Peerplays Sidechain Deposit - BTC Flow

1 A user with BTC decides to make a Peerplays account. They visit the Peerplays DEX and create a new account.

2 The user needs two Bitcoin accounts (one for deposits, one for withdraws) that they can use for their Peerplays sidechain transfers. These Bitcoin accounts will be mapped to the user's Peerplays account using:

- The Deposit Account Public Key
- The Withdrawal Account Public Key
- The Withdrawal Account Address

The Private Keys are not used and are left safely with the user.
(This step only has to be done once!)

3 Using the user's Bitcoin deposit account public key, the Peerplays SONs will create a new multi-signature deposit address.

Now to make a deposit to Peerplays, the user simply needs to send some BTC to the multi-signature deposit address.

4 When the funds land in the multi-signature deposit address, the SONs will see the transaction, validate the data, move the BTC to a SONs controlled Bitcoin wallet, and release the same amount of pBTC (minus a small transaction fee) to the Peerplays account that has been mapped in step 2.

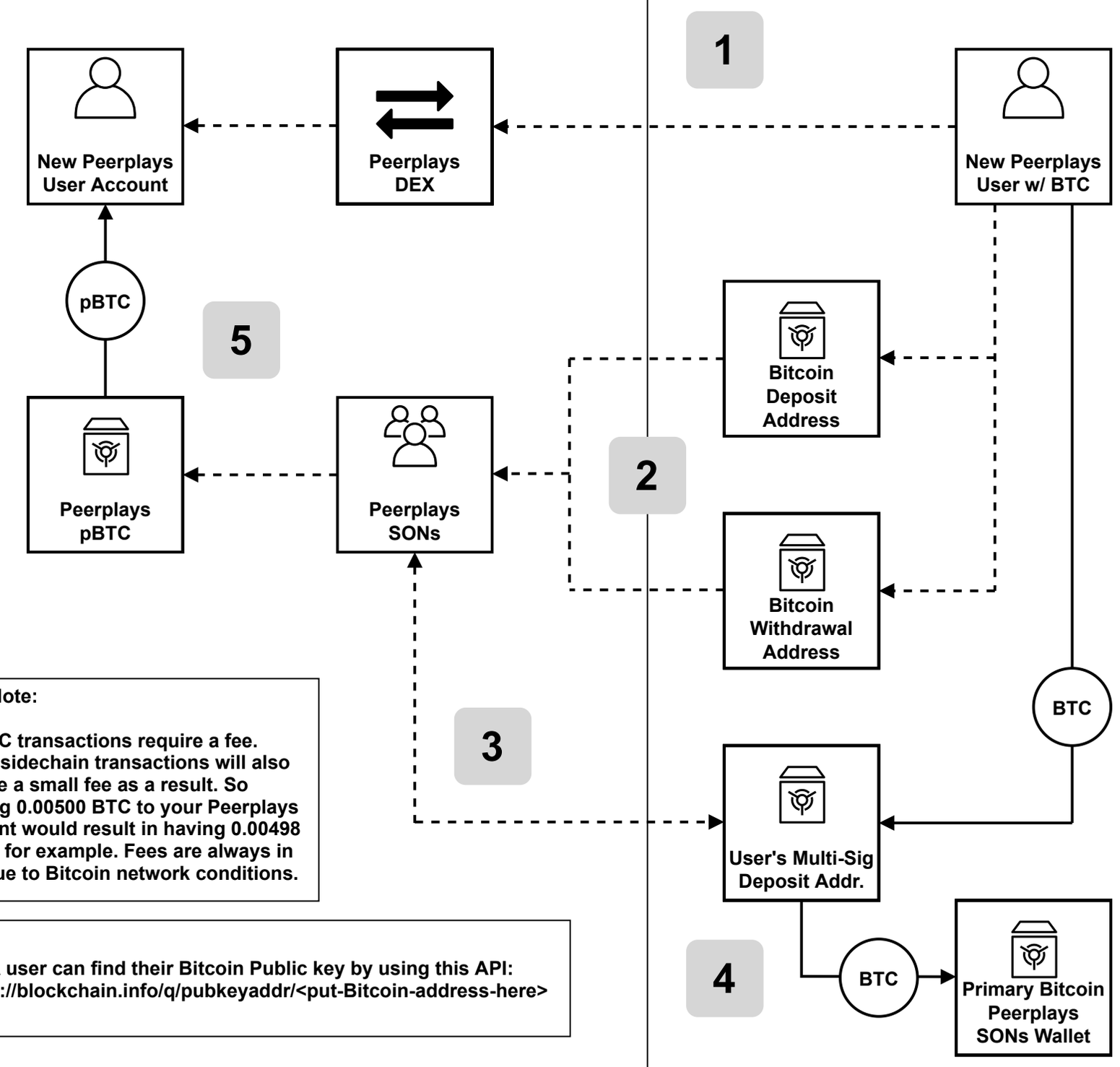
5 The user has successfully deposited their BTC into their new Peerplays account! Their pBTC is backed by the BTC stored in the Peerplays SONs Bitcoin wallet.

It can be used like any other Peerplays asset: traded, staked, sent and recieved, bought and sold, and more!

Side Note:

All BTC transactions require a fee. SONs sidechain transactions will also require a small fee as a result. So moving 0.00500 BTC to your Peerplays account would result in having 0.00498 pBTC, for example. Fees are always in flux due to Bitcoin network conditions.

A user can find their Bitcoin Public key by using this API:
https://blockchain.info/q/pubkeyaddr/<put-Bitcoin-address-here>



Peerplays Chain

Bitcoin Chain

Peerplays Sidechain Withdraw - BTC Flow

1 A Peerplays user with pBTC decides to send some of the funds to an account on the Bitcoin blockchain.

First, a deposit and withdrawal address must be registered on the Peerplays blockchain (just like in the flow chart above). This only needs to be done once to map the Bitcoin addresses to a Peerplays account. If the user has already done this to make a deposit, this step isn't required and we move on to step 2.

2 If a Bitcoin withdrawal address is mapped, the user can send their pBTC funds to the SONs controlled pBTC account on the Peerplays chain. This kicks off the withdraw process.

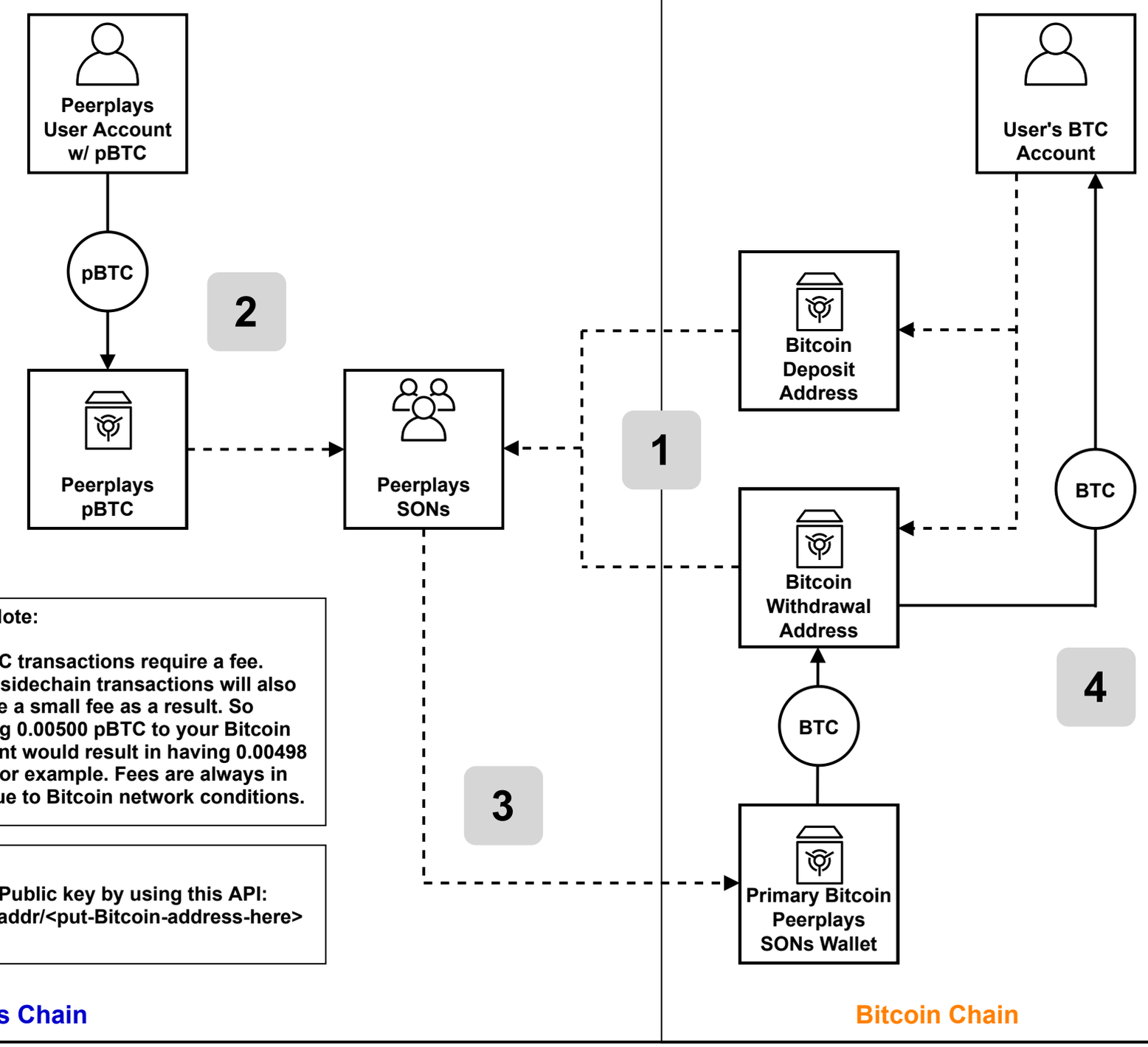
3 When the withdraw is triggered, the Peerplays SONs send the BTC (minus a small transaction fee) from the Peerplays SONs Bitcoin wallet to the user's mapped withdraw address.

4 At this point, the user can withdraw their BTC from their withdarw address. They have successfully withdrawn their BTC from the Peerplays chain back to the Bitcoin chain!

Side Note:

All BTC transactions require a fee. SONs sidechain transactions will also require a small fee as a result. So moving 0.00500 pBTC to your Bitcoin account would result in having 0.00498 BTC, for example. Fees are always in flux due to Bitcoin network conditions.

A user can find their Bitcoin Public key by using this API:
https://blockchain.info/q/pubkeyaddr/<put-Bitcoin-address-here>



Peerplays Chain

Bitcoin Chain