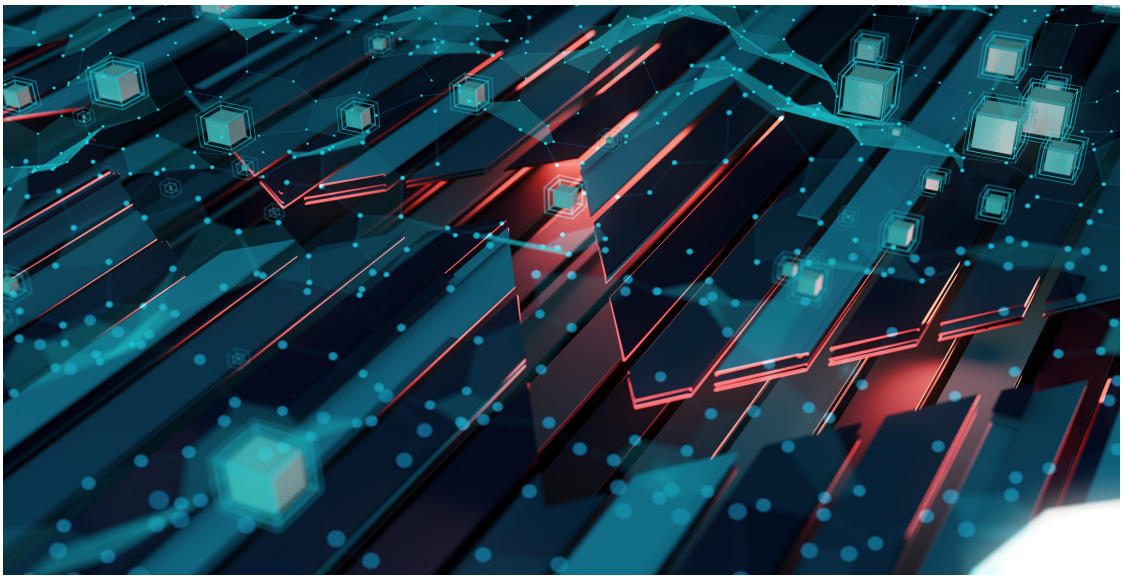
Digital Asset Risk Management

Managing Digital Asset Risk Using an Integrated, Composable Framework

A collaborative report by Chartis and Metrika



Introduction

The growth in digital assets and decentralized finance introduces an important set of risk considerations for CROs, technology leaders and other financial stakeholders. For these entities, failing to address these novel risks demonstrates a lack of diligence in properly recognizing, planning for and investing in the data, analytics, education and infrastructure necessary to not only modernize classic enterprise risk programs and governance, risk and compliance (GRC) systems but also keep pace with financial innovation.

To help firms understand these considerations and their implications, this paper presents a way to frame risk management in the digital asset ecosystem in the context of the traditional risk universe that Chief Risk Officers (CROs) and risk professionals understand today. It also outlines a set of actions for incorporating these considerations and implications into existing enterprise risk management programs.

Executive summary

Because of their dependence on technological foundations and their governance, digital assets and related protocols present a variety of unique challenges for risk managers. These include operational and technological risks, governance risks and protocol security and reliability risks that are not considered directly in existing risk frameworks. These are the foundational asset risks that firms must consider in roughly the same way as they would think about the risks inherent in commodities. As an example, when commodities entered financial markets in the early twentieth century, risk managers had to account for the reliability of infrastructure such as pipelines and grids - factors far less relevant in equities or fixed income. Similarly, digital assets require risk frameworks that consider protocol resilience and governance as foundational, much like infrastructure risks in energy markets.

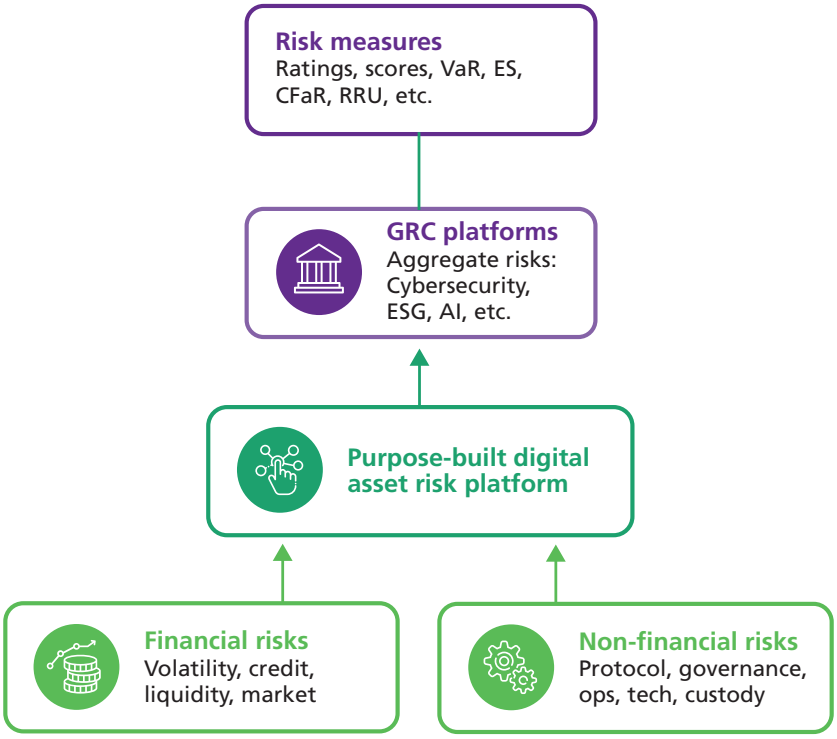
There are foundational differences between digital asset risk and risk in traditional asset classes. The main structural difference is the need to consider the various technological, operational and governance factors involved, the ‘composability’ of the smart contracts and the interoperability of blockchain protocols.

Chartis Research is establishing a new risk category for digital assets and protocols labeled 'integrated composability risk' (ICR), using methodologies and knowledge gained from the introduction of value at risk (VaR) measures and the risks inherent in blockchain technologies. ICR is an integrated risk measure that looks across financial and non-financial risk measures, and combines technology, operational, regulatory and interoperability risks with traditional credit, market and counterparty risks that CROs and risk managers manage today.

- Operational risk and infrastructure providers should work toward data and protocol requirements that would allow for the interchange of blockchain and digital asset data and content and enable interoperability between systems on a global scale.

- CROs and risk professionals should adopt an approach to ICR and modify it as necessary to understand what constitutes effective digital asset risk analysis. ICRs should be informed by, composed, monitored and reported through integrations between classical operational risk systems, the blockchain networks, protocols and the content and systems that support digital assets. An example architecture can exist where purpose-built solutions, which provide real-time monitoring of protocol health, governance transparency and composable risk indicators, can serve as the connective layer between financial and non-financial risk systems and existing enterprise risk management and GRC platforms (see Figure 1).

Figure 1: Where purpose-built digital asset risk platforms fit



ES: expected shortfall; CFaR: cash flow at risk; RRU: risk return units
Source: Metrika/Chartis Research

We will look to define ICR risk via a variety of risks that have developed over the past few years, as well as risk areas that CROs have experience of (such as commodities, credit ratings and credit scores). In a process analogous to that used for credit risk ratings, digital asset ratings leverage ICR data to synthesize a risk-based view of those assets. As in other domains (such as credit ratings for fixed-income issuances), we believe that largely statistical measures of mappings between various technological, operational, governance and interoperability issues that are inherent to blockchain-based assets will emerge and grow, alongside the overall risk of the assets. And based on the evolution of risk measures in other asset classes, and the dynamic and volatile nature of the digital assets' underlying characteristics (including potential dynamic shifts in governance and the software-driven structure of contract terms), we believe that the need for these more statistical, largely automated models will be inevitable.

In this report, we explore the various attributes that such a mapping should have, based on the success and failure of the development of risk measures such as VaR and ordinal risk scores (including credit, cyber and other non-financial risk measures). We also examine complex assets (such as commodities) to learn how this statistical mapping should proceed. We recognize that while some initial steps have been taken – data for the technological, operational, governance and operability elements mentioned above is already being collected and is increasingly commercially available – current mappings (i.e., ratings) are only partial statistical maps, and are largely semi-subjective analyses by ratings analysts.

Based on the evolution of analogous areas such as commodities and non-financial risks, we also argue not only that ratings will be supplemented by other measures (such as VaR, expected shortfall [ES], event probability measures and ordinal scores that capture relative event probability), but also that the risk measures that find adoption will have certain characteristics. When we look to risk-manage commodities, we need to understand the operating environment in which different commodities function, not just their pricing history:

- Bulk commodities: logistics (pipelines, shipping), warehousing, etc.
- Electricity: storage (batteries, pumped storage), network conditions, inertia and other operating characteristics of the network, the logistics of input fuels, weather and climate risk, physical risk to the infrastructure (including generating and distributional assets).
- Gas: very similar to electricity.

The increased commercial availability of ICR data also lends itself to a variety of supplementary analytical models and risk measures that – again in light of the dynamic nature of digital assets – will be central.

Chartis believes that CROs and risk professionals, to understand what constitutes effective digital asset risk analysis, should adopt an approach to ICR and modify it as necessary. ICRs should be informed by, composed, monitored and reported via integrations between classical operational risk systems, blockchain networks, protocols and the content and systems that support digital assets. Risk data aggregation platforms and tools that provide real-time monitoring of protocol health, governance transparency and composable risk indicators can serve as the connective layer between blockchain infrastructure and existing enterprise risk management and GRC platforms, as well as risk analytics layers. These layers could potentially generate a broad range of risk measures (including ratings, scores, VaR measures, cash flow at risk, ES, funding gaps, risk gaps and risk return units).

Throughout this report, we will argue that having multiple risk measures is not a bad thing, and that, with complex composable assets such as digital assets (or their analogues in energy or commodity products or other non-financial risks such as cyber risk), a 'more is more' strategy is optimal, allowing us to capture and control the underlying risks more effectively.

Our approach

In this paper, we:

- Outline and define the ICR concept.
- Consider how CROs should think about it, particularly in the context of the ongoing evolution of traditional risks such as market, credit and counterparty risks, and the inherent risk in blockchain protocols.
- Examine the history of how non-financial risk has been quantified.

ICR is an integrated risk measure that combines technology, operational, regulatory and interoperability risks. In principle, interoperability risks can be classified under technology or operational risks, but we believe – based on the fundamental nature of decentralized finance and digital assets – that interoperability presents a foundational risk challenge.

In our analysis, we draw on the lessons learned from applying various GRC-oriented analytics (and specifically cyber risk quantification) to digital assets and decentralized finance. Increasingly, cyber risk quantification is becoming a standard part of the CRO's ecosystem. But unlike other risk domains, cyber risk models need to synthesize diverse risk factors and technological, operational, behavioral/organizational and regulatory considerations (including privacy laws). Nevertheless, despite the challenges, the quantification frameworks currently available are becoming increasingly robust, providing material support and a degree of due diligence for risk managers.

Context

As the digital asset revolution becomes firmly established, the need for standard structures and flexible risk modeling is becoming increasingly critical. At the same time, regulators are laying down clearer guardrails: the Guiding and Establishing National Innovation for U.S. Stablecoins (GENIUS) Act and the Market Clarity Act are among several new regulations that provide legislative foundations and market structures; joint-agency guidance now allows financial institutions to interact directly with public blockchain networks; the New York State Department of Financial Services (NYDFS) **has issued new guidance** on blockchain analytics; and the Office of the Comptroller of the Currency (OCC) has **set explicit expectations** for digital asset risk management and governance. The recent **repeal of SAB 121** further removes a key obstacle that had discouraged banks from offering digital asset custody, signaling stronger institutional participation ahead.

Against this backdrop, the vast and sophisticated ecosystem developing around decentralized finance and tokenized assets makes it imperative that financial institutions implement risk frameworks that can capture the novel technological, operational and governance risks of these products, while integrating seamlessly with existing enterprise risk management structures.

Risk management techniques and models have been evolving for some time, but the 'Big Bang' for market risk management was most likely the arrival of J.P. Morgan's VaR modeling framework in the 1980s. This didn't mark the 'beginning' of risk management modeling, but rather the beginning of the industrialization of risk management models. Prior to that, considerable foundational work had also been carried out using financial mathematics to price and manage the risk of options and other contingent claims. Since then, there have been key developments: a unified framework for assessing the risk of diverse financial assets, and innumerable extensions to the basic idea (such as measuring the risks of holding illiquid assets or private credit).

The history and the evolution of cyber risk, and the diffusion of risk measures across the financial ecosystem, holds many lessons for how CROs should think about digital asset risk. To begin with, there are many clear analogies: just as cyber risk arises from information moving across internet networks, digital asset risk stems from value being transferred and secured over the public internet. Secondly, the dynamic of collecting new information has radically transformed the techniques and methodologies that can be used. As new technologies emerge that can monitor and store digital network infrastructure in a highly granular way (such as assessing the state of cyber hygiene on specific nodes, the state of all computational nodes in near real time, near misses, etc.), they have enabled deeper, more sophisticated modeling, probabilistic distribution analyses and more sophisticated benchmarking. This has been transformational in terms of making cyber risk more usable.

There are vital lessons to be learned from introducing, adapting and diffusing other risk measures in the CRO's ecosystem – market risk, credit risk, operational risk (from Basel measures) and especially cyber risk – that carry forward into future frameworks for digital asset risk management. They include:

- To interoperate industry-wide, models must be tractable and explainable.
- Risk models must operate at various levels of granularity and should combine a variety of asset types.
- The probability of different risk events should be intuitively clear.
- The underlying statistical framework should be relatively transparent.
- Results should be easily reproducible.

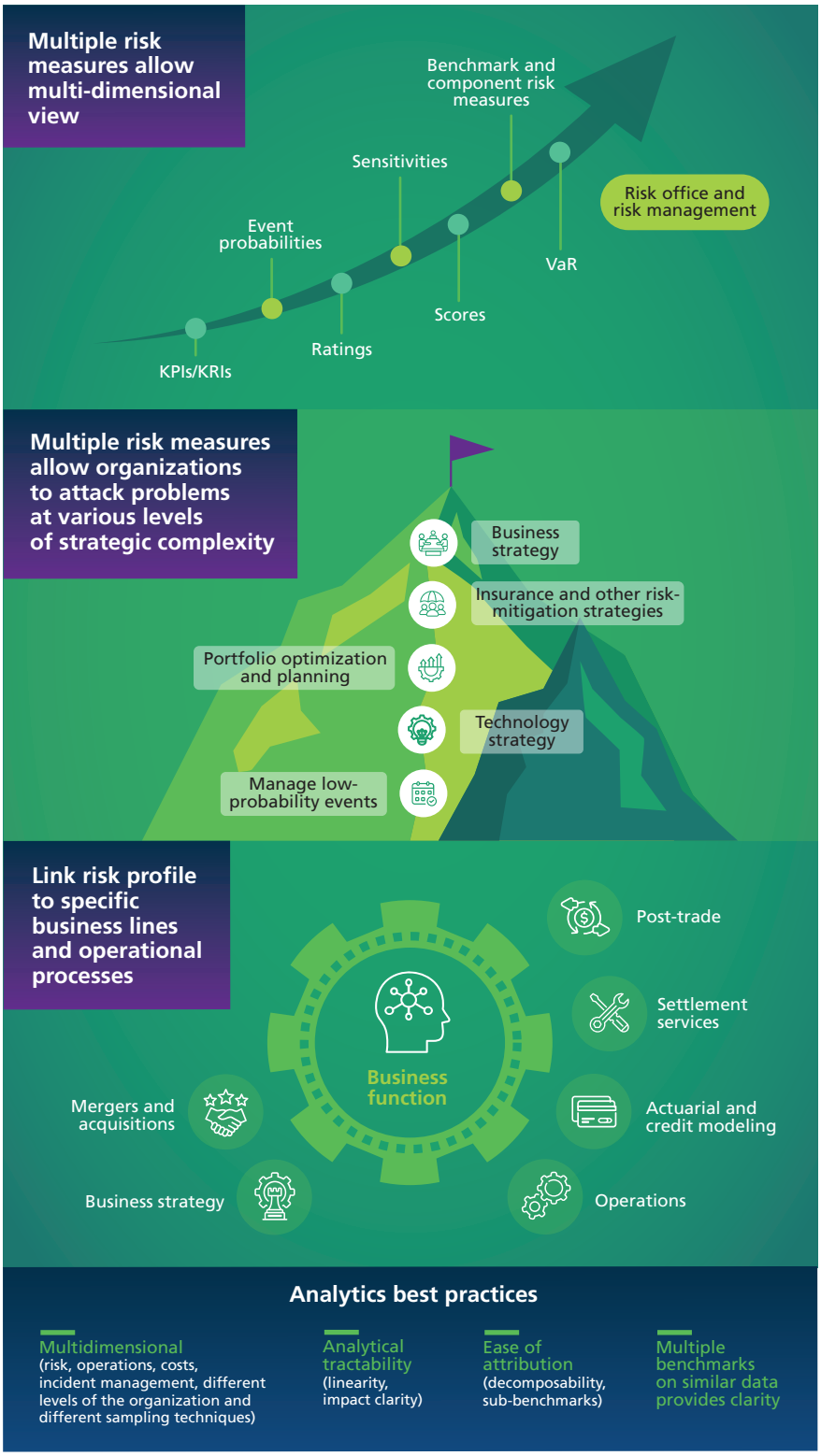
In developing frameworks for digital asset risk management, the dynamic of 'more is more' should be considered, as far as the underlying composability and structure of risk measures are concerned, particularly for these complex assets (see Figure 2). By comparison, commodities generally take networked structure (gas), asset quality (iron ore), operational characteristics (congestion, network conditions, power uptake) into account, and often use many different risk measures to get an accurate idea of the risk of an asset. Equally, cyber risk quantification techniques (and GRC analytics in general) are better seen as a cluster of measures, benchmarks and sub-risk measures. Some cyber risk models break down the core risks into a series of sub-scores that measure elements such as cyber hygiene.

Digital asset risks – a taxonomy

The fundamentals of risk management and measurement are relatively asset-agnostic. The key issue with digital assets is a fundamental shift in the nature of the assets themselves: the inherent composability of these assets and the foundational technological, operational and governance elements that underpin them.

All assets (digital or otherwise) have a core set of risks (market, credit and counterparty), and quantity makes for quality. Some adjustments to standard market, counterparty and credit risk models will have to be made as a result of the price distribution of digital assets, including their higher volatility, skewed distributions and the relative newness of many of the organizations that will be counterparties. But financial institutions have seen these elements before, particularly in emerging markets, in currency markets during times of crisis, and in various commodity markets – including, recently, the European power markets.

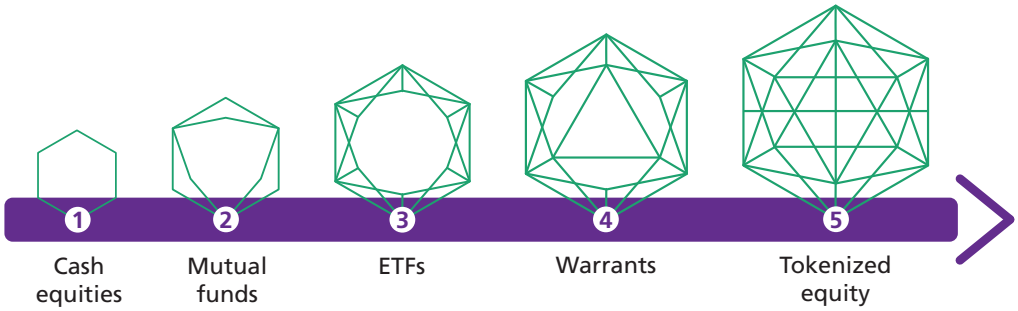
Figure 2: 'More is more': lessons learned from the history of financial markets (and especially illiquid assets) and non-financial risk quantification



Source: Chartis Research

Even standard equity products contain elements of composability. It is possible to hold equities directly – in a mutual fund, an equity basket, separately managed accounts (SMAs)/individually managed accounts (IMAs)/wrap accounts, exchange-traded funds (ETFs), ETF derivatives or ultimately tokenized equity (or a tokenized equity wrapper, for that matter). Each equity product has undergone some transformation along the legal, commercial and regulatory dimension of risk, and as one moves along the complexity chain, more institutional, operational and regulatory risks become embedded (see Figure 3).

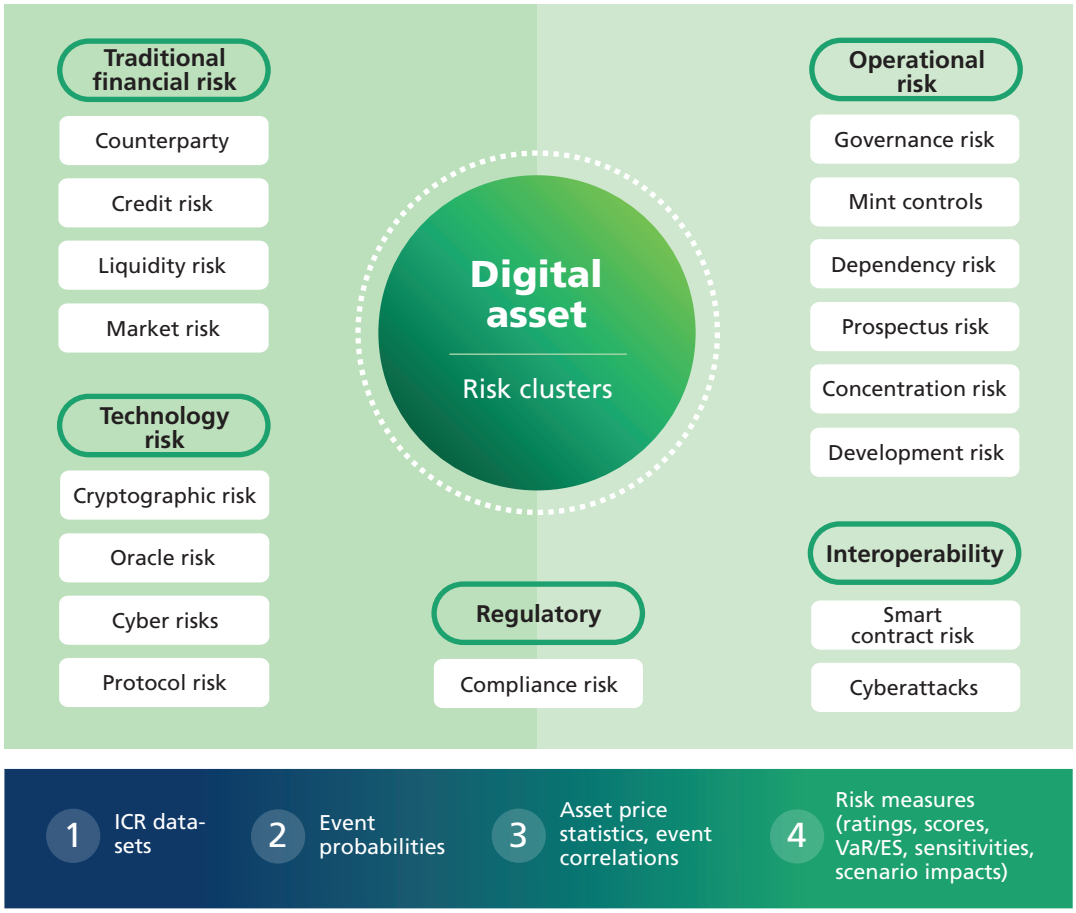
Figure 3: The wrappers – technology, operations, governance – around standard financials vary, and become more complex as they are tokenized



Source: Chartis Research

However, certain new risk elements are intrinsic to digital assets and are due to the nature of the assets themselves. Here we briefly outline some of these risks and consider the various clusters of underlying risks that are not present among traditional assets. We have clustered them into the following risk groups: technological, operational, regulatory and interoperability (see Figure 4).

Figure 4: High-level taxonomy of digital asset risks



Source: Chartis Research

Because of their fundamental reliance on technological wrappers, open decentralized possibilities and novel governance requirements, digital assets present a variety of unique challenges, including operational and technological risks (including interoperability and cross-protocol risks), governance risks and protocol security and reliability risks. These are the foundational asset risks that firms must consider in roughly the same way as they would think about the risks inherent in specific commodities.

Integrated composability risk (ICR)

Adjusting to standard market/credit/counterparty risk measures with more volatility-friendly model variables (either in terms of the credit quality of a counterparty or the volatility of the underlying prices) can help firms define traditional risks for digital assets. But they leave out key foundational risks. We define this set of risks (which are associated with the composition, definition and operationalization of the asset itself) as:

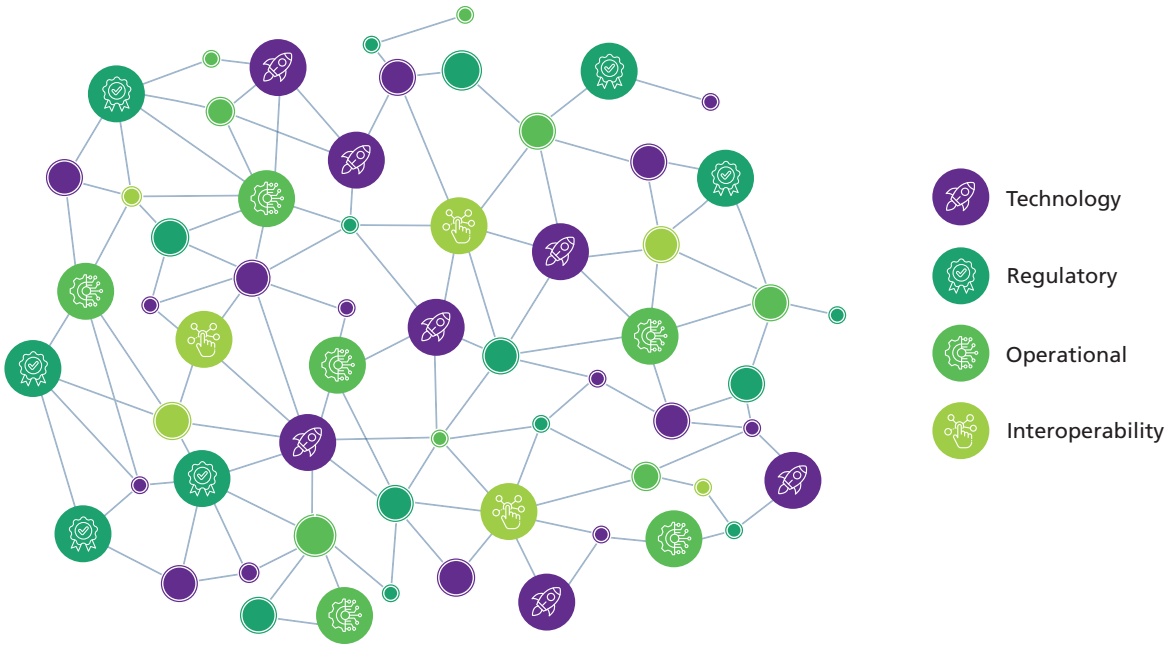
- Technology risks (developmental risks, protocol risks, cryptographic risks, cyber risk).
- Operational risks (governance, legal and compliance, dependency, prospectus).
- Regulatory risks (compliance with evolving legislation, such as the GENIUS Act and Market Clarity Act, jurisdictional requirements like the NYDFS blockchain analytics guidance, OCC digital asset governance expectations, licensing and registration requirements, and cross-border regulatory coordination).
- Interoperability or composability risks (interprotocol transfer risk, interprotocol coordination risk).

Chartis defines 'integrated composability risk (ICR)' as:

Technological risks + operational risks + regulatory risks

As for all non-financial risk measures, the structural challenge is measuring and defining these individual risks using reliable, high-quality data in a real-time environment, with a degree of scheduled or continuous monitoring that digital systems demand (see Figure 5). This can be thought of as analogous to how we think about the risks in other physical goods, such as commodities or physical real estate. When we think about commodity trading, of course, we think about the price. We can look at price

Figure 5: Understanding the risks – analyzing the interconnected technological, operational and governance elements

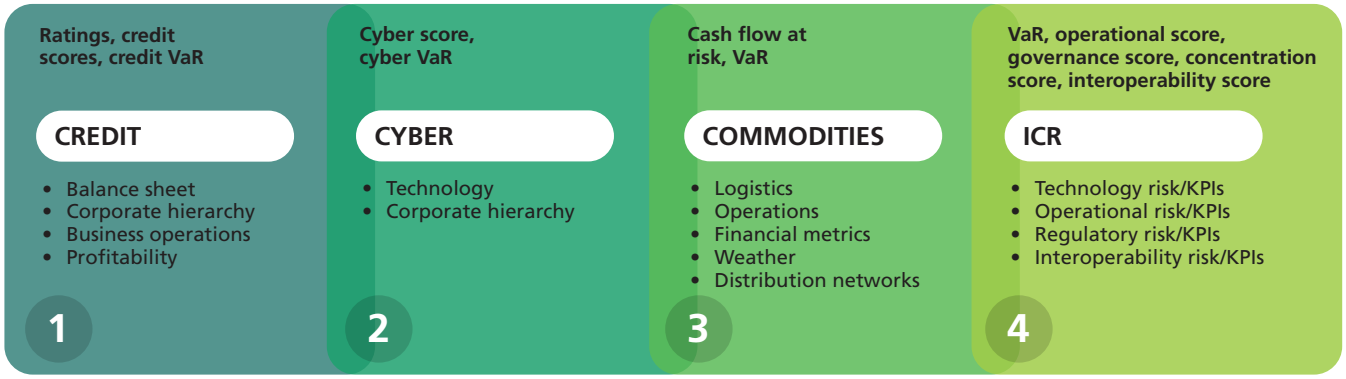


Source: Chartis Research

formation and develop the market risk of commodity assets – but commodities have other properties too. Similar issues occur in the trading of power. Power plants must generate power, which means that operational risk, along with the physical challenges of operating the power plant in specific network systems, must be factored in when constructing and valuing the underlying asset.

In energy markets, each risk is 'composed' of and constructed from more specific individual operational and market risks. These must be quantified and incorporated to bring together the overall risk of an energy asset, whether we are thinking about power plants (on-ramp/off-ramp dynamics, the physical risk of the operating power plant and power equipment) or fuel risks, scheduling dynamics, transportation risks, distribution networks, network congestion risk, etc. Of course, we can look at the pure price history in formulating our view, but without a clear analysis of the many operational components we will be unable to accurately forecast, understand or manage the risks in a power plant or portfolio of generating assets. The concept of 'virtual power plant' brings these 'composability' attributes to the fore, suggesting strongly that market participants also view the risks from this composable perspective (see Figure 6).

Figure 6: Composability and asset complexity have been issues for other assets, particularly energy and commodities



Source: Chartis Research

These risks are recognized by the operational and technological, governance, security and reliability components of ICR defined in this paper. In addition, the scale and multiple blockchain designs supporting the digital asset and distributed finance industry, noted above as interoperability and cross-protocol risks, pose unique challenges to this emerging asset class.

In addition, the use of multiple blockchain designs results in trade-offs. For example, the performance of the network may be lower if security is higher, and new consensus mechanisms, programming languages, system designs, encryption options, privacy protection mechanisms, etc. are all in a rapidly evolving state.

The state of ICR modeling is relatively nascent but evolving rapidly. The underlying data is increasingly available and, more importantly, is available in well-defined taxonomized and structured frameworks. Agency ratings for these assets are increasingly available; however, the secondary set of more statistical risk measures is evolving.

Considering the unique risks inherent in blockchain networks

Digital assets, including tokenized and crypto-native assets, operate on blockchain networks, typically classified as either distributed or decentralized by their architectures and governance models. These network architectures and protocols, designed to manage and transfer the value of digital assets, introduce new inherent risks that are not easily captured in existing risk indicators and measurements. For example, not only is the use of the underlying cryptographic technology in blockchain fairly novel when deployed in this form, blockchain networks also introduce new end points, potential cyber vulnerabilities and new identity variables, all enabled by somewhat unique governance mechanisms.

In a decentralized blockchain network, for example, there is no central authority and operating nodes are equal, with authority and control, including consensus and transaction validation, collectively handled by the operating rules of the participants. Bitcoin and Ethereum are examples of decentralized blockchain networks. Distributed blockchain networks, such as those used within an enterprise, spread data and computational tasks across many nodes and can operate with a central authority that coordinates tasks. Distribution is a technique to increase the redundancy, reliability and scalability of these blockchain architectures.

Moreover, the use of multiple blockchain architectures also requires an understanding of potential trade-offs. For example, the performance of one architecture may be lower if security is higher. Lastly, it is critical to understand that elements such as consensus mechanisms, cryptographic and key management options and privacy protection mechanisms are still evolving, along with technical standards for audit support, risk assessment and multi-network interoperability.

Call to action

To understand what constitutes effective risk analysis in the context of digital assets, firms should place the different elements of digital asset risk (those that are relatively traditional, such as market, credit and counterparty risks), as well as those that are relatively non-traditional (such as technological, operational and compatibility risks) in the context of risk measures that have diffused widely across the financial industry. We also believe that by examining risk measures in analogous contexts, CROs can structure their risk-focused analysis and concentrate on developing expertise, systems and industry standards in this area.

We believe that, if ICRs are not taken into account, financial institutions will miss critical operational, technological and regulatory risks when looking at digital asset risk. As financial institutions have more exposure to digital assets as portfolio managers, depository operators, clearing houses, brokers or counterparties, they need to understand where the actual risks are and leverage aggregated operational, technological and regulatory risk data to create and synthesize the appropriate risk measures.

We argue that CROs have seen this before – and although digital assets look somewhat unfamiliar there are many current analogues (in energy, bulk commodities, real estate and even, to an extent, in credit ratings and scores). Equally, the increasing diffusion of non-financial or technological risk measures (such as cyber risk analytics) is a good example of how the CRO's world has expanded.

We have also made the case that, for standard financial assets, legal, operating and regulatory wrappers are critical in, say, the transformation of equities (held in, for example, individual accounts) into equities held in ETFs. Unpacking the operational and legal risks becomes central as the wrappers become more complex and multi-layered. Were equities to be held as tokenized assets, the need to look into the detailed risks of technological wrappers would be critical (in addition to considering the operational, governance, legal and regulatory risks).

In summary, as the digital asset ecosystem and traditional finance converge, we believe that CROs must:

- Frame the variety and diversity of digital asset risks within the context and history of the evolution of 'traditional' asset risk management.
- Consider the challenges, successes and issues generated in quantifying technology and operationally intensive risk measures (such as cyber risk).
- Work collectively with industry partners to establish the proper frameworks, expertise, standards and technologies needed to incorporate digital asset and protocol risks into existing enterprise risk management programs.