SMITH+CROWN

ORIGINAL RESEARCH

Decred

Decred is a governance-focused cryptocurrency designed for peer-to-peer payments, whose hybrid PoW/PoS consensus architecture and proposal system attempt to address perceived shortcomings with development funding and stakeholder influence in distributed protocols.

Overview

Jake Yocom-Piatt, Decred's founder, developed an outlook on Bitcoin while working on btcsuite that would come to inform Decred's development. Bitcoin, in Jake's experience, had an ineffective and inefficient governance structure, lacked funding for protocol development, and inadvertently gave Proof of Work miners outsized influence on development decisions. Decred's design and architecture intends to address these issues, building a cryptocurrency with governance rights for what the project views as a broad array of stakeholders.

The network was launched in February 2016 by the developers of btcsuite, a Bitcoin implementation written in Go. While not a fork of Bitcoin, Decred utilizes several of its design elements. A cryptocurrency designed for P2P payments that utilizes a hybrid PoW/PoS consensus architecture, Decred emphasizes stakeholder governance input through on-chain voting and Politea, a public proposal system used to allocate Decred's $10 million dollar treasury. Proof of Work in Decred contributes to blockchain security through block timestamping, and uses the Blake-256 hash function. Proof of Stake voting provides an additional security layer, as stakeholders' ability to invalidate blocks allows for oversight of the mining process, discouraging secret-and-empty block mining, as well as enforcement of network consensus rules. Decred's implementation of Proof of Stake uses a novel ticket system, where tickets generated by long-term token staking enable holders to vote on Politea proposals and confer a

"Decred's design and architecture intends to address these issues [gridlocked decision making and lack of development funding], building a cryptocurrency with governance rights for what the project views as a broad array of stakeholders."

NOTABLE DEVELOPMENTS

2013
Decred's origins trace back to a 2013 Bitcointalk thread and subsequent whitepaper.

2013
The Proof of Activity whitepaper, co-authored by Litecoin founder Charlie Lee, informs design.

2014 - 2015
Development efforts merge with the open-source software engineering firm Company Zero.

January 2016
DCR airdrop ends, allocating 4% of total Decred supply to early adopters.

February 2016
Decred network launches.

June 2017
Ticket holders confirm the first consensus algorithm change via the governance process.

November 2017
On-chain vote enables opcodes for Lightning Network support.

September 2017
Litecoin founder Charlie Lee completes an LTC-DCR atomic swap.

October 2018
Politea proposal system launches.

Late 2018
Early Politea votes allocates funds to open source research, bug bounties, and PR.

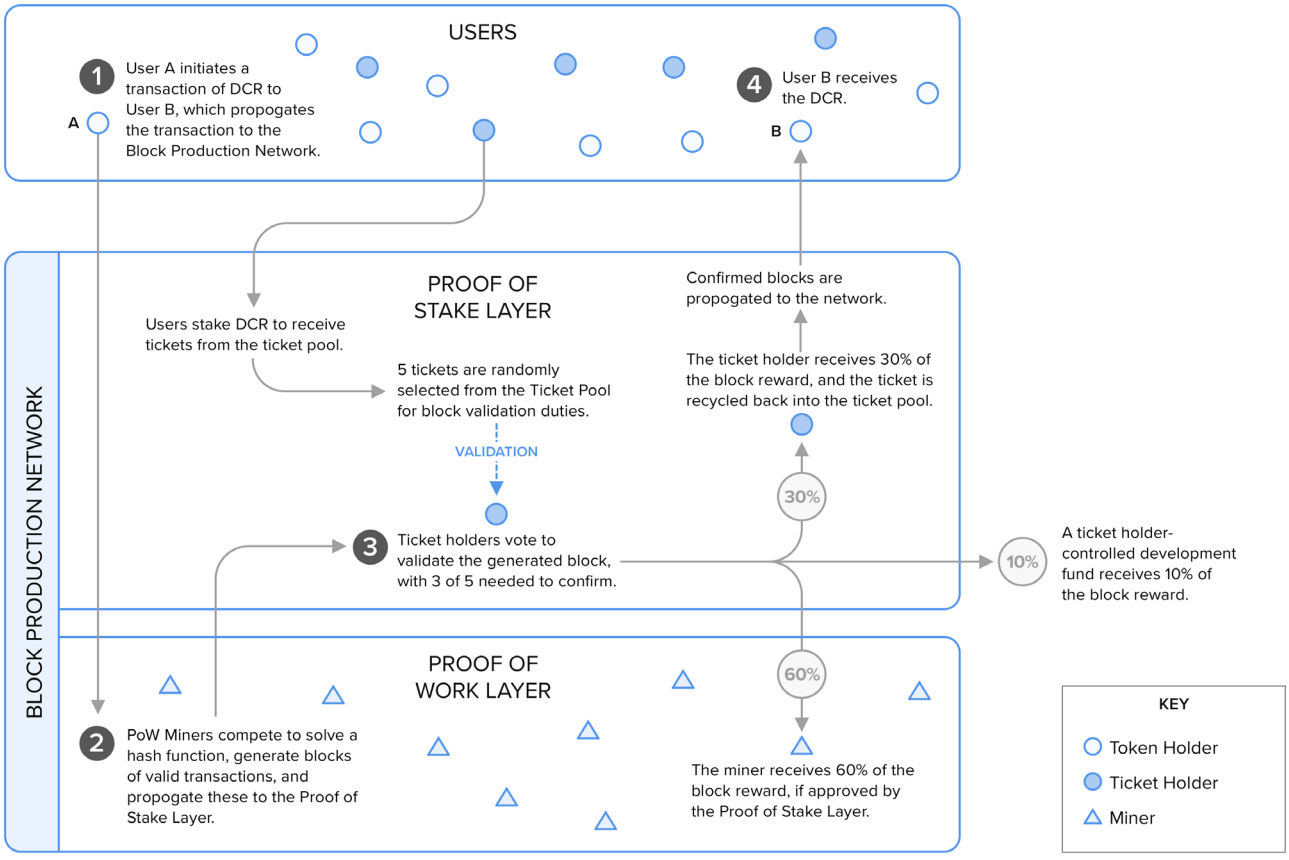
chance of voting upon software changes. In general, Decred has prioritized developing mechanisms for stakeholder input over development of features designed to make the currency, DCR, a more attractive form of peer-to-peer payment so as to remain true to its ideals for governance, although privacy features are included in the project's roadmap.

Decred's initial project development was funded through a developer pre-mine of 4% of the total DCR supply; there was no VC financing or token sale of DCR. An additional 4% was airdropped to the community to spur adoption. Block rewards are split 60/30/10 between PoW miners, PoS stakers, and a development fund controlled by community vote.

The Decred Network

The Decred cryptosystem utilizes neither solely the '1 CPU = 1 vote' of Bitcoin/PoW nor the '1 token = 1 vote' of a pure PoS protocol. Transactions on the Decred network are instead validated through a hybrid PoW and PoS system. At a high level, PoW miners generate blocks that a randomly selected set of PoS validators must validate before the block is appended to the main chain. This consensus architecture is part of Decred's overall goal of giving various stakeholders input in managing the network. PoS validators act as an explicit check on PoW miners; the former can reject invalid blocks or those that use software versions not preferred by token holders. The block rewards are split 60/30/10 between miners, stakers, and the development pool. The 60% PoW miner reward is reduced proportionally

How Decred Functions



Visual elements are for informational representational purposes only and do not accurately portray quantities or ratios of actors within the ecosystem

if the block is not approved by all five randomly chosen PoS validators. Participation in the PoS process is voluntary through a ticket system.

PROOF OF STAKE DETAILS

Decred's ticket system is integrated with the project's PoS consensus layer. DCR holders who wish to participate in the PoS validation and governance process must stake DCR to receive 'tickets', which exist as a non-tradable cryptoasset on the Decred network. Five ticket holders are randomly selected by a Poisson distribution to validate each block that is created by PoW miners.

The opportunity costs in generating tickets is dynamic, varying according to market demand for DCR and Decred's so called 'stake difficulty algorithm.' Staked DCR is refunded once the ticket expires. There is a target ticket pool size of 40960 tickets available on the Decred network, designed such that a ticket will be chosen for block validation duties within 28 days on average. Tickets expire if not selected for block validation after 40960 blocks (about four months); any one ticket has a 99.5% probability of being chosen before it expires. Five tickets are randomly selected for an approval vote on each Decred block. At least three of the five selected tickets must approve the block generated by the PoW miners; blocks failing to gain three votes are orphaned. Once selected, ticket holders who vote on block validation split the 30% portion of the total block reward. Tickets can be delegated to staking pools to provide protection against missed votes— if a wallet with a ticket is not online when its ticket is randomly selected, they lose the staking rewards and that opportunity to participate in blockchain governance. (Ticket holders can still vote on funding allocations made through Politea, however.)

Decred uses an algorithm to determine a ticket price that maintains a constant ticket supply, referred to as the 'stake difficulty algorithm.' The purpose of this is to maintain PoS subsidy returns over time and expected ticket holder influence over the several week timespan that tickets are typically held. Users purchase tickets by submitting the determined DCR price to the network. Up to 20 tickets are available for purchase in each block; in the event that demand exceeds this supply, preference is given to tickets with higher transaction fees. Tickets are eligible to be selected for block validation and voting 20 hours after they are purchased. Short term fluctuations in ticket price are limited an algorithm change implemented in mid-2017.

"The staking mechanism is designed to disincentivize users with only short-term interests in the network from participating in consensus and governance—short-term speculators and day traders of DCR will not be able to participate in consensus or governance without making their holdings illiquid."

Effectively, only a subset of existing DCR is used in the blockchain governance process. Blockchain governance influenced is measured not by DCR balance, but by ticket balance. The staking mechanism is designed to disincentivize users with only short-term interests in the network from participating in consensus and governance—short-term speculators and day traders of DCR will not be able to participate in consensus or governance without making their holdings illiquid.

Indeed, this design aims to tackle a general issue in staking systems: the amount of voting weight to give

exchanges or other large holders. Here, a centralized exchange that holds a large amount of DCR could only leverage that to influence voting/governance if it was willing to lock up their DCR for several weeks. For an exchange that allows users to immediately withdraw deposited DCR, this is unworkable. Further, the ability for large token holders to influence the network by acquiring many tickets is limited, since the ticket price dynamically adjusts according to demand in previous periods. A significant DCR holder would face a rapidly increasing marginal cost to acquire a large supply of tickets over a short time frame. Further, allocated tickets must 'mature' for 256 blocks before they are eligible for staking rights, which reduces the potential for a rapid attack on the network. Generally, Decred aims to minimize the influence of large PoW/PoS pools, exchanges, and individuals with large holdings in the governance and block validation processes.

Decred's consensus process additionally reduces the prevalence of hard forks through long-range attacks. In pure PoW networks, particularly those with low total hashrate, attackers can secretly mine dozens of blocks in advance, eventually convincing the network that their chain is the canonical version. As community contributor Richard Red has noted, Decred wallets do not permit ticket holders voting on blocks that are further than 5 blocks behind the latest. Thus, even if a parallel chain had a significant amount of hash power, it could not cause a hard fork or block re-organizing of more than 5 blocks, since each block must be approved by ticket holders.

One concern in the Decred community is that the rising ticket price (about 110 DCR, as of early-2019) excludes small holders from participating in governance and block validation. To remedy this, Decred will implement a ticket splitter, which effectively allows users to pool funds to purchase tickets. The voting decision of the split ticket is weighted by stake. The splitting process' implementation reduces the variability in DCR's locked duration; as a consequence of the change, users can split their claim over many partial tickets and receive unlocked DCR gradually as those tickets are randomly selected, instead of locking 100 DCR for up to 4 months.

"The percentage of the Decred supply staked as part of the ticket system has gradually increased from 25% in mid 2016 to nearly 50% in early 2019."

STAKING RETURNS

The chart below illustrates the trends in staking and the ticket system in Decred since network inception, and compares the financial returns to staking with two partial substitutes. The percentage of the Decred supply staked as part of the ticket system has gradually increased from 25% in mid 2016 to nearly 50% in early 2019, as shown in red. Given that these staked DCR are locked for an average of 28 days until the ticket is selected, this signals increased confidence in the security of the Decred network and utility of DCR as a store of value. In contrast, the net monthly returns in USD to staking has gradually decreased from over 5% at network launch to under 1.5% in early 2019. These returns can be compared to baseline cryptoasset staking alternatives such as Dash, which currently has a monthly return of ~0.6%. However, the comparison with Dash is imperfect, since the staking requirement there is much higher (1000 DASH, ~$300k), there is no illiquidity through token lock-up, and the Dash network is significantly larger by market cap and transaction volume. Further, returns to DCR staking can be compared with baseline risk-free alternatives in the traditional financial markets, such as one month US T-bills currently yielding around 2.4%. Of course, staking DCR is not truly risk-free; allocated tickets cannot be redeemed at will to respond to

"In contrast to other base blockchains that have attempted to eliminate or reduce ASIC based mining through changes to mining algorithms or other measures, Decred approach is notably comparably pro-ASIC"

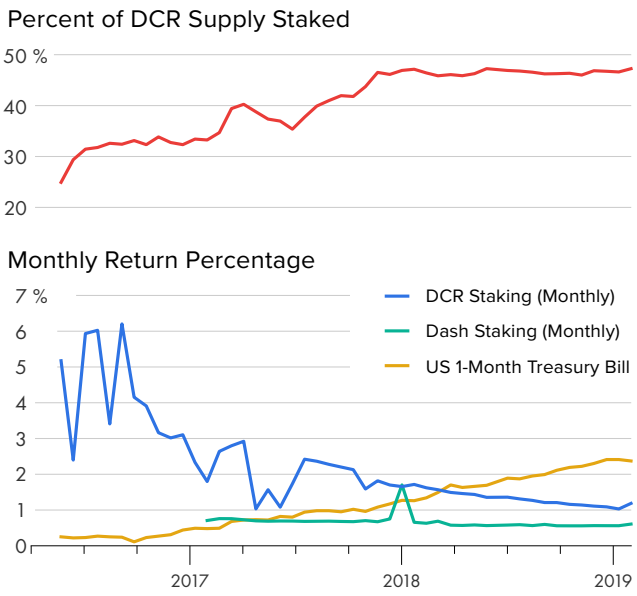
market movements or code bugs, and the underlying price risk associated with holding DCR persists. The data below is sourced from Dash and Decred network statistic explorers, and the US Treasury Department.

Individuals are incentivized to claim tickets for two primary reasons: to accrue a portion of the block reward allocated to the PoS component, and to participate in network governance through on-chain voting rights. Given this dual function, the trends illustrated above are notable, as they display increasing staking participation in tandem with falling block reward returns. There are multiple explanations for these trends. From a purely financial view, where users decide to stake based solely on estimated returns and risk/reward calculations, this is perhaps unsurprising: as trust in the network grows, more users are willing to bid for a finite number of tickets and the market return falls accordingly through this competitive process. The trend may also reflect users' valuation of the utility of DCR's unique structure: DCR users are willing to stake for a lower effective return because the ticket system also grants them direct input in the Decred governance process. In that case, the value of holding a ticket and participating in staking is more than just the financial return of the block reward; direct governance rights are arguably a desirable feature in cryptoassets. While the chart above and trends specific to DCR certainly do not prove a causal relationship, as governance decisions in Decred have been uncontroversial thus far, it may be indicative of an emerging trend in valuing governance that will require further observation and consideration when examining and valuing other cryptoassets.

MINING

Proof-of-work mining in Decred uses the Blake-256 hashing algorithm, and is primarily conducted through mining pools that run ASIC configured hardware. Decred developed and supports 'Gominer', the recommended mining software. Other unofficial yet popular mining software include cgminer, ccminer, and sgminer. Block mining rewards are split 60%, 30%, 10% amongst PoW miners, PoS voters, and the Decred treasury.

Decred Staking Returns vs. Benchmarks



In contrast to other base blockchains that have attempted to eliminate or reduce ASIC based mining through changes to mining algorithms or other measures, Decred approach is notably comparably pro-ASIC. Decred's hybrid PoS/Pow consensus process may influence the project's permissiveness; the PoS layer arguable provides users some recourse to ASIC mining' perceived centralizing effects.

The Cryptoeconomics of Decred

DCR TOKEN FUNCTION

Broadly, DCR functions as a means of payment within the Decred network. DCR is a means to compensate PoW miners and PoS validators for their contributions to network security. Staking DCR generates tickets, which can provide holders network influence, enabling selected holders to vote on software changes, provide oversight on mining activity, and approve treasury allocations through Politeia.

DCR SUPPLY AND DISTRIBUTION

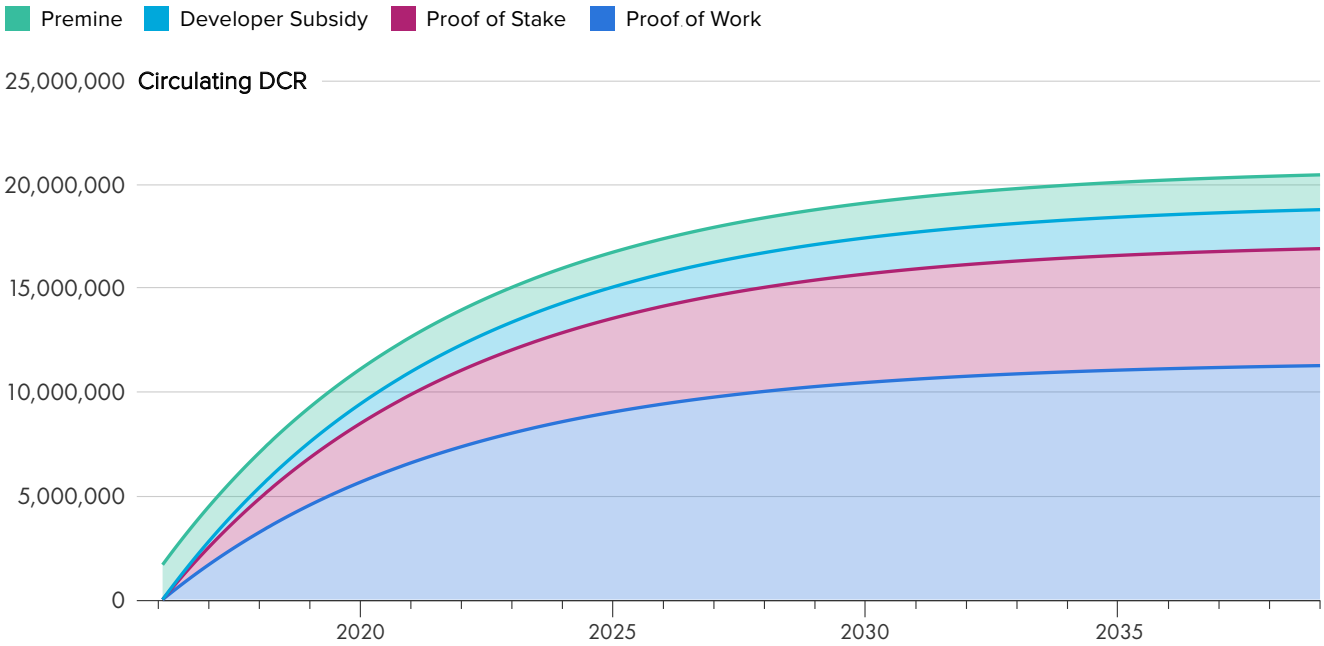
Company 0 and CEO Jake Yocom-Piatt oversaw initial project development, with the network launching in February 2016. Early developers split a premine of 8% of the total DCR supply (1.68 million DCR) as compensation for their work, and individuals contributing to technological advancement and with demonstrated interest in Decred received a curated airdrop. The developers were compensated for their initial work at a rate of $0.49 per DCR.

The target Decred block time is five minutes, and each block has a maximum size of 393kb. Through

"Decred transactions use the UTXO model, similar to Bitcoin, as opposed to the account model of networks such as Ethereum. Decred is developing integration with the Lightning Network, and was involved in the first atomic swap with Litecoin in September 2017."

early 2019, network congestion has not been an issue in Decred as it has in Bitcoin. The supply schedule of Decred is similar to that of Bitcoin; the long term supply is capped at 21 million DCR, with a decreasing block reward schedule that divides rewards between PoW miners, PoS stakers, and the development fund. The last block reward will be created in 2039; afterward, the network will be secured by transaction fees alone. Blocks that receive fewer than the maximum of 5 PoS votes receive a proportionally slashed block reward; as such, a portion of the 21 million maximum DCR

DCR Issuance by Group



supply is effectively removed from the supply and not allocated to any user. The total block rewards for Decred decrease by 1% every 21 days; this is in contrast to Bitcoin, where block rewards decrease by half every four years. This is intended to minimize sudden changes to mining profitability and ensure a more stable ecosystem. Decred transactions use the UTXO model, similar to Bitcoin, as opposed to the account model of networks such as Ethereum. Decred is developing integration with the Lightning Network, and was involved in the first atomic swap with Litecoin in September 2017.

The PoW component of Decred uses the Blake-256 hashing algorithm. In early 2018, ASIC mining units for Blake-256 hashing algorithms were released, quickly increasing the total hashing power of the Decred network by a factor of 20. These ASICs can also be used in Sia. Similar to Bitcoin, hashing power in Decred is relatively concentrated to a small number of mining pools. Due to Decred's hybrid consensus mechanism, where PoS stakers can reject fraudulent blocks, the introduction of ASICs and mining centralization are arguably not as crucial issues as in Bitcoin or other pure PoW networks. However, the development of ASICs will likely contribute to greater security for the network and generate miner interest in DCR.

GOVERNANCE

Funding for project initiatives, changes to the consensus algorithm or core software, and amendments to the constitution outlining Decred's mission are all managed through formal governance processes designed to add transparency, increase oversight, and give various groups of network stakeholders a say in decision making.

BLOCKCHAIN GOVERNANCE: SOFTWARE AND CONSENSUS

Decred's approach to blockchain governance is informed by Jake Yocom-Piatt experiences working on btcsuite, and is, in some respects, a reaction to perceived shortcomings in Bitcoin's blockchain governance. These include issues the Bitcoin

Overview of Decred's Governance Processes

	Proposal	Discussion	Decision	Oversight
Software Upgrades	Network nodes independently adopt consensus software with dormant code changes. Sufficient adoption prompts a vote. PoW blocks, produced on average every five minutes, prompts a PoS validator vote.	Voting progress and results are publicly displayed by Decred	Consensus changes require a majority of network nodes to have 'upgraded' for vote to begin Ticket holders vote on consensus changes over a four week period. Adoption requires approval of 75% of non-abstaining tickets PoS validation of PoW block production requires approval of three of five ticket holders	Voting prerequisites ensure miner's support changes, while offering token holders veto power The Decred organization archives records of votes and makes them accessible to the public
Funding Allocation	Anyone can submit a funding proposal for their own project by submitting a form and paying a 0.1 DCR fee	Discussion and voting tracking occurs on Politeia forums	Ticket-based voting occurs in one week intervals, with approval requiring 60% approval amongst at least 20% of the eligible voters Payment claims are manually handled by the Decred Holdings Group	Proposals are reviewed for spam by Politeia admin 'Censorship tokens' issued to rejected proposals are intended to make administrative process more transparent
Meta-Governance	Constitutional amendments are proposed through Politeia.		Constitutional amendments are approved by above described ticket-voting process.	Decred's constitution articulates project's core principles. How the constitution is to be interpreted or enforced in particular circumstances is largely undefined.
Personnel	• Contractors self-select by proposing projects that receive funding. • Governance participants self-select by locking tokens. • Members of the constitutionally described boards are determined through off chain processes described in Decred's constitution.			

community has debated considerably, with many in that community viewing these factors as significant roadblocks to Bitcoin's progress.

For example, Bitcoin has no formal governance structure, and decisions to alter the protocol are made entirely off-chain, typically by insiders/ early adopters and heads of large mining operations. Changes to the Bitcoin protocol must be approved by consensus of the Bitcoin Core developers and adopted by miners, and there is no direct way for Bitcoin users or associated groups to vote on protocol changes. In particular, the Bitcoin Improvement Proposal (BIP) system provides a collaborative repository for proposing protocol upgrades, though no formal system for implementation.

Changes to the blockchain in Decred require both miner and token holder support. In addition to validating blocks of transactions, ticket holders can vote on-chain for proposed network changes. These changes are first considered through informal community discussions, then published as Decred Change Proposals (DCPs). All DCPs include clear documentation and motivation for the change, as well as working code and evidence of a tested implementation. The DCP system is similar to Bitcoin's BIP system, except that approved DCPs are automatically adopted by the network at the end of the voting period.

Decred's voting process for DCPs follows a two-phase schedule to coordinate new code implementation and voting procedures. The Decred documentation includes a detailed guide to this process. First, the network validators must meet the upgrade threshold by utilizing the updated codebase version that uses the code proposed in the hard fork. Once 95% of the 1000 most recent blocks and 75% of the votes cast within the previous

"To manage information about governance proposals, allocate treasury funds, and amend its constitution, Decred utilizes a proposal system called Politeia."

2016 blocks have upgraded to the latest version, a voting period of the next 2016 blocks begins.

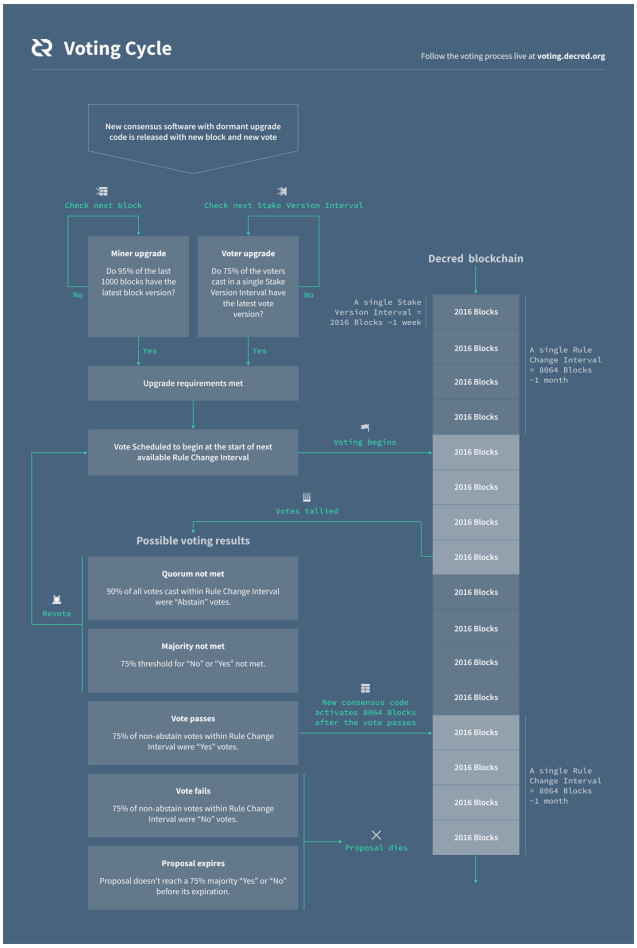
In this voting period, Decred ticket holders who are randomly selected to validate a block also vote or abstain from voting on the proposal. For a vote to resolve, at least 10% of votes need be non-abstaining and at least 75% of those votes need be affirmative or negative. If these conditions are not met, there is a revoting period over the next 2016 blocks by a new set of chosen ticket holders. Since node operators have already updated with the additions, the protocol change directly causes the hard fork immediately following the voting period. In addition to the stake difficulty algorithm hard fork, the Decred network voting has also signaled support for developers to begin work on Lightning Network integration and to implement new opcodes for the Lightning Network. Given that code for proposed network changes must be developed prior to voting, it is perhaps unsurprising that the voting results for the three implemented hard forks suggested the changes were uncontentious; less than 2% of participating voters rejected the proposal in each case.

POLITEIA: TREASURY ALLOCATIONS AND CONSTITUTIONAL AMENDMENTS

To manage information about governance proposals, allocate treasury funds, and amend its constitution, Decred utilizes a proposal system called Politeia. Politeia stores a timestamped record of data related

to Decred's governance off-chain, in order to reduce on-chain costs. Described as 'git plus timestamping' for governance proposals, it also feature a user interface for voting on development fund allocations. Users can submit projects to the Decred community for funding from the 10% development fund block subsidy. This is similar to the Dash treasury system. The development fund functions as a smart contract-controlled DAO with on-chain voting for allocations, proposals, and amendments. Prior to this network upgrade, the development funds accrue to the fund wallet.

Anyone can submit a funding proposal for their own project by submitting a form and paying a 0.1 DCR fee. Politeia administration review proposals for spam, and censorship tokens are issued to rejected proposals in an attempt to reduce 'silent censorship.' Discussion and voting tracking occurs on Politeia forums, with ticket-based voting occurs in one week intervals. Proposals require 60% approval amongst at least 20% of the eligible voters to pass. Payment claims for successful proposals are manually handled by the Decred Holdings Group. Some notable adopted proposals include a bug bounty program and a contractor clearance and quality control process.



Consensus Voting Cycle, reprinted from Decred website

Decred vs. Key Crypto Projects

RELATIVE TO BITCOIN

In some respects, Decred resembles Bitcoin in vision and execution: it is a general purpose cryptocurrency utilizing PoW mining-incentivized timestamping for network security. In the short term, Decred distinguishes itself from Bitcoin through its comparatively more inclusive governance, greater feature flexibility, and a sustainable, independent funding model for project development. In the long term, stakeholders will be responsible for further distinguishing Decred from Bitcoin in terms of feature development, partnerships, and growth strategy, through participation in Decred's governance systems.

- One clear example of Bitcoin's governance difficulties is the multi-year scaling debate saga, with various stakeholders advocating a variety of solutions to network transaction congestion on the Bitcoin network, including increasing the base block size, SegWit, and layer 2 solutions such as the Lightning Network. Potential solutions to the scaling issue have been negotiated off-chain by prominent stakeholders, leading to off-chain coordination mechanisms such as the New York Agreement. Indeed, these protocol upgrades must ultimately be adopted by miners, who are increasingly influenced by a limited number of ASIC manufacturers, such as Bitmain. However, this type of process is often complex and without enforcement measures, which in this case led to a break from the NYA and the eventual BTC/BCH fork in August 2017. Though many groups of financial stakeholders in the Bitcoin network exist, the core developers and large mining entities have a perhaps outsized influence on governance.
- The lack of clear development funding methods in Bitcoin is often seen as problematic. The core network software exists as open source code on Github, but it is difficult for developers to directly monetize their contributions to the codebase. Funding for Bitcoin Core developers was entirely donation driven until 2014. Instead, the ecosystem effectively supports development through external businesses such as Blockstream and non-profits such as the MIT Media Lab's Digital Currency Initiative, both of which employ Bitcoin Core developers directly. Particularly in the case of Blockstream, a for-profit entity, this could create real or perceived conflicts of interest for developers. While developers may support themselves through early investment in BTC or ancillary work, the Bitcoin protocol itself does little to incentivize development work.

RELATIVE TO DASH

Decred closely resembles Dash, the project analyzing and learning from Dash's longer running treasury governance and proposal mechanics. Dash represents a more fully-developed governance-focused cryptocurrency—its stakeholder-influenced vision for its cryptocurrency and adoption strategies are currently more defined, while Decred's are more inchoate. Other differences between the projects lay in their respective approaches to blockchain and project governance.

- Suffrage in Dash requires Masternode status, so limits direct governance participation to those who can afford to stake 1000 DASH and have the technological know-how to run a node. Assuming ticket-splitting functionality, suffrage in Decred is conferred more widely.
- Blockchain governance in Decred arguably offers miners greater influence than in Dash; software changes must already be adopted by a majority of nodes to be subject to ticket-holder vote. Dash's masternodes can make changes to mining algorithms unpopular to miners, such as attempting to limit ASIC mining through algorithm change.
- Dash Masternodes could vote to replace the project's 'core team'. It is less clear that the Decred organization is so open to replacement—if not, this represents a tradeoff between organizational stability and token holder oversight powers.
- Decred's constitution articulates the project's mission and values, though how the document might be interpreted or appealed to in practice is less clear.

Prospects and Challenges

One's outlook on Decred will likely be shaped by one's estimation of what value Decred's focus on governance adds to the project. In the same sense that Monero appeals to those who like Bitcoin generally but desire more advanced privacy and ASIC resistance, Decred appeals to those who find core flaws in the Bitcoin community and in particular its approach to governance. Industry entrants, such as institutional investors, may value Decred's more structured governance, as such entrants are apt to be accustomed to structured decision making processes and could view the 'consensus by hard fork' of Bitcoin as problematic for a long-term investment.

Decred is a general purpose cryptocurrency, similar to Bitcoin and other cryptoassets facilitating payment as their primary function. With the proposed Lightning integration, it has potential for both everyday payments and 'store of value'. Decred competes primarily with Bitcoin, Litecoin, and Dash as a general purpose cryptocurrency. Decred has also proposed development of privacy features, which would place it in more direct competition with zCash and Monero, and even newer entrants like Beam or Grin. though it is uncertain to what degree this is a long-run emphasis of the network.

"It will be critical to watch how the Decred community allocates the ~$10 million in accumulated treasury funds, now that they can be allocated directly with Politeia. Critical, in part, because such proposals will shape the marketing, adoption, and use-case targets decisions currently (intentionally) left open."

It will be critical to watch how the Decred community allocates the ~$10 million in accumulated treasury funds, now that they can be allocated directly with Politeia. Critical, in part, because such proposals will shape the marketing, adoption, and use-case targets decisions currently (intentionally) left open. Early quality of community discussion around, i.e the Wachsman & Ditto PR proposals, is quite high. Project lead Jake Yocom-Piatt must currently sign all disbursements from the treasury wallet; a smart contract is in development to remove this feature over the next few quarters and permit trustless distributions of the treasury funds to approved proposals.

RISK FACTORS

Decred's long-term ability to succeed as a general purpose cryptocurrency could be undermined should any of the following occur:

The market for general-purpose cryptocurrencies proves to be winner-takes-all, and Bitcoin is the only widely accepted crypto means of payment, unit of account, and store of value. Established general purpose cryptocurrencies such as Bitcoin have existing network effects, merchant adoption, a distributed mining network, and a longer record of immutability. Decred may need to make hard decisions about product direction to distinguish itself in such a scenario.

Decred fails to see major adoption when it finally starts marketing in earnest. Decred has spent very little on marketing or exchange listing—it was listed on Binance only in October 2018— both a testament to the anti-hype ethos of the community and the potential increase in public awareness that could be spurred by spending some of the treasury on marketing efforts. Decred has done little to promote adoption as a means of payment compared to projects like Dash, though Decred does have fairly low TX fees (~ $0.05), making it a plausible candidate for merchant adoption and everyday payments.

Decred's governance process appears to function comparably or worse to its predecessors, undermining its claim to finally improving on decentralized governance. The Politeia treasury system could prove inefficient in allocating funds to third party service providers. There must be checks and balances in place to ensure that proposal cost estimates are reasonable, and that funded proposals are executed.

This is an active issue in Dash, as some proposals are funded as a one-off, and there isn't always a check that the proposed work actually gets done, or that the quoted cost is fair. Moving to to a milestone-based or escrow model can improve efficiency here, but still requires actual stakeholder participation in active governance, and does not entirely solve the issue that stakeholders do not necessarily have the expertise to evaluate well proposal team's capabilities or progress. Likewise, even knowledgeable stakeholders may be limited in exercising good judgment by the system's format—for example, stakeholders depend on contractors to provide complete information.

Decred fails to fully decentralize network and treasury governance control, leaving it seeming like a centrally managed protocol in all but name. While Decred may have greater claims to inclusivity and transparency, many crypto-advocates also highly value

decentralization in decision making processes. It remains to be seen whether control over network management and in particular over the treasury move away from Company 0 and the core Decred team. There are many promises of decentralizing this control, but with a large centrally controlled treasury, this does remain a small risk—though Decred certainly is not uniquely in this position compared to other projects tackling governance.

MARKET OUTPERFORMANCE SCENARIOS

DCR may outperform the broader market for cryptoasset investments in the following scenarios:

Perceived flaws in traditional blockchain structures or peer project governance systems drive users towards Decred. Events precipitating such a shift could include a hard-fork induced drop of value, trenchant misalignment between miners and chain developers, or controversial top-down decision making not subject to oversight through forking.

Historically, events such as the 2018 BCH/BSV hard-fork and prolonged hash-war go some way to discredit Bitcoin's approach to governance. One individual's conviction regarding the networks future was sufficient to cause a disruption to the markets; the act of forking served to create two networks both drastically more vulnerable to 51% attacks, compared to their predecessor. Such factors help motivate adopting an alternative governance structure that aligns stakeholders by reducing such risks and providing a forum for cooperative decision-making around network parameters.

Network stability and high staking returns offer prospective investors a compelling risk/reward tradeoff. This is somewhat mitigated by the high inflation rate - a staker must also bank on DCR price appreciation to view staking as a good investment.

Politeia leads to compelling partnerships or product strategy. A broad question for the industry is how many 'general purpose cryptocurrencies' can co-exist in the long term. Carving out unique and compelling use cases could become more important in circumstances where an established project begin to monopolize that function. Decred has prioritized establishing a stakeholder-informed decision making procedure over directing its extensive treasury into the sorts of marketing, research, development, or partnership decisions that will come to define its product. Whether this prioritization will lead to comparably better decisions remains to be seen.

Extended Discussion

GOVERNANCE'S CONTRIBUTION TO A PROJECT'S VALUE

Decred is among a generation of industry projects responding to perceived shortcomings in initial entrant's governance. The question of how to value a project's focus on governance, while pertinent for Decred, is also a more general question the industry faces, as more and more projects look to innovate in this area. Smith and Crown plans to address this question more broadly in future thought pieces offering a framework for understanding governance in distributed systems.

In the case of Decred, it is worth highlighting how Decred's accomplishments can be viewed from two perspectives. Governance arguably has claim to both intrinsic and extrinsic value. From one perspective, Decred is to be praised for building a more inclusive, transparent, fairer process—to the extent that such characterizations are accurate—regardless of whether the decisions made through that process turn out to help or hinder Decred's success as a cryptocurrency.

"The question of how to value a project's focus on governance, while pertinent for Decred, is also a more general question the industry faces, as more and more projects look to innovate in this area."

From a second perspective, it is still much too early to say anything about the merits or faults of Decred's process not couched in the language of probabilities. Industry observers might reasonably disagree about Decred's governance prospects. To better help readers form an outlook, Smith and Crown has summarized several relevant thesis on what to expect from Decred's governance, as well as considerations that might lead readers to lean one way or another.

Conjectures on Decred's Governance's Value

Thesis	Reasons to Believe	Reasons to Doubt
Decred's Governance will lead to better decisions.	'Better decisions' is broad enough to be true in some respect or other...	The claim leaves open whether decisions will be 'better' in any sense that matters....
Decred's Governance will be influenced by a broader range of stakeholders' interests.	'Broader' looks to a comparison class: Decred's governance appears to solve shortcomings in its predecessor's design. With ticket-splitting, participating in Decred's governance would seem to require less an investment compared to stockholding	Many of Decred's mechanisms are inherently plutocratic; legitimate stakeholder concerns can be circumvented in decision making through DCR purchased influence. Vote buying is an issue distributed systems haven't solved: it is easier to buy, bribe, or coerce stakeholder's votes than in traditional processes.
Decred's Governance will help good development initiatives get funded.	Compared to other projects, there actually is money set aside earmarked for development, and plans for maintaining treasury. A broader range of stakeholders means development decisions will be based on a broader set of interests.	Tokenholders aren't necessarily technology, finance, or marketing experts. Nothing prevents holders from directing funds based on personal relations—the somewhat less capable but better connected team can still win the proposal. Governance isn't entirely necessary for this; Bitcoin has robust core features and new development initiatives funded through third party businesses..
Decred's Governance will increase DCR's value in the long run.	Decred's governance is designed so that those with a long-term interest in the platform influence its development—Decred's stakeholders have incentive to make decisions that increase the currency's value, utility, or adoption.	The confered right to to govern won't drive DCR's value alone—there must be demand for the token outside its use in governance. Incentive alone won't lead to value-increasing decisions should stakeholders prove to lack expertise, or their exercise of it be impeded by the limitations in distributed decision making processes.