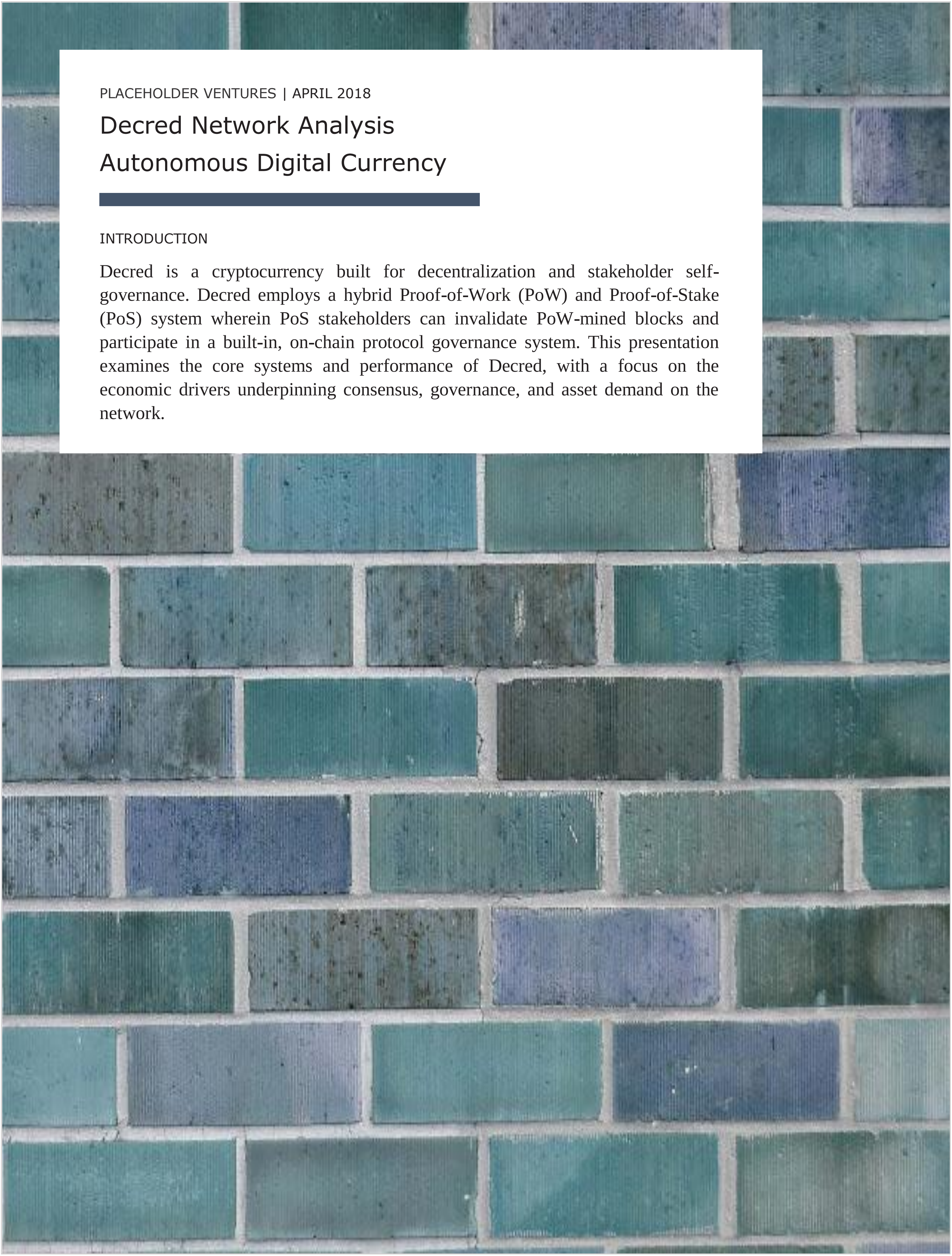
PLACEHOLDER VENTURES | APRIL 2018

Decred Network Analysis
Autonomous Digital Currency

INTRODUCTION

Decred is a cryptocurrency built for decentralization and stakeholder self-governance. Decred employs a hybrid Proof-of-Work (PoW) and Proof-of-Stake (PoS) system wherein PoS stakeholders can invalidate PoW-mined blocks and participate in a built-in, on-chain protocol governance system. This presentation examines the core systems and performance of Decred, with a focus on the economic drivers underpinning consensus, governance, and asset demand on the network.

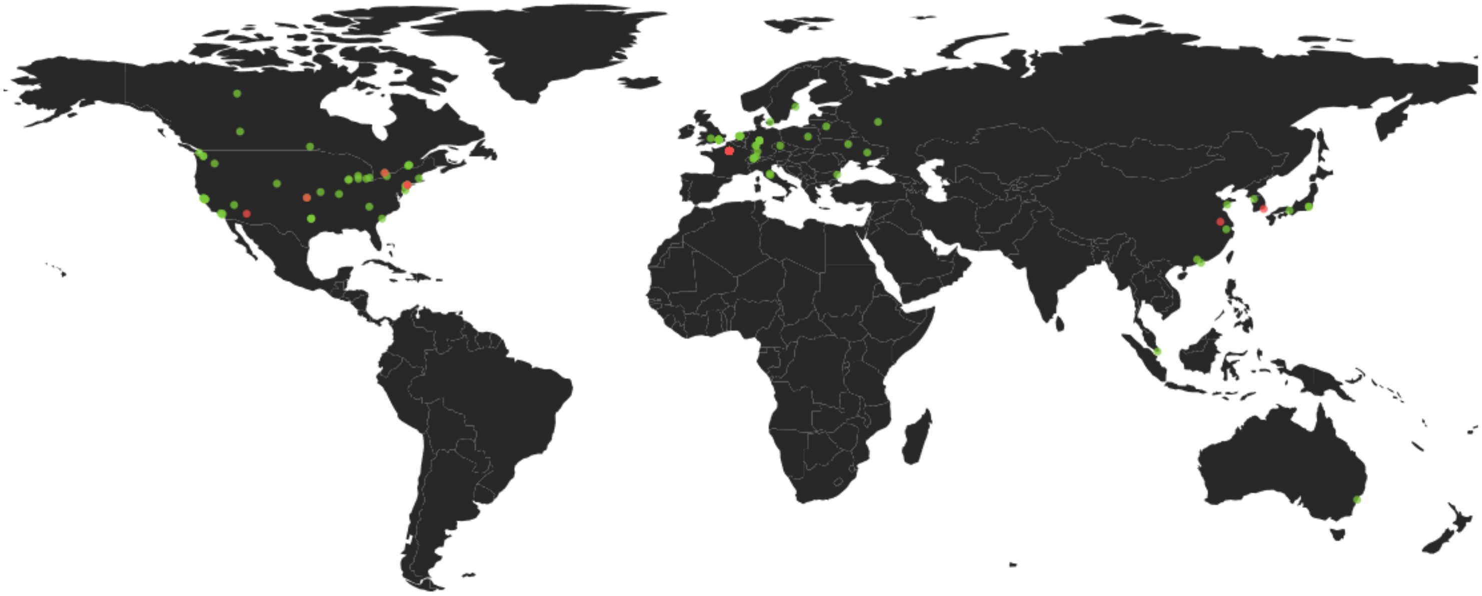


SECTION I

300,000-FOOT VIEW OF DECRED

Decred is a cryptocurrency that implements a hybrid proof-of-work (PoW) and proof-of-stake (PoS) consensus algorithm to mitigate the risks of mining centralization. In addition to block validation, stakeholder votes serve as the core component of Decred's community input and stakeholder governance system. Decred was launched in February 2016 by Company 0, which includes some of the main developers of btcsuite, an alternative full-node bitcoin client. As of April 2018, Decred has a network value of around $437 million and boasts a vibrant ecosystem of users, miners, stakeholders, and developers.

FIGURE 1 ***The Decred Network (207 Active POW Nodes)***



Source: DCRStats: **Network Map**
Resources: Decred documentation: hybrid **consensus**, **PoS protocol**, and **voting process**.

SECTION II

CONSENSUS IN DECRED

In Decred's consensus protocol, blocks are generated through conventional PoW mining and validated by a majority of randomly-selected voting tickets for each block height. Decred holders who wish to participate in PoS validation can mint tickets by locking up DCR balances in stake transactions and earn DCR by casting votes on block validity and outstanding governance issues when their ticket is called to vote. In each block, five tickets are selected from the outstanding ticket pool subject to a pseudorandom lottery based on the block header. Each of these tickets must either attest to or reject the validity of the block and can accept, reject, or abstain from governance agenda items. Network maintainers earn DCR both from hash-based mining as well as by staking their coins in ticket transactions and voting. The PoW reward diminishes for each missing vote to incentivize miners to include all tickets. Blocks without a clear majority agreement are excluded from the chain, while down-voted blocks remain on the chain with their contents invalidated.

2.2 ISSUANCE & REWARDS

Initially, the Decred network subsidizes stakeholders and miners through a diminishing block reward. This reward in Decred subsides in a smoother fashion than Bitcoin's coinbase reward halving, but retains the same hard-cap at 21 million DCR. Decred supply initialized with a pre-mine of 8% or around 1.68 million DCR (worth roughly $830K at launch), which was split evenly between an airdrop and a grant to Company 0 developers (the founding team) who bore the initial bring-up costs for the network. Of each block reward, 60% is granted to PoW miners, 30% to PoS voters, and 10% is reserved for the Decred project subsidy, which can be spent at the discretion of stakeholders. Over time, Decred plans to delegate control of project subsidy/development funds to stakeholders (see Section 3.5). The block reward and issuance schedule is summarized in Figure 2. As of April 2018, Decred has issued around 34% of potential supply and has an implied 2050 network value of around $1.3Bn at current prices.

FIGURE 2A ***Block Reward Distribution***

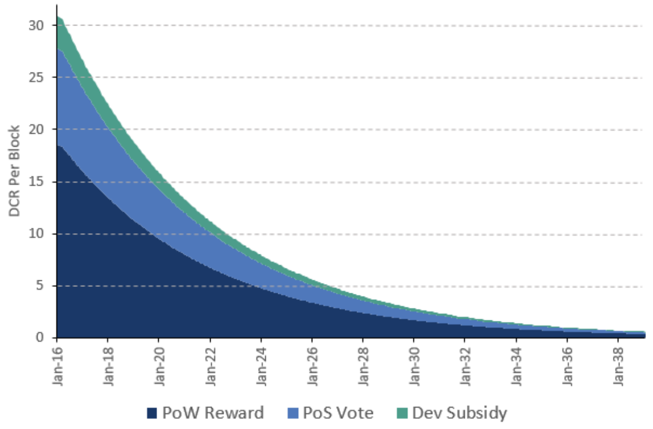
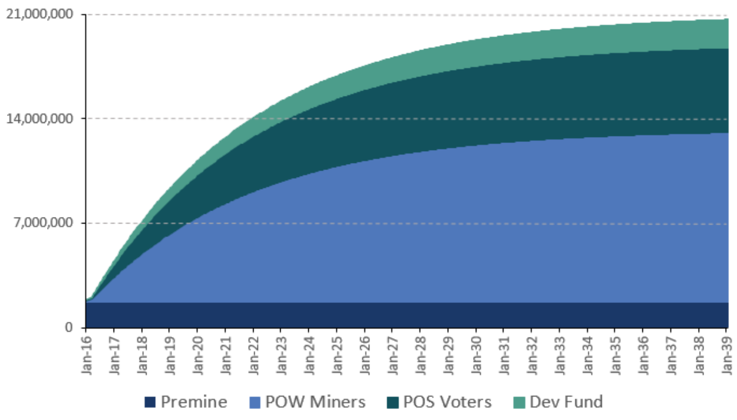


FIGURE 2B ***DCR Issuance Schedule***



Source: Author's tabulations; Data from DCRStats: **Subsidy**

2.3 POW MINING IN DECRED

2.3.1 MINING ALGORITHM

PoW in Decred is based on the Blake-256 hashing algorithm. This hash function choice was motivated by performance and security considerations rather than ASIC-resistance, which was a popular design choice among similar new projects at the time of launch (see resources in notes for additional perspectives). This choice also allowed regular users to GPU mine at launch as no ASICs had been developed for Blake-256, which was still simple to implement in hardware, making it easy to eventually create ASICs for Decred. The Decred community has been welcoming of ASIC development.

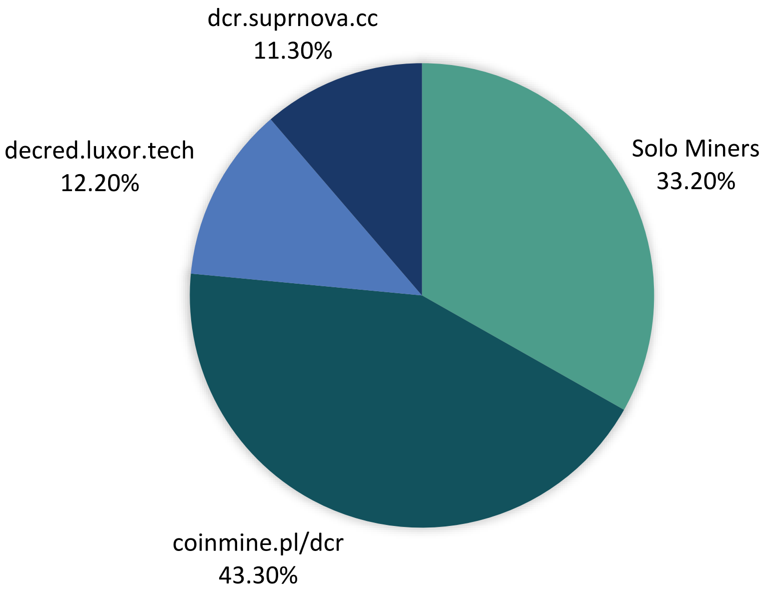
2.3.2 HASHRATE

Decred has recently been experiencing abrupt growth in network hashrate, currently just under three thousand THash per second, equivalent to Bitcoin's hashrate in late 2014. This number has more than doubled since March 2018.

2.3.3 HASHPOWER CENTRALIZATION

Mining pool power in Decred is even more concentrated than in Bitcoin (Figure 3). Currently, Coinmine controls 43.3% of mining power (about 12.6K THash/second), though spread across 17,337 workers. On several occasions in recent weeks, Coinmine has controlled over 51% of the hashpower of the network. The effect of mining centralization is, by design, far less pernicious in Decred than in Bitcoin, as PoS votes may invalidate blocks and strip malevolent miners of rewards. Nonetheless, current levels of centralization remain an important concern, especially as the community anticipates new ASICs to come online in the coming months.

FIGURE 3 ***DCR Network Hashrate Distribution (total network THash/s, 2908.56)***

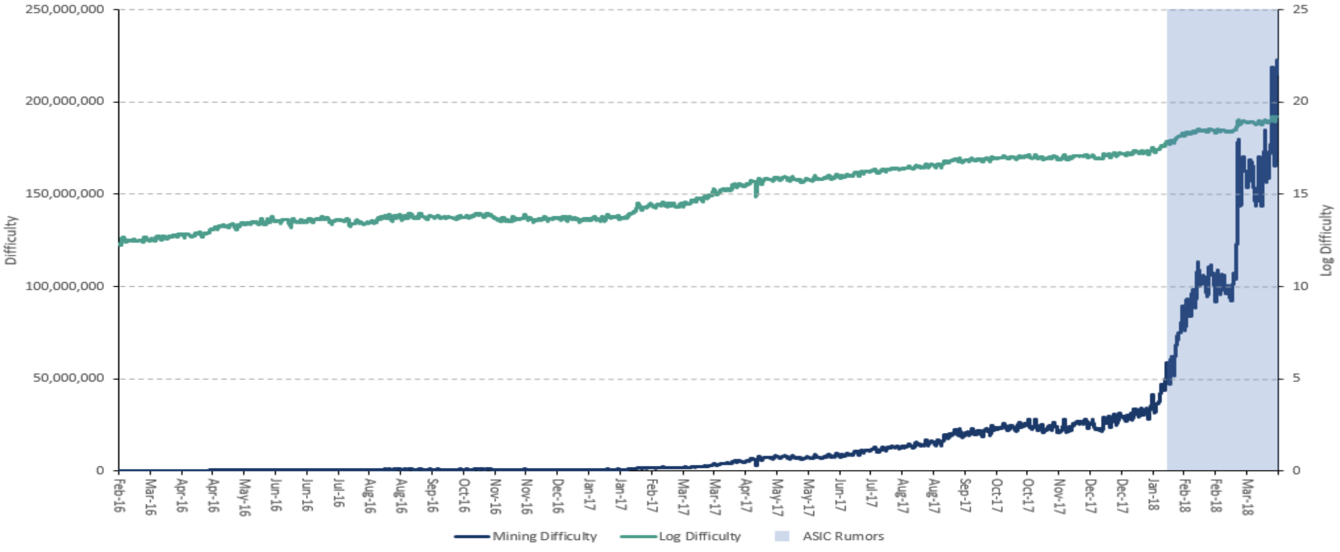


Source: Author's tabulations; Data from DCRStats: **POW**
Resources: Decred Documentation: **Blake-256**; Reddit, r/decred: **Why Blake 256**?; Reddit, r/decred: **ASICs or…**

2.3.4 RUMORED ASIC DEVELOPMENT

In January 2018, Bitmain announced it was launching Antminer A3, an ASIC specifically designed for Blake(2b), used by Sia and Railblocks. The abrupt growth in Decred's network hashrate has led to speculation in the community of a similar ASIC being under development for Decred, given the similarity of Blake(2b) and Blake-256 which would make it feasible for a company developing ASICs for Sia to create a DCR product without significant marginal R&D cost. Prior to the announcement, Siacoin founder David Vorick's company, Obelisk, had been planning to release both Sia and Decred ASICs and several companies have since announced miners for both networks. Currently, Obelisk DCR1, Baikal Giant-B, Dragonmint DCR ASIC, and Bitmain's potential ASIC are all purportedly in the running for advanced Decred ASICs. The recent growth in hashrate has been attributed by some to Bitmain and other companies 'testing' their equipment prior to sale as well as migration of GPU/CPU miners from Sia due to incoming ASIC competition. Neither narrative is possible to confirm at this time; however, there was a clear point of inflection in hashrate growth around the time of the initial ASIC rumors (Figure 4), despite this also coinciding with a period of overall price decline. Critics argue that Bitmain's rapid development of ASICs, which is reflective of its enormous R&D budget, poses unique centralization risks to the future supply of cryptocurrencies. Its affiliation with Antpool, one of the largest miners in the world, and past behavior of empty-block mining and support for controversial forks have created unease in PoW-centric networks. The Decred development community has indicated its confidence in the ability of PoS voters to invalidate blocks corresponding to deviant mining behavior. On the positive side, ASIC development will contribute greater security to the network and signifies a longer-term commitment from the mining hardware community to Decred.

FIGURE 4 ***Decred Mining Difficulty Since Network Launch***



Source: Authors Calculations; Data from DCRData **Block Explorer** API (see: **endpoint**; **documentation**)
Resources: Motherboard, **Siacoin story**; The Decred Miner's Union: Decred **ASICs**. Reddit, r/decred: **Sudden Increase in Difficulty?**

2.5 POS VALIDATION

In Decred’s PoS system, stakeholders obtain tickets by submitting fresh stake transactions to the network with inputs corresponding to a number of coins at or above current ticket price plus a ticket fee (ticket price can be thought of as equivalent to PoW difficulty). After submission, the tickets need to ‘mature’ for 256 blocks, after which they are eligible to be selected for voting. Staked coins are unspendable until after they are selected to vote. For each block, five tickets are selected from the mature ticket pool based on a deterministic pseudorandom number generator with a seed of the header of the block. Each ticket corresponds to one vote on the validity of a block, returning the original ticket price plus a PoS reward to the holder.

2.5.2 STAKE CONCENTRATION

As DCR coins are convertible to tickets, one estimate of economic power concentration is the wealth distribution among coin holders. As with most major cryptoassets, Decred’s distribution is relatively inegalitarian, though not strikingly so (Figure 5). Concentration of DCR in few addresses is relatively benign for the network, as the ticket price algorithm increases price alongside demand and caps ticket purchases to 20 per block, preventing even a holder with a majority of DCR from quickly overtaking the network. Predictably, tickets are relatively more concentrated than DCR coins, with the top 100 addresses representing a near majority of votes. Additional transaction graph analysis and address clustering should be examined to identify whether multiple of these addresses are controlled by the same entity as this may generate substantial risks of system centralization (see Section 2.4).

FIGURE 5A ***Wealth & Vote Concentration By Address***

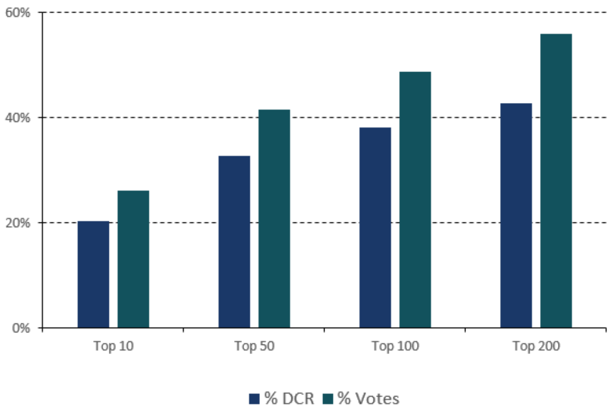
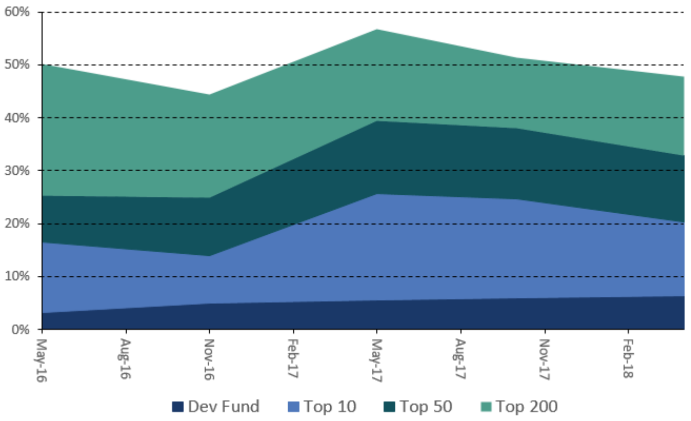


FIGURE 5B ***Historical DCR Concentration By Address***



Source: Author’s Tabulations; Data from: DCR Observer: **Top Addresses** & **Top Voters**

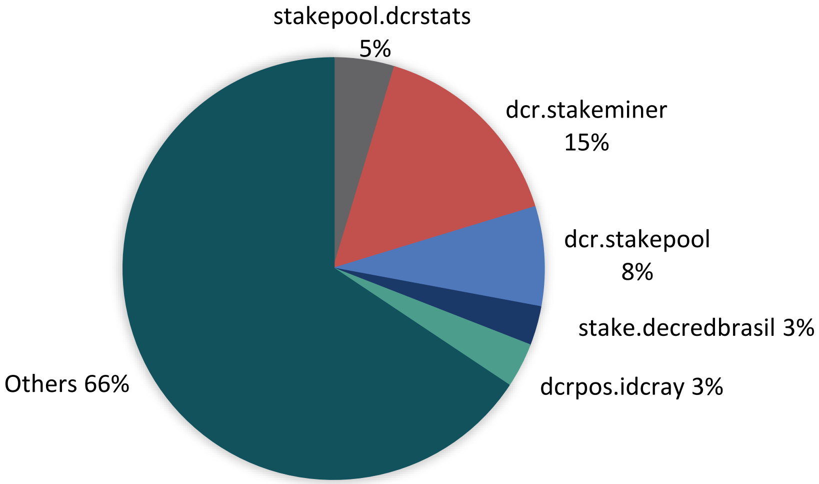
2.5.3 STAKE POOLS

When a given ticket is randomly selected to vote, the holder must be online to ensure the vote gets included in the block or forfeit the reward. Users may instead opt to use stake pools, which can vote on their behalf in exchange for a small fee. These are essentially one-of-two multi-signature transactions, where either the holder or the pool administrator may vote on each block. Stakepool providers offer a commodity service and attempt to compete on fees, branding, service, and percentage of missed votes. For example, dcr.stakeminer has gained significant adoption due to its aggressively low fees and quick response time of admins on online forums. Stakepools do not currently exhibit alarming concentration (see Figure 6) and are not a significant risk to the system as switching costs are low and users can regain control of pooled tickets from misbehaving operators. Pools also cannot misappropriate funds, as the contract specifies an address for rewards.

2.6 DECRED CONSENSUS ASSESSMENT

The resilience of the Decred network to a 51% PoW attack through the checks-and-balances afforded by the hybrid consensus model is an advantage over competing systems as hashpower centralization shows no signs of abatement. The ticket price mechanism precludes a large stake position being abruptly built without community detection. Furthermore, such an attack would risk upwards of half of the value of the outstanding ticket pool for the attacker, which becomes increasingly expensive as DCR appreciates. There are currently no detailed analyses of deviant validator strategies that involve collusion between miners and stakeholders, such as withholding votes to competing miners or manipulating voter selection randomness by withholding blocks. The stability of the protocol after the block subsidy is supplanted by transaction fees is another interesting area for future research.

FIGURE 6 ***Top 5 Stakepools By Vote %***



Source: Author's Tabulations; Data from **DCRStats: PoS Pools**

SECTION III

DECRED GOVERNANCE

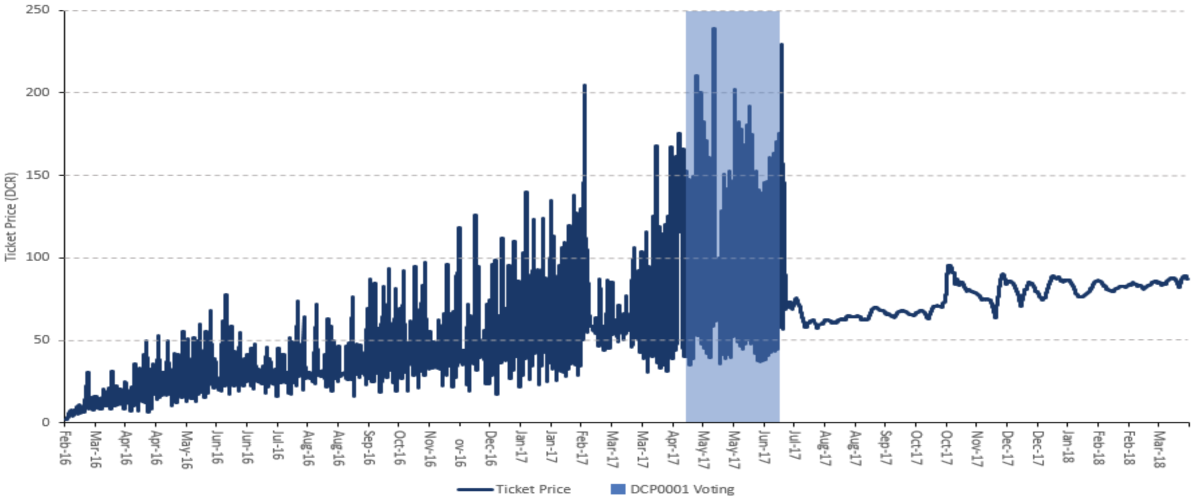
3.1 STAKEHOLDER GOVERNANCE

PoS tickets selected to validate each block may also vote on outstanding consensus rule changes. Stakeholder voting is the ultimate arbitration mechanism for protocol changes when deciding on hard-fork consensus changes. Nodes and voters first update their versions with dormant update code, which is activated subject to a successful vote. Voting occurs during successive “Rule Change Intervals” (RCIs) until a 75% majority of non-abstaining votes either accept or reject the change or the proposal expires (see resources for a full description of the voting process). The Decred developers are only empowered to make changes to the protocol subject to the approval of stakeholders.

3.2 DECRED CHANGE PROPOSAL 0001

Decred’s on-chain stake-based governance system was first put to the test on the mainnet in DCP0001, a hard-forking issue that adjusted the stake difficulty (“sdiff” i.e. ticket price) algorithm. At the launch of the Decred network, the sdiff algorithm was successful in keeping the ticket pool near the target size (40,960), but failed to facilitate price discovery and stability. The core issue was the algorithm’s oversensitivity to recent ticket purchase intervals, where even a single interval of high purchase activity would cause ticket price to greatly overshoot demand leading to several periods of little to no purchases, causing price to collapse again and the cycle to repeat. This effectively prevented price discovery, leaving validators to compete over fees for inclusion of their purchases in low-sdiff blocks. After rigorous review of new sdiff algorithm candidates (see resources), the final algorithm was put to a vote on the mainnet in RCI 16 (blocks 125,056 to 133,119) and received 86% of votes in RCI 17 (ending on June 11th, i.e. block 141,183). The final algorithm produced significant stability in ticket prices as seen in Figure 7 and can be claimed as the first success of Decred governance.

FIGURE 7 ***Decred PoS Ticket Price (“sdiff”)***



Source: Authors Calculations; Data from DCRData **Block Explorer API** (see: **endpoint; documentation**)
Resorces: Decred Documentation: **Mainnet Voting Guide**; Decred Blog: **A New Ticket Price Algorithm**; Decred Proposals: **New Sdiff Algorithm**

3.3 DCP 0002 & DCP 0003

In late 2017, the community voted to hard-fork Decred to activate the requisite features to fully support Lightning Network deployment (see resources for more details). The "lnfeatures" agenda included DCP0002 and DCP003, which were successfully voted on in RCI 21 (blocks 165,376 to 173,439, i.e. September 2017). Development towards full LN support is ongoing.

3.4 POLITEIA

A core proposal for moving Decred towards stakeholder self-governance is Politeia, a permanent public record of proposals, comments, and stakeholder votes. Rather than store governance-related information on-chain, Decred has made the design decision of storing data in a version-controlled git repository with timestamps anchored on the Decred chain. In that sense, Politeia can be thought of as a public governance record similar to whitehouse.gov or senate.gov that create accountability for both users and admins who participate in Decred governance.

3.5 ROADMAP & PHILOSOPHY

Decred has released an ambitious roadmap for 2018 (see resources), including proposals for scaling, privacy, and on-chain stakeholder governance, some of which may require hard forks for implementation. Over time, Decred plans to move to full on-chain stakeholder self-governance. Concurrently with Politeia, Decred's near-term roadmap includes proposals for decentralized control of the project subsidy/development fund, allowing ticket holders to vote on fund disbursements on-chain.

3.6 DECRED GOVERNANCE ASSESSMENT

The Decred governance system has gracefully handled both the sdiff and LN hard-forks with virtually no disruption and rapid time to deployment. One potentially problematic trend was the suppressed participation from voters during the lnfreatures vote, compared to DCP 0001. Abstention on lnfeatures was 31% in RCI 21 and 37% in RCI 22, while only 12% of voters abstained on the sdiff vote in RCI 17. While two data-points do not suffice to generalize, the timing of the two votes (early vs. late 2017) may explain the difference in engagement as the influx of speculative users in mid and late 2017 may have diluted the share of long-term ecosystem participants in the voter base. Abstention should be a key metric of the health of Decred governance going forward, as persistent stakeholder apathy can be a hindrance if large sections of the voter base free-ride on few active members. Meanwhile, increasing rewards for voting in order to rectify apathy may have a perverse effect on user incentives as otherwise uninformed speculators may still vote arbitrarily to gain access to rewards. A related challenge for Decred governance will be to align the incentives of voters with the long-term success of the network. Currently, a stakeholder can expect to hold her ticket for an average of 28 days and a maximum of four months. This creates an incentive to not support proposals that destroy medium-term network value, but does not necessarily engender long-term incentive-alignment. Comparatively, Dfinity's "Neurons" require locking deposits for a minimum of 3 months.

Resoruces: Thundestruck **Development Update**; Decred Blog: **Politeia**; Decred Blog: **2018 Roadmap**; Dfinity **BNS**

SECTION IV

DECRED DEMAND

4.1 TRANSACTIONS DEMAND

Decred is intended to be used as a currency, making transaction flows a reasonable proxy for the utility users derive from the Decred network. Coinmetrics data implies that Decred currently records fewer than one thousand on-chain transactions per day, with total transaction volume averaging around $15 million in recent months. Coinmetrics does not provide documentation on how transaction volume is estimated for Decred, but scrapping the Decred block explorer for a few sample dates reveals that stake-based transactions (ticket purchases and votes) are likely not included in Coinmetrics estimates. Removing these PoS transactions reveals a small divergence where Coinmetrics transaction count estimates slightly exceed those implied by the Decred block explorer. Additional analysis is required to reveal the source of the error. Regardless, non-stake-based transaction volume on Decred remains relatively low compared to most large-cap cryptocurrencies (Figure 8A).

4.1.2 NVT Signal

Figure 8B depicts Network-to-Transaction-Volume signal (i.e. NVT using 90-day moving averages) based on Coinmetrics data for Decred. The ratio demonstrates some, albeit limited, predictive potency for Decred price movements. For example, the NVT signal crosses above 50 in June 2017 in advance of a 58% price correction in the following weeks and again in late December 2017, preceding the early-2018 downturn. NVT crossed below 20 in September and October 2017, preceding the bull market near the end of 2017, despite significant price appreciation prior to those dates. The ratio again crossed below 20 immediately prior to the rally in recent days. Overall, while NVT appears to demonstrate some correlation to price performance, it does not capture staking demand. On-chain non-stake transaction demand is only a portion of the utility derived from the Decred network with staking demand being arguably more significant (at least currently).

FIGURE 8A ***On-Chain TX Volume & Count***

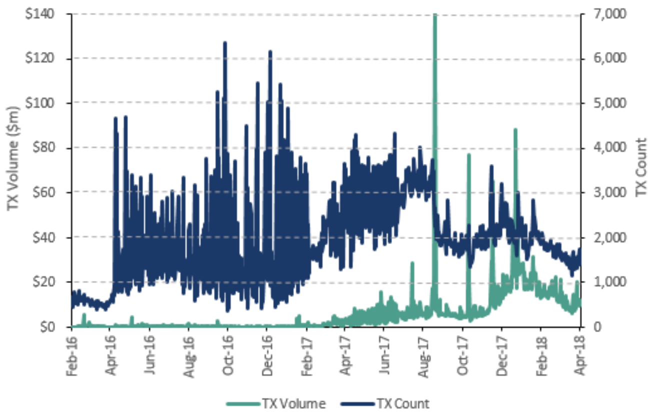
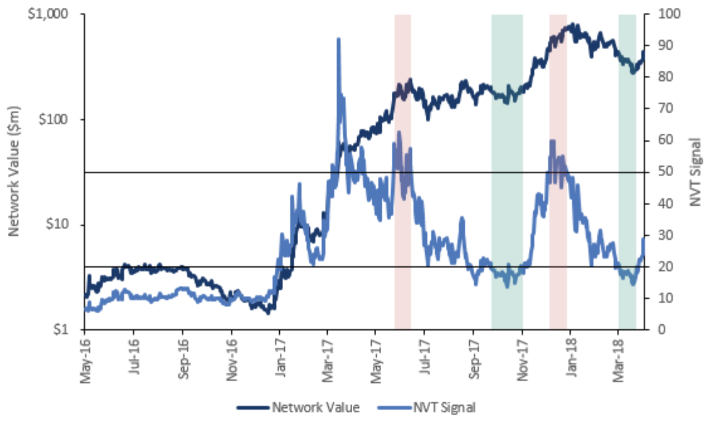


FIGURE 8B ***NVT Signal & Network Value Since Launch***



Source: Author's Tabulations; Data from **Coinmetrics**

4.2 STAKING DEMAND

A large portion of demand for Decred results from staking for PoS validation (note: ticket price dynamics are discussed in more detail in Section 3.2 in the context of DCP0001). While the sdiff algorithm updates created smoother prices, ticket prices have continued to increase in DCR terms despite appreciation in overall network value (Figure 9A). In DCR terms, the price of a PoS ticket has increased 162% since the start of 2017 to a current price of over 86 DCR. In USD terms the price of a PoS ticket has increased 16,600% from $26 at the start of 2017 to a current price of $4.3K (note that PoS rewards are DCR-denominated and have also increased proportionately in dollar terms). USD ticket price since network launch is summarized in Figure 9A. In recent weeks, 48% of Decred supply, on average, has been staked in PoS, representing more than $165M in value. In other words, around half of the supply of DCR is out of circulation at any given point and is unavailable for non-stake transactions (Figure 9B). If ticket price repeats its year-over-year growth from April 2017, by April 2019, approximately 59% of Decred supply will be locked up in PoS deposits. The economics of PoS in Decred make ticket growth at these rates very difficult to sustain over the long-term, due to lower yield, diminishing block subsidies, and potential liquidity effects. In long-run equilibrium, PoS stakeholders will have to rely on network transaction fees for yield, meaning that sufficient outstanding supply will have to be untethered to tickets to provide liquidity for fee-paying users of the network. On-chain, non-stake transaction volume will have to grow in lockstep with declining block subsidies to sustain the incentives of validators to secure the network.

FIGURE 9A ***USD Ticket Price (logscale)***

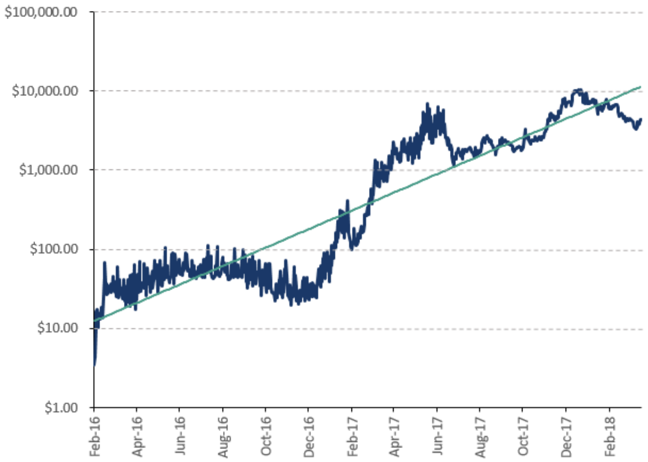
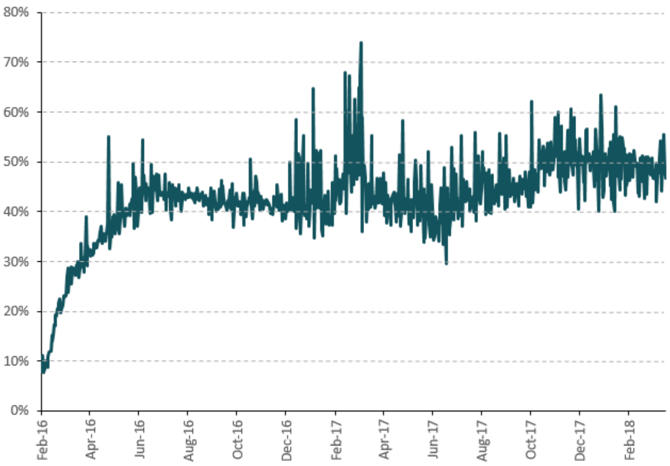


FIGURE 9B ***% of DCR Staked in PoS Tickets***



Source: Authors Calculations; Data from Coinmetrics & DCR Data **Block Explorer API** (see: **endpoint**; **documentation**)

4.2.2 STAKING YIELD

In addition to participation in Decred governance (see Section 3), DCR staking for ticket purchases is driven by expected return from PoS rewards. In each block, ticket selection follows a Poisson process with a mean of 28 days. Accordingly, gross yield on a deposit is a function of ticket price, validation reward per vote, and the probability of missing a vote. At current ticket prices, PoS rewards, and missed vote percentages for major stakepools, the annualized yield of a Decred deposit exceeds 21%. Incorporating a 0.001 DCR ticket fee and pool fees of 5%, as well as an opportunity cost of 5%, gives an implied yield of 17.9% in DCR terms. Current ticket holders must therefore anticipate DCR appreciation slightly above 10% during 2018 to offset current inflation (~30%). As the block subsidy diminishes over time, this return will decline and will have to be supplanted by transaction fees (even as inflation subsides as well). Figure 10 summarizes the annualized average yield of a PoS ticket based on PoS subsidies from 2018-2021. The results also point to an upper limit on the percentage of Decred staked as higher ticket prices require ticketholders to underwrite aggressive returns for DCR.

4.3 DCR DEMAND ASSESSMENT

The analysis of transaction volumes and staking yields reveals that demand for DCR will have to grow sustainably while retaining a balance between staking and transactions to realize incentive-alignment alongside continued network value appreciation. Currently, this balance is slightly skewed towards staking, but yields remain healthy relative to inflation and transaction volume is growing. Sustained growth in ticket prices beyond this point without commensurate transaction growth to subsidize validators will be difficult as increasing portions of DCR supply are pulled out of circulation, unless velocity of DCR circulation registers proportional increases.

FIGURE 10 ***Sensitivity of Block-Reward PoS Returns***

		Block Reward DCR Yield (Annualized Avg)			
Parameters	Changing Factors	2018	2019	2020	2021
Ticket Price	60	29%	24%	20%	16%
	85	20%	16%	13%	11%
	150	11%	9%	7%	6%
Discount	1.68%	17%	14%	11%	9%
	5%	14%	10%	8%	6%
	10%	9%	5%	3%	1%
Pool Fee	0%	21%	17%	14%	12%
	5%	19%	16%	13%	11%
	10%	18%	15%	13%	10%
Ticket Fee (DCR)	0.001	19%	16%	13%	11%
	0.1	18%	14%	12%	9%
	0.3	14%	11%	8%	6%
Missed Tickets	0.01%	19%	16%	13%	11%
	5%	18%	15%	13%	10%
	10%	17%	14%	12%	10%

Source: Authors Calculations; Data from DCRStats; **Subsidy** & PoS

SECTION V
CONCLUSION

5.1 CURRENT STATE OF THE NETWORK

Over the last two years, the Decred team has been building the foundation for a self-governing digital currency, owned and operated by a community of stakeholders. At the core of the system is Decred's consensus algorithm that aims to to strike a more equitable balance of power between miners and stakeholders. In recent months, the Decred network has been experiencing strong supply-side growth, both in terms of hash power committed to PoW and total value staked in PoS. Growth in transaction volume has also been impressive, but continues to lag behind most 'large-cap' cryptocurrencies. In terms of governance, the two major hard-fork issues put to a mainnet vote to date have been managed successfully, with strong stakeholder participation and engagement (albeit with a slight increase in voting abstention that the community will have to monitor in future mainnet votes).

5.2 LOOKING FORWARD: GOVERNANCE

In the long run, what sets Decred apart is the team's diligent focus on building the tools and community for stakeholder self-governance. While other blockchain governance systems remain in development, Decred has been live since 2016, cultivating a stakeholder community and prudently managing a gradual transition to full-blown on-chain governance. The next major milestone in Decred's governance roadmap is the upcoming Politeia update, which will serve as the foundation of Decred's future governance platform. While Decred's developers have avoided setting a specific date for launch, it appears that most of the proposal system was completed after a development push in the second half of 2017 (see Figure 11). Meanwhile, voting support was the focus in the most recent quarter. Politeia can eventually be used to facilitate on-chain disbursement of funds by stakeholders, as well a variety of community governance tools.

FIGURE 11A ***Politeia Github Commit Activity***

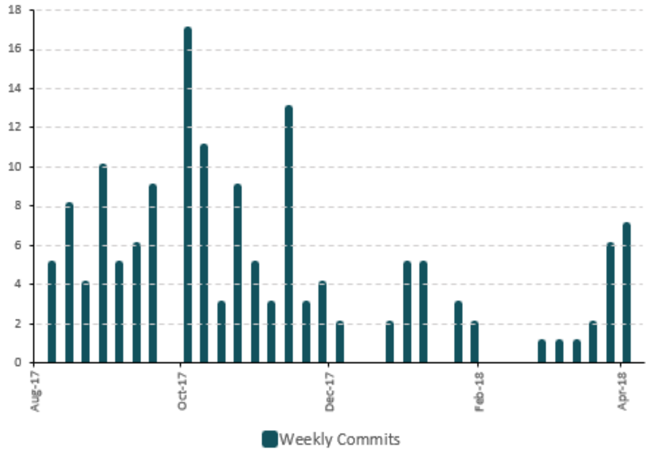
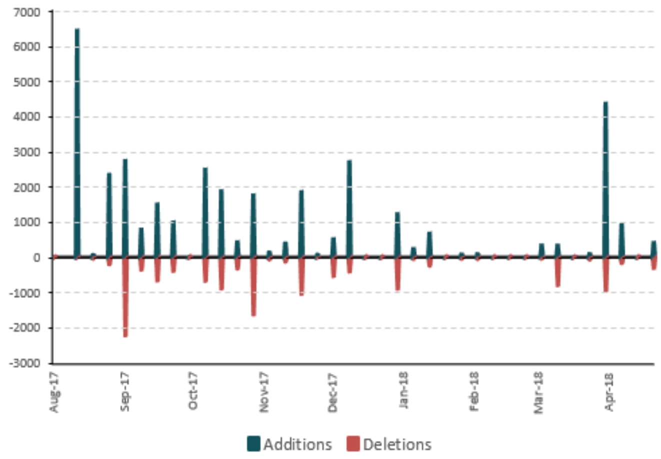


FIGURE 11B ***Politeia Github Code Frequency***



Source: Data from Github: Decred/Politeia