



Circle Internet Financial, LLC

99 High Street
Suite 1701
Boston, MA 02110

May 8, 2023

Submitted electronically to rule-comments@sec.gov.

Secretary Countryman
Securities and Exchange Commission
100 F Street NE
Washington, D.C. 20549

Re: File Number S7-04-23 (Proposed Rule on Safeguarding Advisory Client Assets)

Dear Ms. Countryman,

Circle Internet Financial, LLC (“Circle”) appreciates the opportunity to comment on the Securities and Exchange Commission’s (SEC) proposed rule regarding Safeguarding Advisory Client Assets. Circle supports the SEC’s goals in the proposal as they pertain to the cryptoasset industry: it believes that the proliferation of best practices for cryptoasset custody will protect investors, increase confidence in the cryptoasset industry, and keep investment activity in this generational technology inside of the United States. In this letter, Circle provides background information and recommendations for how the SEC can finalize the rule in a way that most effectively accomplishes its outlined goals.

As a financial infrastructure company, Circle is deeply invested in technology that enables the secure, reliable, and robust safekeeping of assets for all entities, including Registered Investment Advisers (RIAs). Among Circle’s many activities, it is a leading provider of cryptoasset custody solutions using proprietary multi-party computation (MPC) technology and a unique, distributed risk and responsibility model to allow businesses to access the benefits of cryptoassets in a secure way. It also issues USD Coin, the largest U.S.-regulated payment stablecoin. Circle is commenting on the SEC’s proposal in its capacity as a provider of secure cryptoasset custody technology. Circle is not an RIA, nor is it a qualified custodian.¹

¹ Circle does own an SEC-registered broker-dealer through its business subsidiary SI Securities LLC (dba SeedInvest), but it does not offer custody of assets, including cryptoassets, through SeedInvest.

I. Executive Summary

While the benefits of cryptoassets extend far beyond their possible use as investments,² Circle believes that U.S. investors would benefit from being able to receive investment advice on their cryptoasset investments from an RIA and that the custodial protections offered by qualified custodians will provide important protections to investors in the entire cryptoasset ecosystem. Circle's comments focus on the application of the proposal to the cryptoasset industry and the unique operation of financial services provided via public blockchains.

First, Circle encourages the SEC to ensure that the final rule is workable with a diverse and expansive universe of qualified custodians for cryptoassets. The SEC should finalize the rule as proposed and explicitly affirm that state-chartered banking organizations may continue to serve as qualified custodians. Additionally, the SEC should eliminate the conflict that Staff Accounting Bulletin No. 121 presents to the ability for banking organizations to provide cryptoasset custody. This will ensure that RIAs and their clients have access to high-quality custody services for their assets.

Next, Circle explains that cryptoasset custodians using industry best practices can maintain "possession or control" of cryptoassets, as defined by the proposal, but only if the SEC defines the term in line with reasonable commercial standards. Advanced technology, such as Circle's MPC technology, combined with rigorous operational controls and practices, means modern cryptoasset custody has similar risks and assurances as does the storage of any other digital item of value, such as book-entry securities recorded electronically. Provided the SEC defines "possession or control" to a reasonable standard, cryptoasset custodians can satisfy the proposed requirement.

Finally, Circle encourages the SEC to clarify that RIAs will be able to take advantage of the benefits of public blockchains under the final rule. In particular, market participants may have questions about the permissibility of exchanging cryptoassets on protocols that do not require pre-funding, such as smart contract protocols, which enable the simultaneous settlement of cryptoasset trades. Circle believes that transactions which settle simultaneously are compatible with the rule as proposed and reduce risk for investors. RIAs will also need clarity as to whether

² See, e.g., Stellar Development Foundation, *UNHCR launches pilot Cash-Based Intervention Using Blockchain Technology for Humanitarian Payments to People Displaced and Impacted by the War in Ukraine*, UNHCR, Dec. 15, 2022, <https://www.unhcr.org/ua/en/52555-unhcr-launches-pilot-cash-based-intervention-using-blockchain-technology-for-humanitarian-payments-to-people-displaced-and-impacted-by-the-war-in-ukraine-unhcr-has-launched-a-first-of-its-kind-int-eg.html>; or Marina Lammertyn, *Chileans Take Refuge in Stablecoins Amid Economic Turmoil*, CoinDesk, Aug. 3, 2022, <https://www.coindesk.com/business/2022/08/03/chileans-take-refuge-in-stablecoins-amid-economic-turmoil/>. See also *Circle Responds to a U.S. Treasury Department Request for Comment on the Cause and Benefits of Stablecoin Mass Adoption* (Aug. 10, 2022), <https://www.circle.com/blog/circle-responds-to-a-u.s.-treasury-department-request-for-comment-on-the-cause-and-benefits-of-stablecoin-mass-adoption>, full response available at <https://www.regulations.gov/comment/TREAS-DO-2022-0014-0181>.

they will be permitted to direct their qualified custodian to encumber assets in a smart contract for the purposes of achieving investment return in line with their client agreements. Circle believes that encumbering assets in a smart contract is compatible with the rule as proposed, provided certain conditions are met, and it encourages the SEC to make this explicit in the final rule.

II. When finalizing the rule, the SEC should ensure that there exists a diversity of firms that can effectively provide safe crypto-asset custody services to RIAs.

Circle supports the SEC's goals in proposing the Safeguarding Rule, and it supports the expansion of the scope of assets covered by the rule to include cryptoassets.³ To maximize the positive benefit of the Safeguarding Rule, however, the SEC must ensure the final rule is workable. If RIAs are not able to obtain qualified custody services, then they will not be able to offer investment advisory services to their clients. This will not protect investors, who will likely continue to purchase cryptoassets with or without advice, so the SEC should ensure that RIAs can provide qualified custody services through a sensible regulatory framework.

The SEC should also ensure that there is a diversity of well-qualified custodians that can provide cryptoasset custodial services to RIAs. A diverse, competitive market of qualified custodians will drive down costs, encourage high standards, and make it easier for investors to obtain secure custody services. This is especially true for the nascent cryptoasset industry, where qualified custodians still vigorously compete on features, price, and other client services.

A. The SEC should finalize the rule as proposed as it pertains to the kinds of financial institutions that qualify as qualified custodians, and it should make explicit that state-chartered trust companies may serve as qualified custodians.

Circle agrees with the SEC's approach in the proposed rule, which does not make any changes to the high-level types of entities that may serve as qualified custodians.⁴ The SEC should finalize the rule as proposed and allow state-chartered trust companies to serve as qualified custodians.

Licensed, state-chartered trust banks are market-leading custodians that provide secure, reliable custody for the largest asset classes in the United States. For example, the Depository Trust Company, a New York State trust company, retains custody of a diverse range of securities valued at \$87.1 trillion and underpins the vast majority of U.S. capital markets.⁵ Bank of New York Mellon, a venerable and foundational U.S. custodian that owns a New York State trust company, holds

³ Safeguarding Advisory Client Assets, 88 Fed. Reg. 14672 (Mar. 9, 2023) (proposing to amend 17 C.F.R. 275.206(4)-2), at 14677.

⁴ *Id.* at 14683.

⁵ DTCC, *About DTCC - The Depository Trust Company (DTC)*, <https://www.dtcc.com/about/businesses-and-subsidiaries/dtc> (last visited Apr. 14, 2023).

\$43 trillion of assets in custody.⁶ Investors in U.S. capital markets have for decades trusted these organizations, the state financial regulations and supervisor that oversee them, and the bankruptcy-remote business practices of the custodians under their state banking law. Circle supports the SEC's proposed account requirement, and it expects that state banking organizations will be able to meet it.⁷

For the cryptoasset space specifically, Circle believes it is important for the SEC to continue to permit state banking organizations to provide qualified custody given that best practices for cryptoassets can change quickly, and state financial regulatory regimes overseeing custody are generally well positioned to adapt to innovation while still maintaining high standards. For example, the State of New York approved the first state-chartered trust company for cryptoasset custody in 2015.⁸ For national banking organizations, the Office of the Comptroller of the Currency (OCC) first promulgated guidance about the permissibility of cryptoasset custody in 2020.⁹ The regulatory and supervisory standards for cryptoasset custodians are equally as stringent, if not more so, under the best state financial regulators (e.g., New York state) as they are for traditional markets, but states can adapt more quickly and are better-suited to update standards to accommodate the latest advancements in cryptoasset custody. The SEC will best protect investors if it promulgates rigorous minimum standards (i.e., the proposed rule and existing state financial regulations) while simultaneously empowering custodians to use the best tools available for cryptoasset custody.

B. The application of SAB 121 for bank regulatory capital treatment means that well-qualified banking organizations are functionally unable to provide crypto-asset custody services to RIAs.

⁶ BNY Mellon, *BNY Mellon Launches New Digital Asset Custody Platform*, Oct. 11, 2022, <https://www.bnymellon.com/us/en/about-us/newsroom/press-release/bny-mellon-launches-new-digital-asset-custody-platform-130305.html>.

⁷ See *supra* note 3 at 14683, proposing to add a new requirement that bank or savings associations “hold client assets in an account that is designed to protect such assets from creditors of the bank or savings association in the event of the insolvency or failure of the bank or savings association” in order to qualify as a qualified custodian. Because of the variability in and unsettled nature of state bankruptcy laws, the SEC should make clear that the proposed requirement for banks to hold client assets in such an account is not intended to categorically prohibit state banking organizations from qualifying as qualified custodians. It may also consider providing additional clarity that so long as the entity itself takes all reasonable steps to structure the account as proposed, the bank or savings association may qualify as a qualified custodian.

⁸ Reem Nasr, *NY grants first banking license to bitcoin exchange itBit*, CNBC, May 7, 2015, <https://www.cnbc.com/2015/05/07/ny-grants-first-banking-license-to-bitcoin-exchange-itbit.html>.

⁹ Interpretive Letter 1170 (July 22, 2020), <https://www.occ.gov/topics/charters-and-licensing/interpretations-and-actions/2020/int1170.pdf>. The OCC placed Interpretive Letter 1170 under review in the summer of 2021 but later affirmed the legal analysis. See Anna Hrushka, *OCC will revisit crypto charters, interpretive letters, acting chief says*, Banking Dive, Jun. 3, 2021, <https://www.bankingdive.com/news/occ-will-revisit-crypto-charters-interpretive-letters-acting-chief-says/601228/>; and *OCC Clarifies Bank Authority to Engage in Certain Cryptocurrency Activities and Authority of OCC to Charter National Trust Banks*, Office of the Comptroller of the Currency, Nov. 23, 2021, <https://www.occ.gov/news-issuances/news-releases/2021/nr-occ-2021-121.html>.

Absent the regulatory requirement to do so, some RIAs currently use qualified custodians to hold their clients' cryptoassets. However, while SEC-reporting banks can nominally serve as qualified custodians, they have effectively de-risked themselves from crypto custody activity because of the potentially unintended consequences of SEC Staff Accounting Bulletin no. 121 (SAB 121). SAB 121 expresses the staff view that SEC-reporting entities should reflect their obligations to safeguard crypto-assets for customers on their balance sheets as a liability with a corresponding asset.¹⁰ For banking organizations, this quasi-requirement has extraneous effects on their regulatory capital requirements. In particular, cryptoassets held on a bank's balance sheet generally require an equal dollar amount in Tier 1 capital to protect against potential losses.¹¹ Because of these burdensome capital requirements, banks – many of which would likely offer industry-leading custodial services – have decided against offering cryptoasset custody services to the market.

This unfortunate interplay between investor protection rules and prudential banking regulations leads to two outcomes that ultimately harm investors. First, it may create an unequal playing field where SEC-reporting banks are disadvantaged relative to privately-held banks. Banks are generally not required to hold regulatory capital to offset custodial market, liquidity, and credit risks because assets held in custody are not owned by the bank. However, because SEC-reporting banks must report cryptoassets held in custody on their balance sheets, SEC-reporting banks may need to hold additional regulatory capital to offset those risks. This treatment of cryptoassets would result in asymmetric business incentives between SEC-reporting banks and non-SEC-reporting banks that could ultimately reduce competition in, and availability of, custodial services.

Second, it limits the ability of some banking organizations to provide high-quality custody to customers, including RIAs. As is evident in the design of the Safeguarding Rule, banks are important and reliable providers of custody services to investment advisers and others. When banks are precluded from providing their custody services for a specific asset class, investors in that asset class are worse off.

The interaction of SAB 121 with bank regulatory capital requirements inadvertently harms investors. For the final Safeguarding Rule to be workable and most effectively protect investors, the SEC should resolve this conflict and coordinate with the banking regulators to ensure comprehensive clarity in the obligations applying to banks in providing cryptoasset custody services to their clients.

III. Modern cryptoasset custody practices are analogous to custodial practices for other assets. The SEC should make clear that the proposed definition of “possession or control” permits means of custodying cryptoassets that are as secure, or more secure, than traditional means of custodying other assets.

¹⁰ See Staff Accounting Bulletin No. 121, 87 Fed. Reg. 21015 (Apr. 11, 2022).

¹¹ See *Prudential treatment of cryptoasset exposures* (Basel Committee, Dec. 2022).

A. Cryptoasset custody has matured past basic implementations of private key protection.

To maintain “possession or control” of an asset held by a qualified custodian under the proposal, the qualified custodian is required to participate in any change in beneficial ownership of that asset.¹² In the context of an asset secured cryptographically on a public blockchain, this would require the qualified custodian to effectuate the change by signing each transaction using the private key securing that cryptoasset. It would also require the qualified custodian to ensure that no other entity has the full private key material.

The Commission notes that it may be challenging for a qualified custodian to demonstrate possession or control of a cryptoasset to this standard.¹³ For the most basic implementation of cryptoasset custody — storing and protecting the private key in full and unified form — this may be the case. However, key management and custodial practices have evolved significantly for cryptoasset businesses, and these newer practices allow custodians to ensure, to any reasonable standard, that no other entity has the private key material.

Circle’s custodial solution (called Circle Vaults) combines MPC technology with a proprietary operational system which it calls the Distributed Risk and Responsibility (DRR) model. In short, Circle’s MPC technology independently generates individual components of a single private key (referred to as “key-shares” or “shards”) which never exist on the same infrastructure. Because the key-shares are stored, in encrypted form, on physically and logically separate servers, an attacker would have to compromise multiple different physical premises and computer networks to gain control over the complete private key. The encryption algorithms Circle uses (AES-256, RSA4096, Elliptic Curve Cryptography, and others) are employed by the U.S. military and national security apparatus; one of the techniques (AES-256) is the only publicly accessible cipher approved by the U.S. National Security Agency (NSA) for securing top secret information.¹⁴ When a Circle Vault user wishes to make a transaction, proprietary cryptography enables each key-share to contribute to a single signing event. The DRR model is an equally important operational requirement that further reduces the risk of unauthorized access. At a high level, the DRR model includes custom cryptographic protocols, virtual secure enclaves that prevent data leakage, intrusion detection systems, and other tools to ensure the security of customer assets.¹⁵

B. Cryptoasset custodians can ensure that their participation is required for a change in beneficial ownership, fulfilling the proposed definition of “possession or control,” but only if the SEC finalizes the definition in line with reasonable commercial standards.

¹² *Supra* note 4, at 14687.

¹³ *Supra* note 4, at 14688 - 14689.

¹⁴ *Data at Rest Capability Package* (National Security Agency, Jan. 2018).

¹⁵ To clarify, Circle does not offer qualified custody itself; instead, Circle provides software that businesses can set up with a qualified custodian or on their own physical and computer systems.

When cryptoassets are held with the rigor of Circle Vaults, the risks of unauthorized access are similar to the risks associated with the storage of any other high-value digital record subject to significant cybersecurity protections, such as the record of a primary dealer’s account balance at a Federal Reserve bank or the record of an investor’s ownership of book-entry securities. In fact, because of the rigor of the encryption Circle Vaults uses, the risks are almost certainly smaller. Custodians of these electronic records provide the same assurances that cryptoasset custodians do, such as: that the records are accurate; that there has not been unauthorized access to the record-keeping system; and that the custodian has adequate systems in place to detect changes to records and attempts at unauthorized access.

Using Circle’s technology, then, a custodian can demonstrate beyond reasonable concern that no other party can gain control over the private key material required to sign a blockchain transaction. As a result, Circle believes that its custody solutions would enable a qualified custodian to meet the possession or control requirement as proposed. The SEC should clarify in its final rule that if a qualified custodian takes all steps in line with reasonable commercial standards to prevent the unauthorized access of cryptoasset private key material, and if the qualified custodian is required to participate in any change in beneficial ownership of that asset, the SEC would consider the custodian to have exclusive possession or control of the cryptoasset.

Analogously, while an attacker could theoretically hack the systems of a U.S. central securities depository (CSD) and change ownership records without detection, it is exceedingly unlikely. U.S. CSDs are not required to prove that such a hack *has not occurred* because such assurances would be impossible to provide. Likewise, custodians of cryptoassets should not be required to prove the impossible, i.e., that no one has compromised cryptography that is used by the U.S. national security community to resist nation-state attacks. Instead, they should only be required to prove that they have taken all steps in line with reasonable commercial standards to prevent unauthorized access of cryptoasset private key material.

Providing this clarification in the final rule would require the U.S. cryptoasset investment advisory industry to use rigorous and secure business practices to hold clients’ cryptoassets in custody. Steps in line with reasonable commercial standards to prevent unauthorized access of private key material could include:

- eliminating single points of failure that could lead to the unauthorized transfer of funds, i.e., by using MPC technology for asset custody;
- following National Institute of Standards and Technology (NIST) best practices for generating entropy and minimizing data leakage when generating private keys;¹⁶ or

¹⁶ See, e.g., Meltem Turan et al., *Recommendation for the Entropy Sources Used for Random Bit Generation*, NIST, Jan. 2018, <https://csrc.nist.gov/publications/detail/sp/800-90b/final>.

- obtaining System and Organization Control (SOC) 1 and 2 certifications for the operational processes and controls of the qualified custodian.¹⁷

However, even as the SEC seeks to ensure that RIAs are holding client assets in a secure way, it should finalize the rule in a technology neutral way that permits RIAs to use modern innovations to keep assets safe. As such, the SEC should not prescribe the use of specific technologies or standards, especially because the crystallization of formal government or industry standards may lag technological development by a decade or more.¹⁸

Separate from the regulatory requirements proposed by the SEC, market participants already seek custodial solutions that provide protection against unauthorized transfer of funds, accurate account statements, and liability for error. The cryptoasset market has already evolved to provide the assurances considered by the SEC such as a demonstration that the custodian's participation is required to effectuate any change in beneficial ownership. Finalizing the rule as Circle recommends will produce a workable framework for secure, reliable cryptoasset custody that will protect U.S. investors and permit them to access investment advice for the cryptoasset investments they seek to make with or without advice.

IV. The SEC should provide clarity about how the proposed Safeguarding Rule will allow for the beneficial usage of public blockchains by Registered Investment Advisers.

- A. Simultaneous settlement facilitated by smart contracts reduces investor risk and is compatible with the safeguarding rule as currently proposed.*

In response to Question 53, Circle understands the term “atomic settlement” to commonly mean the *simultaneous* exchange of assets during a trade. Akin to modern Delivery-Versus-Payment (DVP) and Payment-Versus-Payment (PVP) processes across the financial system, atomic settlement ensures that the transfer of underlying assets occurs if, and only if, all assets are transferred between counterparties together. In the blockchain context, atomic settlement refers to transactions that occur simultaneously within the same “block,” i.e., a set of valid transactions

¹⁷ The SOC 1 certification focuses on financial processing controls and the security of the technologies that support them. The SOC 2 certification focuses on information security and technology controls that ensure the confidentiality, availability and integrity of systems. Both certifications are routinely provided to customers and regulators to show that a company is committed to protecting customer assets and to demonstrate the robustness of a controls program. For more information, see, e.g., *SOC for Service Organizations: Information for Service Organizations*, American Institute of CPAs, <https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/serviceorganization-smanagement> (last visited Apr. 14, 2023).

¹⁸ For example, the first efficient post-quantum cryptographic solutions emerged in the late 1990s, and cryptographers have been improving the solutions over the past 20 years. However, because it takes time to develop official standards, NIST only standardized quantum secure cryptographic algorithms last year. See *NIST Announces First Four Quantum-Resistant Cryptographic Algorithms*, NIST, Jul. 5, 2022, <https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms>.

that are being added to the blockchain/ledger at the same time. Importantly, because the transactions occur in the same block, which is the only method by which the blockchain's ledger can change, there is no point at which one leg of a transaction can settle while another does not — true simultaneous settlement.

Circle recommends the Commission clarify that exchanging assets through blockchain-based smart contracts would at no point result in a qualified custodian losing possession or control of assets, provided the trades settle atomically. When a blockchain transaction settles atomically, there is no point during which the RIA's qualified custodian would not have possession of the RIA clients' assets. The RIA never needs to transfer the assets to an entity that is not a qualified custodian, such as a centralized cryptoasset exchange; instead, the transaction settles atomically within the same block. While centralized cryptoasset exchanges may require pre-funding of trades that would not be compatible with the proposal's requirement for RIAs to hold assets with a qualified custodian, RIAs should still be able to exchange cryptoassets through smart contracts that enable atomic, simultaneous settlement.¹⁹

Simultaneous settlement has been recognized as a way to reduce counterparty risk and settlement failure. The SEC itself acknowledged the benefits of using DVP settlement in the original Custody Rule, noting that “(a DVP) arrangement minimizes the risk that an investment adviser could withdraw or misappropriate the funds or securities in its client’s custodial account.”²⁰ More broadly, the Global Foreign Exchange Committee has called for market participants to move to PVP trades whenever possible, and it has codified this requirement into its FX Global Code with the support of the Bank for International Settlements’ Basel Committee on Banking Supervision.²¹ By clarifying that exchange of cryptoassets through simultaneous settlement would be compatible with the rule as proposed, and by highlighting that such DVP systems better protect investors, the SEC could reduce investor risk while maintaining its high standards for asset custody.

B. The SEC should clarify that it would consider cryptoassets deployed within blockchain smart contracts by a qualified custodian to be in the possession or control of the qualified custodian, provided certain conditions are met.

RIAs are empowered to maximize returns for their clients, subject to their client agreements. Some RIAs seek to achieve this by interfacing with blockchain smart contracts that create economic incentives.²² To do this under the rule as proposed, RIAs would direct their qualified custodian to encumber client cryptoassets into smart contracts and to un-encumber the assets

¹⁹ See *supra* note 4, at 14689.

²⁰ Custody of Funds or Securities of Clients by Investment Advisers, Release No. IA-2176 (Sept. 25, 2003), n. 10.

²¹ Marc Glowka and Thomas Nilsson, *FX settlement risk: an unsettled issue*, BIS Quarterly Review (Dec. 2022), https://www.bis.org/publ/qtrpdf/r_qt2212i.pdf.

²² Blockchain smart contracts use economic incentives to incentivize good behavior, liquidity provision, and other services. Profit-seeking entities can capture these economic incentives to earn return for themselves or their clients. See, e.g., Raphael Auer et al., *The Technology of Decentralized Finance*, Jan. 2023, <https://www.bis.org/publ/work1066.pdf>, at 13 describing incentive mechanisms in lending protocols.

subsequently. The SEC should clarify that when qualified custodians encumber cryptoassets in a smart contract, and the smart contract meets the conditions described below, the cryptoassets would still be deemed to be in the possession or control of the qualified custodian. The conditions should be:

- the smart contract source code is published and verified.²³
- the source code of the blockchain on which the smart contract is deployed is published and verified;²⁴
- assets committed to the smart contract are only able to be released by the key that committed them; and
- the commit/release mechanism for the smart contract is not upgradeable.²⁵

These conditions could be verified by an RIA or by a qualified third party, such as a professional auditing firm or a credit rating business.²⁶ When these conditions are met, the RIA and its qualified custodian have perfect information about the economic incentives and operation of the blockchain smart contract, and the qualified custodian's participation will still be required to effectuate a change in beneficial ownership. RIAs regularly encumber their clients' assets through legal contracts to maximize potential investment return for their clients. For example, an RIA might commit certain client positions as collateral for a margin position. An RIA encumbering assets in a blockchain smart contract is similar to an RIA encumbering assets through a legal contract: in both situations, the RIA has the opportunity to conduct due diligence on the terms of the arrangement and the likely outcome to which the terms will lead, based on various exogenous events. And if the conditions detailed above are met, the contract terms will not change.

Some market participants may have questions about whether this behavior is permissible under the rule as proposed because the financial value of the client position may decline. While the financial value of the client's position may fluctuate depending on market conditions (just like the market value of any other client position in widely traded stocks or bonds may fluctuate), this is

²³ It is customary for public blockchain developers to publish the source code of smart contract protocols for public inspection, which has well-documented benefits for safety and innovation. Secondly, the most widely-used blockchains enable on-chain verification of the open source code against the compressed "bytecode" of the smart contract deployed on the blockchain. As such, investment advisers, or any other party, can review the published source code, understand how it works, and then verify that the code matches the actual smart contract deployed on the blockchain. For more information, see Zubin Pratap, *What Are ABI and Bytecode in Solidity?*, Chainlink Blog (Aug. 17, 2022), <https://blog.chain.link/what-are-abi-and-bytecode-in-solidity>.

²⁴ It is also customary for blockchains to publish the codebase of the blockchain. The published code can be verified against the actual operation of the blockchain by running a blockchain node.

²⁵ Developers may maintain the ability to upgrade certain parts of a smart contract to respond to market conditions (e.g., adjusting which cryptoassets may be encumbered in the contract). However, they may leave other parts of the smart contract non-upgradeable to instill confidence in the software, protect users, or for other reasons. Provided that the commit/release mechanism for the smart contract is not upgradeable, the qualified custodian's participation will remain a condition precedent to any change in beneficial ownership of client cryptoassets. For more information see Mobin Hajizadeh, *Upgrading Smart Contracts*, Ethereum Foundation (Apr. 3, 2023), <https://ethereum.org/en/developers/docs/smart-contracts/upgrading/>.

²⁶ Some firms' full-time business is to audit blockchain smart contracts. The function would also be very similar to the credit risk ratings for corporate obligations offered by certain firms.

investment risk and distinct from the question of whether assets are properly held in custody under the proposal. The qualified custodian's participation is still required to effectuate a change in beneficial ownership because it is the entity that commits the cryptoassets to the smart contract, and it is the only entity that can release the assets from the contract. As such, this method of achieving return for clients is compatible with the rule as proposed, and the SEC should clarify that this would be the case in the final rule.

V. Conclusion

Circle appreciates the SEC's work to create a rigorous, workable framework for custody of investor assets, including cryptoassets. Circle supports the SEC's goals in proposing the Safeguarding Rule and proposals including the expansion of the rule to include cryptoassets, among other client positions. It believes that the Safeguarding Rule will protect investors, increase confidence in the cryptoasset industry, and keep investment in this generational technology inside of the United States. As the SEC finalizes the rule, it should pay attention to unintended effects that would lead to investor harm as described above. Circle appreciates the SEC's consideration and welcomes opportunities for future engagement.