Question w/ regards to SFRX and 5 Second BTC:

“My interpretation is that they will offer a custodian service which will hold your BTC and give the sapphire wallet owner some sort of IOU which can be transferred within this network for no fees in a dex which is...built in the wallet client / native to the chain? And does the SFRX wallet have the private key?”

Main SFRX/EGEM dev (Osoese) responds:

To answer your later question, **NO, the SFRX wallet does not have the private key**.
If it did then you could not trust the receipt of it.
The EGEM (SFRX) address CONTROLS the private key but it does not - “have” it.
The network needs the encryption and a signed transaction from the EGEM address to unlock the encrypted function on the network where it is hidden.
Its hidden in a concept I call "NOT ME"
What that means is ....it’s not buried in my memory.
So, if I am a node, it is buried in my friends memory, but I don’t know which friend
I have an algorithm where the node you connected to contacts other nodes in secret (using encryption), and hides the address/functions using the signature/encryptions from three parties.
But essentially, **the wallet with the EGEM address can then sign a transaction that works to trigger functions on a node that it does not have access to or know how to find.**

The algorithm locates the hidden encrypted address and runs a function on it - and **the most important part is the node running it does not know what it is doing**.
The function is triggered on one node and then routed through the network to another node to call it up and make it happen.
So, even though technically the bitcoin is residing on chain on every node, you can't access it without routing through the hidden memory of a peer
That part was very important because otherwise someone could unplug the computer and dump the memory to get the BTC address.
But since it hops through peers and no peer knows the route (kind of like TOR) and no peer knows what is happening on its run time - that is what makes it secure.
YES it's kind of complex to explain and yes **YOU own the EGEM keys** that unlock it.
That is the whole point.
Let me know if you have any more questions or he needs more explanation!
Pretty soon we will just show him and the code because it will be released 😂.

For the rest of the conversation, this link to the 5 second BTC/quantum swaps proof may be helpful: https://github.com/osoese/5SECPDF/blob/master/5-second-btc-proof-of-concept%20.pdf

There is NO custodian service. Here is what happens...and its shown in that proof above but you have to look at what it's happening in the transaction:

1) Your EGEM address signs a transaction asking for a BTC address to be created on the chain. That is then owned by your EGEM address and operates through on chain signatures from your EGEM address.

2) You can then sign a proof with that BTC address using your EGEM address that says "this egem address owns this bitcoin address" and it is signed - I show these in the PDF.

3) Then you can deposit BTC to that address and it is controlled by your EGEM account.

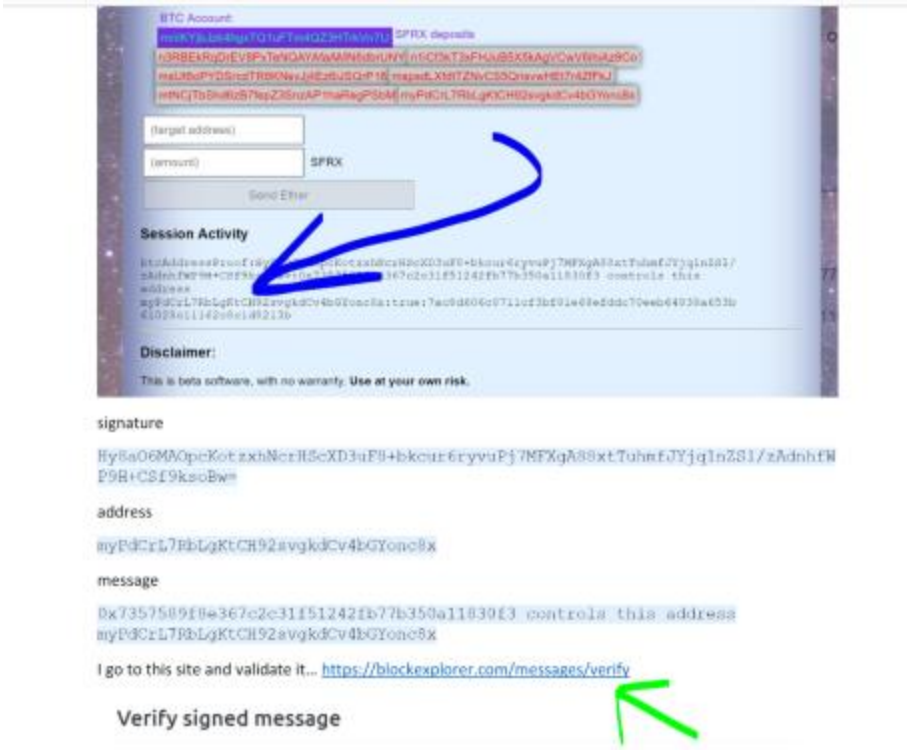
But you do NOT have the private key to the BTC address - it is embedded on the network through an algorithm I developed, encrypted, but you can manage it.

You can trade that BTC on the dex, or send it to any other sapphire wallet. What happens in either case is you end up with a transaction between your EGEM address and the destination EGEM address....

4) You transfer ownership of the BTC address (or part of the BTC address to the recipient if you split the funds) and then the recipient can now control the BTC address.

They can sign a proof that says THIS RECIPIENTS EGEM ADDRESS OWNS THIS BTC address.

Images below (and on github proof page) verify this work.

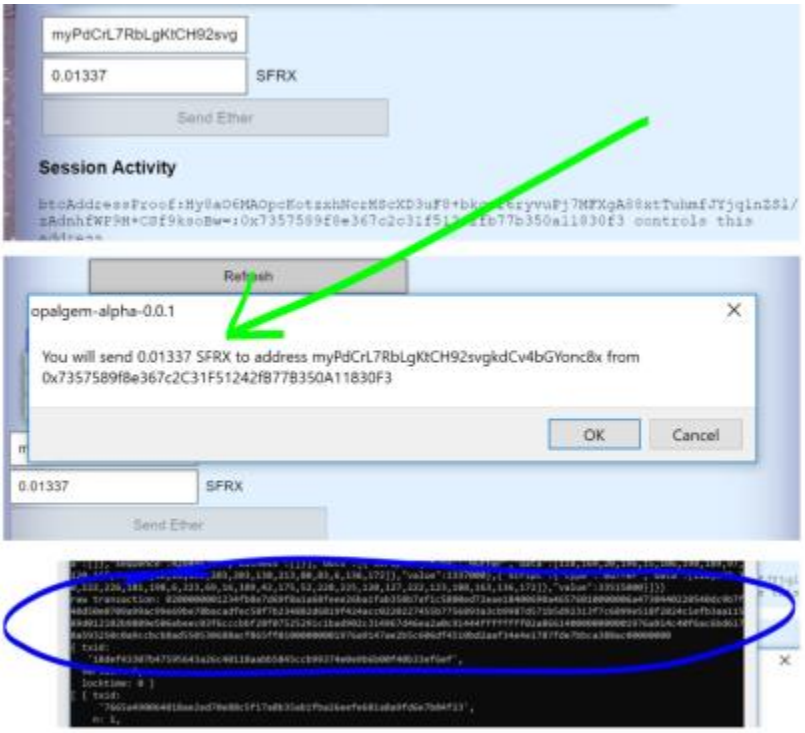


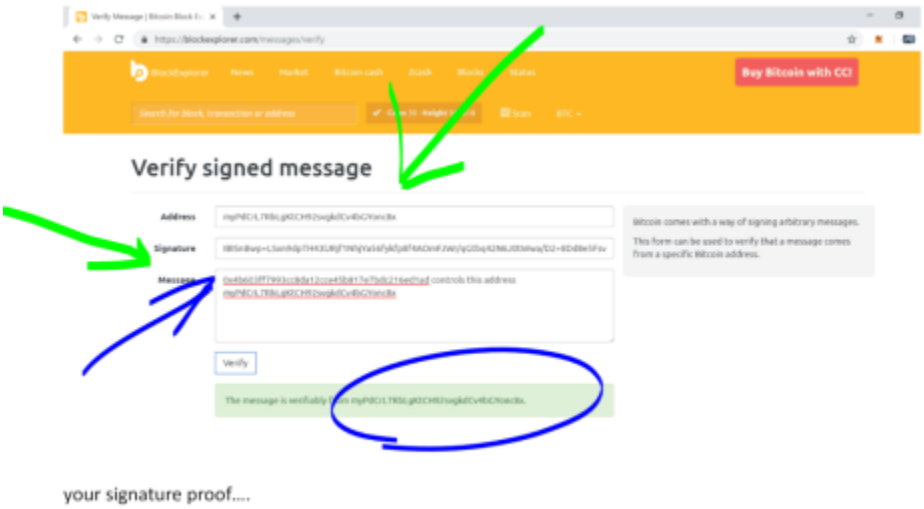
I show you the signature and the parts to put into the verification website for both signatures.

Here is the first signature verification; look and see it was signed by that bitcoin address.

And that EGEM address.

The image says SFRX but it WAS Bitcoin. SFRX is a typo.





your signature proof....

Then, this is the same Bitcoin address but a recipient EGEM address. And there is a SFRX transaction record also. Now that recipient controls the Bitcoin address. And since you never had the private key, he can

trust it. You own nothing but control everything. That is how it works in a nutshell.
This process is explained in the paragraph above the pictures in the “NOT ME” memory.

Extra Note: I started with BTC to my own EGEM BTC address, which I then send to the system generated bitcoin address that my EGEM address owns, and that I can trade to someone else, but this is not the 5 second bitcoin – it could have originated from any BTC address.