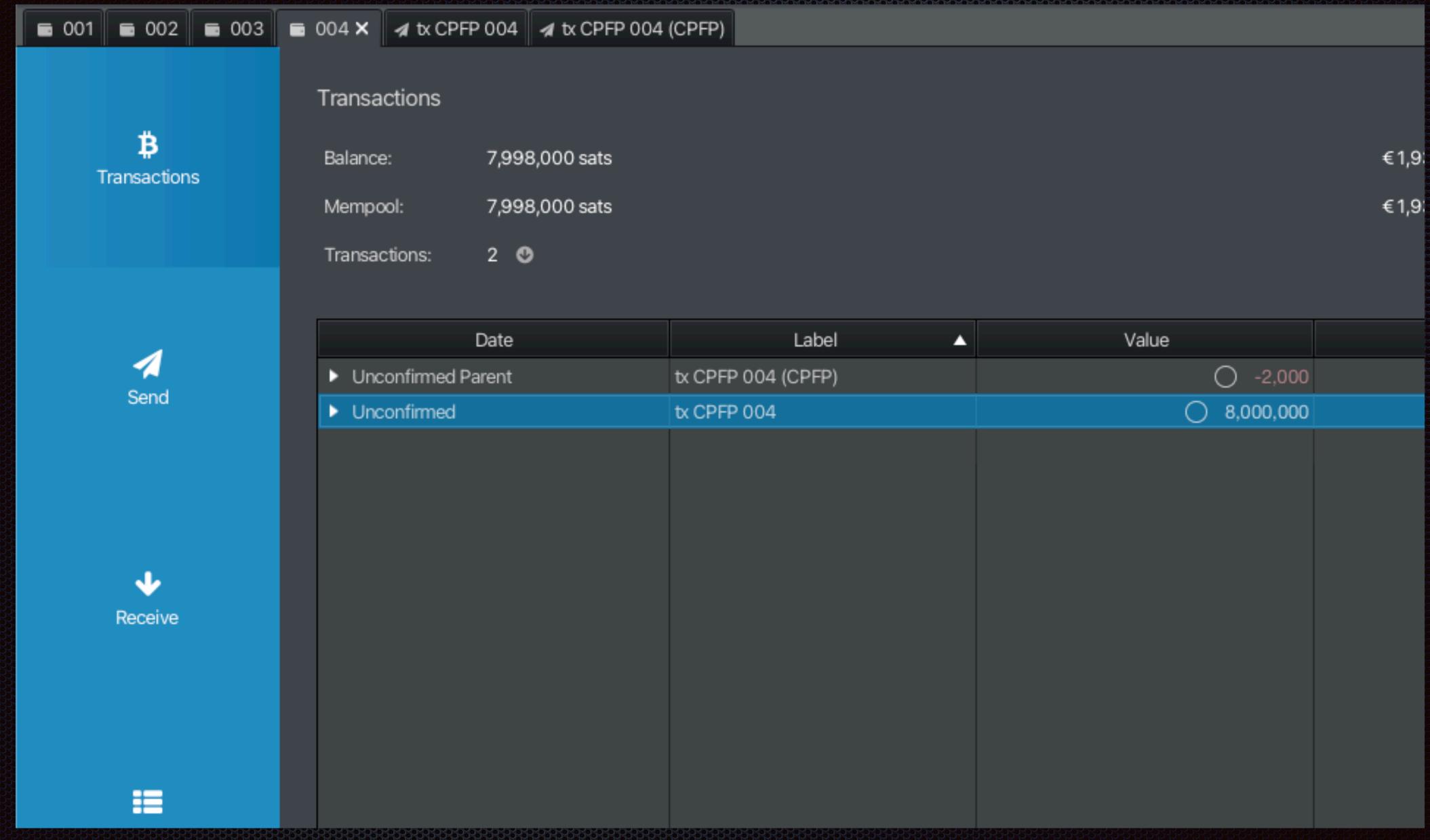






















## Which one should you use?

If you're the spender and want your transaction to confirm faster, use RBF. If you received a payment and are unable to convince the sender to up the fee, or the transaction is marked as non-replaceable, use CPFP.

Better yet, send your transaction with the proper fee the first time





## Notes:

- RBF: Transactions has a finger print (chain analysis)
- RBF is cheaper than CPFP, one transaction vs two transanctions.
- You can use CPFP in the change amount.
- There is a limit in the amount of CPFP you can concatenate.
- RBF and CPFP do not guarantee it will be applied.





## Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshin@gmx.com 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