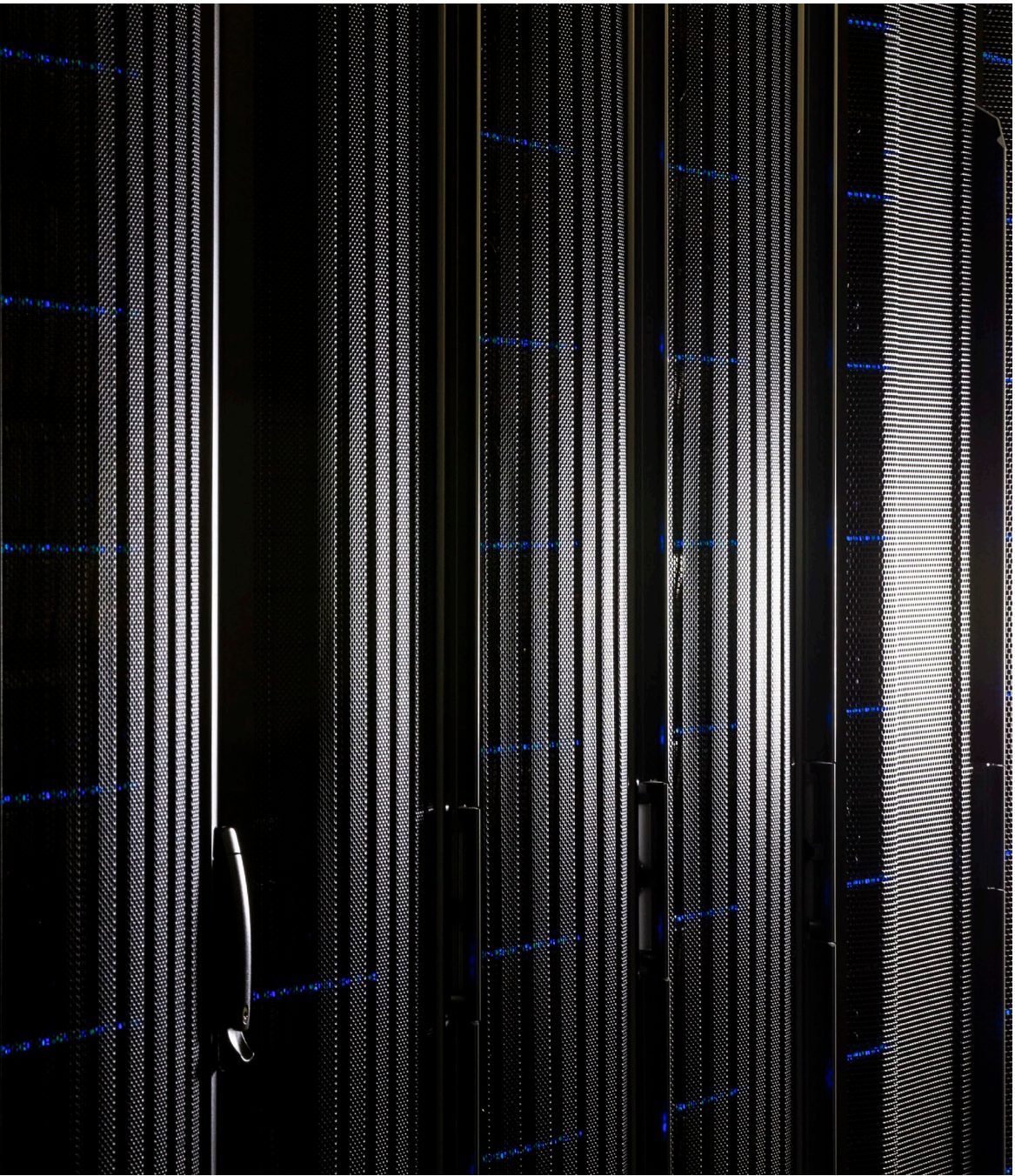
S&P Global
Ratings

How DeFi's Operational Risks Could Influence Credit Quality

June 7, 2023

This report does not constitute a rating action



Contacts

Miguel de la Mata
Englewood
+1-303-721-4478
miguel.de.la.mata@spglobal.com

Lapo Guadagnuolo
London
+44-207-176 -507
lapo.guadagnuolo@spglobal.com

Lisa Schroeer
Charlottesville
+1-434-529-2862
lisa.schroeer@spglobal.com

Key Takeaways

- Decentralized finance (DeFi) systems introduce new operational risks that can affect the credit quality of issuers exposed to the sector and of digital financial instruments.
- These risks span the life of a DeFi-based operation, beginning with onboarding risk, then bridge and transfer risk, storage risk, chain-specific risk, and concluding with exit strategy risk.
- The threats primarily relate to fund-flow mechanics, security, and custody. They weigh on credit quality through their potential to interrupt, diminish, or result in the loss of cash flows to investors.

The recent emergence of DeFi means it remains one of the least understood sectors of the financial industry. That will have to change.

DeFi systems, which use blockchain technology to remove financial intermediaries, promise to revolutionize financial platforms and instruments by offering new levels of transparency, lower costs, and technological robustness. But the new technologies and systems also comes with novel operational risks that demand attention from nonfinancial companies, traditional finance (TradFi) players, and credit markets. Understanding this emerging technology's risks and their potential effects on credit quality has thus been a necessity for S&P Global Ratings.

For the time being that work remains largely preparatory. DeFi-based issuers of debt are rare, typically little connected to the "real" economy (including TradFi), and are yet to demand a rating from us. DeFi-related products, meanwhile, have required our credit analysis only in specific and limited instances, including the issuance of digital bonds by traditional issuers (see "Digital Bonds: The Disruption Is Underway," Feb. 27, 2023) and in some structured finance transactions (see "DeFi Protocols For Securitization: A Credit Risk Perspective," Feb. 7, 2023).

The most important aspects of DeFi risk relate to fund flow mechanics, security, and custody

Breaking Down DeFi Risk

The most important aspects of DeFi risk relate to fund flow mechanics, security, and custody considerations that could interrupt, diminish, or result in lost returns for investors. That remains the case regardless of whether we are considering their possible effects on an instrument or an issuer.

We use a relatively loose definition of DeFi, encompassing operations that leverage blockchain technologies. We also acknowledge that many such operation still rely to some degree on TradFi institutions, such as banks and custodians, or centralized institutions (CeFi), such as centralized exchanges and crypto lending/borrowing platforms. These institutions can play a key role in mitigating operational risks, and the importance of novel operational risks to various DeFi operations is influenced by the degree to which key functions are truly decentralized.

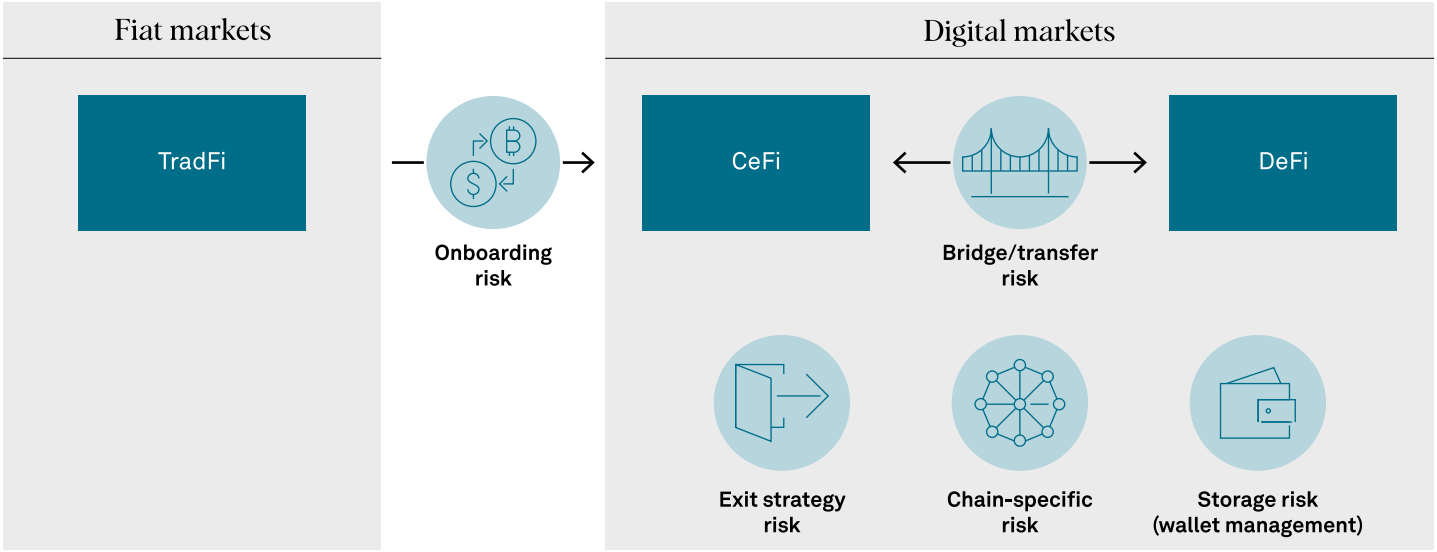
We categorize operational risks related to DeFi into five areas:

- Onboarding risk.
- Bridge and transfer risk.
- Storage risk (or wallet management).
- Chain-specific risk.
- Exit strategy risk.

While we consider these categories individually, we also recognize that each category is broad, constantly changing, and often strongly connected to other DeFi risk categories [see chart 1].

Chart 1

DeFi's key operational risks



TradFi--Traditional Finance. CeFi--Centralized Finance. DeFi--Decentralized Finance. Source: S&P Global Ratings.

Onboarding Risks

In DeFi, onboarding risk occurs when a user converts fiat currency into a digital asset, typically during the process of joining a network. Examples include the purchase of an NFT with fiat currency and the conversion of fiat currency into crypto currency--for the purpose of investing in a bond or interacting with a lending platform that is denominated in a crypto currency.

Onboarding risks in TradFi are also linked to joining a network. For example, when a client opens a bank account, they accept the risk inherent to their bank's network and to the central bank network it is connected to. The bank network is effectively a record of the transaction history of all its participants, is managed by the responsible bank, and stored on a digital database that is typically located on private servers or contracted to cloud services (or a combination of both). The operational risk is therefore linked to the efficient and safe management of the database.

Blockchain technologies, which underpin DeFi operations, provide the same tracking function as a bank's database. Yet, unlike the bank, which tracks only transactions linked to its network, the blockchain stores the entire transaction history of an instrument (such as a digital token). Furthermore, it does this using a decentralized system of nodes, which means there is no single entity responsible for the data and thus little role for the institutions that dominate TradFi.

The four onboarding avenues

There are four main ways in which fiat money is converted into digital assets. These onboarding avenues are:

- Centralized exchanges.
- In-wallet purchases.
- B2B private exchanges.

- Private anonymized exchanges.

Each of those avenues comes with varying levels of risk, including in relation to liquidity, consumer protection, and compliance with know-your-customer (KYC) requirements and anti-money-laundering regulations(AML). And each avenue comes with varying costs to users (see chart 2).

Table 1

Onboarding avenues' characteristics

	Know your customer/ anti money laundering	Consumer protections	Liquidity	Transaction costs
Centralized exchanges	★★★	★★☆	★★★	$$☆
In-wallet purchases	★★★	★★☆	★★☆	$$$
B2B private exchanges	★☆☆	★☆☆	★☆☆	$☆☆
P2P private exchanges	☆☆☆	☆☆☆	☆☆☆	☆☆☆

B2B--Business-to-business. P2P--Peer-to-peer. Source: S&P Global Ratings.

The different avenues, generally, exhibit the following characteristics:

- **Centralized exchanges** provide high levels of liquidity and (depending on where exchanges are registered) can offer strong consumer protection and compliance with KYC/AML regulations. However, users' transaction costs (e.g., commission and intermediary fees) tend to be high as the user pays for the services provided by the centralized exchange.
- **In-wallet purchases** are utilized by some decentralized applications (Dapps) and enable fiat to be transferred directly to a privately-custodied wallet. This reduces risk incurred when transferring funds from a centralized-exchange wallet to a private wallet. Dapps use third-party liquidity providers that perform onboarding from fiat and send digital assets to private wallets. In-wallet purchases generally have weaker liquidity than a centralized exchange and less transparent pricing. Transaction costs associated with in-wallet purchases can be high compared to other avenues.
- **B2B private exchanges** can be operated by institutions in the same way as other institutional private asset exchanges. Consumer protections and applicable KYC/AML regulations depend on the jurisdiction of both parties to the trade. Liquidity is assumed to be considerably lower than for centralized exchanges and in-wallet purchases.
- **Private, anonymized exchanges** (or P2P private exchanges) typically provide the least liquidity, consumer protections, and KYC/AML regulation compliance, but are also typically the lowest cost avenue for users. These exchanges may offer users the ability to make bids or offers in fiat currency for specified amounts of digital assets.

How onboarding defines risk

Understanding how KYC/AML compliance, liquidity, consumer protection, and costs differ across onboarding avenues is critical to the assessment of DeFi-related risks.

That is the case for users seeking to judge how the avenues introduce risk to investments, and for the assessment of credit worthiness--given the potential for the onboarding method to

impact payment flows. For example, if a bond (or other structure) promises to make a full and timely payment in fiat currency with proceeds from digital assets, then liquidity and transparency in price discovery could determine if, or when, a conversion from digital assets into fiat can be made. Similarly, fees associated with a more-expensive onboarding avenue could reduce the net value of digital assets that back a fiat-denominated obligation.

We are agnostic about how onboarding occurs. But we recognize that each avenue comes with unique risks (and benefits) that need to be evaluated in the context of different situations.

Bridge And Transfer Risk

Bridge risk, in the context of DeFi, is incurred when moving digital assets from one network to another, while transfer risk is incurred when moving digital assets from one wallet to another--including from a third-party wallet (such as a centralized exchange) to a private wallet, or between private wallets.

The TradFi equivalent of this risk is payment-settlement-system transfer risk, which occurs each time funds change hands, and is thus common. For example, funds used to purchase a bond will typically pass through numerous accounts, and often multiple parties, before being returned to an investor when the bond matures or is sold.

Across both TradFi and DeFi it is reasonable to expect that money will flow without disruption or delay, though DeFi systems introduce some unique risks to that expectation. For example, TradFi's legal frameworks and tested procedures limit the risks that funds will become unrecoverable due to mistakes or fraud, not least because specific parties are usually responsible for recovery of lost funds. Those safeguards can be unfeasible, or at least much more difficult to offer, in a DeFi system because they lack central entities that assume responsibility. For the same reason, DeFi systems tend to provide no practical customer support and there is only a limited track record of successful legal recourse.

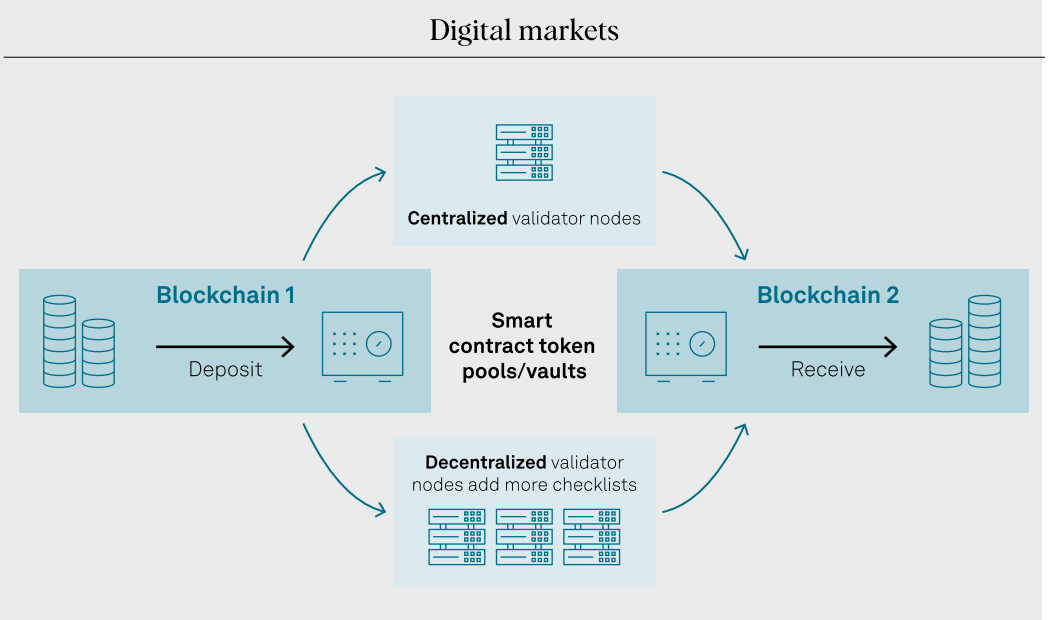
Some mitigation of DeFi transfer risk can be offered by automated systems designed to catch human errors (such as a wrong recipient address), but errors can be expected to be more damaging than in TradFi. For those reasons, we consider that all DeFi-based transactions should be assumed to be final and immutable. Understanding how (and if) a platform mitigates the resulting risk of loss is therefore critical.

Decentralized versus centralized bridges

Bridge systems fall into two categories, centralized and decentralized, with each system offering different strengths and weaknesses that can influence credit risk.

Chart 2

Centralized and decentralized bridge systems



Source: S&P Global Ratings.

Decentralized bridges typically work by locking digital tokens onto an initial blockchain (within smart contracts), then use a decentralized protocol to verify a transaction, and finally mint the equivalent token, known as a wrapped token, on a second blockchain.

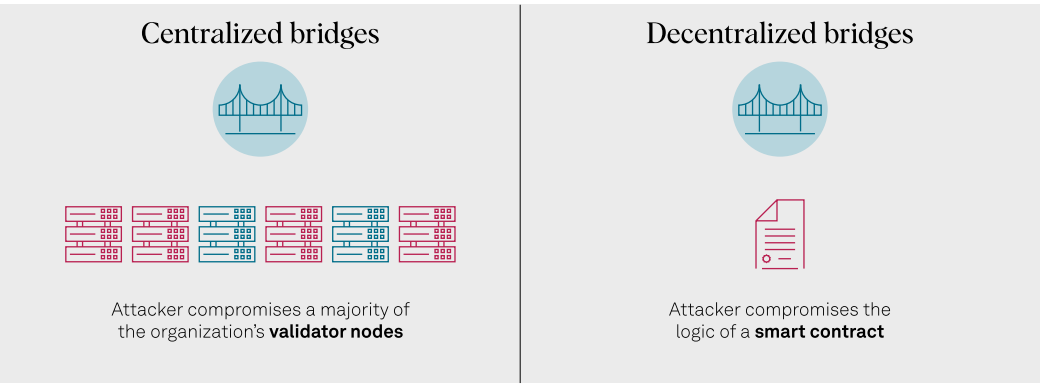
A reliance on decentralized validator nodes to verify a transaction is a strength of the system as it results in a high number of independent checks. Decentralized bridges are however highly reliant on smart-contract logic, which can be a point of weakness, and are exposed to the vagaries of decentralized governance. DeFi users of decentralized bridges need to be particularly aware of the possibility and consequences of bugs or mistakes in code and be aware of back-up procedures that are available (or not).

Centralized bridges operate in the same way as decentralized bridges, but a single entity performs the transaction verification process. That typically means there is clearer accountability, compared to decentralized bridges, though that still depends on the jurisdiction in which the central entity is registered. On the downside, that concentration also increases risk linked to the failure of the centralized validator node, introduces custodial risk, and heightens counterparty risk.

Adding to the risks inherent to DeFi's bridges is the threat of exploitation by malevolent actors. Bridges have been targeted by hackers who have used security failures in organizational structures and smart contracts to hack DeFi systems. More specifically, centralized bridges have been targeted with private key thefts that have afforded hackers control of a majority of validator nodes and thus control of a centralized bridge. Decentralized bridges, meanwhile, have suffered code hacks that compromised smart contracts, allowing bad actors to secure additional debt and post faulty collateral.

Chart 3

The exploitation of bridges



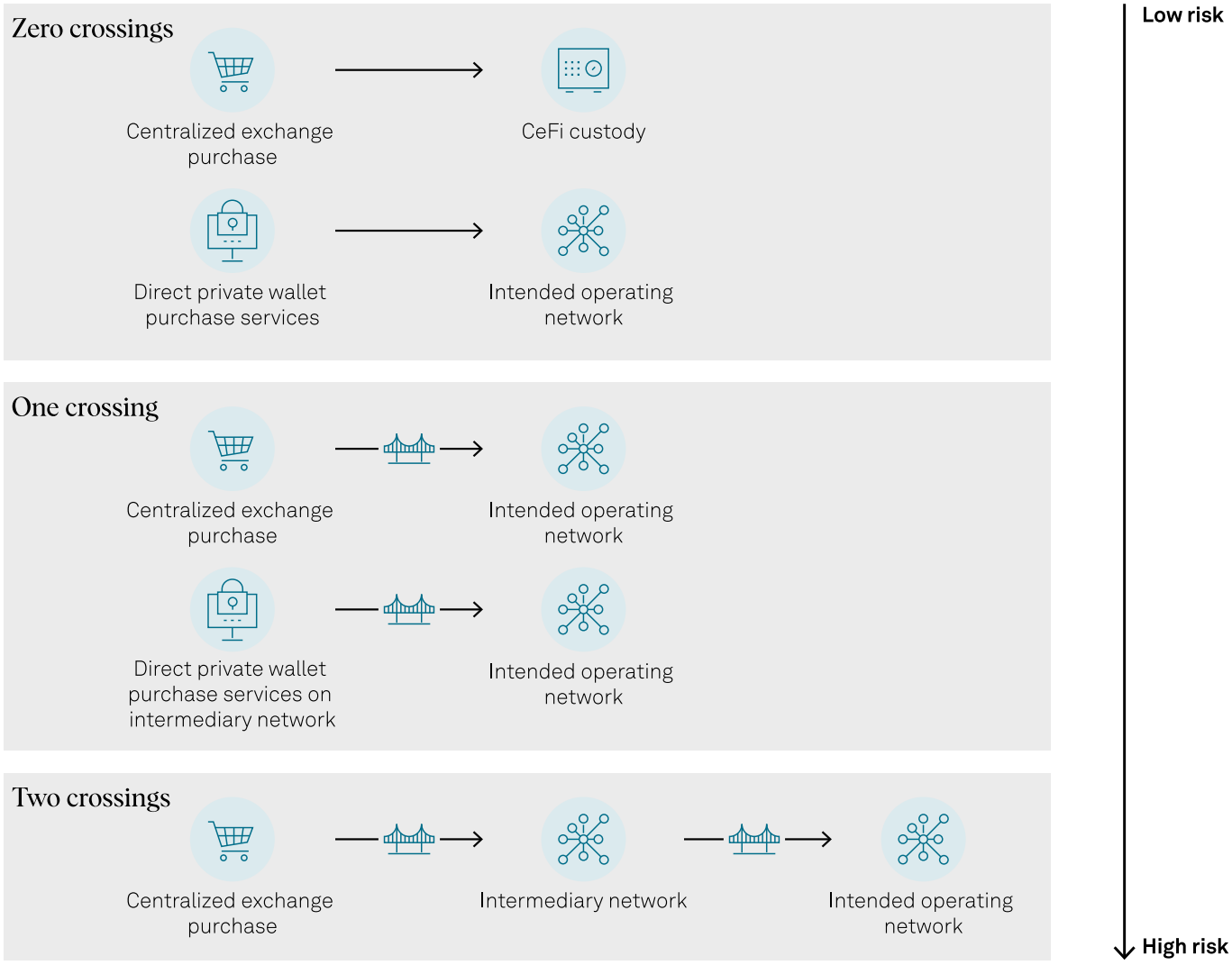
Source: S&P Global Ratings.

More transfers equal more risk

DeFi systems typically require funds to traverse more bridges to reach their destination, at least compared to CeFi and TradFi systems. Each of these crossings represents an opportunity for loss, so a system with fewer bridges or transfers will, all else being equal, be less risky (see chart 5).

Chart 4

Bridge risk increases with each crossing



Source: S&P Global Ratings.

Storage Risk

Storage risk refers to the possibility of loss resulting from asset custody. In DeFi, this typically relates to private custody of digital assets--where an individual or entity assumes responsibility for storing and protecting digital assets. This private custody mitigates counterparty risk from exposure to a centralized exchange, but it also introduces new burdens, including issues surrounding confirmation of ownership and information protection. For example, the loss of a password component in a DeFi system typically renders funds unretrievable.

Storage risks are markedly different in TradFi, where funds are typically held in accounts managed by a single organization, and benefit from insurance and central depository guarantees that mitigate counter-party risk. While funds are typically protected by passwords, encrypted pins, or a human gatekeeper, users that lose access can typically regain it using other types of identity confirmation.

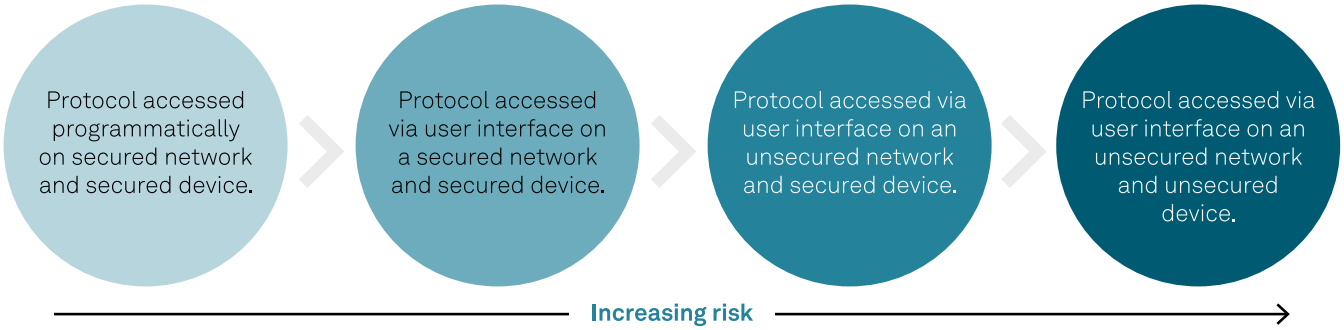
Storage risk can affect a rated obligation's credit quality. For example, if investors (or other parties related to an instrument) are not covered by agreements with reputable custodians, or if they are interacting with the issuing entity via blockchains rather than traditional channels. In both instances the risk of disruption to payments can increase, and remedies should be understood in advance.

The differences between TradFi and DeFi mean that users of the latter need to be more technically savvy, aware of best practices (notably risk prevention measures), and understand the inherent risks. Specifically, DeFi exposes users to three novel storage-related risks:

- **Interaction risks** refers to the danger that DeFi users disclose their private keys to malicious actors or sign an unintended transaction that results in a loss. Interaction risk can be mitigated by using wallets that require multiple signature keys, known as multisig wallets, or by accessing a smart contract directly rather than through a user interface (UI). The use of secured networks, secured devices, and adherence to security policies on how to store laptops, mobile phones, or any other devices used to access digital markets can also reduce the risk of falling victim to bad actors (see chart 6)

Chart 5

The tradeoff between interaction ease and security

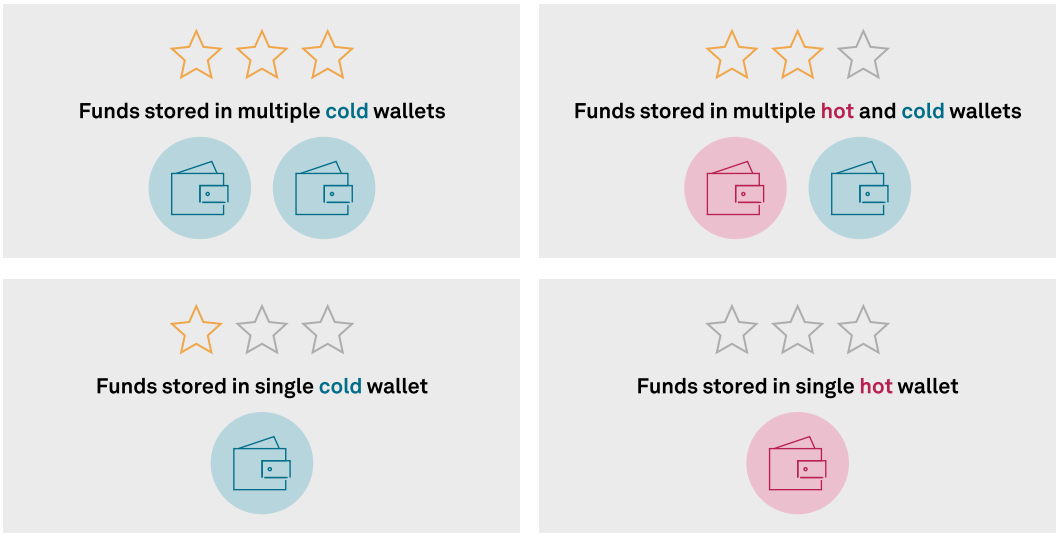


Source: S&P Global Ratings.

- **Wallet security risks** relate to the type of wallet in which digital assets are stored. There are two basic wallet categories: hot wallets, which are connected to a cryptocurrency network and store access codes on a device or a provider's database; and cold wallets, which use keys stored independently of the wallet and which need to be manually entered. Hot wallets offer convenience but are more susceptible to a malicious attack, while cold wallets are more difficult to hack but come with greater risk of losing access due to lost keys. Users should understand the tradeoffs between the different wallets and be aware of how risks can be mitigated and security increased--including by the use of storage structures using multiple wallets and a mix of wallet types (see chart 7).

Chart 6

Storage security and wallet configurations

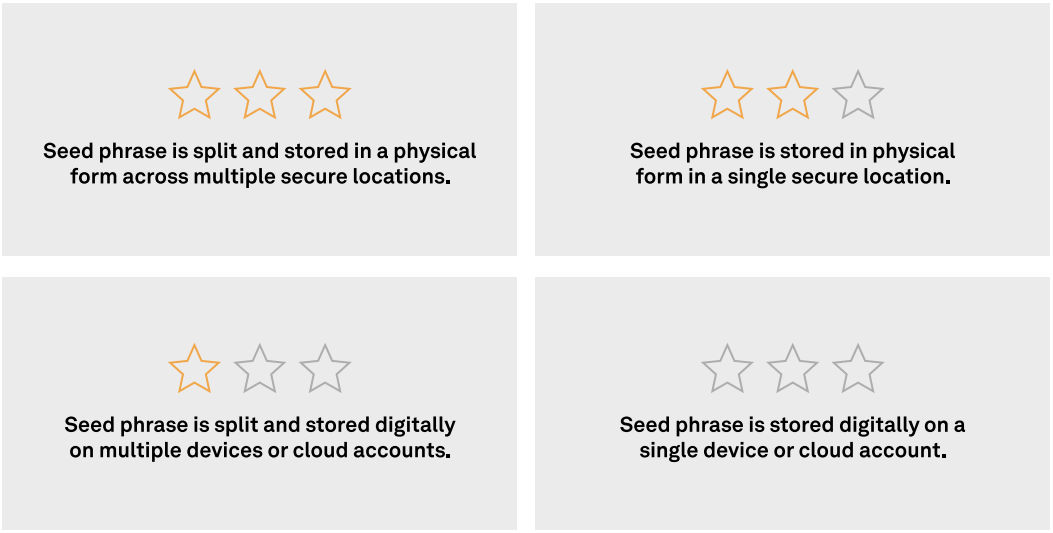


Hot wallets are connected to the internet. Cold wallets are a physical, offline device.
Source: S&P Global Ratings.

- **Private key access management** refers to the method employed for storing a seed phrase, which is a sequence of words required to generate the key needed to access a digital wallet. There are numerous approaches to private key access management. At the most basic level, an individual could store a seed phrase digitally for ease of access, though this exposes them to the greatest security risks. Security can be relatively easily increased by storing a seed phrase on a physical item, ranging from a piece of paper to a more robust material like stamped stainless steel plates, and increased further by partitioning a seed phrase and storing it among multiple secure locations. Organizations can provide a further layer of security by requiring multiple signatures in order to secure access to a seed phrase.

Chart 7

Private key access management systems and security



Seed phrase--Sequence of random words required to generate the key needed to access a digital wallet.
Source: S&P Global Ratings.

Chain Specific Operational Risk

Chain specific operational risks are threats particular to DeFi networks, and thus additional to the risks that are shared with TradFi networks. These chain specific operation risks largely fall into three categories:

- **Network-specific outage risk** refers to the possibility that a blockchain network could fall out of service for a meaningful duration. This could be due to a technical issue or a malicious attack, though decentralized networks' lack of a single attack surface is a security advantage compared to centralized networks. Outage risk increases with complexity, meaning base-layer blockchain networks, known as L1 networks, are less susceptible to outages than L2 networks, which build on L1 networks to add functionality and speed. Users of DeFi need to be aware of their outage risk, which notably include the possibility that a payment could be blocked, resulting in temporary or permanent financial losses. These risks can be mitigated with back-up solutions, or the presence of specific services accountable for restoring functionality.
- **Variable gas costs** are unplanned increases in transaction costs that could affect operational cash flows. These are particularly pertinent to structured or project finance transactions, where fees and expenses can be important cash flow considerations. DeFi network transaction costs can vary significantly depending on timing, special events, and network adoption. DeFi users should be particularly wary of costs that can increase meaningfully and, more importantly, unpredictably.
- **In-network transaction times** are a measure of how long transactions take, on average, to be confirmed. Reducing transaction times is critical to DeFi's widespread adoption and its ability to compete with TradFi networks, such as credit card networks. Performance varies across blockchains, and when blockchains are under stress, i.e., when there is a significant increase in activities such as prepayments, recoveries from defaulted assets, or trading of unpaired assets in structured finance transactions.

Exit Strategy (Or Stablecoin) Risk

Exit strategy risk, also known as stablecoin risk, occurs when moving out of a volatile digital asset into a core position denominated in stablecoins. The risk, which is specific to DeFi, reflects a stablecoin's stability in terms of value and its ability to maintain a peg to a fiat currency, which can affect the ability of a holder to redeem an investment at parity and in a timely manner.

The presence of these variables is a key difference between stablecoins and cash (in the TradFi sense). Yet despite the additional risk, DeFi market participants may prefer to exit a digital asset by purchasing stablecoins because it allows them to remain in the digital arena and thus avoid costs associated with transitioning to fiat currency.

Exit strategies come with different levels of value stability (or lack thereof) depending on the stablecoin adopted. It is thus important that DeFi participants consider and understand the differences between stablecoins structures and their different levels of value stability. For example:

- Typically-higher value stability: A stablecoin that is supposed to be pegged to a fiat currency, but which is actually backed 1:1 by regularly audited and liquid real-world assets that TradFi would recognize as near-cash equivalent.
- Typically-lower value stability: A stablecoin that is supposed to be pegged to a fiat currency but is actually 1:1 backed by undefined real-world securities, with undefined credit quality. Such assets would not be considered as equivalent to near cash in TradFi.

- Typically-even-lower value stability: A stablecoin that is supposed to be pegged to a fiat currency but is overcollateralized with other crypto currencies or digital assets.

Familiar Concepts In A New Arena

There is evidently much that is new about digital markets and DeFi. That novelty can be daunting and may prove a barrier to adoption for some. Furthermore, because the space remains young and growing it will be apt to change, and therefore requires ongoing attention.

Yet the established rules of financial risk management generally hold true. In DeFi, as in TradFi, it remains necessary to frame risks to measure them and understand how they can affect credit quality. Participants need to comprehend market conventions, security issues, and the dangers of disruption to money flows between an issuer and an investor. Those factors remain crucial to risk, regardless of whether a system is traditional, centralized, or decentralized.

Related Research

- Digital Bonds: The Disruption Is Underway, Feb 27, 2023
- DeFi Protocols For Securitization: A Credit Risk Perspective, Feb. 7, 2023

Writer: Paul Whitfield

Digital Design: Tom Lowenstein, Joe Carrick-Varty