INVENIAM
AUT VIAM INVENIAM AUT FACIAM

1 (212) 220-6681
One World Trade Center, Suite 8500
New York, NY 10007

39500 High Pointe Blvd., Suite 200
Novi, MI 48375

May 8, 2023

Submitted electronically

Ms. Vanessa Countryman, Secretary
United States Securities and Exchange Commission
100 F Street NE
Washington, DC 20549-1090

RE: Release No. IA-6240; File No. S7-04-23 – Safeguarding Advisory Client Assets

Dear Ms. Countryman:

Inveniam Capital Partners, Inc. ("Inveniam") is pleased to respond to the Securities and Exchange Commission's request for comments on the proposed rule for Safeguarding Advisory Client Assets and welcomes the Commission's attention to the sector.

Inveniam is a technology services provider that enables the information exchanges necessary to support business processes that span multiple enterprises;[1] such business processes are central to the financial services industry.

The following section provides detailed comments on the proposed rule. As will become apparent from many of the comments, when used judiciously, blockchain technologies can promote regulatory compliance and strengthen the safeguarding of advisory client assets that the Commission's proposed rule is trying to achieve. The last section presents our conclusions.

Detailed Comments

A. **Definition of Custody – Comments Applicable to Questions 8, 9, and 17**

> **"The proposal generally would preserve the current rule's definition of 'custody,' and apply when an adviser 'holds, directly or indirectly, client assets, or has any authority to obtain possession of them.' The general principle of this definition is to apply the rule when an adviser has the ability or authority to effect a change in beneficial ownership of a client's**

[1] For those familiar with information technology terminology and service-oriented architectures, Inveniam is like an Enterprise Service Bus operating across companies (Cross-Enterprise Service Bus).

assets." (pp. 30-31)

"Custody includes: (i) Possession of client assets […] (ii) Any arrangement (including, but not limited to a general power of attorney or discretionary authority) under which you are authorized or permitted to withdraw or transfer beneficial ownership of client assets upon your instruction; and (iii) Any capacity (such as general partner of a limited partnership, managing member of a limited liability company or a comparable position for another type of pooled investment vehicle, or trustee of a trust) that gives you or your supervised person legal ownership of or access to client assets." (§ 275.223-1(d)(3))

"The proposed rule would further define 'possession or control' to mean holding assets such that the qualified custodian is required to participate in any change in beneficial ownership of those assets." (p. 21)

We are concerned that this broad definition could classify many technology services providers as custodians or, at the very least, create uncertainty. Modern delivery of convenient financial services to a client's end device (computer, cell phone, etc.) routinely involves a complex system of interconnected computers operated by different technology providers. As information (including instructions to custodians) flows through this web of technologies, various cybersecurity measures (typically involving digital keys of some kind) are used by technology services providers to keep unauthorized activity away and allow only legitimate activity. The keys encrypt transmissions, authorize connectivity between systems, authorize invocation of application programming interfaces (APIs), etc. For the avoidance of doubt, we are *not* referring to a custodian's keys that enable the custodian to perform authorized transactions involving the assets; we are referring to keys protecting the rest of the digital infrastructure.

The technology services providers mentioned above do not have any legal authority to perform any transaction on assets or to instruct anyone to perform any such transaction; the providers act merely as information conduits. However, unauthorized possession of infrastructure keys could enable someone to inject unauthorized information into the digital infrastructure and potentially initiate unauthorized transactions. Thus, possession of cybersecurity keys could potentially be viewed as a "capacity that gives […] access to client assets," so the question arises whether technology services providers could unintentionally be considered as having custody.

If the phrase "ability or authority to effect a change in beneficial ownership of a client's assets" leaves the word "ability" unqualified and allows a broad interpretation of the word to include technical ability, technology services providers could unintentionally be considered as having custody.

In the illustrative examples in the rule's definition of custody, it is unclear whether the adjective

"legal" qualifies only the noun "ownership" (*i.e.*, "legal ownership of, or [any kind of, including technical] access to, client assets") or the adjective "legal" qualifies both the noun "ownership" and the noun "access" (*i.e.*, "legal ownership of, or [legal] access to, client assets"). Under the former interpretation, the technical (even if illegal) access to client assets could be considered custody. Under the latter interpretation, since the technology services provider does not have legal access to assets, the technology services would not meet the definition of custody.

The definition of "possession or control" to mean "that the qualified custodian is required to participate in any change in beneficial ownership of those assets" increases the ambiguity for technology services providers. If "required" is interpreted in the legal sense (*i.e.*, obligated by law, by contract with the client, etc.), then technology services providers would not be included. If "required" is interpreted broadly as "necessary," then technology services providers could potentially be viewed as being in possession or control of assets, since the providers' technical participation is required to effect any change in beneficial ownership of assets.

If the technical access to assets is tantamount to custody, technology services providers will be reluctant to provide cybersecurity measures. Thus, the only entity that could apply security keys is the client (end user) itself. However, placing the onus of security entirely on the end user is dangerous. The end user may be the least sophisticated entity and the one most likely to skip security measures entirely or apply them carelessly, thus making theft of credentials (and consequent theft of assets) more likely. Furthermore, even if an end user applies security measures, intermediate components will be less secure than they would have been otherwise.

As a result of the above, in an effort to protect clients from a relatively small number of insider threats (insider with respect to the technology services providers), an interpretation of "custody" that includes technology services providers may inadvertently be opening the door to a much larger number of potential threats, including insiders and outsiders. The result would be antithetical to the Commission's own policy goals.

We recommend that the Commission clarify (or interpret) the definition and the examples of custody to encompass only the legal authority or the legal capacity to access assets and to explicitly exclude the technical capacity associated with cybersecurity measures of technology services providers.

B. **Necessary Distinctions between Different Categories of Digital Assets / Crypto Assets – Comments Applicable to Questions 46, 47, 49, 50, 53, 54, 57, 60, 66, 68-71, 127, 128, 132, 156, 160, 161, 178, and 253**

Cryptocurrencies[2] were the first applications on blockchain networks. Early blockchain networks, *e.g.*, Bitcoin, were designed for this single application (cryptocurrencies), just like the public switched telephone network (PSTN) had been designed for a single application (voice communication). Despite the limited scope of the early blockchain networks and cryptocurrency applications, they demonstrated the power of immutable entries created on a distributed ledger. The immutability was so strong[3] that people became willing to trade with completely anonymous and otherwise untrusted counterparties based solely on an absolutely minimal amount of information: a fixed-point number representing the quantity of a cryptocurrency. The mathematics of cryptography and the physics of the underlying computing technologies obviated the need for any other corroborating information.

The rapid adoption of cryptocurrencies demonstrated the capacity of blockchain technologies to represent, distribute, and exchange assets. This demonstration was performed in the context of assets with the simplest possible representation that minimized the need for information exchange between the parties involved. If the immutability offered by blockchain technology can generate such efficiencies for assets requiring minimal amounts of information, one can only imagine the efficiencies that blockchain can generate for more complex assets that require market participants to exchange much larger amounts of information for various purposes (*e.g.*, asset description, performance, valuation, regulatory compliance, asset ownership). If Bitcoin was analogous to the single-purpose public switched telephone network, newer blockchain infrastructure is analogous to the Internet, which can carry many types of traffic (*e.g.*, data, voice, still images, video).

The efficiencies mentioned above can be achieved using data provenance technologies that anchor data to the blockchain[4] to demonstrate data immutability and facilitate the detection of any changes in the data. These technologies enable the efficient exchange of trustworthy

[2] For clarity, our discussion of cryptocurrencies focuses solely on their *technical* characteristics in relation to blockchain networks. We are not considering any *legal* aspects of cryptocurrencies such as legitimacy of uses, asset classification, applicable regulations, etc.

[3] It should be noted that cybersecurity attacks on blockchain systems have been primarily on ancillary infrastructure (key storage applications, bridges, etc.) rather than on the core blockchain algorithms.

[4] Data anchoring is a process by which a practically irreversible computation (*e.g.*, calculation of a SHA-256 hash) is performed on some data and the result (typically much smaller in size than the original data) is recorded on the blockchain. The data itself need not be recorded on the blockchain or even disclosed. If one is subsequently presented with a purported copy of the original data, one can derive the hash of the new copy, compare it with the hash recorded on the blockchain, and if the two hashes match, conclude that the new copy is identical to the original one that had been anchored to the blockchain.

information between different parties that participate in the financial markets. This information exchange will in turn enable the representation of assets (tokenized securities) on the blockchain and the more efficient distribution and trading of these assets. We believe that this market transformation will begin with private assets (privately issued securities), which stand to gain the most from the improvements in transparency, efficiency, compliance, and liquidity that this technical approach can bring. We also believe that this transformation will assuage many of the concerns that the Commission expresses about privately offered securities in the proposed ruling.

Footnote 25 on page 16 states that **"[t]he term 'digital asset' refers to an asset that is issued and/or transferred using distributed ledger or blockchain technology, including, but not limited to, so-called 'virtual currencies,' 'coins,' and 'tokens.' … A digital asset may or may not meet the definition of a 'security' under the Federal securities laws. […] To the extent digital assets rely on cryptographic protocols, these types of assets also are commonly referred to as 'crypto assets.'"**

The grouping of all digital assets into a single category regardless of the asset type and the technology used to represent it creates conflation that may lead to incorrect conclusions. We suggest that a more granular classification scheme may serve both the policy goals of the Commission and the needs of the industry in a much better way.

There is a fundamental distinction between bearer instruments and non-bearer instruments. Virtual currencies or cryptocurrencies are bearer instruments, whereas tokenized securities are non-bearer instruments. An additional distinction is between coins that are native to a blockchain network and tokens that are created using a digital computational application or smart contract on a blockchain; smart contracts have the programmatic flexibility to address many of the concerns raised by the Commission.

Page 17 states that **"this [blockchain] technology generally requires the use of public and private cryptographic key pairings, resulting in the inability to restore or recover many crypto assets in the event the keys are lost, forgotten, misappropriated, or destroyed. By design, DLT finality often makes it difficult or impossible to reverse erroneous or fraudulent crypto asset transactions, whereas processes and protocols exist to reverse erroneous or fraudulent transactions with respect to more traditional assets. These specific characteristics could leave advisory clients without meaningful recourse to reverse erroneous or fraudulent transactions, recover or replace lost crypto assets, or correct errors that result from their adviser having custody of these assets."** There is a similar statement on page 77: **"the design of blockchains and other distributed ledgers that require irreversibility of crypto asset transactions (without the consent of all parties to reverse), and the bearer nature of private keys make it challenging to recover assets that have been lost or stolen or to reverse benign trading errors**

even if an owner of a crypto asset wallet may be identified."

Blockchain does rely on public and private cryptographic keys; this is a well-understood technology, and it is routinely used in countless applications. For example, the issuance of the digital certificates that identify most websites[5] relies on a digital signature by the private key of the certifying authority. There are well-developed techniques for safeguarding private keys, and many custodians of digital assets have already adopted such techniques. Furthermore, there are techniques that can mathematically partition a key into multiple shares (computational fragments) in such a way that no single share suffices but all shares together can create a valid key or signature. It is also possible to arrange for a subset of the shares to create a valid signature, so that even if any single share is lost, the remaining shares can still be combined to provide a valid signature.[6] Finally, we note that, for digital bearer instruments, the situation is conceptually not much different from the situation with physical bearer instruments. For example, lost or stolen cash is very difficult to recover, and hidden cash can be forgotten – we periodically read in the press about cash found hidden behind a wall during a home remodeling by a new owner or cash found in the cushions of a second-hand couch. Admittedly, loss or misplacement of digital keys is probably easier than loss or misplacement of physical objects.

The concerns examined above in relation to cryptographic keys apply primarily to digital bearer instruments. As mentioned at the beginning of this comment, early blockchains were focused on a single application – cryptocurrencies, which are bearer instruments. Blockchain technology has evolved to allow the creation of tokens that can be used to represent any kind of asset, including securities, which are non-bearer instruments. These tokens are typically implemented using smart contracts – programming code that is recorded on and executed by the blockchain. The programmability of the smart contracts affords multiple benefits that neutralize the concerns of the Commission:

- The smart contracts that implement the digital security tokens can be programmed to allow transfers only to approved ("white-listed") blockchain wallet addresses[7] (asset

[5] For example, as of the time of this writing, the certificate of the Commission's own website https://www.sec.gov/ is issued (signed) by GeoTrust, a brand of DigiCert Inc. The current certificate was issued on 5/29/2022 and expires on 5/31/2023.

[6] These techniques are the subject of the fields of multi-party computation (MPC) and threshold cryptography. If there are *N* participants in total, a *(t,N)*-threshold scheme enables *t* of the shares to decrypt a ciphertext or create a valid signature.

[7] It is unfortunate that the term "wallet" is overloaded in the blockchain literature. Sometimes the term is used to denote an asset holding address on the blockchain ("wallet address") with an associated private key, and sometimes it is used to denote a user application ("wallet application") like MetaMask that manages a user's private keys and interactions with the blockchain. In this context, we use the term with the first meaning; to avoid confusion, we subsequently use the term "blockchain account" instead. The Commission's document is not immune to this confusion. For example, the references to "wallets" on pages 66-67 appear to be in the context of

holding addresses on the blockchain that serve as accounts) whose owners are traceable and have passed KYC/AML/CFT, investor status (*e.g.*, accredited investor, qualified purchaser) and other checks. Thus, misappropriation of a tokenized security would be very difficult in the first place.

- The smart contracts that implement the digital security tokens routinely include features that allow an appropriately authorized party (*e.g.*, security issuer or transfer agent) to "burn" lost or stolen tokens and "remint" (reissue) those tokens to their legitimate owner. Thus, for non-bearer instruments like tokenized securities any error or malfeasance can be rectified. It should be noted that all actions, including those of the authorized party, are recorded on the blockchain, so they are visible, immutable, and auditable.

The statement that "[b]y design, DLT finality often makes it difficult or impossible to reverse erroneous or fraudulent crypto asset transactions" is accurate with respect to early, single-purpose blockchains (*e.g.*, Bitcoin) that were designed to accommodate a single type of asset – a cryptocurrency. Given that the accounts (wallet addresses) on these early blockchains were intended to hold only a bearer instrument (the cryptocurrency), the ability to reverse transactions was superfluous and undesirable, since it would have undermined the users' trust. Once a transaction was signed by a blockchain account's private key, the transaction could only be reversed if there was agreement among a majority of the blockchain miners, which majority forms the trust basis for a blockchain network. Keys were always associated with a blockchain account (wallet address) and there was no "appellate" entity between an account and the pool of miners.

Blockchain technology has evolved. With smart contracts, one can create such an appellate entity having authority to reverse transactions. Such authority may be vested in a single entity (*i.e.*, a single signature suffices for reversal), or it may require consensus among a designated group of entities (*i.e.*, multi-signature approval is required). The burning and reminting of tokenized securities discussed earlier is an example of such authority. Thus, it is possible to reverse erroneous or fraudulent crypto asset transactions, recover or replace lost crypto assets, or correct errors, particularly when the transactions involve non-bearer instruments. The reversals are also recorded on the blockchain to ensure immutability, traceability, and auditability.

The latest blockchain technologies make such reversal arrangements even easier, while preserving the immutability and trust of earlier blockchains. There are new blockchain platforms

"wallet addresses." In contrast, the references to hot and cold "wallets" on page 85 appear to be in the context of "wallet applications."

that, unlike early blockchains, treat public keys as first-class objects: public keys (documenting signature authority) can be recorded on the blockchain, revoked, changed, etc. Furthermore, these new blockchain platforms enable the creation of arbitrarily complex hierarchies of keys or key combinations that can effect a transaction for a blockchain account or set of accounts.[8] Such key hierarchies can represent the authority hierarchies (including legal powers) that exist in real life. Thus, the capability to reverse transactions can be specified in a declarative fashion, obviating the need to write smart contract code, an activity which might have been prone to programming error. Key hierarchy capabilities also facilitate the replacement of lost keys and the revocation of compromised keys.

In light of the above, we urge the Commission to reconsider its position of aggregating all digital assets into a single category. At the very least, tokenized securities should be placed into a separate category. For such non-bearer instruments, modern blockchain technologies can not only overcome the concerns that the Commission has expressed, but can also offer higher levels of transparency, security of custody, compliance, and oversight than the existing processes and protocols associated with the traditional representation of these assets. The benefits brought by blockchain are particularly pronounced in the case of privately issued securities, which are of concern to the Commission.

Notably, other financial services companies and highly reputable consulting firms, including Citigroup Inc.,[9] BlackRock Inc.,[10] Goldman Sachs,[11] Bain & Company,[12] and McKinsey & Company,[13] are among many predicting significant growth in tokenized assets.

[8] Ethereum, a popular Layer 1 blockchain, offers similar capabilities through account abstraction and smart contract accounts rather than explicit signature hierarchies.

[9] *See* "Money, Tokens, and Games: Blockchain's Next Billion Users and Trillions in Value" in Citi GPS: Global Perspectives & Solutions, March 2023, *available at* https://icg.citi.com/icghome/what-we-think/citigps/insights/money-tokens-and-games.

[10] *See* statements made by Larry Fink, CEO of BlackRock, Inc. at the New York Times DealBook Summit event in New York City on November 30, 2022, *available at* https://www.nytimes.com/events/dealbook-summit/sessions/esg-investing-the-promise-the-backlash-and-the-way-forward.

[11] *See* op-ed in the Wall Street Journal on December 6, 2022 titled "Blockchain Is Much More Than Crypto" by David Solomon, CEO of Goldman Sachs, *available at* https://www.wsj.com/articles/blockchain-is-much-more-than-crypto-david-solomon-goldman-sachs-smart-contracts-11670345993.

[12] *See* "Web3 Remains Highly Relevant for Private Equity" in Global Private Equity Report 2023 (pp. 39-54) by Bain & Company, *available at* https://www.bain.com/globalassets/noindex/2023/bain_report_global-private-equity-report-2023.pdf.

[13] *See* Anutosh Banerjee, Robert Byrne, Ian De Bode, and Matt Higginson "Web3 beyond the hype" *available at* https://www.mckinsey.com/industries/financial-services/our-insights/web3-beyond-the-hype.

C. **Ownership, Possession, and Authority for Tokenized Securities – Comments Applicable to Questions 39, 46, 47, 49, 50, 53, 54, 57, 60, 66, 68-71, 82, 127, 128, 132, 133, 156, 160, 161 and 178**

For centuries, ownership rights have been represented by paper certificates or entries in paper-based accounting books. Business processes have relied on the exchange or copying of paper documents. Accounts are maintained (*e.g.*, by a custodian) for a person (in the legal sense), and assets or liabilities are held in an account, hence associated with a person. With respect to data governance, each party maintains its own accounts / books. Agreement between parties is reached through bilateral reconciliation of their entries (*e.g.*, matching a buyer's account payable entry to a seller's account receivable entry in their corresponding accounting books).

Digitization has largely replaced paper with electronic copies (including dematerialized securities), but it has not changed the underlying model of asset representation or the associated business processes. Business processes still rely on the exchange or copying of (digital) documents. Digital accounts are still maintained for a person, and digital representations of assets or liabilities are still held in an account (in electronic book-entry form) and associated with that person. Each party still maintains its own (digital) accounts / books. Agreement between parties is still reached through bilateral reconciliation of their electronic book entries, which reconciliation is now facilitated by digital data transmissions. The preservation of the traditional business processes is attributable to several factors, including, *inter alia*, operational considerations, established legal frameworks, and the practical need for coexistence of paper-based processes and digital processes.

Here are some noteworthy aspects of the traditional world:

- Possession of an asset is typically proven through possession of a document (paper or electronic) that represents the asset. A change in possession of the asset is typically effected through the transfer of the corresponding document, hence the paper/data transfers mentioned above.
- Possession of an asset is typically necessary to effect a transaction.
- To receive financial services, an asset owner must typically give possession of the asset to a financial services provider, so that the provider can perform transactions. Thus, the assets go to the financial services provider, and it is very common for owners to say, "I moved my assets from [financial services provider] X to [financial services provider] Y."
- When the assets go to the financial services provider, possession is divorced from ownership.

- The traditional world is typically organized into a hierarchy with financial services providers (agents) in the upper layer and asset owners (principals) in the lower layer: to locate a particular asset, one must first go to the financial services provider holding the asset (for securities, typically in street name or nominee name) and then locate the owner's account within the financial services provider's electronic book entries. Thus, the recordation of ownership is "in the shadow of" possession. The asset owner relies critically on somebody else (an agent) to properly preserve the recordation of the principal's beneficial ownership of the assets.

This principal-agent problem may enable abuse in the traditional world when a financial services provider (*e.g.*, an adviser also acting as a custodian) has both the authority to initiate transactions and the ability to effect those transactions. Since ownership is recorded in the shadow of possession, the provider could change the beneficial ownership of an asset unbeknownst to or against the will of the client who is the legitimate owner of the asset.

The above scenario is exactly what the custody regulations[14] try to prevent. In the words of the Commission, **"the proposal maintains the core purpose of protecting client assets from loss, misuse, theft, or misappropriation by, and the insolvency or financial reverses of, the adviser"** (page 19). In the traditional world, where ownership may be divorced from possession and ownership may be represented by an entry on the books of a financial services provider, the Commission has rightly tried to ensure client protection through controls (authorizations, account statements, reports, written agreements, audits, surprise examinations, etc.) that force bilateral reconciliation of information between multiple parties (clients, advisers, custodians, auditors, *et al.*). These cross-checks bring the ownership to light (*i.e.*, "pull" the recorded ownership "out of the shadow" of possession) and reduce the possibility for anyone to unilaterally effect an unnoticed change in the beneficial ownership of a client's assets, thus reducing the probability of abuse.

Using blockchain, assets can be represented with tokens or similar data objects (*e.g.*, coins). The blockchain can play the same role that central security depositories play in the immobilization and dematerialization of securities: when tokens change hands, the change is recorded immutably on the blockchain.

It is possible, and currently common, to use blockchain technology within the traditional framework. In this case, possession of the private keys for a blockchain wallet address (blockchain account) implies possession of the corresponding assets and the authority to execute transactions involving those assets. However, the holder of the private keys may or may

[14] For expositional purposes, in this comment we focus only on the Commission's policy goals with respect to custody and ignore the details of the custody rule and the proposed safeguarding rule, the exceptions to these rules, and the differences between these rules.

not be the beneficial owner of the assets. For example, the owner of tokenized assets may send the assets to a wallet address (blockchain account) controlled by a financial services provider (*e.g.*, a custodian). The financial services provider takes custody of the tokenized assets, and the beneficial owner of the assets is then recorded in the books of the financial services provider, so the principal-agent problem mentioned above and the concomitant risks to the asset (loss, misuse, theft, or misappropriation by, and the insolvency or financial reverses of, the adviser) are still present. The assets still go to the financial services provider. The recordation of ownership is still in the shadow of possession.

When the full capabilities of newer blockchain technology are used, blockchain can introduce a disruptive change that completely inverts the previous model: blockchain accounts (blockchain wallet addresses that hold assets) can represent ownership, not possession. Thus, instead of ownership being recorded in the books of a financial services provider that has possession of the assets, ownership is recorded directly with immutable entries on a blockchain. Assets move from one blockchain account to another only when beneficial ownership changes.

This seemingly small change ushers in a new model of the world:

- Ownership of an asset is recorded directly on the blockchain and is visible to everybody with access to the blockchain.[15] As a result, any change in ownership is also immediately visible to everybody with access to the blockchain, including the owner. There is no longer a need to pull ownership out of the shadow of possession.
- Any transaction performed on the assets is immutably recorded, immediately visible to / detectable by anyone with access to the blockchain (including the asset owner), traceable, and auditable. If desired, the detection can be performed automatically by software and the owner can be notified. The owner does not have to worry about the validity of invisible entries made in the books of other parties. Abuse cannot go undetected.
- Authority to perform or approve transactions can be granted by an asset owner to an agent (*e.g.*, an adviser or a custodian) using one of the blockchain authorization mechanisms (signature hierarchies, account abstraction, etc.) described earlier.[16] The authority can be one-time or standing. The owner does not have to give possession of the assets to receive financial services.

[15] Note that, for privacy reasons, the identity of the owner need not be visible on the blockchain. The identity of the owner may be known to (and possibly recorded immutably by) the entity that performed the screening of the blockchain wallet address (account) that is holding the asset on the blockchain. This identity can be revealed when the need arises (*e.g.*, in legal proceedings). *See supra* comment (B); *see also* comment (X) *infra*.
[16] *See supra* comment (B).

- Any authority granted can be recorded on the blockchain in an immutable, traceable, and auditable way, thus providing full accountability. Any exercise of such authority is also recorded on the blockchain and is traceable and auditable.
- The assets of a client are readily segregated from those of other clients and those of the service provider(s) (*e.g.*, adviser, custodian).
- Audits of assets and activity can be performed directly, in an automated fashion (*i.e.*, using software), and comprehensively (*i.e.*, without the need for sampling or applying a threshold of materiality).
- Account statements of holdings and transactions can be created by reviewing the blockchain. This task can be automated with a software tool and performed by the asset owner or by a third party.

Various parties can maintain their own records, but the entry on the blockchain is the "golden copy" of the data that represents the widely accepted truth. Because of the distributed data governance of blockchain, no single party has control of the golden copy. Instead of parties reconciling their entries bilaterally, each party can reconcile its own entries with the entries on the blockchain in a hub-and-spoke arrangement, where the blockchain entry is the hub and the entries of individual parties are the spokes.[17] Business processes can be implemented through a series of operations that individual parties perform on the blockchain rather than a series of document exchanges between parties.

The use of the full capabilities of blockchain in this way turns the traditional model of the world upside down:

- Asset owners are in the upper layer of the hierarchy and service providers are in the lower layer. Asset ownership is recorded directly on the blockchain. One first locates the asset and then looks "inside" the asset to see if the owner has granted any authorizations (*e.g.*, to service providers like advisers or custodians).
- Instead of the assets going to the services provider, the services provider comes to the assets. The owner does not need to "move" the assets to switch providers; the owner can simply revoke the authorizations previously granted to the old provider and grant authorizations to the new provider.

In addition to resolving the principal-agent problem outlined above, this model of the world offers many additional benefits. There is no longer a need to divorce possession from

[17] When there are *N* parties that need to reconcile their entries bilaterally, each party needs to perform a reconciliation with each of the *N-1* other parties; thus, the overall process has complexity $O(N^2)$. In contrast, with a hub-and-spoke arrangement, each party only needs to reconcile its entries once, with the golden copy on the blockchain, thus resulting in a lower *O(N)* complexity for the overall process.

ownership. For securities, the owner can effectively receive the combined benefits of street name (nominee name) registration and direct registration. Furthermore, it will be possible for many of the custody tasks to be self-performed by the asset owner, particularly as software tools advance and user interfaces become simpler and more intuitive.[18] Therefore, we anticipate that the role of custodians in tokenized securities will gradually diminish in favor of self-custody by the owners.

The full ramifications for tokenized securities of the changes introduced by blockchain will be very profound and are discussed in subsequent comments. We encourage the Commission to consider these ramifications.

D. **One-Way Transfer vs. One-for-One Exchange of Tokenized Private Assets – Comments Applicable to Questions 15, 49, 53, 54, 57, 60, 127, 128, 132, and 239**

The Commission repeatedly highlights the implicit protections offered by one-for-one exchange of assets. For example:

- On page 9, the Commission mentions that the expansion of the concept of adviser custody in the 2003 Adopting Release did not include authorized trading, **"stating that clients' custodians are generally under instructions to transfer funds or securities out of a client's account only upon a corresponding transfer of securities or funds into the account."**
- The same statement is repeated on page 13, with the additional comment that **"[a]t the time, the Commission's view was that such an arrangement would minimize the risk that an adviser could withdraw or misappropriate the funds or securities in its client's custodial account."**
- Footnote 15 on page 12 quotes expert testimony that **"the custodian requirement largely removes the ability of an investment adviser to pay the proceeds invested by new investors to old investors. The custodian will take the instructions to buy or sell securities, but not to remit the proceeds of sales to the adviser or to others (except in return for share redemptions by investors). At a stroke, this requirement eliminates the ability of the manager to 'recycle' funds from new to old investors."**
- On page 13, the Commission notes that **"[d]iscretionary trading practices today, however, do not necessarily involve a one-for-one exchange of assets under a custodian's oversight."** This observation led the Commission to explicitly include

[18] The situation will be analogous to people typesetting their own documents using tools like Microsoft Word instead of relying on a typesetter as was the case before the development of such tools.

"discretionary authority" within the definition of custody in the proposed rule. However, as the Commission notes on page 33, it does **"continue to believe more limited risk of loss exists when a qualified custodian participates in transactions,"** so it is **"also proposing a limited exception to the surprise examination requirement of the rule."** This exception applies to cases where an adviser's discretionary authority **"is limited to instructing the client's qualified custodian to transact in assets that settle only on a delivery versus payment ('DVP') basis."**

Privately issued securities appear to be of particular concern to the Commission.

- On page 13, the Commission presents a scenario where **"an adviser may instruct an issuer or a transfer agent that recorded ownership of a client's privately offered security to redeem the client's interest and direct the proceeds to a particular account. Because there is no qualified custodian involved in such a transaction, a client's ability to monitor its investments for suspicious activity is limited (*e.g.*, a qualified custodian would not attest to this transaction on the account statements it provides), and a surprise examination or an audit may not discover any misappropriation until the assets are gone. Moreover, if the security is not included in the sample over which an accountant performs its procedures during a surprise examination or if the client's holdings of the security do not meet the materiality threshold for a financial statement audit, misappropriation may go undetected for an indeterminate amount of time."**
- On page 33, the Commission presents a similar scenario of a one-way transfer where an adviser **"could use its discretionary authority over a client's assets to instruct an issuer's transfer agent or administrator (*e.g.*, the administrator for a loan syndicate) to sell its client's interest and to direct the cash proceeds of the sale to an account that the adviser owns and controls, thereby depriving the client of ownership, unbeknownst to the client or its qualified custodian."**
- The Commission's concerns are heightened by the fact that a **"growing number of assets are not receiving custodial protections as a result of certain of the current rule's exceptions from the requirement to maintain assets with a qualified custodian, particularly the exception for privately offered securities"** (p. 14) and the fact that **"the volume of privately offered securities has vastly expanded with the expansion of private capital"** (p. 15), as evidenced in part by the growth in private capital assets under management shown in the report referenced in footnote 19 on page 14.[19]

[19] The Commission cites additional data on the growth of private assets in footnote 213 on p. 128.

We agree with the Commission's view that **"DVP transactions reduce the risk that the seller of an asset could deliver the asset but not receive payment or that the buyer of an asset could make payment but not receive delivery of the asset"** (p. 34) and with the Commission's assumption that a one-way transfer of assets from an account at a qualified custodian is a riskier form of discretionary authority than DVP transactions (question 239).

Data provenance technologies (which anchor data on blockchain) in combination with advances in blockchain networks are enabling the tokenization of securities, including privately issued securities, whose volume is rapidly growing. This tokenization will in turn provide several benefits that promote the Commission's goals:

- Transparency in ownership recordation. The ease of tokenizing securities (afforded by technical evolution) will eliminate any excuse for **"privately offered securities where the only evidence of the client's ownership was recorded on the issuer's books"** (p. 9). Ownership recordation will be easy and transparent on blockchain.
- Transparency in transaction recordation. All transactions will be recorded on the blockchain and will be visible to those with access to the blockchain, including the beneficial owner. Thus, any unauthorized change in beneficial ownership will be immediately detectable.
- Easier custody by qualified custodians. The tokenization will make it easier for qualified custodians to hold privately issued securities.
- Reduction in one-way transfers. The one-way transfers of assets like the redemption scenarios mentioned on pages 13 and 33 will be reduced if not completely eliminated. The purchase or sale of the securities will take place through an exchange of assets (*e.g.*, DVP), with both sides of the trade recorded immutably on blockchain. This will lead to a corresponding reduction in or elimination of opportunities for abuse by an adviser.
- More effective surprise examinations and audits. The recordation of transactions on blockchain makes surprise examinations and audits easier and more efficient since the transactions will be directly observable by the auditors. The audits may also become more comprehensive, since the digital automation of such audits may obviate the need for sampling, which was one of the concerns articulated by the Commission.

The above will reduce the probability that any abuse could go undetected, let alone for a significant amount of time. As clients realize the benefits offered by tokenized securities and adoption of tokenization increases, uncertificated issues recorded only on an issuer's books will become automatically suspect, will be subjected to increased scrutiny, and may suffer a price discount. This competitive market pressure will force private security issuers to switch to tokenized recordation and DVP trading of their securities.

We anticipate that the dissemination of trustworthy information enabled by blockchain-based technology platforms and the transparency in security ownership recordation and DVP trading enabled by subsequent asset tokenization are likely to lead to the reduction and potential extinction of the scenarios that are of concern to the Commission. Thus, these technologies align with the Commission's policy goals and may eventually obviate the need for an exception for privately offered securities in the rule.

E. **Response to Question 8 – Definition of Custody & Suggested Changes**

We agree that the current definition of custody works well for advisers. We urge the Commission to refine the definition of custody to (i) qualify words like "capacity" and "ability" appropriately to ensure the proper context in which these words are interpreted and avoid inadvertently classifying technology services providers as custodians; or (ii) to adopt an exception from the definition of custody for technology services providers. As mentioned in an earlier comment,[20] subjecting technology services providers to custody regulations could have side effects antithetical to the policy goals of the Commission.

F. **Response to Question 9 – Definition of Custody & Adviser's Discretionary Authority**

We agree that the rule should apply when an adviser has discretionary authority over client assets, as proposed. To avoid confusion in the market, we urge the Commission to explicitly exclude from the rule (or to interpret the rule to exclude) the mere conveyance by the adviser to the custodian of authorizing instructions that the client issues to the custodian. Such instructions would not constitute discretionary authority. By having the ability to electronically convey the client's (explicitly) authorized instructions to the custodian, an adviser may be able to simplify the client's on-line experience and reduce the onus on the client, thus making the transmission easier, more secure, and less prone to error. These benefits promote the Commission's policy goal of protecting advisory clients' assets.

G. **Response to Question 15 – Temporary Processing of Assets Avoided by Tokenization**

The Commission states that **"[w]e understand that for certain private fund advisers and trustees it is difficult to avoid temporarily possessing client checks and physical assets because there may not be an independent representative to arrange the movement of such assets into a qualified custodian."**

[20] *See supra* comment (A).

We note that the tokenization of assets (including private assets) and the atomic settlement of trades involving these assets using blockchain[21] will avoid temporary custody of assets by advisers and trustees in such situations and will thus eliminate many of the special cases that are of concern to the Commission.

H. **Response to Question 17 – Exception Needed to Avoid Inadvertent Custody for Technology Services Providers**

As noted in earlier comments,[22] we believe that there should be an exception or interpretation that third-party technology services do not constitute custody.

I. **Response to Question 39 – Transfer Agents as Qualified Custodians for Tokenized Assets**

As noted in an earlier comment,[23] we anticipate that the role of custodians in tokenized securities will gradually diminish in favor of self-custody by the owners. The remaining tasks could be performed by a transfer agent, who could be involved in the deployment and operation of the smart contracts that create and transfer the security tokens. The anticipated rapid adoption of tokenized securities will probably necessitate a revision to the safeguarding rule in the future, as clearer market trends and needs emerge. In the meantime, we suggest that allowing transfer agents to act as qualified custodians for tokenized securities may facilitate the deployment of technological advancements and the gradual development of the market in a compliant way.

J. **Response to Question 46 – Possession or Control for Crypto Assets**

As the Commission notes on p. 66, **"it is possible for a custodian to implement processes that seek to create exclusive possession or control of crypto assets (*e.g.*, private key creation, maintenance, etc.)."** If the custodian has created the private key for the account, nobody else has the key and the custodian can apply well-understood technical approaches to safeguard the key. This simple approach is applicable to all kinds of assets (bearer and non-bearer) and all technical generations of blockchains. For older blockchains, this approach may require the transfer of assets from a client's wallet address (blockchain account) to a custodian's wallet address (blockchain account), since this is the only way to ensure that the custodian is the only entity with access to the private key of the wallet address (blockchain account).

[21] *See infra* comment (N); *see also* comment (D) *supra*.
[22] *See supra* comments (A), (E) and (F).
[23] *See supra* comment (C).

The Commission is **"mindful of crypto asset custody models in which an advisory client and a qualified custodian might simultaneously hold copies of the advisory client's private key material to access the associated wallet with the client's crypto assets, and thus both have authority to change beneficial ownership of those assets"** (p. 66). This is a valid concern for earlier generations of blockchain technology where there was only one key associated with each account (wallet address). Under these circumstances, it is unlikely that a custodian would accept custodial liability, since the custodian could find itself liable for actions of others, which actions are beyond the custodian's control.

As mentioned in earlier comments,[24] newer blockchain technologies (key books / key pages, account abstraction, smart contract accounts, etc.) allow complex key hierarchies, including the possibility of having two (or more) separate keys for the same blockchain account (wallet address). The transactions recorded on the blockchain include the signatures of the originators, so there is no ambiguity about who approved (*i.e.*, which key signed) a particular transaction even when two entities (*e.g.*, owner and custodian) share control of the blockchain account (wallet address). The asset owner and the custodian may share control of the account by each having their own separate (private) key and the asset owner recording on the blockchain that the custodian's key can also sign transactions involving the owner's account (wallet address). Alternatively, the owner may delegate authority entirely to the custodian by specifying that only the custodian's key can sign transactions involving the owner's account. Such delegation can be revoked when the asset owner chooses to do so.

With modern blockchain technology, authorized signatures can be added to or removed from accounts the same way that tokens can be added to or removed from an account. The transactions granting and revoking account authority to a party (*e.g.*, a custodian) are also recorded on the blockchain, so there is full accountability for all actions. Typically, the right (authority) to grant or revoke signature authority for an account can be exercised only by the account owner, but even this authority (to grant/revoke signatures) can be tailored to suit any situation that may arise.[25] Note that the granting of signature authority to an account does not require the revelation of any private key. The grantor need only record on the blockchain the

[24] *See supra* comment (B).

[25] For example, an account owner who is concerned about safeguarding its own private key and who prefers to rely on the professional-grade security measures employed by a custodian may choose to delegate account authority entirely to the custodian; the owner's key would be unauthorized to sign transactions for the account. Even so, the owner may be concerned that someone may steal the owner's private key, execute a transaction re-authorizing the owner's key to execute transactions on the account, and then execute a fraudulent asset transfer with the stolen and reauthorized private key. To protect against this scenario, the account owner may specify (on the blockchain) that the custodian needs to sign any transaction re-authorizing the owner's key and request (privately) that the custodian authenticate the owner (*e.g.*, with some off-chain multi-factor authentication scheme) before signing the re-authorization transaction on the blockchain.

public key of the grantee. This powerful concept of granting signature authority for an account enables the new model of the world and the associated benefits mentioned earlier,[26] where the ownership is recorded on the blockchain and there is no need to transfer assets to a custodian's blockchain account (wallet address).

In the new model of the world, the arrangement where an asset owner can execute a transaction in addition to the custodian is tantamount to an arrangement in the old model of the world where the custodian can transfer the assets temporarily to the owner's wallet address, the owner can execute a transaction with the owner's private key, and then the owner can send the remaining assets back to the custodian's wallet address. The new model just makes this sequence of operations much simpler.

Given the accountability enabled by the newer blockchain platforms, we do not see any reason why an asset owner and a custodian should not share control of an account. We believe that whether the custodian and the owner have joint control of an account is a matter to be decided between them. If the two parties decide that the custodian should have exclusive control of the account, the custodian's key should be the only one with authorization to execute transactions on the account; this authorization will be recorded on the blockchain, and the custodian will be able to prove that it has exclusive control of the account and the assets. In any case, we believe that the practice of recording authority on the blockchain is the best way to demonstrate who has control of an asset.

In light of the above, we recommend that the Commission revise the definition of custody to account for the fact that a change in beneficial ownership requires participation by the custodian *or* the asset owner.

K. **Response to Question 47 – Participation in Change of Beneficial Ownership for Crypto Assets by Custodian**

Any entity (including a custodian) with signing authority for a blockchain account can participate in a change of beneficial ownership for an asset held in the account by signing a transaction with the private key corresponding to the entity. All transactions are recorded on the blockchain, so the change in beneficial ownership is visible to the owner. Since transactions are signed with the private key of the entity submitting the transaction, the recordation includes proof of the transaction's signer and creates full accountability and auditability. As noted previously,[27] modern blockchains enable signature arrangements that can mirror the complex authority

[26] *See supra* comment (C).
[27] *See supra* comment (J); *see also* comments (B) and (C) *supra*.

arrangements encountered in real life.

L. **Response to Question 49 – Pre-Funded Trades of Crypto Assets & Custody by Trading Platform**

The Commission's concern about pre-funded trades and potential custody of the associated assets by the trading platform **"from the time the crypto asset security was moved to the trading platform through the settlement of the trade"** (p. 68) applies to cases where possession of the asset by a financial services provider (in this case a trading platform) is necessary for the performance of those services.

As noted earlier,[28] an asset and its ownership can be recorded explicitly on the blockchain, and there is no need to divorce possession from ownership to deliver financial services. The services go to the asset, not the other way round. Thus, the Commission's concerns regarding pre-funded trades can be addressed through atomic settlement[29] on the blockchain. The atomic settlement will obviate the need for the trading platform to take temporary possession or assume temporary custody of the traded assets. While it might also be possible to achieve a similar effect through the advanced account authority mechanisms discussed earlier,[30] we view atomic settlement as the most elegant approach and recommend that the rules reflect this.

M. **Response to Question 50 – Sharing of Private Keys**

We believe that sharing a private key between parties is undesirable because the sharing would obfuscate accountability for transactions effectuated with this key. Thus, we recommend that key sharing arrangements in older blockchain technologies that allow only a single key under the old model of the world (where the blockchain reflects possession rather than ownership)[31] should not be allowed. However, as noted in detail earlier,[32] newer blockchain technologies allow the use of separate keys on the same account, which arrangement preserves accountability. Thus, it is easy for an owner and a custodian to share control of an account with full accountability for the transactions originated by each and without sharing any keys.

[28] *See supra* comment (C).
[29] *See infra* comment (N); *see also* comment (D) *supra*.
[30] *See supra* comments (J) and (B).
[31] *See supra* comment (C).
[32] *See supra* comment (J); *see also* comment (B) *supra*.

N. **Response to Question 53 – Atomic Settlement & Its Vast Implications**

In the context of atomic settlement of crypto asset trades, the Commission asks, **"Is this is [*sic*] commonly understood and used term? Does it mean that both legs of the trade settle simultaneously (similar to a delivery vs. payment transaction), or that the trade settles instantly, or both? Which aspect of crypto asset settlement (simultaneous settlement or instantaneous settlement) is preferable from an investor protection standpoint?"**

There is a well-developed body of knowledge around computer transactions and their properties in the field of computer science. Some of the pioneering work in this field was performed by Jim Gray, a famous computer scientist,[33] in the 1970s.

Atomicity is considered one of the defining properties[34] of computer transactions: either all changes made by a transaction take effect or none does. For example, in the case of a DVP transaction involving a tokenized security, the token representing the security must move from the seller's wallet address (blockchain account) to the buyer's wallet address (blockchain account) and the funds (*e.g.*, cryptocurrencies, stablecoins, etc.) need to move in the opposite direction. The DVP transaction consists of two blockchain transfers: the transfer of the token and the transfer of the funds. Atomicity mandates that either both transfers complete or neither does.

Transaction atomicity can be difficult to achieve, particularly in situations where the actions that constitute a transaction need to be performed by different entities operating asynchronously on different computers. Software crashes, hardware failures, lost network messages, etc. can thwart atomicity. The problem is challenging even when participants are within the same organizational domain and have an incentive to cooperate to achieve atomicity. For example, consider a bank that has two computer systems, one serving accounts for the eastern part of the U.S. and one serving accounts for the western part of the U.S. To perform a funds transfer from a California account to a New York account (when both accounts are with the same bank), the computer serving all western accounts needs to debit the California account and the computer serving all eastern accounts needs to credit the New York account. If one or more network messages are lost, the western computer may perform the debit, but the eastern computer may

[33] In 1998, Jim Gray received the ACM (Association for Computing Machinery) A.M. Turing Award "for seminal contributions to database and transaction processing research and technical leadership in system implementation" (*see* the ACM web page *available at* https://amturing.acm.org/award_winners/gray_3649936.cfm). The Turing Award is widely considered the equivalent of the Nobel prize in computer science.

[34] In computer science literature, computer transactions are often defined as ACID: atomic, consistent, isolated, and durable. For a quick overview of computer transactions and their properties, *see* the ACM web page that highlights Jim Gray's contributions *available at* https://amturing.acm.org/info/gray_3649936.cfm#transactions. For readers interested in learning more, there is a vast technical literature on this subject.

not perform the credit, thus resulting in violation of atomicity and a loss of funds.

There are well-known and long-proven techniques[35] (*e.g.*, two-phase commit) to ensure atomicity when all participants are within the same organizational domain and have an incentive to cooperate. In the above example with two computers from the same bank, one of the computers can act as a coordinator to ensure completion or rejection of both parts of the funds transfer. However, the problem becomes much more difficult when participants span organizational boundaries, since no organization will cede (technical) control of its computers to an external computer managed by another organization, even if the two organizations are trying to cooperate (*e.g.*, two banks trying to effectuate a funds transfer). The situation becomes even worse when the participating parties may not be trusted to cooperate; for example, in an asset exchange, the party that receives the other party's asset first may choose to renege on its obligation in order to keep both assets.

Blockchain is the first widely deployed technology that ensures the following properties:

- Consensus on a single, immutable version of the data
- Platform accessible to and usable by multiple parties without any single party having control of the platform
- Common sense of "time" (at block-level granularity), since all computers eventually agree on the order of accepted blockchain blocks

These properties enable the implementation of atomic transactions on blockchain without any need for trust between the parties. The mathematics of cryptography and the physics of the underlying computing technologies ensure that either all actions of a transaction will complete, or they will all be aborted. Smart contracts or similar blockchain technologies can be used to provide this assurance.

In the DVP example, either both the delivery and the payment will succeed or neither of them will. Atomic settlement can be generalized to transactions of arbitrary complexity involving an arbitrary number of participating parties and an arbitrary number of asset transfers.[36]

The ramifications of atomic settlement are extremely profound. If the blockchain is used as the immutable record of assets, atomic settlement obviates the need for intermediaries like central

[35] *See* J. N. Gray. Notes on data base operating systems. In Operating Systems, pp. 393-481. Springer, 1978. *See also* P. A. Bernstein, V. Hadzilacos, and N. Goodman. Concurrency control and recovery in database systems. Addison-Wesley 1987.

[36] There is also technology that enables the atomic settlement of a transaction even when the actions of the transaction span multiple blockchains.

securities depositories, settlement agents, clearing agents, et al. As mentioned earlier,[37] there is no need for the asset owner to give up possession of the assets in order to receive financial services. For example, atomic settlement can obviate the need for pre-funded trades and the potential custody of the associated assets by the trading platform.[38] From a risk perspective, as mentioned repeatedly by the Commission, a one-for-one exchange of assets, which an atomic settlement is, reduces the opportunities for abuse of an investor's assets.[39]

The Commission asks whether atomic settlement means simultaneous settlement of both legs of a trade, or instant settlement, or both. Neither "simultaneous" nor "instant" describes atomic settlement properly. The most accurate way to describe atomic settlement is that both legs of the transaction settle "indivisibly."[40] When a business transaction (*e.g.*, a trade with two or more legs) commits, the blockchain will *inevitably* reflect all actions of the transaction, *i.e.*, the actions form an "indivisible" group whose members all have the same eventual fate. In this context, "inevitably" means that the outcome is guaranteed through cryptographic means by the pre-programmed logic of the blockchain.

In practice, atomicity typically means:

- The various parties to a business transaction can operate independently and without trust in each other until certain conditions are satisfied and a commit point – effectively a point of no return – is reached.
- From the commit point on, all actions, *e.g.*, "legs of a trade," are guaranteed to reach completion.
- If the commit point is not reached, typically within a predetermined amount of time, it is guaranteed that no action will reach completion and that any actions temporarily taken will be rolled back (*e.g.*, assets will be returned to the original owners automatically).

From a technology standpoint, atomic settlement can be achieved by programmatic means (*e.g.*, smart contracts) that act as "software escrow agents" to ensure that the point of no return is reached simultaneously for all legs of a trade. From that point on, all legs will proceed to completion.

Both "simultaneous" and "instant" carry a timing connotation which does not lend itself to precise definition in the context of blockchain technologies for several reasons:

[37] *See supra* comment (C).
[38] *See supra* comment (L).
[39] *See supra* comment (D).
[40] The etymology of the word "atom" comes from the Greek "α-" ("non") and the verb "τέμνειν" (phonetically "temnein" – "to cut").

- The finest level of time granularity in a blockchain is the *block time*, *i.e.*, the period between successive blocks. This time varies from block to block and from blockchain to blockchain. Thus, the word "instant" is difficult to define in this context.
- Instant completion of a portion of a transaction is of little value. Let us consider the case of a trade with two legs. Even if each leg completes instantly, one of the two legs could be triggered first. The party receiving assets in this first leg would have temporary possession of both assets involved in the trade, so this party would have an incentive to renege on its obligations. Thus, even if instant execution of the individual legs of a trade was possible, simultaneity of execution would still be required.
- Because of their fully decentralized nature (*i.e.*, lack of central coordination), blockchain protocols are almost invariably designed to attain *eventual consistency*. The blockchain data structure may temporarily diverge between different groups of nodes, but eventually all nodes converge to a single version. The bigger the *depth* of a block, *i.e.*, the position of a block relative to the latest (most recently added) block, the "safer" the block is. Thus, it is customary for an application to wait until the block containing a blockchain transaction submitted by the application has reached a certain depth before the application considers that the submitted blockchain transaction has attained finality. This depth of assumed finality is a subjective parameter, so "instant" cannot be defined precisely. Furthermore, even if two legs of a trade reach completion in the same blockchain block, the corresponding beneficiaries may have different risk tolerance, so they may each wait for a different number of blocks before they declare finality. Thus, "simultaneous" cannot be defined precisely, either.
- Once the commit point (point of no return) is reached, it may take several blocks for all steps required for a portion of a business transaction (leg of a trade) to reach completion, even if such completion is guaranteed as inevitable. This is another obstacle that makes "instant" difficult to define in this context.
- The commit point (point of no return) is typically common (*i.e.*, a single entry in one block) for all actions (legs) of a business transaction (trade). However, the number of blockchain blocks required for different actions (legs) to complete may be different. Such differences may be caused by differences in the number of steps required to complete each action (leg) or by operational variability (*e.g.*, a particular action may not fit in the current block and may have to wait for the next block).

We recommend defining atomic settlement of a business transaction as the indivisibly common fate of all its actions: inevitable eventual completion of all actions or inevitable eventual roll-

back of any tentative actions.[41]

From a practical standpoint:

- Given that the block time for most blockchains is a few minutes or even a few seconds, the atomic settlement on blockchain within a few block periods can be considered almost instant in comparison to traditional (non-blockchain) settlement timeframes measured in days.
- Given that the commit point is typically reached at the same time (*i.e.*, in the same block) for all actions and that the completion of all actions becomes inevitable thereafter, atomic settlement can be considered to provide almost simultaneous settlement of both legs of a transaction, similar to DVP.
- Differences between trade time and settlement time fade or disappear. The commit point can be considered a common reference point for both trade and settlement.

In conclusion, indivisibility of trades is the property which reduces the opportunities for abuse of an investor's assets, and it is also the property that atomic settlement provides. In light of this risk reduction and of the efficiency and speed benefits outlined above, we urge the Commission to promulgate rules and interpretations that expressly permit and encourage the use of blockchain for atomic settlement of trades. We further recommend that the Commission articulate safe harbors which enable parties to a transaction to avail themselves of atomic settlement in a way that they can be sure is compliant.

O. **Response to Question 54 – Execution of Trades while Preserving Custody by Qualified Custodian**

As mentioned earlier,[42] when the blockchain records asset ownership, there is no need for a change in possession in order to receive financial services. The atomic settlement approach[43] ensures that the assets remain in the possession of the original owner (or its custodian) until the commit point of the transaction. After that point, the assets move to the receiving owner (or its custodian). At no point does any other party (including the adviser) exercise any control over the assets.

The trade can involve any counterparty using any custodian – or even no custodian at all if the counterparty opts to rely on self-custody by the owner. It is even possible to trade assets that

[41] The Commission's terms "trade" and "leg of a trade" correspond to the respective broader terms "transaction" and "action" used in our definition.
[42] *See supra* comment (C).
[43] *See supra* comment (N); *see also* comment (L) *supra*.

reside on different blockchains and still use atomic settlement with the immutability and auditability that a blockchain offers.

P. **Security for Custody of Blockchain Assets**

The Commission's discussion of security for crypto assets on page 85 (including footnote 155) appears to be heavily oriented towards cryptocurrencies, which are bearer instruments. As noted earlier,[44] tokenized securities are non-bearer instruments and enjoy (i) additional checks and balances (confirmation of owner identity, screening of wallet addresses, etc.); and (ii) the additional protection offered by the ability to reverse erroneous or fraudulent transactions.

Regardless of the type of blockchain-based instrument (bearer or non-bearer), the discussion in footnote 155 focuses only on cold wallets and hot wallets and ignores the additional security mechanisms (*e.g.*, multi-signature schemes) mentioned in a previous comment.[45]

We recommend that the Commission take into account these additional security considerations and reflect them into its rules and interpretations.

Q. **No Liens Unless Authorized in Writing**

"The proposed rule would require the adviser to obtain reasonable assurances in writing from the qualified custodian that the qualified custodian will not subject client assets to any right, charge, security interest, lien, or claim in favor of the qualified custodian or its related persons or creditors, except to the extent agreed to or authorized in writing by the client" (p. 94).

We note that, in the context of tokenized securities and newer blockchain platforms, ownership is represented directly on the blockchain. Any right, charge, security interest, lien, or claim in favor of another party (including the custodian) would have to be recorded on the blockchain and would thus be immediately visible to the owner. In the absence of such recordation, the owner retains all rights to the asset. Arrangements for margin accounts, payment of fees, etc. can be implemented easily through smart contracts and will be visible to all parties involved. Any such arrangement will require approval (*e.g.*, via a digital signature using the account's private key) by the asset owner. This transparency will increase investor protection by enforcing the proposed regulation's policy objective through technology.

[44] *See supra* comment (B).
[45] *Ibid.*

R. **Response to Question 56 – Due Care Reasonable Assurances Requirement**

On page 79, the Commission states that **"[a] qualified custodian should exercise due care and implement appropriate measures to safeguard the advisory client's assets."** On page 84, the Commission makes a similar statement: **"The proposed rule would require that the adviser obtain reasonable assurances in writing from the qualified custodian that the qualified custodian will exercise due care in accordance with reasonable commercial standards in discharging its duty as custodian and will implement appropriate measures to safeguard client assets from theft, misuse, misappropriation, or other similar types of loss."**

We support the Commission's preference for a more asset-neutral approach over asset-specific approaches, and we agree with the Commission's belief **"that the asset neutral approach of the current rule has been and will continue to be more effective because it relies on the expertise of the various types of qualified custodians and allows the rule to remain evergreen as the types of assets held by custodians evolve"** (p. 78). However, in the context of tokenized securities and blockchains, the rapid evolution of technology will necessitate a continual interpretation of the terms "reasonable commercial standards" and "appropriate measures." We encourage the Commission to promulgate specific safe harbors that enable clients, custodians, and advisers to avail themselves of the advantages and protections of evolving blockchain technologies and to do so with certainty about compliance.[46]

S. **Response to Questions 57 & 60 – Indemnification and Insurance Arrangements by Custodian**

We agree that the proposed rule should include the reasonable assurances requirement that the qualified custodian will indemnify the client (and will have insurance arrangements in place that will adequately protect the client) against the risk of loss in the event of the qualified custodian's own negligence, recklessness, or willful misconduct. This requirement will drive adoption of the most effective technologies by the industry, since custodians will try to minimize the cost of the indemnification and the insurance premium.

As noted in several comments,[47] the tokenization of private securities offers significant advantages in terms of safeguarding assets. Thus, we expect that the reasonable assurances requirement requiring the qualified custodian to provide indemnity and have insurance arrangements in place to adequately protect its clients will accelerate the tokenization of private

[46] We were pleased to see the Commission state that **"because crypto assets and distributed ledger technology are still evolving, we expect the methods used to safeguard crypto assets will likewise evolve, which may lead to reevaluation of best practices in the future"** (pp. 84-85). However, it is important that the frequency of reevaluation should match the speed of technological evolution.

[47] *See supra* comment(D); *see also* comments (B), (C), (J), and (N) *supra*.

securities.

T. **Response to Questions 66, 68, 69, 70 and 71 – Segregation of Client Crypto Assets, Client Name in Accounts, and Commingling of Assets**

We agree with the Commission's belief **"that segregation is a fundamental element of safeguarding client assets"** (p. 91). Our response is focused on assets whose ownership is represented and recorded on blockchain.

As explained in detail earlier,[48] if the full power of state-of-the-art blockchain technologies is used, the blockchain accounts can represent ownership rather than possession, and authority can be granted to financial services provider(s) in a way that is explicit and auditable. To wit:

- The assets need not "move" into the possession of financial services provider(s) and can remain with the original owners, thus offering maximum protection to investors.
- This arrangement will eliminate the problem of segregation since no assets will have been commingled in the first place. The assets of each client as well as those of the adviser or the custodian will be held in separate accounts, thus eliminating any concerns related to the name in which accounts are held, commingling of assets, omnibus accounts, etc.
- Furthermore, we anticipate that the superior administrative convenience and efficiency offered by the representation of assets on blockchain will subsume any administrative convenience or efficiency achieved through commingling and will obviate the need for such commingling, thus offering further protection to investors.

In the interim, while the blockchain is still used to represent possession or control rather than ownership, we believe the Commission's requirements are appropriate and applicable to digital assets.

We encourage the Commission to create clear safe harbors which will enable the industry to transition to the state-of-the-art blockchain technologies in a manner participants will know is compliant. We also suggest that the Commission distinguish between the two blockchain approaches (representation of ownership vs. representation of possession) in its interpretations.

[48] *See supra* comment (C); *see also* comment (J) *supra*.

U. **Response to Question 82 – Transfer Agents as Custodians**

As noted in an earlier comment,[49] we suggest that allowing transfer agents to act as qualified custodians for tokenized securities may facilitate the gradual deployment of technological advancements and the development of the market in a compliant way.

V. **Response to Question 86 – Providing Custodial Account Records to Independent Public Accountant**

We agree that the proposed rule should include the contractual provision that the qualified custodian will promptly, upon request, provide records relating to client investments to an independent public accountant for purposes of compliance with the rule. We also agree with the Commission's belief that the proposed provision would facilitate the public accountant's ability to obtain custodial account records.

We note that in the case of tokenized securities, the immutable and auditable record of transactions recorded on the blockchain will facilitate the task of the accountant.

W. **Response to Questions 117 & 121 – Custodial Services for Privately Offered Securities**

On page 128, the Commission states its understanding **"that the current market for custodial services of privately offered securities is fairly thin."** We anticipate that tokenized private securities will have a broader impact on the market for such custodial services. This will be the case particularly once there is clear guidance that enables market participants to avail themselves of such services without assuming risks associated with regulatory ambiguity.

The technology needed for the custody of tokenized securities (*e.g.*, safeguarding of private keys) overlaps significantly with the technology needed for the custody of other digital instruments represented on a blockchain (*e.g.*, cryptocurrencies). Thus, companies that currently offer custodial services for these other digital instruments could easily expand to offer custodial services for tokenized privately offered securities. We are aware of vendors who are planning such expansion.

We believe that the development of the custodial services market for tokenized private securities will further accelerate the adoption of security tokenization, since it will provide an additional incentive for issuers of non-tokenized private securities to switch to tokenization. We expect that this switch will in turn contribute to the growth of the custodial services market for

[49] *See supra* comment (I).

tokenized private securities, leading to a virtuous cycle. We anticipate that all privately issued securities will eventually become tokenized and that the recordation of privately offered securities only on the non-public books of the issuer or its transfer agent will become largely a relic from a prior era, just like paper stock certificates. At that point, the privately offered securities exception in the proposed regulation will become unnecessary.

As the Commission notes, **"advisers with trading authority of privately offered securities that do not settle DVP often have custody of these securities because of the broad, general power of attorney-like authority required to trade these securities"** (p. 128). Although **"[t]here are certain impediments to transferability typically associated with certain privately offered securities"** (p. 128), none of these impediments offers the level of protection that investors will receive from the DVP settlement of tokenized private securities and the recordation of transactions with immutability, transparency, and auditability on the blockchain. Furthermore, the tokenization of securities will protect investors from misuse, misappropriation, or losses that may result from the adviser's insolvency or bankruptcy, against which the impediments to transferability mentioned above are ineffective.

Finally, we note that, although the exception for privately offered securities would not cover tokenized securities, any investor protections offered by the impediments to transferability of privately offered securities would still be applicable to holders of tokenized private securities, in addition to all the other protections that tokenized securities offer. For example, the need to obtain the consent of the issuer or other securities holders prior to any transfer of ownership would apply also when the privately offered securities are tokenized; the consent could be granted through the submission[50] of a digitally signed approval by the issuer or the other securities holders.

X. Response to Questions 127 & 128 – Definition of Privately Offered Securities in the Context of Tokenized Securities

We agree that the proposed definition of privately offered securities is clear (question 127). However, some of the surrounding commentary by the Commission in reference to crypto asset securities merits attention.

The Commission states, **"[w]e understand that transactions and ownership involving crypto asset securities on public, permissionless blockchains are generally evidenced through public keys or wallet addresses"** (p. 134). We are concerned that this statement is too broad to be

[50] The submission of the approvals can be to a smart contract implementing the transfer. Alternatively, the owner's account in which the tokenized private securities are held may be set up to require additional signatures (those of the issuer and/or other holders) to effect a transfer out of the account.

relied upon for regulatory purposes. It is certainly true that tokens representing securities are held in wallet addresses (blockchain accounts). However, this is not the only evidence associated with ownership of crypto asset securities.[51]

In most blockchains, the tokens representing tokenized securities are implemented using smart contracts – programming code that is recorded on and executed by the blockchain.[52] The smart contracts keep track of the total number of tokens in circulation, the wallet addresses that hold tokens, all the transactions involving transfer of tokens, etc. To ensure compliance with the SEC's regulations for securities, these smart contracts typically impose and enforce constraints on transactions. For example, transfer of securities may be allowed only to wallet addresses that have been white-listed based on screening of their owners for KYC/AML/CFT, investor status (*e.g.*, accredited investor, qualified purchaser) and other applicable criteria.[53] Credible parties perform due diligence and provide attestations for wallets that meet these criteria, which attestations can be recorded on the blockchain. The identity of the wallet owner is known to the attesting organization, although that identity may not be visible on the blockchain. If anything goes wrong, the owner can be easily revealed. The entity operating the smart contracts that implement the tokenized securities (*e.g.*, issuer or transfer agent) can reverse erroneous or illegitimate transfers of tokenized securities by burning and reminting the corresponding tokens. These elements make tokenized securities distinctly different from cryptocurrencies. The elements also mitigate many of the transactional risks which have prompted concern in the context of cryptocurrencies.

On page 134, the Commission states that **"[a]s proposed, in order for a security to be a privately offered security under the proposed safeguarding rule, among other conditions, it must be uncertificated, and the ownership can only be recorded on the non-public books of the issuer or its transfer agent in the name of the client as it appears in the adviser's required records. As a result, we believe that such crypto asset securities issued on public, permissionless blockchains would not satisfy the conditions of privately offered securities under the proposed safeguarding rule."** In question 128 the Commission asks whether **"commenters agree with our belief that ownership of crypto asset securities that is evidenced through public keys or wallet addresses on public blockchains would not qualify for the proposed privately offered securities exception."**

We agree with the Commission that crypto asset securities issued on blockchains would not satisfy the conditions of privately offered securities under the proposed safeguarding rule. Consequently, we agree that "ownership of crypto asset securities that is evidenced through

[51] *See also* comment (B) *supra*.
[52] This is true at least for EVM-compatible blockchains that implement Ethereum Virtual Machines. Such networks include Ethereum, Polygon, Avalanche, and many others.
[53] The Commission mentions potential criteria in question 156 on p. 158.

public keys or wallet addresses on public blockchains would not qualify for the proposed privately offered securities exception." However, we fail to see any reason for the distinction between public, permissionless blockchains and permissioned blockchains. In both cases, the ownership of tokenized private securities (not involving any public offering) can be readily represented / recorded on a blockchain, so *in both cases the securities fail to meet the requirement* that they **"be capable of only being recorded on the non-public books of the issuer or its transfer agent"** (p. 133). Thus, we believe that ownership of crypto asset securities that is evidenced on blockchains would not qualify for the proposed privately offered securities exception irrespective of whether the blockchains are public or permissioned.

Furthermore, the implicit distinction that the Commission is drawing between public, permissionless and permissioned blockchains in the context of tokenized private securities points towards a potential misconception. The fact that ownership of a tokenized private security is represented / recorded on a public, permissionless blockchain does *not* imply that any anonymous wallet address can hold the corresponding token or that the securities can be transferred to any anonymous wallet address. As mentioned above, tokens can be held by or transferred to only wallet addresses that preserve compliance with all SEC securities regulations. These restrictions are no different and create no less accountability than the restrictions imposed by a permissioned blockchain. The situation is analogous to a prescription medication: the distribution of the medication is controlled via a prescription whether that prescription is filled by the internal pharmacy of a hospital (to which only hospitalized patients have access) or by a pharmacy within a retail store. The fact that anyone can access the retail store does not mean that anyone can get access to the medication; only those with a prescription can.

For private securities whose ownership is represented on a blockchain, blockchain technology enables the measures mentioned above (smart contracts, whitelisting of wallet addresses, etc.) and the measures mentioned in other comments (atomic settlement,[54] ability of owner to provide explicit and auditable authorization,[55] ability of owner to review and/or confirm transactions,[56] etc.). These measures provide protections that **"mitigate some or all of the risks the rule is designed to address – loss, theft, misappropriation, misuse, and adviser insolvency or bankruptcy"** (question 128). At the same time, such securities do not qualify for and do not need the privately offered securities exception. Thus, recording ownership of private securities on blockchain should be a regulator's dream: (i) it provides higher protections for investors; and (ii) it obviates the need for an exception to the regulation.

In light of the above, we urge the Commission to create a clear regulatory framework which

[54] *See supra* comment (N).
[55] *See supra* comments (B), (C), and (J).
[56] *See supra* comment (C); *see also* comment (AA) *infra*.

eliminates uncertainty regarding the tokenization of private securities. As mentioned earlier,[57] we anticipate that the benefits of blockchain technology will drive adoption of tokenization for private securities and that the recordation of privately offered securities only on the non-public books of the issuer or its transfer agent will become largely a relic from a prior era, just like paper stock certificates. When adoption becomes widely spread, the Commission may choose to eliminate the privately offered securities exception in a future release of the regulation.

Y. **Response to Question 132 – Exception for Privately Offered Securities**

The Commission asks whether it should **"not create an exception for privately offered securities and physical assets."** We limit our response to privately offered securities.

As mentioned earlier,[58] recording ownership of private securities on a blockchain (i) provides higher protections for investors; and (ii) obviates the need for an exception to the regulation. While the exception may find some use in the short term for non-tokenized private securities, we anticipate that the benefits of blockchain technology will drive adoption of tokenization for private securities and that the recordation of privately offered securities only on the non-public books of the issuer or its transfer agent will become largely a relic from a prior era, just like paper stock certificates. When adoption becomes widely spread, the Commission may choose to eliminate the privately offered securities exception in a future release of the regulation.

Z. **Response to Question 133 – Market for Custodial Services of Privately Offered Securities**

We anticipate that the tokenization of privately offered securities will lead to an increase in the supply of custodial services for such securities. This is because the technology needed for the custody of tokenized securities (*e.g.*, safeguarding of private keys) overlaps significantly with the technology needed for the custody of other digital instruments represented on a blockchain (*e.g.*, cryptocurrencies). Thus, companies that currently offer custodial services for these other digital instruments could easily expand to offer custodial services for tokenized privately offered securities. We are aware of vendors who are planning such expansion. This development will further accelerate the adoption of security tokenization and will further reduce the need to utilize the privately offered securities exception.

Our assessment is consistent with the Commission's statement that **"while today it may be reasonable under appropriate circumstances for an adviser to determine that a qualified custodian cannot maintain possession or control of a particular privately offered security, we**

[57] *See supra* comment (D); *see also* comment (W) *supra*.
[58] *See supra* comment (X); *see also* comment (C) *supra*.

believe that determination may be more difficult to support as the custodial industry continues to evolve" (p. 137).

Furthermore, as mentioned earlier,[59] the maturation of software tools could make self-custody of tokenized assets by owners not only a viable approach, but possibly a preferred, safer, and easier one. Self-custody by owners would automatically eliminate all concerns about commingling of assets, name used for account registration, omnibus accounts, etc.

AA. **Response to Question 156 – Client Serving as its Own Independent Representative**

The Commission asks whether "commenters believe that a client could serve as its own independent representative." We provide a commentary in the context of tokenized private securities.

As mentioned earlier,[60] tokenized private securities enable the implementation of powerful checks-and-balances. These checks-and-balances can include the notification of an asset owner about an imminent transaction initiated by another party (*e.g.*, adviser) and the requirement for explicit, recordable, and auditable approval (authorization) of such a transaction by the asset owner. While the utilization of such checks-and-balances is rendered moot by the fact that tokenized securities will not qualify for the privately offered securities exception[61] and will need to be custodied by a qualified custodian (or by the owners themselves), the discussion highlights once again the benefits of private security tokenization and why we believe that the Commission should create a regulatory framework to facilitate such tokenization.

BB. **Response to Questions 160 & 161 – Asset Verification & Audits for Tokenized Securities**

We comment from the perspective of tokenized privately held securities. While such securities do not qualify for the privately offered securities exception[62] and will need to be custodied by a qualified custodian (or by the owners themselves), we note that the transparency offered by a blockchain facilitates auditability and allows a higher degree of automation through software. When an accountant performs an audit of blockchain-based assets, there is no need to use sampling or set a threshold for materiality. Thus, audits can be comprehensive and eliminate the Commission's concern on p. 131 that **"these assets may not be included in the sample of assets subject to verification procedures during a surprise examination or meet the materiality**

[59] *See supra* comment (C).
[60] *See supra* comments (B) and (C).
[61] *See supra* comments (X) and (Y).
[62] *Ibid*.

threshold for verification during a financial statement audit. As a result, a loss could similarly go undetected by an independent public accountant for a substantial period." The Commission expresses a similar concern on p. 146.

Consequently, the tokenization of private securities serves the policy goals of the Commission and should be encouraged by the Commission through the creation of a regulatory framework that removes ambiguity.

CC. **Response to Question 178 – Segregation Requirements for Crypto Assets**

The response to this question mirrors our response to question 66 regarding segregation of assets by the custodian.[63] Once again, we focus on tokenized private securities, but similar considerations apply to other types of assets represented on blockchain.

As explained in detail earlier,[64] if the full power of state-of-the-art blockchain technologies is used, the blockchain accounts represent ownership rather than possession, the assets are automatically registered in the name of the client, and authority can be granted to financial services provider(s) (including the adviser) in a way that is explicit and auditable. The assets need not "move" into the possession of financial services provider(s) and can remain with the original owners, thus offering maximum protection to investors. This arrangement will eliminate the problem of segregation since no assets will have been commingled in the first place.

The assets of each client as well as those of the adviser (or the custodian) will be held in separate accounts. Since the blockchain will record the ownership of the assets by the client, the assets will be protected in the event of a bankruptcy or financial losses involving an adviser or custodian with custody of crypto assets.

DD. **Response to Questions 180 & 181 – Liens and Other Claims on Tokenized Assets**

In the context of tokenized securities and newer blockchains, ownership is represented directly on the blockchain. Any right, charge, security interest, lien, or claim in favor of another party (including the adviser) would have to be recorded on the blockchain and would thus be immediately visible to the owner. In the absence of such recordation, the owner retains all rights to the asset.

[63] *See supra* comment (T).
[64] *See supra* comment (C).

Arrangements for securities lending, margin trading, payment of fees for services rendered by the adviser, etc. can be implemented easily through smart contracts and will be visible to all parties involved. Any such arrangement will require approval (*e.g.*, via a digital signature using the account's private key) by the asset owner. This transparency will increase investor protection by enforcing the proposed regulation's objective through technology.

EE. **Response to Question 239 – Risks to Client Assets from Discretionary Authority**

We agree with the Commission's assumption that a one-way transfer of assets from an account at a qualified custodian is a riskier form of discretionary authority than DVP transactions. We note that, as explained in detail earlier,[65] the representation of assets on the blockchain enables atomic settlement, which **"transfer[s] assets out of a client's account only upon corresponding transfer of assets into the account"** (p. 207) and is a form of DVP. Thus, transactions involving tokenized securities reduce risk for the account owners.

FF. **Response to Question 253 – Irreversibility of Crypto Asset Transactions & SLOA Exception**

We believe that the answer to the Commission's question depends on the type of crypto asset. As noted earlier,[66] transactions involving non-bearer instruments (*e.g.*, tokenized securities) are reversible on both permissioned and permissionless blockchains. Thus, there is no reason why the proposed standing letters of authorization exception should be unavailable for these assets.

With respect to bearer instruments (*e.g.*, cryptocurrencies), transfers out of a client's accounts may indeed be irreversible. In this case, explicit confirmation of a transaction by the account owner could prevent erroneous or fraudulent transactions. Such a confirmation mechanism can be easily enforced by the account owner through account authority arrangements.[67]

Furthermore, we ask the Commission to consider whether the situation with bearer instruments for crypto assets is different from the situation with bearer instruments that are not represented on blockchain. For example, if a cybercriminal steals the on-line banking credentials of the legitimate holder of a checking account and then remits cash to an overseas account, would such a transaction be reversible? Our experience indicates that reversal of such transactions is not always possible. Thus, there may be no need to treat crypto assets differently than other classes of assets.

[65] *See supra* comment (D); *see also* comment (N) *supra*.
[66] *See supra* comment (B).
[67] *See supra* comments (J) and (AA).

Conclusion

In the context of privately offered securities, the tokenization of private securities offers significant advantages that protect clients and align well with the Commission's policy goals related to custody of assets. We urge the Commission to:

- Distinguish between bearer instruments and non-bearer instruments represented on the blockchain, rather than aggregate all digital assets into a single category.
- Cater to the "evergreen" nature of the rule by keeping up with technological developments and issuing interpretations of "reasonable commercial standards" and "appropriate measures," express safe harbors, clear rules, and decisive no-action letters that will enable the adoption of newer blockchain technologies and benefit clients in multiple ways:
    - Asset ownership is reflected directly on the blockchain and changes in ownership are immediately visible.
    - Clients can receive financial services by granting authorizations rather than transferring assets to service providers (which would have obfuscated asset ownership).
    - Atomic settlement enables DVP and eliminates risky one-way asset transfers.
    - Client assets can be readily segregated from assets of other clients or service providers.
    - Data transparency on the blockchain facilitates auditability of account activity.
- Enable the migration of the industry to tokenized private securities without the risk of regulatory ambiguity, which migration will provide clients the benefits mentioned above and also obviate the need for the privately offered securities exception to the proposed regulation.

Separately, we urge the Commission to revise the definition of custody to avoid inadvertently ensnaring technology services providers into custody regulations because of the implementation of cybersecurity measures in technology infrastructure. An overly broad application of the definition of custody adds little, if any, investor protection and could impede the adoption of technology that ultimately furthers the Commission's policy goals.

Respectfully submitted,

/Christos A. Polyzois/

Christos A. Polyzois, Ph.D.
Deputy CTO for Intellectual Property & Innovation
INVENIAM CAPITAL PARTNERS, INC.