

Introduction to DASH

A two-tier approach to decentralization

Konstantinos Karasavvas

Outline

- Brief history
- Main characteristics
 - Masternodes network
- Instant Send
- Private Send
- Governance
 - Blockchain Budget / Treasury
- Evolution

Brief History

- Launched 18 Jan 2014 as XCoin
 - Part-time, hobby project
 - Bug caused 2M coins to be issued very vast
- Renamed to DarkCoin on 28 Feb 2014
 - Promoted as an anonymous coin
- Rebranded as DASH on 25 Mar 2015
 - Digital Cash
 - Focus on becoming a *practical* currency based on *decentralized* governance
- Currently \$60M in market capitalization (7th)
- Forked directly from Bitcoin's codebase
 - Originally forked from Litecoin (a fork of Bitcoin)

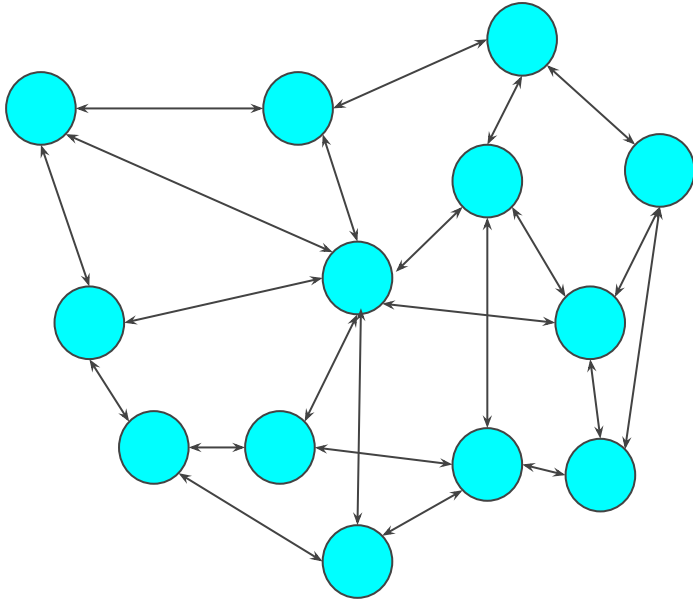
Main Characteristics

- Block reward is about 3.9 DASH
 - 7.1% decrease per year
- Rewarded every about 2.5 minutes
 - 45% / 45% / 10%
- Difficulty adjustment every block
 - Dark Gravity Wave algorithm (impr. of Kimoto's GW)
- Introduced the X11 hashing algorithm for mining
 - Chains 11 different hashing algorithms
 - ASIC resistant... until recently
- Introduced a two-tier blockchain architecture
 - Masternode network
 - Proof-of-Service
 - decentralized services to the network

Masternodes

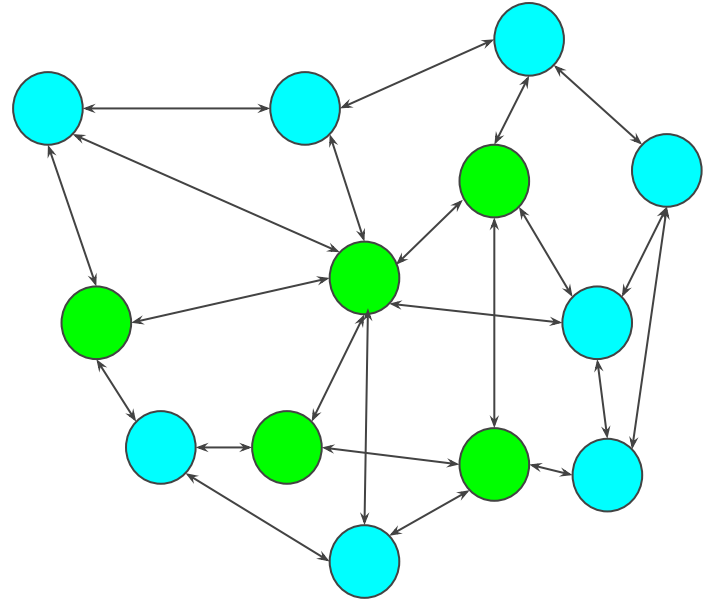
- Mining nodes

Bitcoin



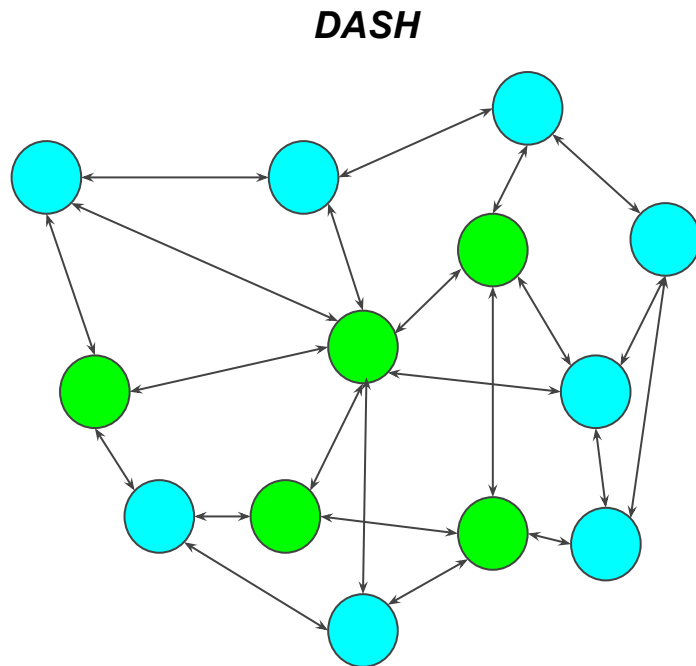
- Mining nodes and masternodes

DASH



Masternodes, explained

- Requires 1000 DASH as collateral
- Proof-of-Service
 - PrivateSend
 - InstantSend
 - Decentralized Governance
- Masternode reward program
 - 45%



Next: PrivateSend

PrivateSend

- Send coins anonymously
- Mixes transactions to obfuscate amounts and addresses
- CoinJoin
 - centralized
- CoinShuffle
 - decentralized
- PrivateSend is also an improved CoinJoin
 - decentralized, chaining, denominations, ahead-of-time mixing

PrivateSend, cont.

- Uses standard denominations to obfuscate amounts
 - 0.1, 1, 10, 100
 - from at least three users
- Uses the masternode network
 - random masternodes is selected
 - then several more to form a chain
- Each masternode waits for more clients to connect
 - similar denominations
- Takes time to aggregate transactions!

PrivateSend, security

- Note (on 11/11/2016):
 - Current masternode count: 4161
 - Current available DASH: 6,875,945
 - DASH used as collateral: 4,161,000

Controlled/Total	Chain depth	% of success (n/t) ^r	DASH required
100/4161	4	0.000033%	100,000
100/4161	8	0.000000000011%	100,000
2125/4161	4	6.8%	2,125,000
2125/4161	8	0.46%	2,125,000

Next: InstantSend

InstantSend

- Send coins instantly
- Uses masternode quorums
 - a set of 10 masternodes is (deterministically) selected
- Instant tx is propagated
 - Quorum masternodes verify and propagate further
 - Funds are locked on consensus
- No one else can spend locked funds

InstantSend, security

- Note (on 11/11/2016):
 - Current masternode count: 4161
 - Current available DASH: 6,875,945
 - DASH used as collateral: 4,161,000

Controlled/Total	% of success $\prod_{i=1}^n ((r-(i-1))/(t-(i-1)))$	DASH required
100/4161	$4.08 \times 10^{-15}\%$	100,000
2125/4161	0.11%	2,125,000
2800/4161	1.89%	2,800,000

Next: Decentralized Governance

Decentralized Governance

- Decentralized budget / treasury
 - 10% of all block rewards
- Anyone can make a proposal!
 - and submit to the network
 - description, mount per month / vote start-, end-date
- Masternode owners vote for the proposal
 - if it passes, proposal owners receives funds
 - votes can be changed
- First successful DAO
 - operating from 2015
 - depending on definition Bitcoin was the first DAO

Decentralized Governance, cont.

- Proposals will typically improve network's value
 - masternode owners are stakeholders
- Examples
 - integrate DASH into Lamassu ATMs
 - create youtube videos to promote DASH
 - pay translators
 - pay developers that enhance the ecosystem
 - create equivalent of localbitcoins for DASH (Dashous)
 - pay core developers!
- Proposals could also stir direction for the network
 - proposal to increase the block size from 1MB to 2MB
 - 24 hours

Next: Evolution

Evolution

- Focus: User friendliness
- Decentralized API
- DashPay
 - Merchants
- Social Wallet
 - Users (username / password)
- DashDrive

Questions?

Website: www.kkarasavvas.com
Linkedin: <https://www.linkedin.com/in/kkarasavvas>
Twitter: [@kkarasavvas](https://twitter.com/kkarasavvas)
Email: kkarasavvas@gmail.com
Bitrated: <https://www.bitrated.com/kostas>