Custody of Digital Assets: *Centralized* Safekeeping of *Decentralized* Assets under the Investment Advisers Act

December 17, 2018

Interest in cryptocurrencies and other digital assets on blockchains or distributed ledgers[1] has increased exponentially in recent years. The total market capitalization of cryptocurrencies and other digital assets on blockchains increased from slightly more than $17.5 billion in January 2017 to an all-time high of more than $813.5 billion in January 2018. While prices and market capitalization have dropped significantly since then, readings in the neighborhood of $135 billion as of late November 2018 still suggest significant, longer-term interest in digital assets for investment and other purposes.[2]

Debevoise & Plimpton

Significant uncertainties remain, however, in applying existing laws, regulations and practices to these digital assets. One area of significant concern is custody. Without a way to safely store and hold digital assets, institutional investors are often reluctant to make—and, in some cases, may be legally precluded from making—investments in this space.

Custody generally refers to the holding and control of an asset. What does it mean to have or retain custody of a digital asset? What practical concerns do investors in digital assets have regarding the custody and safeguarding of such assets? What legal obligations are imposed in the custody of digital assets? Do current methods of custody adequately address these legal and practical concerns?

---

1 A digital asset is, in essence, anything that exists in a binary format and comes with the right to use, the right to take possession of real world assets or certain other proprietary or contractual rights. Digital assets include (but are not limited to) digital documents, audible content, motion pictures and other relevant digital data, and recently emerged cryptocurrencies and other blockchain tokens that are currently in circulation or are, or will be, stored on digital appliances such as personal computers, laptops, tablets, electronic storage devices, mobile devices and any other apparatuses that exist now or in the future as technology progresses to accommodate the conception of new modalities able to carry those digital assets. The ownership of a digital asset is typically unique from, and independent of, the proprietorship of the physical device on which the digital asset is located. In this update, the term "digital asset" refers solely to such an asset that is recorded on a distributed ledger.

2 A global total market capitalization chart for cryptocurrencies is published by CoinMarketCap, *available at* https://coinmarketcap.com/charts/.

This paper focuses on these and related questions, with a particular emphasis on the custody requirements imposed on registered investment advisers under the U.S. Investment Advisers Act of 1940 (the "Advisers Act").[3]

In our view, current methods for the custody of digital assets can provide significant protections against third-party cyber threats and similar risks. However, it is not clear whether such methods address concerns arising from potential fraud on the part of an adviser, its employees or representatives.

Custody of Digital Assets

Custody generally refers to the possession and/or control of an asset. For physical assets (e.g., precious metals, artwork or bottles of wine), custody can be established by delivering physical possession of the asset to the relevant custodian. For certain intangible assets (e.g., uncertificated shares in a company), various mechanisms for custody have been developed through national laws and industry practices. For example, in many countries, a central securities depository holds legal title to publicly traded securities, with a series of custodians (or, in the United States, securities intermediaries) holding entitlements to such securities through a chain of entries on the books and records running from the central securities depository down to the last custodian facing the ultimate beneficial owners.

But what does it mean to have custody of *digital* assets? Digital assets are reflected on distributed ledgers in the form of binary digits (which represent a series of characters in decimal, hexadecimal or some other numeral system).[4] What a digital asset represents varies depending on the asset. Some digital assets like Bitcoins do not represent any real world assets, others represent the ownership of physical assets like a bushel of corn, and still others represent the right to use certain services like the right to execute smart contracts on a certain blockchain platform.

---

[3] We do not address the custody issues faced by registered investment companies under the Investment Company Act of 1940.

[4] More technically, in a typical distributed ledger, a digital asset itself is not represented on the ledger. Rather, the owner of an asset spends it by sending a transaction ("output transaction") to another person (or the recipient), and the recipient can spend such asset by claiming it by way of an input transaction in a new output transaction to be sent to another person. Each person on the ledger has its own digital identity (which is a public key of such person or, more frequently, a hash of such public key called an address). A public key is derived from a private key, which is created by using a digital signature algorithm. The owner of digital assets recorded in a specific address (or public key) can spend those assets by signing one or more output transactions involving such assets with the related private key. The private key is only known to the owner, preventing anyone else from accessing those digital assets.

It is helpful to review the mechanics of distributed ledgers. A digital asset on a particular ledger is recorded to an address (i.e., a hash of a public key) that is cryptographically derived from a specific private key. A public key is a digital identity of a person who controls the related private key, and the private key is necessary to claim and spend all digital assets associated with the related address (or public key). Therefore, the owner of digital assets must keep its private key to itself; otherwise, any other person who accesses the private key can spend those assets and, given the immutability of the distributed ledger system, those assets will not be recoverable by the owner. Control of the relevant private key thus is a paramount concern, and safeguarding the private key through secure custodial arrangements is a primary goal.

Hot and Cold Wallets

At the most basic level, an investor in digital assets could self-custody those assets. One way of doing so would be to maintain them online in a "hot" digital wallet for which the investor maintains the private key. This method is relatively easy and provides quick access for trading and transfer purposes, but it also is at a high risk of being hacked or suffering a similar cyber attack. It is also possible that the private key will be forgotten or lost, which may make it impossible for anyone—including the owner—to access the related digital assets.

Investors also use "cold" storage techniques for the private key, such as an offline hardware wallet. Some cold wallets are offline (or air gapped) except for limited time periods and, therefore, offer better protection than a hot wallet against cyber threats. But there is still a possibility for loss resulting from a cyber intrusion. Some cold wallets allow a wallet owner to sign a transaction while the wallet is offline and then go online to send the signed transaction, thereby avoiding exposure of the private key to the outside world. But as with "hot" digital wallets, the private key may be lost. In addition, the hardware wallet itself may be lost or damaged.

Third-Party Custodians

Alternatively, an investor can seek to use the services of a third-party custodian. A number of service providers have been established to safeguard digital assets and more are expected to enter the space. However, custody fees are currently high and services are generally limited to institutional and high-net-worth investors.

While there are variations, a typical current approach to third-party custody works as follows (using Bitcoin as an example):

- A customer owns 100 Bitcoins.[5]

- If the customer wants its 100 Bitcoins to be stored with a custodian with which it has entered into a contractual relationship, the customer sends an output transaction to an address designated by the custodian.

- Once the transaction is mined to be included in a block (which is confirmed by waiting for the customary six new blocks to be built on that original block in about 60 minutes), the custodian sends a transaction (with an input equal to the customer's output transaction to the custodian) to another address the custodian has established specifically for this customer.

- Once this second transaction is put on the blockchain and confirmed after about 60 minutes, the private key associated with this second address is put into cold storage (i.e., stored in a computer that is not connected to the internet and often maintained at a remote and secret location). The customer does not know the address or the private key associated with that address.

- If the customer later wants to transfer those 100 Bitcoins, the customer requests that the custodian retrieve the private key so that the custodian can sign the instructed transaction for the customer to spend those Bitcoins.

- The custodian will typically employ a procedure to verify the recipient and its control of the address to which the Bitcoins are being transferred. For example, this may involve a video conference with the recipient and a transaction involving a very small amount of Bitcoin (say one satoshi[6]) to be confirmed by the recipient at the time of receipt. Some custodians require all addresses of potential recipients to be pre-screened and whitelisted well before the customer desires to send Bitcoin transactions to them.

Some custodians automate the entire process, so that none of the initial storage and retrieval processes involve manual steps and, therefore, no employee of the custodian knows the private key generated for the customer.

---

[5] As noted above, the customer does not have an account on the blockchain showing the balance of Bitcoins owned. Rather, the blockchain contains one or more input transactions to the address of the customer, and, in this example, the aggregate amount of Bitcoins sent to that address adds up to 100 Bitcoins. The customer can spend all or some of those 100 Bitcoins by sending transactions signed with its private key. Other digital assets such as Ethereum are represented in an account on the Ethereum blockchain, but the approach remains the same with respect to such assets.

[6] One Bitcoin equals 100,000,000 satoshis.

This approach provides a number of useful safeguards against cyber attacks and the inadvertent loss of private keys. As we discuss in more detail below, however, this approach still has limitations, particularly with respect to protection against fraud in an investment advisory context.

It is also worth noting that introducing a third-party custodian as a trusted intermediary is inconsistent with a fundamental principle of distributed ledger technology. To distributed ledger purists, the custody fee is just a new type of rent that is being extracted by a trusted third party. In addition, from a practical viewpoint, the use of a third-party custodian creates a new risk for a "single point of failure" since it opens up the possibility of theft of the digital assets by a custodian's employee or loss resulting from destruction or other physical failure of the custodian's computer system or facility.

The SEC'S Custody Rule

Rule 206(4)-2 (commonly referred to as the "Custody Rule") under the Advisers Act establishes certain safekeeping requirements applicable to funds or securities held on behalf of clients by registered investment advisers.[7] Although the Custody Rule applies only to registered investment advisers, its concepts are relevant for nonregistered advisers and other intermediaries as well, since their clients or customers have a practical interest in assuring that managed assets are appropriately safeguarded and the absence of appropriate custody arrangements may preclude a client from investing with a particular adviser.

Scope of the Custody Rule

On its face, the Custody Rule applies to the custody of client "funds or securities." Digital assets can be characterized in a number of ways. The U.S. Securities and Exchange Commission (the "SEC") has taken the view that many digital tokens, particularly those issued in so-called initial coin offerings, constitute securities under U.S. federal securities laws.[8] Almost certainly, these types of security tokens would fall within the scope of the Custody Rule.

---

7 17 CFR 275.206(4)-2.

8 See, e.g., Jay Clayton, SEC Chairman, Statement on Cryptocurrencies and Initial Coin Offerings (Dec. 11, 2017), *available at* https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11; *In the Matter of Munchee Inc.*, SEC Release No. 33-10445 (Dec. 11, 2017) (cease and desist order), *available at* http://www.sec.gov/litigation/admin/2017/33-10445.pdf.

However, the SEC has stated that, in its view, Bitcoin and other pure virtual currencies are not regarded as securities under U.S. federal securities laws.[9] But could Bitcoin constitute "funds" under the Custody Rule? To date, the SEC has not provided any clear guidance on this question.[10] However, from a policy perspective, it is difficult to distinguish Bitcoin and other virtual currencies from other types of securities or funds held for clients, particularly when those virtual currencies are being held for investment purposes. Because of that—and the heightened level of regulatory scrutiny being placed on digital assets—it is certainly possible that the SEC would take the view that Bitcoin and other virtual currencies (whether held for investment or as a monetary substitute) are the equivalent of "funds" as contemplated by the Custody Rule.

Purposes of the Custody Rule

While appropriate custody arrangements can guard against inadvertent loss or theft by third parties, another key purpose of the Custody Rule is to protect against fraud or misconduct on the part of an adviser or its employees or representatives. In adopting amendments to the Custody Rule in 2009 in the wake of the Madoff scandal, the SEC noted:

> We believe these amendments…will provide for a more robust set of controls over client assets designed to prevent those assets from being lost, misused, misappropriated or subject to advisers' financial reverses. We acknowledge that no set of regulatory requirements we could adopt will prevent all fraudulent activities by advisers or custodians. We believe, however, that this rule, together with our examination program's increased focus on the safekeeping of client assets, will help deter fraudulent conduct, and increase the likelihood that fraudulent conduct will be detected earlier so that client losses will be minimized.[11]

So, broadly speaking, custody through an independent third party might be viewed as providing (or at least seeking to provide) three key protections:

---

[9] See, e.g., William Hinman, Dir., SEC Div. of Corp. Fin., Remarks at the Yahoo Finance All Markets Summit: Digital Asset Transactions: When Howey Met Gary (Plastic) (Jun. 14, 2018), *available at* https://www.sec.gov/news/speech/speech-hinman-061418; CryptoCoinNews (CCN), "SEC: ICO Tokens Should Be Regulated as Securities, Not Bitcoin" (Apr. 27, 2018), *available at* https://www.ccn.com/sec-ico-tokens-not-bitcoin-should-be-regulated-as-securities/ (summarizing a portion of testimony by SEC Chairman Jay Clayton on April 26, 2018 before the Financial Services and General Government Subcommittee of the House Committee on Appropriations).

[10] In a slightly different context, Dalia Blass, Director of the SEC's Division of Investment Management, issued a letter on January 18, 2018 (*available at* https://www.sec.gov/divisions/investment/noaction/2018/cryptocurrency-011818.htm) raising questions regarding custody of cryptocurrencies held by registered investment companies (i.e., mutual funds). This suggests that the SEC is actively considering how cryptocurrencies and other digital assets fit within the rules and practices relating to asset custody.

[11] SEC Release No. IA-2968 (Dec. 30, 2009), *available at* https://www.sec.gov/rules/final/2009/ia-2968.pdf.

- Protection against theft or misappropriation by third parties
- Protection against bankruptcy or insolvency of the adviser or custodian (by segregating the assets and identifying them as being held on the client's behalf)
- Protection against fraud, theft or misappropriation by the adviser itself

Summary of Custody Rule Requirements

Unless certain exceptions apply (which may make all or part of the Custody Rule inapplicable to certain securities or in certain situations), an investment adviser that is registered or required to be registered under the Advisers Act must comply with certain requirements if it has custody of client funds or securities.[12] Among those requirements are the following:[13]

Qualified Custodian

Funds or securities of which the adviser has custody must be maintained by a "qualified custodian." The assets must be maintained either (i) in a separate account for each client under that client's name or (ii) in accounts that contain only the adviser's clients' funds and securities, under the adviser's name as agent or trustee for the clients.

Each of the following is a "qualified custodian" under the Custody Rule:

- Certain banks and savings associations[14]

---

[12] Even in the case of traditional assets, the question of whether an investment adviser has custody of client assets can itself be complicated. In general, custody by an investment adviser means (i) the holding of client funds or securities, directly or indirectly, or (ii) having the authority to obtain possession of client funds or securities. For example, an adviser has custody where it has possession of client funds or securities or has power of attorney to sign checks on a client's behalf, to withdraw funds or securities from the client's account (including fees) or to otherwise dispose of a client's assets for any purpose other than trading activity authorized by the client. The general partner of a pooled investment vehicle is also deemed to have custody of the pool's assets by virtue of its capacity as general partner because such status "gives [the general partner]…legal ownership of or access to client funds or securities." See 17 CFR 275.206(4)-2(d)(2); see also the SEC investor bulletin entitled "Investor Bulletin: Custody of Your Investment Assets" (Mar. 1, 2013), *available at* https://www.sec.gov/investor/alerts/bulletincustody.htm. In addition, the SEC staff has identified arrangements that might provide the investment adviser with "inadvertent" custody of client assets in situations where neither the adviser nor the client believed that the adviser had custody. See IM Guidance Update entitled "Inadvertent Custody: Advisory Contract Versus Custodial Contract Authority," *available at* https://www.sec.gov/investment/im-guidance-updates.html.

[13] See 17 CFR 275.206(4)-2(a).

[14] Specifically, this includes banks as defined in section 202(a)(2) of the Advisers Act and savings associations as defined in section 3(b)(1) of the Federal Deposit Insurance Act that have deposits insured by the Federal Deposit Insurance Corporation under the Federal Deposit Insurance Act. Section 202(a)(2) of the Advisers Act defines a bank to include, among others: (A) a banking institution organized under the laws of the United States or a Federal savings association (as defined in section 1462(5) of title 12 of the U.S. Code (Banks and Banking)),

- Registered broker-dealers holding client assets in customer accounts

- Registered futures commission merchants holding client assets in customer accounts (but only with respect to client funds and security futures or other securities incidental to transactions in contracts for the purchase or sale of a commodity for future delivery and options thereon)

- Foreign financial institutions that customarily hold financial assets for their customers, provided that the foreign financial institution keeps the advisory clients' assets in customer accounts segregated from its proprietary assets[15]

Notice to Clients

Notice must be provided to clients if an account is opened with a qualified custodian on a client's behalf.

Account Statements

The adviser must have a reasonable belief that the qualified custodian is sending account statements to the client at least quarterly.

Verification and Surprise Audit

The funds and securities held in custody must be verified at least once during any calendar year, generally by an independent public accountant. The examination and verification must be at a time chosen by the accountant without prior notice or announcement to the adviser or the custodian and must be a time that is irregular from year to year.[16]

(B) a member bank of the Federal Reserve System, and (C) any other banking institution, savings association (as defined in section 1462(4) of title 12 of the U.S. Code) or trust company, whether incorporated or not, doing business under the laws of any State or of the United States, a substantial portion of the business of which consists of receiving deposits or exercising fiduciary powers similar to those permitted to national banks under the authority of the Comptroller of the Currency which is supervised and examined by State or Federal authority having supervision over banks or savings associations and which is not operated for the purpose of evading the provisions of the Advisers Act. 15 U.S.C. 80b-2(a)(2). The Federal Deposit Insurance Act defines a savings association as including: (A) any Federal savings association or Federal savings bank chartered under section 1464 of title 12 of the U.S. Code, (B) any State savings association (which includes any building and loan association, savings and loan association, homestead association or cooperative bank (other than a cooperative bank that is treated as a State bank) which, in each case, is organized and operating according to the laws of the State in which it is chartered or organized), and (C) any corporation (other than a bank) that the Board of Directors and the Comptroller of the Currency jointly determine to be operating in substantially the same manner as a savings association. 12 U.S.C. 1813(b)(1).

15 See 17 CFR 275.206(4)-2(d)(6).

16 The base requirements under the Custody Rule can differ when clients are private funds. For example, an adviser to a private fund or similar pooled investment vehicle is not subject to the notice and account requirements, and is deemed to have satisfied the surprise audit requirement with respect to a fund that is subject to an annual audit if: (i) the fund sends its audited financial statements, prepared in accordance with

Practical Impact and Considerations

In order to broaden their potential client base, certain digital asset custodians have actively sought to take steps to establish "qualified custodian" status. For example, many of them have acquired existing trust companies or broker-dealers or taken steps to establish a state-chartered trust company or broker-dealer.[17] However, a number of practical difficulties surrounding the custody of digital assets still need to be overcome:

- **Limits on Scope of Custody Services**. Unlike typical broker-dealer arrangements, where one security is readily tradable for another security or cash and the proceeds of a transfer or sale can be received and held by the broker-dealer in the brokerage account on a "payment versus delivery" basis, digital asset custodians now typically only provide for custody of a limited range of digital assets. They may or may not have the capability or desire to hold cash for a client. They almost certainly will not agree to hold any and all digital assets in which a client may choose to invest.

- **Audit Difficulties**. It remains to be seen whether typical independent accountants will be willing to provide the surprise audits required by the Custody Rule. Some accounting firms have taken an active interest in the digital asset space. But a custodian may be very reluctant to expose a private key to accountants, and accountants may not be able to confirm that a private key held by a custodian actually represents an ownership interest in the particular underlying digital asset. Unlike typical investments in securities and debt instruments, there are no registrar records, trusted securities intermediaries, trusted counterparties, administrative agents or other traditional sources of ownership verification. Verifying ownership of digital assets may require technical expertise and knowledge that traditional accounting firms may not have at their disposal.

---

generally accepted accounting principles, to each limited partner (or member or other beneficial owner) at least annually within 120 days of the end of the fund's fiscal year, (ii) the fund's audit is conducted by an independent public accountant that is registered with (and subject to regular inspection as of the commencement of the professional engagement period and as of each calendar year-end by) the Public Company Accounting Oversight Board in accordance with its rules, and (iii) the fund is subject to audit upon liquidation and, in such case, distributes its audited financial statements, prepared in accordance with generally accepted accounting principles, to each limited partner (or member or other beneficial owner) promptly after the completion of such audit.

[17] See, e.g., Ben McLannahan, "Wall Street starts to dip its toes in crypto" (Aug. 13, 2018), *available at* https://www.ft.com/content/db5a20ea-9ca1-11e8-9702-5946bae86e6d; Kate Rooney, "Companies race to solve bitcoin's security problems despite slumping prices" (Sep. 13, 2018), *available at* https://www.cnbc.com/2018/09/13/companies-race-to-solve-bitcoins-custody-problem-despite-slumping-prices.html.

Adviser Fraud Risk

Current custody methods can provide significant protections against hacking and other cyber threats involving third parties as well as the inadvertent loss of private keys. But it is not clear that such methods will satisfy the key current objective of the Custody Rule: to provide substantial protections against adviser fraud or misappropriation of assets.

A custodian of digital assets primarily serves as a secure storage point for those assets. However, when providing custody for assets managed for an investment vehicle or other ultimate client by an investment adviser, the custodian basically acts at the instruction of the adviser. If the adviser wants to transfer digital assets out of custody and does so in accordance with established procedures, the digital assets can leave the custody arrangement without cash or other replacement assets being simultaneously received by the same custodian ("delivery versus payment"). Transfers of digital assets can occur almost instantaneously, and an adviser or a third party may be able to abscond with digital assets or the proceeds thereof in quick order. The SEC staff, in other contexts, has raised questions concerning custody arrangements that do not provide for delivery versus payment.[18]

It is possible, of course, that digital assets that are traced back to a fraudulent transaction can later be flagged or blacklisted in some manner, which may limit trading of those assets going forward. No digital exchange or broker will conduct transactions with digital assets that originate from or have been traced to a flagged or blacklisted address. Similarly, an institutional investor or high-net-worth investor will likely engage in chain analysis in order to avoid digital assets traced to such address.

However, this approach has several potential shortcomings. Innocent recipients of the proceeds of the fraudulent transaction (i.e., those who had no knowledge that the original digital assets were misappropriated) may suffer harm. More importantly, even if an adviser who stole investor assets is unable to spend those assets, the assets will not be recoverable by the investor unless the adviser provides the private key of the

---

[18] See, e.g., IM Guidance Update entitled "Inadvertent Custody: Advisory Contract Versus Custodial Contract Authority," *available at* https://www.sec.gov/investment/im-guidance-updates.html ("An adviser's authority to issue instructions to a broker-dealer or a custodian to effect or to settle trades does not constitute 'custody.' Clients' custodians are generally under instructions to transfer funds (or securities) out of a client's account only upon corresponding transfer of securities (or funds) into the account. This 'delivery versus payment' arrangement minimizes the risk that an adviser could withdraw or misappropriate the funds or securities in its client's custodial account.") In addition, the SEC staff, in the course of examinations, has asserted that the investment adviser had "custody" of client assets because the adviser had the ability to sell and purchase assets—loans—that are traded on a basis other than delivery versus payment. See The Loan Syndications and Trading Association, "Bank Loan Trades and Custody of Client Assets" (Jul. 12, 2017), *available at* https://www.lsta.org/news-and-resources/news/bank-loan-trades-and-custody-of-client-assets.

blacklisted address. This approach also may not be a significant deterrent to a large theft by an adviser, who can quickly exchange digital assets for cash and abscond with the cash before any custodian, investor, digital asset exchange or other buyer has knowledge of any wrongdoing.

Possible Solutions

Solving for adviser fraud risk will require additional thought and evolution in the digital asset custody industry. We summarize a few possible developments below, although there is substantial potential for variations on these concepts or the development of completely different solutions.

- **Expansion of the Custodian Role**. In order for digital assets and the proceeds from them to be maintained consistently in a custodial account, custodians will need to expand the list of digital assets that are available to be held in custody and will need to hold cash. Once it is realistically possible to permit the flexibility for active trading of assets within the custodial account, a custodian may develop methods that would permit such trading to occur on a basis equivalent to "delivery versus payment," with digital asset proceeds directed to the same custodial account and cash proceeds directed to the cash account of the customer or directed by the custodian to be delivered to a related cash custody account or brokerage account. Possible methods that would permit trading of assets within the custodial account include:

  - **Custodian as Broker**. A custodian could act as the equivalent of a broker in digital assets. Basically, the custodian would locate trades through exchanges or other brokers based on buy or sell instructions provided by the adviser client, execute those trades and collect a commission or spread. This is similar to custody bank services used in foreign exchange trades.[19]

  - **New Custodian System Technologies**. Technologies could be developed that would permit traders to access and effect trades on the custodian's system subject to the proceeds settling into wallets and cash accounts maintained by the custodian. For example, trading employees of the adviser might have a limited "private key" generated by the custodian's system that provides access to only a specified subset of digital assets and that is linked to an instruction set that requires proceeds to be delivered to the same or related wallet on the custodian's system or the cash account at the custodian or designated bank or broker-dealer.

[19] See, e.g., "The Custody Services of Banks" (Jul. 2016), The Clearing House, *available at* https://www.theclearinghouse.org/advocacy/articles/2016/07/20160728-tch-issues-white-paper-on-custody-services-of-banks.

However, such an approach might raise an issue of whether the assets are maintained at the custodian.

- **Adviser-Side Solutions**. Advisers, working in conjunction with custodians, may also be able to implement additional safeguard procedures designed to give institutional investors, as well as the SEC, increased comfort regarding the protection of client assets. There may be practical difficulties with such procedures, including potential delays in effecting timely trades. But such procedures may give institutional investors the additional assurance that they require to make substantial investments in the digital asset space. For example:

  - **Digital Asset Investor Committee**. An adviser to a commingled investment vehicle could establish a Digital Asset Investor Committee, which would sign off when instructions are provided to a digital asset custodian to transfer assets out of the custodial account. Depending on adviser needs and investor demands, this approval process could work in a variety of ways. One possibility would be for an actual formal conference call meeting to take place with a member of the Digital Asset Investor Committee before a proposed transfer occurs, with an authorized representative of the committee then serving as one required sign-off signature for the custodian. Alternatively, this committee might consist of an identified list of significant independent investors, with the signatures of a member (or some subset of members) required for sign-off with the custodian. However, this solution assumes that the address of the recipient must also be approved by the committee or one or more designated members, which may not be practical given the nature of cryptographically generated addresses.

  - **Enhanced Reporting and Auditing**. An adviser could voluntarily adopt special reporting and/or auditing procedures for digital assets. These procedures could include arrangements for more frequent surprise audits by specialized, independent accounting firms that have developed the necessary expertise. They could also include detailed reporting on digital asset holdings to investors generally or to a subset of investors (such as a Digital Asset Investor Committee). While these procedures in themselves may not reduce the potential for adviser fraud or misappropriation significantly, they would provide investors with increased transparency and, potentially, enable the earlier detection of fraudulent activities.

  - **Multiparty Custody Arrangements**. It may be possible for advisers and multiple custodians to enter into a coordinated set of custody arrangements, including digital and other assets. For example, if one digital asset custodian supports only digital asset X and another supports only digital asset Y, and the adviser wants to sell X for Y, a signature and destination address provided by a representative of

the second custodian (as well as the adviser) might be required by the first custodian for a transfer that results in proceeds being delivered outside of the first custodian's custodial account. Similarly, if the proceeds are cash or another form of a security, the signature and destination account information of an agreed bank or broker-dealer might be required by the first custodian. There are obvious limits to this approach, as it may not be possible to get all the necessary custodians lined up with this arrangement (though perhaps the agreement could provide for joinder of additional custodians over time).

Conclusion

Currently available solutions for digital asset custody are expensive and may not adequately address certain risks, such as the risk of fraud or theft by an adviser managing pooled assets or the risk of theft by the custodian or its employees. The risk of rogue employees of the custodian stealing digital assets held in custody is likely mitigated by the selection of well-known custodians, by custodians providing fully automated processes or by the requirements around qualified custodians under the Custody Rule and by common law principles holding an employer responsible (at least under certain circumstances) for the acts of its employees.

The risk of theft by an adviser or its employees is more difficult to address based on current methods of digital asset custody. We have discussed some possible solutions, but none are perfect and there may be limits to their practicality. It remains to be seen, however, whether further technological developments will solve the issue and if a workable tradeoff—and one acceptable to the SEC—can be struck between security and efficiency.

At a more fundamental level, the application of current rules around custody of traditional assets simply may not be consistent with distributed ledger technology. After all, one of Satoshi Nakamoto's goals in creating blockchain and other distributed ledger-based assets was to eliminate reliance on trusted third parties. An owner of such digital assets is expected to safeguard such assets solely by way of cryptography at the transaction and asset level and by relying on the network consensus mechanism at the ledger level. Use of a trusted custodian goes against the very basic premise of distributed ledger technology and introduces a new type of trusted third party, creating a potential single point of failure and promoting rent-seeking and other issues Satoshi Nakamoto set out to eliminate. If an investor relies on a third party adviser for digital asset investment and provides that adviser with investment discretion over such assets, yet another trusted third party will be added to the ecosystem, further compounding the problem.

The application of the Custody Rule and equivalent concepts, perhaps combined with related, evolving solutions, may provide a basis in the near term for increased investment in digital assets by institutional investors. But it is ultimately difficult to square these concepts with the core focus on decentralization. If the developers and users of blockchains and related digital assets continue to emphasize decentralization, it is difficult to predict the evolution of the space over time. But it is at least possible that we might see an increase in the use of advisers who provide digital asset investment advice for a fee but who do not control the digital assets of clients. This avoids issues around adviser risk and the need to introduce trusted intermediaries. But it does require a certain level of sophistication of such clients and an increased focus by such clients on secure self-custody methods.

* * *

Please do not hesitate to contact us with any questions.

WASHINGTON, D.C.

Kenneth J. Berman
kjberman@debevoise.com

NEW YORK

Byungkwon Lim
blim@debevoise.com

Gary E. Murphy
gemurphy@debevoise.com