SPXED

SPHINXCOIN-DEX

[SPXED]

The Draft

Version: 0.1

By: MegaCrypto

February 19th, 2019

Quick Intro

When I started my first crypto project was last October, SphinxCoin 10 or SPX10, my idea behind it was to introduce what I like to call a “crypto-basket” coin, in which 1 SPX10 represented multiple coins. I launched the project, and I was aware that the method I set forth to obtain the SPX10 was very tedious, but I could not risk any other way to provide SPX10. In short, one had to make ten transactions from ten different coins in order to obtain the SPX10 wanted …. no way anyone would do that :)

To cut a long story short, while I was working on a solution for the SPX10 selling obstacle, I came across a training course that explains how to build a blockchain from the ground up, not a fork, not a token, but absolutly your own blockchain / cryptocurrency. So, I halted the SPX10 project and started looking into writing a blockchain, my own blockchain … and this is what I did, or rather doing right now.

SPXED, which comes from SphinxCoin-DEX, which in short would be SPX-DEX, which then I played around with it to reverese the DEX to XED, and ended up with SPXED (the X is common in both words – if one would call SPX and DEX words!!). So, SPXED is my own blockchain written, again or rather being written, from scratch.

SPXED

My problem with SPX10 was that there was no tool out there that can ease the process of moving coins across chains. Yes we have “atomic-swaps” and other services that enable the “swap” from blockchain to another in what seems to be a seamless transaction, still I wanted to dive in and bid my bid in the “DEX” scene. My goal is to end up with a decentralized platform, of course using blockchain / distributed ledger (DLT), that will allow the movement across any digital asset blockchain, and not just crypto-currencies ... eventhough the immidiate target is to cover the crypto-currencies spectrum. Not only that, SPXED should be as much as possible decentralized, that part I’m still working on … it’s not that simple :)

Roadmap … sort of

Right now I have the "alpha" release online with only one algorithm supported, which is "ethash". SPXED now should be able to conduct any transaction across any ethash-based coin, given that they have a public RPC node that I can point SPXED to it … and does work with the standard rpc-commands of ETH (Im actually using nodejs and web3js to make the transactions). So, if the coin works with those, then it can be added to SPXED right now. At the moment there are 15 coins listed on SPXED:

Akroma	AKA*	EtherSocial	ESN	Nilu	NILU
Atheios	ATH	Ethereum Classic	ETC*	Nekonium	NUKO
DubaiCoin	DBIX*	Ethereum	ETH	Pirl	PIRL
EtherGem	EGEM	Ether-1	ETHO	Ubiq	UBQ
Ellaism	ELLA	Expanse	EXP*	Victorium	VIC

* These nodes are running locally, where as the others are using public rpc nodes.

So, my roadmap is basically:

1) Launch the alpha platform (what I'm doing right now)

2) Either:
   - Complete the Peer-2-peer protocols,
     or
   - Complete the inclusion of other algorithms,
     and
   - Release the white paper and source code

   I'm still debating this, on one hand completing the P2P layer will make the project "decentralized", and on the other hand, adding more algorithms to the trading base will give the platform more momentum …. still haven't decided which way I will go!!

   The source code will be released with the release of the P2P layer.

3) This comes after finished both the P2P layer and inclusion of a good variaty of algorithms, then will come the "client" interfaces, which will mostly be mobile app to easily communicate with SPXED … and I say communicate, because client-app will have to be able to connect to multiple nodes running SPXED, based on a few criterias that I will explain more in details in the white paper.

4) Of course to have a legit working exchange, it should have some level of compliance with KYC/AML standards, so that would be my next stop to complete!

So we have:

- Exchange platform (now in alpha release)
- Multi-Digital-Assets accomodation
- Distributed / Decentralized network
- End-user apps
- KYC/AML compliance

My traget to finish the P2P and have it up for testing is 3-4 weeks.

For the addition of algorithms, I'm giving each algo 1-2 weeks the most to write its interface, and mostly I will focus on adding SHA-256, Equihash, and ERC20 tokens at first. Of coruse, once the source code is published on github, anyone will be able to add more algorithms to work with SPXED.

The end-user / client app, I'm giving it also around 3-4 weeks to publish a beta version of it.

So, I think within 9-12 weeks from now, there should a version 1 of SPXED working!

What do we have now

SPXED right now can processes cross-chain transactions simply by acting as the "middle-man" in between both sides. Like with ethereum's smart contracts (as far as I understand that's somehow how atomic swaps work … didn't really look much into it yet) where they can hold the funds, or should hold the funds, of both exchanging parties, until both sides make their transfers to a designated account (or contract) and then the contract releases the oposing funds to their respected sides. SPXED, and this is something I'm still working on enhancing, right now does the same. Instead of working on the ethereum network, SPXED works on its own blockchain, and for each incoming "transaction request", a temp address is generated for the sender to send their funds to. SPXED will have, again so far, two types of transactions, and this will be explained in the white paper in details, but for now, there will be:

- **Private transactions:** in which both parties in the transaction are in agreement of what they will exchange and identify each other in their transaction requests, by stating both their recipient's address and their designated receiving address for their incoming oposing transaction.

- **Public transactions:** in which only one side wants to trade a certain digital asset and requests another digital asset in return. This type of transaction is not activated yet in the alpha release.

So, to clarify the process more, Bob and Peter have agreed (off SPXED) that they will exchange Bob's ETH for Pete's ETC as in 1 ETH = 15 ETC. Bob will make his transaction request stating his "originating" chain (which is ETH), his own sending ETH address, the ETH amount he wants to send, and of coruse Pete's ETH receiving address. Bob will also state in his transaction request that he is expecting to receive ETC with the amount of 15, and that these coins should go into his ETC address. When Bob makes his transaction request on SPXED, he will be presented with, what I call, an "intermediary storage address", or ISA, to which he is requested to make his transfer to. This ISA is unique for every transaction request, in order to isolate each transaction's funds from running into eachother. The funds remain in the intermediary address until Pete does the same on his side. Once both sides of the transaction have made their funds into their corresponding ISA's, SPXED then releases the oposing transaction to each Bob and Pete. On average, and of course depending on the network's transaction processing speed of the coins that parties choose (example ETH and ETC in the case of Bob and Pete), I noticed that it will take around 5-10 minutes for both sides to receive their respective funds, and 15-25 minutes for the remainder to the transaction to complete.

SPXED completes a full cycle of transaction on several stages:

- First stage: is when a new transaction request is received, SPXED starts listening to the corresponding blockchain's network and tries to locate the incoming transaction. Once its located, then the transaction request is marked with the according status update (SPXED has A LOT of status updates... as of now there are 17 statuses for a transaction!).

- Second stage: SPXED starts looking into the transaction requests pool for matching requests that carry the same information and have already completed their ISA transfer (stage 1). Once SPXED locates both sides of the transaction, then it releases the corrosponding funds to both sides, and again marks the transaction as "Match completed".

- Third stage: SPXED starts releasing the SPXED transaction fee/commission to the node that executed the successful transaction. Right now the fee is 0.1% of the amount being sent. And again marks this stage completed.

- Fourth stage: SPXED looks into the ISA to see if there is any "dust" remaining in the account, and if any is found, then it is sent back to the "originating" address of the sender.

The transaction right now is overloaded with:

1) SPXED fees which is 0.1% of the coin being sent, and
2) The required blockchain fees used to make both the oposing transaction and the SPXED fees transaction.

   In theory, the transaction should be overloaded with 2x the blockchain's network fees, but unfortunatly that is not the case. If the user for some reason does not complete his initial transfer into the ISA with in prompt time, the blockchain's network fee might vary, and that can result in "insufficient funds" to complete the necessary transaction thereafter, and we need to make two transactions (one to the recipient and another to the node that executed the transaction in the form of fees). Now if we try to set the blockchain's network fees multiplier to 3, and the fees do change while the transactions are still in progress, then what happens is that the amount remaining in the ISA is usually less than the network's fee amount, and SPXED won't be able to remmit it back to its originating address. So I ended up with setting that multiplier to 4x the given blockchain network's fee at the time of making the request, this way even if the fees increase while the transaction is in progress, whatever remains in the ISA will be enough to remmit back to the originating address. Of course this is something that I'm sure will be worked on and tweaked to the best possible formula to avoid spending un-necessary fees.

What now !?

Right now, and it will be very helpful, you can start playing with SPXED at:

https://spxed.sphinxcoin.net

and my advice is give it a try with creating small amount transaction immitating both sender and receiver (that's what I do to test it), and send me your feedback. I usually even use the same address for sender and recipient on both sides and then go and follow that blockchain's block explorer and see how the transactions moved!

Again, SPXED is still in it's very early alpha stage, so do not use it for heavy loads (actually don't know how much load the current VPS can handle, but we'll find out!) and more importantly, **DO NOT USE IT** for high value transactions … not that it won't work, it should work, but for now my objective is to see how the code will handle traffic and at what point it will crash :)

I can always be reached at spxed@sphinxcoin.net in case (hopefuly not) something goes wrong!

