April 7, 2021

Via email (rule-comments@sec.gov)
Ms. Vanessa A. Countryman
Secretary
U.S. Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549

Re: File No. S7-25-20; Custody of Digital Asset Securities by Special Purpose Broker-Dealers (Release No. 34-90788)

Dear Ms. Countryman:

tZERO Group, Inc. ("tZERO Group") and its broker-dealer subsidiaries (collectively, "tZERO") appreciate this opportunity to comment on the U.S. Securities and Exchange Commission's (the "SEC" or the "Commission") Statement on Custody of Digital Asset Securities by Special Purpose Broker-Dealers (the "Statement") issued on December 23, 2020.[1] Along with the Commission's recent no-action letter setting forth a three-step process for broker-dealers to facilitate trading in digital asset securities custodied by customers with a third-party custodian[2], the Statement is an important step forward in clarifying the regulatory regime applicable to digital asset securities. We are grateful to the Commission and its staff for their leadership in this space. We particularly welcome the Commission's recognition that the current legal and regulatory framework (particularly behind the operational segments of the industry) needs to adjust to enable innovation leveraging digital infrastructure and blockchain technology in the financial services industry. tZERO, a long-standing advocate in this space, believes that we have seen a secular shift towards reshaping financial architecture using digital technology to make financial markets instantaneous, less encumbered by layers of intermediation and more cost effective, efficient, inclusive and secure. We are at a critical inflection point in

[1] *Custody of Digital Asset Securities by Special Purpose Broker-Dealers*, 86 Fed. Reg. 11,627 (Feb. 26, 2021) (to be codified at 17 CFR 240), https://www.federalregister.gov/documents/2021/02/26/2020-28847/custody-of-digital-asset-securities-by-special-purpose-broker-dealers.

[2] Elizabeth Baird, *ATS Role in Settlement of Digital Asset Security Trades*, SEC No-Action Letter to Kris Dailey (FINRA) (Sept. 25, 2020), https://www.sec.gov/divisions/marketreg/mr-noaction/2020/finra-ats-role-in-settlement-of-digital-asset-security-trades-09252020.pdf.

the development of next-generation capital markets using technology and processes better suited for recording, tracking, exchanging and settling value. It is competitively important that the United States remains at the forefront of this change. Enabling broker-dealers to facilitate trading and custody of digital assets begins to remove a critical barrier to the next leg of the journey.

In this comment letter, we will respond to certain of the requests for comments made by the Commission in the Statement and comment on additional ways to fortify the objectives of the Statement. These comments are aimed at offering a step forward in the blockchain continuum, with the goal of permitting broker-dealers to offer their customers a uniform way to trade and custody a variety of assets, including digital asset securities, other securities, and non-security digital assets under one umbrella, and to fund and settle such trades with non-security digital assets. Our key comments include:

- We suggest that the Commission not create unusual and unnecessary product-specific industry silos, and, instead, permit special purpose broker-dealers to offer their customers access to traditional and digital asset securities. We understand the Commission is concerned that the loss or theft of digital asset securities may cause a special purpose broker-dealer ("SPBD") and its customers to incur substantial financial losses and potentially cause the SPBD to fail. The Commission's concern, however, is premised on an effort to determine whether and how digital asset securities, by virtue of their technology architecture, may be inherently riskier than securities that do not utilize this technology. We believe that these risks are contained and managed by the regulated environment contemplated by the Statement and present risks and challenges that are not materially asymmetric to those posed by the traditional securities ecosystem. Furthermore, regulators, courts and the industry have developed decades' worth of ways to address the liquidation of failing broker-dealers with traditional securities, including the Securities Investor Protection Act of 1970 (as amended, "SIPA") regime. These same measures and protections would apply to SPBDs engaging with traditional securities. The Statement outlines additional safeguards for SPBDs' digital asset security businesses in a risk-compliant way. These two worlds can work together to offer customers one touchpoint for their brokerage services, while ensuring investor protection, and driving innovation. It will also offer customers increased optionality in SPBDs and decrease the concentration of risk associated with a digital asset securities business, as the single purpose business requirement is likely to make it harder for the monoline boutique SPBDs (especially those not part of larger families of companies that can subsidize such operations) to sustain their growth. There is no need to balkanize the industry based on technology rails that power otherwise similar, from economic and corporate perspectives, interests.

- We suggest that the Commission allow SPBDs to use non-security digital assets as a means of funding and settlement for digital asset securities transactions and to conduct a non-security digital assets business. The Statement provides the industry a five-year incubator to assess the viability of digital asset securities – such an assessment cannot be properly made if market participants are using legacy technology for the cash funding and settlement phase of a digital asset security lifecycle. Real-time settlement is a critical benchmark and benefit of the digital asset securities ecosystem. It cannot be meaningfully achieved if traditional fiat currency and banking systems are still driving the settlement of the cash leg of securities transactions on the current timetable. The compliance architecture the Commission outlines for digital asset securities, augmented with certain other measures we suggest in this letter, should address concerns with broker-dealers permitting customers to fund their accounts with non-security digital assets, conducting a non-security digital assets business, custodying non-security digital assets (directly or with a third-party regulated custodian) and using non-security digital assets to facilitate real-time settlement of digital asset security transactions across the participating firms.

- We ask that the Commission clarify that the Statement is solely applicable to digital asset securities and the broker-dealers that custody such securities. We believe the Statement only requires broker-dealers that custody digital asset securities to be SPBDs. The Commission should confirm that broker-dealers that conduct a digital asset securities business, but do not custody digital asset securities, are not required to be SPBDs. For example, broker-dealers that facilitate trading in digital asset securities on an agency basis and introduce customer accounts to SPBDs on a fully-disclosed basis, or broker-dealers that operate alternative trading systems that match trades in digital asset securities would not be required to be SPBDs. Likewise, we would suggest that the Commission clarify that securities utilizing digital technology in ways that do not meet the definition of a digital asset security, including those securities that are already in the market, would continue to be treated in the same manner as other conventional uncertificated securities.

1. About tZERO

tZERO Group is a financial technology company committed to democratizing access to capital markets through the development and adoption of securities that leverage blockchain technology. We focus on developing the supply side of this marketplace by creating technology that enables issuers and relevant regulated market participants to support the issuance, trading, clearance and settlement of securities with blockchain functionality. We also support the demand for, and adoption of, such securities by developing technology for regulated venues on which those securities can

trade. tZERO Group has invested in broker-dealer subsidiaries to help drive this mission. These subsidiaries include tZERO ATS, LLC and tZERO Markets, Inc. ("tZERO Markets"). tZERO ATS, LLC is an SEC-registered broker-dealer and member of the Financial Industry Regulatory Authority ("FINRA"). It operates an alternative trading system (an "ATS," such ATS is known as, the "tZERO ATS") that facilitates the trading of securities by broker-dealer subscribers to tZERO ATS.

tZERO Markets is an SEC-registered broker-dealer, member of FINRA and one of the subscribers to the tZERO ATS. It operates an online platform that permits investors to trade securities that are quoted on the tZERO ATS. These securities utilize blockchain technology elements that are intended to enhance the investor experience through added transparency. The blockchain allows for a courtesy carbon copy of certain ownership records to be viewable, as a convenience and with no controlling effect, on a publicly available distributed ledger. While the courtesy carbon copy of certain ownership records is publicly viewable on the blockchain, it is also is pseudonymized, meaning that such copies do not contain personally identifiable information. In all cases, books and records of regulated market participants continue to be the sole controlling authority on ownership and other matters. These securities are not digital asset securities within the meaning of the Statement given the non-controlling elements of blockchain technology.

The focused application of blockchain technology in use today by tZERO is beneficial – but it is a slice of the benefits that would result from broader adoption of blockchain technology in capital markets. These benefits include decreasing settlement times for securities transactions (with the potential to eliminate settlement lags altogether) and reducing risks associated with delayed settlement, streamlining back-office processes, reducing costs associated with manual processes and intermediation and automating corporate actions. While others in the international community have taken steps to define and, in some cases, implement a framework to facilitate digital asset securities, none have achieved the widespread adoption necessary to fully benefit from this potential for transformation. The United States can take this moment to build on the guidance set forth in the Statement and be the leader in the digital evolution – showing the world a better way to issue, record, transfer and settle securities by leveraging digital technology that is superior to the legacy systems and infrastructure in place today. The alternative would be to sideline innovation to niche domestic environments that are not likely to scale and, more importantly, off-shore markets, which may offer less transparency and investor protection. To these ends, we are enthusiastic about the promise of the Commission's vision in the Statement and respectfully offer the following comments.

2. Responses to the Commission's Requests for Comments

   a. Should the Commission expand this position in the future to include other businesses such as traditional securities and/or non-security digital assets? Should this position be expanded to include the use of non-

> security digital assets as a means of payment for digital asset securities, such as by incorporating a *de minimis* threshold for non-security digital assets?

We suggest that the Commission expand its position to allow SPBDs to engage in a traditional securities business.

The Statement notes that digital asset securities provide unique risks of fraud, theft or loss as compared to traditional securities. To help isolate these risks, the Commission requires a broker-dealer that custodies digital asset securities to be a "special purpose broker-dealer," limiting its activities to those involving digital asset securities. Such a broker-dealer would not be permitted to engage in a traditional securities business. To support the perspective regarding the inherent riskiness of digital asset securities as compared to traditional securities, the Statement cites the Report of the Attorney General's Cyber Digital Task Force: Cryptocurrency Enforcement Framework (the "DOJ Report").[3] In citing the DOJ Report, the Commission draws a parallel between the risks associated with digital asset securities and the risks associated with non-security digital assets, including those that are offered and traded on offshore venues. While both types of assets look to leverage digital infrastructure, the differences in their DNA are critical. Digital asset securities are not anonymous bearer instruments like non-security digital assets that change hands on a range of domestic and foreign venues, liquidity pools and through other transactions. Digital asset securities are created and issued by a known issuer in accordance with U.S. securities laws. Their ownership is known and tracked by an issuer, its transfer agent or other regulated market participants. Digital asset securities are governed by a software protocol known as a smart contract, or the underlying protocol and consensus algorithms of the associated blockchain network, which controls all transactions relating to the digital asset security and, in most cases, the issuer of a digital asset security retains permission rights to override erroneous or fraudulent transactions.

The DOJ Report relies, in part, on a *Reuters* article, dated February 11, 2020, that reported cryptocurrency crime losses more than doubled to $4.5 billion in 2019.[4] This data, in turn, came from a 2019 CipherTrace report.[5] The examples of fraud, theft or loss cited in the 2019 CipherTrace report included non-U.S. regulated cryptocurrency exchanges that misused customer assets[6] and utilized poor private key management

---

[3] U.S. Dep't of Just., Report of the Attorney General's Cyber Digital Task Force: Cryptocurrency Enforcement Framework, at 15-16 (2020), https://www.justice.gov/archives/ag/page/1326061/download.
[4] *Id.* at 15 n.33.
[5] *Cryptocurrency Anti-Money Laundering Report, 2019 Q4*, CipherTrace Cryptocurrency Intelligence (January 2020) [hereinafter *Cryptocurrency Anti-Money Laundering Report*], https://ciphertrace.com/wp-content/uploads/2020/02/CipherTrace-CAML-2019-Q4-20200220.pdf.
[6] Affidavit of Sammy Wu, *British Columbia Sec. Comm'n v. Gokturk, et al*, No. S-1912424, (November 1, 2019), https://docs.grantthornton.ca/document-

practices, such as entrusting one person with control of a private key or exposing a private key to hacks.[7] With proper safeguards in place, administered by regulated firms as contemplated in the Statement, there is no reason to believe that digital asset securities, or non-security digital assets for that matter, present some sort of irreducible and inherent risk due to their technological DNA or that there is a greater risk that SPBDs taking custody of those assets will misuse or mismanage them in some way (as compared to a broker-dealer taking custody of traditional securities and cash, for example).

Consistent with a broker-dealer's obligation to safeguard and segregate its customers' securities pursuant to Rule 15c3-3 under the Securities Exchange Act of 1934 (as amended, the "Exchange Act"), the Statement requires robust standards for secure private key management for digital asset securities. We very much agree with that priority. This requirement recognizes that the main way to gain access to a digital asset is to obtain access to the private key controlling access to the wallet address that is the recorded owner of the digital asset on a blockchain.[8] By implementing and following robust standards for secure private key management, the risk of any digital asset (whether a security or not) being subject to fraud, theft or loss is greatly reduced. Even if an SPBD's private keys were compromised, there are usually steps an issuer of a digital asset security, in cooperation with the relevant firm, can take to override or reverse any fraudulent or erroneous transactions and make the SPBD and its customer whole (arguably, in a manner that is far more transparent, efficient and rapid than the procedures available for traditional securities in similar circumstances which can and do arise in the industry).

Rule 15c3-3, moreover, helps ensure that a broker-dealer that carries customers' accounts segregates its proprietary business from its customer business by requiring that the broker-dealer take physical possession or control over customers' fully-paid and excess margin securities and requiring the broker-dealer to segregate the net cash it owes to customers in a reserve bank account. In addition, the Statement imposes requirements with respect to establishing and maintaining control over customers' digital asset securities tailored to the certain aspects of these securities identified by the Commission. SPBDs will also be subject to the same robust financial responsibility requirements as a traditional broker-dealer, in addition to Rule 15c3-3 and the requirements of the Statement. For example, an SPBD will be subject to the same minimum net capital requirements under Rule 15c3-1 under the Exchange Act as a traditional broker-dealer that handles customer funds and securities. The net capital rule is intended to help ensure that a broker-dealer maintains sufficient liquid assets so that it can continue to operate or be wound down in an orderly fashion without resorting to

folder/viewer/docul8LWsxcWho7J/298293881135748939?_ga=2.196575148.1496879602.1572969739-839882587.1572969739.

[7] *Cryptocurrency Anti-Money Laundering Report*, *supra* note 2, at 17.

[8] This assumes that the smart contract or underlying protocol is properly programmed, which should be confirmed by an SPBD during its assessment of a digital asset prior to taking custody of such asset.

insolvency proceedings in the event that the broker-dealer experiences financial difficulty. These financial responsibility requirements do – and should – remain in place with respect to digital asset securities. Arguably, the digital asset securities business is more regulated and contained than the traditional business – we are not arguing the wisdom of that approach, given the relative novelty of these assets. We are suggesting, however, that it should not be isolated further into unusual and unnecessary vehicles that can only offer limited (but hopefully increasing) product offerings to their customers with little corollary justification and significant impact on the potential viability of firms that choose to operate in this space, unable to offer their customers even a meaningful securities product set as the market evolves. That result does not further the objective of the Statement to drive innovation.

Additionally, bifurcating digital asset securities business from traditional securities business will not impact the customer protection regime set out in SIPA if an SPBD were to fail. SIPA provides that, in the event of a broker-dealer insolvency, customers of the insolvent broker-dealer are entitled to share pro rata in the estate of "customer property."[9] "Customer property" includes "cash and securities (except customer name securities delivered to the customer) at any time received, acquired, or held by or for the account of a debtor from or for the securities accounts of a customer."[10] The definition of "security" under SIPA largely mirrors the definition of that term under the Exchange Act and the Securities Act of 1933 (as amended, the "Securities Act") and includes "any note, stock, treasury stock, bond, debenture, evidence of indebtedness," among other things; it specifically excludes unregistered investment contracts.[11] The technological features of digital asset securities would not be a factor in determining whether such securities are a "security" under SIPA.[12] If a digital asset security is an equity or fixed-income security, for example, it would be covered under SIPA just as traditional equity or fixed-income securities would be. Similarly, if a digital asset security is an unregistered investment contract, it would not be covered by SIPA, just as a traditional investment contract would not be. Therefore, in the event of an insolvency of an SPBD carrying customers' digital asset securities, those securities would form a part of the SPBD's estate of customer property entitled to protection under SIPA, just as traditional securities carried for the accounts of customers would. To the extent the Commission remains concerned that the risk of theft or loss of digital asset securities would reduce the overall pool of "customer property" for traditional securities investors in the event of a broker-dealer dissolution,

[9] 15 U.S.C. § 78fff-2(b).
[10] *Id.* § 78lll(4).
[11] *Id.* § 78lll(14).
[12] We would welcome a conversation with relevant policymakers, the Commission and the Securities Investor Protection Corporation regarding expansion of SIPA coverage to these types of investment contracts. A number of legacy or proposed digital assets in the market may arguably be investment contracts under applicable court and regulatory guidance and encouraging, and making it easier for, parties to accept their status as a security, issue them in an appropriate exempt offering and provide for secondary liquidity on a regulated venue consistent with U.S. securities laws would inure to the benefit of the investors and the marketplace more than continuing a situation that creates compliance disincentives.

there are safeguards available to address this concern without requiring a single purpose broker-dealer to engage in a digital asset securities business. These safeguards may include: (a) additional customer disclosures and/or (b) requiring an SPBD that engages in a traditional securities business to maintain additional capital reserves and/or carry additional insurance or other security for its digital asset securities in custody. Creating a bifurcated regulatory structure to address the conceptual risk of an SPBD incurring substantial financial losses and potentially failing solely as a result of custodying digital asset securities delivers a solution that is far broader than the issue it is seeking to address. Narrower tools are available.

The Commission also states "[t]he technical requirements for transacting and custodying digital asset securities are different from those involving traditional securities."[13] The Commission notes that to comply with paragraph (b) of Rule 15c3-3, which requires a broker-dealer to custody its customers' securities by establishing physical possession or control of such securities in the manner set out in such Rule, an SPBD custodying digital asset securities may not be able to rely on the same control mechanisms as it would for traditional securities. We understand, however, that the Statement's key objective is to address that gap – to provide a path for a broker-dealer to custody their customers' digital asset securities in compliance with Rule 15c3-3. We believe it would be superfluous – and contrary to the intent of the Statement – to require that, in addition to the custody requirements of the Statement, a broker-dealer separately also meet the requirements of the enumerated legacy control mechanisms in paragraphs (b) and (c) of Rule 15c3-3. Rule 15c3-3 would require an SPBD to carry its customers' securities in compliance with such Rule, irrespective of whether those customers hold digital asset securities or traditional securities. An SPBD would therefore establish custody of its customers' digital asset securities for purposes of Rule 15c3-3 in accordance with the Statement's custody regime and, in parallel, would continue to establish physical possession or control of its customers' traditional securities in compliance with the requirements of paragraphs (b) and (c) of Rule 15c3-3 – much like a broker-dealer may use multiple control mechanisms now under Rule 15c3-3 to account for various types of securities in its custody. It is unclear why bifurcating digital asset securities and traditional securities businesses between separate monoline broker-dealers would limit risks to customers when a combined entity would apply the same customer protection regimes as two separate entities – or why a broker-dealer custodying digital asset securities will find itself in want of a control mechanism, when the Statement provides that path (irrespective of whether such securities are the exclusive product set of that firm).

The bifurcated approach to regulation of digital asset securities and traditional securities also does not align with the historical approach to addressing varying risks within a broker-dealer. For example, a self-clearing or correspondent clearing broker-

[13] 86 Fed. Reg. at 11,628.

dealer that carries customer accounts and thus handles customers' funds and securities, has a higher minimum net capital requirement than one that does not carry customer accounts. If that broker-dealer engages in margin lending to its customers, that business line will attract a higher minimum net capital requirement for such broker-dealer. If that broker-dealer engages in proprietary trading, its proprietary securities positions are subject to risk-based haircuts to help ensure that the broker-dealer maintains sufficient liquid assets with respect to its business. Just as the Commission has not required bifurcating proprietary securities trading and a customer securities business into separate broker-dealers, despite the unique risks of each business, there is no reason to bifurcate customer digital asset securities and traditional securities businesses into separate broker-dealers where the risks unique to digital asset securities are addressed by the manner of establishing control of such securities established in the Statement.

To these ends, the bifurcated approach to customer protection under the Statement is unlikely to provide incremental risk mitigation (or at least not one proportional to the risk at hand). More importantly, it is likely to make it harder for the monoline boutique SPBDs (especially those not part of larger families of companies that can subsidize such operations) to sustain their growth. The market and the innovation the Statement rightly seeks to fuel will suffer. In addition, this approach will not inure to the benefit of the investors, who will be required to maintain brokerage accounts at different broker-dealers in order to trade both digital asset securities and traditional securities. This would cause unnecessary inconvenience, duplication and confusion, particularly for customers of affiliated broker-dealers. Since SPBDs will be limited in the products they can offer their customers, it will make it harder for customers of SPBDs to diversify their securities holdings and may cause them to have a less diversified portfolio than if traditional securities services were offered by SPBDs. As noted above, the requirement is also likely to discourage broker-dealers from custodying digital asset securities, which will result in fewer options available for investors in digital asset securities and a correspondingly higher risk for the industry if one SPBD were to fail than it otherwise might. Therefore, in seeking to protect investors by isolating risk, the Statement delivers a result that does not optimize the environment which would best serve and protect the investors and sustain innovation.

<u>The Commission should consider permitting the use of non-security digital assets as a means of funding and settling digital asset securities transactions and allow broker-dealers to conduct a non-security digital asset business.</u>

The Commission should permit SPBDs to accept deposits of non-security digital assets from customers and to settle customer transactions in digital asset security transactions using non-security digital assets because it is necessary to assess the viability of digital asset securities. The Statement does not allow an SPBD to accept or hold customers' non-security digital assets. SPBD customer accounts will need to be funded with fiat currency and the cash leg of a digital asset securities transaction,

therefore, will need to settle through traditional cash payment systems. This would considerably delay the settlement process and undermine one of the main benefits of blockchain technology – real-time settlement. Currently, fiat currency and the traditional banking system is not interoperable with the ecosystem for digital asset securities, at least not in a manner that does not neuter the key benefits of digital infrastructure.

We recognize that policymakers and banking regulators have started their journey towards adopting a path and regulatory framework for central bank digital currencies.[14] We support those initiatives. Given the scale of the undertaking, they will likely take time to be implemented, particularly in larger markets. Yet the cash leg of the settlement cycle must be synched with the instantaneous transfer of digital asset securities. Without that, we are using a mule to pull a racecar.

Since there is no central bank digital currency that can be used by SPBDs to settle transactions in digital asset securities today; other non-security digital assets must be used for settlement. Those solutions exist and they can be deployed in a measured, incremental manner that does not inject more risk into the ecosystem.

During the five-year effective period of the Statement, we suggest that the Commission permit the incremental steps forward, which are set forth below, to modernize the cash leg of a securities transaction. This is a fundamental element in realizing the benefits of distributed ledger technology and its potential to positively transform capital markets. Real-time settlement cannot be achieved if SPBDs are required to clear and settle transactions using traditional fiat currency. Further, if clearance and settlement occurs on the blockchain, it ensures the accuracy of transaction records because the blockchain recording the transfer of non-security digital assets and digital asset securities is the actual settlement (there are no records of off-blockchain events that need to be transferred to the blockchain record or reconciled with the blockchain record). If the cash leg of the transaction occurs through legacy systems – the blockchain record will either be incomplete (if it only records the securities leg of a transaction) or exposed to heightened risk of potential error, data loss or manipulation (if the operational process for copying the governing record of the cash transfer to the blockchain experiences a disruption or error). In addition, multiple sets of records that either exist in parallel or have to be reconciled increases the potential for security breaches and other illicit activities. Without the use of non-security digital assets, the

[14] *See Central bank digital currencies have the power to upend global finance*, Cointelegraph, (October 26, 2020), https://cointelegraph.com/news/central-bank-digital-currencies-have-the-power-to-upend-global-finance ("An astonishing 80% of central banks are engaging in work around central bank digital currencies, from research to experimentation and pilot programs."). *See also* Raphael Auer, Giulio Cornelli & Jon Frost, *Rise of the central bank digital currencies: drivers, approaches and technologies*, Bank for International Settlements, BIS Working Papers No. 880, (August 2020), https://www.bis.org/publ/work880.pdf ("Based on a survey of central banks in the BIS Committee on Payments and Market Infrastructures (CPMI) in late 2019, Boar et al (2020) show that in advanced economies (AEs), central banks are researching [central bank digital currencies] to promote safety and robustness, or domestic payments efficiency…").

Commission's five-year examination of digital asset securities will not be a complete examination and will lack fundamental data points. In fact, it is likely to deter participants or steer them towards establishing isolated, closed-loop ecosystems that deprive customers of the choice and liquidity offered by a connected market.

Initially, SPBDs could take custody of non-security digital assets for the following purposes:

1. To enable customers to fund their accounts with non-security digital assets accepted by the SPBD in accordance with its risk management policies and procedures, in addition to traditional fiat currency.
2. To settle transactions in digital asset securities using customers' non-security digital assets (and to pay for associated network fees, which, as we discuss below, may only be funded in non-security digital assets).
3. To liquidate customers' non-security digital assets to fund traditional securities transactions (assuming the Commission permits SPBDs to have a traditional securities business, as discussed earlier).

These activities can be conducted in a risk-conscious manner to protect investors. The prudent compliance architecture that an SPBD must implement under the Statement to custody digital asset securities can be applied to an SPBD holding non-security digital assets as well. Among other things, the SPBD would safeguard and maintain the private key controlling access to the wallet address that is the recorded owner of its customers' non-security digital assets, whether directly using a key management service, in conjunction with cold storage and/or multi-party computation (we touch on these concepts in more detail below), or through an appropriate banking institution or other regulated custodian – thereby largely mirroring the risk profile of fiat cash that is currently custodied by firms. The SPBD would have in place and enforce appropriate policies and procedures to confirm that the non-security digital assets are not securities and are otherwise lawful non-security digital assets.[15] The SPBD would not facilitate any transaction in non-security digital assets if material security or operational problems arose. The SPBD would have in place policies and procedures to address, among other things, 51% attacks, airdrops and hard forks. Lastly, the SPBD would inform customers that non-security digital assets are not securities and not protected under SIPA, just as they would for securities not covered by SIPA.

[15] In performing this task, an SPBD can leverage existing analytical tools to assess whether a digital asset is a security under U.S. securities laws. It is beyond the scope of this letter for us to comment on the current of state of jurisprudence with respect what may constitute a security for purposes of federal securities laws and recent Commission actions on this topic relating to digital assets. Whether further positive guidance and clarity would inure to the benefit of an evolving marketplace is likewise a topic we would be happy to address for the Commission, if requested. We would welcome further dialogue with the Commission and industry participants to develop tools for an SPBD to document and make such determination.

An SPBD could take custody of non-security digital assets in a manner very similar to the manner it custodies traditional fiat currency. As we touch on above, the Office of the Comptroller of the Currency ("OCC") recently confirmed that national trust banks may custody a variety of digital assets, including non-security digital assets. This allows an SPBD to maintain a type of reserve bank account for its customers' non-security digital asset positions. The SPBD could calculate its reserve bank account deposit requirement in accordance with the applicable provisions of the Reserve Formula set out in Appendix A to Rule 15c3-3. The non-security digital asset account would be maintained in the name of the SPBD's non-security digital asset customers and thus would effectively be bankruptcy remote. We expect that in the event of an insolvency, those customers would be entitled to the return of their non-security digital assets.

We understand that the Commission expressed concern that, in the event of an insolvency of an SPBD, non-security digital assets carried for the account of customers would not be customer property within the meaning of SIPA, which would cause customers holding non-security digital assets to be general creditors of the SPBD in a SIPA liquidation. To address this concern, an SPBD could purchase insurance for the benefit of its non-security digital asset customers. In the event of an insolvency of the SPBD, the non-security digital asset customers or trustees acting on their behalf would file a claim with the insurer for reimbursement up to the policy limits outside of the insolvency proceedings. The insurer may, in turn, assume such customers' general creditor claims and have a right to pursue those claims in the insolvency proceeding. To the extent the Commission wanted to make additional insurance coverage a condition to an SPBD taking custody of a customer's non-security digital assets, we would welcome the opportunity to work with the Commission, self-regulatory organizations and market participants on uniform standards for such insurance coverage – much like how the industry has developed similar credit protection mechanisms for other assets. Only here, instant settlement greatly reduces counterparty and settlement risk – so the incremental cost of this insurance could be offset by reduction in risk mitigation measures around the settlement cycle.

We also note that without any access to non-security digital assets, the digital asset broker-dealer experiment will never get off the ground at all. To enable an SPBD to send and receive digital asset securities, the Commission must permit an SPBD to custody some amount of non-security digital assets, either for its customers or on a proprietary basis,[16] so that the SPBD can pay the network fees for each digital asset security transaction it submits to be processed on a blockchain network. Network fees compensate miners for the computing energy required to process and validate transactions. For example, if an SPBD requests that digital asset securities issued on the

[16] Such assets would have no value for net capital purposes. Thus, an SPBD's net capital requirements would be funded entirely by traditional securities and cash. In other words, an SPBD would need to maintain a sufficient level of traditional securities and cash to support both its customer securities business and its proprietary trading pursuant to Rule 15c3-1.

Ethereum blockchain and in its custody be sent to another SPBD, the wallet address of the SPBD which made such request would have to have a sufficient amount of ether to pay for the network fees to process and validate such transfer. If an SPBD cannot hold non-security digital assets for this purpose, it cannot send and receive digital asset securities.[17] The business does not work. Now, technology and methods (including those developed by tZERO) exist to optimize network usage and fee efficiency and reduce costs to the SPBDs and the investors – but it cannot be zero.

Finally, we ask the Commission to expand its position to allow SPBDs to engage in a non-security digital asset business.

To enable SPBDs to offer a complete range of product offerings to their customers, we suggest that the Commission expand its position to allow SPBDs to engage in a non-security digital asset business. SPBDs could facilitate purchases and sales for non-security digital assets for their customers.[18] SPBDs could custody these non-security assets for their customers or work with various services providers to assist it in sourcing and custodying non-security digital assets. Expanding the Statement in this manner would bring these services under the purview of a controlled and regulated environment, which will ultimately enhance investor protections and complete the full breadth of services needed to offer customers a single touch point to trade and custody a variety of assets under one umbrella (in conjunction with expanding the Statement to allow SPBDs to engage in a traditional securities business and to accept non-security digital assets as a form of funding for brokerage accounts and payment for digital asset securities transactions).

b. What are industry best practices with respect to protecting against theft, loss, and unauthorized or accidental use of private keys necessary for accessing and transferring digital asset securities? What are industry best practices for generating, safekeeping, and using private keys? Please identify the sources of such best practices.[19]

The Commission's focus on safeguarding against the theft, loss, and unauthorized or accidental use of private keys with respect to the custody of digital assets, including digital asset securities, is well placed. SPBDs will establish custody over a digital asset

[17] At a minimum, we suggest that the Commission clarify that SPBDs will be subject to a de minimis threshold to allow SPBDs to pay network fees.

[18] Similarly, consideration should be given to permitting traditional broker-dealers to engage in such activities on an agency basis. We acknowledge, however, that traditional broker-dealers would have to implement additional operational and compliance architecture before engaging in such activity.

[19] There are processes, software and hardware systems, and other formats or systems that are currently available to broker-dealers to assist them in creating, storing, or using private keys and protecting such from loss, theft, or unauthorized or accidental use. While we have not provided a list of each of these vendors, we would be pleased to engage in further dialogue with the Commission and the industry on this topic. Of course, we would expect SPBDs to conduct due diligence of such vendors in accordance with their current vendor procurement management programs and applicable rules.

security when it is sent from a third-party wallet address to the SPBD's custodial wallet address. Once a digital asset security is sent to an SPBD's wallet address the main way to compromise the custody of such digital asset security or send it elsewhere is by obtaining access to the private key that controls such wallet address.

Each wallet address is controlled by a pair of keys: a public key and private key. The private key is used to sign transactions, whereas the public key is used to verify the signatures of these transactions. A public key cannot be tampered with or used without access to its associated private key. Therefore, safeguarding an SPBD's private key is necessary and critical for the SPBD to safeguard its customers' digital asset securities.

Private keys that need online network access to sign transactions (for example, deposits, withdrawals, trades and other transfers), as with the private keys of an SPBD, should be encrypted using a robust symmetric-key encryption algorithm and managed using the technology industry's best practices of encryption key management. To create, store and manage private keys during their life cycle, SPBDs can use a key management service, offered by a vendor that specializes in encryption. SPBDs would conduct due diligence on the key management service and vendor offering such services (as any firm is required to do with current vendors) to confirm the service is offered in accordance with the technology industry's best practices for generating, safekeeping and using private keys. These include the Federal Information Processing Standard Publication 140-2, a security standard that sets forth requirements for cryptographic modules, published by the National Institute of Standards and Technology. We understand that certain vendors' key management services are validated to comply with this standard. Using a key management service does not mean a third-party will have control over an SPBD's private keys. It provides the SPBD the tools it needs to generate and securely store private keys.[20] After an SPBD creates a private key, it should not allow such private key to travel across an online network. Instead, transactions should be sent across an online network to the server holding such encrypted private key to be signed.

The process described above is likely to be reasonably tailored to the risk profile of most digital asset securities because most issuers of digital asset securities, or such issuer's transfer agent, have control of a private key that has the ability to reverse an erroneous or fraudulent transaction. In these cases, SPBDs will be able to work with such issuers (or their transfer agents) if an erroneous or fraudulent transfer were to occur in a

[20] If the SPBD uses a software-as-a-service ("SaaS") key management service, we understand that the SaaS provider would store the encrypted form of the private key(s), but decryption of the private key(s) would only possible by the SPBD. The SPBD's private keys would then essentially be encrypted using another private key that only the SPBD controls, ensuring that the SaaS provider does not have the ability to decrypt them on their own. The SaaS provider would be responsible for hosting the service and storage of the encrypted forms of the private key(s). An SPBD could also self-host a key management service within their own infrastructure.

pre-defined process and reverse[21] such transaction – in a process that is quicker and more frictionless than the current process for replacing lost or other types of securities.[22]

In the case of digital asset securities with no such functionality or non-security digital assets, however, SPBDs should take additional steps to safeguard its private keys for such digital assets. Cold storage, where the private keys for digital assets are stored in a secure location not accessible to an on-line network, with multiple stakeholders and other proprietary processes required to authorize a transfer using such private keys in cold storage, is one method. As the Commission is aware, it has been used widely in the non-security digital asset industry for some time, with a range of service providers, technologies, processes and innovations. One downside – albeit one that is mitigated by some market innovation – is that digital assets secured with cold storage type solutions are not easily accessible. To mitigate that, we understand that custodians may also keep a certain (smaller) amount of non-security digital assets in a wallet governed by a private key accessible online, using a key management service described earlier. This split approach would enable them to process transfers and withdrawals on a real-time basis.

Multi-party computation is another method for safeguarding private keys. It allows a party to store a private key online – making it more easily accessible than most types of cold storage – but also splits a private key into multiple parts stored on different devices, which ideally are geographically diversified, with a certain process that governs how the several parts may be brought together to complete the private key. This significantly mitigates the risk of a single point of vulnerability in the event of a cybersecurity incident. Although this is a very fast-moving space, we would expect multi-party computation to play an increasingly more visible role for private key management in the future. In any event, these additional measures can be taken by an SPBD which custodies digital assets with no central party managing a private key that can override erroneous or fraudulent transactions.

An SPBD should have multiple private keys for different purposes and different categories of digital assets so one private key does not control all of the digital assets in its custody, which will minimize the potential for loss if its private key(s) are compromised. Likewise, it should implement different key management procedures reasonably tailored to the risk of theft or loss for such digital assets controlled by such private key. This would

[21] By "reverse" we mean that a new transaction would be submitted to the blockchain to transfer the digital assets back to their rightful owners – the record of this transaction and the erroneous transaction would, of course, continue to be visible on the blockchain record, which is immutable.

[22] One approach to safeguard this private key after it is generated is Shamir's Secret Algorithm, which can be used to secure a private key in a distributed way. It works by splitting the private key into multiple parts. These parts are reconstructed when the private key needs to be used. To reconstruct the private key, you need a minimum number of parts. This is called the threshold. Each part of the private key is held by different authorized persons in a separate secure location. The private key can be programmed to work if the threshold number of parts of the private key are re-complied to sign off on a transaction.

align with the current imperative for broker-dealers to ensure the integrity of their technologies, systems, data and assets.

c. What are industry best practices to address events that could affect a broker-dealer's custody of digital asset securities such as a hard fork, airdrop, or 51% attack? Please identify the sources of such best practices.

As a preliminary matter, it is important to note that hard forks, airdrops, and 51% attacks will not affect an SPBD's custody of its customers' digital assets, including digital asset securities. In other words, these events, in and of themselves, will not lead to a customer's digital asset securities being lost or stolen and such events, in and of themselves, will not affect the security of an SPBD's private key. In certain cases, hard forks and 51% attacks may cause disruption of a blockchain network. Any technological system, however, may be subject to operational disruption. Legacy architecture, assembled across a patchwork of systems, uncoordinated intermediaries, other participants and standards, is far from immune, and should not be used as a gold-standard point of reference. In the case of blockchain technology, these events, if they were to occur, would happen publicly, and would often be in the public domain before disruption to a network occurs (compared to the opacity and responsiveness of legacy systems). SPBDs can assess the threat of these events to a network prior to supporting them and follow their policies and procedures in the event they occur.

Immediately following a hard fork, the updated network has a duplicate of each asset that was on the original network, and the owners of such assets and their historical transaction history is copied onto the updated network as well. The owner of a digital asset that resides on the original network will continue to own that asset on the original network after a hard fork, but will also own the duplicate digital asset that is created on the updated network after the hard fork. The SPBD's receipt of the duplicate digital asset created by the hard fork will not permit or cause any malicious malware to affect its custodial wallet address(es) or private keys. The SPBD receives the duplicate digital asset security following the hard fork because the smart contract or underlying protocol for each digital asset security on the original network is also duplicated on the updated network.[23] This will not cause any changes to the nature of the duplicate digital asset security created by the hard fork, the digital asset security will continue to be governed by its smart contract or underlying protocol, which is controlled by the issuer of the digital asset security and, if properly programmed, cannot be altered by a consensus of nodes on the network.

In many cases, an SPBD will have foresight that a hard fork is coming as new code first becomes available to network users as an optional update and only when a specified

[23] Likewise, even if a digital asset is not governed by a smart contract, all wallet addresses on the existing network owning a digital asset will be recorded as the owners of the duplicate digital asset on the updated network in the same form and quantity.

percentage of the nodes implements the update, the mandatory hard fork occurs.[24] For certain networks, the SPBD may even have the opportunity to vote on whether the update should be implemented by the network.[25] In any case, the SPBD would have procedures in place to monitor for software updates to each blockchain network that is utilized by the digital asset securities it custodies for its customers. Therefore, in many cases, it will have sufficient advance time to act on any potential hard fork. We would expect that, upon becoming aware of a potential hard fork, the SPBD would notify its customers of the potential hard fork and remind them of existing disclosures regarding that risk and possibility (similar to existing broker-dealer disclosures regarding business continuity plans). The SPBD would also determine, based on existing procedures, if it can custody the new digital asset security in accordance with the Statement, including whether the updated network has any material security or operational problems or weaknesses. Once the fork occurs, the surviving rails need to be determined. The SPBD is unlikely to be put in a position to need to drive that determination. The users of a blockchain network may reach a consensus as to which network they want to follow (there have been examples, however, where the original network and updated network continue to run in parallel). An issuer of the digital asset security running on the original network may determine that the creation of duplicate digital asset securities on the updated network is a new issuance of securities issued not in compliance with applicable securities laws and burn the digital asset securities on the network it does follow. If the issuer decided to follow the updated network or if the original network was abandoned, the SPBD would follow its documented assessment done earlier and communicate such updates to its customers. In cases where an SPBD receives custody of duplicate digital asset securities that are associated with an updated network that the SPBD determines it cannot support, it would have procedures in place to return such assets to its customers (again a plan which can be set in advance given that hard forks are unlikely to sneak up on the market for reasons described above).

Likewise, an airdrop may be planned. In case of airdrops that are supporting a corporate action, like a dividend, the timeline will be dictated by, and communicated in advance by the issuer in accordance with applicable securities laws and corporate law. An SPBD would have policies developed in advance to support this activity, as broker-

---

[24] *See* Luit Hollander, *History of Ethereum Hard Forks*, My Crypto, (May 4, 2020), https://medium.com/mycrypto/the-history-of-ethereum-hard-forks-6a6dae76d56f (giving a history of planned and unplanned hard forks on the Ethereum; even in the case of unplanned hard forks users of the network, who were monitoring network changes, still had foresight such updates were in process). *See also* Ethereum Foundation Blog, https://blog.ethereum.org/search/?query=hard%20fork (citing articles that describe changes in planned and unplanned hard forks) and Tim Beiko, *Ethereum Berlin Upgrade Announcement*, Ethereum Foundation Blog, (March 8, 2021), https://blog.ethereum.org/2021/03/08/ethereum-berlin-upgrade-announcement/ (describing planned upgrades in the next expected Ethereum hard fork).

[25] For example, each network update to the Tezos network goes through on-chain governance, first. Once a proposal has been implemented, and is ready for inclusion, an on-chain vote takes place among all stakeholders. The network as a whole either upgrades, or doesn't, depending on the outcome of the vote.

dealers currently do with respect to corporate actions. Where an SPBD has notice of an expected airdrop, it would follow its policies to assess the characteristics of a digital asset's distributed ledger technology and associated network prior to undertaking to maintain custody of the digital asset. As noted, that work could be done while the announced airdrop is pending.

We do acknowledge, however, that airdrops can happen unexpectedly. Unexpected airdrops of digital assets can occur since permission is not needed to receive a digital asset to a wallet. We understand, however, that an airdrop (expected or unexpected) cannot be used to send malware or any harmful software that would compromise an SPBD's custody of digital asset securities or the SPBD's private keys. An airdrop will simply have the effect of notating the SPBD's wallet address as the record owner of the non-security digital asset on the applicable blockchain network. The SPBD would have procedures to monitor for unexpected airdrops (as broker-dealers do now to monitor and govern attempts to transfer assets into an account) and seek to ascertain the source of such airdrop, including from its customers, which would be incorporated into its anti-money laundering policies and procedures for suspicious activities. Depending on confirmation of the identity of the sender, proper ownership of the digital asset, and its assessment of the digital asset and its associate network, the SPBD could choose to either custody the digital asset for its customer, allow the customer to send the digital asset to its personal wallet address, send back the digital asset to the sender, or liquidate the digital asset and donate the proceeds to charity in accordance with its policies and procedures.

Fraudulent activities associated with airdrops are not new risks that arose because of the emergence of blockchain technology. For example, certain bad actors have used planned airdrops as an opportunity to masquerade as the issuer of the digital assets in a planned airdrop to solicit personal identifiable information, private keys or assets from the public.[26] They achieved this by soliciting information directly or through a website under the context that if you give the information, private key or asset requested, you will be added as the recipient of a valuable asset in the airdrop. In these cases, however, the airdrop itself did not cause losses, it was the solicitation of private information or assets under false pretenses that lead to theft or loss. Obtaining valuable information or assets under false pretenses is nothing new or particular to blockchain technology[27] and broker-dealers are experienced in safeguarding customer information and assets and identifying red flags related to such fraudulent activities. Bad actors attempting to use blockchain

[26] *See Crypto Airdrop — Separate Free Money and Scams*, Airdrop King, (May 15, 2019), https://medium.com/@airdropkingio/crypto-airdrop-separate-free-money-and-scams-264abdebdb44#:~:text=Information%20Gathering%20Scam%3A%20This%20is,party%20or%20used%20for%20phishing (describing information gathering, private key and bait and switch airdrop scams).
[27] *See Common Scams and Frauds*, USA Gov, https://www.usa.gov/common-scams-frauds#item-35527 (describing telephone scams when false promises are made to gain personal information and census scams when someone pretends to work for the Census Bureau to steal your personal information, among others).

technology for illicit purposes should not be construed as an inherent risk in the technology. In many ways, it is better suited to respond to these activities than the traditional institutions and ecosystems that, for example, are powered by a relatively discrete number of balkanized and competitive actors, rely on antiquated identification and authentication methodologies that rely on devices, information and processes that were not designed for those purposes (such as mobile phones), and are often more prone to insider threats and systemic stability concerns (too-big-to-fail risks) than distributed systems.

Lastly, assessing a blockchain network's vulnerabilities to 51% attacks should be part of the SPBD documented assessment of a digital asset's associated network prior to custodying such digital asset, just as it would review the security and operational resiliency of any technology it uses in its business. Digital assets powered on networks easily vulnerable to 51% attacks should not be appropriate for the SPBD.

It is worth noting that blockchain networks commonly used by digital asset securities would likely require an astronomical amount of financial investment to even potentially be subject to a 51% attack.[28] Expected network updates to Ethereum (known as Ethereum 2.0) will further reduce the probability of a 51% attack because it is transitioning to a proof-of-stake network (in such case, one would have to acquire over 51% of a network's staked non-security digital assets to successfully launch a 51% attack). Additionally, 51% attacks usually negatively affect the value of the native non-security digital asset of the network – this is likely to be a discouraging factor for one or more actors considering a 51% attack because, in many cases, the target of a 51% attack is the native non-security digital asset of the network.

Nonetheless, were an actor or a group of actors to obtain control of the majority of nodes on a blockchain network and such actor or group created new rules governing the network, we do not expect these new rules to change the nature of a digital asset, affect an SPBD's custody of a digital asset or compromise an SPBD's private keys. These network updates, however, could change the processing times for transaction settlement or affect network costs, which could impact how digital asset securities clear and settle on such network. Following a 51% attack, an SPBD would use its established policies and parameters to review the new rules governing the network, including whether the new rules expose the network to any material security or operational problems or weaknesses. In an outside worst-case scenario where a blockchain network was severely compromised by a 51% attack, and is potentially unrecoverable, an issuer whose securities are governed by smart contracts that are blockchain-agnostic and support multi-chain access (for example, tZERO's smart contract technology) could freeze their smart contract on the compromised blockchain network and transition their digital asset securities to a new blockchain network. In such case, the SBPD would confirm the new

[28] *See PoW 51% Attack Cost*, Crypto 51 (Dec. 2, 2020), https://www.crypto51.app/ (estimating that a 51% attack on the Ethereum network would cost $418,438 per hour).

network was one they could support (working with the impacted issuers). If an issuer did not take such action, the SPBD can cease custodying digital assets associated with the compromised network and return such digital assets to its customers in accordance with its appropriate procedures and with disclosures that summarize such 51% attack procedures, and associated risks, like disruption to the clearance and settlement of digital asset securities using such network and market volatility. In addition, if a disruptive 51% attack were to occur, this is likely to be an industry issue where a number of financial firms, together with regulators, would be involved in ensuring an appropriate response to the event.

d. What are accepted practices (or model language) with respect to disclosing the risks of digital asset securities and the use of private keys? Have these practices or the model language been utilized with customers?

Disclosures relating to digital asset securities should include risks associated with traditional securities and the disclosure requirements set forth in the Statement. We expect disclosures relating to digital asset securities to standardize as SPBDs begin to operate in accordance with the Statement. We would welcome the opportunity to work with the Commission, self-regulatory organizations and market participants to develop accepted practices and/or model language that SPBDs can use to disclose the risks associated with digital asset securities and the use of private keys.

e. What differences are there in the clearance and settlement of traditional securities and digital assets that could lead to higher or lower clearance and settlement risks for digital assets as compared to traditional securities?

There are three main differences in the clearance and settlement of digital asset securities as compared to traditional securities (when, in each case, trading is facilitated by a broker-dealer on a regulated trading venue): (1) digital asset securities can be settled real-time (traditional equity securities settle T+2); (2) digital asset securities can clear and settle without a central counterparty (most traditional public securities in the United States clear and settle through a central counterparty);[29] and (3) digital asset

[29] We would welcome further dialogue with the Commission and other industry participants regarding how the current custody, clearing and settlement ecosystem for public securities, which is built around a central counterparty, such as The Depository Trust & Clearing Corporation ("DTCC"), can be adapted for public digital asset securities, including during a transition period. The central counterparty, for example, could continue to serve as the control location (as it does now for most publicly-traded securities in the United States pursuant to Rule 15c3-3(c)(1)) and manage the private key for digital asset securities in its custody. In this role, the central counterparty can oversee clearance and settlement of digital asset securities on the blockchain and maintain central compliance registries. For example, the DTCC's Project Ion proposed design of a Digital Accelerated Settlement Service, which included asset digitization, trade capture, netting and settlement services. See *Project Ion Case Study*, The Depository Trust & Clearing Corporation (DTCC), (May 2020), https://www.dtcc.com/news/2020/may/18/dtcc-unveils-proposals-to-explore-further-digitalization (providing a link to the Project Ion case study).

securities clear and settle using distributed ledger technology (traditional securities clear and settle on a book-entry basis using legacy systems).

First, if the Commission permits SPBDs to settle digital asset securities transactions with non-security digital assets, SPBDs will be able settle digital asset security transactions with each other directly on a real-time basis on the blockchain (also referred to as real-time gross settlement).[30] This greatly reduces the current T+2 settlement cycle, offers real-time access to digital assets and real-time liquidity following a transaction and eliminates a lot of the risks and inefficiencies that stem from the delayed settlement cycle. Delivery of digital asset securities can be made in exchange for non-security digital assets on a delivery versus payment ("DVP") basis as transactions are submitted to a blockchain network by SPBDs. The blockchain network will certify every transaction and it will be settled after the blockchain network confirms the transaction has processed. In this respect, the clearance and settlement of digital asset securities is less risky than the clearance and settlement of traditional securities because a longer settlement cycle increases the risk that an unforeseen event could cause a trade to fail,[31] which can include a counterparty failing to deliver securities or payment or the breakdown in operational processes used to settle such transaction during the settlement lag. As noted earlier, however, this requires a real-time solution to the cash part of the settlement process which we described.

Certain industry participants have expressed concern that moving to a real-time settlement model would eliminate the benefits of netting.[32] While we acknowledge the liquidity and risk-mitigating benefit of netting in the current market infrastructure for regulated market participants, a blockchain-based market infrastructure would largely address or eliminate many of the concerns raised by market participants. Netting would therefore become a solution to nonexistent or largely mitigated problems.

Second, digital asset securities do not need to trade through a central counterparty because the blockchain provides market participants with "a shared database of securities ownership that can be updated without relying on multiple, specialized intermediaries or a third-party infrastructure."[33] Traditional public securities are governed by private, opaque and fragmented databases of ownership controlled by different parties, which includes a shareholder register controlled by the issuer or its transfer agent, a central counterparty's records of its participant broker-dealer holdings of a security and

---

[30] A broker-dealer that clears and settles securities transactions is exempt from clearing agency registration when performing such functions as part of its customer brokerage activities under Section 3(a)(23)(B) of the Exchange Act (15 U.S.C. §78c(a)(23)(B)).

[31] *Advancing Together: Leading the Industry to Accelerated Settlement*, The Depository Trust & Clearing Corporation (DTCC), (February 2021), https://www.cibcmellon.com/en/_locale-assets/pdf/straight-talk/2021/st20210302-dtcc-accelerated-settle-wp-2021.pdf.

[32] *Id.*

[33] Jonathan Chiu and Thorsten V. Koeppl, *Blockchain-Based Settlement for Asset Trading*, Bank of Canada, Staff Working Paper No. 2018-45, (September 2018), https://www.bankofcanada.ca/wp-content/uploads/2018/09/swp2018-45.pdf.

broker-dealers' records of beneficial ownership entitlements. These fragmented databases lack transparency and real-time methods of knowing how many shares are available. They also impose costs and administrative burdens on market participants, not just to maintain their fragmented record of security ownership, but also to reconcile their records with other books and records of market participants. In the desired end-state, digital asset securities will have one distributed record of all ownership on a blockchain that can be accessed by all relevant market participants in real-time, in a secure and privacy-conscious way.

Transitioning away from a centralized clearance and settlement model dependent on one central counterparty also reduces systemic risk (too-big-to-fail risks).[34] A blockchain-based clearance and settlement trading ecosystem, which is not dependent on a central counterparty, decentralizes the financial system and reduces interconnectedness, and reduces systemic risk and the likelihood of widespread market contagion in the event of the failure of a large and interconnected market participant (or the central counterparty itself). Broker-dealers will also not be burdened with posting collateral to or maintaining reserve funds with a central counterparty as financial guarantees to ensure that the transactions settle, including as a result of market volatility that we observed recently in some securities. These reserves can and do change, sometimes dramatically and quickly, in cases of particular market dislocation, and sometimes in ways that a firm may not be able to absorb. They serve as a safeguard in the case of an individual member's default and as safeguard against systemic risk. The cost to market participants to protect against the systemic risk created by a central counterparty is reduced by the adoption of blockchain technology.

Lastly, digital infrastructure and blockchain technology is superior to the legacy technology used to settle traditional securities transactions. A blockchain-based clearance and settlement system reduces operational risk in the clearance and settlement process. There is no reason that a digital asset security transaction will fail if it is properly submitted to a blockchain network. Certain industry participants have raised concerns associated with clearance and settlement on a blockchain, such as a delay in settlement due to off-market network fees being offered to process a transaction[35] and errors, flaws

---

[34] Systemic risks associated with central counterparties include: "(a) funding-liquidity shocks relating to both the supply of cash and collateral that spiral out of control; (b) the failure of critical [central counterparty] operations; (c) the failure of a [central counterparty] clearing member or connected party spilling over, coupled with the inadequacy of pre-funded [central counterparty] resources to cover an open position, and (d) the risk of interconnectedness, which is heightened due to the levels of concentration of [central counterparty] services and operators at the global level." Emilios Avgouleas & Aggelos Kiayias, *The Promise of Blockchain Technology for Global Securities and Derivatives Markets: The New Financial Ecosystem and the 'Holy Grail' of Systemic Risk Containment*, Eur Bus Org Law Rev 20**,** 81, 92 (2019), https://doi.org/10.1007/s40804-019-00133-3.

[35] If the network fee an SPBD offers to process a transaction is not in line with the prevailing rate of network fees at the time, a delay in settlement on the blockchain could occur. In this case, the transaction would remain in a pending state until a miner is willing to mine the transaction at the network

or faults (*i.e.* "bugs") in smart contracts.[36] These risks can be managed by the industry, regulators and technology providers (as they are now in analogous circumstances) and do not outweigh the efficiencies realized from clearance and settlement on a blockchain.

f. What specific benefits and/or risks are implicated in a broker-dealer operating a digital asset alternative trading system that the Commission should consider for any future measures it may take?

We do not anticipate the risks implicated in a broker-dealer operating a digital asset security alternative trading system[37] to be appreciably different from those implicated in operating an ATS for traditional securities. Initially, we expect that, like an ATS facilitating trading in traditional securities, an ATS facilitating trading in digital asset securities would operate a central limit order book off the blockchain. This is to ensure that network fees and technology speed associated with distributed ledger updates do not interfere with the speed of execution at this point.[38] In fact, it could use the same matching engine for digital asset securities and traditional securities. If the Commission expands the Statement to permit SPBDs to accept non-security digital assets as a means of payment for digital asset security transactions, below is an outline of how digital asset securities

---

fee offered by the SPBD. There is technology, however, that can monitor the current network fees at the time a transaction is submitted to the blockchain. Further, this same technology can monitor pending transactions of an SPBD and re-calibrate the network fees offered by such SPBD after a period of time specified by the SPBD. This technology can ensure that the network fees offered by the SPBD are at rates that will be accepted by the network of miners to mine the transaction within the timeframe desired by the SPBD in an automated and programmatic way. SPBDs in need of such technology could license it from a vendor, such as tZERO, which has its own proprietary software that can accomplish this. It is also worth noting that expected network updates to Ethereum (known as Ethereum 2.0) will greatly reduce the network costs on the Ethereum network. Other networks, like Tezos, have very low gas costs because the network limits the amount of gas one operation can consume.

[36] Others have noted that bugs in smart contacts may expose a digital asset security and the way it settles to operational vulnerabilities. All code is subject to bugs, including the computer programs that manage how traditional securities are settled and run our banking system. Unlike bugs in conventional systems, however, the bugs in smart contracts are visible to all markets participants. When an SPBD conducts and documents an assessment of the characteristics of a digital asset security's blockchain network, it should audit such digital asset security's smart contract for any bugs; it will also be able to monitor for bugs on an ongoing basis. Likewise, regulators will be able to audit the functionality of smart contracts, without a formal request, and make inquiries if any bugs are present on a network. Bugs present a risk to both legacy systems and distributed ledger technology, but with distributed ledger technology, a bug is more easily identified and therefore less likely to result in on-going disruption of the clearance and settlement processes.

[37] It may be helpful for the Commission to define the term "digital asset alternative trading system." For purposes of this letter, we have assumed such term means an ATS that matches orders in digital asset securities.

[38] As we discuss elsewhere in this letter, upcoming upgrades in blockchain technology, existing tools that help to optimize network fee usage and hybrid technology that optimizes the number of times changes have to be written to the distributed ledger can help to mitigate this concern and reduce its relevance in the near term as digital asset security volumes scale up.

can trade off the blockchain through an ATS and clear and settle using blockchain technology:[39]

1. Investor 1 submits sell order to SPBD 1;
2. SPBD 1 confirms on the blockchain that Investor 1 has digital asset securities;
3. Investor 2 submits buy order to SPBD 2;
4. SPBD 2 confirms on the blockchain that Investor 2 has non-security digital assets to settle the transaction;
5. SPBD 1 and 2 submit orders to an ATS for matching and execution;
6. The ATS matches orders through a conventional matching engine;[40]
7. The ATS sends execution reports to SPBD 1 and 2;
8. SPBD 1 submits the transaction on the blockchain (it sends delivery instructions for Investor 1's digital asset securities to be sent to SPBD 2 for Investor 2);
9. SPBD 2 submits the transaction on the blockchain (it sends delivery instructions for Investor 2's non-security digital assets to be sent to SPBD 1 for Investor 1);
10. The transactions submitted by each SPBD will be mined; note, however, the transaction will not be minded if delivery of both the digital asset securities and the non-security digital assets is not submitted to the blockchain (the applicable smart contract can be programmed to require DVP settlement);
11. Each SPBD will monitor its transactions on the blockchain for a predetermined amount of confirmations (a confirmation is a node confirming the transaction has occurred) showing a consensus that the transaction is settled; and
12. SPBD 1 and 2 notify their respective customers that a transaction is complete; the digital asset securities and non-security digital assets are available for trading.

As set forth above, initially, we expect SPBDs to custody, clear and settle transactions on a blockchain network. We do not expect broker-dealer operators of ATSs to be SPBDs (assuming they do not custody digital asset securities). The steps set forth above are somewhat analogous to the SEC's recent no-action letter setting forth a three-

[39] Each SPBD will need software to take these actions. They could license the software from a company like tZERO. The software would be installed on the SPBD's network to be operated by the SPBD.
[40] Note, in the future, as we discuss in this letter, a transaction could and would be matched on the blockchain.

step process for broker-dealers to facilitate trading in digital asset securities if such securities are custodied by customers with a third-party custodian[41] – but now SPBDs can take on the custodial role handled by customers and their third-party custodians in accordance with the Statement. Additionally, aside from clearance and settlement being facilitated on the blockchain, this process is also similar to the trading flow for existing securities that utilize non-controlling blockchain elements to enhance the issuer and investor experience but do not constitute digital asset securities. Adoption of the process above for over-the-counter digital asset securities would be a process familiar to many broker-dealers and largely consistent with conventional market practices in place today.

As market participants continue to adopt different applications of distributed ledger technology, and as technology advances, increases in network cost efficiency, increases in network speed, and the regulatory framework for distributed ledger technology advances, matching engines that match transactions on the blockchain may emerge as a superior operational system for ATSs. tZERO continues to assess the appropriate time for this step forward in the adoption of blockchain technology.

3. Additional Comments for the Commission's Consideration

In addition to the comments solicited by the Commission in the Statement, we respectfully request consideration of the following matters related to broker-dealer custody of digital asset securities:

a. We suggest the Commission clarify that the requirement to operate as an SPBD is limited to broker-dealers that custody digital asset securities.

We believe that the Commission intends to only require broker-dealers that custody digital asset securities to become SPBDs, given the focus in the Statement on the unique risks posed by custodying such securities and the Commission's qualification that its position in the Statement "is expressly limited to paragraph (b) of Rule 15c3-3."[42] That is, a broker-dealer that does not custody digital asset securities should be able to engage in both a digital asset securities business and a traditional securities business. Such broker-dealer should be able to effect transactions in digital asset securities solely on an agency basis and establish introducing/clearing arrangements with an SPBD for custody, clearance and settlement and/or operate an alternative trading system that matches orders in digital asset securities away from a blockchain. The Commission states, however, that to guard against the risk of fraud, theft and loss it believes are associated with digital asset securities, and "to operate in a manner consistent with the Commission's position [in the Statement], the broker-dealer could not deal in, effect transactions in, maintain custody of, or operate an alternative trading system for traditional securities."[43] The preceding language suggests that a broker-dealer that

[41] Baird, *supra* note 2.
[42] 86 Fed. Reg. at 11,631.
[43] *Id.* at 11,629.

engages solely in a non-custodial digital asset securities business might have to operate as an SPBD and refrain from engaging in a traditional securities business. These broker-dealers, however, will not have digital asset securities customers under Rule 15c3-3 and there is no risk of losses related to a digital asset securities business impacting the traditional securities business in the event of a broker-dealer insolvency. We suggest the Commission clarify that the requirement to operate as an SPBD is limited to broker-dealers that custody digital asset securities.

b. We suggest that the Commission confirm that securities that do not meet the definition of digital asset security should continue to be treated as traditional securities.

The Commission defines a "digital asset security" as "a digital asset that meets the definition of a 'security' under the federal securities laws."[44] The Commission, in turn, defines a "digital asset" as "an asset that is issued and/or transferred using distributed ledger or blockchain technology ("distributed ledger technology"), including, but not limited to, so-called "virtual currencies," "coins," and "tokens."[45] Based on existing guidance issued by the Commission relating to digital asset securities, stretching back to the Joint Staff Statement[46] issued on July 8, 2019 by the staffs of the Commission's Division of Trading and Markets and FINRA's Office of General Counsel, it would appear that securities that do not meet the definition of a digital asset security should be treated as any other uncertificated security in accordance with conventional market practices, rules and regulations.

It would be helpful for the Commission to confirm that limited blockchain enhancements to uncertificated securities do not cause a security to become a digital asset security. With the emergence of blockchain technology in capital markets, certain issuers of uncertificated securities have arranged for a digital courtesy carbon copy of its transfer agent's shareholder register and/or a carrying broker-dealer's records of beneficial ownership for such security to viewable on a blockchain to enhance the investor experience through added transparency.[47] The digital courtesy carbon copy on the blockchain, however, does not govern ownership of such securities. The only controlling record ownership for corporate and securities law purposes is the transfer agent's conventional books and records. The only controlling record of beneficial ownership is the carrying broker-dealer's conventional books and records. If such securities trade on an ATS, the only controlling execution records are the conventional books and records of

---

[44] *Id.* at 11,628-29 n.1

[45] *Id.*

[46] Div. of Trading & Mkts., U.S. Sec.& Exch. Comm'n, & Off. of Gen. Counsel, Fin, Indus. Regul. Auth., Joint Staff Statement on Broker-Dealer Custody of Digital Asset Securities (July 8, 2019), https://www.sec.gov/news/public-statement/joint-staff-statement-broker-dealer-custody-digital-asset-securities.

[47] tZERO has referred to such securities as digitally enhanced securities.

the broker-dealer operator of that ATS.

Broker-dealers can, and have, establish(ed) control of those securities for purposes of complying with Rule 15c3-3, in many cases under paragraph (c)(5) of Rule 15c3-3, which is self-operative. Consequently, the customer experience with these securities is not analogous to one involving a virtual currency or any other anonymous bearer digital instrument that trades peer-to-peer on a distributed ledger because such securities, as noted, are conventional, uncertificated securities operating within the conventional trading, clearing and settlement framework with regulated market participants playing their traditional controlling roles.

Therefore, to avoid any market confusion relating to existing securities in the market with limited blockchain functionality (the courtesy carbon copy of the controlling records of regulated market participants), the Commission should consider confirming that any security not meeting the definition of a digital asset security will be treated as a traditional security for regulatory purposes.

c. <u>We suggest the Commission clarify that a broker-dealer that maintains its customers' digital asset securities at a control location identified in paragraph (c) of Rule 15c3-3 under the Exchange Act is not an SPBD.</u>

The Statement permits a broker-dealer to establish custody of its customers' digital asset securities in accordance with the terms set out in the Statement. Such a broker-dealer would be an SPBD. The statement does not address broker-dealers holding customers' digital asset securities at control locations. Paragraph (c) of Rule 15c3-3 identifies locations at which a broker-dealer may establish control over its customers' securities for purposes of meeting the control requirement of paragraph (b) of the Rule for such securities. Paragraph (c)(5), for example, permits a broker-dealer to use a bank, as that term is defined under Section 3(a)(6) of the Exchange Act, as a control location. In connection with our earlier comment, the OCC recently confirmed that national trust banks may custody a variety of digital assets that would include digital asset securities.[48] Paragraph (c)(5) is self-effecting, so a broker-dealer should be able to establish a bank as a control location for its customers' digital asset securities without regulatory approval. Since these institutions already are permitted to custody digital asset securities, it will allow for greater market diversity of holdings and more efficient adoption of digital asset securities. The Commission should confirm that a broker-dealer is not required to custody digital asset securities itself; rather, it can hold such securities at control locations set out in paragraph (c) of Rule 15c3-3. Moreover, because the broker-dealer would not itself custody its customers' digital asset securities, it would not be an SPBD within the meaning of the Statement.

[48] Any other entity that meets the definition of a bank under Section 3(a)(6) of the Exchange Act, likewise, should be able to custody digital asset securities, provided in can maintain control of such assets.

d. We suggest that the Commission clarify that digital asset securities custodied by an SPBD will be considered to be held in "street name" for purposes of Section 12(g) of the Exchange Act.

The Commission should clarify digital asset securities registered in "street name" on a shareholder register will be given the same treatment as traditional securities registered in "street name" on a shareholder register under Section 12(g) of the Exchange Act. An issuer of a security must register under Section 12(g) of the Exchange Act if a class of its equity securities is held of record by either (1) 2,000 persons, or (2) 500 persons who are not accredited investors and, on the last day of the issuer's fiscal year, its total assets exceed $10 million. In the case of traditional securities held by broker-dealers for their customers, the holder of record is typically considered to be the broker-dealer, or the entity which custodies such securities for the broker-dealer, and not the underlying customers (the security is registered in "street name"). Therefore, issuers have not been required to look through to, and count, such broker-dealer's customers for purposes of determining if it is required to register such class of securities under Section 12(g) of the Exchange Act. The rationale for registering a security in "street name" was in part due to an issuer's, or its transfer agent's, limited ability to confirm, with up-to-the-minute accuracy and granularity (something, incidentally, that distributed ledger technology is really good at), which investors had beneficial ownership entitlements to their securities through a broker-dealer from time to time (vs. relying on the veracity of just listing an aggregated position carried by such broker-dealer).

As with traditional securities, we expect digital asset securities custodied by an SPBD to be registered in "street name" on transfer agents' books and records. While blockchain technology has the potential to eliminate the information asymmetries that were the impetus for the treatment of traditional securities registered in "street name" for purposes of Section 12(g) of the Exchange Act, imposing a different standard for counting holders of record on issuers of digital asset securities will have the result of giving disparate treatment to such issuers, which may disincentivize certain issuers from issuing digital asset securities in private offerings, decrease the appeal of this new technology for private securities which are expected to be the main category of securities that would take advantage of this technology at the start (as compared to public markets that take longer to change) and curtail some of the key benefits of the Jumpstart Our Business Startups Act, which was intended to encourage funding of small businesses in the United States. We ask that the Commission not make Section 12(g) of the Exchange Act a key determining factor in whether private issuers issue traditional or digital asset securities.

e. We suggest that the Commission clarify that SPBD blockchain records are suitable records for purposes of complying with Rule 17a-3 and Rule 17a-4 of the Exchange Act.

To further realize the efficiencies of blockchain technology, we encourage the Commission to consider clarifying that records created on the blockchain by an SPBD,

which the SPBD is required to make under Rule 17a-3 under the Exchange Act, may be solely stored on the blockchain in accordance with Rule 17a-4(f) under the Exchange Act. For example, an SPBD will be required to make and maintain daily, itemized records of all receipts and deliveries of securities under Rule 17a-3. Digital asset securities will be delivered and received on the blockchain, so all records of receipts and deliveries of digital asset securities will be stored on the blockchain. An SPBD should not be required to duplicate blockchain records in legacy systems, thereby introducing additional costs, inefficient redundancies and more potential for error, data loss, illicit activities and security incidents. As described above, the receipt and delivery of a digital asset security occurs when a transaction is recorded and validated on a blockchain network. The controlling record for whether a digital asset security was received or delivered is the blockchain record. If an SPBD were required to create legacy system records, such SPBD would need to create and maintain an operational process to transfer blockchain records to a legacy system and reconcile legacy systems records to blockchain records. There is no need for this costly redundancy (now that we have access under the Statement to securities where blockchain records may control), as an SPBD will be able to maintain duplicate copies of its blockchain records by standing up multiple nodes in its software managing its blockchain activity. Blockchain records also meet the storage medium requirements in Rule 17a-4(f): they are immutable, serialized, indexed, and readily downloadable. Therefore, requiring SPBDs to maintain legacy system records of their blockchain activity undermines that digital asset securities are governed by an error-proof, resilient, transparent, immutable and decentralized record keeping system.

f. <u>We suggest the Commission expand the Statement so that SPBDs may rely on smart contracts to automate broker-dealer compliance functions.</u>

We suggest that the Commission expand the Statement to permit SPBDs to rely on smart contracts to automate certain broker-dealer compliance functions, such as an SPBD's obligation to analyze whether a digital asset security is offered, sold and resold in compliance with the U.S. securities laws. All of the change in ownership transactions on the blockchain for such digital asset security have to comply with the rules that govern permission rights to change or update a digital record on a blockchain with respect to a digital asset security defined in its smart contract. We are not proposing that a smart contract replace all of an SPBD's existing compliance tools, but advocating that it is a powerful addition to the tools an SPBD has on hand, and in certain cases, can replace manual compliance processes.

Different technology providers have developed smart contract protocols. For example, tZERO's technology team has developed the Global Securities Standard, which is comprised of three different contracts that govern a digital asset security – the digital asset security contract, the compliance contract and the global registry contract. tZERO's compliance contract can be a useful tool for SPBDs in their analysis of digital asset securities compliance with applicable securities laws. The compliance contract is a hub

to which multiple compliance rules can be mapped to govern the allowable functions, holders, and transfers of a digital asset security. Through the compliance interface, permissions can be set that will dictate which functions a wallet address can execute. For example, the compliance interface permissions can:

1. Restrict transfers on restricted securities during the one-year holding period pursuant to Rule 144 under the Securities Act;
2. Restrict international investors who were issued shares in a Regulation S under the Securities Act offering from transferring their shares to a U.S. person;
3. Freeze all transfers at the digital asset security or individual wallet addresses level;
4. Restrict what addresses can hold a digital asset security based on investor status (for example, whether you are an accredited investor or a qualified purchaser); and
5. Enforce a holder limit (for example, for purposes of Section 12(g) of the Exchange Act or Section (c)(1) and Section (c)(7) of the Investment Company Act of 1940).

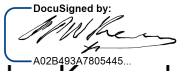
The compliance contract can assist an SPBD to, among other things, confirm that an offering of digital asset securities under Regulation D was only issued to accredited investors, confirm that digital asset securities are seasoned under Rule 144 and confirm that an issuer of digital asset securities is not required to register such digital asset security under Section 12(g) of the Exchange Act. SPBDs should be permitted to audit smart contract protocols, like tZERO's Global Securities Standard, to determine if it is a reliable tool for compliance purposes. If it is, an SPBD should be able to rely on the information provided by a smart contract, without the need for additional manual confirmations, during its documented diligence of a digital asset security, for example, to help ensure requirements under applicable law are met for its digital asset security business.

4. Conclusion

tZERO shares the Commission's interest in advancing and supporting innovation in a compliant manner, which is focused on investor protection. We welcome the step forward the Commission has taken towards a regulatory framework for digital asset securities in issuing the Statement. We ask that the Commission consider broadening the Statement, particularly to permit SPBDs to engage in a traditional securities business and to accept non-security digital assets as a form of funding for brokerage accounts and settlement for digital asset securities transactions and as an asset class in a symbiotic digital product offering. These enhancements would encourage more market participants to join the digital evolution of securities markets and allow regulators and market participants to assess the full breadth of benefits of blockchain technology. We are grateful for this opportunity and welcome the opportunity to engage with the Commission,

self-regulatory organizations and other market participants to advance the adoption of, and regulatory framework for, digital assets.

Respectfully Submitted,



Alan Konevsky
Chief Legal Officer

cc: Saum Noursalehi
Amit Goyal
Vanessa Savino
(tZERO Group, Inc.)

Jonathan E. Johnson III
(Overstock.com, Inc. and Medici Ventures, Inc.)