At the time of writing, silent payments software libraries are being finalised in order for developers to easily adopt it. In the meantime, there are already a a couple of trailblazers like Cake wallet, Wasabi wallet (send only) etc. that support silent payments.

🚀	📠	🏷
Convenient	Contacts	Auto-labelling

Silent payments remove the hassle of sharing new addresses every time you want to receive a payment, allow tracking payment sources with labels and enable robust Contacts feature. The result is a safer, easier and more powerful payments experience!

🌐 Visit bitcoin.design to learn more.

📧 yashrajdca@proton.me to get in touch! 👋

UX edition

YASHRAJ'S POCKET GUIDE

to

SILENT PAYMENTS

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

Improved privacy!

Of-course silent payments improve your privacy by auto-generating new on-chain addresses for every payment. Interestingly, when smartly used, Labels information might even be useful in preserving your privacy when you spend bitcoin!

Let's say you buy bitcoin every week from your bitcoin exchange, but also receive bitcoin directly from customers, friends etc. It's always a good idea to keep & spend bitcoin from these sources separately.

Now that labels can be auto-applied, you can add the proper labels (just once per payment source!) before generating & sharing a customised address. These will now be auto-applied to incoming payments, and help your wallet use the correct coins when you spend bitcoin!

This new, reusable address type (starts with sp1) solves our convenience & privacy issues:

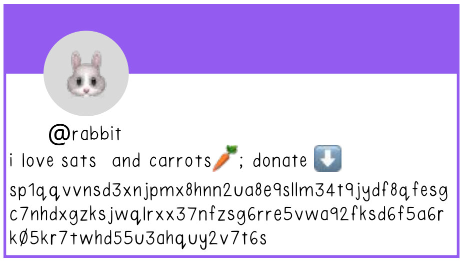
- avoids repeated interactions between senders and receivers to get payment details

- prevents on-chain address being reused since it is auto-generated during send process

Here's what makes silent payments cool:

Convenience!

You can simply share or request this addresses once, then reuse it repeatedly. You can even post in public location like social media



@rabbit

i love sats and carrots🥕; donate ⬇️

sp1qqvvnsd3xnjpmx8hnn2ua8e9sllm34t9jydf8qfesg
c7nhdxgzksjwqlrxx37nfzsg6rre5vwa92fksd6f5a6r
kØ5kr7twhd55u3ahquy2v7t6s

When we want to call our friends or family, we just use their phone number that we used and stored earlier. But since bitcoin is a transparent, public network, using the same on-chain address every time we want to send or receive payments is not private or safe.

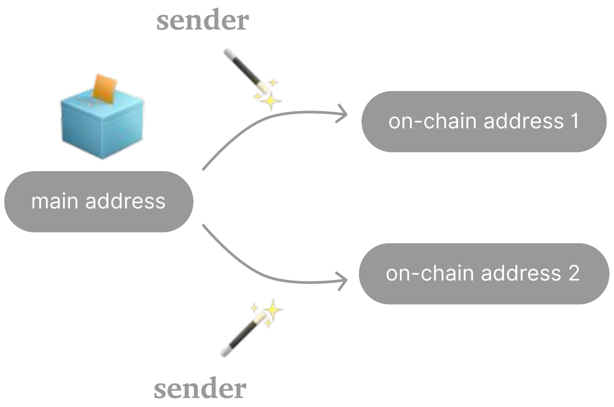
This gives rise to the inconvenience of sharing/getting fresh address every time one needs to make or receive a payment. This process can be error-prone, takes time and requires manual effort.

☎	✉	₿
Reusable ✅	Reusable ✅	Not-reusable ❌

Silent payments protocol (BIP-352) aims to address these issues by providing a new type of address that can be reused because it does not appear on the public blockchain.

Ok great!
But how to use silent payments in a transaction? 4 simple steps or less!

1. The receiver shares/publishes a static payment address (one-time)
2. The sender's wallet uses it to derive an unique on-chain address (automatic)
3. The sender broadcasts the transaction that pays this derived address (manual)
4. The receiver scans the blockchain & identifies their payments (automated)



Contacts:

Like phone numbers or email addresses, it is natural to want to store reusable bitcoin addresses for future use.

Contacts are a great way to do this in an intuitive way, instead of constantly dealing with long & unwieldy addresses before making bitcoin payments!

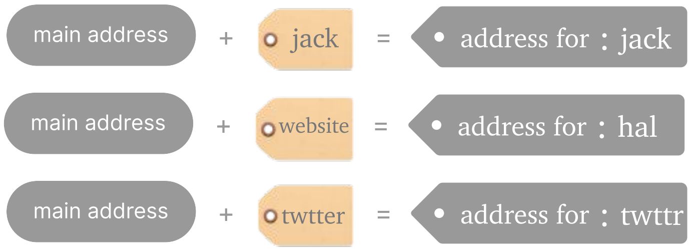
People can store static addresses for their friends/family, clients, or even exchanges as Contacts.

For the first time, native bitcoin payments can be made like you make phone calls or send fiat payments through your bank!

Labels: better & stickier

Labels are great to track valuable & useful information! The problem is, adding such info every time you send or receive bitcoin can be tedious, and people tend to avoid it. Also we forget such details soon after our task is completed!

Silent payments allow receivers to add useful labels or even sender information to their addresses before sharing them. When payments are received, these labels are auto-applied to incoming transactions and be detected by your wallet (but no one else).


main address
+
jack
=
address for : jack
main address
+
website
=
address for : hal
main address
+
twtter
=
address for : twttr