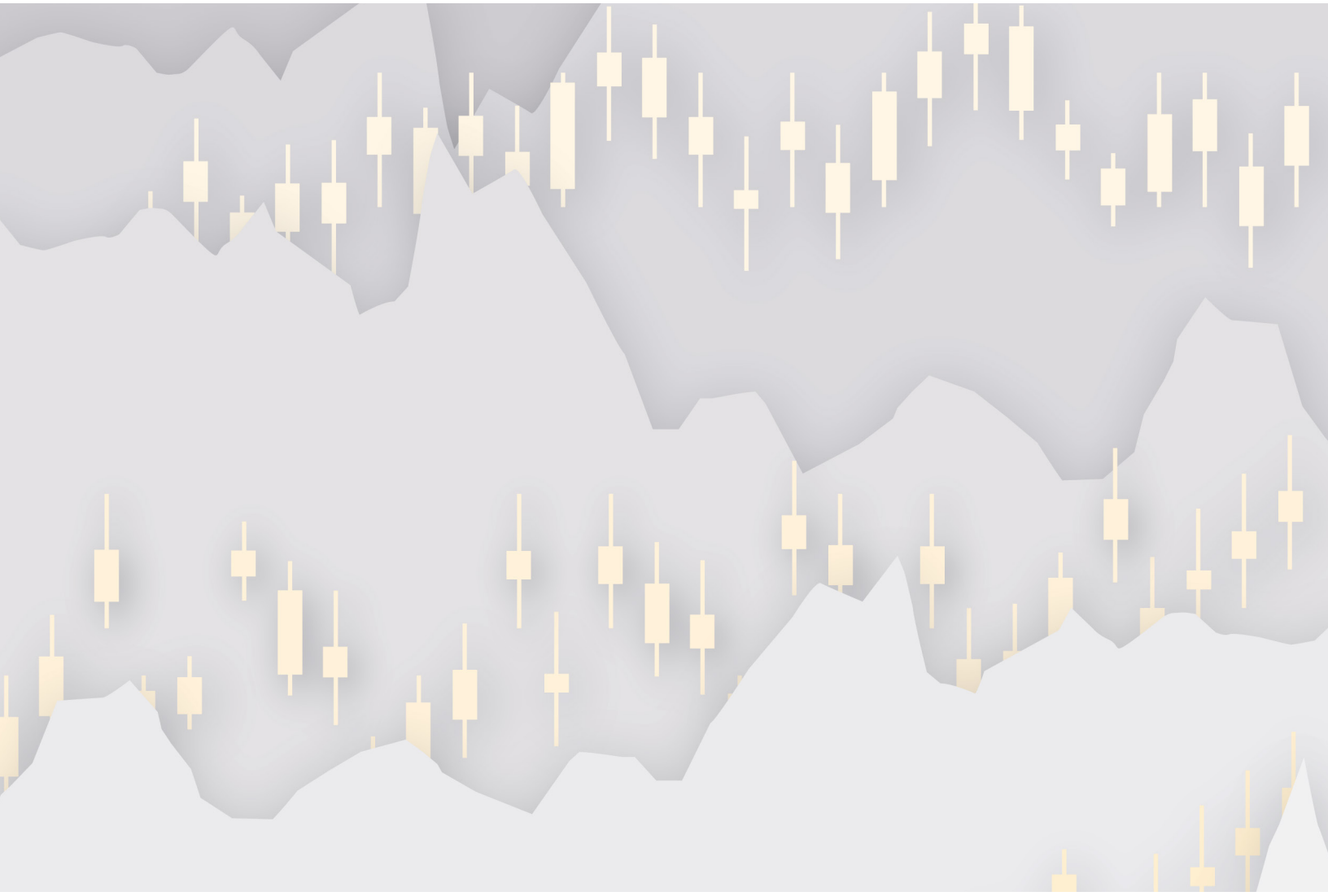
coindesk®



CUSTODY

Crypto Assets' Unique Challenge and Opportunity

By Galen Moore

July 2019

coindesk®

CONTENTS

INTRODUCTION

Bitcoin has emerged as a legitimate asset category for professional investors, drawing increasing attention from institutions large and small. Bitcoin's innovation is digital ownership, without an intermediary organization. Its value proposition is "digital gold": a digital store of wealth that is difficult to seize, freeze or devalue. Understanding how to custody these assets is not only an operational challenge to investors, it is also a key concept for understanding the value of bitcoin and any other crypto asset.

This white paper defines the unique custody challenges crypto assets present, and provides an overview of efforts to solve them. You can find it and more research like it at coindesk.com/intro-to-crypto-investing, where we are building a library of research for early adopters among institutional investors in crypto assets. We welcome your comments and questions; the author can be reached directly at galen@coindesk.com.

BEARER ASSETS, PROS & CONS

"Owning" bitcoin means possessing a cryptographic password, or private key, which allows the holder control over a definite portion of the global ledger of ownership. Balances of bitcoin recorded there are subject to transfer by whoever holds the key. As such, bitcoin is a bearer asset: who holds the key, controls the asset; there is no third party to restore ownership rights in the event of theft or loss.

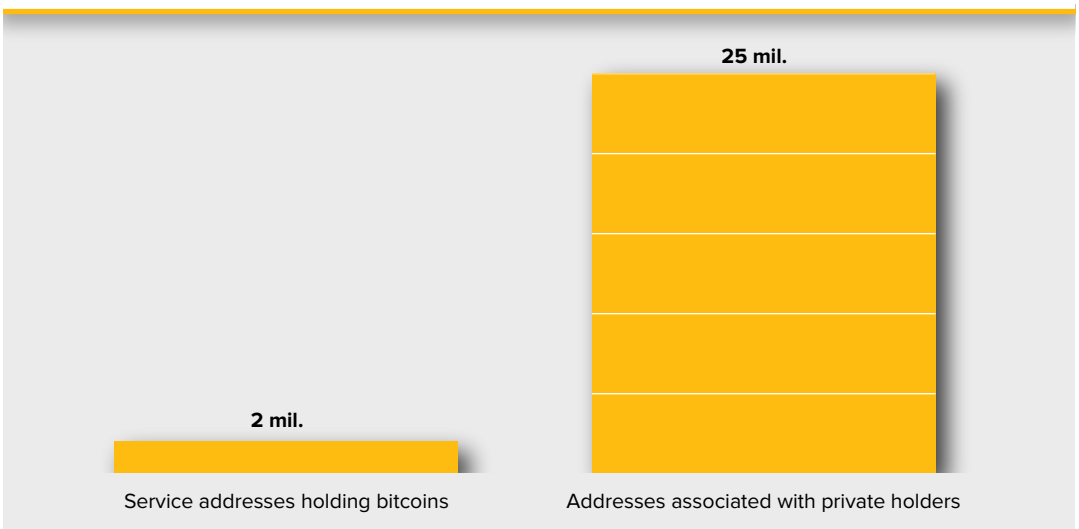
Advantages conferred by crypto's bearer asset status

As bitcoin's "digital gold" narrative strengthens, this bearer asset quality becomes its salient value proposition. As long as governments exist that will not liberalize their national economies, this will be an attractive quality. China is the most prominent example today; as nations lean toward protectionism, use of capital controls may increase. Even in liberalized economies, like the U.S., increasingly loud voices call for progressive tax proposals – another stimulus to demand for assets beyond the reach of governments.[1]

While service providers and private holders use bitcoin addresses differently, and the amount each group holds is difficult to pinpoint, this chart shows the extent to which bitcoin is held by individuals, rather than custodians.

Figure 1. Bitcoin custody is different

Far more of bitcoin's addresses belong to private holders than to service providers



Source: Chainalysis, "Mapping the Universe of Bitcoin's 460 Million Addresses," December 2018, Retrieved July 22, 2019.

Risks & limitations in crypto's bearer asset status

As such, bitcoin is unlike any other digital asset known to investment advisers. Loss of control of a bitcoin account's private key, through cyber attack or mishap, means losing that account's bitcoin – there is no recourse. Safeguarding a key on behalf of clients is a risk that makes fund managers uncomfortable. In some jurisdictions, it may be one that they cannot legally undertake since they cannot "guarantee" its security.

1 Tyler Cowen, "Bitcoin Is (Probably) Here to Stay," *Bloomberg*, June 28, 2019.

Under U.S. securities regulations, custody compliance is complex, and subject to frequent no-action letters and clarifying statements from the Securities and Exchange Commission (SEC). In familiar asset categories, investment advisers already face risk of noncompliance with custody laws.[2] With a new type of asset that runs on an unfamiliar technology, the risk is greater.

Unease with a novel asset category, in which custody requirements have not been specifically defined, is understandable. For many institutions, given the relatively small size of the asset category,[3] the risk is not yet worth the potential return. Providers, both startups and incumbent financial institutions, perceive growing demand and are working to develop secure custody solutions that meet institutional clients' needs.

For many institutions, given the relatively small size of the asset category, the risk is not yet worth the potential return.

2 Kelley A. Howes, "The Custody Rule Under the Investment Advisers Act: Time for a Change," *IAA Newsletter,* November 2017.

3 Galen Moore and Noelle Acheson, "Crypto in Context: The Social and Technical Underpinnings of an Emerging Asset Category," *CoinDesk*, July 2019.

CUSTODY SOLUTIONS FOR INSTITUTIONAL INVESTORS

Unlike other exotic, new financial instruments, crypto assets caught on first with retail investors. For many of this asset category's earliest innovators, the ability to self-custody a digital asset was what made bitcoin attractive. Some holders use systems as simple as writing down private keys on paper. Others rely on dedicated offline hardware devices. As bitcoin grew, many among its successive waves of adopters required a less hands-on way to secure assets. Early service providers responded, offering managed custody solutions.

For many of this asset category's earliest innovators, the ability to self-custody a digital asset was what made bitcoin attractive.

Nothing could be more remote from this retail custodian landscape than the custody banking business in more established asset categories. Size and longevity are preferred in a custodian bank. The top four custodians (BNY Mellon, State Street, JPMorgan and Citigroup) together have centuries of experience and more than $100 trillion in assets under custody.[4] These four do not, at this writing, offer crypto asset custody, though BNY Mellon will store bitcoin private keys for Bakkt, a startup[5] developing bitcoin custody and futures offering, in a unique partnership with that firm.

There are crypto custodians targeting the institutional market, but none yet on the scale of the giants. Fidelity Investments, through its subsidiary, Fidelity Digital Assets, is bringing to market a custody offering backed by one of the largest and best-known financial services brands in the market. Northern Trust, with assets under custody and administration of $10.9 trillion[6] was reported last year to be developing a custody offering.[7] That offering has not emerged yet, but Northern Trust remains outspoken in the area of crypto assets and offers other services to crypto investors, including fund administration.[8]

CoinDesk has identified more than 40 service providers offering stand-alone custody services. Many are marketing themselves as "qualified custodians," a term used by US regulators to describe custodians certified to operate on an institutional scale. It's not clear what that term may mean in the context of crypto: US regulators have not yet specified what infrastructure, governance or controls would be required for qualified custody of crypto assets.

CoinDesk has identified more than 40 service providers offering stand-alone custody services.

Table 1: Largest known custodians of crypto assets

Name	Headquarters	Assets under custody (US$ bil)
Kingdom Trust	US	$12
Xapo	Switzerland	$5.5*
Coinbase Custody	US	$1.3
Bank Frick	Liechtenstein	$0.8

*Reported figure, not confirmed by the custodian

Source: CoinDesk research

4 Trefis Team, "Largest Custody Banks Saw Negligible Growth In Their Asset Bases Over Q2," *Forbes*, August 8, 2018.

5 Nathan DiCamillo, "How a Startup Fits Into BNY Mellon's Blockchain Strategy," *American Banker,* June 3, 2019.

6 Northern Trust, "Northern Trust Makes Key Business Development Hire for Private Capital Administration Practice," Business Wire press release, July 1, 2019.

7 Olga Kharif, "Northern Trust Looks to Join Burgeoning Crypto Custody Business," Bloomberg, July 31, 2018.

8 Jonathan Watkins, "Current Crypto Ecosystem Not Yet Viable for Institutional Investors, Says Northern Trust," The Trade Crypto, May 1, 2019.

Most crypto custody providers have not publicly discosed assets under custody. The table above lists the four largest known custodians of crypto assets, by assets under custody as stated by the firm or reported by others.

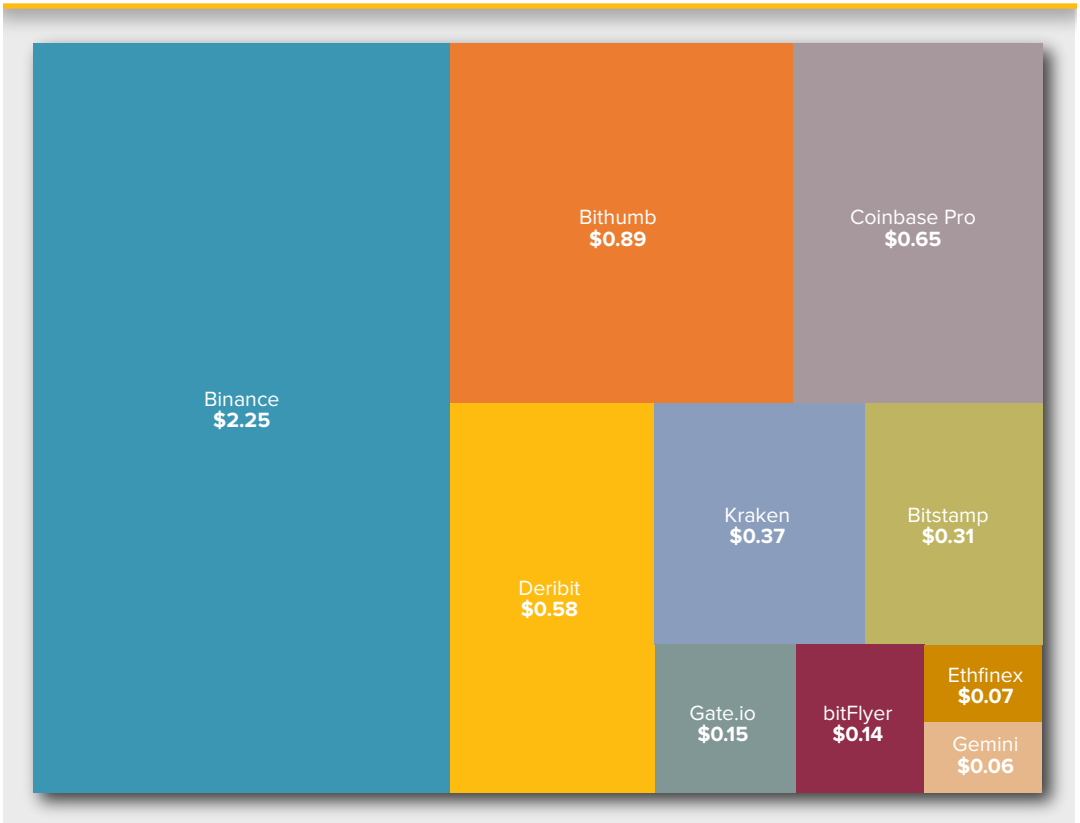
"Exchange" custody

Among the largest custodians of crypto assets today are so-called crypto "exchanges," catering mostly to retail investors, the largest among them operating outside US financial regulation. Traders hold crypto assets on deposit with the exchanges, where they are ready for fast transactions across the dozens of crypto-asset trading pairs the exchange may list. In this, the custodial exchange acts as both custodian and venue, a service relationship with the investor that is not duplicated outside of this new investment category. Some custodial exchanges also carve out specific custody offerings for larger investors, and the ability to trade from those custodied funds on credit is now emerging as a component of those offerings.

The custodial exchange acts as both custodian and venue, a service relationship with the investor that is not duplicated outside of this new investment category.

Figure 2. The hybrid custodians

Largest custodial crypto exchanges by 24-hour volume, US$ bil



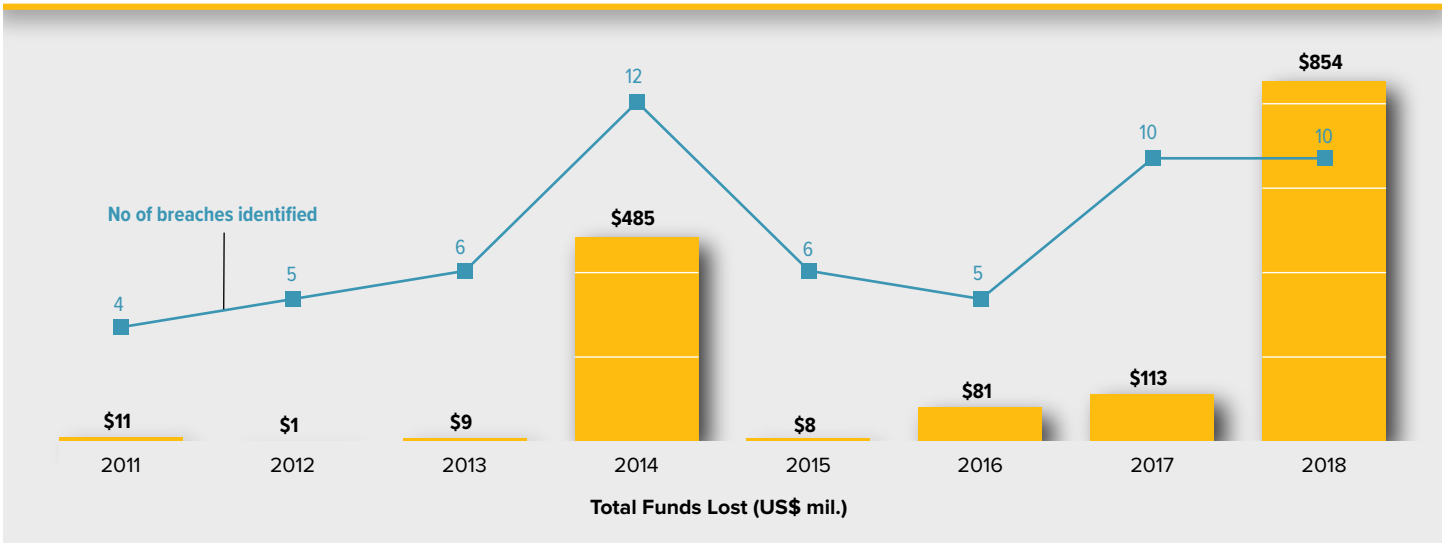
Source: nomics.com/exchanges, retrieved July 9, 2019, 1425 EDT

Exchange hacks

As concentrators of crypto assets, exchanges have presented thieves with an attractive target. The history of high-profile crypto asset theft goes back to Mt. Gox, one of the first platforms that allowed users to trade bitcoin for fiat currencies. At a time when few options available for trading or custody, Mt. Gox was an on-ramp for many among the first waves of bitcoin's early adopters. Its collapse after $450 million worth of cryptocurrency was found to be missing was a rude awakening to the vulnerability of digital assets, especially those stored in so-called "hot wallets," or accounts managed on connected machines.

Figure 3. Crypto custody's checkered past

Bitcoin losses resulting from known security breaches at service providers



Source: Michel Rauchs et al., "2nd Global Cryptoasset Benchmarking Study," Cambridge Centre for Alternative Finance*, December 2018, p. 63.*

CRYPTO CUSTODY TECHNOLOGY

The mechanisms to secure ownership of stocks, bonds and even gold are well understood. Despite occasional mishaps, like the creation of millions of phantom shares of Dole Foods stock in 2013,[9] these mechanisms are trusted. Crypto assets' security is built on cryptography that is novel to many and sometimes difficult to understand. What follows is a brief description of some of the elements of the technology that secures bitcoin.

Public and private keys: Every time a user creates a new account, bitcoin's software applies a cryptographic algorithm to generate paired keys, one public and one private. The public key is like an address: any other account on the network can send bitcoins to that address. The private key is like a signature: any bitcoins coming from an address must be signed with the private key that is cryptographically paired with that public key. Transactions and signatures can be completed without revealing the private key to others. Whoever knows the private key has the ability to send funds from the account, without limit.

Wallets: It is possible to interact directly with the bitcoin protocol using public and private keys, but most bitcoin users rely on a software application called a "wallet," provided by someone else. Wallets provide a user interface with a record of transactions and functions like sending and receiving funds. They sometimes include security features, such as alerts and daily transaction limits. The term "wallet" can be misleading, because a bitcoin wallet does not actually contain any funds. Think of a wallet as the app that provides access to bitcoin's distributed database of transaction and ownership records.

Hot storage: Since a private key is needed to sign every transaction, traders, exchanges and others that need to transact frequently may keep their private keys handy, on computers or mobile devices that are "hot," i.e., connected to the internet. They accept the risk that a connected machine is vulnerable to security breach. Security best-practices dictate keeping a limited percentage of total funds stored in this easy-access manner.

Cold storage: Cold wallets maintain private keys on dedicated computers, disk drives or even hard-copy records that are not connected to the internet. During transactions, a cold-wallet device must be connected to the network; it should be able to sign transactions internally, without transmitting private keys in a way that could be compromised.

Cold wallets maintain private keys on dedicated computers, disk drives or even hard-copy records that are not connected to the internet.

Multi-signature: We discussed earlier the security features that wallet providers can offer. Bitcoin itself has some simple security capabilities at the protocol layer. One of these is multi-signature addresses. These are public keys that require signatures from multiple private keys, in order to send funds. Think of a multi-signature wallet as being similar to the two keys required to open a safe deposit box: one is held by the bank, the other by the account holder.

Institutional custody's future road map

Technologies described above provide the tool set for secure custody of crypto assets. Using these technologies and applying their own governance and control frameworks, custodians can securely custody crypto assets for their clients. Responsible custodians exist that have track records securely managing hundreds of millions of dollars worth of crypto assets. However, as the table of the largest known crypto custodians shows, the largest custody banks have not yet brought a crypto custody offering into this market. The custody options available to professional investors remain limited and relatively immature. For many institutions, custody remains an operational obstacle to investment. Below are some of the milestones that must be crossed before that will change.

9 Matt Levine, "Dole Foods Had Too Many Shares," *Bloomberg Opinion,* February 17, 2017.

Technological milestones

- **Controls:** The technology involved in securing crypto asset ownership is not new to banking institutions. What is new is the introduction of a digital bearer asset. Custodians must develop controls and governance to custodize private keys and effect their transfer into and out of custody.[10]
- **Audits:** In addition to confidence in their own technology, crypto custodians must have confidence in the code behind crypto wallets, clients and the protocol itself. Technical security audits are required that will encompass the risks and benefits of crypto.
- **DeFi:** As digital-only investments, crypto assets may be programmed in new ways. So-called "decentralized finance," or "DeFi," allows holders to lend assets or post them as collateral programmatically, across peer-to-peer networks. How might custodians handle a demand for both agility and security in crypto assets?
- **Forks:** Assets that, like bitcoin, are based on open-source code may be "forked," with new coins issued to the holders of the precedent asset, as in the emergence of Ethereum Classic in 2016.[11] How will custodians handle custody of newly minted assets that may be due to their clients?

Regulatory milestones

- **KYC/AML:** Financial Action Task Force guidelines released in June 2019 provide significant clarity for crypto asset service providers related to know-your-customer (KYC) and anti-money-laundering (AML) policies.[12] Questions remain as to how institutions will implement these guidelines, and what will be the viability of assets that do not flow through these sanctioned channels.
- **Liability:** No audit is perfect. Crypto assets custodied by a bank may be vulnerable to theft due to security flaws beyond the bank's visibility and its control. Who would be liable for such a loss?
- **Qualification:** Earlier, we discussed problems in the way some crypto asset custodians use the term "qualified custodian," as US regulators responsible for setting the meaning of that term have not yet defined it for crypto assets. This may be the largest obstacle of any to institutions' comfort with custody solutions for crypto assets.
- **Insurance:** Large insurers have been more nimble than large custodians to offer policies covering loss of crypto assets.[13] It remains to be seen whether insurance will be required of qualified custodians, and if so, how much it will cost.

10 Kara Kennedy, "Crypto Custody," *BNY Mellon, r*etrieved July 9, 2019.

11 Pete Rizzo, "Ethereum Hard Fork Creates Competing Currencies," *CoinDesk,* July 24, 2016.

12 FATF, "Virtual Assets and Virtual Asset Service Providers: Guidance for a Risk-Based Approach," June 2019, retrieved July 9, 2019.

13 Philip Martin, "On Insurance and Cryptocurrency," *The Coinbase Blog,* April 2, 2019, retrieved July 14, 2019.

NON-CUSTODIAL TRADING

Many retail investors have looked for ways to transact in crypto assets without ever putting their funds on a centralized exchange. These investors have turned to so-called “decentralized exchanges,” or “DEXes,” which allow participants to transact without giving up custody to a middleman. Decentralized exchanges allow investors to transact without exposure to third-party risk. Some decentralized exchanges also present an attractive option to those who wish to avoid government oversight of their transactions.

Non-custodial trading

While DEXes have grown out of bitcoin users’ desire to develop an alternative to government-controlled investment avenues, there are areas in which the interests of individualist bitcoin holders intersect with those of major institutions. Professional crypto investors also would prefer to trade across multiple venues without having to accept multiple custodians. Professional investors may also wish to achieve a higher degree of privacy than exchanges can offer. With these market needs in mind, some providers have emerged offering non-custodial trading for institutions.

There are areas in which the interests of individualist bitcoin holders intersect with those of major institutions.

CONCLUSION: CUSTODY QUESTIONS TODAY AND FOR THE FUTURE

For the investor exploring self-custody today, there are many credible resources offering advice on the best ways to do so securely. We offer a list of such resources in an appendix, below.

For those seeking a crypto asset custodian, a handful of firms have reached scale, longevity and transparency such that early waves of institutional investors, like pure-play crypto funds and venture capital firms, are trusting them to custody assets. The table of the largest known crypto asset custody providers, above, serves as a guide to some of these firms. It will be updated as we gather new information from these custodians. To receive updates, sign up here.

Meanwhile, a road map is in view to a more broadly acceptable set of custody solutions. These solutions are not here today, but it is reasonable to expect they will arrive if demand continues to grow for bitcoin as an investment, and even if it doesn't, to satisfy existing demand.

A road map is in view to a more broadly acceptable set of custody solutions.

However, there are other areas where the technological challenges seem thornier and less likely to be solved. For example:

Custody of title: Many advocates of broader use of crypto assets point to real estate, especially in emerging markets, as an area where minimizing trust in central institutions can increase trust in the sanctity of ownership records. However, in a truly trust-minimized network, such as bitcoin, private keys once lost cannot be restored. What would happen to real property in the event of title theft or loss?

Custody of securities: So-called "security tokens" are another area of crypto asset technology development that has generated enthusiasm. Securities issued on a public blockchain could trade peer-to-peer, with compliance programmed into the assets themselves. What would happen to Apple's stock if a 5 percent holder lost track of the private keys?

Custody of identity: In most countries, government offices are prepared to furnish a replacement for a lost birth certificate or passport. How would that work in an environment where control over those identification documents is proven on a peer-to-peer basis, using private-key cryptography?

These questions may be answerable at some point in the future. For now, simply asking them points to new opportunities and challenges that arise with the emergence of the world's first form of truly digital proof of ownership.

Bitcoin is a global financial network that anyone with a computer and an internet connection may access. As such, it suggests new possibilities in global finance, such as cross-border lending and investing. However, many of those possibilities are founded on bitcoin's bearer asset qualities. These qualities bring challenges in custody that are central to unlocking the potential perceived in crypto assets, whether as a store of value as bitcoin is known today, or in other applications yet to be demonstrated.

RECOMMENDED READING

Custody, Trading, Staking (AVC) – May 2019
https://avc.com/2019/05/custody-trading-staking/?ref=usvwidget

SEC must solve its cryptocurrency custody conundrum
(Financial Times, paywall) – May 2019
https://www.ft.com/content/6411aaff-dd80-382f-ab1c-80cae225673d

Control as Liability (Vitalik Buterin) – May 2019
https://vitalik.ca/general/2019/05/09/control_as_liability.html

Crypto Asset Safekeeping and Custody: Key Considerations and Takeaways
(Global Digital Finance) – April 2019
https://www.gdf.io/wp-content/uploads/2019/02/2_2_2019-Crypto-Asset-Safekeeping-draft-for-mini-summit.pdf

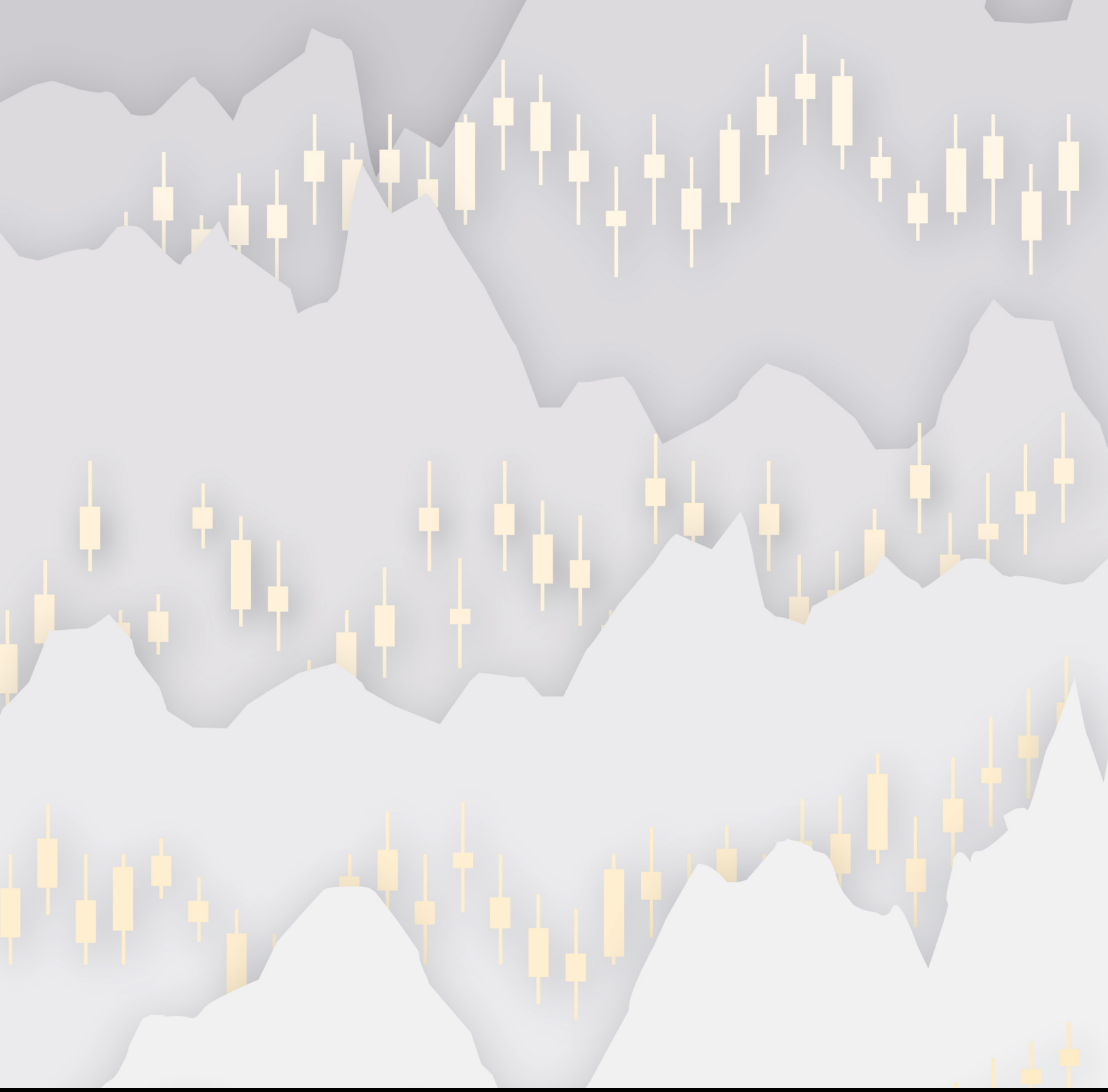
Cryptocustody: What you need to know (Freshfields Bruckhaus Deringer LLP) – April 2019
https://www.lexology.com/library/detail.aspx?g=fcfe6cbd-e5e2-4832-be48-327bfb061645

Engaging on Non-DVP Custodial Practices and Digital Assets (SEC) – March 2019
https://www.sec.gov/investment/non-dvp-and-custody-digital-assets-031219-206

Busting Myths About Cryptocurrency Custody (Fortune) – Feb 2019
http://fortune.com/2019/02/21/cryptocurrency-custody-misconceptions-coinbase-ceo/

Four Crypto Gospels: [1] Custody (Su Zhu, via Medium) – Dec 2018
https://medium.com/@suzhu/four-crypto-gospels-1-f152fd245824

The Crypto Custody Conundrum (Crowdfund Insider) – Oct 2018
https://www.crowdfundinsider.com/2018/09/139614-the-crypto-custody-conundrum/



coindesk®