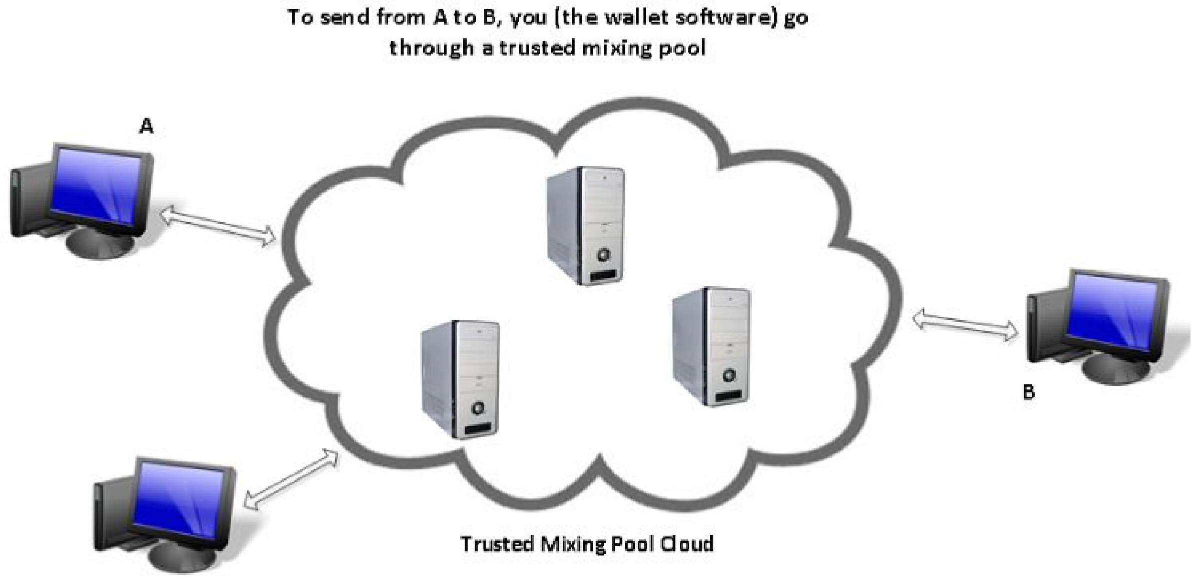
SuperCoin is an innovative X11 PoW/PoS coin, with PoW and PoS superblocks, and with anonymous wallet features. The anonymous send is done through SuperSend technology.

- What is SuperSend?

SuperSend is an anonymous send technology belonging to the Coinjoin catalogue. It is implemented natively for SuperCoin (and may be used by other coins in the future as well). SuperSend uses a cloud of de-centralized mixing nodes. These nodes use the same SuperCoin wallet client, only configured differently. The clients send coins to mixing nodes, mixing nodes mix the incoming coins and also with their own buffer, then forward the coins to the destinations. Incoming/outgoing addresses are dynamically generated and refreshed at regular intervals. This ensures the anonymity of the coin transaction details.


To send from A to B, you (the wallet software) go through a trusted mixing pool
A
B
Trusted Mixing Pool Cloud

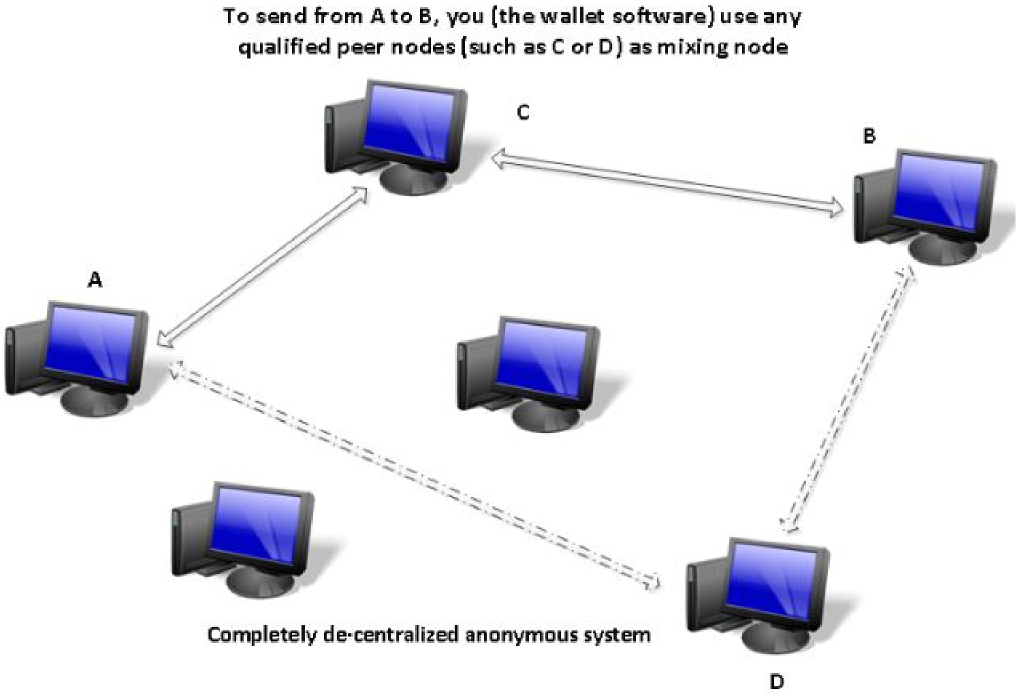
The mixing nodes will be hosted initially by SuperCoin dev team, and can also be hosted by credible mining pools. The anonymous send will be directed to these mixing pools by wallet and mixed and then send to its destination.

Basically the flow goes like this:
A (source) -> {Xi} (i = 1, ..., m), then {Yi} (i = 1, ..., n)->B (destination)

where {Xi} and {Yi} are randomly chosen addresses from a large pool of dynamic addresses.

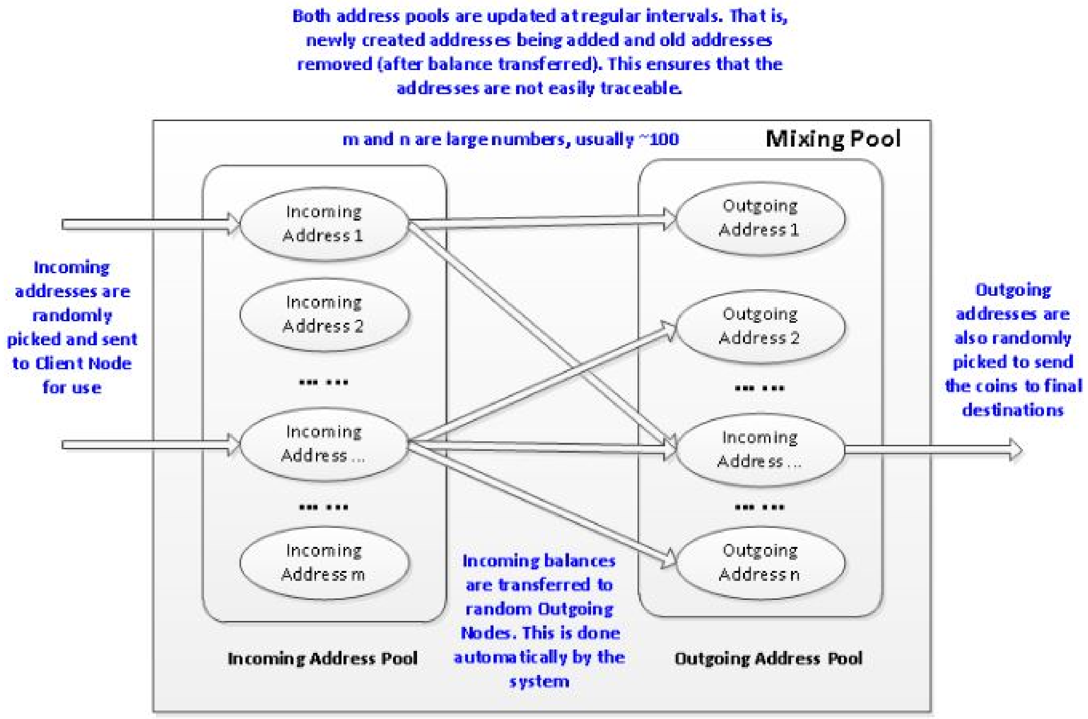
The source amount from A is split randomly into m parts (for now we choose m =1-4, but it will be a configurable parameter), they are sent to m random addresses in randomly chosen mixing pool. The pool, on confirming the amounts received, will send the same amount in n parts to the destination (n can be changed, configured or randomized). The result transaction is not traceable (at least extremely difficult to trace, given the large number of addresses in the mixing pool and dynamism of the addresses).

In the future release of SuperSend each node will be exactly the same, any client will be able to perform the mixer function if some minimum conditions are met. This will be the fully trustless system.


To send from A to B, you (the wallet software) use any qualified peer nodes (such as C or D) as mixing node
C
B
A
Completely de-centralized anonymous system
D

Trustless system is more complex, as you have to assume any party will fraud whenever it can. We designed a great scheme to handle this situation, with mini-escrows, and multisignature wallet addresses and transactions. This is the future of SuperSend.

Now some details on the mixing nodes. The following diagram shows details of processing in the mix pool.



Both address pools are updated at regular intervals. That is, newly created addresses being added and old addresses removed (after balance transferred). This ensures that the addresses are not easily traceable.

m and n are large numbers, usually ~100

Incoming addresses are randomly picked and sent to Client Node for use

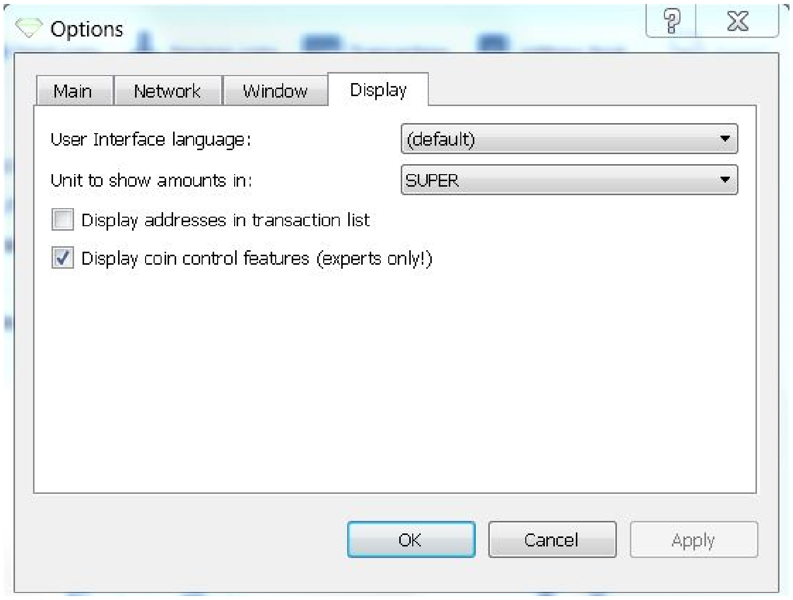
Outgoing addresses are also randomly picked to send the coins to final destinations

Incoming balances are transferred to random Outgoing Nodes. This is done automatically by the system

Arrays of the incoming/outgoing addresses are created and refreshed dynamically, and randomly chosen for each transaction. Incoming and outgoing addresses balance their coins with predefined algorithms.

- How does SuperSend integrated with SuperCoin?

SuperCoin made SuperSend very easy to use. First, there are no complicated configurations to turn on and off the SuperSend feature. Just turn on the Coin Control feature from menu Setting->Options the click on Display tab. Select “Display Coin Control Features” checkbox.



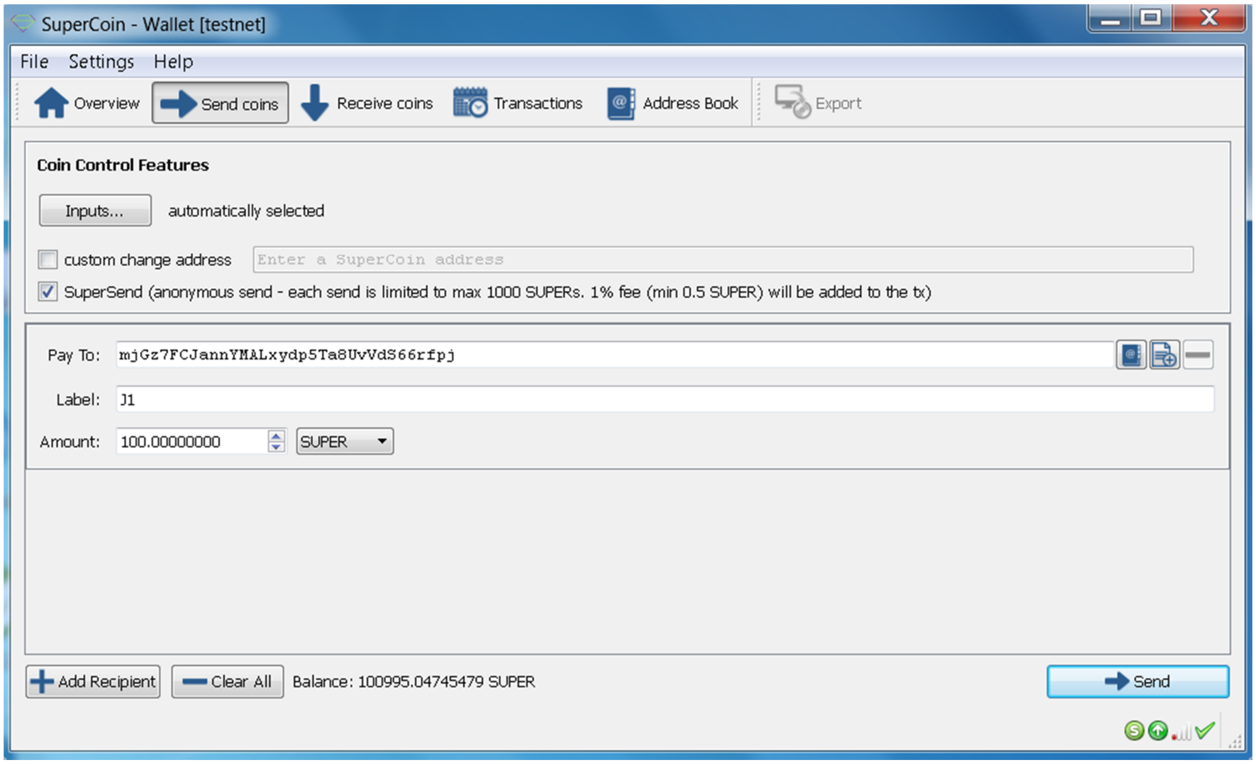
User Interface language: (default)

Unit to show amounts in: SUPER

□ Display addresses in transaction list

☑ Display coin control features (experts only!)

Now you will see in the “Send Coin” tab, the Coin Control features. You will see now the checkbox “SuperSend (anonymous send)” checkbox, at the bottom of the Coin Control.



Coin Control Features

Inputs... automatically selected

□ custom change address Enter a SuperCoin address

☑ SuperSend (anonymous send - each send is limited to max 1000 SUPERs. 1% fee (min 0.5 SUPER) will be added to the tx)

Pay To: mjGz7FCJannYMALxydp5Ta8UvVdS66rfpj

Label: J1

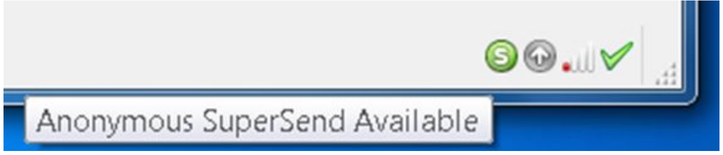
Amount: 100.00000000 SUPER

Balance: 100995.04745479 SUPER

You don’t have to use Coin Control to send coins. When you want to send coins using SuperSend, just select the checkbox. It is very simple: it is based on each send.

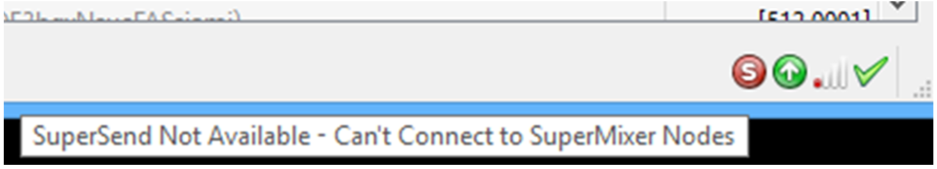
SuperSend will charge 1% fee (with 0.5 SUPER minimum). This fee is provided to mixer. Also it prevents scams with many small amount transfers. The fee will be added automatically to the required sent amount from sender's balance.

On the lower right corner of the QT client, there is a newly added indicator for availability of the SuperSend. The SuperSend is enabled when you have connections to one of the mixers. At this time the "S" icon displays green color.



Anonymous SuperSend Available

If the "S" icon displays red, it indicates that you don't have connections to mixers, so in consequence the SuperSend feature is not available.



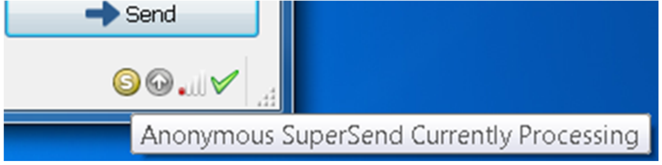
SuperSend Not Available - Can't Connect to SuperMixer Nodes

Despite we have a few mixers in different geographical locations, sometimes due to various reasons you may not be able to connect to one of them. We also provide additional secondary mixers, and you can add them by putting the following in the SuperCoin.conf, and restart qt client:

mixpool = (ip address)

where (ip address) is the ip address of the secondary mixer. You can put multiple lines for different mixers.

If the "S" indicator displays yellow, this means the current SuperSend job is in process. You will have to wait it finishes before make another SuperSend. This yellow indicator will last for maximum 20-30 seconds. So it is just a transition state. If you try to send during this period, an error message will be displayed.



Anonymous SuperSend Currently Processing

- So what about trustless system and de-centralized p2p anonymous system?

Yes this is our phase-2 plan. To make a trustless system, many details need to be done, especially an algorithm that will "force" all parties behave correctly. Today, several coins claim they do trustless system anonymous wallet, for example, CloakCoin. But by reading their "whitepapers" I can ensure you that they don't even know what is a trustless system. Let me describe it in more details here.

A trustless system is characterized by the following rules:

- Each party will do the best they can by gaining (e.g. coins).
- Whenever possible, they will cheat to gain advantages.
- They will not sacrifice their own benefits to do damages (e.g. cheat).
- They will do damages even they don't gain anything (make others lose, but they themselves will not lose, they may not gain either).

So for a system ***A***->***X***->***B***, when ***X*** is arbitrary selected (can meet some minimum requirements), without using special measures (such as multisignature addreses), this will never work. Because if ***A***->***X*** is performed first, ***X*** is not obliged to perform ***X***->***B*** next. ***X*** can take all A sent as his own profit. Similarly ***X***->***B*** cannot be performed before ***A***->***X***, because otherwise ***A*** will not send anything to ***X***, why should he since it is a trustless system?

Some may say this is governed by the client software, as long as you use the software then there is no issue. This is true. But who cannot guarantee that people won't use a fake software X, just by responding purposely to the messages and collect free coins?

A true trustless system, is whatever you do, you cannot gain or make others lose without losing yourself.

With multisignature addresses and transactions, a true trustless system is possible, but it is complex and not obvious. Many seemingly "correct" algorithms are in fact not working. For example, let's take a look at the following algorithm:

1. Client ***A*** makes a request to a randomly select ***X*** for an anonymous send.
2. ***X*** responds favorably and creates a 2-to-2 address and sends it to ***A***.
3. ***A*** makes a deposit (equal to the sending amount + commission) to the 2-to-2 address and also creates a tx T, sending that amount to ***X***'s address.
4. ***X*** sends the required amount to destination ***B*** (***X*** will do so because he wants commission, and ***A*** already deposited and created tx T, sending the amount to him), with transaction S.
5. ***X*** then signs the tx T, and then send the tx S to ***A***.
6. ***A*** verifies tx S, and then sign tx T, so ***X*** receives the sending amount + commission.

This scheme seems fine, because ***A*** deposits the coins first, and creates tx T to send to ***X***. ***X*** has no reason not to send to ***B***, because he wants his commission. After sending to ***B***, ***A*** verifies all, and releases the fund to ***X***.

But this is not really working, because ***A*** has no obligation to complete the last step. Although he will not be able to get his deposit (to 2-to-2 address) back, he can make the ***X*** lose the amount, as (a) the coins already sent to ***B***; and (b) without his signing, ***X*** will not be able to get the coins he deposited. Though ***A*** cannot gain anything from this transaction, he can cause damages to others (in this case ***X***) without losing additional coins on his part. Therefore this is not a working algorithm for a trustless system.

The great news is that we have already designed a working scheme for the trustless system. We of course will not reveal it at this time. Our phase-2 work is in good progress, and we will provide more details in the future. Unlike many other coins, we know what we are doing, and we follow a good plan to the success.