Dash

Idea behind currency:

On 18th January 2014, Evan Duffield launched XCoin[1]: a new cryptocurrency forked from Litecoin, with a focus on privacy and security. Its main new feature was the use of the X11 hashing algorithm which allowed the currency to grow in its early stages. Very early in development, XCoin was rebranded as DarkCoin, to highlight the emphasis on security and anonymity. On 15th January 2015 DarkCoin was rebased to Bitcoin and on 13th March 2015, finally became Dash (short for Digital Cash), with this choice being to move towards a focus of a fast cash-like currency for everyday transactions. Dash was designed to have faster transaction confirmations than Bitcoin, and to be more future-proof regarding any development changes. Essentially, Dash was created to combat the main issues people previously had with Bitcoin and other cryptocurrencies: privacy, speed and governance.

Technical differences[2] [3]

Most differences between Bitcoin and Dash can be explained through Dash's two-tier network. Bitcoin relies on a peer-to-peer network where any node can be either a user or a miner. Dash builds on this and introduces a second-tier in the network, made up of nodes called master-nodes. Any user can create a master-node if they have 1000 Dash as collateral, which must be broadcast in a signed message to the network. This money is not locked away, however if it is spent or moved, then the user loses access to the master-node. Master-nodes do not mine, however they essentially act as a trusted layer in the Dash network, which allows for many extra features that Bitcoin does not have:

InstantSend: Transactions have to wait for six new blocks to be added to the blockchain in order to be verified, which takes one hour in Bitcoin. Dash blocks are created on average every 2.5 minutes, so verification only takes 15 minutes. However, master-nodes can further facilitate instant transactions through the InstantSend function. The basic idea is as follows: a group of master-nodes (quorum) is chosen randomly using the hash of the previous block to become the InstantSend authority. Any transactions marked as InstantSend get reviewed by this group and if they are valid, the inputs are locked making it almost certain that the transaction will be added to the next block on the valid chain. This action typically results in five confirmations within 1.3 seconds when using InstantSend, allowing Dash to be used in real-time. InstantSend has recently become the default transaction method so Dash has much quicker transactions than Bitcoin[4].

PrivateSend: The aim of PrivateSend is to obscure of the origins of funds. Although Bitcoin claims to be anonymous, with enough forensic work the funds can be traced. When a Dash user wants to privately make a transaction, the transaction inputs are first split into standard denominations (i.e 0.1, 0.01, etc.). A PrivateSend request is then sent to a master-node which mixes up the inputs with two other users' transactions and then the users' wallets are instructed to pay the transformed input back to themselves in a change address (each wallet allows a user to have 1000 of these addresses). This process is repeated up to 16 times with each round making it exponentially more difficult to trace the funds.

Distributed Autonomous Organization: Any user can pay 0.33 Dash to make proposals within a month, which can be for anything including development changes and marketing. Each master-node is given one vote per proposal ("yes", "no" or "abstain") and if any proposal achieves more than 10% approval at the end of the month, then a superblock is created which allocates funds to the approved proposal/s. The budget of the Dash system is created by taking 10% of all block rewards within each month. Dash has a similar decaying block reward to Bitcoin, with the limit set at 18 million coins, and so over time, the budget from block rewards will decrease, however the hope is that Dash will increase in value and so the actual monetary value of the budget should not decrease. The success of this distributed governance can be shown by an example from 2016[5], whereby distributed consensus and funding was reached within 24 hours to increase the block size; this problem previously plagued Bitcoin for years, eventually resulting in a hard-fork (BitcoinCash). An interesting point to note is that as of October 2016, 73% of all funding had been allocated to insiders of the system[6]. That is fine for early development but if it were to continue, it would result in a more centralized system, destroying some trust in the currency. As of 05/03/2019, there are 4554 active master-nodes and the budget is 6176 Dash.

ChainLocks: An upcoming development change will introduce Long-Living Masternode Quorums (LLMQ). Essentially, these are the same as the quorums used in InstantSend but are larger and last for a longer amount of time. This development will allow the use of ChainLocks: each participating member of an LLMQ signs the first block that it sees extending the active chain. If more than 60% of the members see the same first block, they will be able to lock the transaction in place, removing the need to wait for 6 confirmations. Furthermore, this reduces the risk of a 51% attack as a user would need to own 60% of the LLMQ and 51% of miners to affect the blockchain.

Two other smaller technical differences are sporks and dark gravity wave (DGW). Sporks ("soft-forks") are a way to update the code on the network without creating hard-forks of the chain. When a new feature or version of Dash is released, users update their clients to run the code without activating the change fully on the blockchain. Once more than 80% of users have updated and the team is happy with the changes, members of the core development team sign a message in the network which activates the changes (this can be reversed in the same way). DGW is an open-source difficulty-adjusting algorithm for Bitcoin-based cryptocurrencies authored by Evan Duffield. Instead of changing the mining difficulty every 2016 blocks like in Bitcoin, DGW changes the difficulty between every block which makes it possible to issue blocks with relatively consistent times, even if hashing power fluctuates a lot.

Going forwards, Dash is making changes to allow special non-financial transactions, and allow master-nodes to delegate votes to other users. The main aim of Dash is to become as easy to use as PayPal, and this is currently being realised through the creation of a distributed API (DAPI) that will allow websites to integrate easily with the Dash service for payments.

<u>How is it mined</u>

Much like Bitcoin, Dash uses proof-of-work (PoW), however it uses X11 instead of SHA256 as the hashing function. X11 was created by Evan Duffield and consists of 11 chained hashing algorithms. The idea was to make it more difficult for ASICs to be created at first, so that global hash power centralization wasn't a threat before it could be properly developed. ASICs were developed in 2016 and are now readily available[7]. Dash provides more reassurance than Bitcoin; if SHA256 was broken Bitcoin would break, but 11 hashing algorithms would need to be broken to break X11. Much like Bitcoin, the time between blocks is controlled, but this time is set at 2.5 minutes as opposed to 10 minutes for Bitcoin. Unlike in Bitcoin where 100% of a block reward is given to the miner, in Dash the block reward is split: 10% goes to the budget that is used for funding proposals, and the rest of the block reward along with the transaction fees are split 50/50 between the miner and the master-nodes.

<u>How has it performed</u>

Much like a lot of other cryptocurrencies, Dash peaked towards the end of 2017, with an all-time high value of $1,493.59 per coin on 20 December 2017, before coming back down in 2018[8]. On 28/02/2019, the market value was $81.493 per coin and on 01/02/2019 Dash's market cap was $728,547,564 [9] which places it 15th in the list of cryptocurrencies. Multiple exchanges in Japan have stopped accepting Dash (along with other alt-coins) as they are favoured by criminals and hackers. However, in Venezuela, Dash has become the most popular cryptocurrency, with popular brands such as Subway and Calvin Klein accepting the currency[10]. Its popularity may be due to the fact that Dash has lower transaction fees than Bitcoin, allowing it to service as an everyday cash-like service much more easily. Furthermore, of the 9 cryptocurrencies that Uphold (a cryptocurrency exchange) supports, Dash saw the biggest gains in user holdings during 2018[11], which was largely seen as a tough year for cryptocurrencies due to the previously mentioned crash.

<u>Any major attacks or history</u>

In its early development, Darkcoin had a problem with criminals using the currency on the dark web to buy drugs[12], which prompted it to change its name to Dash and focus more on user-experience and speed than privacy in 2015. Another early issue with Dash was caused by a bug in the software that caused 2 million coins to be mined in the first two days after going online. Master-nodes have a bigger influence on the system than normal miners or users, and with the requirement being that a user must possess 1000 coins to create a master-node, influence over the system was unfairly weighted towards those early adopters who were there at the time of this bug[13]. The Dash core team is confident that the distribution of coins is now healthy, but this does raise the question of whether the use of master-nodes will lead to a more centralized system where the richest users can unfairly influence the direction of development. Furthermore, as ChainLocks have not yet been implemented, there are suspicions that Dash is currently susceptible to a 51% attack, with one user controlling more than 51% of the global hash rate[14].

<u>My assessment</u>

In my view, Dash is a very interesting idea that builds well on top of Bitcoin. It alleviates some of the main issues that Bitcoin has, mainly speed of transactions and how to implement development changes, and seems to be well on its way to becoming a genuine cash-like payment alternative if the success in Venezuela is anything to go by. It has

Dash

implemented a lot of technical improvements over Bitcoin, but has managed to do so in a user-centred way such that it is not invasive or hard-to-use. In the past it has had issues with the dark web and countries such as Japan clearly see it as dangerous due to its anonymity, however I believe this is a problem with most cryptocurrencies and the benefits of Dash outweigh the potential negatives. The two main downsides seem to be the potential centralization as master-nodes have so much control and the current risk of a 51% attack, however it is yet to be seen if these will continue to be problems in the future.

[1] https://blog.dash.org/happy-5th-birthday-dash-6da05af9b5d2

[2] https://www.dash.org/roadmap/

[3] https://docs.dash.org/en/stable/introduction/features.html

[4] https://dashnews.org/dash-releases-historic-0-13-update-with-default-instantsend-privacy-improvements-masternode-overhaul/

[5] https://docs.dash.org/en/stable/governance/index.html#governance

[6] https://iohk.io/research/papers/#NSJ554WR

[7] https://docs.dash.org/en/stable/mining/index.html#mining

[8] https://www.cryptoglobe.com/latest/2018/04/crypto-market-down-q1-2018/

[9] https://coinmarketcap.com/all/views/all/

[10] https://www.businessinsider.nl/dash-cryptocurrency-surges-in-venezuela-as-hyperinflation-explodes-2018-8/?international=true&r=UK

[11] https://www.dash.org/2019/02/27/dash-leads-the-growth-figures-of-the-uphold-cryptocurrency-exchange/

[12] https://www.wired.com/2014/11/darkcoin-and-online-drug-dealers/

[13] https://dashpay.atlassian.net/wiki/spaces/OC/pages/19759164/Dash+Instamine+Issue+Clarification

[14] https://www.reddit.com/r/CryptoCurrency/comments/ae90zd/someone_controls_51_of_dashs_hashrate_currently/