

The following is the requested independent legal analysis of the convertible virtual currency Private Instant Verified Transaction (“PIVX”). This report was commissioned by the requestor to be a fully independent legal review.

## Useful Terms and Definitions:

Virtual Currency = A medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency. In particular, virtual currency does not have legal tender status in any jurisdiction. Virtual currency either has an equivalent value in real currency, or acts as a substitute for real currency

ICO = Initial Coin Offering – meaning the classic sense of the term “coin” from a mined algorithm as opposed to a tokenized asset created on top of an existing chain (i.e. bitcoin is a “coin” or, “convertible virtual currency”<sup>1</sup> while ERC-20 assets on the Ethereum chain are “tokens.”

ITO = Initial Token Offering – meaning the majority of the fundraising/sales activity launched in the past several years on the Ethereum network (i.e. “token sales,” etc).

STO = Securities Token Offering – meaning a fully registered security offered in compliance with state and federal law, generally created as a token asset on top of an existing chain. A fully registered and compliant ITO.

**Question presented:** To the extent PIVX were to be listed on a cryptocurrency exchange, would such listing constitute the listing of a security? Short Answer: No.

## Analysis

The Securities Act of 1933 and the Securities Exchange Act of 1934 created the Securities Exchange Commission (“SEC”). According to the SEC, the main purpose of the Act can be summarized to satisfy two major concerns:

1. Companies offering securities to the public for investment dollars must be truthful about their businesses, the securities being sold, and the investment risks.
2. Sellers and traders of securities – brokers, dealers, and exchanges – must fairly and honestly treat investors, putting their interests first.

<sup>1</sup> FIN-2013-G001 “...“virtual” currency is a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency. In particular, virtual currency does not have legal tender status in any jurisdiction...This type of virtual currency either has an equivalent value in real currency, or acts as a substitute for real currency.”

In order to analyze PIVX under federal securities laws, we begin with the definition of “security” contained in Section 2(a)(1) of the Securities Act of 1933, which defines a security as:

“...any note, stock, treasury stock, security future, security-based swap, bond, debenture, evidence of indebtedness, certificate of interest or participation in any profit-sharing agreement, collateral-trust certificate, preorganization certificate or subscription, transferable share, investment contract, voting-trust certificate, certificate of deposit for a security, fractional undivided interest in oil, gas, or other mineral rights, any put, call, straddle, option, or privilege on any security, certificate of deposit, or group or index of securities (including any interest therein or based on the value thereof), or any put, call, straddle, option, or privilege entered into on a national securities exchange relating to foreign currency, or, in general, any interest or instrument commonly known as a “security”, or any certificate of interest or participation in, temporary or interim certificate for, receipt for, guarantee of, or warrant or right to subscribe to or purchase, any of the foregoing.”<sup>2</sup>

All securities offered and sold in the United States must be registered with the SEC or must qualify for an exemption from registration requirements.

The foundational Supreme Court case for determining whether an instrument meets the definition of a security is *SEC v. W.J. Howey*, 328 U.S. 293 (1946). The Supreme Court has reaffirmed the Howey analysis more recently in *SEC v. Edwards*, 540 U.S. 398 (2004). Howey focuses specifically on the term “investment contract” within the definition of security, noting that it has been used to classify those instruments that are of a “more variable character” which may not fit neatly into other categories.

Not every contract or agreement is an “investment contract.” Rather, the Supreme Court has developed a four-prong test to determine whether an agreement constitutes an investment contract:

A contract constitutes an investment contract that meets the definition of security if there is (i) an investment of money; (ii) in a common enterprise; (iii) with an expectation of profits; (iv) solely from the efforts of others (e.g., a promoter or third party), “regardless of whether the shares in the enterprise are evidenced by formal certificates or by nominal interest in the physical assets used by the enterprise.”<sup>3</sup>

In order to be considered a security, all four prongs must be satisfied. For many coins in operation like PIVX, the question is whether a digital asset that was originally offered, adapt in a manner that does not constitute an offering of a security or, whether PIVX may be something

<sup>2</sup> See The Securities Act of 1933

<sup>3</sup> *SEC v. W. J. Howey Co.*, 328 U.S. 293 (1946)

else entirely. We believe that PIVX has become decentralised enough to be something else entirely and that it may well resemble a *convertible virtual currency*<sup>4</sup> more than it does a security:

**(i) [A]n investment of money;** PIVX had no ICO and was fully self funded by a group of developers when it was launched on January 1, 2016. No offering was made specifically to anyone, except for open source code released on github.<sup>5</sup> No money (digital currency or virtual currency) was received by the developers who created the architecture of the PIVX code. PIVX does not meet that prong of the test.

**(ii) [I]n a common enterprise;** Anyone can contribute to PIVX, so perhaps PIVX does meet that prong of the test.

**(iii) [W]ith an expectation of profits;** There was no expectation of profits from PIVX. No PIVX were allocated to the developers and none were offered to any particular group for the expectation of an increase in value, or even market adoption. PIVX was created as an experiment and shared with the world on a universal code repository.

**(iv) [S]olely from the efforts of others (e.g., a promoter or third party);** The PIVX developers created the code but there have been many changes through consensus since then. Countless independent actors who choose to join the consensus mechanisms of PIVX set the price through market participation construct. In other words, the PIVX developers cannot set, change the price or redeem PIVX on the market even if they were to shut down their computers and servers all at once. There simply is no centralised station for the operation of PIVX.

Under PIVX's Community Designed Governance, there are no curators or process for censorship of proposals put to a vote. Any PIVX community member can submit proposals and the entire Masternode community may vote on these proposals. At the time of writing, there have been 24 proposals by 24 unique users with participation of over 1000 Masternodes voting. A list of the

4 FIN-2013-G001

5 <https://github.com/PIVX-Project/PIVX> (Last retrieved September 12, 2018)

votes are in the public record. <sup>6</sup> *Prima Facie*, under the Howey analysis, the facts surrounding the creation of PIVX do not fit satisfy the prongs of the test enough to resemble that of a security.

**PIVX may resemble “convertible virtual currency” more closely than a (tokenized) security:**

The Financial Crimes Enforcement Network ("FinCEN") issued an interpretive guidance to clarify the applicability of the regulations implementing the Bank Secrecy Act ("BSA") to persons creating, obtaining, distributing, exchanging, accepting, or transmitting virtual currencies. The guidance classifies three unique groups: "users," "administrators," and "exchangers," FinCEN's regulations define currency (also referred to as "real" currency) as "the coin and paper money of the United States or of any other country that [i] is designated as legal tender and that [ii] circulates and [iii] is customarily used and accepted as a medium of exchange in the country of issuance." In contrast to real currency, "virtual" currency is a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency. In particular, virtual currency does not have legal tender status in any jurisdiction. The guidance addresses "convertible" virtual currency as an asset class which either has an equivalent value in real currency, or acts as a substitute for real currency.<sup>7</sup> The guidance refers to the participants in generic virtual currency arrangements, using the terms "user," "exchanger," and "administrator."

- 6 Masternode Budget Proposals Voting Status:  
Proposal 1: PIVXBrandandCreative Yes: 757 / No: 237  
Proposal 2: PIVX-Trans-V4 Yes: 655 / No: 325  
Proposal 3: Support-Team-Q2 Yes: 865 / No: 9  
Proposal 4: Bizdev Yes: 659 / No: 200  
Proposal 5: BizDevFund Yes: 644 / No: 200  
Proposal 6: Brandingandcreative Yes: 408 / No: 449  
Proposal 7: core-dev-fuel3 Yes: 885 / No: 0  
Proposal 8: New-Bug-Bounty Yes: 218 / No: 0  
Proposal 9: PIVXpressNEW Yes: 869 / No: 5  
Proposal 10: pivx-qa-team-renewal Yes: 851 / No: 0  
Proposal 11: PRandMedia1 Yes: 836 / No: 37  
Proposal 12: PRandMedia Yes: 309 / No: 422  
Proposal 13: AmbassadorPRG Yes: 643 / No: 211  
Proposal 14: MrktgSupport-Social Yes: 636 / No: 209  
Proposal 15: Newsletter Yes: 652 / No: 2  
Proposal 16: PIVX-Class-Phase-3 Yes: 624 / No: 205  
Proposal 17: PIVXGodotEngine Yes: 646 / No: 3  
Proposal 18: PIVXtermsstyleguide Yes: 618 / No: 0  
Proposal 19: Core-Dev-Network Yes: 595 / No: 8  
Proposal 20: New-PIVX-Website Yes: 160 / No: 0  
Proposal 21: ProvenanceSeoulKorea Yes: 9 / No: 2  
Proposal 22: Support-Team-Q3 Yes: 7 / No: 0  
Proposal 23: TransBlogSubt Yes: 0 / No: 2  
Proposal 24: TransWhitePaper Yes: 1 / No: 2
- 7 FIN-2013-G001

A *user* is a person that obtains virtual currency to purchase goods or services. An *exchanger* is a person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency. An *administrator* is a person engaged as a business in issuing (putting into circulation) a virtual currency, and who has the authority to redeem (to withdraw from circulation) such virtual currency.

Although there is no BSA definition of virtual currency, FinCEN differentiates between “real currency” by stating in the guidance that it is “a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency.”<sup>8</sup>

**A user is a person that obtains virtual currency to purchase goods or services:** Anyone can be a user of PIVX and there are no BSA reporting or record-keeping requirements for users of virtual currencies.<sup>9</sup> Thus, anyone who solely uses PIVX for goods or services is by definition a user under the definition and exempt from MSB registration, record-keeping and reporting.

**An exchanger is a person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency:** The PIVX developers are not engaged as a business in the exchange of PIVX for real currency, funds, or other virtual currency and therefore, are exempt from MSB registration, record-keeping and reporting.

**An administrator is a person engaged as a business in issuing (putting into circulation) a virtual currency, and who has the authority to redeem (to withdraw from circulation) such virtual currency.** There was no business model for PIVX and it was offered to the world via a publicly accessible online repository.<sup>10</sup> Whilst the creators of PIVX did put into circulation the technology, it had to be adopted by others for there to be a working network. Moreover, the architects of PIVX do not have the power to redeem or withdraw PIVX from circulation; the code simply does not allow for that ability.<sup>11</sup>

Another department of the United States Treasury, the Internal Revenue Service (“IRS”), affirms the FinCEN definition by stating in Notice 2014-13 that:

“Virtual currency that has an equivalent value in real currency, or that acts as a substitute for real currency, is referred to as “convertible” virtual currency. Bitcoin is one example of a convertible virtual currency. Bitcoin can be digitally traded between users and can be purchased for, or exchanged into, U.S. dollars, Euros, and other real or virtual currencies. For a more comprehensive description of convertible virtual currencies to date, see Financial Crimes Enforcement Network (FinCEN) Guidance on the Application of FinCEN’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies (FIN-2013-G001, March 18, 2013).”<sup>12</sup>

8 *Id.*

9 31 CFR § 1010.100(ff)(1-7)

10 <https://github.com/PIVX-Project/PIVX> (Last retrieved September 10th, 2018)

11 *Id.*

12 Notice 2014-21

Whilst the IRS mentions bitcoin in its notice, the finCEN guidance does not. The PIVX code was written to resemble the decentralized model of bitcoin more than that of an ERC 20 model which is commonly used for tokenized security assets. PIVX was launched in January 2016 under the name of Darknet as a code fork of Dash and the primary focus of Darknet was decentralized transactional privacy. Initially, the coin was a mineable Proof-of-Work (“PoW”) cryptocurrency (using the ASIC-resistant Quark algorithm) to generate its initial distribution of approx. 43 million coins which later transitioned to Proof-of-Stake (PoS) once the initial mining phase was completed 180 days after the genesis block. At its release, 60,000 coins were generated on a nexus block to create an initial set of 6 masternodes for the network and these were burnt at the completion of the PoW stage. The initial PoW distribution phase ended in August 2016 and transitioned to the Proof of Stake (PoS) phase.

The above brings us to the Hinman letter analysis. On June 14, 2018, speaking at the Yahoo Finance All Markets Summit, William Hinman, Director of the SEC’s Division of Corporation Finance, definitively gave analysis to support that neither bitcoin nor ether are securities and that offers and sales of these cryptocurrencies are not securities transactions. He also indicated that even though the initial issuance of a digital asset may have represented a securities offering, once the asset is no longer controlled by a central authority or used primarily to purchase goods or services on a functioning network, it may not make sense to regulate the digital asset as a security:

“If the network on which the token or coin is to function is sufficiently decentralized – where purchasers would no longer reasonably expect a person or group to carry out essential managerial or entrepreneurial efforts – the assets may not represent an investment contract. Moreover, when the efforts of the third party are no longer a key factor for determining the enterprise’s success, material information asymmetries recede. As a network becomes truly decentralized, the ability to identify an issuer or promoter to make the requisite disclosures becomes difficult, and less meaningful.

And so, when I look at Bitcoin today, I do not see a central third party whose efforts are a key determining factor in the enterprise. The network on which Bitcoin functions is operational and appears to have been decentralized for some time, perhaps from inception. Applying the disclosure regime of the federal securities laws to the offer and resale of Bitcoin would seem to add little value. And putting aside the fundraising that accompanied the creation of Ether, based on my understanding of the present state of Ether, the Ethereum network and its decentralized structure, current offers and sales of Ether are not securities transactions. And, as with Bitcoin, applying the disclosure regime of the federal securities laws to current transactions in Ether would seem to add little value. Over time, there may be other sufficiently decentralized networks and systems where regulating the tokens or coins that function on them as securities may not be required. And of course there will continue to be systems that rely on central actors

whose efforts are a key to the success of the enterprise. In those cases, application of the securities laws protects the investors who purchase the tokens or coins.”<sup>13</sup>

### **Conclusion:**

Based on our review of PIVX and independent analysis of its network, we cannot find any evidence to support that it was ever offered as security and the manner in which it was “offered” do not satisfy the prongs of the Howey test. We have found that the PIVX structure more closely resembles that of bitcoin which is considered by FinCEN and the IRS to be a “convertible virtual currency”. Moreover, PIVX was never “offered” but rather, its code was placed on a universally accessible open source code repository where anyone in the world would be able to contribute to its build without compensation or announcement. And, much like bitcoin, if its architects were to disappear tomorrow, it would remain in circulation as long as contributors to its consensus network chose to devote computing power to its continued circulation.

### **More About The PIVX Nuts and Bolts:**

<sup>13</sup> <https://www.sec.gov/news/speech/speech-hinman-061418>

**History and How it works:** PIVX was launched without pre-sale, airdrop, was not offered through an ICO and has a fast growing, active community base. PIVX is an MIT licensed open source blockchain-based cryptocurrency utilizing Bitcoin codebase and is focused on advancing the privacy, decentralization, maintaining its fungibility and real-world utilization of the coin as a virtual currency. PIVX was launched in January 2016 under the name of Darknet as a code fork of Dash. As its original name suggests, the primary focus of Darknet was decentralized transactional privacy. The coin was initially a mineable Proof-of-Work (“PoW”) cryptocurrency (using the ASIC-resistant Quark algorithm) to generate its initial distribution of approx. 43 million coins which later transitioned to Proof-of-Stake (PoS) once the initial mining phase was completed at block 259,200 or, 180 days after the genesis block. At its release, 60,000 coins were generated on a nexus block to create an initial set of 6 masternodes for the network and these were burnt at the completion of the PoW stage. The initial PoW distribution phase ended in August 2016 and transitioned to the Proof of Stake (PoS) phase. The project was later re-branded to PIVX in February 2017.

On July 5, 2018, PIVX traded at \$2.18 USD per coin or 0.00033059 BTC, with a rank of 83 on CoinMarketCap. The Market Cap was an estimated \$123.5 Million and the 24-hour volume was reported at \$889,070. According to CoinMarketCap, the then-circulating supply of PIVX was 56,648,257 coins. As of this writing, PIVX had 1770 Masternodes enabled with 1762 of those active. To acquire a PIVX masternode, each owner must stake 10,000 PIVX coins. The total number of coins staked in Masternodes is currently over 17.7 million PIVX or 31% of the circulating supply. There is no hard coded maximum coin supply for PIVX and up to a maximum of 3.1536 million new PIVX coins are newly minted every year. Masternodes are nodes running the same wallet software on the same blockchain to provide services such as instant transactions and PIVX governance that distributes a decentralized budgeting system with an immutable proposal and voting systems. PIVX implements a Dynamic zPoS Rewards Mechanism where for every 60 seconds on average, 5 PIV are newly created (Also sometimes called minting). These 5 new PIV are then automatically divided between the Masternodes and the Staking nodes. The split between Masternodes and individual Staking node is based on the zPoS algorithm which constantly shifts the larger portion of the reward (3 PIV) to each type of wallet node based on which type of coin was staked to validate that particular block. When zPIV is used to stake a block, then the staking node receives 3 zPIV while the masternode receives 2 PIV. When PIV is used to stake a block, then the staking node receives 2 zPIV while the masternode receives 3 PIV. This creates incentive for the network users to mint and stake zPIV. Staking with PIVX does not have a minimum number of PIVX coins requirement, but requires the owner to keep the wallet actively staking and running on a computer connected to the internet.

On January 31, 2016, Private Instant Verified Transaction (PIVX) was launched under the original name of DNET as a fully operational donation and self treasury funded decentralized cryptocurrency. Unlike the majority of current projects in the ICO market today, PIVX was built, developed and released without any pre-sale or ICO. In February 2017, DNET was officially rebranded to PIVX.

**Governance:** PIVX utilizes a blockchain-level treasury system. Up to 20% of each block reward over every 30-day period fund its projects and proposals (Equivalent to 1 PIV per block) A maximum allotment of 43.2k PIV are available to be used monthly and is distributed by PIVX’s proposal and voting system; which is decentralized by the use of Masternodes. **PIVX blockchain and its treasury is governed by its community network.**

PIVX is not governed or owned by any single person, organization or identifiable third party. Its network is highly secured by globally distributed Staking Wallets and its treasury is governed by thousands of Masternodes spread across different parts of the world by PIVX users. PIVX Masternode Owners voted and approved for PIVX to develop and implement an improved ‘Community Designed Governance’ system that changes the distribution of votes, to include all PIVX currency owners. The Community Designed Governance is one example of a decentralized autonomous organization--a term used to describe a “virtual” organization embodied in computer code and executed on a distributed ledger or blockchain. All areas of PIVX's Community Designed Governance follows the same process in terms of submitting a proposal, and Masternode owners voting to accept/reject the proposal.



Community Designed Governance voting and eventual payout occurs every 30 days. PIVX Masternode owners also voted and approved three different treasury categories: “PIVX will work towards a ‘Community Designed Governance’ system that dramatically expands the reach of voting power from simply Treasury Governance, to also include Manifesto Governance, and Protocol Governance.” Today, any PIVX community member can create a project or proposal, vote, and fund projects supporting PIVX itself through its Community Designed Governance.