

Custody of Digital Assets

*Wulf A. Kaal^{1**} & Hayley Howe*

Abstract

The custody of digital assets plays an essential role in the evolution of the digital asset industry. Fully compliant legal custody solutions for digital assets increase legal certainty and mainstream investor confidence which, in turn, helps build markets in digital assets. Once digital asset markets evolved, self-custody solutions help increase the decentralization of the digital asset market. This article examines the evolving custody solutions for digital assets.

Key Words: Custody, Digital Asset, Emerging Technology, Legal Certainty, Supply, Demand, Tokens, Blockchain, Distributed Ledger Technology

JEL Categories: K20, K23, K32, L43, L5, O31, O32

^{1**} Professor of Law, *University of St. Thomas School of Law (Minneapolis, USA)*

Table of Contents

I.	2	
II.		3
1.		6
2.		12
a)		15
b)		17
III.		18
1.		19
2.		22
3.		28
IV.		31

I. *Introduction*

The growing consumer interest in digital assets and the digital asset market evolution² has triggered an avalanche of custody needs for digital assets. Custody of digital assets has become an increasingly pressing issue for the evolution of the digital asset market. Key custody providers, such as BitGo,³ are becoming increasingly important players in the digital asset market. The institutional digital asset market is partially consolidating around custody solutions through mergers.⁴

Workable custody solutions are important for the proliferation of digital asset uses in the existing financial markets. The importance of workable custody solutions in the digital asset market can be traced back to the needs of institutional investors. Custody solutions increase digital asset ownership accessibility by increasing investor confidence that their assets are secure. Without the ability to rely on proven custody providers, mainstream and legacy institutional investors are restrained from making digital asset investments for legal and / or business reasons. The majority of digital asset custody providers and digital asset exchanges are requiring customers to surrender digital asset ownership in order to get access and trade. State and federal laws are evolving to allow more institutionalized custody services for retail customers. However, institutional custody solutions are still developing.

² See, e.g., COINMARKETCAP, coinmarketcap.com (last visited Oct. 5, 2021); DEFI PULSE, defipulse.com (last visited Oct. 5, 2021) (showing growth data for digital assets accelerating over 2020 Q3-2021Q3).

³ See BITGO, bitgo.com (last visited Oct. 5, 2021) (BitGo provides wallet, qualified, and self-managed custody services for institutional investors and service providers as well as digital asset insurance).

⁴ See Kevin Reynolds, Galaxy Digital to Buy BitGo for About \$1.2B in Stock, Cash, COINDESK.COM (May 5, 2021), <https://www.coindesk.com/markets/2021/05/05/galaxy-digital-to-buy-bitgo-for-about-12b-in-stock-cash/>.

Despite the proliferation of custody solutions, users' self-custody of digital assets is key for the decentralization of emerging blockchain networks. In other words, the more digital assets are held by their owners in self-custody, the less likely intermediation of custody service providers becomes.

The article evaluates the tension between self-custody and custody solutions by emphasizing the particular regulatory requirements that custody solutions need to comply with.

II. *Custody of Assets*

The term custody is generally used to describe ownership, possession, and / or control of funds or assets. For tangible physical assets, such as real estate or chattel, custody of the asset can be established through physical possession. In other words, the owner of an asset can surrender possession and control of the asset to a custody provider. In the intangible digital asset context, the transfer of custody over such an asset is less clear. Custody of digital assets is typically associated with ownership and control over a digital asset wallet and its assets. Such ownership and control over a digital asset wallet typically means holding the private keys and the responsibility of keeping funds safe.⁵

In traditional assets, "Custody" is a broader term that may involve all aspects of bank services performed for customers in relation to items they are holding for them (i.e., processing, settlement, fund administration).⁶ A national bank is permitted to escrow encryption keys used in connection with digital certificates,⁷ provide secure

⁵ Binance Academy, *Crypto Security 101*, BINANCE BLOG (Dec. 12, 2018), <https://www.binance.com/en/blog/279914390447808512/Crypto-Security-101-co-Binance-Academy>.

⁶ Jonathan V. Gould, Interpretive Letter #1170 Re: Authority of a National Bank to Provide Cryptocurrency Custody Services for Customers, OFFICE OF THE COMPTROLLER OF THE CURRENCY, 1, FN 23 (Jul. 22, 2020) <https://www.occ.gov/topics/charters-and-licensing/interpretations-and-actions/2020/int1170.pdf> [hereinafter OCC Letter 1170].

⁷ *Id.* at 6 (citing Julie L. Williams, *Conditional Approval #267 January 1998*, OFFICE OF THE COMPTROLLER OF THE CURRENCY (Jan. 12, 1998),

web-based document storage, retrieval and collaboration of documents and files containing personal information or valuable confidential trade or business information.⁸

For traditional assets, the custody business developed from safekeeping and settlement services provided to customers for a fee.⁹ Historically, traditional community banks served the local community through safeguarding customer deposits and lending to neighbors and small businesses.¹⁰ National banks have long provided safekeeping and custody services for a wide variety of customer assets, including both physical objects and electronic assets.¹¹ “Safekeeping” implies the basic service of a bank holding on to an asset for a customer (e.g., gold or securities).¹² An asset may be held in physical form at one of the custodian’s premises, a sub-custodian facility, or an outside depository.¹³ Custodian banks provide trusted gateways for customers to trade in regulated securities and commodities markets.”¹⁴

Traditionally, financial institutions acting as custodians do not have legal ownership of a given asset but instead are tasked with holding and securing the asset, such as stocks, bonds, commodities,

<https://www.occ.gov/topics/charters-and-licensing/interpretations-and-actions/1998/ca267.pdf>).

⁸ *Id.* At 6 (citing OFFICE OF THE COMPTROLLER OF THE CURRENCY, *Conditional Approval #479* (July 27, 2001) [hereinafter OCC Conditional Approval 479]; 12 C.F.R. §§ 7.5002(a)(4), 7.5005(a) (interpretive rulings codified in 12 C.F.R. Part 7.28)).

⁹ Office of the Comptroller of the Currency, *Custody Services*, COMPTROLLER’S HANDBOOK 1, 14 (Jan. 2002) [hereinafter OCC Custody Handbook].

¹⁰ Kraken FX, *Kraken Wins Bank Charter Approval*, KRAKEN BLOG (Sep. 16, 2020), <https://blog.kraken.com/post/6241/kraken-wyoming-first-digital-asset-bank>.

¹¹ OCC Letter 1170, *supra* note 6 ; *see also* OCC Conditional Approval 479, *supra* note 7. Historically, banks only offered safekeeping services, which then evolved into banks providing custodial services to their customers. *See also* OCC Custody Handbook, *supra* note 9.

¹² OCC Letter 1170, *supra* note 6, at FN 23.

¹³ OCC Custody Handbook, *supra* 9, at 15.

¹⁴ Kraken FX, *supra* note 10.

or other assets.¹⁵ A custodian is a bank or other financial institution that provides safekeeping, transaction processing and settlement, asset servicing, record-keeping, banking services, and administers securities for its customers.¹⁶ Custody by investment advisers means holding client funds or securities, directly or indirectly, or having the authority to obtain possession of them.¹⁷ A domestic custodian may invest cash balances as directed, collect income, process corporate actions, price securities positions, and provide recordkeeping and reporting services.¹⁸ A global custodian provides custody services for cross-border securities transactions such as executing foreign exchange transactions and processing tax reclaims.¹⁹ In the crypto sphere, tax documentation is also provided by two-thirds of crypto asset providers.²⁰

The custody business is a highly competitive and technology-dependent service.²¹ The ability to gather custody assets, effectively employ technology, and efficiently process large volumes of transactions are essential in the custody business.²² This requires

¹⁵ Fidelity Digital Assets, *Custody in the Age of Digital Assets*, FIDELITY DIGITAL ASSETS (Oct. 15, 2018), <https://www.fidelitydigitalassets.com/articles/custody-in-the-age-of-digital-assets> [hereinafter Fidelity Custody Whitepaper].

¹⁶ OCC Custody Handbook, *supra* note 9, at 73. *See also The Custody Services of Banks*, THE CLEARING HOUSE i, 4 (Jul. 2016), https://www.theclearinghouse.org/-/media/tch/documents/research/articles/2016/07/20160728_tch_white_paper_the_custody_services_of_banks.pdf [hereinafter The Clearing House].

¹⁷ SEC, *Investor Bulletin: Custody of Your Investment Assets* (Mar. 1, 2013), <https://www.sec.gov/investor/alerts/bulletincustody.htm>

¹⁸ OCC Custody Handbook, *supra* note 9, at 1.

¹⁹ OCC Custody Handbook, *supra* note 9, at 1.

²⁰ Apolline Blandin, et al., *3rd Global Cryptoasset Benchmarking Study*, CAMBRIDGE CENTRE FOR ALTERNATIVE FINANCE 1, 52 (Sept. 2020), <https://www.jbs.cam.ac.uk/wp-content/uploads/2021/01/2021-ccaf-3rd-global-cryptoasset-benchmarking-study.pdf> [hereinafter 2020 Benchmarking Study].

²¹ OFFICE OF THE COMPTROLLER OF THE CURRENCY, *Custody Handbook Cover Letter* (Jan. 2002), <https://www.occ.gov/publications-and-resources/publications/comptrollers-handbook/files/custody-services/cover-custody-service.pdf>

²² *Id.*

specialized knowledge and experience to manage the business and strong controls over transaction, credit, and compliance risks.²³

1. Custody Requirements for Traditional Assets

Traditional assets are subject to specific regulatory requirements for custody solutions. For example, in the context of traditional stocks, custodians hold and secure the stock certificate and handle settlement services, recordkeeping, and foreign exchange transactions.²⁴

Before the 1930s, self-custody of assets was the traditional and most common form of custody. Self-custody was a fully decentralized system of bearer assets where investors were responsible for securing the paper certificates that claimed rights to their investments.²⁵ When a corporation went public or a bond was issued, each purchaser received an elaborately designed paper certificate in the investor's name detailing the issuer's name, the date of issue, the number of shares, and the par value.²⁶ To sell, before the new purchaser could receive proof of ownership, a new certificate had to be issued.²⁷ Self-custody decreased in prevalence after the Stock Market Crash of 1929 when investors recognized how inherently risky this system was.²⁸

The historical development of custody solutions for traditional assets was largely driven by financial institutions. During and after the 1930s, financial intermediaries such as trust companies functioned as custodians. In 1967, the Committee on Uniform Security Identification Procedures (CUSIP) added a unique

²³ *Id.*

²⁴ Fidelity Custody Whitepaper, *supra* note 15.

²⁵ Fidelity Custody Whitepaper, *supra* note 15.

²⁶ Virginia B. Morris and Stuart Z. Goldstein, *Lifecycle of a Security*, LIGHTBULB PRESS 1, 5 (2010), <https://www.dtcc.com/-/media/Files/Downloads/Settlement-Asset-Services/Underwriting/LCoaS.pdf>.

²⁷ Morris and Goldstein, *supra* note 26, at 5.

²⁸ Fidelity Custody Whitepaper, *supra* note 15.

identifying number to paper certificates to identify the issuer the issue, and a check digit, which helps the computer ensure that the CUSIP entered was correct.²⁹ Today, the CUSIP service is owned by ABA and administered by Standard & Poor's Financial Services. Other numbering systems exist for international securities, with the most common being ISIN, or International Securities Identification Numbers.³⁰ To sell, the owner endorsed and delivered the certificate to a broker, who delivered it to the buyer's broker in exchange for payment.³¹ Before the purchaser could receive proof of ownership, a new certificate had to be issued.³² This was evidently a cumbersome system requiring significant paperwork to custody, clear, and settle transactions.³³ The trust companies and intermediaries quickly became overwhelmed with changing ownership records, and from 1967 to 1970, a reported \$400 million was lost or stolen in securities.³⁴

The inefficiencies in custodial requirements for paperwork led to the introduction of the first central securities depository (CSD). CSDs provide the custody and recordkeeping services enabling electronic transfer of ownership when investors buy and sell securities and initiate settlement.³⁵ CSDs provide safekeeping for securities immobilized in their vaults and electronic ownership records for those that are dematerialized.³⁶ Using book-entry accounting methods, a CSD updates ownership records

²⁹ Morris and Goldstein, *supra* note 26, at 5; 11.

³⁰ Morris and Goldstein, *supra* note 26, at 5; 11.

³¹ Morris and Goldstein, *supra* note 26, at 5.

³² Morris and Goldstein, *supra* note 26, at 5.

³³ Fidelity Custody Whitepaper, *supra* note 15.

³⁴ See Nick Gray, *The New York Stock Exchange Used to Be Closed Every Wednesday*, MEDIUM (Jun. 7, 2017), <https://medium.com/@nickgraynews/the-new-york-stock-exchange-used-to-be-closed-every-wednesday-4d693133e06>; Tim Ferholz, *The Solution to Wall Street's 1960s Paperwork Crisis Could Also Save Bitcoin*, QUARTZ (Mar. 29, 2015), <https://qz.com/370553/what-the-cigar-chomping-schleppers-of-1960s-wall-street-mean-for-bitcoins-future/>.

³⁵ Morris and Goldstein, *supra* note 26, at 4.

³⁶ Morris and Goldstein, *supra* note 26, at 4.

electronically.³⁷ Some CSDs record the names of the beneficial owners and others the names of only their member firms.³⁸

The first CSD was the Depository Trust Company (DTC) created in 1973 as a subsidiary of the Depository Trust & Clearing Corporation (DTCC) to handle settlement. The DTC introduced a computerized book-entry system that eliminated the exchange of paper certificates by immobilizing them (holding them in custody in a central location—the DTC—now the largest central securities depository in the world).³⁹ The DTC was the first set of centralized ledgers and certificates of clearing.⁴⁰ Eventually, depository functions throughout the United States would be consolidated into the DTC.⁴¹ As of 2010, DTC acted as a CSD for virtually all US municipal securities, as well as the vast majority of equities and corporate bonds issued in the United States.⁴²

In addition to its recordkeeping and custody services, the DTC provides a number of asset processing services such as settling institutional trades directly, managing all phases of a security's life cycle, and offering underwriting, interest, dividend, and corporate action services, including reorganization processing and tender offers for securities it holds in its custody.⁴³

The Employee Retirement Income Security Act of 1974 (ERISA) also changed the securities landscape. ERISA introduced significant changes to how United States pension funds invest and manage assets, including a requirement that plans separate investment management and custody of plan assets.⁴⁴ Mutual fund investing took off in the 1980s, creating a global custody system.⁴⁵

³⁷ Morris and Goldstein, *supra* note 26, at 4.

³⁸ Morris and Goldstein, *supra* note 26, at 4.

³⁹ Morris and Goldstein, *supra* note 26, at 5.

⁴⁰ Fidelity Custody Whitepaper, *supra* note 15.

⁴¹ Fidelity Custody Whitepaper, *supra* note 15.

⁴² Morris and Goldstein, *supra* note 26, at 5.

⁴³ Morris and Goldstein, *supra* note 26, at 5.

⁴⁴ Fidelity Custody Whitepaper, *supra* note 15.

⁴⁵ Fidelity Custody Whitepaper, *supra* note 15.

As of 2018, custody had become very centralized. Custody services are provided by four large banks (BNY Mellon⁴⁶, J.P. Morgan, State Street, Citigroup).⁴⁷ At the end of the first quarter of 2018, these four banks had approximately \$114 trillion in assets under custody.⁴⁸ Recent trends suggest this highly concentrated model will continue, as ongoing barriers to entry have prevented other firms from challenging these incumbents.⁴⁹ A problem with the DTC was the costly reconciliation processes between interconnected ledgers.⁵⁰

Like cash, securities are fungible. Investors hold interests in a DTC eligible security in one of three ways: street name, direct registration, or physical stock certificate, which is very cumbersome to trade and risky in case of loss.⁵¹ As of 2010, between 85% and

⁴⁶ See BNY Mellon Pershing, *Understanding the Protection of Client Assets* (Q1 2021), https://www.pershing.com/_global-assets/pdf/understanding-the-protection-of-client-assets.pdf; see also Justin Baer, *Bitcoin to Come to America's Oldest Bank, BNY Mellon*, WSJ.COM: MARKETS (Feb. 11, 2021), <https://www.wsj.com/articles/bitcoin-to-come-to-america-s-oldest-bank-bny-mellon-11613044810#:~:text=Bank%20of%20New%20York%20MellonCorp,of%20its%20asset%2Dmanagement%20clients>.

⁴⁷ Fidelity Custody Whitepaper, *supra* note 15 (citing Trefis Team & Great Speculations, *Largest Custody Banks Overcome Industry Headwinds to See Further Growth*, FORBES (May 18, 2018), <https://www.forbes.com/sites/greatspeculations/2018/05/18/largest-custody-banks-overcome-industry-headwinds-to-see-further-growth/?sh=4d078ef363be>); see also The Clearing House, *supra* note 16, at 16.

⁴⁸ Fidelity Custody Whitepaper, *supra* note 15; see also The Clearing House, *supra* note 16.

⁴⁹ Fidelity Custody Whitepaper, *supra* note 15 (citing Thorsten Ehinger, Promilla Gurbuxani, Jonathan Klein, and Matthias Voelkel, *A Calm Surface Belies Transformation in Securities Services*, MCKINSEY & COMPANY (Mar. 27, 2018), <https://www.mckinsey.com/industries/financial-services/our-insights/a-calm-surface-belies-transformation-in-securities-services#>).

⁵⁰ Fidelity Custody Whitepaper, *supra* note 15.

⁵¹ DTCC, *In What Ways Can Investors Hold Interests in a DTC Eligible Security*, DTCC FAQs: HOW ISSUERS WORK WITH DTC (last accessed Apr. 24, 2021), <https://www.dtcc.com/settlement-and-asset-services/issuer-services/how-issuers-work-with-dtc> [hereinafter DTCC FAQs]. For a discussion of DTC custody services, see DTCC, *Custody Service Guide* (Mar. 24, 2021),

90% of all equities and corporate and municipal bonds that were issued in paper form in the United States were immobilized by DTC.⁵²

When an investor holds shares in street name, the investor's name is listed on its brokerage firm's books as beneficial owner and the investor has all the rights and risks associated with owning stock, but they don't hold the shares directly.⁵³ The investor uses a brokerage firm who records the investor's security position on their books. The DTC holds the securities and are registered in their nominee name "Cede & Co." which is an acronym for CEntral DEpository and is listed as registered owner on the records of the issuer maintained by its transfer agent.⁵⁴ DTC holds legal title to the securities and the ultimate investor is the beneficial owner.⁵⁵ The brokerage firm name listed in DTC's ownership records.⁵⁶

When investors buy or sell their position, that position changes hands electronically through DTC's book-entry accounting system, but the securities remain in DTC custody.⁵⁷ When you sell stock you hold in street name, the shares are debited electronically from your broker's account at DTC and credited to the DTC account of the brokerage firm whose client bought shares.⁵⁸ Your brokerage firm updates its books to reflect the sale from your account, and the buyer's brokerage firm updates the buyer's account to reflect the purchase.⁵⁹ But the physical certificate doesn't have to be changed, since Cede & Co. continues to be the sole registered owner of the shares.⁶⁰ Both you and the buyer receive electronic confirmations

<https://www.dtcc.com/-/media/Files/Downloads/legal/service-guides/Custody.pdf>. See also Morris and Goldstein, *supra* note 26, at 11.

⁵² Morris and Goldstein, *supra* note 26, at 10.

⁵³ Morris and Goldstein, *supra* note 26, at 9; DTCC FAQs, *supra* note 51.

⁵⁴ Morris and Goldstein, *supra* note 26, at 9; DTCC FAQs, *supra* note 51.

⁵⁵ DTCC FAQs, *supra* note 51.

⁵⁶ DTCC FAQs, *supra* note 51.

⁵⁷ Morris and Goldstein, *supra* note 26, at 9.

⁵⁸ Morris and Goldstein, *supra* note 26, at 10.

⁵⁹ Morris and Goldstein, *supra* note 26, at 10.

⁶⁰ Morris and Goldstein, *supra* note 26, at 10.

that detail the number of shares and the price of your transactions.⁶¹ In addition, as long as the buyer holds the shares, his or her brokerage firm provides proxy materials and regular account statements, which show the security's value and dividends the issuer has paid that have been credited to the beneficial owner's account.⁶²

Investors may also hold their shares via the direct registration system (DRS).⁶³ Via the DRS, the investor can register their name and address, as the owner of the securities, directly on the issuer's books or the books of the issuer's transfer agent.⁶⁴ An investor/owner can hold securities electronically in their own name via DRS and is listed as the registered holder directly on the issuer's books and records, maintained by its transfer agent.⁶⁵ The issuer or transfer agent sends all investor information, dividends, and other corporate communications, including proxy materials, directly to the investor. Investors who use direct registration receive a statement providing evidence of ownership.⁶⁶ Investors who use direct registration receive a statement from the transfer agent providing proof of ownership instead of a stock certificate.⁶⁷

Via the DRS system, investors can sell shares directly from their DRS account, but transfer agents cannot provide a current price or limit price.⁶⁸ In order to sell shares at the market or a limit price, the securities must usually be transferred electronically from the investor's account with the issuer or its transfer agent to the investor's broker/dealer through DTC.⁶⁹ Transfer agents register for DTC's Fast Automated Securities Transfer program.⁷⁰

⁶¹ Morris and Goldstein, *supra* note 26, at 10.

⁶² Morris and Goldstein, *supra* note 26, at 10.

⁶³ See DTCC, *Direct Registration System*, <https://www.dtcc.com/settlement-and-asset-services/securities-processing/direct-registration-system> (last accessed Apr. 24, 2021).

⁶⁴ Morris and Goldstein, *supra* note 26, at 10.

⁶⁵ DTCC FAQs, *supra* note 51; Morris and Goldstein, *supra* note 26, at 10.

⁶⁶ DTCC FAQs, *supra* note 51.

⁶⁷ Morris and Goldstein, *supra* note 26, at 10.

⁶⁸ Morris and Goldstein, *supra* note 26, at 10.

⁶⁹ Morris and Goldstein, *supra* note 26, at 10.

⁷⁰ Morris and Goldstein, *supra* note 26, at 10-11.

Fidelity reports two custody models: omnibus and segregated. The segregated model separates and accounts for client assets at all levels, including within separate private and public key pair groups on chain.⁷¹ The omnibus model⁷² is the street name holding method described above. A broker-dealer consolidates client positions held at mutual fund companies into single omnibus accounts.⁷³ Broker-dealers maintain a separate account for each of their shareholders, but on the books of the mutual fund one account is maintained for all of those shareholders.⁷⁴ In the digital asset sphere, the omnibus model combines clients' assets and spreads the assets across multiple digital asset private and public key pair groups⁷⁵ and achieves client by client segregation at the books and records level.⁷⁶

2. *Custody Requirements for Digital Assets*

Digital assets are unique in the way they are stored which necessitates key innovations for custody providers. Digital assets are stored on blockchains, aka distributed ledgers, in the form of binary code, represented in decimal, hexadecimal or some other numeral system.

Digital assets may represent a variety of underlying physical assets or no real physical assets at all. Bitcoin, for example, is a mere store of value which is not associated with any real world physical asset. Other digital assets may be a representation of an underlying physical asset, such as a piece of art or half of a cow etc. Other

⁷¹ Ria Bhutoria, *The Omnibus Model for Custody*, MEDIUM (Jan. 21, 2020), <https://medium.com/@FidelityDigitalAssets/the-omnibus-model-for-custody-96b69710f92d>.

⁷² *Id.*

⁷³ DTCC, *Overview of Omnibus Processing*, DTCC LEARNING CENTER (last accessed Apr. 24, 2021), <https://dtcclearning.com/omnibus-processing.html>.

⁷⁴ *Id.*

⁷⁵ Bhutoria, *supra* note 71.

⁷⁶ Bhutoria, *supra* note 71.

digital assets may represent rights to a network or use rights within a network. In the context of digital assets that give rights, the common distinction between utility tokens and securities tokens focuses mainly on the use rights associated with utility tokens versus the stock-like characteristics of securities tokens.

Rights deriving from digital assets necessitate access rights to digital assets. Access rights to digital assets are recorded on a particular layer one solution, e.g. the actual blockchain on which the digital asset is recorded to an address which is typically a hash of a public key. The respective public key on a given layer one solution is typically cryptographically derived from a specific private key.

Public and private keys have several key distinguishable features. A public key can be seen as the public facing digital identity of a user who owns a given digital asset by controlling the related private key to the wallet in which the digital asset is stored. Such a private key is the key to any form of ownership rights over digital assets through the wallet in which they are held. In a sense, the private key provides access to the self-custody wallet solution in which any digital assets are held. Protection and safeguarding the private key to a given wallet through secure custodial arrangements is a primary goal of any wallet owner.

Public and private key management is a key custodial arrangement. The key management process determines how digital assets are held and secured. Every digital asset owner holds both a private and a public key.⁷⁷

The public key is used for transacting with digital assets. As its name suggests, this key is shared publicly. The public key functions as a destination address for receiving funds for digital asset transactions and is shared with parties to the transaction.⁷⁸

⁷⁷ See BINANCE ACADEMY, *What is Public Key Cryptography* (Dec. 2, 2020), <https://academy.binance.com/en/articles/what-is-public-key-cryptography> (discussing public key cryptography).

⁷⁸ Fidelity Custody Whitepaper, *supra* note 15.

The private key represents ownership of the asset and is a unique, large alphanumeric string. Via cryptographic digital signature technology, the private key is used to confirm that the owner of the digital asset is in fact who they claim to be.⁷⁹ The asset's wallet generates the private key and assigns the key to transactions originating from that wallet.⁸⁰ The private key may only partially be compared with a password in that it is never shared publicly and is entirely specific to the holder.⁸¹ However, private keys are distinguishable from a password in that a private key is immutable – it cannot be reset.⁸² If a user loses their private key or if the private key is stolen, access to the digital asset may be lost.⁸³ Thus, private key management is critical to security.

The right to a particular unit of digital asset is transferred from party to party through the use of unique cryptographic keys.⁸⁴ Signatures determine the execution of access rights to a given wallet and the digital assets therein. Through a signature, a digital asset may be transferred from one wallet to another. The private key owner of a wallet needs to execute her access rights to the wallet through the private key or other access rights in order to execute a signature.⁸⁵

The quality of custody solutions for digital assets depends on the extent to which they are capable of keeping digital assets safe. A

⁷⁹ Fidelity Custody Whitepaper, *supra* note 15..

⁸⁰ Fidelity Custody Whitepaper, *supra* note 15.

⁸¹ Fidelity Custody Whitepaper, *supra* note 15.

⁸² Fidelity Custody Whitepaper, *supra* note 15.

⁸³ Fidelity Digital Assets, *Custody in the Age of Digital Assets*, FIDELITY DIGITAL ASSETS (Oct. 15, 2018), <https://www.fidelitydigitalassets.com/articles/custody-in-the-age-of-digital-assets>; OCC Letter 1170, *supra* note 6, at 4 (citing Jeff John Roberts and Nicolas Rapp, *Nearly 4 Million Bitcoins Lost Forever, New Study Says*, FORTUNE (Nov. 25, 2017), <http://fortune.com/2017/11/25/lost-bitcoins/>); Alison Sider and Stephanie Young, *Good News! You Are a Bitcoin Millionaire. Bad News! You Forgot Your Password*, THE WALL STREET JOURNAL (Dec. 19, 2017), <https://www.wsj.com/articles/good-news-you-are-a-bitcoin-millionaire-bad-news-you-forgot-your-password-1513701480>).

⁸⁴ OCC Letter 1170, *supra* note 6, at 5.

⁸⁵ OCC Letter 1170, *supra* note 6, at 5.

custody provider needs to demonstrate vigorous security measures which include robust technological protections over technology, cybersecurity, and operations.⁸⁶ Key distinctions of custodial safekeeping revolve around hot storage of keys versus cold storage of keys.

a) Hot Storage

Hot storage self-custody generically refers to users keeping digital assets in wallets that are stored and accessible online. Users have access to such hot wallets via their private keys. Hot storage ensures the easy access and quick transferability of digital assets but is also subject to possible asset security issues in the form of cyber attacks or issues with keeping private keys safe.

Hot wallet custody solutions are particularly important in the digital asset space because of the unique relationship between custody and exchanges. Because the main function of digital asset exchanges is to provide liquidity – not to provide custody – cryptocurrency exchanges typically store digital assets or private keys in hot storage, that is in wallets that are connected to the Internet. While registered legacy stock exchanges facilitate trading but do not take custody of (a.k.a., hold securities on behalf of investors) traded securities,⁸⁷ users of cryptocurrency exchanges are typically required to hand over their assets to the exchange. Most cryptocurrency exchanges are centralized, maintained by a third-party intermediary who is responsible for conducting all trades and transactions.⁸⁸ These centralized cryptocurrency exchanges require users to hand over their assets to the exchange, who then acts as a custodian and essentially issues IOUs for users to trade with on the platform.⁸⁹ When a wallet provider/exchange has custody of a

⁸⁶ Fidelity Custody Whitepaper, *supra* note 15.

⁸⁷ Fidelity Custody Whitepaper, *supra* note 15.

⁸⁸ BINANCE ACADEMY, *Exchange*, GLOSSARY (last accessed Apr. 24, 2021), <https://academy.binance.com/en/glossary/exchange>.

⁸⁹ Werner Vermaak, *What are Decentralized Exchanges (DEX)?*, COINMARKETCAP.COM (Dec. 6, 2020), <https://coinmarketcap.com/alexandria/article/what-are-decentralized-exchanges-dex>.

digital asset, this gives them full control over transactions.⁹⁰ As such, a hack of a digital asset exchange is akin to robbing a bank--getting hold of valuable cryptocurrencies that they can cash out of.⁹¹

As of April 25, 2021 according to CoinMarketCap.com, 308 centralized cryptocurrency exchanges and 60 decentralized exchanges were operational.⁹² As of 2017, 73 percent of digital asset exchanges took custody of private keys while 23 percent let users maintain control over their keys.⁹³ Between 2011 and 2018 there were 56 cyberattacks directed at cryptocurrency exchanges, initial coin offerings and other digital-currency platforms around the world, totaling \$1.63 billion in hacking-related losses.⁹⁴ Just 53% of small custodial exchanges and 78% of large custodial exchanges have a written policy outlining what happens to customer funds in the event of a security breach resulting in the loss of customer funds.⁹⁵

Decentralized exchanges (“DEX”) are a new development as of late 2020 that do not require users to give up control over their

⁹⁰ Fidelity Custody Whitepaper, *supra* note 15.

⁹¹ Steven Russolillo and Eun-Young Jeong, *Cryptocurrency Exchanges Are Getting Hacked Because It's Easy*, WALL STREET JOURNAL (Jul. 16, 2018), <https://www.wsj.com/articles/why-cryptocurrency-exchange-hacks-keep-happening-1531656000>.

⁹² *Top Cryptocurrency Spot Exchanges*, COINMARKETCAP.COM (last accessed Apr. 25, 2021), <https://coinmarketcap.com/rankings/exchanges/>; *Top Cryptocurrency Decentralized Exchanges*, COINMARKETCAP.COM (last accessed Apr. 25, 2021), <https://coinmarketcap.com/rankings/exchanges/dex/>.

⁹³ Fidelity Custody Whitepaper, *supra* note 15 (citing Garrick Hileman & Michel Rauchs, *Global Cryptocurrency Benchmarking Study*, CAMBRIDGE CENTRE FOR ALTERNATIVE FINANCE 1, 27 (2017), <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2017-04-20-global-cryptocurrency-benchmarking-study.pdf>).

⁹⁴ Russolillo and Jeong, *supra* note 91.

⁹⁵ Garrick Hileman & Michel Rauchs, *Global Cryptocurrency Benchmarking Study*, CAMBRIDGE CENTRE FOR ALTERNATIVE FINANCE 1, 27 (2017), <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2017-04-20-global-cryptocurrency-benchmarking-study.pdf> [hereinafter 2017 Benchmarking Study].

funds to an intermediary or custodian.⁹⁶ DEXs are in many ways the future of decentralized asset exchanges. For example, the growth rate of Uniswap and other DEXs in 2020 is unprecedented. Yet, because DEXs rely entirely on self-custody by users, the impact of the DEX growth rate on digital asset custody providers remains unclear. If anything, the DEX growth rate may be an early indicator of increasing decentralized self-custody reliance by digital asset retail users. Mainstream institutional investor adoption of digital assets, in turn, may not materialize via self-custody and DEXs.

b) Cold Storage

Cold storage provides an alternative approach to hot storage. Key to cold storage as opposed to hot storage is that in cold storage the digital assets and associated private keys are stored in wallets that are not connected to the Internet. Because of these distinguishing features, cold storage has several key benefits. For one, cold storage custody solutions are much more secure and resistant to cyber attacks.

A key downside of cold storage involves the lacking accessibility of the stored digital assets. Removing digital assets from cold storage is subject to significant technological uncertainty. Cold storage requires addressing connectivity and recognition of cold storage device concerns. Timing is another issue. In some cases, it can take many hours or even days for investors to obtain control of digital assets that are stored in cold storage devices. The timing makes it especially difficult to use cold storage security for dynamic trading strategies.

Cold storage solutions also raise the issue of control by company employees. Unlike hot storage solutions where multisig wallets are common and allow multiple parties only to act together to gain access to the hot wallet, cold wallets don't have the multisig feature typically. Accordingly, the person who acts as an agent to a corporation who holds the assets on behalf of the company may be the only access point to the corporate assets. This brings with it

⁹⁶ Vermaak, *supra* note 89.

significant insecurity and may not be suitable to any treasury management system.

III. Custody Requirements for Institutional Investors

Institutional investors are less likely to engage in digital asset investments if the custody solutions for digital assets are underdeveloped. Institutional investors' concerns for client safety have generated an unprecedented demand for custodial services.⁹⁷ Institutional investors are finding it difficult to commit fully to digital assets until there is a reliable and respected custody solution.⁹⁸ A cryptocurrency custody service is usually designed for institutional investors and is a secure, off-chain storage solution for cryptocurrencies.⁹⁹

Accordingly, institutional custody solutions for digital assets need to be as equally robust as those provided for traditional assets.¹⁰⁰ Institutions face specific regulatory, market/network, security, and client challenges.¹⁰¹ For example, institutions must work with a custodian that can demonstrate a significant track record and experience in safeguarding client assets.¹⁰² Private keys or maintaining passphrases for individual digital assets is too cumbersome for institutional investors.¹⁰³

1. Depository Institution Requirements

⁹⁷ Vermaak, *supra* note 89.

⁹⁸ Vermaak, *supra* note 89.

⁹⁹ Anna Buczak, *Best Crypto Custody Providers in 2021 – Comparison*, ULAM LABS (Jan. 22, 2021), <https://www.ulam.io/blog/best-crypto-custody-providers/> (discussing Genesis, Digivault, Fireblocks, Gemini, Coinbase, Kingdom Trust, and BitGo).

¹⁰⁰ Fidelity Custody Whitepaper, *supra* note 15.

¹⁰¹ For full discussion, *see* Fidelity Custody Whitepaper, *supra* note 15.

¹⁰² Fidelity Custody Whitepaper, *supra* note 15.

¹⁰³ Fidelity Custody Whitepaper, *supra* note 15.

Prior to July 2020, digital asset custody was the province of specialist firms who typically needed a state license, such as a trust charter, to offer the service to large investors.¹⁰⁴ Various states provided specialized state-backed regulatory solutions for digital asset companies. More recently, several states have introduced more digital asset-friendly legislation.¹⁰⁵

Money transmitters are regulated under federal and state law. Money transmitters register under the federal Bank Secrecy Act (BSA) and are licensed under state law.¹⁰⁶ In 2013, the Financial Crimes Enforcement Network (FinCEN) announced money transmission laws would not distinguish between fiat currency and digital assets.¹⁰⁷ Coinbase is registered as a money services business with Financial Crimes Enforcement Network, or FinCEN, and also has a specialized New York state license for crypto businesses, called the BitLicense, from the DFS.¹⁰⁸

In many states, an exemption from money-transmitter licensing is a state trust charter.¹⁰⁹ State trust charters are non-FDIC-insured, nondepository trust companies.¹¹⁰ State chartered trust companies

¹⁰⁴ Nikhilesh De, *Banks in US Can Now Offer Crypto Custody Services, Regulator Says*, COINDESK (Jul. 22, 2020), <https://www.coindesk.com/banks-in-us-can-now-offer-crypto-custody-services-regulator-says>.

¹⁰⁵ OCC Letter 1170, *supra* note 6, at FN 16; *See, e.g.*, regulations in Wyo. Admin. Code 021.0002.19 promulgated pursuant to Wyo. Stat. 34-29-104 (mandatory compliance for banks that elect to provide digital asset custodial services and the new regulations (known as the enhanced digital custody opt-in regime)); *See* Hawaii S.B. 2594 (Jan. 17, 2020); Rhode Island H.B. 7989 (Mar. 11, 2020).

¹⁰⁶ Marco Santori, *What is Money Transmission and Why Does it Matter?*, COIN CENTER (Apr. 7, 2015), <https://www.coincenter.org/education/policy-and-regulation/money-transmission/>.

¹⁰⁷ *Id.*

¹⁰⁸ Paul Vigna, *JPMorgan Extends Banking Services to Bitcoin Exchanges*, WALL STREET JOURNAL (May 12, 2020), <https://www.wsj.com/articles/jpmorgan-extends-banking-services-to-bitcoin-exchanges-11589281201>.

¹⁰⁹ Lalita Clozel, *Are Trust Charters the Key to Simplifying Fintech Regulation?*, AMERICAN BANKER (Nov. 8, 2016), <https://www.americanbanker.com/news/are-trust-charters-the-key-to-simplifying-fintech-regulation>

¹¹⁰ *Id.*

can be qualified custodians as a “simplified version of banking, with much higher physical, technical and financial security relative to traditional financial institutions,” with tailored digital custody services to different customer needs so that users can seamlessly utilize both digital dollar (and future CBDCs) as well as cryptocurrencies.¹¹¹

The applicability of the trust label to digital asset firms, without a fiduciary duty, can be problematic. A typical legal obligation for trust companies is a fiduciary duty – to place customers' interests above the company's own. It is unclear whether fintech firms would satisfy the duty of acting as a fiduciary. Some states are suspicious of attempts to “co-opt” the trust charter for the benefit of companies that do not specialize in traditional trust services. For example, Gemini obtained a trust charter from the New York State Department of Financial Services in 2015.¹¹² When it tried to expand to Washington, the state required Gemini sought to acknowledge it had a fiduciary duty to its customers when it requested trust recognition, which required the company to change its user agreement to state that for every consumer that entrusts them with fiat currency, “we will be performing as a fiduciary.”¹¹³

In 2019, Wyoming introduced the special purpose depository institution (SDPI) model. SDPIs focus on fiduciary activities, safekeeping, asset management and servicing.¹¹⁴ Permitted SDPI purposes under HB 74 include business cash

¹¹¹ Csilla Brimer, *Response: Custody Rule and Digital Assets*, SEC (Dec. 6, 2020), <https://www.sec.gov/investment/csilla-brimer-response-custody-rule-digital-assets>.

¹¹² Vigna, *supra* note 107.

¹¹³ Clozel, *supra* note 109.

¹¹⁴ WYOMING DIVISION OF BANKING, *Special Purpose Depository Institutions* (last accessed Apr. 28, 2021), <http://wyomingbankingdivision.wyo.gov/home/areas-of-regulation/laws-and-regulation/special-purpose-depository-institution>. See also OCC Letter 1170, *supra* note 6, at FN 16. See, e.g., regulations in Wyo. Admin. Code 021.0002.19 promulgated pursuant to Wyo. Stat. 34-29-104 (mandatory compliance for banks that elect to provide digital asset custodial services and the new regulations (known as the enhanced digital custody opt-in regime)).

management and operational accounts. Wyoming law distinguishes SDPIs from custody banks.¹¹⁵ Custody banks focus on storing assets, fiduciary management, securities transactions, commodities markets and customer bank accounts. SDPIs can obtain insurance from the Federal Deposit Insurance Corporation (FDIC), but they are not required to because they are prohibited from making loans with customer deposits of fiat currency. State chartered SDPIs eliminate some of the legal hurdles that burdens technological advances - such as the reluctance of the existing banking sector to change / tailor AML / BSA compliance processes in order to accommodate the global & censorship resistant nature of cryptocurrencies.¹¹⁶

In September 2020, Kraken formed the world's first SDPI, Kraken Bank, under Wyoming state law. Kraken Bank became the first digital asset company in United States history to receive a bank charter recognized under federal and state law and the first regulated, U.S. bank to provide comprehensive deposit-taking, custody and fiduciary services for digital assets.¹¹⁷ Kraken is a cryptocurrency exchange established in 2011.¹¹⁸ As a SDPI, Kraken Bank can operate as a fully independent bank in the United States and still provide deposit-taking, custody, and fiduciary services for digital assets.¹¹⁹ Another Wyoming digital asset bank is Avanti.¹²⁰

2. OCC Requirements

In July of 2020, the Office of the Comptroller of Currency concluded national banks and federal savings associations are permitted to “offer more secure storage services compared to existing options,” and that both consumers and investment advisors

¹¹⁵ See generally The Clearing House, *supra* note 16.

¹¹⁶ Brimer, *supra* note 111.

¹¹⁷ Kraken FX, *supra* note 10.

¹¹⁸ Nicolás Morles, *Kraken — a Review of One of the Oldest Cryptocurrency Exchanges*, MEDIUM (Aug. 22, 2020), <https://medium.com/@nicolasmorles/kraken-a-review-of-one-of-the-oldest-cryptocurrency-exchanges-2837f043f4c6>.

¹¹⁹ Kraken FX, *supra* note 10.

¹²⁰ See AVANTI, <https://avantibank.com/> (last accessed Oct. 5, 2021).

may wish to use regulated custodians to ensure they don't lose their private keys, and therefore, access to their funds.¹²¹ The institution must do so consistent with sound risk management practices, including having adequate systems in place to identify, measure, monitor, and control the risks of its custody services including policies, procedures, internal controls, and management information systems governing custody services.¹²² The OCC assesses banking risk relative to its impact on capital and earnings.¹²³ From a supervisory perspective, risk is the potential that events, expected or unexpected, may have an adverse impact on a bank's capital or earnings.¹²⁴ The primary risks associated with custody services are: transaction, compliance, credit, strategic, and reputation.¹²⁵

A risk is the potential for loss, damage, or operational disruption that emerges from the use of technological information systems, which is actualized if a threat is successful. Operational risks can affect the confidentiality, availability, or integrity of information or information systems.¹²⁶ Operational risk is inherently high in custody services because of the high volume of transactions processed daily.¹²⁷ Transaction/operational risk is the current and prospective risk to earnings or capital from fraud, error, and the inability to deliver products or services, maintain a competitive position, and manage information.¹²⁸ Common causes of losses attributable to custody activities are errors in corporate action, settlement, foreign exchange (FX), and operating (suspense)

¹²¹ Nikhilesh De, *Banks in US Can Now Offer Crypto Custody Services*, *Regulator Says*, COINDESK (Jul. 22, 2020), <https://www.coindesk.com/banks-in-us-can-now-offer-crypto-custody-services-regulator-says>.

¹²² OCC Letter 1170, *supra* note 6, at 9-10.

¹²³ OCC Custody Handbook, *supra* note 9, at 2.

¹²⁴ OCC Custody Handbook, *supra* note 9, at 2.

¹²⁵ OCC Custody Handbook, *supra* note 9, at 2; *see also* The Clearing House, *supra* note 16, at 23-30.

¹²⁶ James J. Cebula and Lisa R. Young, *A Taxonomy of Operational Cyber Security Risks*, CARNEGIE MELLON CERT PROGRAM i, 1 (Dec. 2010).

¹²⁷ *Id.*

¹²⁸ OCC Custody Handbook, *supra* note 9, at 2-3.

account processing.¹²⁹ The risks may be magnified in a global custody operation where transactions occur around the clock in a variety of different markets.¹³⁰ A global custodian must consider a variety of additional factors including differing market rules and conventions, the degree of automation in the foreign market, different types of securities, capital or currency restrictions, and the availability and communication of timely and accurate information.¹³¹ Additional risks in the digital asset space are their highly unpredictable value, increased risk of market manipulation, difficult to cash out investments, conflicts of interest, limited protection from fraud.¹³²

In order to mitigate transactional/operational risk, safeguard assets under custody, produce reliable financial reports, and comply with laws and regulations.¹³³ Information security infrastructure and controls to mitigate hacking, theft, and fraud need to be enhanced when maintaining custody of digital assets due to their unique technical characteristics.¹³⁴ Notably, custodians spend between 6% to 10% of their resources on IT security while non-custodial service providers spend between 11% to 20% of its resources, both financial and human, on IT security.¹³⁵ Non-custodial systems are generally associated with greater development costs and timeline.¹³⁶ IT security includes design and implementation of proper cybersecurity controls (also known as safeguards or risk management practices).¹³⁷ Key risk areas should be protected both

¹²⁹ OCC Custody Handbook, *supra* note 9, at 2-3.

¹³⁰ OCC Custody Handbook, *supra* note 9, at 2-3.

¹³¹ OCC Custody Handbook, *supra* note 9, at 2-3.

¹³² OFFICE OF NEW YORK STATE ATTORNEY GENERAL, *Investor Alert: Virtual Currency Risks* (Feb. 2021) <https://ag.ny.gov/sites/default/files/crypto-investor-notice.pdf>.

¹³³ OCC Letter 1170, *supra* note 6, at 10; *see also Are Crypto Exchanges Safe? How to Choose an Exchange You Can Trust.*, BINANCE: BLOG (Dec. 30, 2020), <https://www.binance.com/en/blog/421499824684901426/Are-Crypto-Exchanges-Safe-How-to-Choose-an-Exchange-You-Can-Trust>.

¹³⁴ OCC Letter 1170, *supra* note 6, at 10.

¹³⁵ 2020 Benchmarking Study, *supra* note 20, at 13.

¹³⁶ 2020 Benchmarking Study, *supra* note 20, at 13.

¹³⁷ Office of Cybersecurity, Energy Security, and Emergency Response, *Cybersecurity Capability Maturity Model (C2M2)*, U.S. DEP'T OF ENERGY 1, 11-13 (Feb. 2014) [hereinafter C2M2]; Mark Lanterman, *The Components of Strong*

to prevent a risk from occurring and to detect either that a preventive control failed or that a risk materialized.¹³⁸ Every risk should have a preventative and detective control and there should be appropriate layers of controls so that if some fail, others will still be there to reduce the risk. This might include a control to detect process failures. An organization's ability to cope with threats and reduce risk increases with levels of security strength.

Some risk management processes may need to be tailored in the context of digital custody.¹³⁹ Administrative controls are typically process-oriented and relate to the establishment of policies and procedures. Identity management, authentication, and access control should be provided on a need-to-know basis.¹⁴⁰ Technically and logically, in order to maintain data integrity, procedures should be in place that govern how to change data stored or transmitted on organization servers.¹⁴¹ Systems should also be protected against denial of service or similar attacks – this is a technical control aimed at maintaining availability.¹⁴² Specialized digital custody audit procedures for verifying the bank maintains access controls for a cryptographic key will differ from the procedures used for physical assets.¹⁴³

Cybersecurity Plans, Part 2: Security Assessment, COMPLIANCE & ETHICS PROFESSIONAL 27, 28 (Dec. 2017) [hereinafter *Lanterman, Part 2*]. For a discussion on thorough integrated system of implementing policies throughout the organizations at all levels and roles, see NIST *Cybersecurity Framework*, *infra* note 138, at 34.

¹³⁸ See NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, *Framework for Improving Critical Infrastructure Cybersecurity* 1, 37-40 (Apr. 16, 2018) [hereinafter *NIST Cybersecurity Framework*].

¹³⁹ OCC Letter 1170, *supra* note 6, at 10.

¹⁴⁰ See CENTER FOR INTERNET SECURITY, *Maintenance, Monitoring, and Analysis of Audit Logs* (last accessed Apr. 28, 2021) <https://www.cisecurity.org/controls/maintenance-monitoring-and-analysis-of-audit-logs/>.

¹⁴¹ See Security Ninja, *CIA Triad*, INFOSEC RESOURCES (Feb. 7, 2018), <https://resources.infosecinstitute.com/topic/cia-triad/#gref>; NIST, *Cybersecurity Framework*, *supra* note 138, at 32 (discussing CIA in data security).

¹⁴² INFOSEC RESOURCES, *supra* note 141.

¹⁴³ OCC Letter 1170, *supra* note 6, at 10.

Reserves audits are more important without proof-of-reserves programs.¹⁴⁴ A good industry practice is to perform reserve audits on digital assets. The transparent nature of the blockchain means multiple options to show reserves. The first way is traditional audits performed by independent third parties.¹⁴⁵ The second way, specific to blockchain, is to keep on-chain proof-of-reserves.¹⁴⁶ The Cambridge Center for Alternative Finance does annual surveys of digital asset companies and reported 54% of surveyed custodial service providers indicated that they performed an externally-led audit of their digital asset reserves over the past 12 months, and were most likely to be operating out of Europe or the APAC region.¹⁴⁷ The report noted this is a 24-percentage point decline compared to their 2018 sample.¹⁴⁸ The Center explained this may suggest firms feel a decrease in scrutiny relative to 2018 after Tether, a stablecoin who was expected to keep 100% reserves, was discovered not to have done so.¹⁴⁹ 59% of firms indicate that they had their digital asset reserves audited by an independent comptroller over the past 12 months, primarily based out of Europe (35%) and Asia-Pacific (31%).¹⁵⁰

The second type of risk to consider is compliance risk. Like commercial banks, custodians are chartered as banks and accept insured and uninsured deposits.¹⁵¹ 46% of service providers surveyed as discussed above reported not being insured against any risks.¹⁵² Insurance plans primarily insure against cybercrimes, professional errors, hazards, and loss or theft of private keys.¹⁵³ Before accepting an account as a client, custodians must analyze individual account risks, including the customer's needs and wants and the account's operational needs and whether the contemplated

¹⁴⁴ OCC Letter 1170, *supra* note 6, at 10.

¹⁴⁵ 2020 Benchmarking Study, *supra* note 20, at 50.

¹⁴⁶ 2020 Benchmarking Study, *supra* note 20, at 50.

¹⁴⁷ 2020 Benchmarking Study, *supra* note 20, at 50-51.

¹⁴⁸ 2020 Benchmarking Study, *supra* note 20, at 13.

¹⁴⁹ 2020 Benchmarking Study, *supra* note 20, at 51.

¹⁵⁰ 2020 Benchmarking Study, *supra* note 20, at 51.

¹⁵¹ The Clearing House, *supra* note 16, at 19.

¹⁵² 2020 Benchmarking Study, *supra* note 20, at 13.

¹⁵³ 2020 Benchmarking Study, *supra* note 20, at 13.

duties are within its capabilities and are consistent with all applicable law.¹⁵⁴ The digital asset space adds another layer of due diligence including understanding the risks of cryptocurrency and a review for compliance with anti-money laundering rules.¹⁵⁵ Banks seeking to engage in these activities should also conduct legal analysis to ensure the activities are conducted consistent with all applicable laws.¹⁵⁶ A national bank should consult with OCC supervisors as appropriate prior to engaging in cryptocurrency custody activities because different cryptocurrencies may also be subject to different OCC regulations and guidance outside of the custody context, as well as non-OCC regulations.¹⁵⁷ SEC-registered brokers are required to comply with the SEC's custody protections, which are designed to protect against the loss or theft of an asset. The Customer Protection Rule requires segregating customer assets from the broker's assets.¹⁵⁸ As long as the broker is not holding the securities, it will generally not need to comply with the custody rule. Provisions of the Investment Company Act of 1940 may also need to be considered.¹⁵⁹ 17 C.F.R. § 275.206(4)-2(a) outlines safeguarding procedures for investment advisers which could open custodians up to liability. An exception to the rule is if a qualified custodian maintains the assets according to 17 C.F.R. § 275.206(4)-2(a)(1)(i) or (ii).¹⁶⁰ 5% of cryptoasset servicers were qualified

¹⁵⁴ OCC Letter 1170, *supra* note 6, at 10.

¹⁵⁵ OCC Letter 1170, *supra* note 6, at 10.

¹⁵⁶ OCC Letter 1170, *supra* note 6, at 10; *see also* Anna Buczak, *KYC/AML Compliance in Crypto Industry - Introduction for Business Owners*, ULAM LABS (Dec. 2, 2020), <https://www.ulam.io/blog/KYC-AML-compliance-in-crypto/>.

¹⁵⁷ OCC Letter 1170, *supra* note 6, at 10 (discussing digital assets considered “securities” (and therefore subject to federal securities laws) may also be subject to the OCC’s regulations on recordkeeping and confirmation requirements for securities transactions (12 CFR Part 12)).

¹⁵⁸ SEC Rule 15c3-3, 17 C.F.R. § 240.15c3-3 (2019).

¹⁵⁹ *See* OCC Custody Handbook, *supra* note 9, at 91; 15 U.S.C. 80a-17(f).

¹⁶⁰ For more, *see* SEC, *Investor Bulletin: Custody of Your Investment Assets* (Mar. 1, 2013), <https://www.sec.gov/investor/alerts/bulletincustody.htm>; Nikhilesh De, *The SEC Is Still Working Out What ‘Qualified Custodian’ Means for Crypto*, COINDESK (Nov. 16, 2020), <https://www.coindesk.com/sec-qualified-custodian-statement>; U.S. SECURITIES AND EXCHANGE COMMISSION, *Custody of Funds or Securities of Clients by Investment Advisers: A Small Entity*

custodians.¹⁶¹ Other laws and regulations that may be of interest include ERISA,¹⁶² Reg D,¹⁶³ Regulation U¹⁶⁴ and others.¹⁶⁵

The May 2019 FinCEN guidance regarding Bank Secrecy Act¹⁶⁶ stated most cryptoasset businesses qualify as money transmitters and must comply with AML/KYC regulations (with the exemption of non-custodial wallets, decentralized exchanges that do not settle trades, and certain infrastructure providers (e.g. DApp developers, cloud miners)).¹⁶⁷

Credit risk, found in all activities that depend on counterparty, issuer, or borrower performance, is the current and prospective risk to earnings or capital arising from an obligor's failure to meet the terms of any contract with the bank or otherwise to perform as agreed.¹⁶⁸ Fortunately, this risk is low in digital asset transactions because transactions are made instantaneously.

Compliance Guide (last modified Mar. 12, 2010), https://www.sec.gov/info/smallbus/secg/custody_rule-secg.htm; and 17 CFR 270.17f.

¹⁶¹ 2020 Benchmarking Study, *supra* note 20, at 52. Among these are Wyoming SDPIs, according to Wyoming Laws Ch. 19 § 4 (a).

¹⁶² 29 U.S.C. § 1001.

¹⁶³ 12 C.F.R. § 204.

¹⁶⁴ 12 C.F.R. § 221.

¹⁶⁵ See, e.g., 31 C.F.R. 103 (Financial Recordkeeping and Reporting of Currency and Foreign Transactions); OCC Banking Circular 196, *Securities Lending* (May 7, 1985), <https://www.occ.treas.gov/news-events/newsroom/news-issuances-by-year/bulletins/banking-circulars.html>; OCC Banking Circular 275, *Free-Riding in Custody Accounts*, OFFICE OF COMPTROLLER OF CURRENCY (Sept. 3, 1993), <https://www.occ.treas.gov/news-events/newsroom/news-issuances-by-year/bulletins/banking-circulars.html>.

¹⁶⁶ 31 U.S.C. § 5311-5330 (Bank Secrecy Act); 12 C.F.R. 21.21 (Bank Secrecy Act Compliance); As of December 2020, convertible virtual currency and digital assets with legal tender status are considered monetary instruments. See Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets, 86 Fed. Reg. 3897 (proposed Jan. 15, 2021); Kevin Reynolds, Proposed Crypto Wallet Rule Not Among Those Frozen by Biden Pending Review, COINDESK: POLICY (Jan. 20, 2021), <https://www.coindesk.com/policy/2021/01/21/proposed-crypto-wallet-rule-not-among-those-frozen-by-biden-pending-review/>.

¹⁶⁷ 2020 Benchmarking Study, *supra* note 20, at 50.

¹⁶⁸ OCC Custody Handbook, *supra* note 9, at 4.

Other considerations include strategic and reputation risk.¹⁶⁹ With regard to strategic risk,¹⁷⁰ digital assets are viewed as a high risk by the banking industry.¹⁷¹ Reputational risk has been considered the top strategic business risk.¹⁷² Liquidity risk is the risk of loss from an actual or perceived inability to meet cash and collateral obligations.¹⁷³

3. *Federal/National Trust Charters*

As of March 2021, 53 active trust banks existed.¹⁷⁴ The CFPB has specific consumer protection enforcement authority, which enforces compliance with enumerated financial consumer protection laws for the financial companies designated by the Dodd-Frank Act.¹⁷⁵ The CFPB's Taskforce on Federal Consumer Financial Law recommended federal charters or licenses to non-bank FinTech companies engaged in payments, remittances, or lending services, or clarify the authority of the OCC.¹⁷⁶ The

¹⁶⁹ See OCC Custody Handbook, *supra* note 9, at 5-6.

¹⁷⁰ See OCC Custody Handbook, *supra* note 9, at 5-6.

¹⁷¹ Daniel Palmer, *JPMorgan Bank Takes on Coinbase, Gemini as Its First Crypto Exchange Customers*, COINDESK (May 12, 2020), <https://www.coindesk.com/coinbase-gemini-first-crypto-exchange-customers-jpmorgan-bank-report>.

¹⁷² See *2014 Global Survey on Reputation Risk*, DELOITTE 1, 4 (Oct. 2014) https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Governance-Risk-Compliance/gx_grc_Reputation@Risk%20survey%20report_FINAL.pdf.

¹⁷³ The Clearing House, *supra* note 16, at 30.

¹⁷⁴ OFFICE OF THE COMPTROLLER OF THE CURRENCY, *Trust Banks Active As of 9/30/2021*, <https://occ.gov/topics/charters-and-licensing/financial-institution-lists/trust-by-state.pdf> (last accessed Oct. 5, 2021).

¹⁷⁵ Office of the Comptroller of the Currency, *Acting Comptroller of the Currency Issues Statement on CFPB Task Force Study Regarding Federal Fintech Charters*, OCC NEWSROOM (Jan. 6, 2021), <https://occ.gov/news-issuances/news-releases/2021/nr-occ-2021-3.html>.

¹⁷⁶ U.S. Bureau of Consumer Financial Protection, *Taskforce on Federal Consumer Financial Law Report Vol. II* 1, 81 (Jan. 2021), https://files.consumerfinance.gov/f/documents/cfpb_taskforce-federal-consumer-financial-law_report-volume-2_2021-01.pdf [hereinafter Taskforce Report].

Taskforce stated that charters or licenses should provide that these institutions are governed by the regulations of their home states, even when providing services to consumers located in other states, similar to the National Bank Act's treatment of federally chartered banks.¹⁷⁷

The Office of the Comptroller of the Currency (OCC) grants national charters to companies engaged in lending, payments, or deposit-taking and agrees that the nation needs federal charters for fintechs to effectively, efficiently, and safely serve the financial needs of consumers across the nation under a single uniform set of rules.¹⁷⁸

Becoming an OCC-regulated trust is one way crypto exchanges can operate nationwide without needing to secure state-level licenses in each of the 49 different U.S. states (Montana doesn't have a licensing requirement).¹⁷⁹ In order to form a full bank, Federal Deposit Insurance Corp. (FDIC) and Federal Reserve approvals are needed.

One way to do this is by, as a state bank or state trust company, applying to convert into a national bank under 12 U.S.C. § 35 with OFF approval and as a non-depository public trust company organized under state law to convert to a national bank under 12 C.F.R. § 5.24.¹⁸⁰

Anchorage Trust offers custody services primarily to institutional investors and a limited number of high-net-worth individuals that transact in digital assets and cryptocurrencies, including but not

¹⁷⁷ Taskforce Report, *supra* note 176, at 81.

¹⁷⁸ Office of the Comptroller of the Currency, *supra* note 175.

¹⁷⁹ Nikhilesh De, *Paxos Becomes Third Federally Regulated Crypto 'Bank'*, COINDESK (Apr. 23, 2021), <https://www.coindesk.com/paxos-becomes-third-federally-regulated-crypto-bank>.

¹⁸⁰ Practical Law Finance, *OCC Grants Conditional Approval for First National Cryptocurrency Trust Company*, THOMSON REUTERS (Jan. 27, 2021). *See also* Stephen A. Lybarger, *Application by Anchorage Trust Company, Sioux Falls, South Dakota to Convert to a National Trust Bank Application for Residency Waiver*, OFFICE OF THE COMPTROLLER OF THE CURRENCY (Jan. 13, 2021), <https://occ.gov/news-issuances/news-releases/2021/nr-occ-2021-6a.pdf>. [hereinafter Anchorage Letter].

limited to certain tokenized securities and cryptocurrencies such as Bitcoin, Bitcoin Cash, Ethereum, Zcash, and Filecoin.¹⁸¹ Anchorage also performs fiduciary custody of digital assets and fiat currency, on-chain governance services, staking services, and settlement services.¹⁸² Since then, Protego and Paxos are two more nationally chartered digital asset banks.

Dozens of start-ups and established firms are developing ways to secure digital assets, but to date, few have focused on the unique challenges of institutional investors. NYDIG promotes itself as providing institutional digital asset custody services.¹⁸³ U.S. Bank is looking into working with a crypto custodian.¹⁸⁴ The CryptoCurrency Certification Consortium (“C4”) spearheaded a group of researchers, security auditors, and company principals to introduce a standardized methodology for securing private keys.¹⁸⁵ Creating a digital vault has also been suggested.¹⁸⁶

IV. Conclusion

¹⁸¹ Anchorage Letter, *supra* note 180.

¹⁸² Anchorage Letter, *supra* note 180.

¹⁸³ See NYDIG, *Platform* (last accessed May 11, 2021), <https://nydig.com/about-nydig/platform>.

¹⁸⁴ Ian Allison, *US Bank Selects Cryptocurrency Custodian, Wins Admin Role for NYDIG’s Bitcoin ETF*, COINDESK (Apr. 27, 2021) <https://www.coindesk.com/us-bank-cryptocurrency-custody-nydig-bitcoin-etf-admin-role>.

¹⁸⁵ C4, *Crypto Currency Security Standard*, CRYPTOCONSORTIUM (last accessed Apr. 28, 2021), <https://cryptoconsortium.github.io/CCSS/>; see also Michael Perklin, *Are There Industry Standards for Securing Cryptocurrencies?*, COIN CENTER (Jul. 5, 2017), <https://www.coincenter.org/education/crypto-regulation-faq/are-there-industry-standards-for-securing-cryptocurrencies/>.

¹⁸⁶ Malte Möser, Ittay Eyal, and Emin Gün Sirer, *Bitcoin Covenants* 1, 7-9 (2016), <https://fc16.ifca.ai/bitcoin/papers/MES16.pdf> (Illustrating vaults as a novel security construct built using an extension to Bitcoin’s script language enabling covenants, a primitive that allows transactions to restrict how the value they transfer is used in the future. Vaults focus on improving the security of private cryptographic keys, disincentivizing key theft by preventing an attacker from gaining full access to stolen funds).

Custody solutions are particularly important to the proliferation of digital assets. Multi-signature wallets and a combination of hot and cold storage solutions are advisable. While the majority of cryptocurrency spot exchanges require ownership to be surrendered in order to transact, DEXs are introducing the ability for users to transact without exposing private keys to vulnerability.

State and federal laws are evolving to allow more institutionalized custody services for retail customers, most notably as state trust charters are evolving to national trust charter approvals for digital asset banks.

From the perspective of decentralization, the application of current legacy rules around custody of traditional assets is inconsistent with decentralization foundations. The very nature of a decentralized system mandates the avoidance and eradication of intermediaries for business transactions. Owners of digital assets can rely on the cryptography of the wallet and of each transaction to avoid reliance on trusted third parties. Without it, single points of failure, rent-seeking behaviors and other suboptimal outcomes of legacy systems are inevitably seeping back into decentralized solutions. Delegation of rights to custody providers is only an incremental step to centralization via delegation to third party investment managers. This becomes a floodgate issue, as each level of investment discretion over digital assets exacerbates the centralization concerns and compounds the rent seeking suboptimalities.

The realities of decentralization and decentralized self-custody would require investment advisers to simply provide digital asset investment advice via fee without taking custody of digital assets. However, the expectations of legacy customers involve typically custodial solutions which may mandate continuous experimentation with digital asset custody solutions within the existing legal framework and the evolving legal legacy framework for digital asset custody solutions.

At the same time, decentralized self-custody of digital assets is here to stay. Collective non-custodial DeFi investment clubs are already emerging where collective decision making in a non-custodial investment setting is a reality. These kinds of experimentation

enable decentralized self-custody solutions that are combined with cutting edge DeFi projects and non-custodial investment clubs that are based on staking unpooled non-custodial assets on deals. Once a deal finds substantial funding it may move forward through smart contracts with staked assets that are released when the deal is fully funded without any pooling or custody.

Until these self-custodial investment deals become mainstream in DeFi, custody solutions for mainstream adoption will remain an issue that is looking for a solution. Ultimately, these two trends will run parallel until both centralized custody solutions and decentralized non-custodial deal platforms are more established. The existing trends in DeFi seem to suggest that the decentralized non-custodial deal platforms will have more innovation and better deals. Only time will tell. For now, the evolution of custody solutions for digital assets remain essential for mainstream adoption.