May 23, 2021Via email (rule-comments@sec.gov)

Ms. Vanessa A. Countryman
Secretary
U.S. Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549-1090

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

Dear Secretary Countryman:

Inca Digital appreciates the opportunity to provide comment on the U.S. Securities and Exchange Commission Statement and Request for Comment regarding "Custody of Digital Asset Securities by Special Purpose Broker-Dealers."

I. About Inca Digital

Inca Digital's mission is to provide enterprise grade data collection, infrastructure, and analytics across the digital asset ecosystem to create a more transparent marketplace where investors, companies, government agencies, and other marketplace participants can make objective, data-driven decisions. Inca Digital utilizes a data platform called NTerminal to analyze phenomena occurring in the digital asset space. NTerminal processes *financial data*—from over five-hundred exchanges such as orders, trades, and third-party reference prices, *technical data*—stemming from blockchain data, blockchain meta-data, GitHub repositories, and more, and *natural language data*—arising from news, blogs, social media, messenger channels, the decisions of financial regulators and law enforcement globally, and other natural language sources to detect patterns useful for understanding trends in the digital asset space. In addition, Inca Digital helps clients with compliance issues by monitoring international regulatory filings, active national security directives, disciplinary actions, regulatory decisions, and KYC and AML compliance. Inca Digital also monitors blockchain for irregularities that may point to fraud, money laundering, terrorist financing, and market manipulations like wash trading or pump and dump schemes.

Our clients are financial regulators, fund managers, custodians, national security agencies, law enforcement agencies, insurance companies, and infrastructure providers. Several clients worthy of mention are the Department of Defense, Commodities Futures Trading Commission, Ontario Securities Commission, Hehmeyer Trading and Investments, Forbes, Bermuda Monetary Authority, and ErisX. These clients rely on Inca Digital for cutting-edge data solutions to strategically structure their market participation.

II. Reply to Request for Comment

As a digital asset analytics firm acutely aware of the risks inherent to this industry, we fully support the Commission's encouragement of broker-dealer's to operate under the circumstances described in Section IV of the comment request. We would, however, note that while the commission has granted direction with respect to the application SEC's Customer Protection Rule, 17 CFR 240.15c3-3 in the digital asset space, there is little information on how to comply with Custody of Funds or Securities of Clients by Investment Advisers 17 CFR 275.206(4)-2. It is Inca Digital's opinion that the satisfaction of Section IV should satisfy both the aforementioned regulative requirements.

There are several measures custodians would be advised to take to ensure the utmost security of their client's cryptocurrency investment. The methods enumerated below might be a good start to applying, to the cryptocurrency arena, the regulatory intent of the SEC's Customer Protection Rule, 17 CFR 240.15c3-3, and Custody of Funds or Securities of Clients by Investment Advisers 17 CFR 275.206(4)-2. Custodians should implement practices to safeguard the investor's fund at every level and opportunity within the crypto ecosystem. Thus, for custodians to ensure proper protection, (1) it is imperative that the wallet holding cryptocurrency be secure; (2) custodian's cybersecurity team must implement mechanisms to solve the single point of failure problem; (3) the company should have digital asset insurance to compensate cryptocurrency holders in case of loss; and lastly, (4) for transparency, it is necessary for custodians to hire third-party compliance organizations to test for general adherence with procedures to manage the risks inherent to financial technology generally and cryptocurrency specifically.

A. Guarding the Crypto Wallet[1]

Custodians store cryptocurrency in several different types of wallets, differentiated by degrees in temperature. The "temperature" measures the degree of accessibility a client has to their wallet's

[1] Allesio Quaglini, *Digital Asset Wallets & Signing Algorithms: A Custodian's Overview*, - HEX TRUST, (July 21, 2020), https://medium.com/hex-trust/digital-asset-wallets-signing- algorithms-a-custodians-overview-ea3badee369c.

funds, and in turn, the exposure to malevolent hacks. There are four wallet temperatures, (a) cold, (b) hot, (c) warm, and (d) freezing.

1. Cold Wallet

Cold Wallets are "air gapped"—placed in a digital storage unit detached from the internet. Because they are disconnected and safe from hackers, they provide a heightened level of security. However, given that they are air gapped, these wallets do not allow quick trading and require anywhere from one to twenty-four hours before a crypto trader may sign off on a transaction.[2] Also, another trade-off, because clients and custodians utilize these wallets manually, it becomes difficult to scale such storage facilities without allowing access to multiple people, potentially undermining the very security a firm seeks to implement. One more subtle issue: air-gapped technology is more complicated to upgrade and integrate new protocols because the technicians must implement these changes manually.

Long-term investors often use Cold Wallets because they plan to hold their investment for long periods of time and are not looking for the flexibility to trade at a moment's notice.

Non-long-term investors also use this sort of wallet if they are storing an enormous amount of crypto and seek increased security measures.

2. Hot Wallet

Unlike Cold Wallets, Hot Wallets are attached and accessible via the internet. Therefore, to some degree, this wallet is more vulnerable to hackers. Those who own smaller amounts of crypto and are less likely the targets of a hacker's machinations are more likely to utilize Hot Wallets. Day traders who have more than the average amount of crypto in their account also use this sort of wallet because they need immediate access to buy and sell crypto at a moment's notice. Serious

[2] *Id.*

investors usually will have most of their funds in a Cold Wallet but leave some in their Hot Wallet to benefit from the unique features of both mechanisms.

3. Warm Wallet

There is no single industry standard or definition for Warm Wallets. Instead, each provider uniquely implements this sort of wallet according to the way they see fit. Some custodians might use this term in reference to a technical setup where they store the crypto in a Cold Wallet, but the wallet is connected to the host computer for the signing process. Others might be referring to Hot Wallets with which the provider has integrated additional layers of security. These measures may include whitelisting—the ability to process transactions only to specific whitelisted addresses and transaction policies—only allowing a predetermined volume and frequency of trades from a particular wallet. Both these measures limit the possibility of hijacked crypto key transactions.

4. Frozen Wallet

Some custodians allow their customers to utilize another wallet type, called Frozen Wallet or Deep Cold Wallet. Like Warm Wallets, the term may refer to a multitude of different wallet features. Firms use this term to reference Cold Wallets with added security features. These features may include completely air-gapped environments for private keys and their servers, the geographical distribution of wallets, and sharding of the wallets (splitting one wallet amongst several different databases). Because Warm and Frozen Wallets do not necessarily have a universal custodial meaning, users need to research and understand each custodian's method of wallet implementation.

Custodians typically use a combination of hot and cold wallets to manage their customer's funds with the option to upgrade hot and cold to warm and frozen, respectively. Regulatory bodies should consider mandating exchanges to inform the user of the pros and cons of each wallet based on the needs of the consumer. As a prerequisite, crypto custodians will need to fully understand each investor's goals to effectively customize the wallet for their use.

After a client deposits crypto with a custodian, the provider typically rebalances the funds between cold and hot wallets, leaving most of the funds—usually more than 90%—in the former for security purposes.[3] Because funds in different temperature wallets impact a client's access to crypto and, therefore, the ability to trade, the allocation of assets amongst wallet types significantly impacts market liquidity in each exchange. Thus, although the trader's interest primarily governs the distribution of crypto among wallets, it is crucial from a regulatory perspective to understand the downstream consequences of such a structure on liquidity and the subsequent impact on market price. To incentivize liquidity—to try and keep crypto at a stable price—regulatory bodies might consider prohibiting traders from keeping 100% of their crypto in Cold Wallets. While the advent of businesses and some state and local governments accepting bitcoin as a form of payment may sufficiently curb any liquidity issue for bitcoin, such a move will help stabilize less popular digital assets.

[3] *Hot and Cold Wallets, Why These Concepts are Outdated*, Vault, (Oct 28, 2020), https://blog.ledger.com/hot_cold/; *SECURITY FOR YOUR PEACE OF MIND*, COINBASE, https://www.coinbase.com/security.

B. Solving the Single Point of Failure Problem[4]

The benefit of a decentralized currency system is that there is no single point of failure (SPOF) through which insurgents can compromise the system.[5] Stated differently, the aspect of universal knowledge and accessibility of crypto data protects it from fraud. A complication arises in that the method of utilizing one's crypto in a transaction—the crypto key—creates a restricted, exclusive domain, hence, a SPOF, undermining much benefit of decentralization. In other words, wallets protect the key, but the necessity for a key to effect a transaction creates an opportunity for exploitation. In response, custodians sought creative methods to solve SPOF and have implemented several different ever increasingly sophisticated crypto key utilization mechanisms to effect crypto transactions, some solving SPOF more effectively than others. There is (a) single and multi-signature, (b) Shamir's secret sharing scheme (SSSS), and (c) multi-party computation (MPC).

1. Single and multi-signature

The simplest method, single signatures, does not solve SPOF because should the key become compromised, the entire account is exposed. Multi-signature addresses this issue to some extent as it requires several keys for a transaction to occur. This way, should one key become compromised, the nefarious actor will still be unable to reach account funds. The downside of this extra security measure is that each blockchain accesses this feature in a unique manner, making it necessary for complex integration to utilize multi-signature on more than one chain. Also, because multi-sigs are more expensive than single, at scale, traders may wind up paying heavy fees for this additional safeguard. Lastly, with multi-sig, should the need arise for a

[4] *Id.*

[5] *Security Threats to Cryptocurrency owners*, VAULT12, (Nov. 19, 2018), https://medium.com/vault12/security-threats-to-cryptocurrency-owners-247b531e4085.

customer to change her wallet scheme, it will be necessary to generate a new wallet and transfer the funds over, which is a tedious and expensive process.

2. Shamir's secret sharing scheme (SSSS)

Another method for solving SPOF is known as Shamir's secret sharing scheme (SSSS). Instead of having several keys, this mechanism essentially takes one key and splits it into several shards. Thus, the transaction is signed on-chain by one key built from a combination of several shards. Because ultimately the transaction utilizes only one signature, this method avoids the problem of complex integration and additional transaction costs, both of which harms multi-sig users. While this method is relatively easy to implement, it only partially solves the SPOF problem: Custodians generate private keys and shards in a single location creating SPOF and there will be a SPOF after the algorithm gathers the shard combination, but before a transaction occurs.

3. Multi-party computation (MPC)[6]

A more recent option, albeit conceptually a more complicated one, is the multi-party computation (MPC). Though it has some drawbacks, this method successfully solves the SPOF issue. Simply put, this approach utilizes three distinct private domains taking the role of three parties in the following analogy: Each party seeks to hide their personal data as a solo entity piece but desires to utilize the sum total of both theirs and each other's data in a manner that precludes others from discovering the value of each solo entity piece. Therefore, the parties mutually agree to fractionate their solo entity pieces using numerical value into three portions. Then each party keeps one slice of their own data for themselves and grants the other two slices, one each, to the two opposite parties. Then, each party, privately, in their own respective domain, adds up the slice of their own data that they retained, and the two pieces of data granted from the

[6] *Id.*; *What is Secure Multiparty Computation*, INPHER, https://inpher.io/technology/what-is-secure-multiparty-computation/; Mike Belshe, *Multi-Sig vs MPC: Which is more secure?*, BITGO, (Sept 11, 2019), https://blog.bitgo.com/multi-sig-vs-mpc- which-is-more-secure-699ecefc8430.

two opposite parties. After this step, each domain goes public with the amalgamated value of the three slices and shares it with the group. The crucial component here is that each domain's final sum added together publicly establishes the sum total of all three domain's confidential data, but each domain's solo entity value is still secret because each party was missing two parts of their co-party's entire data set during the process of evaluation. In this manner, the parties have shared the sum total of each other's data without divulging their own.

This method allows its users to engage in a transaction without divulging their crypto keys, thus avoiding a SPOF. In addition, it is protocol-agnostic and therefore avoids the need for a unique and separate implementation for each blockchain. It also minimizes blockchain transaction expense because it utilizes only one signature. One more benefit is that this method is flexible in allowing modification of thresholds without the tedious and expensive task of generating new wallets.

That said, there are still several drawbacks. First off, because of its anonymity, this method creates a lack of accountability inherent in any crypto transaction that does not show which key is signing off on a transaction. Single and multi-signatures leave evidence of which key signed off on a transaction, and because ideally, one individual controls each key, it is clear who signed off. However, for MPC's, once the transaction is complete, all the signatures look identical, and it is impossible to tell who the three participants were. If the provider stores key materials with three executives and two collude to harness MPC to steal their client's funds, it will be impossible to know who utilized their keys and which executives are guilty and innocent. Also, from a forensics perspective, a fraudulent transaction that utilized three out of five keys located in five different geographical locations will be harder to analyze because it is impossible to know which keys of those locations the perpetrator stole. Lastly, backup key holders are far less likely to be willing to engage with MPC protected custodians for fear that should a fraudulent transaction occur, they will become suspects of the crime because of the MPC anonymity.

A downside unrelated to anonymity is the lack of peer review on MPC cryptography. Cryptographic algorithms take years and sometimes decades to ensure that they are foolproof. Multi-sig has been tested over many years and is known to be of negligible risk. One last issue with MPCs is the lack of compatible Hardware Security Modules (HSM). HSM's are essential to the basic security of key material. Thus, without HSM to house MPC, arguably, even a single signature method is more secure.

C. Digital Asset Insurance

After implementing several temperature wallets for the client's funds and either solving or further securing SPOF vulnerability, the client's currency is by and large secure. However, digital keys may get lost, or through an inside job or outside hacker, the client can inadvertently lose their investment. Many custodians have bought cryptocurrency insurance on their Cold Wallets, should such a case arise, to ensure their client's investment. Bitgo's Cold Wallets, for example, are ensured with Lloyd's of London for up to 100-million-dollars for any third-party hacks, copying, or theft of private keys. In addition, Bitgo allows its customers to supplement this insurance policy with the option of buying up to 500-million-dollar's worth of insurance. Gemini, another custodian, is utilizing a captive insurance company structure to secure a 200-million-dollar insurance policy on their Cold Wallet storage facilities.[7] Because their

[7] Christina Comben, *Gemini now provides crypto's largest insurance coverage*, YAHOO!FIANCE, (Jan. 17, 2020), https://finance.yahoo.com/news/gemini-now-provides-crypto-largest-1000 10855.html.

insurance company is captive, they can secure a policy far higher than other industry competitors. Both Bitgo and Gemini allow clients to buy their own Hot Wallet insurance policies to protect their investments from losses.

D. Third-Party Compliance Testing

The cryptocurrency industry, particularly custodians, heavily intersect technology, finance, and cybersecurity, bringing together a host of potential risks germane to these industries at every level of a firm. To transparently mitigate these risks, it is crucial to have respected third-party organizations audit custodians. Deloitte & Touche LLP has audited Bitgo and Gemini for compliance with SOC 2 for Service Organizations Type 2 provided by the American Institute of Certified Public Accountants (AICPA).[8] This compliance program, while voluntary, is used by firms with sensitive data to ensure the strictest standards of protection for data centers and information systems.[9] SOC 2 for Service Organizations Type 1 is the first compliance level where a prospective auditor evaluates a firm's protection at a given moment in time.[10] Type 2 of SOC 2 for Service Organizations is an upgraded level of compliance where the company is audited over several months or years to see how data and information protection withstands the test of time and market utilization.[11] Regulatory bodies should mandate this sort of inspection across crypto custodians to ensure firms are protecting their client's investment responsibly.

[8] *Gemini Completes SOC 1 Type 2 and SOC 2 Type 2 Examinations — Leading Crypto Industry*, Gemini, https://www.gemini.com/blog/gemini-completes-soc-1-type-2-and-soc-2-type-2-examinations-leading-crypto.

[9] *SOC 2 Type 2 Guide | Everything You Need To Know*, Strongdm, https://www.strongdm.com/blog/what-is-soc-2-type-2.

[10] *SOC for Service Organizations*, AICPA, https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/socforserviceorganizations.html.

[11] *Id.*

III. Conclusion

In order to satisfy the SEC's Customer Protection Rule, 17 CFR 240.15c3-3, and Custody of Funds or Securities of Clients by Investment Advisers 17 CFR 275.206(4)-2, custodians should implement measures at four distinct levels of the digital asset ecosystem. A secured wallet, solving the single point of failure problem, digital asset insurance, and third party auditing should be enough to manage risk inherent to custody of digital assets. Protecting crypto assets responsibly in this manner should be enough to preclude custodians from facing enforcement actions from the SEC or other regulatory bodies.

Inca Digital, once again, appreciates this opportunity to advise the SEC on the best manner for crypto asset custodians to comply with securities regulations. Please reach out to [redacted] with any further questions or concerns.

Respectfully,
Elazar Kosman
Inca Digital
Manager, Business and Legal Affairs