BREEZE WALLET

WITH BREEZE PRIVACY PROTOCOL V1

User Guide

Table of Contents

1. Introduction

The Breeze Wallet with Breeze Privacy Protocol showcases blockchain technology with a strong emphasis on financial privacy and security on the Bitcoin network. The Breeze Privacy Protocol feature enables the Breeze Wallet to automatically connect to a live Breeze Masternode running the Breeze Privacy Protocol. This is achieved by using the Masternode Advertisement and Client Discovery Protocol.

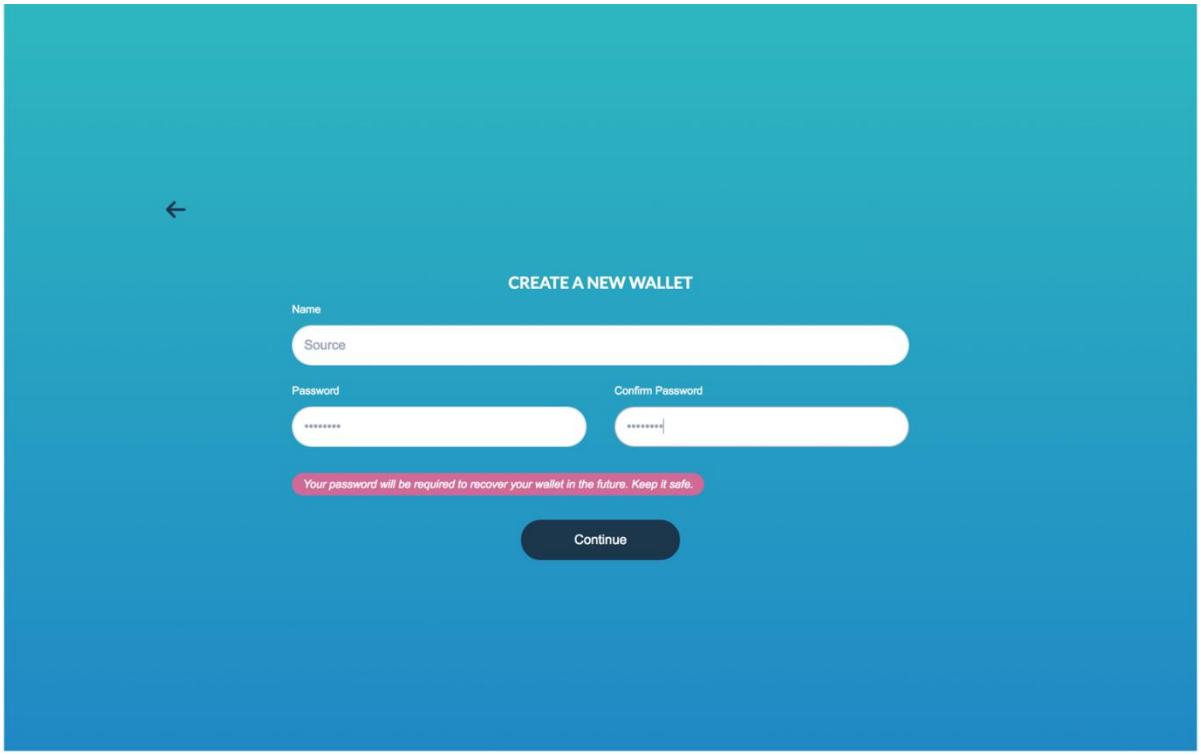
The Breeze Privacy Protocol is used to take a small amount of Bitcoin from a source wallet, shuffle and swap them with other Bitcoins, and then transfer them to a destination wallet. As only small amounts of Bitcoin are taken at a time, it can take some time to transfer large amounts of Bitcoins from the source to the destination. In the Breeze Wallet with Breeze Privacy Protocol, this feature is available in the Bitcoin wallet under the Privacy tab.

The Breeze Wallet with Breeze Privacy Protocol also includes the same features as the regular Breeze Wallet:

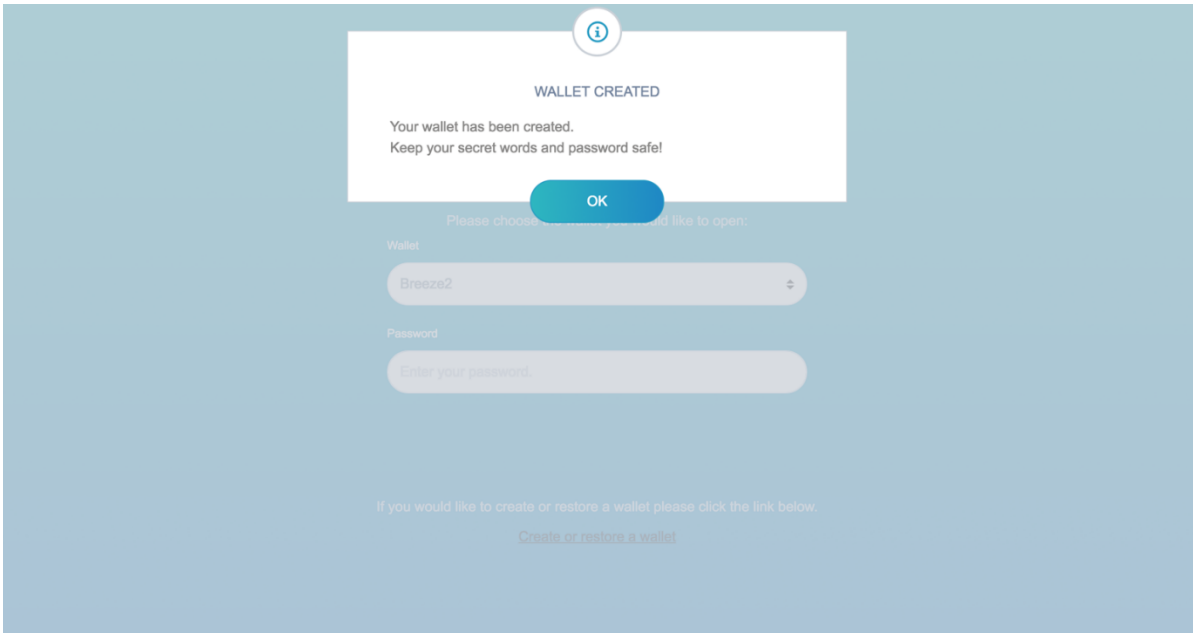
- Dual network functionality: Bitcoin and Stratis
- Full block Simplified Payment Verification (SPV) wallet
- HD (Hierarchical Deterministic) capabilities
- Transaction fee privacy consciousness
- Change address privacy protocol

2. Guide

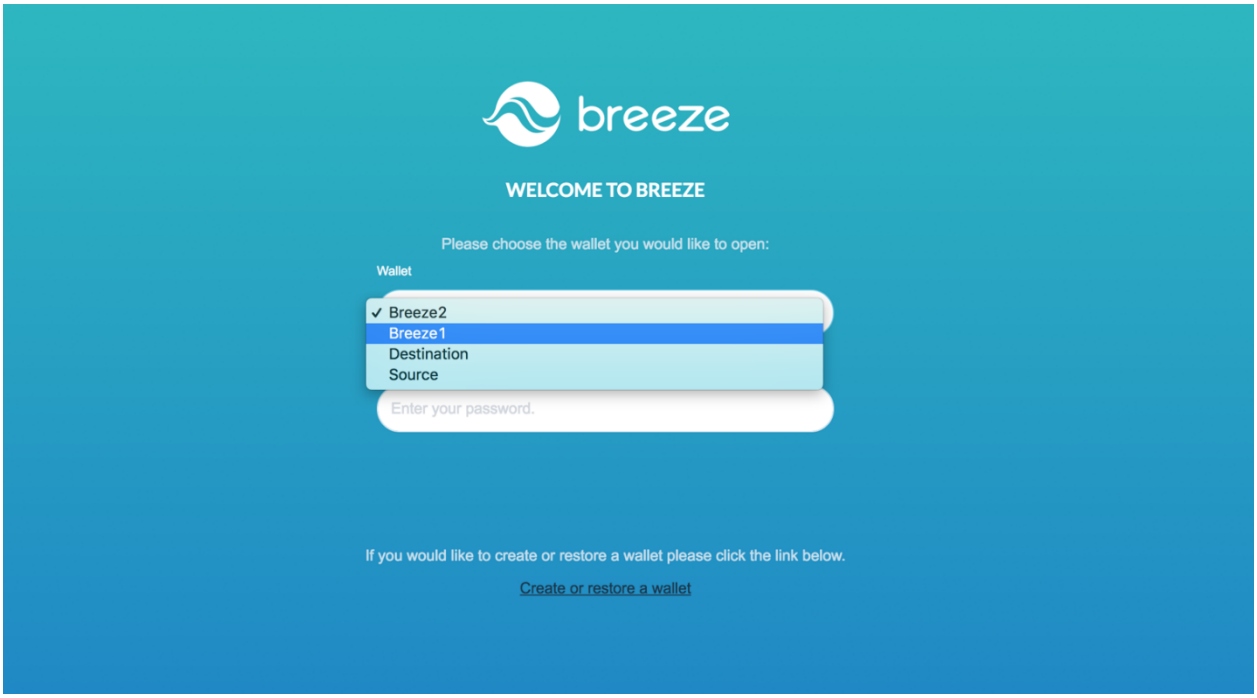
- Create a Source and Destination wallet on the same machine to use the Privacy Protocol.



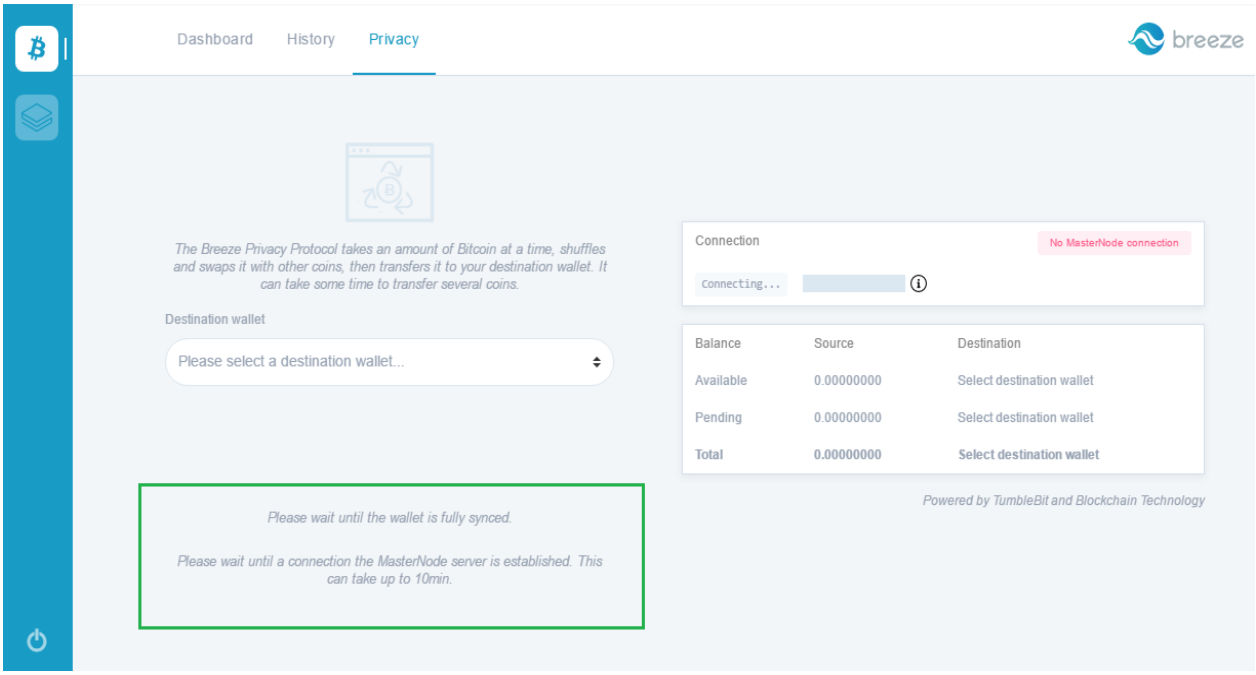
- Keep the secret words and passwords for both wallets safe.



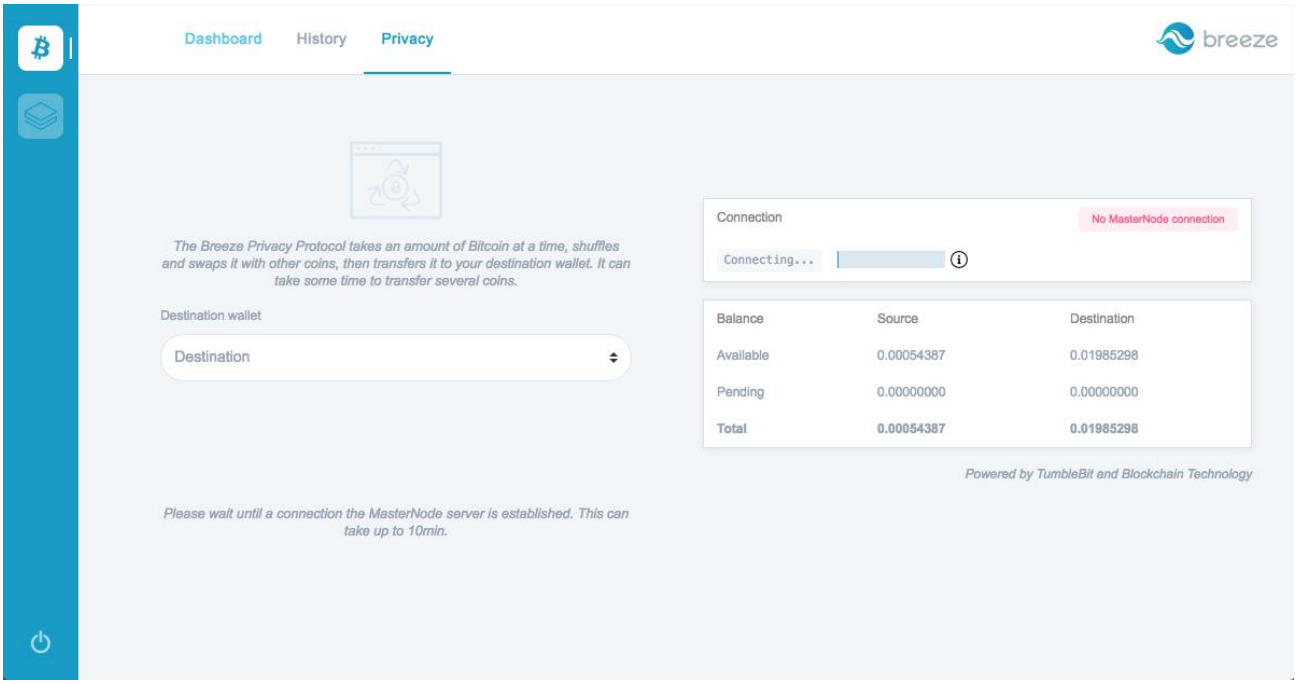
- Log in to the wallet where the funds are located (i.e. the Source wallet).



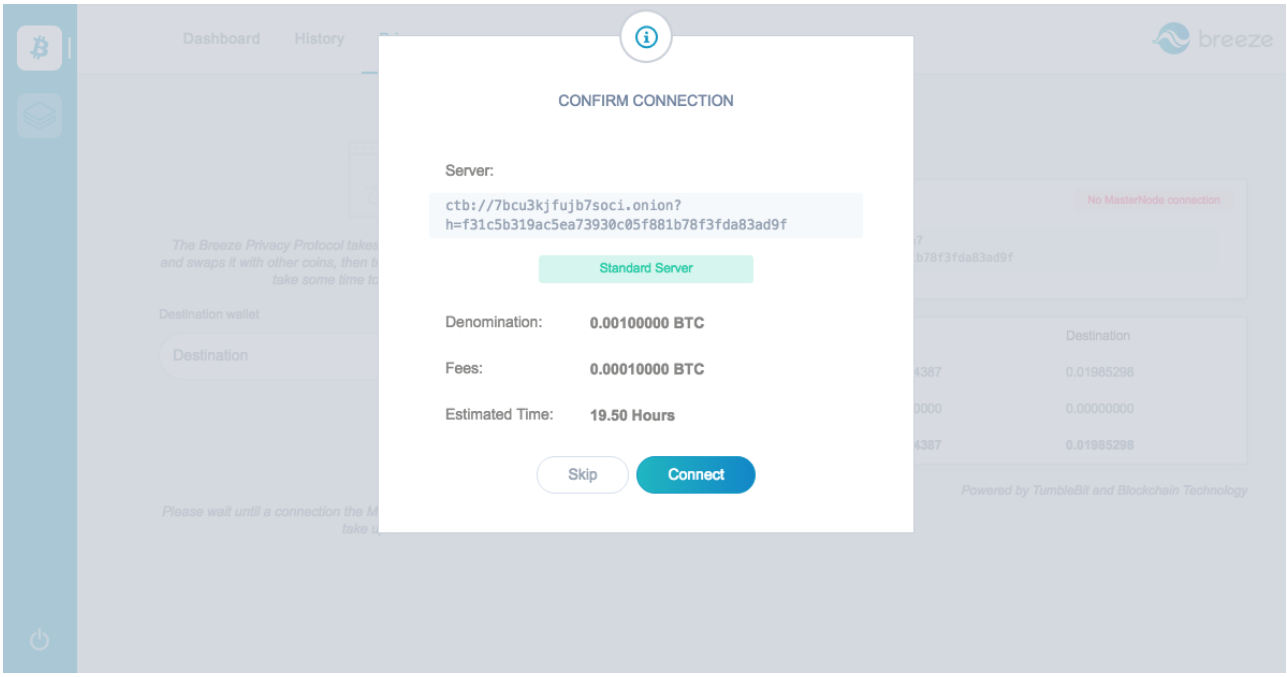
- Wait for the Bitcoin wallet to be fully synced.



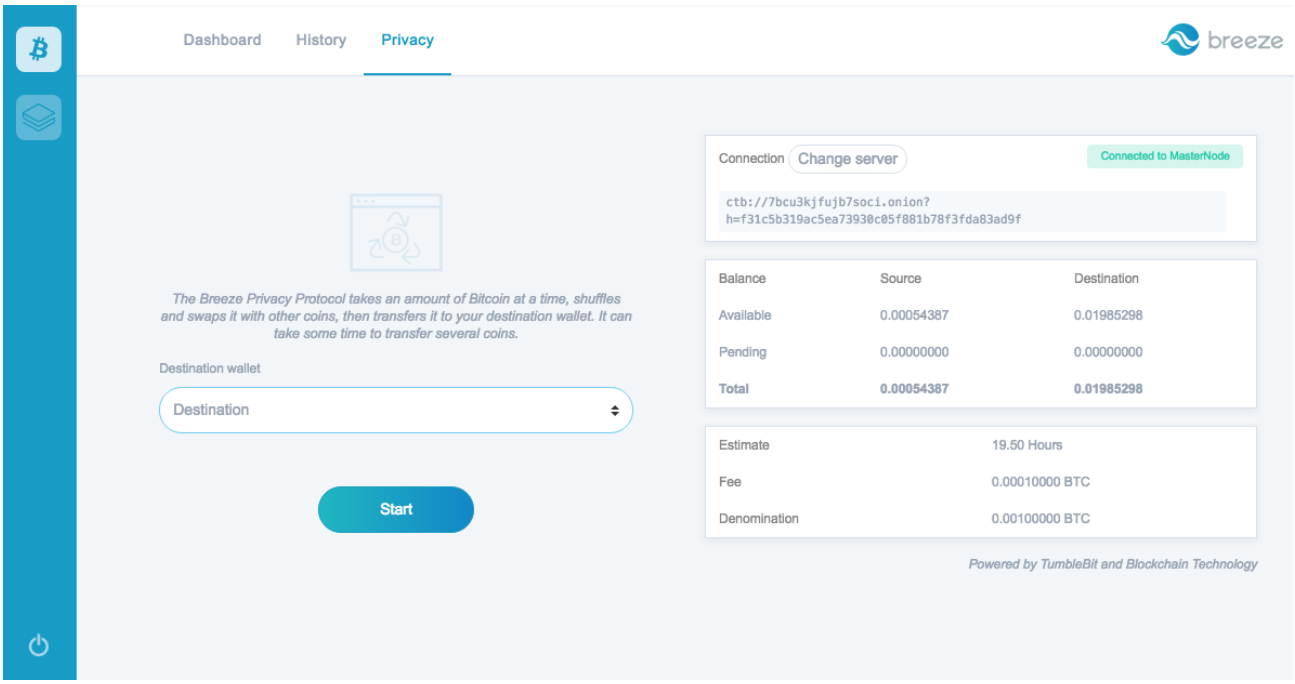
- Allow the wallet to discover available Breeze Masternodes. Masternodes will be fully discovered when the Bitcoin and Stratis blockchain are fully synced.



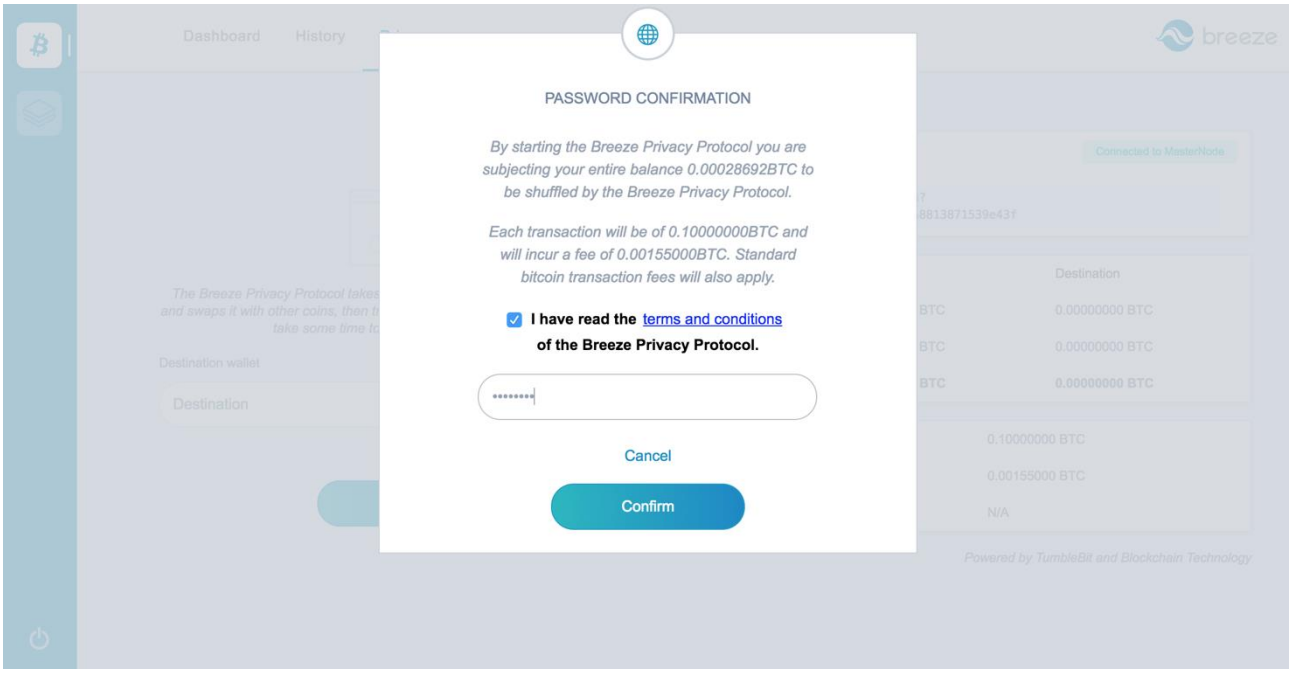
- Connect to the Breeze Masternode. This can take several minutes and assumes Tor network is running.



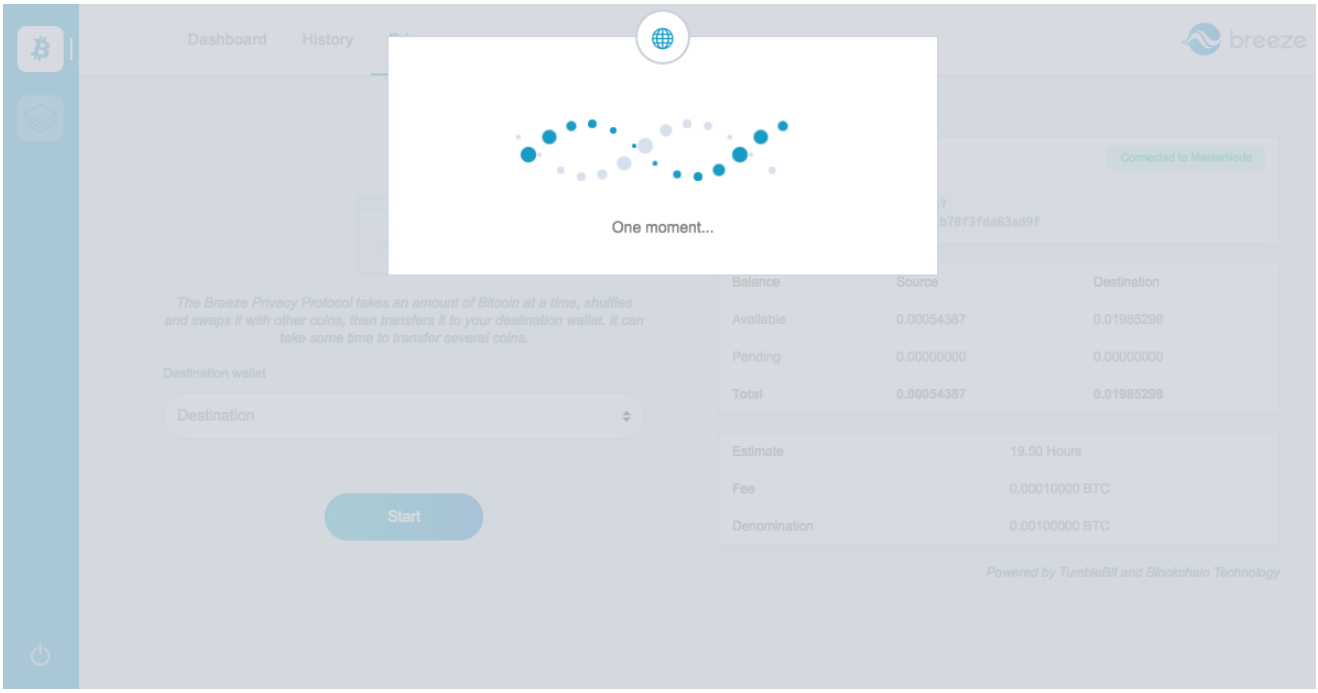
- The following screenshot shows what you will see when a connection has been made to the chosen Stratis Masternode.



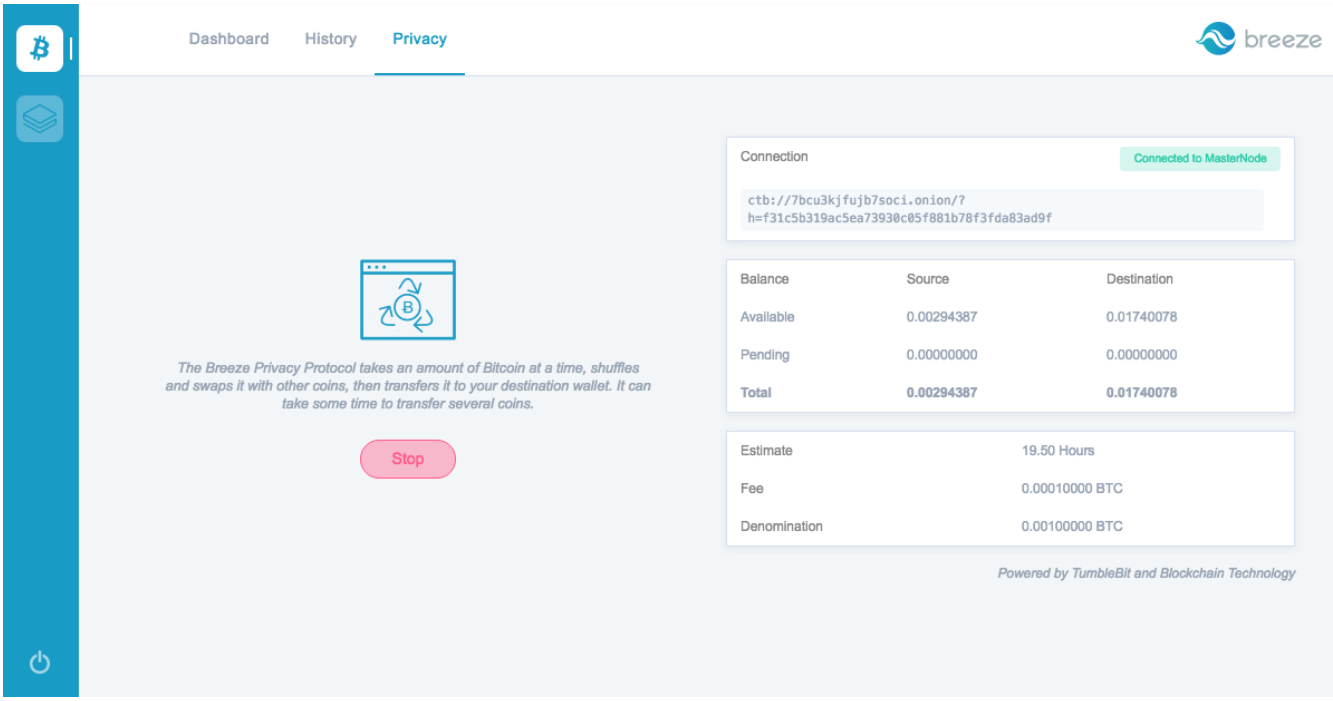
- Press **Start** to initiate the Privacy Protocol. Make sure you read the terms and conditions before ticking the checkbox and enter your password to begin.



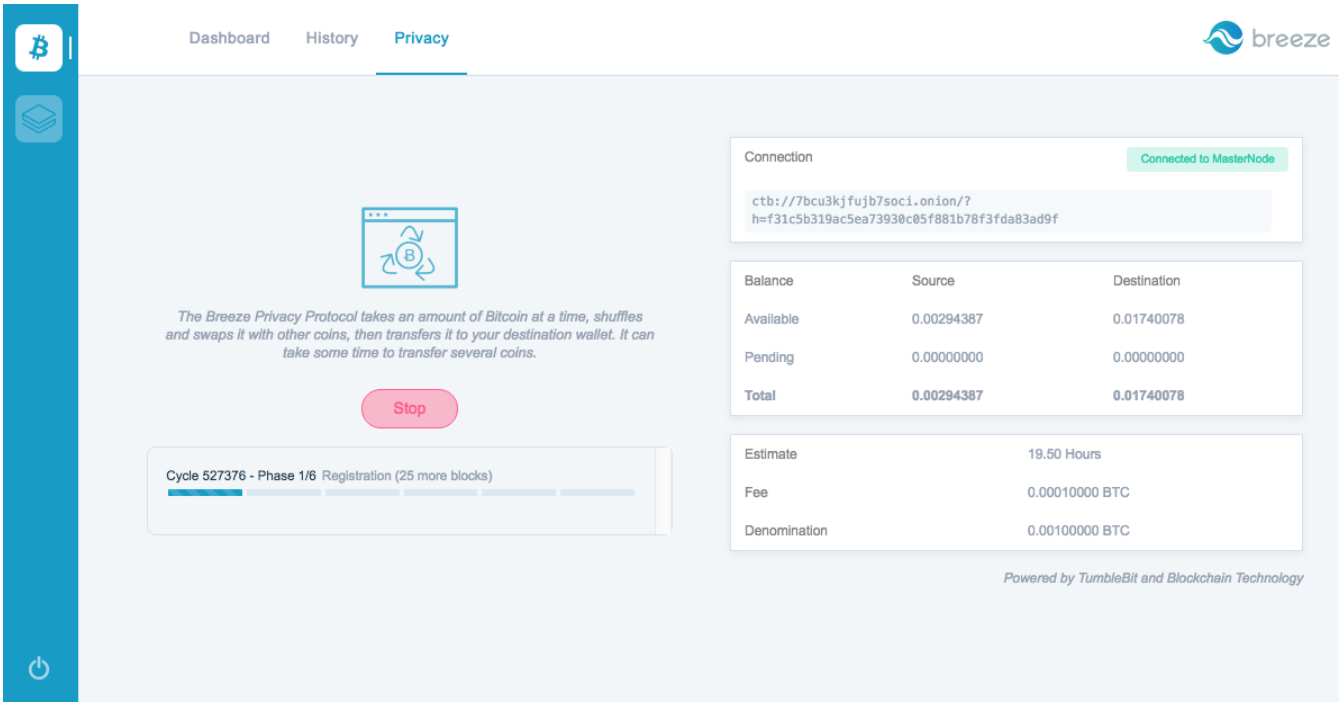
- A connection will now be established and the creation of a cycle will begin.



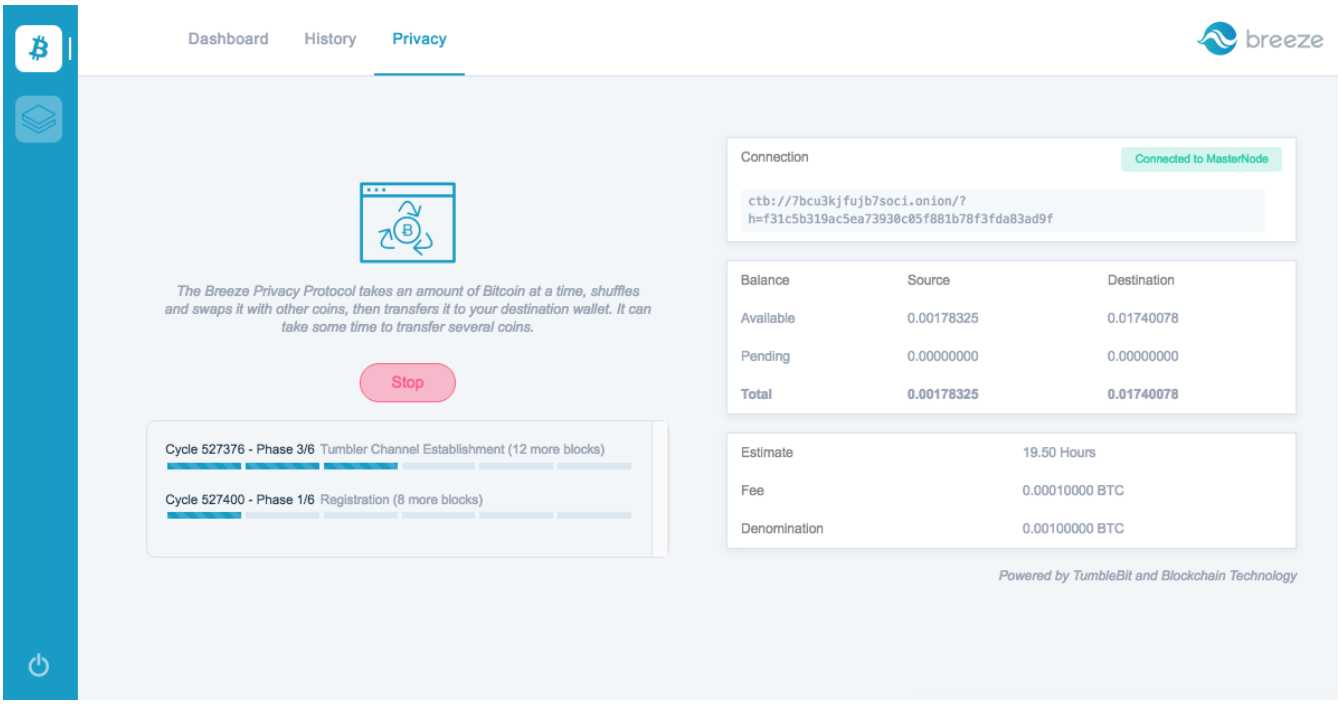
- Creating the first cycle.



- Cycle has been created.

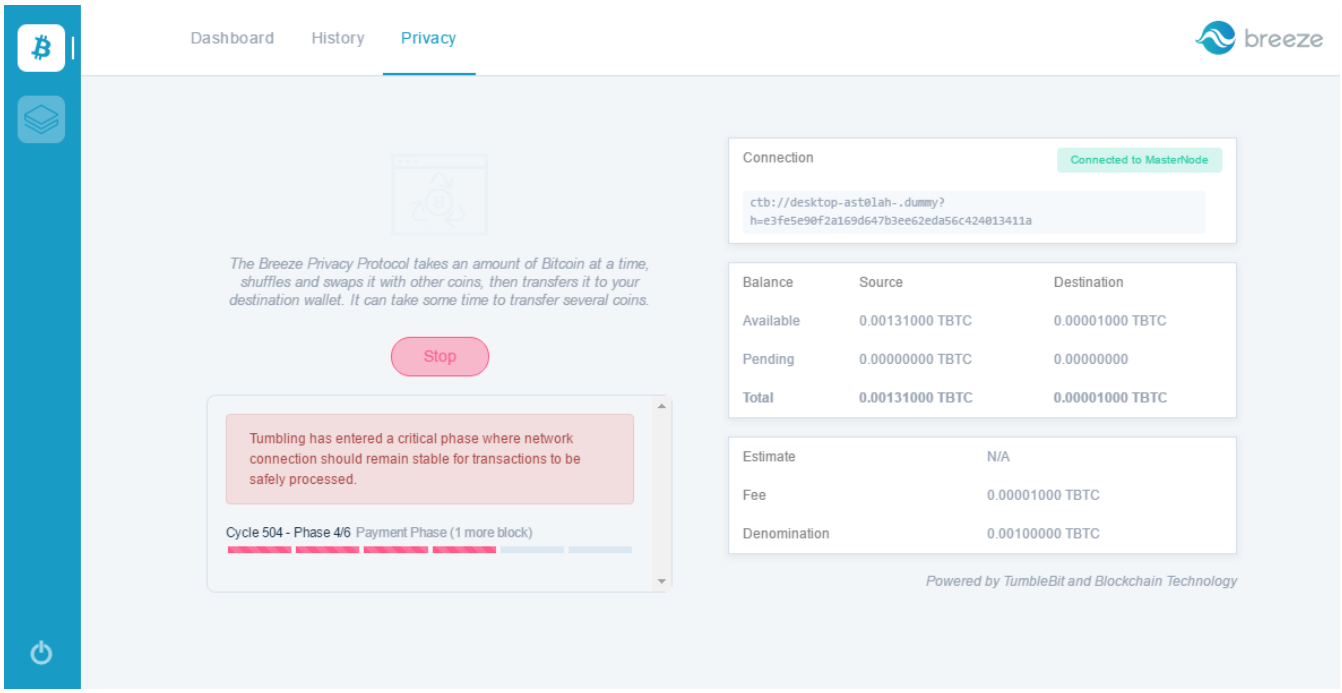


- Two cycles running. Be patient as the cycle creation process can take quite some time.



- Any cycle entering the critical phase requires a stable network connection, complete loss of connectivity and/or power failure during this phase may result in the loss of funds.

  The progress bar will be highlighted in red to signify you are in a critical stage of the cycle.



> *Warning:* Ensuring your client remains online during this phase is critical. If you have an unreliable power supply, it is recommended that you utilize a UPS that can provide at least an hour of up-time to cater for any interruption during this period.

3. Good to Know

- Ensure that the source wallet only contains the Bitcoin balance to be shuffled as the entire Bitcoin balance available in the wallet will be subjected to the Privacy Protocol.

- It is recommended to use a newly created destination wallet with zero balance. This ensures the destination will only contain coins that have all been subjected to the Privacy Protocol.

- The wallet needs a stable environment and needs to run continuously. Therefore, avoid letting the machine go into Sleep mode and disable any automatic OS updates as there are critical phases that require up-time.

- When connecting to a Breeze Masternode ("server"), you are informed whether it is a standard server. A standard server follows the recommended settings for *Denominatio*n and *Fees* (and any other settings) to ensure a higher level of privacy for all participants.

- There is a 3-day expiry period for funds locked in escrow. This means your source wallet needs to be reopened within 3 days of a failed cycle in order for refunds to be issued automatically back to the source wallet.

- The *Denomination* is the unit of coins that will be shuffled per cycle, and the *Fees* are the estimated Stratis Masternode fees incurred for each cycle. Note that these fees do not include the network transaction fees.

- The wallet stops cycles if the number of Bitcoin peers drops below 4 while any cycle is entering or executing the Payment Phase (see section 4). If the wallet remains open, cycles will automatically resume once the number of Bitcoin peers goes back up to 4 nodes.

4. Phases

Each cycle consists of 6 phases that run consecutively in the following order:

1. **Registration Phase**: The destination client registers for the cycle and gets an unsigned voucher, which, when later signed, will serve as a proof of escrow.

2. **Client Channel Establishment Phase**: The source client creates a time-locked escrow with the Stratis Masternode based on the Denomination amount plus the Stratis Masternode

3. **Fee**: The client then blinds the voucher received in the Registration phase and asks the Stratis Masternode to sign the voucher.

4. **Tumbler Channel Establishment Phase**: The destination client unblinds the signed voucher and gives it to the Stratis Masternode. The Stratis Masternode now knows that a source client made a corresponding escrow. The Stratis Masternode can now create a time-locked escrow with the destination client based on the Denomination amount. The destination client asks the Stratis Masternode for a puzzle to solve against the Bitcoin escrowed by the Stratis Masternode. The escrow is now complete.

5. **Payment Phase**: The source client transfers money to the Stratis Masternode through the puzzle solver protocol. Funds are withdrawn from the source client. **This is the most crucial phase where the network connection should remain stable in order for transactions to be safely processed.**

6. **Tumbler Cashout Phase**: The Stratis Masternode simultaneously does a cashout by claiming the escrowed coin of the source client.

7. **Client Cashout Phase**: The destination client, armed with the solved puzzle, can cashout the coins escrowed by the Stratis Masternode with the client cashout transaction. Funds get transferred to the destination wallet.

5. FAQ

1. Why does a cycle take so long to complete?

- Each cycle is divided into 6 different phases (see section 4), and each phase transacts and then waits for a number of blocks before confirming completion. The phases are intentionally prolonged for a number of reasons:

    1) Wider Participation: Given that everybody may not perform the registration phase at precisely the same time, prolonging the phase allows as many clients as possible to participate. The more clients that participate in the phase, the higher the level of privacy for everyone.

    2) Node Stability: Having multiple blocks for each phase spreads the processing load on the server side. It also allows for variances in block times.

    3) Connection Safety: Clients may experience connectivity problems with the Tor network during the course of a cycle. Therefore, having longer phases gives a wider safety margin during which connectivity can be re-established.

2. What happens when the cycles have completed?

- The Privacy tab should allow users to start a new session once all cycles have completed. After the cycles have completed, it is recommended to log in to the destination wallet and check that the balance matches the *Destination* total (on the source wallet's Privacy tab).

3. What happens if I stop my current cycles mid-transfer?

- By stopping all current cycles, it may take, depending on the phase, up to 12 hours to reimburse you with any funds that were mid-cycle. **Please note, cycles should not be stopped during a critical phase, this is evident by red progress bars.**

4. Where do my funds go, and will they come back?

- Cycled funds will be transferred to the destination wallet that was selected. If any of the funds were not cycled, they are reimbursed back to the source wallet. The source wallet needs to be reopened within 3 days of a failed or stopped cycle in order for refunds to be issued back to the source wallet.

5. What if a cycle fails?

- The full transfer amount will be refunded to you minus any Bitcoin transaction fees incurred during the cycle. The server refunds the Stratis Masternode fees for failed cycles. The source wallet needs to be reopened within 3 days of a failed cycle in order for the refund to be issued back to the source wallet.

6. Why is it recommend that I create a new destination wallet?

- A fresh destination wallet preserves the confidentiality of the funds transferred to it as it will not have any addresses previously registered on the Bitcoin blockchain.

7. What happens if I lose a connection mid-way through a session?

- Depending on the phase in which the cycle was in, funds are either reimbursed back to your source wallet or transferred to the destination wallet. This process may take up to 12 hours.

8. How do I recover funds lost in escrow?

- The broadcasters are always running so long as there is a Tor connection available. This means users are unlikely to ever need to recover funds manually. If funds are lost in escrow, just run Tor and reconnect the source wallet within 3 days.

9. What do I need to do to verify that I received the correct amount in my destination wallet?

- The *Available* and *Pending* balances for both the source and destination wallet are displayed under the *Balance* box on the *Privacy* Tab. Users can use the *Balance* box to verify the amounts that should be on each wallet and check transactions per cycle using the approximate formulas:
    - Amount Sent ≈ Denomination + Stratis Masternode Fee + Bitcoin Transaction Fee
    - Amount Received ≈ Denomination - Bitcoin Transaction Fee

10. Why does the Breeze Wallet with Privacy Protocol require users to run on Tor network?

- Running on the Tor network removes any link from a user's IP address to any specific Bitcoin addresses. As a result, the link between sending and receiving addresses is scrambled as well. This ensures greater privacy while running the Breeze Wallet.

11. When exactly in the cycles does my Bitcoin get returned?

- During the Client Cashout Phase (see section 4), Bitcoins will appear in the destination wallet.

12. Why can't I see my destination wallet from the dropdown menu?

- The destination wallet needs to be created on the same computer for it to appear under the dropdown in the Privacy tab.

13. What is a standard server?

- Standard servers are Masternodes that have been configured to run the Privacy Protocol using the recommended settings. Users are advised to check the parameters such as *Denomination*, *Fees* and *Estimated Time* in the "Confirm Connection" box before connecting to a server.

14. What do I do if something goes wrong?

- The best way is to get support using the Discord channels or to check the log files in the Logs folder, which can be found here:
    - `~/.StratisNode/Bitcoin/Main/Logs` for Mac and Linux
    - `~\StratisNode\Stratis\StratisMain\Logs` for Windows

15. What is fungibility and why does Breeze Privacy Protocol help keep Bitcoin fungible?

- In Bitcoin, fungibility means that every Bitcoin has the same value regardless of its history. The fact that the transaction history of every Bitcoin is traceable puts the fungibility of all Bitcoins at risk; “tainted” Bitcoins can be valued less. By obfuscating the transaction history of Bitcoins, the Breeze Privacy Protocol improves the fungibility of the Bitcoin network.

16. I thought Bitcoin was already anonymous so why do I need to use the Breeze Privacy Protocol?

- In the current form, Bitcoin is not truly anonymous. By monitoring the unencrypted peer-to-peer (P2P) network and analyzing the public blockchain, anyone can trace the origins of every Bitcoin transaction ever made. The Breeze Privacy Protocol helps users to transfer money between addresses while breaking the link between them using several layers of cryptography.

17. What is special about Breeze Privacy Protocol?

- Unlike existing centralized Bitcoin mixers, the Breeze Privacy Protocol is not capable of linking transactions being cycled and is unable to cheat and steal funds during the cycle. Also, the server does not know your identity, so it cannot reveal it. The Breeze Privacy Protocol is powered by TumbleBit which provides vital security and privacy for users.

18. I am a business that wants to accept Bitcoins - what are the benefits of using Breeze Privacy Protocol?

- Breeze Privacy Protocol obfuscates the relationship between transaction payer and payee. In contrast to traditional on-chain transactions, Breeze Privacy Protocol transactions allow businesses to transact without revealing their list of suppliers to competitors. Payments contained in a cycle's pay-out transaction are untraceable to any single payer. This obfuscates business' customer and supplier lists from competitors. It is particularly useful for individuals and businesses that accept cryptocurrencies and wish to maintain discretion.