

Are Bitcoin transactions really anonymous and is Dash the cryptocurrency anonymity solution? Interview with Dash core developer Evan Duffield.



Evan Duffield
Founder and Core Developer

March 23, 2016

It has become apparent that Bitcoin is not really anonymous. Websites like WalletExplorer.com and Chainanalysis.com claim to accurately identify not only individual addresses, but the entire wallets. Mixing services (also called tumblers) have been used to mix one's funds with other people's money, intending to confuse the trail back to the funds' original source. Since early in 2013, Darkcoin has become synonymous with anonymity but also with the dark side of cryptocurrency. From Darkcoin's initial meteoric rise, quickly reaching a value of \$15, to the level of security and innovation it provides for privacy seekers through its 'Masternode Network' architecture, Darkcoin was designed with privacy in mind by incorporating a 'Mixer' protocol.

Darkcoin was rebranded last year to Dash, and is the number three cryptocurrency in the world used for consumer payments, behind Bitcoin and Litecoin, with the market current price above \$6 and a market cap of more than \$40 million. I interviewed Dash core developer Evan Duffield, an American programmer based in Phoenix, who is the founder of the innovative cryptocurrency, which has a robust international user base, including almost as many nodes than bitcoin itself. Evan is a software developer and owner of Hawk Financial Group. His areas of expertise include machine learning, artificial intelligence, databases, C++, C, Perl, PHP, MySQL, and Linux.

I asked Evan why Darkcoin was rebranded as Dash, Evan said, "It became apparent that our branding was getting in the way of our mission, so we started investigating rebranding. We believe Dash, which stands for Digital Cash, is a great representation of what we want to become." Evan went on to say, "By 2020, we should have a completely working Masternode system and 100% decentralization. Also mobile wallets for sending and receiving money instantly, in a secure way, without having to wait for block chain confirmation. With all of this technology implemented, the goal is to get many small businesses to take Dash directly through mobile devices. This allows customers to buy something in person and walk out 10 seconds later after InstantX confirms the transaction is valid and locks it."

The Evan feels that the two tier network architecture allows Dash to scale without the latency issues associated with the Bitcoin blockchain, and sees Bitcoin as a platform for larger transaction, where Dash with its 3,500 plus servers around the world, as a practical and low cost solution for micro transaction. Evan said, "Dash is a privacy-centric digital currency with instant transactions. It is based on the Bitcoin software, but it has a two-tier network that improves it. Dash allows you to remain anonymous while you make transactions, similar to cash. With Bitcoin, transactions are published to the blockchain and you can prove who made them or to whom, but with Dash the anonymization technology makes it impossible to trace them. Dash transactions are almost instantly confirmed by the Masternodes network. This is a great improvement on Bitcoin's system, where confirmations take much longer because all the work is done by the miners."

A. Lyle Elias
ATMIA Founding Director