Thanks for reading!

Want to learn more?

⟶ check out the complete list of BIPs: github.com/bitcoin/bips

⟶ start following the ***bitcoin*** dev mailing list. You'll be among the first to hear about new BIPs and updates to ones in progress

Still want more? Head over to
https://satsie.dev/bips
for additional resources

Satsie's Pocket Guide to

PAYJOIN

A short zine about payjoin: what is it, why it's cool and how it works

@satsie ☆ https://satsie.dev/zines

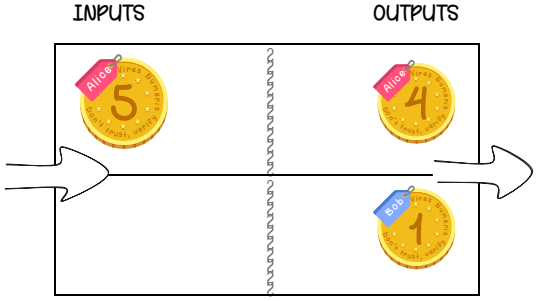
LAST UPDATED: JULY 2024

Payjoin is a technique for batching ***bitcoin*** transactions while preserving privacy and blockspace.

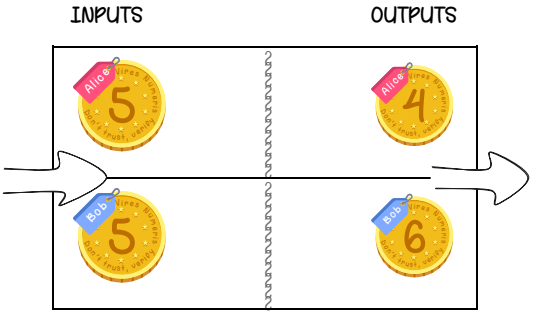
Recall that:

1. ***bitcoin*** uses the UTXO model, and
2. coins (transaction inputs and outputs) can be of any value

Pretend Alice has 5 BTC in her wallet and she sends 1 BTC to Bob. The transaction (tx) looks like this:



With payjoin, the receiver also contributes an input. Let's say Bob already has 5 BTC in his wallet and he wants to use that in a payjoin tx. It would look like this:



So why is this good? The first benefit is scalability. By definition, payjoin does some tx batching. In both scenarios, Bob ends up with a total of 6 BTC, but there's a slight difference in how it's represented. In the 1st example, he has 1 BTC from Alice and the 5 BTC he already had. With payjoin, he has a single 6 BTC.