[compactor]

A privacy-preserving
bitcoin consolidation tool

Problem

- Users of mainchain privacy tools like ECDH addresses and non-custodial mixers are left with dozens, potentially hundreds of utxos in different addresses that can be difficult to manage.

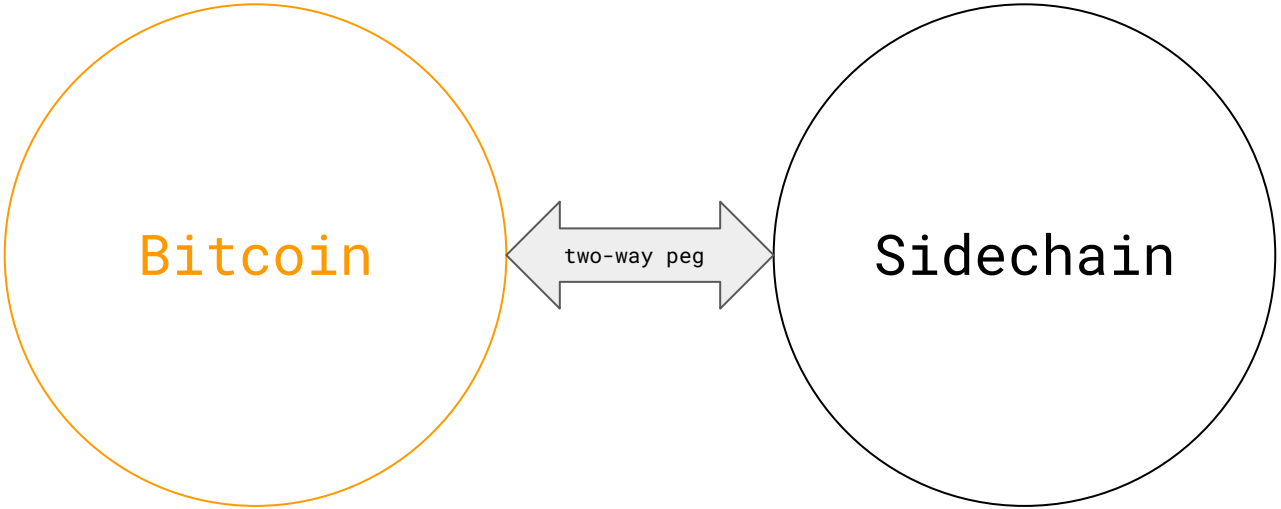
- Merging inputs from different addresses (for example, to make a larger transaction than afforded by the balance of a single address) can cause both individual and systemic privacy harms. The more addresses merged, the smaller the anonymity set.

- Other zero-knowledge protocols that could be used to privately consolidate coins expose users to slippage risks and/or non-bitcoin aligned platforms.

Technology

- Zero-knowledge bitcoin sidechain
- Tor-only connection (unique circuit per deposit/withdrawal)
- BIP158 light client/ZIP307 lightwallet + full node support
- Full, end-to-end hardware wallet support
- Desktop app first, mobile later

The two-way peg mechanism provides a bridge between the bitcoin mainchain and the sidechain



Transaction amount, sender, and recipient are e2e encrypted using zero-knowledge proofs

Example e2e encrypted transaction on the Zcash blockchain, which uses the same zk-SNARK tech as the sidechain.
Source: https://explorer.zecmate.com/tx/35f6674a1691f21aff6a3819467dbba82aaebf061d50c6ac55f39fbeae73b9a6

How [compactor] works

Step 1. Deposit sats in the sidechain

- If depositing from a hardware wallet: manually deposit according to a randomized schedule* set by the app.

- If depositing from a paper or software wallet: import xpriv or individual private keys. The app will then automatically send the deposit transactions in the background on a randomized schedule.

  * When bootstrapping the anonymity set, deposits from different users will be grouped together around the same time, based on a pre-defined schedule programmed into the app. Deposits from the same user will still be sent separately, one at a time.

- Each output from each deposit address will be credited to a different sidechain address to avoid linkage.

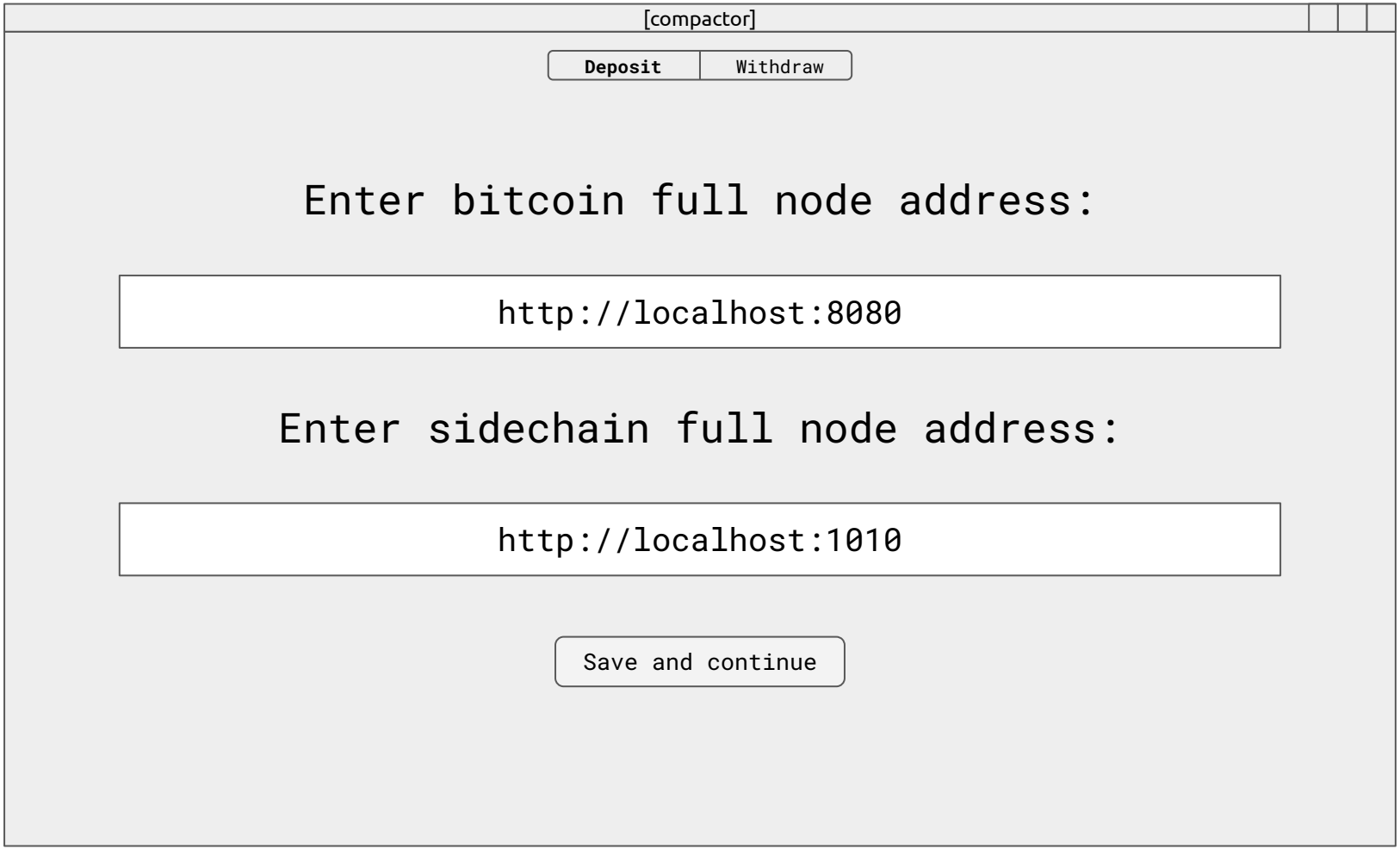
[compactor]

Deposit | Withdraw

How would you like to sync the [compactor] app?

Full node

Light client


[compactor]
Deposit
Withdraw
Enter bitcoin full node address:
http://localhost:8080
Enter sidechain full node address:
http://localhost:1010
Save and continue

Full node

[compactor]

Deposit | Withdraw

Syncing wallet...

Light client

[compactor]

Deposit | Withdraw

What kind of wallet are you depositing from?

Hardware

Paper or software

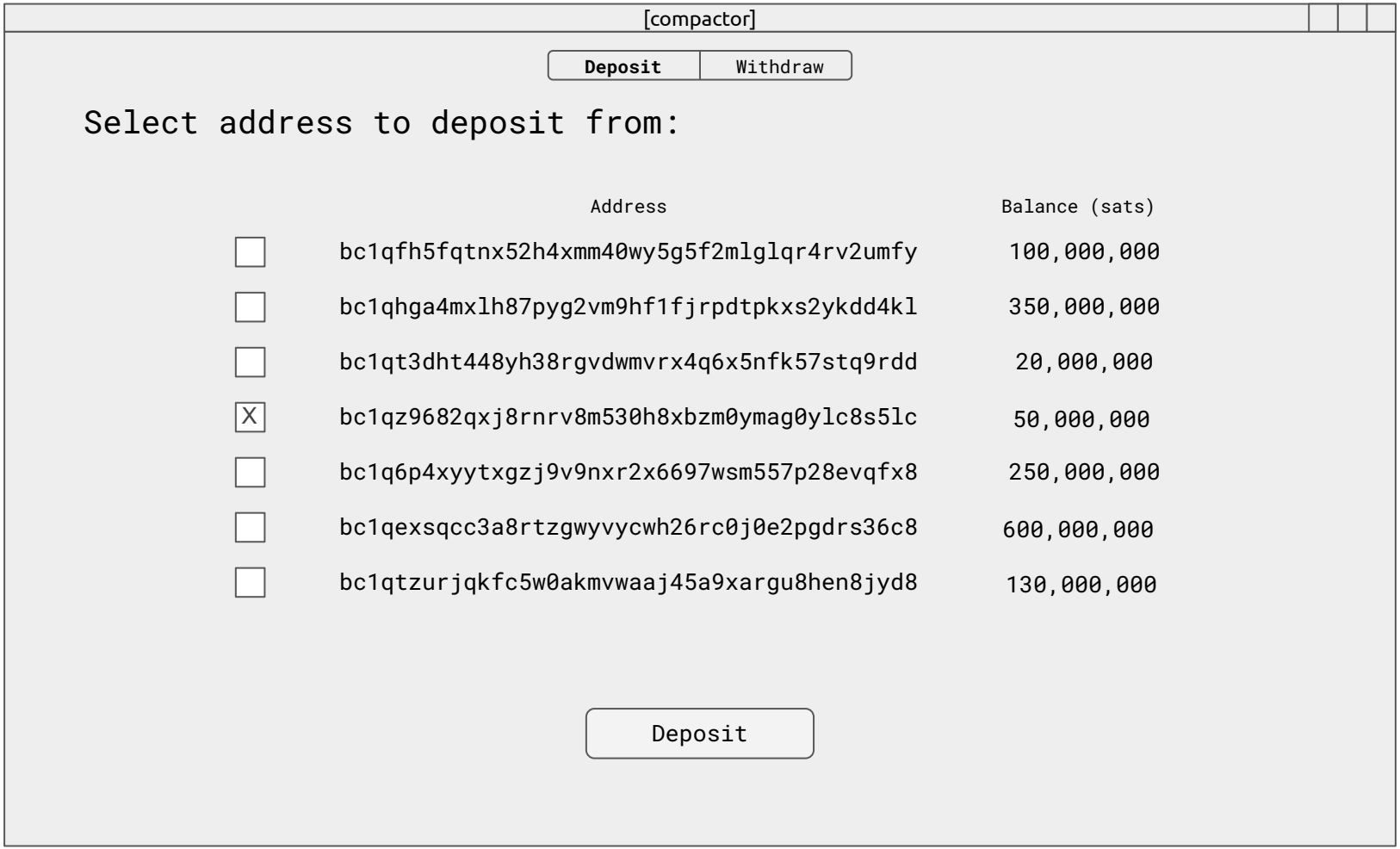
Hardware wallet


[compactor]
Deposit
Withdraw
Import sidechain xpub
Switch your hardware wallet to the sidechain app then click “Import” to continue.
Import

Hardware


[compactor]
Deposit
Withdraw
Import bitcoin xpub
Switch your hardware wallet to the bitcoin app then click “Import” to continue.
Import

Hardware


[compactor]
Deposit
Withdraw
Select address to deposit from:
Address
Balance (sats)
bc1qfh5fqtnx52h4xmm40wy5g5f2mlglqr4rv2umfy
100,000,000
bc1qhga4mxlh87pyg2vm9hf1fjrpdtpkxs2ykdd4kl
350,000,000
bc1qt3dht448yh38rgvdwmvrx4q6x5nfk57stq9rdd
20,000,000
bc1qz9682qxj8rnrv8m530h8xbzm0ymag0ylc8s5lc
50,000,000
bc1q6p4xyytxgzj9v9nxr2x6697wsm557p28evqfx8
250,000,000
bc1qexsqcc3a8rtzgwyvycwh26rc0j0e2pgdrs36c8
600,000,000
bc1qtzurjqkfc5w0akmvwaaj45a9xargu8hen8jyd8
130,000,000
Deposit

Hardware

[compactor]

Deposit | Withdraw

For your privacy,
please wait to make
your next deposit...

Step 2. Leave app open and wait

- The app will ask hardware wallet users to manually approve consolidation transactions one at a time. Notes will be consolidated by shuffling the notes between zero-knowledge addresses, eventually consolidating all notes owned by the user into one zero-knowledge address.

- Consolidation will happen in such a way that blockchain observers cannot tell which bitcoin addresses the notes on the sidechain originated from.

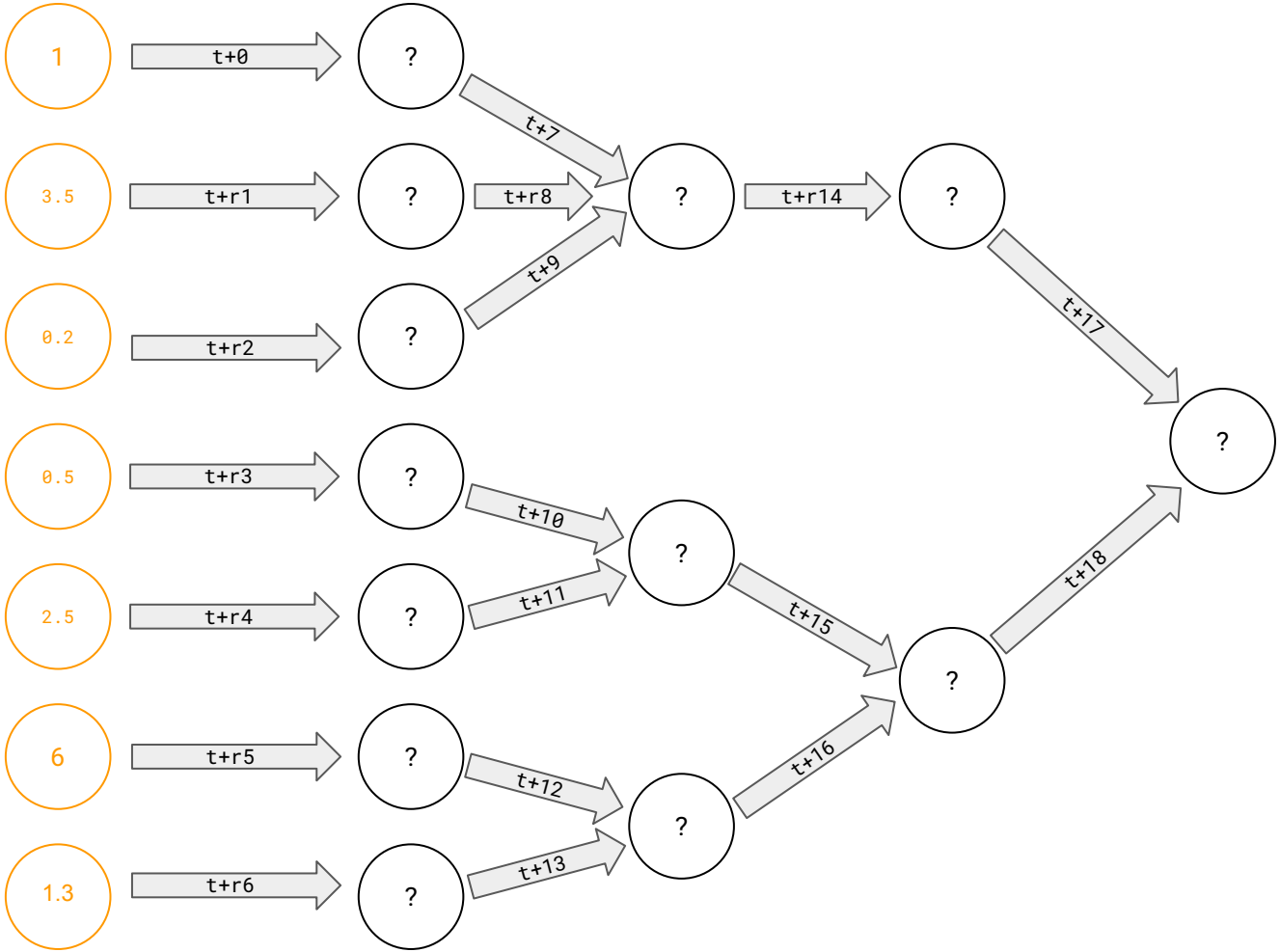

[compactor]
Deposit
Withdraw
Approve consolidation transaction
Switch your hardware wallet to the sidechain app, click “Approve”, then confirm the transaction on your hardware wallet to continue.
Approve

Hardware

[compactor]

Deposit | Withdraw

For your privacy, please wait to approve the next consolidation transaction...


1
3.5
0.2
0.5
2.5
6
1.3
t+0
t+r1
t+r2
t+r3
t+r4
t+r5
t+r6
?
t+7
t+r8
t+9
t+r14
t+17
t+10
t+11
t+15
t+18
t+12
t+13
t+16

Paper or software wallet

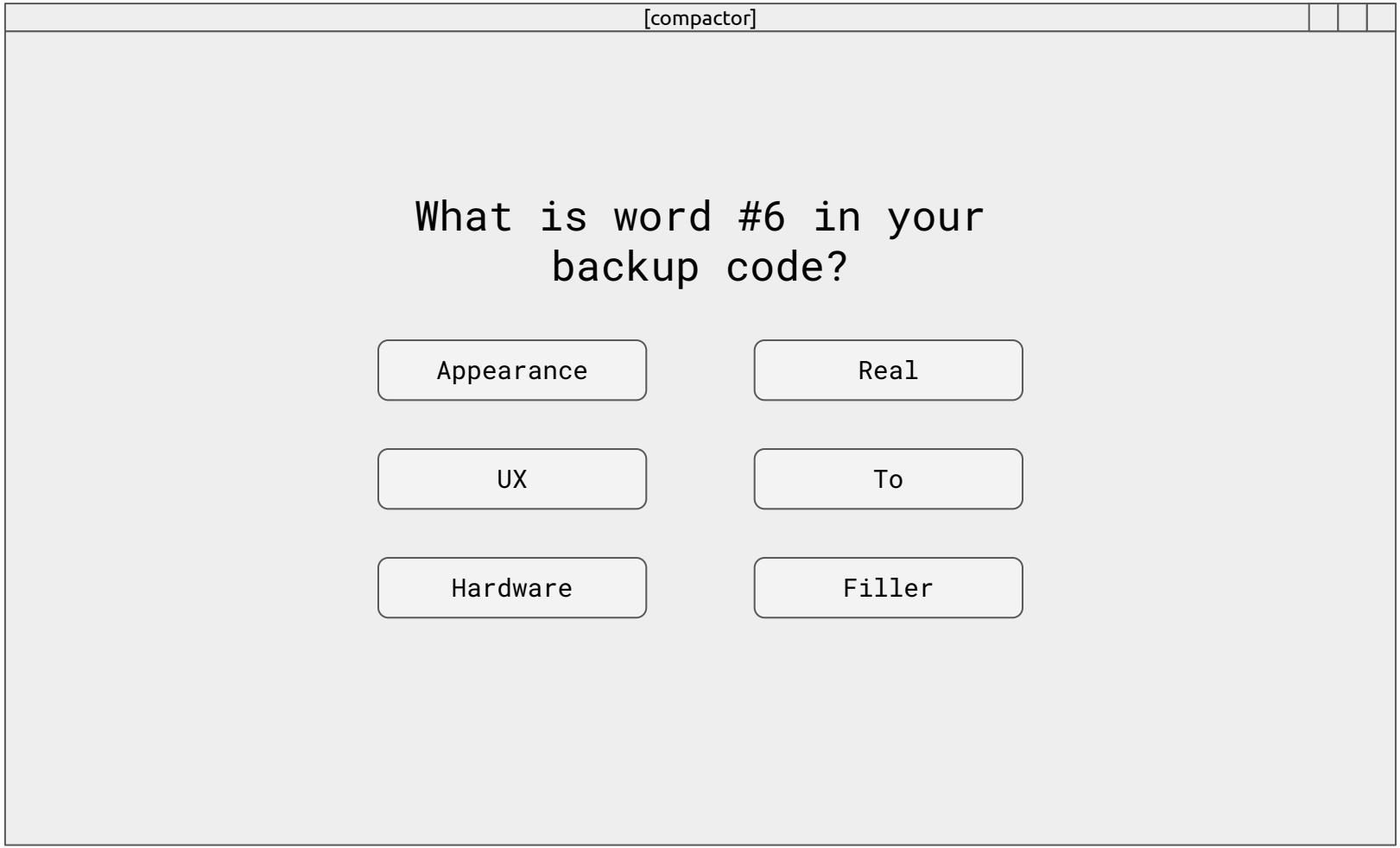
[compactor]

This is your backup code

Copy the code exactly as it is written below and **keep it in a safe place**, for example by storing it in a password manager or writing it down on paper and keeping it where you store other important documents. You can use the backup code to recover your sats if anything bad happens to this app or your computer. **Never share your backup code with anyone else**, or they will gain access to your sats too.

1. This
2. Is
3. Just
4. Filler
5. Text
6. To
7. Give
8. The
9. Appearance
10. Of
11. Real
12. UX

Paper or software



Paper or software

Paper or software

Step 2. Leave app open and wait

- The app will automatically consolidate notes in the background by shuffling the notes between zero-knowledge addresses, eventually consolidating all notes owned by the user into one zero-knowledge address.

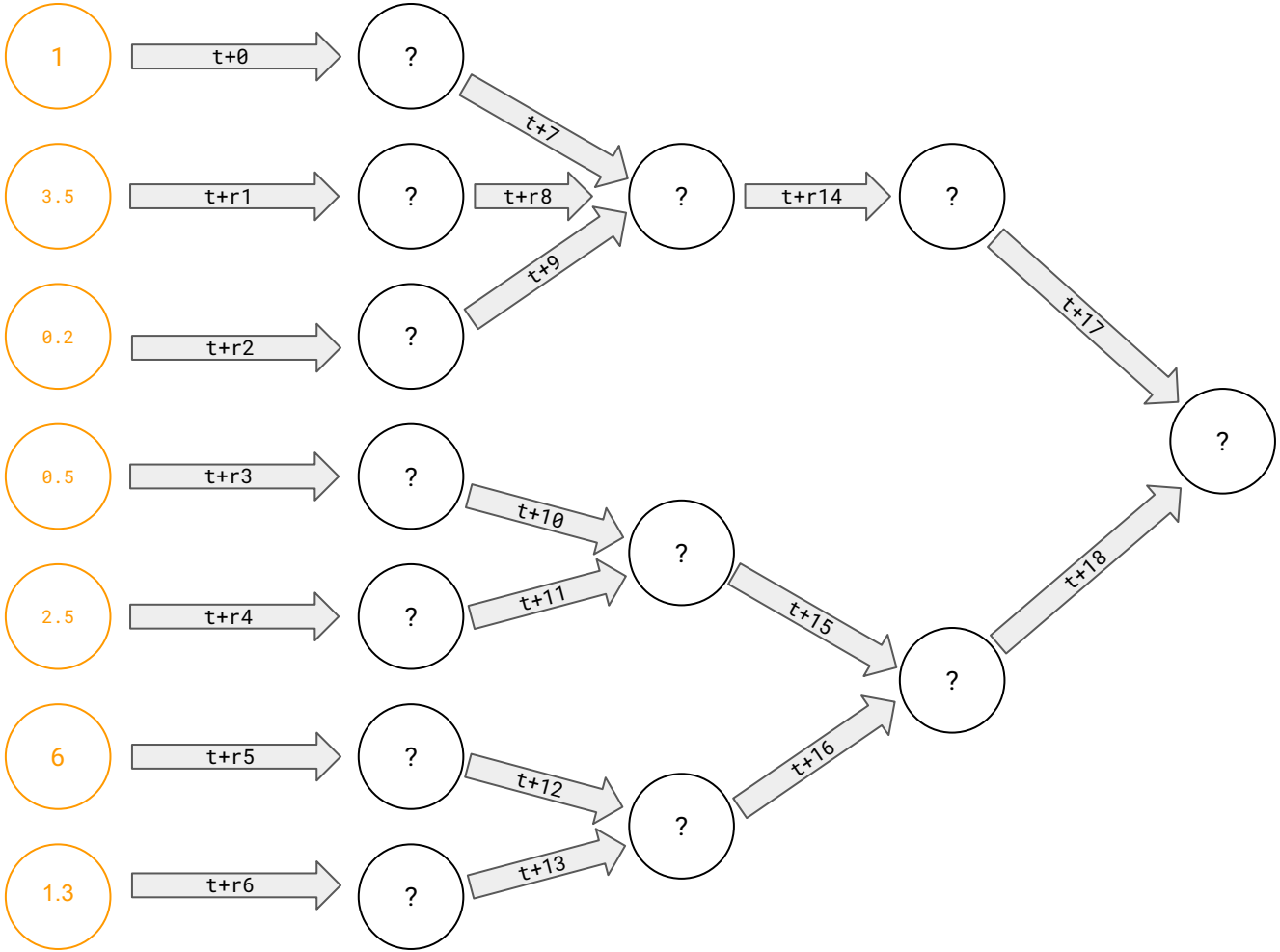
- Consolidation will happen in such a way that observers cannot tell which bitcoin addresses the notes on the sidechain originated from.

[compactor]

Deposit | Withdraw

Consolidating sats...

Paper or software


1
3.5
0.2
0.5
2.5
6
1.3
t+0
t+r1
t+r2
t+r3
t+r4
t+r5
t+r6
?
t+7
t+r8
t+9
t+r14
t+17
t+10
t+11
t+15
t+18
t+12
t+13
t+16

Step 3. Withdraw

- Option 1, automatic: enter xpub and select from a mix of denominations for each output. Each withdrawal output will be sent to an unused address derived from the xpub.

- Option 2, manual: withdraw to separate addresses one at a time in pre-defined denominations.

- Withdrawals are randomly spaced out to prevent timing attacks. The app will also wait until further sidechain deposits and withdrawals are made that provide “cover traffic” for the user’s withdrawal. Finally, each denomination can only be withdrawn on certain days at certain times, providing further cover traffic and enabling users to “hide in the crowd”.

[compactor]

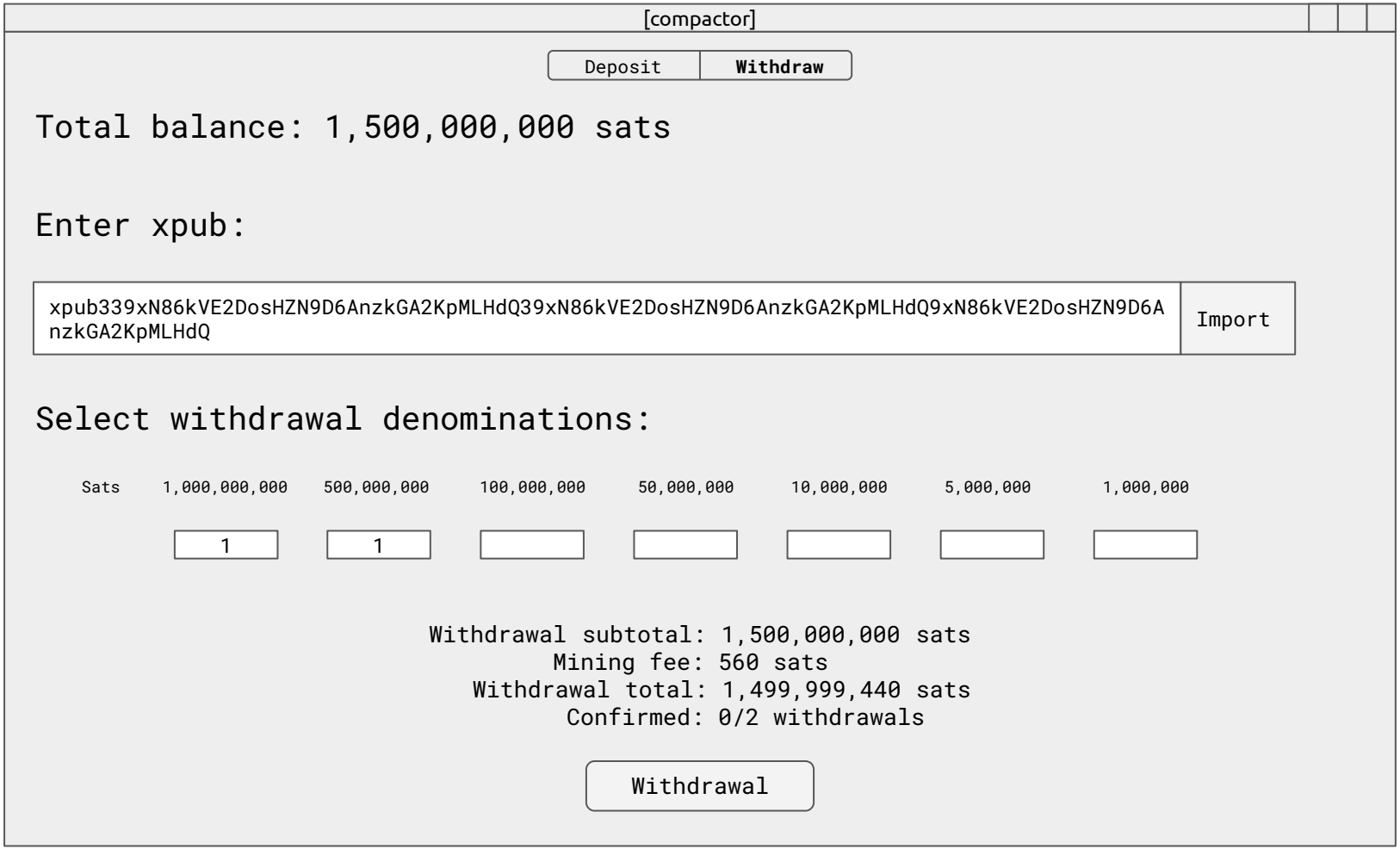
Deposit | **Withdraw**

Ready to withdraw

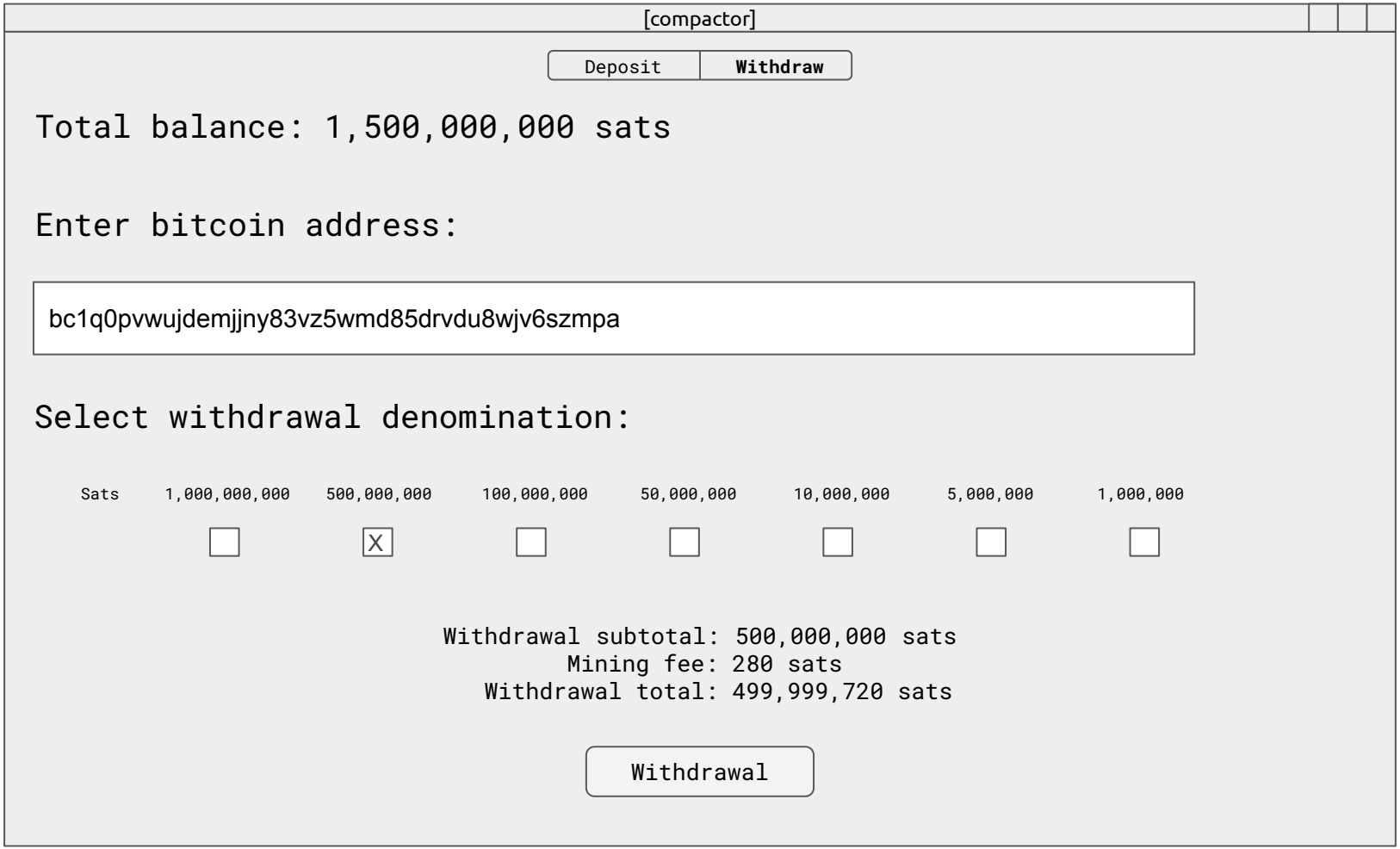
How would you like to withdraw your sats?

Automatic

Manual


[compactor]
Deposit
Withdraw
Total balance: 1,500,000,000 sats
Enter xpub:
xpub339xN86kVE2DosHZN9D6AnzkGA2KpMLHdQ39xN86kVE2DosHZN9D6AnzkGA2KpMLHdQ9xN86kVE2DosHZN9D6AnzkGA2KpMLHdQ
Import
Select withdrawal denominations:
Sats
1,000,000,000
500,000,000
100,000,000
50,000,000
10,000,000
5,000,000
1,000,000
1
1
Withdrawal subtotal: 1,500,000,000 sats
Mining fee: 560 sats
Withdrawal total: 1,499,999,440 sats
Confirmed: 0/2 withdrawals
Withdrawal

Automatic


[compactor]
Deposit
Withdraw
Total balance: 1,500,000,000 sats
Enter bitcoin address:
bc1q0pvwujdemjjny83vz5wmd85drvdu8wjv6szmpa
Select withdrawal denomination:
Sats
1,000,000,000
500,000,000
100,000,000
50,000,000
10,000,000
5,000,000
1,000,000
X
Withdrawal subtotal: 500,000,000 sats
Mining fee: 280 sats
Withdrawal total: 499,999,720 sats
Withdrawal

Manual

[compactor]

Deposit | **Withdraw**

For your privacy,
please wait to make
your next withdrawal...

Manual

[compactor]

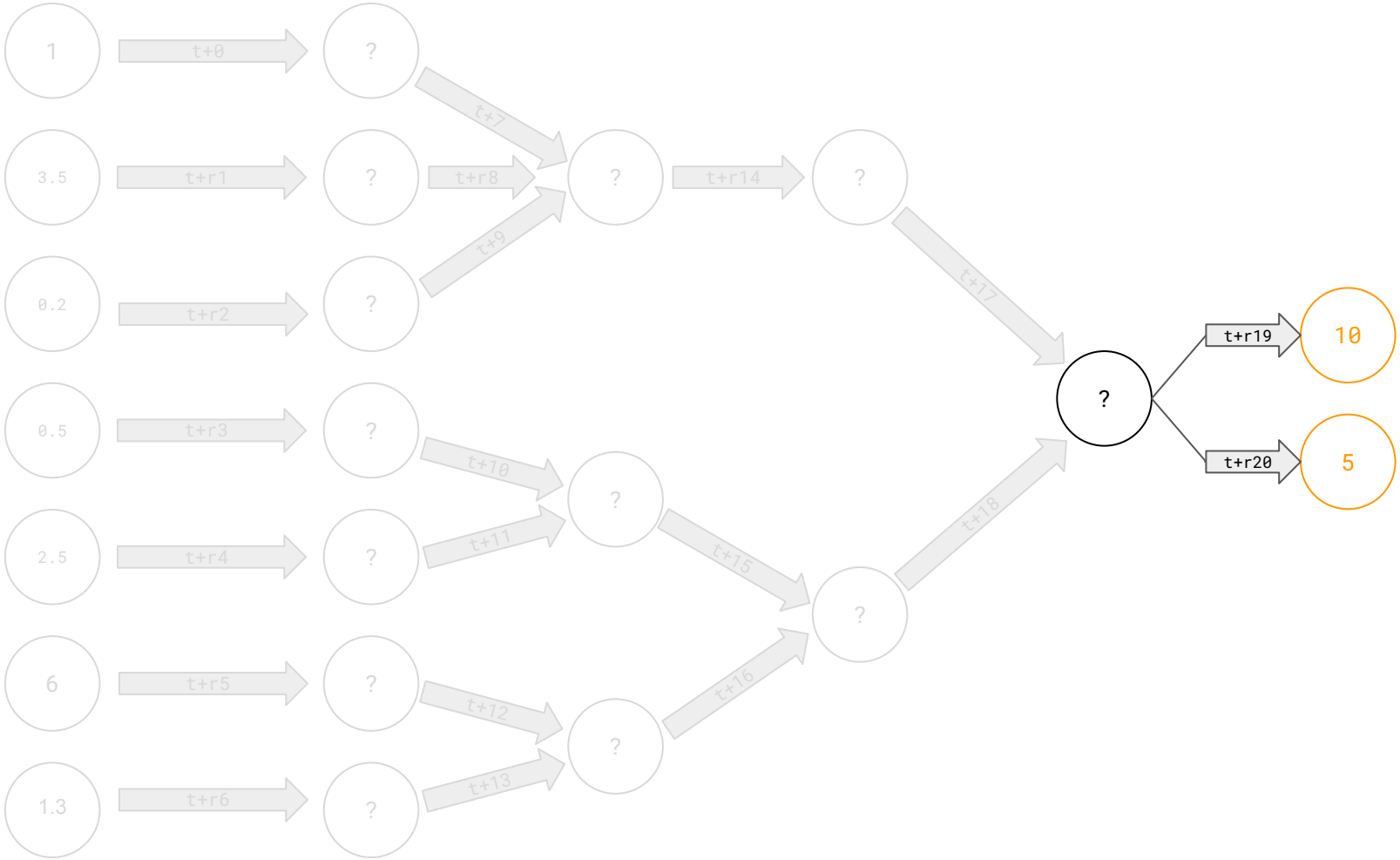
Deposit | **Withdraw**

All done

Your sats have been consolidated into the designated bitcoin addresses.

Start over

Exit


1
t+0
?
3.5
t+r1
?
0.2
t+r2
?
0.5
t+r3
?
2.5
t+r4
?
6
t+r5
?
1.3
t+r6
?
t+7
t+r8
t+9
?
t+r14
?
t+10
t+11
?
t+15
?
t+12
t+13
?
t+16
t+17
t+18
?
t+r19
10
t+r20
5

TODO

- Figure out what to do with “unusable” change that is either present pre-consolidation or leftover due to mining fees during the consolidation process.
    - Idea: pre-calculate end-to-end fees and strip out the unusable change in the deposit step, leaving it in the origin bitcoin address(es).
        - But can’t pre-calculate if we don’t know ahead of time which denominations users will withdraw using.
    - Another idea: (Probably the best option) Simply leave the unusable change in the sidechain and see if it can be combined with the next set of deposits. Also, at some point we’ll release a proper sidechain wallet and then the user will be able to use the unsable change however they’d like.
    - Similar problem: if the sidechain balance is a nice round number like 15 BTC, then when it’s time to withdraw the user won’t be able to have perfect 10 BTC and 5 BTC denominations, because each withdrawal will need to pay a withdrawal fee to sidechain and mainchain miners. Is this acceptable? Or should withdrawals be forced to downgrade to the next highest denomination so that leftover BTC can be used to pay mining fees?
        - It’s probably fine to allow both fee-add and fee-subtract withdrawals.