**StealthCoin was launched on July 8th, 2014 as the first Tor network integrated POW/POS coin. Going through a bumpy transition from POW/POS to POS only, the development team quickly responded by upgrading the client to 1.0.2.1 and then 1.0.3.1. The XST team also posted some development updates that have captured the interest of the altcoin community.**
**On July 13th, the XST dev team posted the following:**

**"First, the goal for Stealth Coin is what we call "government resistant" privacy protection. We've already mentioned the principle parts of our plan, but we repeat them here: Government resistant privacy protection has two facets: (1) block chain analysis resistance using plausible deniability cryptography and (2) network analysis resistance using Tor. So where are we in our plans? Well, Tor is implemented and you are already using it, so Stealth Coin is currently resistant to network analysis. For block chain analysis resistance, we already have a proof-of-concept codebase. So we know what the implementation will be and, more importantly, know that it works. Our goal now is to implement it on top of the Stealth Coin protocol..."**

**While this was interesting, I felt further investigation was in order to convey what XST was trying to accomplish in common terms to the average altcoiner. I reached out to "Hondo" on his 10-day development retreat with a few questions.**

**<u>An interview with StealthCoin lead developer, Hondo, hosted by StatDude (@thestatdude):</u>**

(Disclaimer: Hondo asked that we not use certain terminology or specific details of certain items currently in development until their release. Those parts of the interview have been excluded.)

Q: Hondo, StealthCoin currently has the first fully working Tor integration out of the box in a POS-based coin, providing protection from network analysis. Can you speak to what went into this?
**A: Several recent coding all-nighters! Build-in Tor network integration represents the implementation of the network analysis protection phase of our privacy plan for XST. Razor and Neutrino are the only other coins we've verified as having comparable Tor functionality. It's possible to see evidence of the Tor network yourself by opening the StealthCoin wallet console and typing "getpeerinfo". Notice the obfuscated ".onion" addresses, making it impossible to view IP addresses of peers. This part of privacy protection is not limited to address obfuscation. With Tor, it is practically impossible to link the origin and terminus of any communication channel, such that it is not possible to know which peers are in communication.**
Q: Hondo, now that Network Analysis Resistance is implemented, what do users have to look forward to with blockchain analysis resistance technology?
**A: Our blockchain analysis resistance is a technology that obfuscates the sender. Specifically, this gives a sender probable deniability. In other words, a sender may deny sending a specific transaction and it will be impossible to prove otherwise.**
Q: Will this "Stealth Send" be an optional feature?
**A: Use can be optional, but the best thing to do for privacy protection is to move the coins to a new wallet, and leave it turned on. We will release an optional "always-Stealthed" wallet so users who want persistent privacy protection don't have to think about it.**
Q: What happens to these transactions in the block explorer? Can they be viewed?
**A: Those who search will see a "Stealthed" sender address. No one can be sure about an address's balance moving forward. Auditing the block chain becomes practically impossible. However, total money supply can be validated, so this isn't a way to hide a premine. You can still**

**tally the blockchain transactions and subtract any transaction fees that are burned by the network.**

Q: Couldn't an investigator determine who sent what based on changing balances in the block explorer?

**A: No. The challenge to an audit is that a user can spend money without others seeing the debit to the input address. You would only see the credit to the send-to address. The transaction would be recorded, but there would be no way to know which address was debited. The debit would be from a Stealthed address that no one could associate with an input (credit) with certainty. Each Stealthed address would contain a negative balance of the transaction amount + transaction fees.**

Q: So, the sender still essentially shows the spent balance in their address? Both addresses still show the balance?

**A: Yes – however, there are ways to prove an intact balance for a specific address, though. But, it would require the address owner to provide that proof. This could be accomplished by sending the entirety of the balance back to the address in a non-Stealthed transaction.**

Q: For a change of pace: a new user called "stayinanon" posted a beta version of a "Stealth Market" promising it would utilize exclusively XST. What is the response of the StealthCoin dev team to this development?

**A: The Stealth Market of course sounds exciting. These types of decentralized services require supporting extensions from the blockchain of the coin upon which the service is built. We look forward to ensuring that StealthCoin will support these services.**

Q: Thanks for the updates. The pipeline for XST sounds pretty ground breaking and unique! Best of luck in accomplishing it and enjoy your retreat.

**A: Thanks!**

(StealthCoin (XST) – Ticker: https://bittrex.com/Market/Index?MarketName=BTC-XST)
Twitter: @StealthCoin