September 19, 2018

Ms. Dalia Blass
Director
Division of Investment Management
U.S. Securities and Exchange Commission
100 F Street NE
Washington, DC 20549-1090

Re: Staff Letter: Engaging on Fund Innovation and Cryptocurrency-related Holdings

Dear Ms. Blass:

We are a group of blockchain and cryptocurrency industry professionals whose expertise and experience extends across the entire cryptocurrency space, with extensive experience in financial services, cryptography, and cryptoeconomics. We are responding to the Commission's Staff Letter, "Engaging on Fund Innovation and Cryptocurrency-related Holdings," dated January 18, 2018. Our intent is to assist the SEC by disclosing what we feel are critical considerations for handling cryptocurrency regulation that were not addressed in other comment letters previously made public by the SEC. Thank you for this opportunity for personal comment.

Our individual experience is as follows:

- Christopher Allen has been involved with cryptocurrency for 26 years, going back to working with DigiCash in the early '90s. He co-authored the TLS standard, which is responsible for securing the web and trillions of dollars of payments every year. He recently was Principal Architect at Blockstream and now is Executive Director of Blockchain Commons, a benefit corporation supporting critical internet security infrastructure.
- Bryan Bishop has since 2013 been a contributor to Bitcoin Core, the reference implementation of the Bitcoin system. From 2014 to 2018, Bishop worked to build out a software solution for digital currency custody at LedgerX, the first CFTC-regulated Bitcoin clearinghouse. Before that, Bishop worked on software development at various startups.
- Angus Champion de Crespigny jointly established the global blockchain team at Ernst & Young in 2014 and led their financial services blockchain and cryptocurrency strategy until his departure from the firm in August 2018. He has advised large enterprises, financial institutions, startups, regulators, and policy makers, both in the US and internationally. He has 11 years of experience in financial services across regulation, performance improvement, technology transformation, and cybersecurity.

- Gavin Fearey is an attorney with 17 years of corporate, investment funds, and regulatory compliance experience. He counsels fund managers and entrepreneurs in structuring transactions and navigating compliance issues, with a current focus on blockchain and cryptocurrencies. Gavin is Of Counsel with Winstead PC.
- Caitlin Long worked in the securities industry for 22 years, most recently as Managing Director and Head of Pension Solutions and Corporate Strategies at Morgan Stanley in New York. Her involvement with Bitcoin dates to 2012. She was chairman and president of Symbiont, a blockchain start-up, from 2016-2018, and is a gubernatorial appointee to the Wyoming Legislature's Blockchain Task Force.

Opinions in this letter are our own and should not be construed to be those of organizations with which we are affiliated.

We believe that digital assets are a unique asset class with unique strengths and abilities.

As a result of division of labor, any economy will over time develop services that assist savers in keeping their assets secure. The institution of third-party custody itself is about as old as civilization, with the earliest records dating back to 3,300 B.C.[1] We don't believe that the advent of digital assets will necessarily change this. That said, digital assets differ in material respects from traditional securities and other financial instruments. We believe that fitting them into existing market infrastructure introduces risks to investors that would not otherwise exist. In fact, it may be possible for market infrastructure to be updated to take advantage of Bitcoin and other technology, further strengthening the financial system.

While the value of third-party custody solutions was recognized and discussed early in the evolution of Bitcoin,[2] the Bitcoin protocol was developed with the specific intent of allowing individuals or entities to manage and move value without the need for an intermediary or trusted third party.[3] As a consequence, Bitcoin technology is security-hardened and built from the ground up to allow for granular, personal custody solutions. We suggest that policymakers and regulators look at the advantages of the available technology and incorporate them into the rules and regulations instead of solely relying on present-day rules and regulations that were developed for traditional assets.

The unique strengths of digital assets arise from the fact that they are individually controlled bearer instruments that are designed to settle gross and in near-real time within their own

[1] Jesus Huerta de Soto, "Money, Bank Credit, and Economic Cycles", pp. 40 - footnote on Babylon.

[2] E.g. see Hal Finney's comment on 12/30/2010: https://bitcointalk.org/index.php?topic=2500.msg34211#msg34211.

[3] See Satoshi Nakamoto, 2009: "With e-currency based on cryptographic proof, without the need to trust a third party middleman, money can be secure and transactions effortless." https://satoshi.nakamotoinstitute.org/posts/p2pfoundation/1/

settlement environments (namely, on their blockchain base layers). In many cases they offer improved transparency and stronger resilience relative to traditional securities.

We caution against applying rules to digital assets in ways which do not reflect their strengths.

As digital assets are bearer instruments developed for direct ownership, they are not designed to be commingled (in fungible bulk) in omnibus accounts. Additionally, being bearer instruments, they face much greater risk of theft than other assets traditionally used in exchange-traded products, most of which are (1) immobilized at a central securities depository, bullion bank, or warehouse, and (2) in the case of securities, issued in fungible bulk and therefore natively commingled from their inception. In contrast, digital assets are usually finite in number and have no lender-of-last-resort. This means that theft, failures to deliver, or other discrepancies with off-chain balances relative to on-chain assets (in timing or amount) create heightened potential for investor losses.

For these reasons, there are risks in applying the existing practices, rules and regulations pertaining to clearing, settlement, and custody to digital assets. Securities laws were initially written to apply to paper securities certificates, later adapted to book entry form, and now to digital representations of security entitlements recorded in centralized databases. They were not written with purely digital assets such as cryptocurrencies in mind.

Due to their bearer instrument nature, leading practices for digital asset custody should differ from traditional assets as follows:

(a) No commingling of digital assets in an omnibus account[4] by custodians would be the lowest-risk practice, owing to significant cybersecurity risks of commingling, despite the transaction cost efficiencies available from commingling. Digital assets are natively segregated, and maintaining this natural segregation at all times would best protect investors by conforming to the architecture of digital asset technology, thereby avoiding introduction of risks that would not otherwise exist. Commingling creates a "honeypot" for hackers to attack, and the ability of financial institutions to manage this security risk is likely to vary widely.[5]

[4] We are referring to assets stored in fungible bulk and no longer allocated to their individual owners on the ledger. For example, many digital asset platforms "commingle" unspent transaction outputs (UTXOs) when a client transfers BTC to the platform. The manner in which these UXTOs are secured and divided will vary by platform such as using one or more hardware wallets or by separate private keys on the same hardware wallet.

[5] NFA has been cognizant of commingling at digital asset exchanges, as reflected in mandated risk disclosures (in Interpretive Notice 9073):

> "Virtual currency exchanges generally purchase virtual currencies for their own account on the public ledger and allocate positions to customers through internal bookkeeping entries while maintaining exclusive control of the private keys. Under this structure, virtual currency exchanges collect large amounts of customer funds for the purpose of buying and holding virtual currencies on behalf of their customers. The opaque underlying spot market and lack of regulatory oversight

(The authors of this letter had deep discussions about this point and were not unanimous that cybersecurity risks always outweigh cost efficiencies,[6] which is why we encourage the SEC to seek the input of qualified engineers to gain the skills necessary to develop appropriate guidance and evaluate each ETF applicant's disclosures regarding their capabilities and operational risk management on a case-by-case basis. Similarly, it is essential that traditional financial institutions and any other new market entrants obtain significant input from qualified engineers about protecting the security of digital bearer instruments, particularly since few have needed to handle bearer instruments for decades and "trial by fire" is key to securing bearer assets that are digital.)

If one client's digital assets are to be commingled with the assets of another client in limited situations as permitted under the SEC's rules,[7] a custodian's public keys could be used for real-time monitoring of the omnibus account's coins (including potentially by the SEC itself) to ensure compliance with rules at all times and, in the case of an ETF, verify its net asset value (NAV). The appropriate parties to whom public keys are disclosed may differ depending on whether the product is an ETF or a private investment fund (for which perhaps public keys are disclosed only to administrators and auditors). Furthermore, "locktime" transactions can be provided by clearinghouses to recover assets in the event of loss of cryptographic keys at the clearinghouse.

Disclosure by the fund managers about whether and how it (or its custodian) will commingle or segregate the fund's digital assets would also be a leading practice. This is especially important if the fund manager intends to transact with the fund's coins at a custodial digital asset exchange, which requires the fund's custodian to turn over custody of the coins temporarily to

> creates a risk that a virtual currency exchange may not hold sufficient virtual currencies and funds to satisfy its obligations and that such deficiency may not be easily identified or discovered."

[6] Others have recognized the trade-offs between omnibus accounts and segregated accounts. For example, the Asia Securities Industry and Financial Markets Association (ASIFMA) outlines key advantages and challenges of each in its June 2018 report on Best Practices for Digital Asset Exchanges, available here. At least one author believes it should be a customer choice (if the risks are disclosed appropriately) whether to use a segregated account or one in which digital assets of a client are commingling with digital assets of other clients. That approach would be consistent with recent approaches taken by the CFTC, both generally with respect to Chairman Giancarlo's "do no harm" view on DLT and also on collateral rules for cleared swaps, which the CFTC has recently taken further steps to simplify pursuant to Project KISS.

[7] When custody is present, the custody rules under the Company Act and the Advisers Act currently permit the assets of one client to be commingled with the assets of other clients in limited situations (although they do not permit commingling of client assets and proprietary assets). For instance, Rules 17f-1 to 17f-7 under the Company Act apply different segregation and other custody requirements depending on the type of custodian and asset.

- § 270.17f-1 Custody of securities with members of national securities exchanges.
- § 270.17f-2 Custody of investments by registered management investment company.
- § 270.17f-3 Free cash accounts for investment companies with bank custodians.
- § 270.17f-4 Custody of investment company assets with a securities depository.
- § 270.17f-5 Custody of investment company assets outside the United States.
- § 270.17f-6 Custody of investment company assets with Futures Commission Merchants and Commodity Clearing Organizations.
- § 270.17f-7 Custody of investment company assets with a foreign securities depository.

Similarly, although registered investment advisers with custody are generally required to use a qualified custodian to keep funds and securities in a separate account under that client's name, the Advisers Act also permits the qualified custodian to maintain commingled accounts that contain only the clients' funds and securities, under the adviser's name as agent or trustee for the clients.

the digital asset exchange. In general, such digital asset exchanges commingle client assets and no information about their financial condition is publicly available.[8] The practice of turning over custody of coins to such exchanges temporarily, and the corresponding risks of doing so, should be clearly disclosed to investors.

(b) No building of *uncovered* exposures to digital assets via securities lending-type practices, even intra-day. To be clear, this leading practice pertains to *uncovered* exposures only, which means loans that are covered (100% collateralized) by on-chain coins are acceptable practice. The building of *uncovered* exposures can happen in many ways, including rehypothecation, margin lending at less than 100% margin, substituting collateral on bitcoin exposures with non-bitcoin collateral, naked shorting, or similar type of uncovered exposure that is less than 100% collateralized with on-chain coins at all moments, thereby giving rise to gap risk.

There are two reasons why we consider it a leading practice to avoid allowing *uncovered* exposures in digital assets to build. First, US GAAP accounting rules pertaining to collateral lending in certain instances[9] require multiple parties to report that they own the same asset at the same time, which means *uncovered* exposures can build ***undetected*** within the financial system. Auditors won't catch them at the financial institution level, and regulators will not be able to measure the degree of double-counting at a systemic level. This double-counting is a form of double-spending, and digital assets were designed to prevent this. Second, there is no lender-of-last-resort for most digital assets. This means any uncovered exposure is particularly risky to financial institutions exposed to it. "Failure to deliver" a digital asset is the same as a default. The bigger that an *uncovered* short position for a digital asset is allowed to build within the financial system, the bigger the solvency risk to exposed institutions in run-on-the-bank or certain hard fork scenarios.

Owing to the heightened risks involved with re-lending digital assets and the potential for accounting rules to obfuscate at an aggregate level how many times the same coin is owned simultaneously, if a fund (or any intermediary handling the fund's coins) intends to engage in coin lending, leading practice would be for the funds to disclose in detail their policies and risks with regard to coin lending and rehypothecation.

Finally, an optimal structure—-supposing the construction of appropriate infrastructure—would be for the fund to offer investors a choice to redeem their shares in the underlying digital asset

[8] Some digital asset trading platforms and exchanges offer custodial services to clients in which the client's digital assets are not commingled with the digital assets of other clients. In other words, each client has a different digital asset address, which is independently verifiable and auditable. Such custodial services are currently available only at a significant premium (for example, the initial setup fee was $100,000 for a fully segregated account), although this is likely to change over time.

[9] For example, uncovered exposures (i.e., multiple parties recording ownership of the same asset) arise when the transferee in a securities lending transaction or repurchase agreement sells the pledged collateral to a third party, resulting in both the third party (Party C) and the original transferor (Party A) reporting ownership of the same asset. For illustrations, see pp. 152-154 of this report: https://www.ey.com/publication/vwluassetsdld/financialreportingdevelopments_bb1921_transfers_26july2017/$file/financialreportingdevelopments_bb1921_transfers_26july2017.pdf, including footnotes detailing what happens when Party B sells pledged collateral to Party C, while Party A still reports ownership of the asset. As this situation repeats, the magnitude of uncovered exposures in the financial system builds undetected, since GAAP financial statements are not synchronized across all parties involved in a particular chain of collateral.

itself. This would help impose discipline to ensure *uncovered* exposures do not build within the financial system.

We should leverage the technology of this asset class to protect investors in ways not previously possible.

While the technology behind digital assets was created to enable individuals to control their own assets and for parties to trust the movement of those assets without confirming the identity of the counterparty, there are many additional features of the technology that leverage cryptography to achieve unique capabilities. As you know, multi-sig solutions provide control tools to ensure proper authority exists before coin transfers occur. In addition to multi-sig transactions, advanced cryptographic processes allow features for the safekeeping of assets such as the following:

1. Funds that are locked for a certain period of time, or until a particular condition is met, and
2. Proof of client holdings of digital assets, without exposing underlying digital asset balances.

Many other features are being researched and built to provide further flexibility and security to individuals and institutions that wish to manage these assets. By having these features embedded directly in the blockchain, much of the security that regulations seek to enforce through policy can be encoded at the asset level.

In other words, we can establish secure models for digital assets that protect both the investor and the solvency of major financial institutions without sacrificing the convenience and innovation that the asset class can provide.

Solutions in this space might be dependent on technology, not policy.

As we have outlined above, we believe that current SEC rules surrounding custody do not reflect the risks inherent in managing digital assets and do not use the technical strengths of the technology. These technical strengths have the potential to lead to a stronger, more robust custody environment. To better understand these possibilities, to build to strengths of technologies, and to not harm its advantages, we recommend that the SEC engage with those who are experienced with technology, such as cryptographic engineers, software developers, Bitcoin exchanges, smart-contract designers, blockchain developers, and existing digital-asset managers to ensure best practices are implemented.

In summary, best practices regarding custody of digital assets should incorporate some of these new technologies to achieve transparent, auditable and provably solvent funds. The new tools are in many ways better for this asset class than existing tools, and achieve the same goals without introducing risks that would not otherwise be there.

Best regards,

Christopher Allen
Bryan Bishop
Angus Champion de Crespigny
Gavin Fearey
Caitlin Long