Managing Risk for the Next Wave of Digital Currencies

July 2023

By Bernhard Kronfellner, Steven Alexander Kok, James Mackintosh, and Christian N. Schmid (BCG); Mike Balestrino (B Capital); and Samir Ghosh (FalconX)

BCG + B Capital + FALCONX

Managing Risk for the Next Wave of Digital Currencies

The digital-currency marketplace has been in turmoil since the current "crypto winter" began in mid-2022. Holdings have been breached, fraudulent and illicit schemes have been revealed, and digital-currency offerings have lost value, making the risks more evident.

(For an overview of what led to the crypto winter, and of where things stand now, see the sidebar "DeFi Summer, Crypto Winter, and the Future.") Recent actions by the US Securities and Exchange Commission (SEC) have further ensured that the risks of digital currency will be top of mind for investors for some time to come.

At the same time, digital currencies are here to stay. Their primary function—to hold and transfer value without a central authority validating and processing transactions—will continue to be attractive to investors and other financial services customers. In addition, the rapid pace of innovation continues. Financial institutions have a duty to provide the same level of asset-specific offerings, capabilities, and guardrails that they do with other comparable asset classes.

This presents financial institutions with a series of strategic challenges. Chief risk officers (CROs) should be asking two questions. First, what are the most important new risks associated with digital currencies? Second, how to best manage those risks? For both these questions, financial institutions need to pay attention to the factors unique to digital currencies—requiring new practices, methods, and ways of thinking.

In this article, we aim to describe the risks that come with supporting and offering digital currencies, as well as appropriate tools and methods to mitigate them. As long as clients demand access to digital currencies, from basic ones to stablecoins and even central bank digital currencies (CBDCs), these risk-mitigation tools should become part of the operating model of most banks and financial services organizations.

Risks Associated with Digital Currencies

While digital currencies are available in a variety of forms and flavors (see the sidebar "A Guide to Digital-Currency Products and Services"), they can all be assessed against common risk categories relevant to financial institutions. Exhibit 1 shows these categories arranged roughly in order of the source of risk—from broad market forces to particular actors in the digital-currency ecosystem to gaps in the financial institution's own range of capabilities.

DeFi Summer, Crypto Winter, and the Future

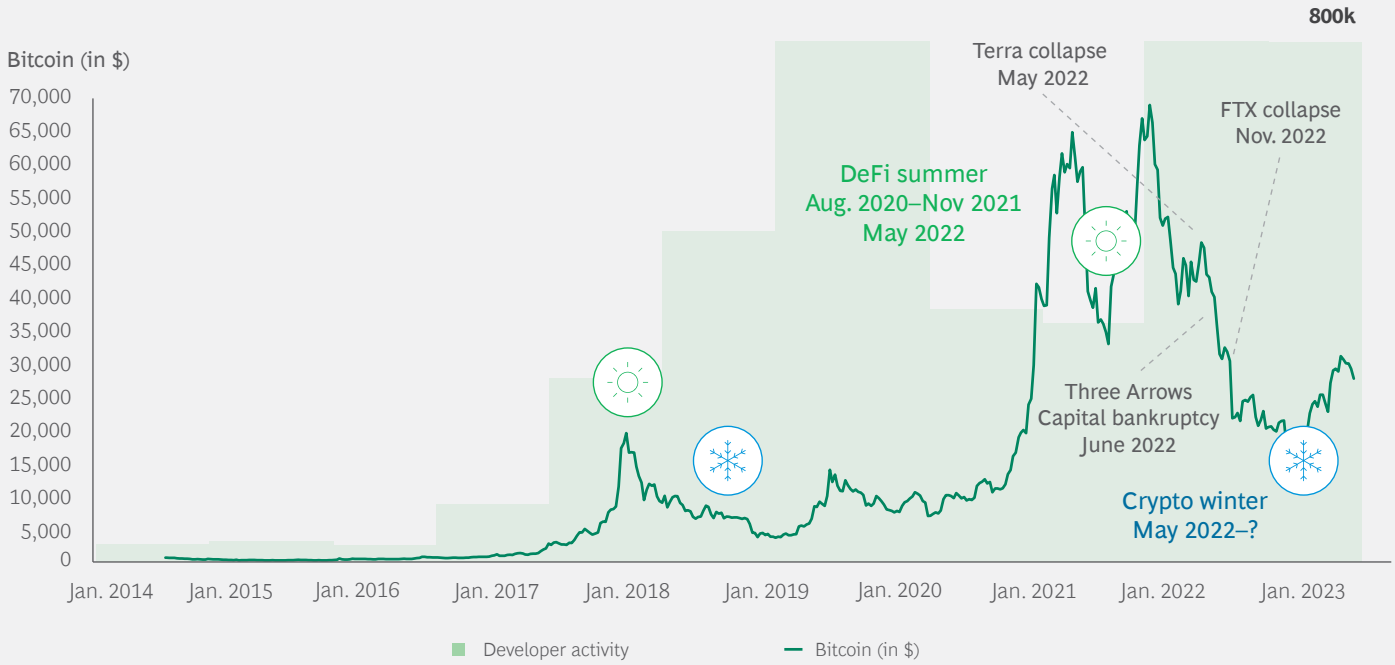
Many investors acquired digital-currency holdings during the steep upswing of "DeFi summer," which began in August 2020. As the COVID-19 pandemic surged, so did the value of decentralized finance (DeFi) offerings. (See the exhibit.) Like many speculative investors before them, some asset managers made digital-currency-related bets without fundamental risk-management practices in place.

DeFi summer ended in November 2021. Later came the collapse of the stablecoin Terra in May 2022, followed in June by the bankruptcy of the Singapore-based hedge fund Three Arrows Capital. Then came further interest rate hikes from the Federal Reserve and the FTX bankruptcy. Each time, the risks became clearer, and more investors pulled back. By May 2022, the current crypto winter was fully underway, marked by a steep drop in values. (The term "crypto winter" makes reference to "Winter is coming," the motto of one of the warring houses in the TV series *Game of Thrones*. The motto refers not only to the harshness of winters in the house's continent but also to the inevitability of difficult times.)

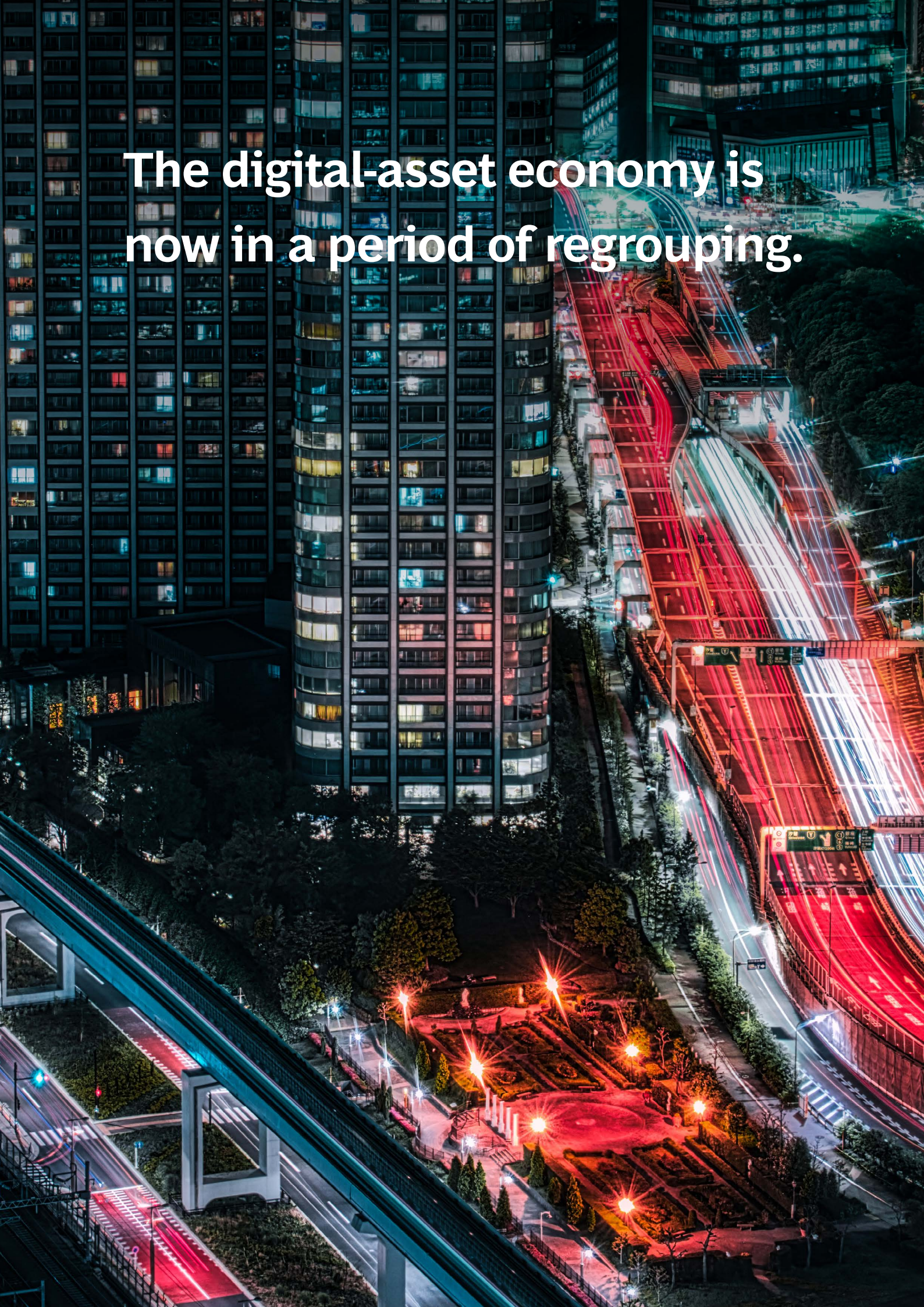
The digital-asset economy is now in a period of regrouping. Analysis indicates a high level of research and development, mostly taking place quietly within innovative companies. As in all bear markets, this is when casual investors and substandard players depart, and digital-asset developers prepare their next wave of offerings.

Developing a risk strategy for digital currencies, including those you already own or oversee, does not mean ignoring the downturn. It does, however, mean continuing to serve customer needs, balancing the value of exposure in digital currencies against the risks and necessary precautions.

Exhibit - Crypto Market Prices vs. Developer Activity, 2014-2023



Sources: Data Statista; CoinMarketCap; BCG analysis.


The digital-asset economy is
now in a period of regrouping.

A Guide to Digital-Currency Products and Services

Main Products

Digital Currencies. These virtual currencies—Bitcoin, Ethereum, and many more—are common financial products that all leverage blockchain technology. Many of them have value primarily as speculative investment vehicles, which increases their volatility and thus affects their risk profile.

Some digital-currency offerings ("coins") have non-speculative value. They are utilitarian, with use cases that include car rentals and the tracing of goods along a supply chain. Because digital currencies are only minimally regulated, a high level of risk monitoring and mitigation is considered best practice for all of them, even those with primarily utilitarian value.

Digital currencies require a system of verification to validate the integrity of each new coin. They do this by linking it credibly to the blockchain. There are two primary approaches. In **proof-of-work** (PoW) verification, each new coin must be generated through mathematical computation, with each successive coin requiring higher levels of processing power. **Proof-of-stake** (PoS) digital currencies verify the value of each digital coin through affirmation by current currency holders, qualified by the number of coins they already have "staked" (committed to keep illiquid).

A typical PoS system is more resistant to cyberattack and uses much less energy than its PoW counterparts. Ethereum converted from PoW to PoS in September 2022, becoming the most prominent digital currency to do so.

Stablecoins. These are digital currencies whose value is pegged to the value of another currency or commodity by the algorithm. They tend to be backed by other financial assets as collateral and are thus relatively protected from some risks. If a chain's token is collateralized, the digital currency is likely to be a stablecoin.

Central Bank Digital Currencies (CBDCs). CBDCs are a form of digital currency being considered by some central banks or national governments. CBDCs would be released through a national financial infrastructure that would manage the digital ledger system and verification.

Main Services

Centralized Exchanges and Brokerages. These hubs and platforms enable people and institutions to trade digital currencies with fiat currencies or with one another. Exchanges facilitate price discovery and match orders among participants. Brokerages facilitate price discovery and transactions across exchanges. Both exchanges and brokerages provide additional services related to credit and derivatives.

Digital-Currency Storage Services. Also known as crypto wallet services, these may be offered by banks or third-party entities to facilitate the management and safekeeping of digital coins, protecting them from being hacked and enabling the recovery of lost keys. They also provide qualified storage when required by regulations. Cold wallets, which have only an intermittent connection to the internet, are safer from cyberattack than more-connected options. Hot wallets, which maintain an internet connection, allow for more convenient exchanges and transfers of funds.

Payment-Processing Services. Retailers and others who receive payments in digital currency use these services to manage the process. These services are also used for conversion from one digital currency to another.

Custody Services. Other services include digital-currency management, in which intermediaries act on behalf of the currency owner, and security services that oversee encryption, safeguard private keys, and perform some of the risk-mitigation functions described in this article.

Exhibit 1 - Seven Categories of Digital-Currency Risk

1	**Market risk**		Price volatility
2	**Counterparty risk**		Another player's default
3	**Illicit-finance risk**		Fraud, money laundering, etc.
4	**Regulatory risk**		Continuously evolving local government thinking
5	**Security risk**		Theft, loss, and attack
6	**Operational risk**		Including smart contracts and technological challenges
7	**Reputational risk**		Damage to the public image

Source: BCG/FalconX/B Capital analysis.

1 Market Risk: Price Volatility

The risk of getting caught in a speculative bubble or market-driven price cash depends on how speculative the activity is in a digital currency. Stablecoins, which are pegged to fiat-currency values and hold underlying collateral (in the peg currency, or more often in highly liquid assets, such as treasuries), are often marketed as being relatively risk free. But even stablecoins can be volatile, especially when the collateral is inadequate (for example, using yet another stablecoin as collateral), insufficient (not fully backed), or algorithmic (stabilized by automatic balance against another stablecoin or underlying collateral pool).

> **Even stablecoins can be volatile, especially when the collateral is inadequate, insufficient, or algorithmic.**

Another issue is the relative lack of market controls that traditionally protect participants from extreme volatility and from borderline-illegal market swings (such as pump-and-dump schemes). In the realm of digital currency, market controls are still catching up, and this can become problematic when a firm is offering clients near real-time exchange for fiat payment purposes. For example, having a wallet that holds bitcoin, and converts to fiat at the point of purchase, can lead to challenges in terms of liquidity management, internal trading pools, and customer expectations. These challenges might result in constraining the offering of some services to a subset of digital currencies, or taking other mitigation measures (described later).

2 Counterparty Risk: Default from Other Participants

The intrinsic characteristics of digital currencies make them akin to a non-transparent illiquid asset. Moreover, while in principle they are decentralized by design, liquidity is channeled via a rather constrained set of market participants (most notably, digital-currency exchanges) that for all intents and purposes have been subject themselves to significant challenges. The challenges for exchanges range from ineffective internal controls to issues mostly related to proprietary-trading-style failures (in some cases, driving these exchanges to bankruptcy). If either these exchanges or some holders of a digital currency cannot meet their obligations, or appear to be likely to default, the value of the digital currency can drop rapidly. As with derivatives markets, losses from counterparty risk can spread rapidly across a digital-currency ecosystem, creating a high level of volatility that affects other asset classes as well. This poses a difficult conundrum for financial institutions from a customer-protection perspective: customers are essentially holding an asset that is perceived to operate as a currency (with market fluctuations akin to those in the foreign-exchange market), but they are exposed to a rather different risk profile, driven by the intrinsic nature of the digital currency and the operating quality of the ecosystem that supports it.

3 Illicit-Finance Risk: Questionable Actors

One common concern about digital currencies is the extent to which fraud, money laundering, price manipulation, and deceptive activity are prevalent. While in absolute terms, the share of fraud related to crypto globally is not large, it can still be material: according to the *Financial Times*, cryptocurrency scams increased by more than 41% in England and Wales (and presumably elsewhere) between 2021 and 2022. The risk of illicit finance challenges the core banking services of value custody and fraud protection.

Practices like "rug pulls"—where promoters withdraw transactions from a digital-currency offering after selling it, thereby diluting its value—are like conventional pump-and-dump schemes. The digital-currency market, in part because of its cross-jurisdictional nature, does not have the same level of protections and controls in place that have evolved over hundreds of years in the financial services industry. But even if all these controls were in place, digital currencies are designed to support person-to-person transactions, without banks or other oversight groups as intermediaries. This exposes clients to the risk of fraud.

4 Regulatory Risk: Continuously Evolving Local Government Thinking

Governments around the world are developing new rules for digital currencies. The SEC, for example, in its June 2023 lawsuit against Bitcoin and Coinbase, named 19 cryptocurrencies as securities, thereby setting the stage for potential regulatory changes. The uncertainties around this case will require attention, and add incremental costs in the servicing of digital currencies. More generally, the constantly evolving nature of digital-currency regulations means that compliance professionals are paying close attention to shifts in direction, "skating to where the puck is headed."

Banks and other financial institutions have played a relatively limited role thus far in helping to shape regulatory efforts. With digital currencies, where offerings tend to cross multiple regulatory jurisdictions, they may have a larger role to play in the future. (See the sidebar "The Call for Digital-Currency Regulation.")

5 Security Risk: Vulnerability to Theft, Loss, and Attack

If not properly secured, digital currencies are vulnerable to theft, loss, and cyberattack. (According to Chainalysis, a large blockchain-analysis firm, $3.8 billion were stolen from digital-currency businesses in 2022, especially from DeFi protocols. Overall, illicit addresses sent nearly $23.8 billion worth of cryptocurrency in 2022, a 68% increase over 2021.) Intruders can steal or deplete digital-currency holdings, and they may also capture private keys (the cryptographic codes used to gain access to holdings). If private keys, passwords, or wallets are stolen or lost, their value may be unrecoverable. Many of the blockchain-intelligence and anti-money-laundering methods described later, in the risk-mitigation section, have evolved to manage security risk.

> **Illicit addresses sent nearly $23.8 billion worth of cryptocurrency in 2022, a 68% increase over 2021.**

Intrinsically, the custodian model for digital currencies is different from custody for any other asset class. In other asset classes, a bank has a single omnibus structure to manage the aggregate exposure to the market (this is typically done with retail securities holdings, for example).

With digital currencies, at the most basic level, banks provide custody to safeguard the key to the holdings. At a more nuanced level, banks can provide customers with an ongoing view of the digital currency's exposure to market risk. Beyond that, banks have limited recourse to support customers, making deposit insurance costs potentially higher. A model similar to other asset classes, recognizing the customer's full level of market exposure, might be preferable. Forthcoming evolutions of digital currencies essentially aim at a higher level of "self custody" as a precondition for peer-to-peer transactions. This, in principle, could reduce transaction costs and offer a jurisdictional payment rail at the potential expense of transferring custody risk to customers.

6 Operational Risk: Complexity, Smart Contracts, and New Technologies

Digital currencies have more underlying complexity than other types of value storage and transfer mechanisms. Typically, they are supported by founding companies (arguably, with the notable exception of bitcoin), with complex and somewhat opaque governance structures (such as decentralized autonomous organizations). Also, they often involve novel technologies and behavioral patterns. As a result, it's possible to lose track of all the ramifications of how the value of the currency should evolve, along with the consequences of any given trade that supports or underpins digital currencies. Some digital-currency investors may have been caught unaware by this complexity.

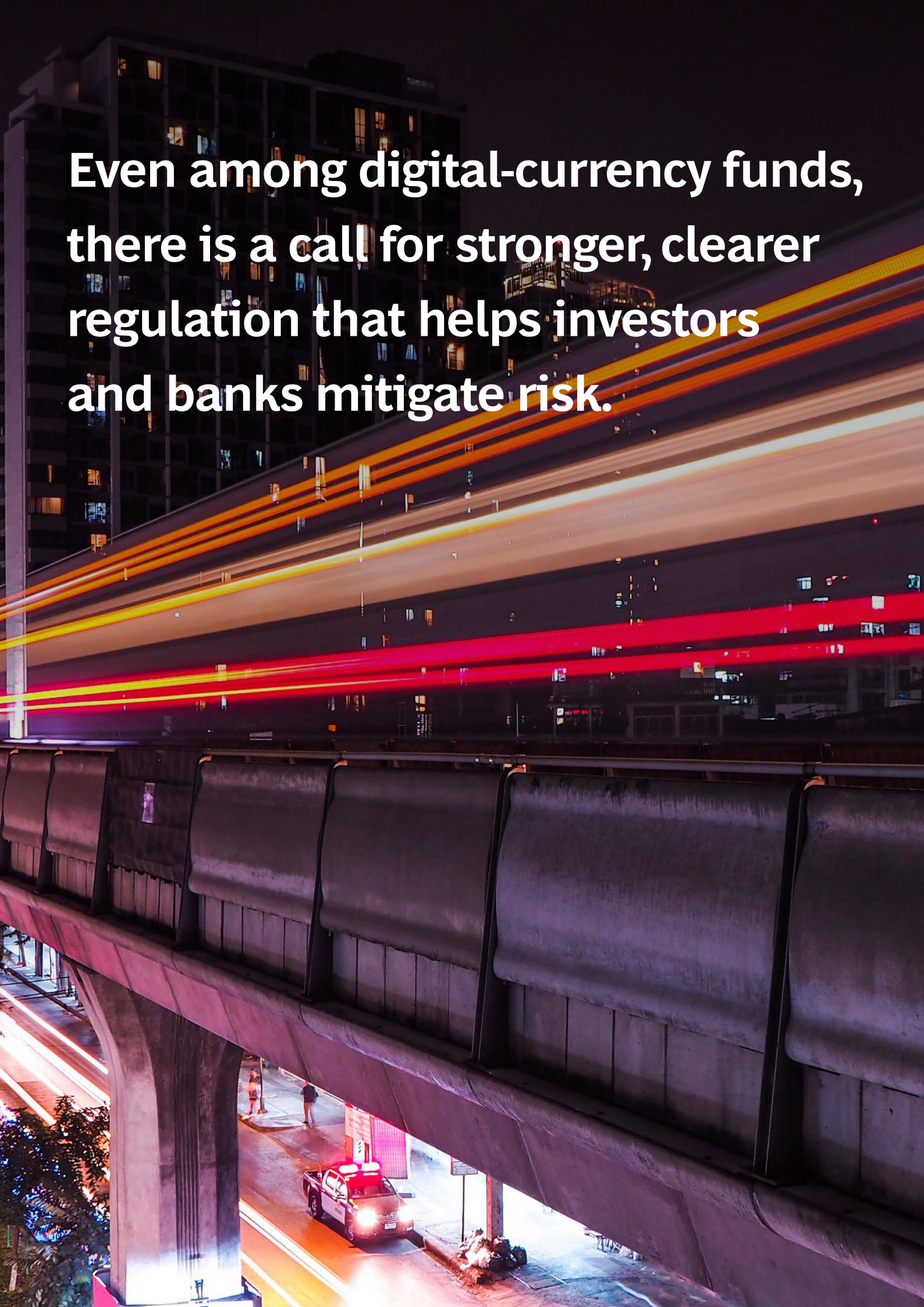
The Call for Digital-Currency Regulation

Even before the SEC actions, many observers were calling for stronger, clearer regulation and more transparency. Regulatory agencies around the world are in the process of finalizing such regulations or at least are developing plans for them. Also, in October 2022, the Financial Stability Board, an international organization that makes recommendations about the global financial system, proposed stricter regulation of crypto assets—in particular, stablecoins—among the nations with the 20 largest economies (the G-20 nations). The Global Financial Markets Association expressed support for this proposal, stating: "In a fast-evolving and competitive environment, it is important for global standard setting bodies to promote the coordination of an effective and aligned global regulatory framework."

Even among digital-currency funds, there is a call for stronger, clearer regulation that helps investors and banks reduce and mitigate risk. Stakeholders ask that the codes and applications be fair, and that the regulations reflect a solid understanding of the technology and its value.

Regulators are well placed to convene the conversations that the industry needs most, with the right people in the room, ready to listen to one another. Crypto-native institutions should be included in early discussions. They have the expertise and hands-on experience to recommend a feasible approach.

Regulators will discover with digital currencies what they have discovered with many other technologies. For every major new technological advance, a balance must be struck between conflicting priorities. In this case, those priorities include innovation, customer privacy, and the transparency needed by law enforcement to track illicit activity.



Even among digital-currency funds, there is a call for stronger, clearer regulation that helps investors and banks mitigate risk.

Consider forking, which takes place when some participants choose not to follow or recognize the original consensus protocol. Instead, they spin out a competing record of transactions, as if creating an alternate timeline. Each path may have its own transaction record, controlled by its own community. In some cases, this is done deliberately—to create new currencies, for example. Nonetheless, the paths share a common history and often assets. This produces a risk of losing value or control.

Another operational risk is an error in a smart contract, a core tenet of many digital-currency and other blockchain-related applications. In simple terms, a smart contract represents the intention to codify automatic execution and provide the code some sort of power of attorney. For example, a smart contract might specify that an automatic sale of digital currencies will take place under pre-established conditions (like a complex standing order). In general, derivative contracts can be linked directly to digital-currency investments so that options can be executed directly and automatically. A mistake in the drafting and coding of that contract could lead to an automatic transaction that was not intentional—and that could lead to substantial accidental losses. Once executed, there is essentially no recourse.

7 Reputational Risk: Damage to the Public Image

Big losses and major missteps in digital currency tend to be widely reported events. With digital currencies, losses result from exposure to the ecosystem, and unlike fiat currencies, their perceived stability is unrelated to how a country or government performs. Reputational damage may result from the sudden collapse of a vendor or exchange, the exposure of a mining scam or Ponzi scheme, a malware outbreak, the rapid decline of utility tokens, or backlash against a fraudulent initial coin offering or wallet service. Although some threats to a bank's image may come from public misperception, much reputational risk reflects decisions made by employees at every level of the hierarchy.

How to Mitigate Risks

Banks can mitigate the risks of digital currencies at two levels at once: specific to each investment ("bottom up") and overall ("top down"), with organization-wide capabilities. Exhibit 2 shows risk-mitigation strategies that can be deployed. Typically, these measures are table stakes, and it is unusual to see a bank or other financial services institution adopt more comprehensive measures and do so consistently. By putting a comprehensive set of complementary mitigations in place, financial institutions can ensure that digital currencies are offered and leveraged effectively.

Let's take a closer look at investment-level strategies, and then we'll examine measures that can be taken at an organizational level.

Blockchain Intelligence (BI). Also known as blockchain analytics, BI is a cornerstone capability intrinsic to digital currencies and blockchain in general. To a large extent, it is the foundation of digital currencies' enhanced capabilities, especially when it comes to granular transparency and traceability.

BI is used by CROs, risk executives, law enforcement, and government regulators to detect and mitigate illicit-finance and counterparty risks. Third-party vendors offer increasingly sophisticated AI-based tools and analytic practices for monitoring digital currencies' blockchain transactions.

> **BI is used to detect and mitigate illicit-finance and counterparty risks.**

For example, BI systems can use machine learning to detect patterns in transaction histories that are consistent with money laundering or illicit finance. These systems often connect directly with law enforcement, regulators, and compliance professionals, giving these authorities visibility into real-time financial flows. When there is a problem with a counterparty, investigators can identify the related transactions. This gives banks more ability to reduce risks to their customers.

Anti-money-laundering (AML) techniques are well-established forms of BI oriented toward counterparty and illicit-finance risks, including the financing of terrorism and sanctions noncompliance. There are some specific ways in which key AML controls operate differently in a digital-currency space:

Exhibit 2 - Strategies for Mitigating Investment Risks

	Blockchain intelligence	Asset research	Assessment of vendor and partner relationships	Proof-of-stake participation	Safe storage	Broader mitigation strategies	Building institutional capabilities
1. Market risk	✓	✓				✓	✓
2. Counterparty risk	✓	✓				✓	✓
3. Illicit-finance risk	✓	✓	✓	✓	✓	✓	✓
4. Regulatory risk						✓	✓
5. Security risk	✓		✓	✓	✓	✓	✓
6. Operational risk	✓				✓	✓	✓
7. Reputational risk	✓	✓	✓			✓	✓

Source: BCG/FalconX/B Capital analysis.

- **Know Your Customer (KYC).** KYC evaluates companies and investors when they join the blockchain or digital currency. It continually compiles knowledge of entities' backgrounds, transactional histories, and expected future activity.
- **Know Your Transaction (KYT).** KYT, a recently developed application, evaluates each blockchain transaction as it happens. This is essentially the process of transaction monitoring, extended to the ecosystem level. An effective KYT system can verify in real time that a transfer is not going to a bad actor or a known sanctioned wallet.

Platforms and dashboards for digital currencies, another important BI offering, bring together information related to all seven risk categories. For example, a dashboard might compare counterparties to see which are highly leveraged and cross-check those findings against these parties' KYC and KYT records. These dashboards enable continuous improvement of crypto-related operations.

BI also plays a role in the deployment of automated controls. These allow banks and other financial services firms to continually monitor and improve their practices. Automated controls, for example, can help limit exposure. In some digital-currency investments, rapid liquidity may not be available. Therefore, banks and investors need to keep their exposure within the limits of acceptable risk—even if all the funds pass muster after asset research (discussed next). As discussed previously, digital-currency holders can be hurt by the domino effect from another fund's or exchange's failure, even if they don't hold that fund or do business on that exchange directly. Thus, as with any risky investment, an automatic stop-loss and hedging should be considered as options.

Asset Research. Also known as "do your own research" (DYOR) processes, asset research involves examining the integrity of the business behind a digital currency to see whether investing in it is worth the possible risk, especially given the potential volatility. There should also be fail-safe internal audits for all transactions and smart contracts, before they are finalized.

Those conducting asset research should closely examine the business fundamentals of the digital currency and its sources (for example, founding institutions or even the exchanges themselves), the financial health of the firm, its software and agreement architecture, its balance-sheet structure, provenance, and business model. One indicator of financial health is a robust ancillary revenue stream. This might be a blockchain-as-a-service offering with cybersecurity, insurance brokering, or low-cost digital-currency trading, or a value-creating exchange for airline frequent-flier miles or online-game costumes. Another indicator is the extent to which exchanges have put mitigation processes in place: upholding sanctions, identifying problematic participants, and verifying the identity of counterparties.

Assessment of Vendor and Partner Relationships. As they become more familiar with digital currency, financial institutions may want to reorient their relationships in the larger ecosystem. Preferred vendors may shift to new names, and the relationships with them may need to be more transparent.

Proof-of-Stake Participation. Financial institutions can gain credibility and income by staking crypto funds, using assets dedicated to that purpose. The income, which accrues to any proof-of-stake participant, should not be treated as a return on investment. It consists of transaction fees and inflationary rewards generated by the blockchain protocol, and is thus a separate category of income. These "rewards" are typically partially transferred to clients, creating the perception of higher savings rates versus traditional deposit savings offerings.

Safe Storage. Many banks currently offer a model where they maintain full custody over a customer's cryptocurrency transactions, offering a high level of protection and oversight. By contrast, a fully crypto-style model can be as extreme as transferring custodial responsibilities to the customer. Within this latter model, several basic protection measures can help prevent crypto keys and other critical data from being hacked or lost. These include basic cybersecurity measures, guarding against phishing and intrusion, and protection for digital-currency holdings. The following is a selection of currently used safe-storage solutions:

- **Hot and Warm Storage Wallets.** A third party, such as an exchange, holds the data. Hot and warm wallets are typically connected to the internet, with warm wallets downloaded as computer or phone apps.
- **Cold Storage Wallets.** Also called hardware security modules (HSMs), these physical storage devices are generally separated from other devices or the internet. HSMs are comparable to a brick-and-mortar bank vault: access requires physical proximity.
- **Multi-Signature Protocols.** These wallet-based security systems require several private keys for each transaction.
- **Multi-Party Computation (MPC).** MPC, the most comprehensive approach, is a wallet-based technique for maintaining secrecy and access. Instead of getting a private key, each participant holds a unique encrypted MPC protocol.

There is an expectation that further innovation will allow clients to be offered the potential benefits of digital currencies (including the ability to trade and pay as promised by CBDCs, or as safe storage with stablecoins), without introducing self-custody risk.

Broader Mitigation Strategies. As banks gain experience with these various forms of mitigation, they will naturally look at their offerings differently. Broader risk-related conversations can lead to stronger oversight practices throughout the organization. A scenario-planning exercise, for example, can help banks and investors game out different risk scenarios, stay alert to possible challenges, and respond to risks more successfully when they arise. Scenario exercises can also involve third-party experts and regulators, helping teams gain and maintain expertise.

> **Broader risk-related conversations can lead to stronger oversight practices throughout the organization.**

A direct consequence of these strategic exercises can be a set of decisions about offerings. Depending on the customer base and risk level, some digital currencies might be removed from an offering or given a longer lead time, relative to less controlled exchanges, to bring onboard.

Building Institutional Capabilities. Ultimately, mitigating risk means continuously improving the bank's functional capabilities, and aligning them with its digital-currency strategy and risk appetite. Each offering needs to be considered as part of a larger whole. As new aspects of digital-currency technology appear, and as risk-mitigation techniques evolve, such as protocols, blockchain innovations, or software bridges, banks will experiment with them. These experiments must be transparent, so that the entire organization can learn from them.

To develop these capabilities, leaders should put in place a clearly defined roadmap: laying out the initial digital-currency offerings, the staffing and skills needed to deliver these offerings, the institutional and technical support required, and the guardrails that help protect customers from risk. Some capabilities may involve outsourcing, especially if they require specialized talent.

Financial institutions can also raise their capabilities by instituting company-wide guidelines that specify approved practices for digital-currency offerings, by recruiting and developing employees with an eye to improving risk management, by developing appropriate communications and compliance policies, and by considering insurance lines for smart contracts and other digital-currency transactions.

Conclusion: Moving Forward

Digital currencies, and their various use cases in finance and other industries, are here to stay. Once banks have determined the level at which they want to participate in this business, it is important for them to support their customers with appropriate risk-management practices. This will help banks benefit from new innovations, such as those in CBDCs.

The range of risks and mitigation measures described here may seem complex. However, most banks are already familiar with this level of risk intensity. They already have most of the tools and capabilities they need. The next step is to reorient them to digital currencies, supplement them with specific capabilities related to this asset class, and train people accordingly.

Expertise with digital currencies can be a source of competitive advantage. These financial instruments are still new enough that relatively few people are addressing their customers with the appropriate mix of caution and excitement. Once banks have appropriate measures in place to counter risk, and have people on hand who can guide their customers, they can confidently explore the opportunities and put themselves in a better position for the future.

About the Authors

Bernhard Kronfellner is a Partner and Director in BCG's Vienna office. You may contact him at kronfellner.bernhard@bcg.com.

Steven Alexander Kok is Partner & Associate Director, Technology & Digital Transformation, in BCG's London office. You may contact him at kok.steven@bcg.com.

James Mackintosh is a Managing Director and Partner in BCG's London office. You may contact him at mackintosh.james@bcg.com.

Christian N. Schmid is a Managing Director & Partner in BCG's Munich office. You may contact him at schmid.christian2@bcg.com.

Mike Balestrino is Vice President, Strategy and Operations, at B Capital. You may contact him at mbalestrino@bcapgroup.com.

Samir Ghosh is Head of Product at FalconX. You may contact him at samir@falconx.io.

For Further Contact

If you would like to discuss this report, please contact the authors.

Acknowledgments

The authors wish to thank Sukand Ramachandran at BCG; Kaj Burchardi at BCG Platinion; Vivek Chauhan, Asad Kassamali, Ave King, and Kushagra Shrivastava at FalconX; Thomas Armstrong, Ari Redbord, and Laura Yungmeyer at TRM Labs; and Lorien Gabel, Annalea Ilg, and Ben Spiegelman at Figment for their contributions to this article.

This article was written in collaboration with B Capital and FalconX.

Boston Consulting Group

Boston Consulting Group partners with leaders in business and society to tackle their most important challenges and capture their greatest opportunities. BCG was the pioneer in business strategy when it was founded in 1963. Today, we work closely with clients to embrace a transformational approach aimed at benefiting all stakeholders—empowering organizations to grow, build sustainable competitive advantage, and drive positive societal impact.

Our diverse, global teams bring deep industry and functional expertise and a range of perspectives that question the status quo and spark change. BCG delivers solutions through leading-edge management consulting, technology and design, and corporate and digital ventures. We work in a uniquely collaborative model across the firm and throughout all levels of the client organization, fueled by the goal of helping our clients thrive and enabling them to make the world a better place.

Cosponsors

B Capital is a multistage global investment firm that partners with extraordinary entrepreneurs to shape the future through technology. With more than $6 billion in assets under management across multiple funds, the firm focuses on seed to late-stage venture growth investments, primarily in the enterprise, financial technology, and health care sectors. Founded in 2015, B Capital leverages an integrated team across nine locations in the US and Asia, as well as a strategic partnership with BCG, to provide the value-added support entrepreneurs need to scale fast and efficiently, expand into new markets, and build exceptional companies.

FalconX is the largest, most reliable digital assets prime brokerage for the world's leading institutions. The company provides the most comprehensive access to the deepest global digital asset liquidity. Through its prime brokerage platform, FalconX 360, investors unlock and scale returns faster and more efficiently than any other platform. The company's 24/7, dedicated team for account, operational and trading needs enables investors to navigate dynamic markets around the clock.


Dusit Thani
BCG + B Capital + FALCONX