Prometheum

April 26, 2021

VIA EMAIL SUBMISSION TO rule-comments@sec.gov.

Ms. Vanessa Countryman
Secretary
Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549-0609

Re: Custody of Digital Asset Securities by Special Purpose Broker-Dealers (17 C.F.R. Part 240, SEC Rel. No. 34-90788, File No. S7-25-20) (the "Proposal")

Dear Ms. Countryman:

Prometheum, Inc. ("Prometheum") appreciates the opportunity to provide comments on the Proposal and recognizes that it is an effort by the Securities and Exchange Commission (the "Commission") to seek a comprehensive approach to the regulation of digital asset securities. We recognize that it is the Commission's goal to ensure that the level of investor protection related to the custody of digital asset securities is equal to or greater than the protection currently offered in the traditional securities (non-digital securities) clearing, settlement and custody model. We also believe, that as is the case with traditional securities, there should be a securities industry alternative for the custody location of digital asset securities.[1] We have prepared this letter in response to the Commission seeking comments from the public in order to gain information and insight relating to potential industry standards and best practices to ultimately determine the rules and policies for the custody and control of digital asset securities.

Prometheum applauds the Commission's effort to create a framework for becoming a Special Purpose Broker-Dealer. While we endeavor to answer the Commission's request for comments in the Proposal, we also seek certain points of clarification as we believe the Proposal creates material unknowns that are critical to the clearing, settlement and custody of digital assets securities.

In the Proposal, the Commission takes the position that a Special Purpose Broker-Dealer must limit its business operations to digital asset securities. The definition of a digital asset security, as used in the Proposal, is "a digital asset that meets the definition of a "security" under the federal securities laws." This definition puts a burden on the industry to determine which

[1] *See OCC Interpretive Letter No. 1170 from July 22, 2020,* opining that national banks can provide custody services for crypto securities pursuant to already established provisions of custody of traditional securities.

[redacted]

digital assets are securities. As a result, we believe clarity is needed for Special Purpose Broker-Dealers, issuers, ATS' and other market Participants (as defined below) to understand the regulatory framework they must comply with. Therefore, we respectfully request that the Commission provide further clarification on the definition of digital asset securities.

It is important to note that regardless of how the Commission defines digital asset securities, we believe the securities industry won't realize the many benefits of using blockchain technology without including stablecoins in the settlement process. Stablecoins are digital assets that are generally pegged to stable assets such as fiat currency, thereby making them a blockchain native solution for performing asset to "cash" settlement. Allowing a Special Purpose Broker-Dealer to settle digital asset securities with stablecoins will result in further settlement efficiencies such as instantaneous and direct settlement. In consideration of the important role stablecoins can play in the digital asset securities settlement process, we respectfully request the Commission clarify whether Special Purpose Broker-Dealer will be able to settle transactions using stablecoins.

We appreciate the Commission's efforts to protect investors while adopting innovative technologies like blockchain. As with any new technology there are inherent risks. With blockchain, risks differ depending on whether a blockchain is public or permissioned (private). Public blockchains inherently run the risk of nodes operated by bad actors, the difficulty of "unwinding" blocks of potentially erroneous transactions, and the general risks associated with malicious actors affecting governance, consensus and ultimately, policy and operations. These risks can be mitigated with a permissioned chain model. Therefore, we respectfully request the Commission provide guidance on how this Proposal applies to permissioned blockchains.

In furtherance of the Proposal's collection of information and of the industry's need for clearly defined practices, Prometheum provides comments herein to the following questions: 1) What are industry best practices with respect to protecting against theft, loss, and unauthorized or accidental use of private keys necessary for accessing and transferring digital asset securities; 2) What are industry best practices for generating, safekeeping, and using private keys? Please identify the sources of such best practices; 3) What are the processes, software and hardware systems, or other formats or systems that are currently available to broker-dealers to create, store, or use private keys and protect them from loss, theft, or unauthorized or accidental use?; 6) What differences are there in the clearance and settlement of traditional securities and digital assets that could lead to higher or lower clearance and settlement risks for digital assets as compared to traditional securities?; and 7) What specific benefits and/or risks are implicated in a broker-dealer operating a digital asset alternative trading system that the Commission should consider for any future measures it may take?

I. Proposal Questions 1 and 3: Question 1) What are industry best practices with respect to protecting against theft, loss, and unauthorized or accidental use of private keys necessary for accessing and transferring digital asset securities? What are industry best practices for generating, safekeeping, and using private keys? Please identify the sources of such best practices; Question 3) What are the processes, software and hardware systems, or

other formats or systems that are currently available to broker-dealers to create, store, or use private keys and protect them from loss, theft, or unauthorized or accidental use?

Questions 1 and 3 are best addressed together as they go hand-in-hand. The Commission has stated that a Special Purpose Broker-Dealer custodying digital asset securities must comply with the Customer Protection Rule by establishing that the digital asset security is in "the exclusive physical possession or control of the broker-dealer". The creation, protection and safe storage of private keys are critical to establishing the exclusive physical possession or control by the broker-dealer of digital asset securities.

A. **Current Industry Best Practices**

Cyber security industry best practices, such as automated control systems, information security, and existing digital financial services and enterprise encryption systems, are the first line defense mechanisms for protecting private keys. Another strategy, more specific to blockchain to secure keys, includes strictly automated key management systems, extensive logging and auditing of key use, role-based access, and key rotation. In addition to the above measures, the combined use of Multisignature Wallets ("MultiSig Wallets"), hardware key/wallet systems and offline use of keys and signatures ("cold storage") provide the highest level of security, and in our opinion, exceeds the level of security offered by databases, cloud, and other hosting solutions currently used to custody non-digital securities.

Digital asset securities are generally created on a blockchain as smart contract "tokens", which means that best practices for the management of keys can include enforcing or expecting certain best practices in the smart contracts themselves (including MultiSig Wallets described below). This is unlike most cryptocurrencies where the options for key management are hard-coded into the underlying blockchain and provide limited options, particularly for multi-signature use.

Multisig Wallets are normally implemented as smart contracts whose access is cryptographically secured via the use of private keys and require at least two cryptographical private keys to access, and by extension, initiate or "call" a transaction. A smart contract is both the means of representing the digital asset on the blockchain and also controls access to the use of the digital asset. The number of keys required to access a wallet can vary depending on the protocols of the smart contract (e.g., a simple majority, 2 out of 3, 3 out of 5), commonly known as "N or M approvals".

Smart contract enabled Multisig Wallets are a simple yet effective solution to solving two major problems inherent to digital assets: 1) losing them due to the loss of a person's private key and 2) theft by another person or entity. Multisig Wallets are a viable solution for ensuring that investors don't lose assets on a blockchain supported clearing, settlement, and custody solution because different required private keys can be entrusted to different persons at the broker-dealer so no one person has complete control. Essentially, the sum of the "pieces" will ensure the whole is not lost.

An "N" of "M" protocol requires authentication of a certain number of keys. Each key would be distributed amongst different authorized persons, each of whom must authenticate using different mechanisms (e.g., different hardware systems). As an illustration, a "3 of 5" system allows for any three (3) of a total of five (5) keys to be used to confirm a transaction.

In the context of the Special Purpose Broker-Dealers holding the digital asset security, two to three of the five (5) keys would be held by different appropriately-authorized associated persons. Each of these persons would use a different hardware key system to authenticate their respective code. All of the hardware systems would be integrated and under the control of the broker-dealer.

In addition to "N of M" threshold systems for multiple keys, smart contract wallets can also be programmed to provide a key rotation or replacement system. For example, in a system that regularly uses specific keys, those keys should be replaced or, in the case of a significant security breach, replaced by less-frequently used keys. Such a system can be engineered to either require all other keys to confirm a replacement key or use of a separate key that is held in a different structure or with a different entity. In an example "3 of 5" system where 1 key is lost, stolen or unavailable it could be expected that three (3) of the remaining four (4) keys will be used to sign a transaction. Therefore, policies for key rotation or key replacement are important to ensure secure systems.

Hardware key/wallet systems are specially designed hardware that store private keys. Such systems often resemble USB memory sticks with a small screen. The advantage of these devices is that they do not connect to the internet permanently (i.e., are normally considered some form of "cold storage") and thus provide a simple mechanism for keeping keys away from internet-connected computers that may be running (or susceptible to running) malicious software. Normally hardware key systems produce the required digital signatures on the devices itself and don't allow for the private key itself to be obtained easily. Multiple types of hardware signing devices from different vendors is critical to maintaining the safety of the "N" of "M" protocol. This protects against potential failure of the protocol should one hardware signing device be compromised, as only one of the "N" of "M" keys would be lost.

Lastly, offline ("cold") use of keys and signatures refers to keys that are stored in an electronic device that is not connected to the internet (a/k/a "air gapped") which is also a strongly recommended best practice.

Ultimately, we believe the above processes and tools are a good foundation for industry best practices.

II. Proposal Question 6: What differences are there in the clearance and settlement of traditional securities and digital assets that could lead to higher or lower clearance and settlement risks for digital assets as compared to traditional securities?

The comparison of clearing and settlement for traditional securities and digital asset securities centers on the systems utilized in the clearing and settlement process, the procedures

(both automated and manual), as well as the overhead and personnel required. Clearance and settlement of traditional securities is complicated, time consuming, and is cost, infrastructure and labor intensive. It is highly dependent on a blend of new and legacy technologies, numerous interconnected entities and organizations, and continuous human/manual procedures related to redundancy and reconciliation that by default introduce some risk. While we have prepared a detailed comparison below, we believe it's important to note that after the execution of traditional securities transactions, they need to be reconciled at the broker dealer level, at the clearing firm level, and at the DTC level where they are ultimately settled by an exchange of securities for cash. Again, significant portions of the process are not automated and involve people entering data and/or comparing files, and as a result, settlement finality takes 2 days. Blockchain technology represents an elegant solution to many of the traditionally manual processes we have described herein.

In the traditional markets, data from many different sources is often manually combined and compared during reconciliation resulting in a critical inefficiency. In comparison, the use of a blockchain to clear and settle digital asset securities is based on self-executing protocols through smart-contracts, and simultaneous books and records updates via the ledger. As discussed herein, there are risks inherent in both systems, however, clearance and settlement of digital asset securities over a blockchain has significantly less risk because it greatly reduces the number of intermediaries involved, the exchange of redundant data and messaging, and removes the possibility of human errors. Ultimately ensuring faster and more accurate verification of transactions, identification of change in beneficial ownership, and clear and contemporaneous books and records of transactions and ownership.

Set forth in Section II(A) below is the typical life cycle of a trade in a traditional security. Section II(B) addresses clearance and settlement of a digital asset security on the blockchain. A summary table of the comparison of traditional clearance and settlement steps and the corresponding blockchain utility is attached as Appendix A hereto.

A. Traditional Clearance and Settlement Cycle

As acknowledged in the Proposal, traditional clearance and settlement (hereinafter, "TCS") is a multi-layered system of separate Participants (as defined herein) performing distinct essential functions for the transfer of beneficial ownership of traditional securities. Broker-dealers, clearing firms, and market centers ("Participants") work with each other and with transfer agents, the Depository Trust and Clearing Corporation ("DTCC") and the National Securities Clearing Corporation ("NSCC"), self-regulatory organizations ("SRO") and banks

throughout the clearing and settlement process to ensure settlement finality. Generally, the timeframe for complete clearance and settlement is trade date + two (2) days ("T+2").

An equity trade life cycle begins when an order to buy and/or sell a US equity security is submitted to a market center (e.g., exchanges, ATS) by a broker-dealer identified by its unique Market Participant Identifier ("MPID") as well as its unique DTCC number. The order is then matched, and the transaction is executed at which point, the market center sends confirmation of

the trade to the counter-brokers involved in the transaction via a proprietary API or messaging format or standardized electronic message protocol ("FIX"). Simultaneously, the market center sends a confirmation to the NSCC via NSCC's Universal Trade Capture ("UTC") system which "locks-in" the trade to the respective brokers by their DTC number. The broker-dealers then send the confirmations they receive to their clearing firms by FIX, as well as, sending an end-of-day ("EOD") file after the close of each trading day.

The transaction is then reconciled, cleared and settled amongst the Participants. During and after the trading day, clearing firms must perform trade reconciliation, and reviews of the trading activity executed by their correspondents. Clearing firms compare their real-time drop copies with EOD reports they receive from their correspondents, exchanges, ATS and the NSCC. Trade reconciliation involves extensive automated and manual labor. Processing systems compare the multitude of aforementioned files and generate alerts and reports. Clearing firm employees must then review these reports for errors, mismatches and other possible trade breaks. Trade breaks must be resolved manually by clearing firm employees by contacting the trade desks, executing brokers, other clearing firms and other market centers. Once a trade break is resolved, new trade data must be uploaded to the clearing firm's systems in order to update the records for correct reports to be submitted to DTCC and NSCC, custodian banks and broker-dealers for the account holders.

Book Entry Only ("BEO") is the accounting system that enables the DTCC to electronically transfer beneficial ownership records for traditional securities. As is the practice, DTCC holds the securities in its nominee name, Cede & Co, for the beneficial owner of the traditional security. The account holder's broker-dealer is responsible for tracking its customers, i.e., the beneficial owner's holdings in the customer's brokerage account.

This fragmented structure creates many points of potential failure and vulnerability. The lack of standardized technology between intermediaries and the high degree of human involvement exposes equities clearing and settlement to significant risk. As discussed below, smart contracts and the blockchain offer a more secure and efficient system for clearing and settling digital asset securities.

B. Clearing and Settlement on the Blockchain

Prometheum believes that settlement of digital asset securities must occur using appropriate and audited smart contracts and network verification in order to take full advantage of blockchain technology. Blockchain technology increases operational efficiency and provides

faster reconciliation, clearing and settlement cycles. The result is a more streamlined and effective path to custody finality, accurate and transparent record keeping, and direct auditing functionality.

1. Smart Contracts

Smart contracts are established to automatically enact a series of predetermined changes according to a technology protocol when a specific act occurs. Smart contracts are used in every

step of the digital asset security trade-cycle to verify the accuracy of information, ownership rights, trade details and the ultimate change in beneficial ownership with significantly less intermediaries and information redundancies than traditional securities clearing and settlement.

Smart contracts enforce protocols for automatically facilitating the transmission of shareholder communications, enforcement of blue-sky qualifications and required protections for jurisdictional limitations. They can also facilitate payment of interest or dividends electronically and enforce limits on trading for restricted securities.

Smart contacts mitigate settlement risks because: 1) no transfer/transaction can be completed without the seller meeting specific conditions established in the smart contract; 2) smart contracts execute without human interaction on the blockchain thereby eliminating intermediaries relaying different parts of trade information which, will result in less trade breaks; and 3) all trades settle on a same day basis.

2. System and Data Security

Current market infrastructure is centralized and is secured by utilizing advanced hosting facilities, security hardware and applications, redundancies, and backup systems. However, the very nature of the centralized system makes it extremely vulnerable to widespread harm through hacking, ransomware and other network attacks.

The blockchain's distributed nature eliminates the potential for a hack, ransomware or other attacks to bring down the whole network. Blockchain technology, governance models and consensus mechanisms have the potential to be substantially more secure than the current central database supported market infrastructure. Additionally, because most of the independent components and manual processes of the traditional securities model can be recreated as Participants or functions on a blockchain, a consistent level of defense can be maintained across the whole ecosystem

3. Operations Efficiency

Today, using blockchain technology, payments can be processed, and debits/credits applied within seconds. The T+2 settlement cycle is inefficient and archaic.

In connection with the post trade settlement process, a blockchain, even with some level of manual oversight, will streamline the current model. MultiSig Wallets are very good at providing secure settlement finality. Smart contracts allow for "intelligent" algorithms to automate clearing level reconciliation between exchanges and BDs.

4. Accurate Recordkeeping and Data Transparency

One of the most fundamental risks in the TCS process is the constant exchange of data being generated and transmitted between intermediaries for execution, reconciliation and recording of changes in beneficial ownership. This section outlines the inefficiencies and redundancies of the TCS process resulting in significant systemic risk.

A digital asset security on a blockchain is the solution to an efficient and accurate record of transactions. A blockchain is made up of distinct, sequential, and time-stamped records of asset ownership resulting from settlement ("Block"). The underlying distributed ledger technology, and smart contract verifications enforces the accuracy of each new Block consisting of the settled transaction and the previous Block. This technologically enforced sequential recordkeeping provides certainty that settlements recorded on a blockchain are accurate and independently confirmed in real-time by the network Participants. The network is responsible for updating the blockchain through the addition of new Blocks, the contents of which can be reviewed by Participants upon distribution, in real-time.

For each Participant, the copy of the blockchain provides data regarding the clearance and settlement status of the Participant's transactions and resulting securities and cash positions. Over time, this would allow each Participant to use the blockchain in lieu of maintaining a separate internal ledger. This has the potential to eliminate the need to reconcile differences in settlement records, either with trading counterparties, or with the omnibus position in an account at the clearing firm and/or at a central securities depository like DTC/NCSS.

Additionally, each Participant could allow its customers (including the end investors) to have direct and individually permissioned access to the blockchain. Thus, the beneficial owner of the security could rely on the blockchain's technologically enforced data for his/her positions. This accountability would eliminate DTCC's nominee holding practice. Moreover, investor access has the potential for enhanced investor protection as it would allow investors to independently confirm their ownership and possession of assets recorded to the blockchain.

5. Regulatory Reporting and Auditing Functionality

The data visibility and accuracy could also be extended to regulators for the fair and consistent enforcement of market rules and regulations. In the traditional securities model, Participants must provide daily reports, requested information, and real-time drop copies to regulators/self-regulatory organizations. Participants are also required to provide access to regulators for auditing purposes. The blockchain solves the transfer of mass volumes of data by using a read-only node on a blockchain. By building in such a node and utilizing a blockchain explorer, Participants can obtain direct uneditable data at any time and in real-time.

Ultimately, performing clearance, settlement and custody on a blockchain presents many clear advantages that allow for greater efficiencies, protections and less mistakes.

III. Proposal Question 7: What specific benefits and/or risks are implicated in a broker-dealer operating a digital asset alternative trading system that the Commission should consider for any future measures it may take?

Based on regulatory precedence, it is clear that only a registered broker-dealer can operate an alternative trading system, regardless of whether the asset traded is a traditional security or a digital asset security. A broker-dealer already has compliance requirements related to record keeping, customer protection, security, risk, AML/KYC, and financial stability. An ATS must meet all of these requirements, as well as maintain a fair and orderly market. Specifically, blockchain, and related technology like smart contracts, public/private key cryptography, and digital wallets can and should be adapted and used to the advantage of the capital markets. We firmly believe that broker-dealers will realize clear and important benefits from operating a digital asset alternative trading system. Clear and important benefits include, but are not limited to:

1. Faster settlement finality;
2. Immediate reconciliation;
3. Real-time balances;
4. Accurate short sell (stock loan/borrow);
5. Ability to always track stock locates on-chain;
6. Streamlined reporting;
7. Real-time auditing;
8. Lower fees;
9. Less overhead cost;
10. Decreased counterparty risk;
11. Eliminates need for central clearinghouse;
12. Eliminates need for NSCC to take on risk; and
13. Automated risk controls (pre-trade).

IV. Conclusion

In conclusion, we would like to thank the Commission for the opportunity to share our thoughts and provide comments on the Proposal. To reiterate, we strongly support the creation of the Special Purpose Broker-Dealer to custody digital asset securities, and believe it is a critical step towards incorporating digital assets into the capital markets. We firmly believe that blockchain represents the "next" technological evolution for capital markets, and that innovation must be compliant with the federal securities laws to ensure the security of investors and the markets.

Prometheum would welcome the opportunity to meet with the Commission to further contribute to the ongoing regulatory progress.

Sincerely,

Benjamin S. Kaplan
Co-CEO, Prometheum Inc.

Appendix A

Traditional Clearance and Settlement	Blockchain Clearance and Settlement
T+2 final settlement of transaction	Immediate and direct clearance and settlement
Multiple unique identifiers for each Participant entering securities transactions (e.g., MPID, DTCC number, etc.`)	Information provided to appropriate parties to be able to identify Participants is inherently digitally and automatically added to each side of the transaction.
Transaction terms creates a contract required to be verified and confirmed over T+2	The execution on the blockchain through the use of smart contracts is the final simultaneous verification and confirmation.
Correspondent/clearing firm relationship	Blockchain technology removes the need for separate verification of transactions amongst the multiple participants in the clearing process.
Multiple steps and messages between trade Participants for one transaction	Limited messages to post a transaction based on automated and real-time writing of transaction to the blockchain
Non-uniform messaging protocols	Uniform protocol on the blockchain
Clearing firm trade reconciliation based on reports from multiple entities and human review.	Smart contracts aggregate data from multiple parties and provide immediate and consistent outputs for reconciliation and other purposes based on pre-agreed and tested protocols.
Clearing firm must resolve trade breaks by humans contacting the multitude of trade Participants	Smart contracts execute transactions in digital asset securities by automating protocols for verification of the terms of the transactions prior to execution, preventing erroneous transactions.
Clearing firms regenerate corrected reports and disseminate to all trade Participants	The blockchain automatically retains all smart contract actions and serves as the standard basis for reporting.
Book Entry Only accounting records the change in beneficial ownership once a transaction is confirmed as settled and holds it in nominee name for the beneficial owner.	The blockchain is the real-time accounting system for smart contract verified digital asset transactions.

DTCC holds the traditional security in nominee name for the beneficial owner.	Digital asset securities are held in wallets that represent both the immediate custodian and the beneficial owner. The blockchain is the ultimate source of truth for beneficial ownership regardless of whether those digital asset securities are held directly by the beneficial owner or on their behalf.
Broker-dealers that hold beneficial owner accounts track the positions.	Beneficial owners typically access positions via their broker-dealer, but those positions are also verifiable via publicly viewable blockchain information.