



decred

“Sound Money Evolved”

Jonathan Spence

Table of Contents

- Basics
- Hybrid Consensus
- Fungibility
- Governance
- Treasury
- DEX
- Institutional Interest

Basics

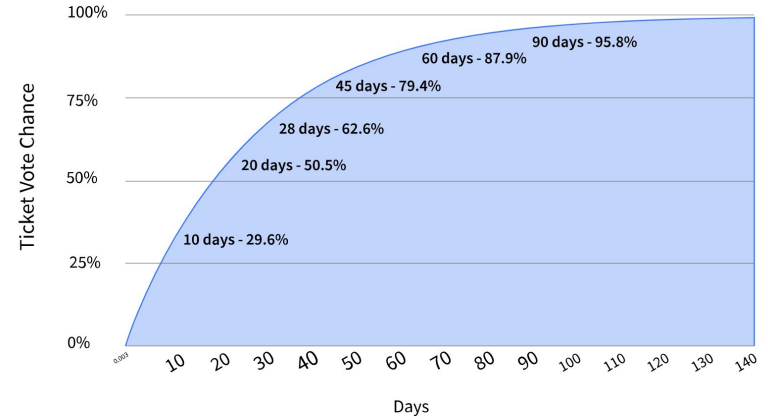
- Native asset: DCR
- Fixed supply: 20,999,999.99800912 DCR
- Slow block time: ~5 minutes
- Small block size: 0.4 MB
- Blockchain size: ~8 GB
- Genesis block: February 8 2016

Proof of Work

- 60% of the block reward goes to miners
- Miners mine and propose a block, Stakers then validate the block
- PoW hash function: Blake256r14
- Difficulty adjustment every 144 blocks or ~12 hours
- Network hash rate: 313,000 Terahash or ~9,000 Antminer DR5

Proof of Stake

- 30% of the block reward goes to stakers
- DCR are used to purchase staking tickets
- Ticket pool size targeting 40,960 tickets
- Ticket price adjusts every 144 blocks
- 5 tickets called to vote (validate) each block
- Average time to vote of 28 days, up to 142 days locked
- DCR are locked while staked in a ticket
- Stake participation: 57% of coins



Proof of Stake Security

- Only 20 tickets can be purchased per block
- Only 2,880 can be purchased before a difficulty adjustment
- It would take a minimum of 3.5 days to acquire 50% of staked tickets
- There are not enough unstaked DCR to do this

PoS Attack

Current total staked is **7,442,909** DCR.

An external % PoS attack would add **7,442,909.35** DCR to the total staked.

New total staked will be **14,885,818.7** DCR.

Attack not possible. Total coin supply is 13,005,277.88 DCR.

The projected ticket price is **369.23** DCR (A **119.61%** increase).

Total PoS attack cost: **\$958,932,954** USD (**7,442,909.35** DCR * **\$128.84** USD/DCR).

Treasury & Proposals

- 10% of the block reward goes to the treasury
- Transitioned from a multisig wallet to a decentralized treasury
- ~\$80 million USD balance



Proposals

In Discussion Voting Approved Rejected Abandoned

Politeia: Pi 2021 Q3 (Proposal System)

lukebp • edited about 1 month ago • version 4

✓ Approved

vote ended 21 days ago

• Yes: 17787 (98.4%) • No: 288 (1.6%)

18075/8216 votes

13 Comments

Design domain budgets: 03.21 - 12.21

linnutee • published 2 months ago

✓ Approved

vote ended 6 days ago

• Yes: 11208 (96.8%) • No: 367 (3.2%)

11575/8279 votes

2 Comments

Video Content Production for Decred Phase 3

exitus • published 2 months ago

✓ Approved

vote ended 6 days ago

• Yes: 16228 (97.9%) • No: 346 (2.1%)

16574/8279 votes

6 Comments



Miner Upgrade

Proof-of-Work



✓ Completed

Current Version:

v8

Upgrade Threshold: 95%

Rolling Window: 1,000 Blocks

Phase Complete



Voter Upgrade

Proof-of-Stake



✓ Completed

Current Version:

v8

Upgrade Threshold: 75%

Upgrade Interval: 530,272 - 532,288

Phase Complete



Enable Decentralized Treasury

Agenda ID: #treasury Voting Interval: 536,320 - 544,383

Enable decentralized Treasury opcodes as defined in [DCP0006](#)

In May 2019, Decred stakeholders approved the development of [a proposed solution](#) to further decentralize the process of spending from the Decred treasury.



✓ Finished

Voting Results:

Quorum: Yes

Abstain 16.72%

No 0.08%

Yes 83.18%

Approval Rating: 99.89%

Locked In: 544,384

Activated: 552,448

The new rules have been activated. Ensure you are running a recent enough software version that supports the new rules. Visit our [Downloads Page](#) to get the latest Software.

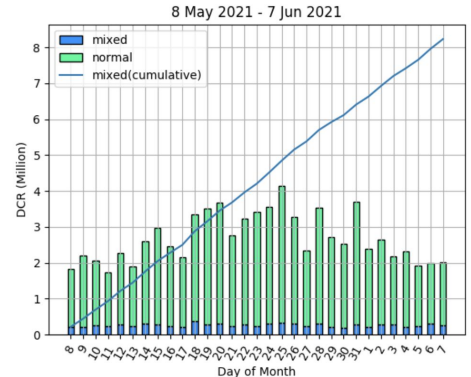
Coinshuffle++ & DCRDEX

- Decred has implemented the whitepaper “P2P Mixing and Unlinkable Bitcoin Transactions” by Ruffing, Moreno-Sanchez, and Kate
- Coinjoin - retains supply auditability
- “Bittrex to Delist ‘Privacy Coins’ Monero, Dash and Zcash”
- DCRDEX uses atomic swaps for peer to peer trades between BTC and DCR
- Currently requires running full Decred and Bitcoin nodes



CSPP_Bot
@CoinShuffle_BOT

2021-06-07 CoinShuffle++ transaction volume was:
271,086 [\\$DCR](#) / 35,889,076 [\\$USD](#)
2.08 % of Circulating Supply Mixed Yesterday (1
DCR = 132.39 USD / 0.00395 BTC)
Total staked in USD: 987,102,620 [#dcr](#) [\\$dcr](#)
[#DAO](#) [#Decred](#) [#bitcoin](#) [#btc](#) [#DCRDEX](#)



Cathie Wood and Ark Investment Management

- “We do have a fund right now only with two currencies in it...That’s Bitcoin and Ether. We’re scouring the scene, some of the custody arrangements associated with others like Decred aren’t quite there yet. We’re picking our spots carefully.” - Cathie Wood, May 2021 - “Cathie Wood SALT talks interview”
- “Decred is promising” - February 2020 - “State of Digital Assets: Keynote by Cathie Wood”