Blogs
August 23, 2018
Why Blockchain Custody Is So Difficult—Paths Forward?

In the first post on this topic, we provided a simple answer to a question posed by the Director of the SEC's Division of Investment Management (the "Division"):

> To the extent a fund plans to hold cryptocurrency directly, how would it satisfy the custody requirements of the 1940 Act and relevant rules?"

Our simple answer was to treat cryptocurrencies as "financial assets" under Article 8 of the Uniform Commercial Code. In the second post, we explained how this simple answer may be hard to implement when it comes to trading cryptocurrencies, because their markets require trades to settle in the next block. Thus, rather than a custodian implementing a portfolio manager's instruction to settle a trade, a portfolio manager trading a cryptocurrency will normally need to have immediate control over the transfer of the cryptocurrency, which is inconsistent with the custody requirements of the Investment Company Act of 1940 (the "1940 Act"). In this post, we consider three potential solutions to the dilemma faced by an investment company that must hold cryptocurrency in compliance with the custody requirements of the 1940 Act while allowing its adviser to trade the cryptocurrency.

Magic

The first approach would be a technological solution, which may as well be magic from an attorney's perspective. Any custodian of cryptocurrency must develop some means for various employees to use the custodian's private keys to generate the cryptographic "signatures" used to validate blockchain transfers. While this could involve giving certain employees access to the private keys, a safer course may be a system that generates signatures from private keys that the system maintains internally. In other words, an employee would provide terms for a trade to the system, which would return a signature valid for only that trade without disclosing the private key used by the signature. If such a system could be designed for internal use, it might be possible to extend it to the custodian's customers. Customers would designate traders authorized to enter into cryptocurrency transactions on the customers' behalf. The custodian would give designated traders access to its system, which would generate signatures for only the cryptocurrency maintained in the accounts over which the traders have trading authorization. Traders would use the signatures to execute trades that would settle in wallets maintained by the custodian, so custody would be maintained by the custodian throughout the trading process.

Become a Cryptocurrency Dealer

The second approach would follow the model currently used for spot foreign exchange trading. The custodian would operate as a dealer in cryptocurrencies. Customers could ask the custodian to purchase or sell cryptocurrencies on their behalf. The custodian would find the other side of the trade at a trading platform or through other cryptocurrency dealers, and charge a spread or commission to its customers for the trades. This approach presupposes that the custodian wants to go into the business of being a cryptocurrency dealer, which would raise a raft of risks and issues, but it would not require technological magic to fulfill the 1940 Act's custody rule requirements.

Self-Custody

Rule 17f-2 under the 1940 Act—the third approach—is misleadingly referred to as the "self-custody" rule. The designation can be misleading insofar as the rule requires investments to:

> be deposited in the safekeeping of, or in a vault or other depository maintained by, a bank or other company whose functions and physical facilities are supervised by Federal or State authority."

So, the rule still requires the fund to maintain investments at a custodian. Rule 17f-2 nevertheless treats an investment company as having custody of these investments whenever "the directors, officers, employees or agents of such company are authorized or permitted to withdraw such investments upon their mere receipt" and imposes certain safekeeping requirements. Our thought is that a fund's adviser could create a trading wallet for the fund, transfer some of the fund's cryptocurrency from the custodian to the trading wallet, execute trades and then transfer the cryptocurrency received back to the custodian. Transferring cryptocurrency to the trading wallet would be a withdrawal upon "mere receipt," so the fund would need to comply with Rule 17f-2. Rule 17f-2 may not apply neatly to cryptocurrencies. For example, the rule would require the trader withdrawing or depositing cryptocurrency to sign a notation recording the date, time and amount withdrawn or deposited, the purpose of the withdrawal and how the deposited cryptocurrency was acquired. The notation would also need to record the name of any person to whom cryptocurrency was delivered from the trading wallet. Cryptocurrency trading platforms generally provide only the public key of the other party to a trade, so there is no way to discover that party's name. Therefore, a fund adviser proposing to take this approach should consider discussing its plans for complying with Rule 17f-2 with the Division's staff before opening a trading wallet.

Conclusion

Treating cryptocurrency as a "financial asset" under Article 8 provides a crisp legal answer to the question of how a securities intermediary can establish custody of cryptocurrencies. But it leaves a myriad of operational and collateral legal questions unanswered. Nevertheless, we believe this approach would be a useful first step toward addressing the questions raised by the Division regarding proper custody of cryptocurrencies and other blockchain assets.

Explore more in

Investment Management