September 22, 2014

Darkcoin Passes Security Review, Prepares to Open Source

Security researcher Kristov Atlas has concluded his code review and security audit of Darkcoin. He was solicited by the developers of Darkcoin, based on 4+ years of professionally reviewing C/C++ software, to review the code and suggest any changes which could improve the software. Kristov Atlas concluded that Darkcoin's claims of functional anonymity are well-founded. He did suggest a few concerns, which the Darkcoin team immediately fixed (the fixes will be released Monday as part of the next scheduled update to the Darkcoin client). Mr. Atlas' primary concern was that a bad actor could launch a so-called Sybil attack against the network. Evan Duffield, lead developer of Darkcoin, closed this potential attack vector and in doing so also found a way to increase the overall anonymity of Darkcoin transactions.

The new update to Darkcoin, "Release Candidate 5" (RC5), will be made publicly available Monday, September 22. It fixes the concerns raised by Mr. Atlas, increases anonymity, fixes bugs, and improves the user experience by implementing a new interface. After eight months of continuous improvement, the developers of Darkcoin are confident that the currency is finally ready to meet the scrutiny of coders world-wide. Duffield has announced that on September 29, the source code of Darkcoin's Darksend technology will be opened and published. This is the final piece of the overall system to be opened up. Darkcoin will then become the first fully open-source, decentralized, anonymous crypto-currency in the industry.

Future plans include the adoption of a new Instant Transactions technology which Duffield has described in his whitepaper [darkcoin.io/downloads/InstantTX.pdf]. This technology will allow Darkcoin to compete with other nearly instantaneous transaction systems such as credit cards. If successful, such an idea could revolutionize crypto-currencies by providing a decentralized payment system usable in retail stores and other face-to-face situations. The delay between sending and confirming transactions would be reduced from one hour (with currencies such as Bitcoin) to as little as twenty seconds. A future press release will describe the system in greater detail.

The Darkcoin client can be obtained at the website: darkcoin.io

More information: darkcointalk.org/threads/rc5-launch-mandatory-update.2443

1 DRK
Darkcoin

Launched
Jan 18, 2014

Website
darkcoin.io

Community
darkcointalk.org

Coins Ranking
CoinGecko #7
Marketcap #8

Developer contact
evan@darkcoin.io

Community contact
vertoe@qhor.net

About Darkcoin: *Bitcoin works with an unprecedented level of transparency that most people are not used to dealing with. Every transaction that has ever happened is stored permanently in a ledger that is made public for the world to see, forever.*

Darkcoin solves this problem by implementing an ahead-of-time CoinJoin implementation called Darksend. A user that wants to be anonymous can use the built-in technology to utilize the Masternode network to make their transaction nearly impossible to track.

Future Press Releases: darkcoin.io/media.html