Tweet the talk: @decredproject

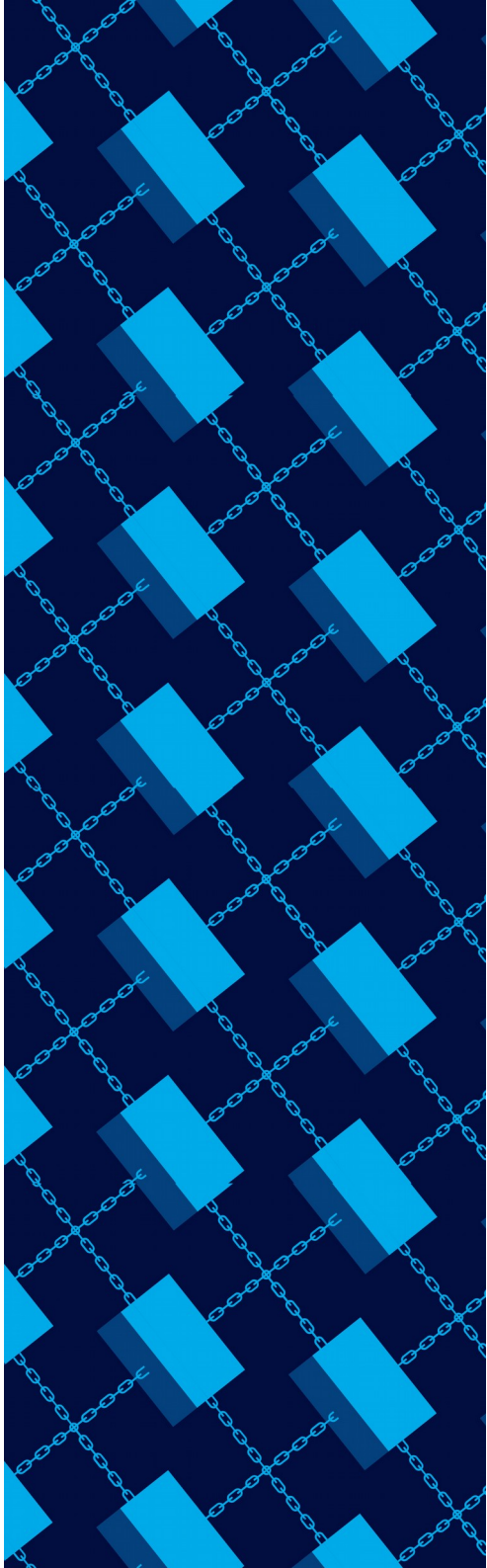
Introduction

Holger Klein
@karamble

Decred Contributor / Frontend Developer

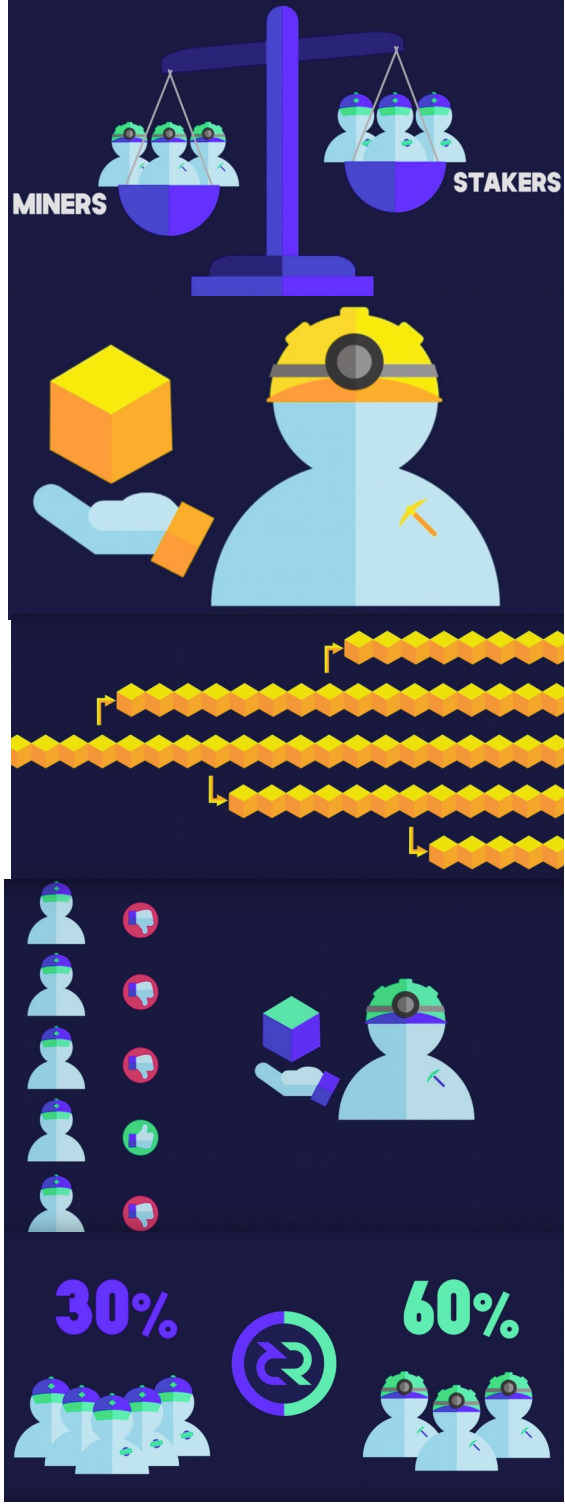
Design Principles

- Created to address a crisis of governance in Bitcoin
- Puts Decred holders in charge of governance, not miners or developers
- Governance system is opt-in and uses Proof-of-Stake
- Development is self sustained
- Tension and incentives



Hybrid PoW / PoS

- Proof-of-Work is a rolling lottery across the hashpower of the PoW network
- Proof-of-Stake is a rolling lottery across the stakeholders, they lock up coins to participate in the PoS voting system
- PoS voting can overwrite PoW and verify new blocks
- PoS miners have ‚skin in the game‘ and receive reward to participate in the voting system
- Pos miners make fundamental decisions about the funding of development and hard forks



PoS System

- Stakeholders can purchase Tickets by locking up funds up to ~4.5 months. Ticketprice depends on demand and size of the ticketpool. Targetsize of the ticketpool is 40960 tickets.

- Tickets go into the ticketpool sitting there until they get chosen by a pseudorandom lottery to cast their vote

- +50% chance your ticket votes between the first 28 days. ~0,5% of your tickets will expire. You can generate ~20% reward annualy

- You can stake ‚solo‘ with a wallet that is online 24/7 or by using a stakepool. Stakepools can only vote on your behalf, they can not access your funds.

Voting tasks

- Securing the blockchain

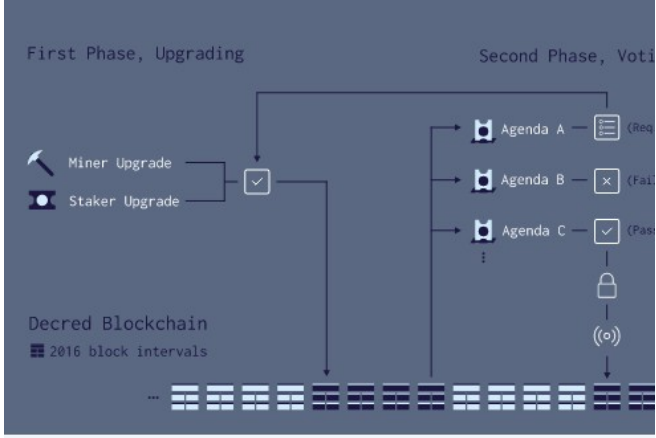
  Each block has to be validated by PoS. 5 Tickets gets chosen on each block. At least 3 votes have to accept the block to validate it

- Hardfork voting

  Consensus voting (hardfork voting) to activate new features and upgrade blockchain functionality

- Proposal and development voting

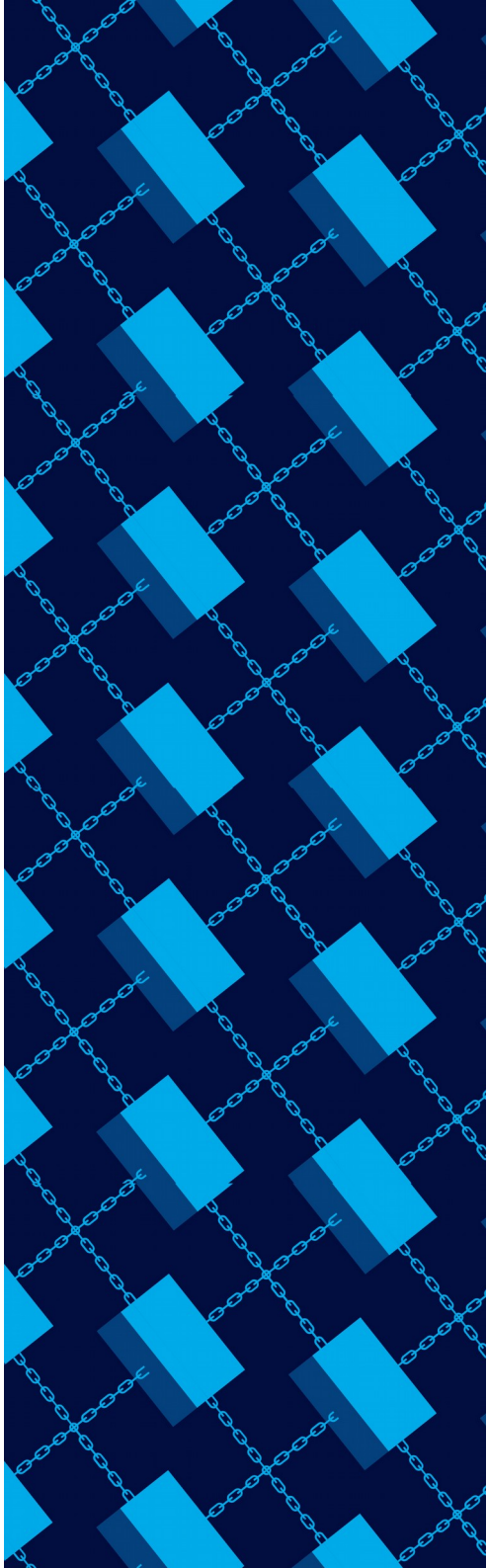
  Development and proposal funding decisions



Consensus Voting

Hardfork Voting

- Software updates have new consensus rules, features and code allready implemented in a dormant state
- Once the network has upgraded to the latest version a vote happens to activate the new features
- On a positive comeout of the voting the new version gets locked in and gets activated (automatic hardfork)



Voting cycle

Hardfork voting

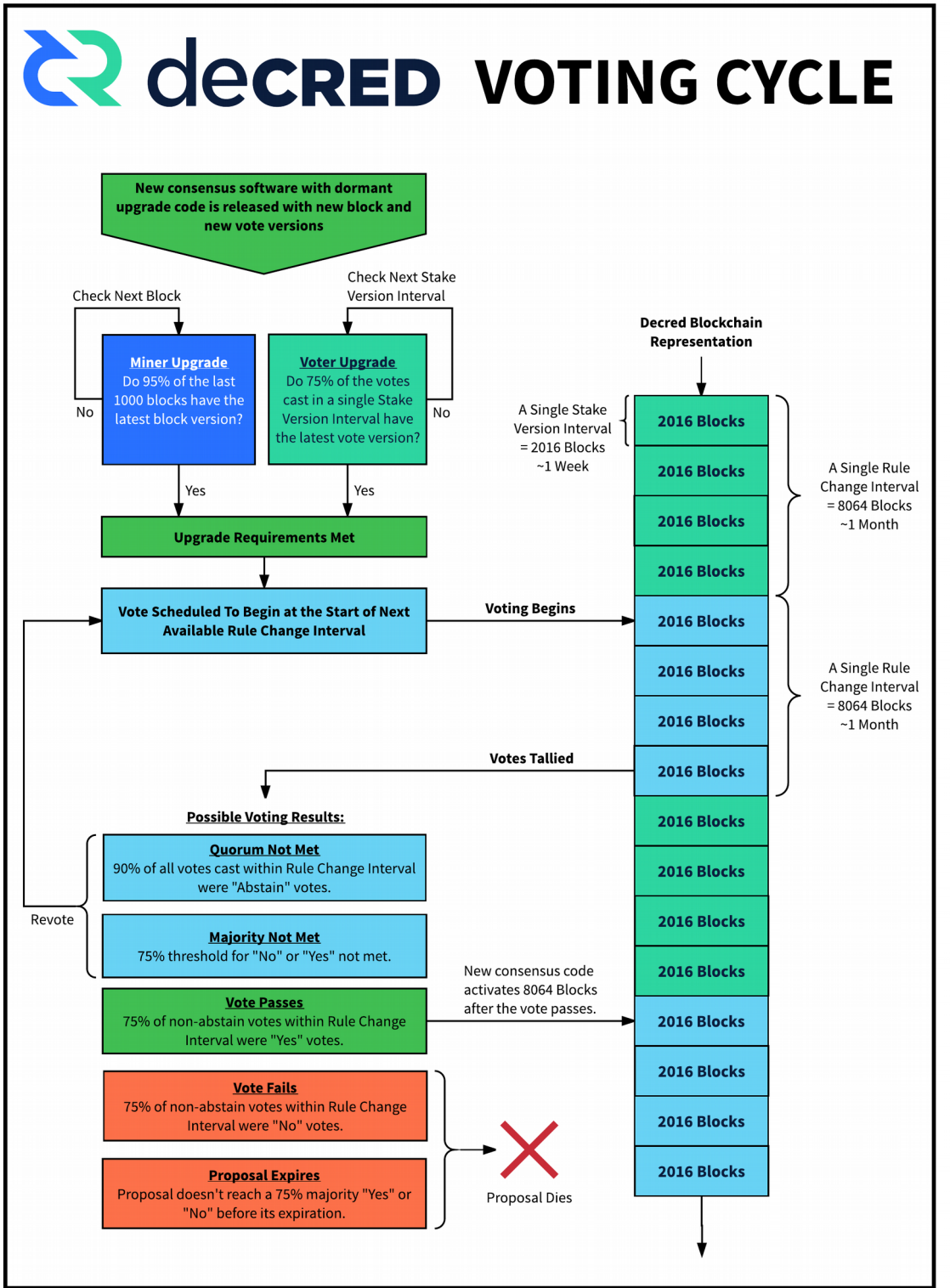
1) Upgrade Phase

2) Voting Phase

3) Lock in phase

4) Activation

5) Enforcement



Voting about proposals and funding

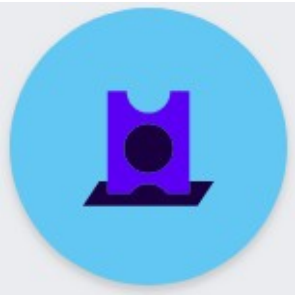
- Politeia
- Currently WIP on testnet, release in the upcoming weeks/months
- Proof of censorship
- Convert Decred into a DAE(DAO)

Decred uses a censorship-resistant blockchain-anchored **public proposal system, which empowers users to submit their own projects for self-funding** from DCR's block subsidy. Politeia(Pi) ensures the ecosystem remains sustainable and thrives.

Learn more about the future of finance at decred.org

Decred highlights

Recent innovations:



- On-chain voting
- Lightning Network
- Cross-Chain atomic swaps

Future:

- Politeia Platform
- Mobile/SPV
- Enhanced user privacy
- Convert Decred to DAE(DAO)

Thank you!

Questions?

Decred.org