MONTGOMERY SECURITIES

Montgomery Securities LLC
655 Montgomery Street, 7th Floor
San Francisco, California 94111

File No. S7-25-20

February 17, 2021
Security Exchange Commission 100F Street NE
Washington, DC 20549-1090
Regarding: Release No. 34-90788; File No. S7-25-20

Custody of Digital Asset Securities by Special Purpose Broker-Dealers

To the Commission:

You will be happy to know that this letter is actually in response to your request for comments regarding custody of digital asset securities and not to comment on the classification of XRP as a security.

We applaud the Commission's effort to consider the creation of Special Purpose Broker Dealers to custody digital asset securities so as to enable this innovation to be established and grow within the regulatory framework of US Securities law. It is our contention that innovation and regulation do not need to be viewed as opposites. However, we do believe that thoughtful consideration and implementation is appropriate. We strongly contend that technology is a vital component of the efficient functioning of capital markets. We also realize that technology could obviate the need for some processes or participants. Implementation of new technology needs to be done to minimize risks, maintain compliance with securities law and regulation, and expand access while protecting investors.

Response to Commission Request for Comments

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.

A public and private key is needed to send digital assets/digital asset securities from a digital wallet to another digital wallet. A public key is like your account number or user ID. Private keys are much like a password associated with a typical login user ID to access account. By providing a hosted wallet service, the broker dealer will manage the private keys for the client. The client will not have to set up a wallet to hold and Ethereum or other blockchain compatible wallet and therefore would not have the private keys in their possession. The BD will be in full control of the clients hosted wallet. The BD can then secure access to the account and funds with a traditional user ID and password, device confirmation, and 2-factor authentication commonly used by financial services firms. Further the BD would utilize a secure cold-storage technology to protect the customer's digital asset securities. The source of best practices would be to look how digital assets are now being secured by market leaders in that field such as Coinbase.

2. What are industry best practices to address events that could affect a broker-

dealer's custody of digital asset securities such as a hard fork, airdrop, or 51% attack? Please identify the sources of such best practices.

Events such as a hard fork, airdrop or 51% attacks that could affect a digital asset security would occur at the protocol level of the underlying blockchain. Using a permissioned blockchain and not allowing for airdrops would likely eliminate an the likelihood of any of these occurring. A hard fork occurs as the result of a consensus mechanism. A 51% attack would be the result of a corruption of the consensus mechanism which would create a conflict in the governance of the chain and probably a hard fork would occur as a result. One approach would be to use a permissioned blockchain that would eliminate forked chains and brue force attacks. Presuming you are utilizing a permissionless blockchain, performing diligence on the underlying protocol is an important step to determining the risks at the protocol level. Hard forks can occur for different reasons other than a 51% attack. In fact, the Ethereum chain has experienced hard forks as a result of network upgrades and the old chain is often abandoned with all historical transactions remaining in the new chain.

This would not affect the functioning of the smart contracts as they would continue to be processed on the whichever chain that they preferred. It would not alter the smart contract as it is using the underlying protocol to transfer ownership.

On the smart contract level, protections could be utilized that would require a delay of freezing of funds for a time period before they could be transferred. Furthermore, smart contract can allow securities issued or transferred as a result of fraud or by mistake could be restored to their rightful owner.

In the context of a digital asset security, it would be doubtful that air drops would be used as the issuance of shares for no consideration and would require traditional authorization of shares and issuer would have to issue the digital shares. I am unclear under what circumstances that they would want to issue shares for no consideration. An airdrop of the underlying protocol would probably be avoided by using a more reputable and established protocol that would be unlikely to utilize an airdrop.

Just as an existing exchange such as Coinbase or existing brokers would have requirement on which digital assets securities they would be willing to list, the same would be true of digital assets securities. Furthermore, digital asset securities would be subject to the same laws and regulations, by having member firms diligence issuers and the securities being offered, this would go a long way in protecting investors.

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?

Offline storage of private keys provides security against loss or theft. Additionally, storing

digital assets securities in different location geographically in safe deposit or vaults can provide another layer of protection. Sensitive data would be stored in "cold storage" or servers that would be disconnected from the internet. Data can then be split, redundant, encrypted and outputted to USB drives or printed. The USB drives and printed records can be store securely in vaults or safe deposit boxes distributed geographically.

All accounts will use 2 Factor Authentication such as an Authentication Application or physical Private Key (YubiKey). In addition to username and password, you will have to enter a code from your mobile phone to access your account.

Utilize payment industry best practice, all website traffic on encrypted SSL and wallets and private keys stored using encryption.

Employees must pass criminal background checks, separate password and 2FA for different devices and services. Employee's hard drives are encrypted, require strong passwords, and screen locking.

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

Similar to disclosing risk investing in digital assets and traditional securities currently in place. AltoIRA provides a list of risks associated with investing in digital assets. These risks could be tailored for digital assets securities; however some risks would not be relevant because digital asset securities do represent an obligation to pay or ownership rights in brick and mortar assets, at a minimum should include the following:

DIGITAL ASSET INVESTMENTS MAY LOSE ALL VALUE.
DIGITAL ASSET INVESTMENTS SUCH AS DIGITAL CURRENCIES MAY BE SUBJECT TO LEGISLATIVE AND REGULATORY CHANGES OR ACTIONS AT THE STATE, FEDERAL, OR INTERNATIONAL LEVEL WHICH MAY ADVERSELY AFFECT THE USE, TRANSFER, EXCHANGE, AND VALUE OF DIGITAL/CRYPTO ASSETS.

Other risks disclosures similar to risks related to private securities or alternative investments should include warning to investors that investments should be made using discretionary capital, not suitable for all investors, ATS trading digital asset securities have limited operating history, these investments maybe be illiquid. Risks should be disclosed regarding the possibility that trades could be irreversible, subject to hacking. Again, many of the major crypto exchanges and disclosures already made by existing member on unregistered securities can be a guide here to provide enough disclosure of the risks.

Further by allowing broker-dealers to custody digital asset securities it should reduce the risks from loss due to accidents or theft. It is also important to understand that digital asset securities

are not bearer instruments as the holder of record which could be the same as the owner are recorded so if shares were transferred illegally, they can be rectified at the issuer level.

5. Should the Commission expand this position in the future to include other businesses such as traditional securities and/or non-security digital assets? Should this position be expanded to include the use of non-security digital assets as a means of payment for digital asset securities, such as by incorporating a *de minimis* threshold for non-security digital assets?

Yes, the commission should expand this position in the future to allow for other business. Expansion to allow other business that include private placements, mergers and acquisitions and other non-custody related business would provide the member firm to generate more revenue and operate profitability rather than be restricted to digital asset securities as this market is nascent and relatively small. In order to gain the most benefit from digital asset securities, payment utilizing digital assets would enable instant settlement. While there may be a concern about volatility of the digital assets, the use of stable coins or a broker issued payment token would allow for instant settlement. The amount of non-security digital assets could be used in part for payment of commission and fees in addition to other fiat currencies. Perhaps some restriction on amounts or the digital assets that are allowed. Certainly allowing the use of Bitcoin and Ethereum would be welcomed and some would argue present minimal risk.

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?

While there are many differences. The main focus is on decentralization and having a more resilient financial system that is less susceptible to external shocks. Most trading today is now electronic, but the clearing and settlement is centralized. If there was a natural or manmade disaster that affect connectivity to the centralized depository institution this would severely affect the functioning of capital markets. Several custodial banks are also making changes to the payment side to realize full value of digital asset securities.

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?

Presuming that we are referencing and ATS that would only trade digital asset securities and not other digital assets. There are benefits to the broker-dealer, investors, issuers and regulators. By allowing a member firm to operate an ATS for the trading of digital asset securities, cost and efficiency are the primary benefits. Secondary benefits are the immutable registry of trades and pro-active regulatory safeguards such as smart contracts that can prevent trades from happening that violate the rules, regulations and laws. Ownership and outstanding shares would be much more accurate and more easily administered which would be beneficial to all

parties. Additionally, by reducing settlement time and having accurate holder and ownership records this can reduce the ability for shorts to outnumber shares in the market. Also, you should consider what are the benefits and risks from not allowing it. Far better to have empower member firms to innovate and improve capital formation, investing than to allow it to develop outside the purview of the regulatory environment by firms that believe that regulation and innovation do not have to be mutually exclusive concepts.

I believe that the benefits that digital asset securities far outweigh the risks. But you have the unenviable task of ensuring that application of technology does not cause unforeseen risks to investor and the efficient functioning of capital markets. I appreciate the opportunity to provide input and look forward to evolutionary change.

Sincerely,

J. Alfred Ritter
CEO
Montgomery Securities, LLC