Eduardo F. Lima III

But Who is in Charge of Decred?: An Analysis of the Lummis-Gillibrand Responsible Financial Innovation Act applied to Decred

On March 09, 2022, President Biden issued an Executive Order on Ensuring the Responsible Development of Digital Assets ("The Order").[1] The Order outlined a whole-of-government approach to the regulation of digital assets, calling on government agencies to address risks stemming from the growth of digital assets and blockchain technology while supporting responsible innovation. The Order instructed executive as well as a handful of independent agencies to implement the stated policy goals of the United States with respect to cryptocurrencies, as outlined in The Order. A non-exhaustive list of the agencies addressed in The Order includes, the Securities and Exchange Commission ("SEC"), the Commodities Future Trading Commission ("CFTC"), and the Internal Revenue Service ("IRS").

Three months later, on June 07, 2022, Wyoming Senator Cynthia Lummis, a Republican, along with Democratic New York Senator Kirsten Gillibrand, introduced a bipartisan comprehensive crypto regulation bill – the Responsible Financial Innovation Act (hereinafter "RFIA").[2] The legislation purports to, "create a complete regulatory framework for digital assets . . . while integrating digital assets into existing law."[3] This article examines the RFIA and applies the act within the context of an existing digital asset – Decred. Decred is a cryptocurrency that challenges legal constructions as they exist today. This Paper hopes to show the reader the inadequacies of the RFIA when applied to Decred. This Paper argues that Decred

[1] THE WHITE HOUSE, EXECUTIVE ORDER ON ENSURING RESPONSIBLE DEVELOPMENT OF DIGITAL ASSETS (2022), https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets/

[2] Press Release, Senator Kirsten Gillibrand, Lummis Gillibrand Introduce Landmark Legislation to Create Regulatory Framework for Digital Assets (June 7, 2022) https://www.gillibrand.senate.gov/news/press/release/-lummis-gillibrand-introduce-landmark-legislation-to-create-regulatory-framework-for-digital-assets

[3] *Id*. at ¶ 1

is a novel technology that does not neatly fit into traditional understandings of securities, commodities, or currency. In other words, the RFIA is "sticking a square peg through a round hole" within the context of Decred.

What is Decred and How does it Work?

This part summarizes the nature and history of Decred, next discusses methods of obtaining and holding Decred, and finally discusses the current uses of Decred.

A. What is Decred?

According to Decred's official website, Decred is a blockchain-based cryptocurrency that focuses on community input, open governance and sustainable funding for development.[4] The header of the Decred website states Decred is "Money Evolved."[5] The Decred Constitution states Decred is secure, upgradable, and self-funding.[6] Decred has a system of community-based protocol governance integrated into its blockchain.[7] Decred resembles Bitcoin in some ways, yet is distinct from Bitcoin in important ways.[8] The primary distinction resides in Decred's mining consensus mechanism. Decred's consensus mechanism utilizes a hybrid Proof-of-Work ("PoW") and Proof-of-Stake ("PoS") system[9], whereas Bitcoin uses pure Proof-of-Work mining.[10] This Paper will address the distinction between PoW and PoS more thoroughly in subsection B below. First, this Paper will discuss the inception of Decred, tracing Decred's history and founding,

[4] Decred, https://docs.decred.org/ (last visited Aug. 26, 2022).
[5] Decred, https://www.decred.org/ (last visited Aug. 26, 2022).
[6] Decred, https://docs.decred.org/governance/decred-constitution/ (last visited Aug. 26, 2022).
[7] Decred, https://docs.decred.org/governance/decred-constitution/ (last visited Aug. 26, 2022
[8] This paper assumes a familiarity with how blockchains work. For a better understanding of Bitcoin, see Brian M. McCall's "How El Salvador Has Changed U.S. Law by a Bit: The Consequences for the UCC of Bitcoin Becoming Legal Tender"
[9] Decred, https://docs.decred.org/ (last visited Aug. 26, 2022).
[10] ANDREAS M. ANTONOPOLOUS, MASTERING BITCOIN: PROGRAMMING THE OPEN BLOCKCHAIN, 27 (Tim McGovern ed., 2nd ed. O'Reilly Media, Inc. 2017)

which is recounted through a collection of online talk forums and software development studio blog posts.

In April 2013, Tacotime, an anonymous user of the online bitcoin forum Bitcointalk.org, posted a white paper for, "a cryptocurrency based on a hybrid PoW/PoS system" that he called "Memcoin2 (MC2)."[11] Tacotime worked alongside another anonymous developer named "_ingsoc" (hereinafter "Ingsoc") to begin building this new cryptocurrency.[12]

In July 2013, TacoTime and Ingsoc approached the CEO of Company Zero, Jake Yokom-Piatt, asking if Yokom-Piatt and his team would be interested in assisting with the development of MC2.[13] Decred is the outgrowth of that work.[14] Before working on Decred, Company Zero had been building an alternative implementation of the Bitcoin protocol called "BTCsuite."[15] Company Zero's work on "BTCsuite" resulted in a bug-for-bug compatible alternative implementation of Satoshi Nakamoto's (the anonymous founder of Bitcoin) original implementation of the Bitcoin protocol – Bitcoin Core.[16] After years of work, however, Yokom-Piatt and his team had grown tired of the hostility they faced towards their work from Bitcoin Core developers.[17] Company Zero outlined these frustrations in a blog post in November 2015.[18]

[11] Tacotime, MC2: a cryptocurrency based on a hybrid PoW/PoS system (Apr. 7, 2013, 12:05:12 PM), https://bitcointalk.org/index.php?topic=169204.msg1760397

[12] *Decred: Where did it all begin?*, Decred Digest, https://thedecreddigest.wordpress.com/2017/06/10/decred-where-did-it-all-begin/ (last visited Aug. 26, 2022)

[13] *Dave Collins & Jake Yokom-Piatt: Decred – A Hybrid Approach to Blockchain Governance*, Epicenter Podcast (July 26, 2017) (streamed from Youtube). https://www.youtube.com/watch?v=E5mXtGvwelU&t=354s

[14] *Id.*

[15] Decred Digest, *supra* note 12.

[16] *Id.*

[17] Epicenter Podcast, *supra* note 13.

[18] Jake Yocom-Piatt, Bitcoin's Biggest Challenges (Nov. 30, 2015) https://blog.companyzero.com/2015/11/bitcoins-biggest-challenges/.

Decred was created to be an alternative to Bitcoin by focusing on sustainability and upgradeability.[19] On February 8, 2016, the Decred blockchain launched.[20] Since Decred's launch, the blockchain has undergone numerous upgrades. The current version, v 1.7.3 of the Decred software was released on May 18, 2022.[21]

B. Proof-of-Work and Proof-of-Stake

Like Bitcoin, Decred has an encoded supply cap of ~21 million coins.[22] As noted above, Decred differs from Bitcoin in that Decred's mining consensus mechanism utilizes a hybrid of Proof-of-Work and Proof-of-Stake.[23] This hybrid consensus mechanism sits at the core of Decred's distinction from Bitcoin. The hybrid consensus mechanism impacts how the coins are created, how the coins are distributed, and how the coins are utilized.

First, this section will look at Proof-of-Work and explain what it is and how it works. Next, it will examine Proof-of-Stake, and how it functions. Finally, this section will examine Decred's hybrid model and discuss its impact and implications for the Decred protocol. This section will illustrate how this hybrid model allows Decred to be self-funding and upgradeable without contentious hard forks.[24]

Proof-of-Work sits at the heart of Bitcoin's inventive genius.[25] The creator of the original blockchain, bitcoin, invented a consensus algorithm called Proof-of-Work.[26] Arguably, PoW is

[19] Epicenter Podcast, *supra* note 13.

[20] Decred Digest, *supra* note 12.

[21] Github, https://github.com/decred/decred-binaries/releases (last visited Aug. 16, 2022).

[22] Decred, Decred Constitution https://docs.decred.org/governance/decred-constitution/ (last visited Aug. 16, 2022).

[23] Decred, supra note 9.

[24] Hard Fork is "a permanent divergence in [a] blockchain; . . . [c]ommonly occurs when nonupgraded nodes don't validate blocks created by upgraded nodes that follow newer consensus rules." See, ANDREAS M. ANTONOPOLOUS & GAVIN WOOD, MASTERING ETHEREUM: BUILDING SMART CONTRACTS AND DAPPS, pg. xxix, (Rachel Roumeliotis, ET AL. eds., 1st ed. O'Reilly Media Inc., 2018). See also, ANDREAS M. ANTONOPOLOUS, MASTERING BITCOIN: PROGRAMMING THE OPEN BLOCKCHAIN, 260 (Tim McGovern ed., 2nd ed. O'Reilly Media, Inc. 2017).

[25] ANDREAS M. ANTONOPOLOUS, MASTERING BITCOIN: PROGRAMMING THE OPEN BLOCKCHAIN, 217 (Tim McGovern ed., 2nd ed. O'Reilly Media, Inc. 2017)

[26] ANDREAS M. ANTONOPOLOUS & GAVIN WOOD, MASTERING ETHEREUM: BUILDING SMART CONTRACTS AND DAPPS, 320,(Rachel Roumeliotis, ET AL. eds., 1st ed. O'Reilly Media Inc., 2018)

the most important invention underpinning bitcoin.[27] The colloquial term for PoW is "mining."[28] This colloquialism creates a misunderstanding about the primary purpose of consensus. The purpose of mining, and all other consensus models, is to secure the blockchain while keeping control of the system decentralized.[29] Proof-of-Work is the solution to a mathematical problem that miners compete to solve.[30] The difficult mathematical problem is based on a cryptographic hash algorithm.[31] The hash function SHA 256 is the function used in bitcoin's mining process.[32] In the simplest terms, mining is the process of hashing the block header repeatedly, changing one parameter, until the resulting hash matches a specific target.[33] Hashing is … The solution to the problem is included in the new block and acts as proof that the miner expended significant computing resources.[34] Mining is the invention that makes bitcoin special.[35]

Mining secures the bitcoin system and enables the emergence of network-wide consensus without a central authority.[36] Miners are rewarded with newly minted coins and transaction fees.[37] This process aligns the actions of the miners with the security of the network.[38] Miners validate new transactions and record them on the global ledger.[39] A new block, containing transactions that occurred since the last block is "mined" occurs every ten minutes.[40] Satoshi Nakamoto's main invention is the creation of a decentralized mechanism for emergent consensus.[41] The genius of the invention of bitcoin is the practical and novel solution to a

[27] *Id.*
[28] *Id.*
[29] *Id.*
[30] Antonopolous, *supra* note 25 at 214
[31] *Id*. at 214.
[32] *Id*. at 228.
[33] *Id*. at 228.
[34] *Id.* at 214.
[35] Id. at 213.
[36] *Id.*
[37] *Id.*
[38] *Id.*
[39] *Id.*
[40] *Id.*
[41] *Id.*

problem in distributed computing known as the "Byzantine Generals' Problem."[42] In short, the problem consists of trying to agree on a course of action or the state of a system over an unreliable network. Nakamoto's solution uses the concept of Proof-of-Work to achieve consensus without a central trusted authority. This results in hostile actors coordinating together in adverse conditions to determine the final state of the ledger. Proof-of-Work solved the Byzantine Generals Problem by connecting the bitcoin network consensus to a real-world scarcity, electricity[43]. Miners compete to solve a difficult mathematical problem based on a cryptographic hash algorithm.[44]

In Bitcoin, Proof-of-Work miners provide 100% of the network security by creating an unforgeable costliness to the production of each block.[45] For their efforts, miners are rewarded with newly minted Bitcoins in a transaction known as the "coinbase" transaction.[46] This transaction accounts for all newly minted bitcoin. In Decred, miners function similarly as they do for Bitcoin. However, Decred has integrated a Proof-of-Stake mechanism, and with Decred, miners only receive 10% of the block reward.[47]

Historically, Proof-of-Work was not the first consensus algorithm proposed.[48] Preceding the introduction of Proof-of-Work, many researchers had proposed variations of consensus algorithms based on financial stake, now called Proof-of-Stake.[49] The Proof-of-Stake (PoS) model ultimately adopted by Decred was first introduced in a paper by Sunny King and Scott Nadal in 2012 and was intended to solve the problem of Bitcoin mining's high energy

[42] *Id.* at 4.
[43] *Id.* at 26.
[44] *Id.* at 214.
[45] *Id.* at 26.
[46] *Id.* at 120.
[47] Decred, https://docs.decred.org/ (last visited Aug. 26, 2022).
[48] Antonopolous & Wood, *supra* note 26 at 320.
[49] *Id.*

consumption.[50] Roughly speaking, Proof-of-Stake means a form of proof of ownership of the currency.[51] Proof-of-Stake attempts to achieve similar security guarantees as Proof-of-Work in a more carbon neutral way by assigning to the blockchain's underlying asset the right to approve blocks. There are various implementations of Proof-of-Stake. In general, a PoS algorithm works as follows: the blockchain keeps a track of a set of validators, and anyone who holds the blockchains base currency (in Decred's case, DCR) can become a validator by sending a special transaction that locks up their DCR into a deposit.[52] The validators take turns proposing and voting on the next valid block. In some PoS systems, the weight of a validators vote depends on the size of its deposit (stake). Thus, PoS forces validators to act honestly and follow consensus rules by a system of reward and punishment.[53]

The major difference between PoS and PoW is that the punishment in PoS in intrinsic to the blockchain (e.g., loss of staked DCR), whereas in PoW the punishment is extrinsic (e.g. loss of funds spent on electricity).[54] Moreover, the Proof-of-Stake typically involves time locking some of a blockchain's native asset for a fixed or indeterminate amount of time. There are various blockchain implementations of Proof-of-Stake today including Solana, Polkadot, and Cardano to name a few. Legal commentators have already discussed some of the issues of Proof-of-Stake.[55] Ethereum, the second largest crypto currency by market cap, plans to switch from Proof-of-Work to Proof-of-Stake by mid-September, 2022.[56]

[50] Sunny King & Scott Nadal, *PPCoin: Peer-to-peer Crypto-Currency with Proof of Stake* (Aug. 19, 2012) https://decred.org/research/king2012.pdf

[51] *Id.*

[52] Antonopolous & Wood, *supra* note 26 at 321.

[53] *Id*. at 321.

[54] *Id.*

[55] Jessica S. Hart, Note, *Policing Proof-of-Stake Networks: Regulatory Challenges Presented by Staking-as-a-Service Providers and the Need for a Tailored Regime*, 23 Colum. Sci. & Tech. L. Rev. 192 (2021).

[56] Richard Lawler, Ethereum's big proof-of-stake blockchain switch could happen on September 15th, The Verge, (Aug. 11, 2022 1:09 PM), https://www.theverge.com/2022/8/11/23301638/ethereum-crypto-blockchain-proof-of-stake-environment

Decred utilizes a hybrid Proof-of-Work and Proof-of-Stake system. In Decred, Proof-of Stake mining serves as a complement to Proof-of -Work.[57] This hybridization allows Decred to have features that cause users to refer to Decred as an "autonomous" digital-currency. This Paper will explain how this hybrid model works, and why it is needed in Decred.

To participate in PoS voting in Decred, stakeholders lock some DCR in return for a ticket.[58] An individual stakeholder can purchase one or more tickets.[59] The amount of DCR locked, or "Ticket Price," is adjusted dynamically every 144 blocks (~12 hrs).[60] The current ticket price can be found on the Decred block explorer.[61] Every ticket owned gives its holder the ability to cast a single vote.[62] Upon voting, each ticket returns a small reward plus the original Ticket Price of the ticket.[63]

In Decred, miners serve as the first layer of security for the network. Miners deploy computing power to the network to solve the Proof-of-Work equation based on Blake-256 hashing function.[64] The hybrid system works by first allowing PoW miners to create a block. Once a miner has solved the mathematical problem, it may propose the new block to PoS miners.[65] PoS voters, also known as "Stakeholders," can override PoW miners, if 50% or more of the Stakeholders vote against a particular block created by a miner.[66] In each newly proposed block, 5 ticket holders are called to vote through a lottery mechanism.[67]

[57] Decred, https://docs.decred.org/proof-of-stake/overview/ (last visited Aug. 26, 2022)
[58] *Id.*
[59] *Id.*
[60] *Id.*
[61] Decred, https://dcrdata.decred.org/ (last visited Aug. 26, 2022)
[62] Decred, https://docs.decred.org/proof-of-stake/overview/ (last visited Aug. 26, 2022).
[63] *Id.*
[64] Decred, https://docs.decred.org/mining/overview/ (last visited Aug. 26, 2022).
[65] Decred, *supra* note 56.
[66] Id.
[67] *Id.*

In a Proof-of-Stake system, users must own the underlying asset in order to lock up their coins. Due to this inherent limitation, Decred had to find a way to get its coins into the hands of users before the blockchain launched, if it wanted the chain to start from the beginning as a hybrid of the two consensus mechanisms. To this end, Decred conducted an "airdrop" of the coins to community members before launch.[68] Sign-up for the airdrop opened with a public announcement on December 15th, 2015 and closed on January 18th, 2016.[69] Not all participants who signed up were selected to participate in the airdrop.[70] When the airdrop concluded, 282.63795424 DCR was awarded to 2,972 participants.[71]

Stakeholders make and enforce the blockchain's consensus rules, set a course for future development, and decide how the project's treasury is used to fund it.[72] Decred's blockchain is similar to Bitcoin's, but with major aspects of governance baked into the protocol.[73] For example, voting is central to Decred's governance. Tickets vote to approve or reject the previous block of transactions created by a PoW miner.[74] At least three out of five tickets called to vote must vote for the block to be mined.[75] If the majority of votes are rejecting the previous block, the miner who produced that block loses their block reward, and the transactions from that block are returned to the mempool.[76] The mempool is the collection of pending transactions that have been broadcast to the network, but are yet to be included in a fully validated block.

Further, Proof of Work miners play a similar role for Decred as they do for Bitcoin, but with Decred miners only receive 10% of the block reward.[77] Proof-of Stake-voting is central to

[68] Decred, https://docs.decred.org/advanced/premine/ (last visited Aug. 26, 2022).
[69] *Id.*
[70] *Id.*
[71] *Id.*
[72] Decred, https://docs.decred.org/ (last visited Aug. 26, 2022).
[73] *Id.*
[74] Decred, https://docs.decred.org/governance/overview/ (last visited Aug. 26, 2022).
[75] *Id.*
[76] I*d.*
[77] Decred, https://docs.decred.org/ (last visited Aug. 26, 2022).

Decred's governance. Decred holders can time-lock (or "stake") DCR to obtain voting tickets.[78] Tickets are randomly called to vote on-chain; this involves both approving the work of PoW miners and voting Yes/No on any open rule change proposals.[79] 80% of the block reward goes to the holders of the tickets that voted in that block.[80] The remaining 10% of the block reward goes into the Decred Treasury.[81] Holders of live tickets decide how that treasury is used through "Politeia," an online forum for proposals and voting.[82]

C. Politeia and Protocol Governance

Decred governance is based on the principle of ticket-holder voting.[83] Changes to the system are voted on and implemented only if the voters approve.[84] Anybody who holds enough DCR may time-lock their coins to purchase tickets and participate in governance.[85] Some of the ticket-holder voting occurs on-chain, and some of it off-chain. Consensus changes and individual block validation takes place on-chain.[86] Voting on issues such as treasury management take place off-chain, but it is still backed by cryptographic techniques that prevent sybil attacks and unfair censorship.[87]

To participate in PoS voting, stakeholders lock some DCR in return for a ticket.[88] An individual stakeholder can purchase one or more tickets.[89] The necessary amount of DCR locked, or "Ticket Price," is adjusted dynamically every 144 blocks (~12 hrs).[90] The current ticket price

[78] *Id.*
[79] Decred, https://docs.decred.org/ (last visited Aug. 26, 2022).
[80] *Id.*
[81] *Id.*
[82] *Id.*
[83] Decred, https://docs.decred.org/governance/overview/ (last visited Aud. 26, 2022).
[84] *Id.*
[85] *Id.*
[86] *Id.*
[87] *Id.*
[88] Decred, https://docs.decred.org/proof-of-stake/overview/ (last visited Aug. 27, 2022)
[89] *Id.*
[90] *Id.*

can be found in Decrediton or on dcrdata.decred.org.[91] Every ticket owned gives its holder the ability to cast a single vote.[92] Upon voting, each ticket returns a small reward plus the original Ticket Price of the ticket.[93] Tickets are selected pseudorandomly according to a Poisson distribution.[94] The average time it takes for a ticket to vote is 28 days, but possibly requiring up to 142 days, with a 0.5% chance of expiring before being chosen to vote (this expiration returns the original Ticket Price without a reward).[95] Every block mined must include a minimum of 3 votes (miners are penalized by a reward deduction if fewer than 5 votes are included).[96]

Further, Decred's process for amending the consensus rules is also driven by stakeholder voting. The process begins when at least 95% of PoW miners and 75% of PoS voters have upgraded their software to a new version with latent changes to the rules.[97] Once these conditions are met, then a voting period of 8,064 blocks (~4 weeks) begins, to decide whether the latent rule changes should be activated.[98] For a rule change proposal to be approved, at least 75% of the tickets not set to Abstain must vote Yes.[99] If this requirement is met, and a quorum of 10% tickets voting Yes or No is achieved, then the rule change will be activated 8,064 blocks (~4 weeks) later.[100]

Politeia is Decred's proposal system.[101] It is used to request funding from the Decred treasury.[102] Anyone may submit a proposal on Politeia, the only requirement is paying a minimal fee that is designed to prevent spam.[103] Ticket holders are then able to vote on whether they are

[91] *Id.*
[92] *Id.*
[93] *Id.*
[94] *Id.*
[95] *Id.*
[96] *Id.*
[97] Decred, https://docs.decred.org/governance/consensus-rule-voting/overview/ (last visited Aug. 26, 2022).
[98] *Id.*
[99] *Id.*
[100] *Id.*
[101] Politeia, https://proposals.decred.org/ (last visited Sept. 3, 2022).
[102] *Id.*
[103] Decred, https://docs.decred.org/governance/overview/ (last visited Aug. 26, 2022).

for or against the proposal.[104] The voting period lasts one week, allowing anyone who holds tickets at the moment voting begins to vote on the proposal.[105] All data on Politeia (proposals, comments, upvotes/downvotes) is periodically anchored into the Decred blockchain, using dcrtime.[106] Dcrtime is a timestamping application that allows users to store hashes of arbitrary data on the Decred blockchain.[107] This auditability enables users to cryptographically prove if censorship has occurred.[108]

D. Usage of Decred

Decred is money evolved.[109] To this end, Decred is seen by investors and enthusiasts as a store of value. This primary use case is achieved by acquiring Decred, either through mining or from an exchange, holding Decred, a fixed supply currency, as opposed to state issued currencies that have been free floating and continually debased since 1971. Furthermore, over the last year, United States inflation has reached local highs.[110] Decred users choose to purchase DCR, the native currency of the Decred blockchain, in order to preserve their purchasing power. It is true that Decred's price undergoes extreme volatility. Within the last 6 months, Decred went from ~$250 to ~$20.00.[111] Although these violent swings in price seem to dispel any idea of store of value, Decred holders usually buy with an intended time frame long enough to weather the volatility.[112] Since Decred's inception, Decred has always been up in price in a three-year window.[113]

[104] *Id.*
[105] *Id.*
[106] *Id.*
[107] Decred, https://docs.decred.org/advanced/dcrtime/ (last visited Aug. 26, 2022).
[108] Decred, https://docs.decred.org/governance/overview/ (last visited Aug. 26, 2022).
[109] Decred, https://decred.org/ (last visited Aug. 26, 2022).
[110] Bureau of Labor Statistics, U.S. Department of Labor, The Economics Daily, Consumer Price Index unchanged over the month, up 8.5 percent over the year, in July 2022 at https://www.bls.gov/opub/ted/2022/consumer-price-index-unchanged-over-the-month-up-8-5-percent-over-the-year-in-july-2022.htm (visited September 07, 2022).
[111] Coingecko, https://www.coingecko.com/en/coins/decred (last visited Aug. 27 2022).
[112] This is an opinion of the author based on personal experiences.
[113] *supra* note 111.

Users of Decred can transact in Decred for goods and services. One of the most pertinent of such payments is paying for development of the protocol.[114] Protocol developers can be corporate entities or independent contractors.[115] A non-exhaustive list of corporate entities that have contracted with decred includes Company 0, Raedah Group, and Eeter.[116] Decred currently has over 50 combined independent contractors and employees of corporate entities.[117]

Another use of Decred is paying a small fee in order to submit a proposal to Politeia, the online governance forum.[118] Anyone can post a proposal, but they must spend a small amount of Decred to have their posts show up.[119] The purpose of this small fee is to prevent spam on the forum.[120]

Another use of Decred is Staking.[121] As discussed above, Staking is the process whereby a user can lock their Decred for an indiscriminate amount of time up to 142 days.[122] Users receive a ticket in exchange for locking up their Decred.[123] This ticket gives the holder the right to vote on any proposals that are up during this time.[124] Once a user's ticket has been voted, he receives a portion of the next block reward along with his original locked deposit.[125]

Yet another use of Decred is to retain financial privacy.[126] This privacy is achieved through a mixing protocol that was used to create Decred CoinJoin transactions called Coinshuffle++.[127] CoinShuffle++ is a non-custodial process for creating CoinJoin transactions,

[114] Decred, https://docs.decred.org/contributing/overview/ (last visited Sept. 7, 2022).
[115] Decred, https://docs.decred.org/contributing/contributor-compensation/ (last visited Sept. 7, 2022).
[116] *Id.*
[117] *Id.*
[118] Decred, https://docs.decred.org/governance/overview/ (last visited Aug. 26, 2022).
[119] *Id.*
[120] *Id.*
[121] Decred, https://docs.decred.org/proof-of-stake/overview/ (last visited Aug. 27, 2022).
[122] *Id.*
[123] *Id.*
[124] *Id.*
[125] *Id.*
[126] Decred, https://docs.decred.org/privacy/general-privacy/ (last visited Aug. 27, 2022).
[127] Decred, https://docs.decred.org/privacy/cspp/overview/ (last visited Aug. 26. 2022).

where the output addresses are anonymized via a mixnet.[128] This particular transaction is available to both stakeholder and non-stakeholders.[129]

Additionally, another use of Decred is to exchange Decred for another cryptocurrency (such as Bitcoin) through a protocol integrated atomic swap decentralized exchange.[130] An "atomic swap" is where one digital asset is exchanged for another (e.g., exchange Decred for Bitcoin) without the use of a trusted third-party intermediary, such as a centralized exchange.[131]

Finally, one of the most important uses of Decred is using Decred as a strong guarantee of property rights. Property rights are attached because Decred is an asset that is impervious to takings by the State. When a user holds Decred in a wallet to which the user maintains the private key, it is impossible for the State to confiscate this from the user, in the same way governments can freeze one's bank account or seize one's house.

. Regulatory Uncertainty: Decred and the RFIA

In this section, Part A provides the reader with some current historical context which frames the introduction of the RFIA. In part B, this paper highlights new terms and definitions introduced in the RFIA. Additionally, Part C explains how the RFIA seeks to create a complete regulatory framework for digital assets. Finally, in part D, this Paper shows why Decred does not fit the proposed framework and how the RFIA creates as many questions as answers when it comes to Decred.

[128] Decred Blog, https://blog.decred.org/2019/08/28/Iterating-Privacy/ (last visited Aug. 26 2022)
[129] *Id.*
[130] Decred, https://dex.decred.org/ (last visited Aug. 26. 2022).
[131] Decred, https://docs.decred.org/advanced/atomic-swap/ (last visited Aug. 27, 2022).

A. The Need for Regulation

On June 6, 2022, Senators Cynthia Lummis and Kirsten Gillibrand proposed the Lummis-Gillibrand Responsible Financial Innovation Act to the United States Senate. [132] The RFIA's stated purpose is "to provide for responsible innovation and bring digital assets within the regulatory perimeter."[133] Senator Lummis reported that the RFIA is unlikely to see a vote this year.[134]

Commentators have noted that, "perhaps the greatest importance the RFIA provides is answer to the most foundational question affecting individuals in the digital asset space - when is activity involving digital assets governed by the federal securities laws and when do federal commodities laws properly apply."[135] To answer this question, the RFIA adopts a novel approach, addressing the concerns raised by the SEC by imposing disclosure obligations on companies that raise funds through the sale of digital assets, even where the funds were raised in private placement transactions.[136]

Broadly speaking, the RFIA proposes that the Commodities Future Trading Commission becomes the default regulator of digital assets.[137] Under the RFIA, a vast majority of digital assets would be presumed commodities with more lenient rules and regulations. The Chairman of the SEC, Gary Gensler, has opposed the RFIA.[138] Gensler believes that most digital assets are

[132] Lummis-Gillibrand Responsible Financial Innovation Act, S.4356, 117th Cong. (2022), http://www.congress.gov/.

[133] Press Release, *supra* note 1.

[134] Alex Nguyen & Allyson Versprille, *Crypto-Regulation Bill Unlikely to Get Senate Vote This Year*, Bloomberg (July 19, 2022, 9:27 AM), https://www.bloomberg.com/news/articles/2022-07-19/crypto-bill-unlikely-to-get-senate-vote-this-year-lummis-says#xj4y7vzkg

[135] Lewis Cohen & Freeman Lewin, RFIA proposals introduce innovative digital asset regulation through ancillary assets, IFLR (June 14, 2022), https://www.iflr.com/article/2a89wn78h6ljzwr097xts/rfia-proposals-introduce-innovative-digital-asset-regulation-through-ancillary-assets

[136] *Id.*

[137]

[138] Paul Kiernan, *Crypto Legislation Could Undermine Market Regulations*, Wall St. J. (June 14, 2022 3:39 PM), https://www.wsj.com/articles/crypto-legislation-could-undermine-market-regulations-gensler-says-11655231512

securities and should be regulated by the SEC.[139] Gensler has said the Lummis-Gillibrand Bill undermines the traditional finance system.[140]

The SEC under Gensler's command has found success in prosecuting cryptocurrency projects. In June 2019, the SEC filed a complaint in the Southern District of New York against Kik Interactive Inc., which sold one trillion of its digital tokens called "Kin" in 2017.[141] Kik claimed that the funds from the offering would help create a "Kin Ecosystem" revolving around its new token.[142] Kin stated the limited supply of Kin tokens along with the ecosystem they anticipated building would cause the token to appreciate.[143] After Kik raised almost $100 million from investors, the SEC subsequently charged Kik with violating Sections 5(a) and 5(c) of the Securities Act of 1933.[144] The SEC alleged the Kin tokens should have been registered as securities and accompanied by the proper investor disclosures.[145]

On Sept. 30, 2020, the Court sided with the SEC.[146] The SEC successfully argued Kik's offering met all three criteria for an investment contract as outlined in *Howey*. The Court sided with the SEC, granting the commission's motion for summary judgment and requiring Kik to pay a $5 million penalty.[147] The Court reasoned that money had been invested in a single integrated scheme with the expectation by investors that they would see a return generated by Kik's future projects.[148]

[139] SEC chair Gary Gensler on his vision for cryptocurrency regulation, Squawk Box (Aug. 4, 2021) (streamed from CNBC), https://www.cnbc.com/video/2021/08/04/sec-chair-gary-gensler-on-his-vision-for-cryptocurrency-regulation.html

[140] Kiernan, *supra* note 116.

[141] *See*, SEC v. Kik Interactive Inc., 1:19-cv-05244.

[142] *Id.* at 3.

[143] *Id.* at 4.

[144] *Id.* at 6.

[145] *Id.* at 6.

[146] Press Release, SEC Obtains Final Judgment Against Kik Interactive For Unregistered Offering (Oct. 20, 2020), https://www.sec.gov/news/press-release/2020-262#

[147] *Id.*

[148] *Id.*

Perhaps most prominently, the SEC brought a lawsuit against Ripple Labs Inc. and certain of its executives in December 2020, alleging that the defendants raised over $1.3 billion through an unregistered, ongoing digital asset securities offering.[149] In that case, the cryptocurrency at issue is XRP, which is at time of writing the seventh most valuable cryptocurrency in the world.[150] The SEC's complaint alleges that the defendants raised money by selling the XRP token in an unregistered securities offering to investors in exchange for non-cash consideration, such as labor and market-making services.[151] The complaint also alleges that the defendants failed to register their offers and sales of XRP or satisfy any exemption from registration, which was in violation of the registration provisions of the federal securities laws.[152] On March 11, 2022, the individual defendants' respective motions to dismiss were denied.[153]

A. Key Definitions

The RFIA begins with a proposed amendment to Subtitle VI of Title 31 of the United States Code – Money and Finance.[154] The amendment proposes ten new terms be added to the definition section of the Money and Finance subtitle of the Code. These terms are used throughout the RFIA in the RFIA’s proposed amendments tor the Securities Exchange Act of 1934, the Commodities Exchange Act, and the Internal Revenue Code. The most relevant terms for this Paper’s purposes are outlined below:

[149] See, SEC v. Ripple Labs, Inc., 1:20-cv-10832, document 4 at pg. 1, https://www.sec.gov/litigation/complaints/2020/comp-pr2020-338.pdf
[150] Coingecko, https://www.coingecko.com/en/coins/xrp (last visited Aug. 27, 2022).
[151] *Id.* at 14.
[152] *Id.* at 1.
[153] SEC v. Ripple Labs, Inc., 1:20-cv-10832, document 441, https://www.nysd.uscourts.gov/sites/default/files/2022-03/Ripple%20-%20Order%20on%20Motion%20to%20Dismiss.pdf
[154] Lummis-Gillibrand Responsible Financial Innovation Act, S.4356, 117th Cong. (2022), http://www.congress.gov/

"Distributed Ledger Technology" is defined as: technology that enables the operation and use of a ledger that is shared across a distributed set of nodes, is synchronized between nodes, has data appended to the ledger by following specific consensus mechanism of the ledger, may be accessible to anyone or a subset of participants.[155]

"Digital asset" is defined as:

> (A) [a] natively electronic asset that (i) confers economic, proprietary, or access rights or powers; and (ii) is recorded using cryptographically secured distributed ledger technology, or similar analogue; and (B) includes (i) virtual currency and ancillary assets in accordance with section 2(c)(2)(F) of the Commodities Exchange Act; (ii) payment stablecoins . . .; and (iii) any other security or commodity that meets the requirements of subparagraph (A).[156]

The language "any other security or commodity. . .," in (iii) implies that a digital asset can be either a security or a commodity.

"Smart Contract" is defined as:

> computer code deployed to a distributed ledger technology network that executes instruction based on the occurrence or nonoccurrence of specified conditions; or (ii) any similar analogue; and (B) includes taking possession or control of a digital asset and transferring the asset or issuing executable instructions for these actions.[157]

"Virtual Currency" is defined as:

> (A) means a digital asset that– (i) is used primarily as a medium of exchange, unit of account, store of value, or any combination of such functions; (ii) is not legal tender, as described by Section 5103; and (iii) does not derive value from or is backed by an underlying financial asset (except other digital assets); and (B) … [158]

Further, the RFIA introduces other new terms throughout its text that are relevant to this analysis. There are two terms proposed to be added to each the Securities Exchange Act and the Commodities Exchange Act. Then, there is one new term proposed to be added to the Internal

[155] Id. at 7.
[156] S.4356 at 4-5
[157] *Id.* at 9.
[158] *Id.* at 10.

Revenue Code. They are noted in this key definitions section for convenience but will be more thoroughly addressed in later sections of the paper.

For example, "Foreign Private Issuer" is a new term found and defined in Title III Sec. 301 of the RFIA, which proposes amending the Securities Exchange Act of 1934 by adding an entirely new "Section 41" to the end of the '34 Act. Foreign private issuer is defined as:

> a foreign issuer, other than a foreign government, except that the term does not include a foreign issuer that, as of the last business day of the most recently completed fiscal quarter of the issuer, satisfies the following conditions: (A) more than 50 percent of the outstanding voting securities of the issuer are directly or indirectly owned by residents of the United States. (B) Any of the following: (i) the majority of the executive officers or directors of the issuer are citizens or residents of the United States; (ii) More than 50 percent of the assets of the issuer are located in the United States; (iii) the business of the issuer is principally administered in the United States.[159]

Next, the term "Ancillary Assets" is a newly proposed statutorily defined term also found in Title III Sec. 301 of the RFIA.[160] If the RFIA is adopted, ancillary asset would be defined as, "an intangible, fungible asset that is offered, sold, or otherwise provided to a person in connection with the purchase and sale of a security through an arrangement or scheme that constitutes an investment contract as that term is used in section 2(a)(1) of the Securities Act of 1933. . ."[161] Explicitly excluded from the definition of an ancillary asset is:

> an asset that provides the holder of the asset with any of the following rights in a *business entity*: (i) A debt or equity interest in that entity. (ii) Liquidation rights with respect to that entity. (iii) An entitlement to an interest or dividend payment from that entity. (iv) A profit or revenue share in that entity solely from the entrepreneurial or managerial efforts of others. (v) Any other financial interest in that entity.[162]

Interestingly, this same list of exclusions is found in the second definition of "Digital Asset" proffered by the RFIA, located in Title IV, Sec. 401 of the RFIA. Title IV proposes amending the definition of "Commodity" in the Commodities Exchange Act to include ". . . a digital asset

[159] *Id.* at 27.
[160] *Id.* at 26.
[161] *Id.* at 26.
[162] *Id.* at 26-27 (emphasis added).

(consistent with section 2(c)(2)(F))".[163] As outlined in Title IV, digital asset means, "the meaning given the term in section 9801 of title 31, United States Code."[164] The definition of digital asset, as it would be added to the Commodities Exchange Act, is specifically defined to exclude:

> an asset that provides the holder of the asset with any of the following rights in a *business entity*: (i) A debt or equity interest in that entity. (ii) Liquidation rights with respect to that entity. (iii) An entitlement to an interest or dividend payment from that entity. (iv) A profit or revenue share in that entity solely from the entrepreneurial or managerial efforts of others. (v) Any other financial interest in that entity.[165]

This exclusionary list of properties makes clear that any asset that has one of the five exclusionary properties, whether a digital asset or an ancillary asset, is excluded from the jurisdiction of the Commodity Futures Trading Commission. Presumptively, such an asset is to remain within the jurisdiction of the Securities Exchange Commission.

Subsequently, the RFIA proposes a definition for "Decentralized Autonomous Organization."[166] The RFIA proposes amending Section 7701(a) of the Internal Revenue Code to define Decentralized Autonomous Organization as:

> an organization (i) which utilizes smart contracts (as defined in section 9801 of title 31, USC) to effectuate collective action for a business, commercial, charitable, or similar entity, (ii) governance of which is achieved primarily on a distributed basis, and (iii) which is properly incorporated or organized under the laws of a State of foreign jurisdiction as a decentralized autonomous organization, cooperative, foundation, or any similar entity.[167]

The RFIA also classifies DAO's as "a business entity which is not a disregarded entity.[168] In other words, a DAO that meets the statutory definition for Decentralized Autonomous Organization will be regarded as a business entity.

[163] Section 2(c)(2)(F) is new section of the CEA proposed by the RFIA. This Paper will address this section in more detail later in the paper.
[164] see *supra* note 155.
[165] S.4356 at 48-49
[166] *Id.* at 18.
[167] *Id.*
[168] *Id.* at 17.

Further, “Digital Asset Exchange” means a centralized or decentralized platform which facilitates the transfer of digital assets.”[169] Digital Asset Exchange” means a trading facility that lists for trading at least 1 digital asset.[170] “Registered Digital Asset Exchange” means a digital asset exchange registered under section 5i of the Commodity Exchange Act.[171]

B. How the RFIA Regulates Digital Assets

Section B provides a detailed overview of the various amendments to the enabling statutes of the SEC, CFTC, and IRS proposed by the RFIA with the goal to create a cohesive regulatory framework. This Section is then subdivided into (i) and (ii) for ease of understanding. Subsection (i) will discuss the RFIA’s proposed changes to the Securities Exchange Act of 1934. Then, subsection (ii) will discuss the RFIA’s proposed changes to the Commodities Exchange Act.

As legal practitioners have noted, the RFIA functions by separating the asset itself from the arrangement or scheme used to issue the asset.[172] In general, digital assets will be commodities.[173] However, arrangements or schemes which constitute an investment contract within the meaning of section 2(a)(1) of the Securities Exchange Act of 1933 shall remain within the jurisdiction of the SEC.[174]

i. Responsible Securities Innovation

Title III of the RFIA proposes amending the Securities Exchange Act of 1934 by adding an entirely new Sec. 41 titled “Securities Offerings Involving Certain Intangible Assets” to the

[169] *Id.* at 16.
[170] *Id.* at 49.
[171] *Id.* at 51.
[172] See *supra* note 134.
[173] S.4356 at 48.
[174] *Id.* at 54.

end of the '34 Act.[175] The proposed amendment defines a new statutory term, "ancillary assets,"[176] and imposes disclosure requirements on *certain* issuers who indirectly or directly provide an ancillary asset to investors through an arrangement or scheme that constitutes an investment contract, as that term is used in section 2(a)(1) of the Securities Act of 1933.[177] The issuers who must comply with these disclosure requirements are outlined in subsection (b)(1) - (3) to the newly proposed Sec. 41. The language specifying who must comply with the disclosure requirements is repeated in each subsection (b)(1)-(3) and reads:

> [A]n issuer engaged in business in or affecting interstate commerce, or that is organized outside of the United States and is not a foreign private issuer, that offers, sells, or otherwise provides a security through an arrangement or scheme that constitutes an investment contract . . . shall be subject to the periodic disclosure requirements . . .[178]

Recall from the key definition section above, "Foreign Private Issuer" is a statutorily defined term proposed to be added via amendment to the Securities Exchange Act of 1934 by the RFIA. "Foreign Private Issuer" means a foreign issuer (other than a foreign government).[179] Foreign Private Issuer does not include issuers who meet certain requirements regarding (1) the citizenship or residency of the issuer's executive officers and/or directors, (2) the location of the assets of the issuer, and (3) the principal place of business of the issuer[180] (see definition of Foreign Private Issuer above). Under the RFIA, Foreign Private Issuers are not subject to the disclosure requirements imposed by proposed Sec. 41. Additionally, under the RFIA, an ancillary asset provided by issuers who are subject to Sec. 41's reporting requirements will be "presumed . . . to be a commodity, consistent with section 2(c)(2)(F) of the Commodity Exchange Act . . . and not . . . a security" so long as the issuer is in compliance with the periodic disclosure

[175] *Id.* at 26.
[176] *Id.* at 26-27.
[177] *Id.* at 31-32.
[178] *Id.* at 28-31.
[179] *Id.* at 27.
[180] *Id.* at 27-28.

requirements imposed by Sec. 41.[181] Title III Sec. 302 of the RFIA also outlines conditions under which an issuer can cease periodic reporting.[182]

ii. Responsible Commodities Innovation

Arguably, the most impactful section of the RFIA is located in Title IV Sec. 403 titled, "CFTC Jurisdiction over Digital Assets."[183] The RFIA proposes amending Section 2(c)(2) of the Commodity Exchange Act by adding a new subsection (F) to the end of Section 2(c)(2). The new Section 2(c)(2)(F) is titled "Commission Jurisdiction Over Digital Asset Transactions."[184]

As the title suggests, Section 2(c)(2)(F) grants the CFTC "exclusive jurisdiction over any agreement, contract, or transaction involving a contract of sale of a digital asset in interstate commerce, including ancillary assets (consistent with Section 41(b)(4) of the Securities Exchange Act of 1934)."[185] In other words, the CFTC has jurisdiction over "ancillary assets" so long as the ancillary asset is in compliance with section 41(b)(4) of the '34 Act. Further, the CFTC is given jurisdiction over digital assets.[186] Recall that digital assets, as the RFIA defines the term in the Commodity Exchange Act, would not include any asset that provides the holder of the asset with any of the five rights, in a business entity, discussed previously.

Further, section 2(c)(2)(F) clarifies the SEC shall remain in charge of the periodic reporting requirements made by an issuer that provided the holder of a security with an ancillary asset.[187] Section 2(c)(2)(F) also reinforces that the SEC shall retain jurisdiction over "the security that constitutes an investment contract (within the meaning of section 2(a)(1) of the Securities Act of 1933."[188] Finally, it is worth noting that the new proposed Section 2(c)(2)(F) imposes a

[181] *Id.* at 32
[182] *Id.* at 42.
[183] *Id.* at 52.
[184] *Id.* at 53.
[185] *Id.*
[186] *Id.*
[187] *Id.* at 54.
[188] *Id.* at 53.

fungibility requirement. The CFTC shall only exercise jurisdiction over an agreement, contract, or transaction involving "a digital asset that is fungible, which shall not include digital collectibles and other unique digital assets."[189]

(iii) Responsible Taxation of Digital Assets

Title II of the RFIA proposes various amendments to the Internal Revenue Code, which seeks to create a rational framework for the taxation of digital assets. This paper will not focus on the policy rationale or offer the author's opinion of the tax policy as reflected in the RFIA. Instead, this paper highlights the relevant sections of the RFIA's proposed changes to the IRC for purposes of our analysis of Decred.

The most important addition to the IRC proposed by the RFIA is the creation, recognition, and definition of "Decentralized Autonomous Organizations."[190] "The default classification of a decentralized autonomous organization shall be as a business entity which is not a disregarded entity."[191] The second noteworthy portion of Title II is the deferral of income recognition for certain digital asset activities. The RFIA provides that, for individuals who receive income from mining or staking, the income from such activities will not be included in gross income for the taxpayer until the taxable year of disposition of the assets produced or received from the mining or staking activities."[192] Income will not include gain or loss from the sale or exchange of virtual currency in a "personal transaction."[193] This gain or loss cannot exceed $200 in aggregate.[194] This exclusion does not apply when a virtual currency is sold or exchanged for "cash, cash equivalents, digital-assets (as defined in section 9801 of title 31,

[189] *Id.* at 54.
[190] See *supra* note 166.
[191] S.4356 at 17
[192] *Id.* at 23.
[193] *Id.* at 11.
[194] *Id.* at 11.

United States Code), or other securities or commodities."[195] Virtual currency is defined as having "the meaning given the term in section 9801 of title 31, United States Code."[196] Moreover, the RFIA requires the Secretary of treasury to provide guidance within 1 year regarding the "classification of forks, airdrops, and similar subsidiary value as taxable, contingent upon the affirmative claim and disposition."[197]

C. The RFIA applied to Decred.

To begin the analysis, recall the definition of "virtual currency" outlined in Title I of the RFIA, which amends Subtitle IV of title 31, United States Code – Money and Finance. Virtual currency is a digital asset used primarily as a medium of exchange, unit of account, store of value or any combination of such functions. A virtual currency cannot be legal tender. A virtual currency cannot derive value from or be backed by an underlying asset. Decred satisfies these requirements because Decred is used primarily as a store of value and medium of exchange.[198] Decred is a virtual currency as defined by the RFIA.

The term "Digital Asset" is defined twice in the RFIA. The first definition of digital asset appears as an amendment to the Money and Finance subtitle of the United States Code mentioned in the paragraph above.[199] The second definition of digital asset appears as an amendment to the Commodity Exchange Act.[200]

In the Commodity Exchange Act, "digital asset" is given the same meaning as the term is defined in the Money and Finance subtitle of the United States Code with one exception; for purposes of the Commodity Exchange Act, the term "digital asset" explicitly excludes any asset

[195] *Id.* at 11-12.
[196] *Id.* at 12 (see *supra* note 140 for "virtual currency" definition).
[197] *Id.* at 20.
[198] See *supra* note 109 & 114.
[199] S.4356 at 4.
[200] *Id.* at 48.

that provides any of the “five rights" previously discussed in a business entity. In the Money and Finance amendment, “digital asset” is defined as: (A) a natively electronic asset (whether a security or commodity) that confers economic, proprietary, or access rights or powers and is recorded using cryptographically secured distributed ledger technology or similar analogue; and (B) includes “virtual currency and ancillary assets in accordance with section 2(c)(2)(F) of the Commodity Exchange Act.”[201]

A question arising from the quoted portion of the definition of digital asset immediately above is whether a *virtual currency* must be in accordance with section 2(c)(2)(F) to be a digital asset or does the *and* functions exclusively to *ancillary assets*. The answer is elucidated through a close textual examination of the proposed amendments to the Commodity Exchange Act – the new section 2(c)(2)(F). This Paper hopes to show the reader how the answer to this question functions simultaneously as the biggest problem regarding the RFIA as applied to Decred. The Paper will analyze how the RFIA creates a regulatory gap in regard to Decred, which naturally begs the question: But who is in charge of Decred?

If the RFIA is to become law, Section 2(c)(2)(F) of the Commodity Exchange Act would grant the CFTC jurisdiction over agreements, contracts, and transactions of digital assets, “including ancillary assets (consistent with section 41(b)(4) of the Securities Exchange Act of 1934). . .”[202] Section 41(b)(4) lays out the conditions under which an ancillary asset will be presumed a commodity and therefore subject to the jurisdiction of the CFTC under Section 2(c)(2)(F).[203] For an ancillary to be consistent with 41(b)(4), it must have been provided directly or indirectly by an *issuer* that “issues a security through an arrangement or scheme that constitutes an investment contract, as that term is used in section 2(a)(1) of the Securities Act of

[201] *Id.* at 5.
[202] *Id.* at 53.
[203] *Id.* at 32.

1933."[204] The issuer must also be meet the requirements of paragraphs (1), (2), or (3) of the proposed Section 41(b) to the '34 Act,[205] and be compliant with the disclosure requirements under proposed Section 41(c).[206]

Is Decred an ancillary asset consistent with section 41(b)(4) and therefore under the CFTC's jurisdiction? To begin, we must consider whether Decred is an ancillary asset. The only definition of "ancillary asset" found in the RFIA is in the newly proposed Sec. 41.[207] An ancillary asset is an intangible, fungible asset provided to a person "in connection with the purchase and sale of a security through an arrangement or scheme that constitutes an investment contract as that term is used in section 2(a)(1) of the Securities Act of 1933." The Paper will now look to these requirements to see how Decred holds up to "investment contract" analysis.

Understanding the role of the "investment contract" analysis for Decred is critical for two reasons. First, ancillary assets, as defined in the RFIA, are given away "in connection with the purchase and sale of a security through an arrangement or scheme that constitutes an investment contract, as that term is used in section 2(a)(1) of the Securities Act of 1933."[208] Second, under 41(b)(4) for an issuer who provides an ancillary asset to benefit from the presumption that the ancillary asset is a commodity, that issuer must be subject to Section 41(b)(1)-(3).[209] Each of the three cross referenced sections do not apply to foreign private issuers. "Foreign Private Issuer" is defined as a foreign issuer, other than a foreign government.[210,211] "Issuer," as defined in Section 3(a)(8) of the Securities Exchange Act of 1934 is, "any person who issues or proposes to issue

[204] *Id.* at 31.
[205] See *supra* note 177.
[206] S.4356 at 32.
[207] See *supra* note 160.
[208]S.4356 at 26.
[209] See *supra* note 177.
[210] *Id.* at 27.
[211] see *supra* note 158 for list of exclusions.

any security."[212] "Person" means any natural person, company, or government.[213] "Security" is defined in section 3(a)(10) of the '34 Act and includes, amongst other things, "investment contract."[214] Therefore, to be a foreign private issuer, the creator of Decred must be an issuer, and to be an issuer one must propose to issue any security.

Amongst the enumerated list of instruments in the statutory definition of "security," "investment contract" is the only possible applicable category for Decred to fall within. For the dual purpose of determining if Decred is an ancillary asset and to determine if the creators of Decred are "issuers" as statutorily defined, we must then apply the *Howey* test to the context of Decred. The Supreme Court gave meaning to this otherwise ambiguous "investment contract" term in the famous case *United States v. Howey*.[215] Since then, for a contract to be considered valid to this category, it must contain the following elements: [1] an investment of money; [2] in a common enterprise; [3] with the expectations of profit; [4] derived from the efforts of others.[216]

i. Investment contract analysis

Early Decred adopters can be broken down into three categories: (1) Non-developer airdrop recipients; (2) Early protocol developers; (3) PoW miners. Element one of Howey requires an investment of money. Non-developer airdrop recipients did not invest any money for the Decred they received. Decred was given (airdropped) to them by the bootstrap community in order to bootstrap the distribution of coins needed for the hybrid PoS system. Element one fails for this group. Element one also fails for early protocol developers because they did not invest

[212] 15 U.S.C. § 3(a)(8).
[213] 15 U.S.C. § 3(a)(9).
[214] 15 U.S.C.. § 3(a)(10).
[215] 328 U.S. 293 (1946).
[216] *Id.*

money for the early Decred they received. The early protocol developers were compensated retrospectively for the work they had already completed. Early protocol developers did invest time and sweat equity, but they did not invest money. For these reasons, element one fails for early protocol developers as well.

Proof of Work miners can be further categorized into two subgroups. Miners who purchased machines to mine DCR and miners who already owned the requisite hardware required to mine DCR. For miners who purchased new machines, one could argue these miners "invested money" and thus meet the requirement for element one. We will see below how this group clearly fails element four, however. Miners who did not purchase machines, because they already owned the requisite mining hardware, did not invest money. Element one is not met for this subclass of miners.

Next, the second element requires a common enterprise. There are generally two ways to understand common enterprise. The *vertical approach* and the *horizontal approach*.[217] The horizontal approach requires a pooling of funds.[218] The horizontal approach typically will involve a pro rata distribution of profits or sharing of losses among investors, horizontal commonality may exist when promised returns are fixed rather than variable provided there is the requisite pooling of investor funds.[219] See, *SEC v. Infinity Group Co*., 212 F.3d 180 (3d. Cir. 2000).

The vertical approach emphasizes the relationship between investors and the promoters.[220] Under vertical commonality, the principal inquiry is whether "the activities of the promoter are the controlling factor in the success or failure of the investment. . ." and a common enterprise may exist even if there is no pooling of investor funds. Vertical commonality

[217] James D. Cox ET AL. , Securities Regulation: Cases and Materials, 42, (Wolters Kluwer, 9th. Ed., 2020).
[218] *Id.*
[219] *Id.*
[220] *Id.*

enterprise can be "strict" or "broad."[221] Broad vertical commonality requires only a connection between the *efforts* of the promoter and the collective success or losses of the investors.[222] In *SEC v. ETS Payphones, Inc.,* the 11th Circuit ruled broad vertical commonality exists when returns for investors are dependent on the expertise or efforts of promoters.[223] Strict vertical commonality requires a relationship between the success (not the efforts) of the promoters and investors.[224] In other words, promoters and investors must share in the risk of the venture.[225]

Returning now to the only group of early Decred adopters that failed element one of Howey – miners who purchased new machines to mine Decred. Horizontal commonality cannot be said to exist, because there was no pooling of funds, as has been outlined in Section I of this Paper. However, strict vertical commonality most likely does exist, because the success of miners who purchased Decred mining machines is shared with the promoters of Decred, because the expected DCR received from mining will only be valuable if the project is successful. For these reasons Miners who purchased Decred mining machines meet the requirement of element two.

Additionally, the third element requires an expectation of profit. According to a report issued by the SEC's Strategic Hub for Innovation and Financial Technology, "price appreciation resulting solely from external market forces (such as general inflation trends or the economy) impacting the supply and demand for an underlying asset generally is not considered 'profit' under the *Howey* test."[226] This part of the test looks at the investor's intent in buying the asset. Is the purchaser engaging in a transaction because they are looking to turn a profit or are they, for

[221] *Id.*
[222] *Id.*
[223] 408 F.3d 727 (11th Cir. 2005).
[224] *Supra* note 216.
[225] *Id.*
[226] Securities Exchange Commission, Framework for "Investment Contract" Analysis of Digital Assets, (Apr. 3, 2019), https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets#

example, trying to store wealth? If it is the former, then that asset checks the box. If it is the latter, then it will likely get classified as something else. The extreme price fluctuations in Decred suggest that coin-holders are looking for profits from market forces like investors in gold coins, rather than innovations by miners or developers. A Nineth Circuit case has provided support for the position that purchasers of Decred are not relying on the efforts of others. In *SEC v. Belmont Reid & Co*., the court held that investors in gold coins during a period of high inflation looked for profits from market forces rather than the efforts of the promoters.[227] Because Decred has a fixed issuance, it is most likely holders of Decred look to market forces to drive the price of Decred as opposed to an expectation of profit. However, if the holder of Decred is also a Stakeholder (one who holds a Decred ticket), one could argue that the Stakeholder does have an expectation of profit, because he receives as payment for his service to the network a small amount of Decred.[228] I demonstrate below how these Stakeholders fail element four of the *Howey* test.

Element four requires the expectation of profits "to be derived from the efforts of others." In *SEC v. Glenn W. Turner Enterprises, Inc.*, the 9th Circuit stated that the critical inquiry is, "Whether the efforts made by those other than the investor are the undeniably significant ones, those essential managerial efforts which affect the failure or success of the enterprise."[229] If the investor has a significant hand in the success of an investment, it is most likely not an investment.[230]

To some extent, one can argue that purchasers of Decred rely on the efforts of miners and developers, however one cannot say that those early miners who purchased Decred machines

[227] 794 F.2d 1388 (9th Cir. 1986).
[228] See *supra* note 93.
[229] 474 F.2d 476, 482 (9th Cir.) *cert denied*, 414 U.S. 821 (1973).
[230] See *United Housing Foundation, Inc. v. Forman*, 421 U.S. 837 (1975) at 852

were not significantly involved in the future success or failure of the project. For this reason, early Decred miners who purchased machines fail the fourth element of the *Howey* test. Additionally, Stakeholders who receive small payments of Decred for their service to the network do not meet the fourth element of the Howey analysis because the payments they receive are only provided if and for as long as they continue to buy a ticket and vote on blocks proposed by miners. Although to some extent market purchasers of Decred may rely on the efforts of miners and developers, the miners and developers are just influential investors and do not have coordinated activities outside the protocol upgrade process which is highly decentralized. Additionally, there is no official hierarchy in Decred.[231]

This analysis has shown that the investment contract analysis fails for all three categories of early Decred adopters. Decred is an intangible fungible asset that was provided to persons, but not through an arrangement or scheme that constitutes an investment contract. As such, Decred does not meet the Sect. 41 proposed definition of ancillary asset because ancillary assets are provided to person in connection with an arrangement or scheme that constitutes an investment contract as the term is used in Section 2(a)(1) of the '33 Act.[232]

Further, early adopters of Decred do not meet the statutory definition of an issuer either, because Decred does not meet the Section 2(a)1 definition of Security. Since Decred is not a security, the creators of Decred are not "issuers" as defined by the '33 Act. And since the creators of Decred are not issuers, they are not foreign private issuers as the term is defined in the RFIA. However, Decred is a virtual currency, as the term is proposed in the RFIA.

A question posed earlier considered whether virtual currencies had to be in accord with Section 2(c)(2)(F) or whether the requirement applied exclusively to ancillary assets. Section

[231] 794 F.2d 1388 (9th Cir. 1986).
[232] See *supra* note 203.

2(c)(2)(F) makes no mention of virtual currency. Instead, Section 2(c)(2)(F) grants the CFTC jurisdiction over digital assets and ancillary assets (that are consistent with section 41(b)(4) of the Securities Exchange Act of 1934).[233] But remember, digital asset is defined in the Commodity Exchange Act to explicitly exclude any asset that provides any of the "five rights" in a business entity.[234] Section 41(b)(4) of the Securities Exchange Act of 1934 outlines the requirements under which an ancillary asset will be presumed a commodity for purposes of Section 2(c)(2)(F).[235] However, as shown above, Decred does was not provided in connection with an "investment contract" and is therefore not an "ancillary asset."

Additionally, the Security Exchange Act definition of "ancillary asset" explicitly excludes any asset which provides the holder with any of the "five rights" in a business entity. If holders of DCR receive a: (i) A debt or equity interest in that entity. (ii) Liquidation rights with respect to that entity. (iii) An entitlement to an interest or dividend payment from that entity. (iv) A profit or revenue share in that entity solely from the entrepreneurial or managerial efforts of others. (v) any other financial interest in a business entity, then DCR Any other financial interest in that entity.[236]

Decred stakeholders, by virtue of their efforts via staking, receive benefits which arguably meet one of the five requirements. The question becomes, is Decred a business entity? RFIA begins to elucidate the direction of Decentralized Autonomous Organizations regulation through an amendment to the Internal Revenue Code. Specifically, the RFIA proposes defining "Decentralized Autonomous Organization." Decentralized Autonomous Organization would means:

[233] S.4356 at 53.
[234] See *supra* note 164.
[235] See *supra* note 180.
[236] S.4356 at 26-27.

> an organization which (i) utilizes smart contracts (as defined in section 9801 of title 31, USC) to effectuate collective action for a business, commercial, charitable, or similar entity, (ii) governance of which is achieved primarily on a distributed basis, and (iii) which is properly incorporated or organized under the laws of a State or foreign jurisdiction as a decentralized autonomous organization, cooperative, foundation, or any similar entity."[237]

Thus, RFIA classifies Decentralized Autonomous Organizations as business entity which is not a disregarded entity.[238] Decred satisfies the requirement of (i) because Decred uses an analogue similar to computer code deployed to a distributed ledger technology network that executes an instruction (upgrade the network) based on the occurrence or nonoccurrence of specified conditions (the stakeholder voting process). Decred satisfies the requirement of (ii) because the governance of the network is achieved through the network upgrade process discussed *supra* and Politea, which is a distributed basis. However, Decred does not meet the requirement of (iii) because Decred is not incorporated under any state or foreign jurisdiction.

Based on my experience and understanding of Decred, I am uncertain what it would mean for Decred to incorporate, nor do I think incorporating Decred under the laws of any state of foreign jurisdiction would mean anything because Decred exists entirely in cyberspace. Decred is empowered by a distributed computer network. Independent miners and stakeholder who run the Decred source code on their machines. I am not certain who would be expected to incorporate Decred. I think the proposed definition of a Decentralized Autonomous Organization does not match the reality of how this novel technology works. But maybe the answer to this question is the obvious response – Decred is not a Decentralized Autonomous Organization. If not, then what is it?

[237] *Id.* at 18.
[238] *Id.* at 17.

Professors Primavera De Filippi and Aaron Wright discuss Decentralized Organizations at length in their Book, *Blockchain and the Law*.[239] According to Filippi and Wright Decentralized organizations are organizations that are native to the Internet, potentially global in scope, decentralized, and pseudonymous.[240] According to Filippi and Wright, Decentralized organization is a new organization that rely on blockchain technology and smart contracts as their primary or exclusive source of governance.[241] In the United States decentralized organizations formed for the purpose of making a profit likely would be deemed a "general partnership" and consequently lack the ability to shield its members' assets if the origination injures a third party or is unable to pay its creditors.[242] According to Filippi and Wright, A DAO is a particular kind of decentralized organization that is neither run nor controlled by any person but entirely by code.[243] As opposed to other decentralized organizations – which are operated by individuals who hold the ultimate decision-making power – DAOs are designed to run autonomously on a blockchain.[244] According to Filippi and Wright, Bitcoin represents the basic genotype of a DAO.[245] According to Filippi and Wright, even though Bitcoin relies on the contribution of individuals to secure and maintain the network, it is both independent and self-sufficient in that it is not controlled by any single entity.[246] Similar to Decred, however, Bitcoin is not incorporated under any state or foreign jurisdiction and would not be considered a Decentralized Autonomous Organization as the term is defined in the RFIA. Filippi and Wright have noted, "even if a government had jurisdiction over a DAO, there are questions as to whether

[239] PRIMAVERA DE FILIPPI & AARON WRIGHT, BLOCKCHAIN AND THE LAW: THE RULE OF CODE, 131-156, (Harv. Univ. Press 2018).
[240] *Id.* at 143.
[241] *Id.* at 136.
[242] *Id.* at 142.
[243] *Id.* at 148.
[244] *Id.* at 148.
[245] *Id.*
[246] *Id.* at 150.

the government would have the authority to impose rules on such an organization. As it has long been recognized, the legal system cannot provide legal rights or impose duties on something devoid of legal personhood."[247] "Even if these tokens were to qualify as securities, there would be no legal entity to hold responsible for failure to comply with the formalities enshrined in the law."[248]

Conclusion

The proposed Lummis-Gillibrand Responsible Financial Innovation Act leaves unanswered the question of who is in charge of Decred. The proposed amendments to the Money and Finance section of the United States Code include general definitions for virtual currency and digital asset. Decred is a virtual currency as defined in the RFIA. The proposed amendments to the Securities Exchange Act of 1934 introduce a new concept, ancillary asset. Ancillary assets are intangible and provided in connection with an investment contract. Ancillary assets are distinct from the security or investment contract used by an issuer to raise money. The RFIA's proposed amendments to the Commodity Exchange Act provide an avenue for ancillary assets to be presumed commodities and under the jurisdiction of the CFTC. The RFIA explicitly limits the CFTC's jurisdiction over any asset that provides any of the "five rights" in a business entity. The RFIA proposes a definition of Decentralized Autonomous Organization and categorizes these cyberspace entities as non-disregarded business entities. None of these provisions successfully capture Decred and furthermore, the Act leaves open the question who would regulate Decred. As Filippi and Wright have stated, the nature of Decentralized Autonomous Organizations (a subset of Decentralized Organizations) is that DAOs do not have a legal entity to hold responsible for failure to comply with the formalities enshrined in the law. According to Filippi

[247] *Id.* at 154.
[248] *Id.*

and Wright, Bitcoin is an example of a Decentralized Autonomous Organization. I argue Decred is an even better example. To this end, the Responsible Financial Innovation Act fails to embrace the realities of this new technology and how it works. As such, we are trying to place these new assets into a framework that is not suited for the digital age. The author believes the solution to this problem is to create a new agency to be charged with the regulation of Digital Assets. The enabling act of this theoretical agency should reflect the limitations that Filippi and Wright have noted in their Book. Namely, it is difficult, if not impossible, to regulate constructions of cyberspace, such as Decentralized Autonomous Organizations.