TALOS

Exploring the DeFi Frontier: Institutional Challenges and Pathways to Success

By: Andrew Murpy, General Counsel, Talos

Introduction

Decentralized Finance, or DeFi, is pushing the boundaries of the traditional financial system. Through the use of smart contracts, it is now technologically possible to trade, lend, borrow and invest at scale, without any intermediaries. This creates opportunities to reduce transaction costs, remove barriers to entry and evolve the financial system. However, current gaps in regulation, infrastructure and understanding often hold back institutions from exploring this new frontier. We examine four key challenges institutions face when interacting with DeFi, based on discussions with our clients and partners. We also share how some of our clients are overcoming these challenges in order to explore the DeFi frontier.

Contents

01

The AML/KYC Challenge in DeFi: Risk Mitigation Techniques

The AML/KYC Challenge in DeFi: Risk Mitigation Techniques

In part 1, we examine DeFi's AML/KYC problem – why it is difficult for institutions to fully comply with traditional AML/KYC requirements when interacting with DeFi, and how responsible institutions are using innovative solutions to achieve the intended objective of the requirements.

DeFi protocols were not designed to support AML/KYC

Just about every financial institution that transacts in the global financial system is subject to some form of anti-money laundering (AML) compliance and/or sanctions compliance.

In the US, AML requirements apply to intermediaries, specifically "financial institutions" under the Bank Secrecy Act, with the goals of documenting, detecting, deterring and preventing illicit activity and threats to national security[1]. In addition, sanctions screening requirements apply to all participants in the US financial system. The goal of the US sanctions program is to prevent US persons from transacting with bad actors and nation states designated by the US government.

The general theory behind both AML and sanctions compliance is that by verifying the identity of parties to a financial transaction – often referred to as KYC (know your customer) or KYB (know your business) – institutions can help keep known bad actors from using the financial system. Illicit activities, such as terrorist financing and money laundering, should be more difficult for these bad actors as a result, as they can't easily access the financial system.

However, decentralized protocols are often created with efficiency and permissionless accessibility top of mind rather than AML/KYC. The decentralized and pseudonymous design of DeFi platforms complicates AML/KYC compliance in various ways. First, the decentralized and disintermediated nature of DeFi transactions means there is no obvious intermediary to perform KYC verifications. In addition, the pseudonymous nature of bilateral blockchain transactions makes it nearly impossible to perform traditional AML or sanctions screening verification on the owner of an unhosted wallet.

This creates a significant challenge: How can institutions avoid unintentionally transacting with bad actors in an ecosystem designed to promote financial privacy and efficiency?

Solutions for AML/KYC compliance in DeFi

Innovative, technology-driven solutions are emerging to help institutions achieve the goals of traditional AML/KYC requirements within DeFi's decentralized architecture. We outline some approaches institutions are currently using to navigate the AML/KYC problem inherent to DeFi.

1. WALLET RISK SCORING

The most commonly used solution among the institutions we work with is "wallet risk scoring". Blockchain analytics companies have developed wallet risk scoring through software risk engines that assign each individual digital asset wallet a risk score based on a variety of factors, such as direct and indirect transactional proximity to illicit transactions or sanctioned wallet addresses, and prior engagement in or proximity to suspicious financial activity on blockchain networks[2].

Risk scoring can be performed pre-trade, post-trade or both. Pre-trade wallet risk scoring allows institutions to filter out wallets based on risk scores before the transaction is executed. The application of risk scores can be expanded to filter out entire liquidity pools, if certain wallets in the pool engage in irregular patterns that signal risk, or if a single wallet in the pool has interacted with a blacklisted address. In both cases, the goal is to prevent risky transactions before they occur. However, if there is insufficient historical data associated with a particular wallet or pool of wallets, pre-trade risk scoring may be less effective.

By contrast, post-trade wallet analysis occurs after the transaction is executed. Here, the goal is to monitor suspicious activity related to a wallet, which institutions may need to report to regulators. Many institutions perform post-trade wallet monitoring in addition to pre-trade risk scoring and may use different vendors to assist with each activity.

While wallet risk scoring doesn't fully solve the AML problem, it does reduce the risk of interacting with bad actors, and therefore promotes sanctions compliance. While there is currently little official guidance from the US government on the usage of wallet screening tools for sanctions compliance, general comments from the US government indicate that sanctions compliance programs require a risk-based approach (notwithstanding the strict liability standard for US persons engaged in sanctions violations[3]). Thus, some institutions are making wallet risk scoring tools a key part of their compliance program for transacting in DeFi.

2. "PERMISSIONED" PROTOCOLS

Another solution gaining traction is "permissioned" protocols that restrict access to whitelisted participants consisting only of KYC'd counterparties. A key advantage of permissioned protocols is that they are built to comply with existing regulations applicable to centralized markets.

In centralized markets, intermediaries such as financial institutions, are responsible for safeguarding the financial system and must take on gatekeeping functions such as performing KYC verification on

customers and reporting suspicious transactions to regulators. Permissioned protocols function similarly by performing KYC verification before distributing tokens to a wallet. In addition, permissioned protocols can grant regulators specific permissions to access transaction data for purposes of investigating suspicious transactions.

3. OTHER SOLUTIONS

In addition, other, more ambitious solutions to DeFi's AML/KYC problem are currently under development. These solutions include zero knowledge proofs, a cryptographic innovation that enables auditable security without undermining secret-keeping[4]. Talos will keep its clients informed about their adoption by institutions as these solutions develop.

Conclusion

While no single solution fully solves DeFi's AML/KYC problem, these innovative approaches are mitigating some of the risks and enabling institutions to explore the potential of DeFi more responsibly. As the landscape continues to evolve, so do the strategies institutions employ to address DeFi's unique compliance challenges.

In the next chapter, we discuss the cybersecurity challenges in DeFi.

02

Cybersecurity Challenges in DeFi: Addressing the Risks

Cybersecurity Challenges in DeFi: Addressing the Risks

DeFi has the potential to unlock new frontiers of innovation in finance. However, institutions are subject to strict regulatory requirements, including some of the most stringent cybersecurity standards in any industry. Meeting these obligations while interacting with DeFi's dynamic and sometimes volatile ecosystem is no small task.

DeFi introduces unique cybersecurity risks

The rise of DeFi has coincided with significant cybersecurity incidents. In 2023, hackers stole nearly $1.1 billion from DeFi protocols. While this figure may seem high, it's worth noting that it marked a significant improvement from previous years. The total value stolen from DeFi platforms dropped by 63.7% from 2022 to 2023, indicating improvement in DeFi security[5]. Nevertheless, the stakes remain high, and institutions must be cautious.

Hackers continually evolve their tactics, seeking out vulnerabilities in smart contracts and exploiting weaknesses in decentralized exchanges, lending platforms, and automated market makers. For financial institutions accustomed to centralized security protocols and regulatory oversight, the decentralized nature of DeFi presents unique risks. The challenge is significant: how can institutions engage with DeFi without exposing themselves to unacceptably high levels of cybersecurity risks?

Solutions for mitigating DeFi's cybersecurity risks

Despite the cybersecurity risks, many institutions are beginning to find pathways into the DeFi space by being more selective about protocols and leveraging specialized cybersecurity solutions. Here's how some are doing it:

1. INTERACTING WITH SELECT DEFI PROTOCOLS

A key strategy for managing cybersecurity risk in DeFi is selectivity. Rather than engaging with any available protocol, many institutions are choosing to work exclusively with established, "blue chip" DeFi protocols. These protocols have demonstrated their resilience over time, have invested significant time and resources into cybersecurity, and tend to have a couple of key indicators of quality.

One of the most important indicators of a blue chip DeFi protocol is whether it has undergone a thorough

smart contract audit. These audits help identify and address vulnerabilities in the code, ensuring that the protocol is less susceptible to exploits. Institutions typically favor protocols that perform ongoing audits, often referred to as "trail audits", which provide a continuous assessment of the protocol's security posture.

Another important indicator is the user experience. Blue chip protocols are more likely to have cybersecurity top of mind and create a user experience designed to mitigate errors and risks. For example, some blue chip protocols have created more secure contracts that allow users to selectively permission tokens for transactions for a limited time. This helps reduce risk of exploitation that comes from "infinite approvals" – users giving applications access to a wallet's entire token balance for an indefinite period of time.

By only interacting with DeFi protocols that have invested in smart contract audits and a safe UX, and demonstrated resilience over time, institutions can reduce the risk of cybersecurity incidents.

2. USING MULTIPLE WALLETS

Another strategy for managing cybersecurity risk is to use multiple wallets to segregate digital assets. The creation of new wallets is typically free, so segregating digital assets into multiple wallets can be an efficient way to reduce cybersecurity risk without adding additional costs.

Segregating assets into multiple wallets (e.g., by client, account, or counterparty) can reduce cybersecurity risk by minimizing the potential impact of a compromised wallet. In addition, rotating wallets periodically can help to reduce the risk exposure generated by a frequently used wallet. This is particularly important if the protocol has the ability to pull money from a wallet. If the protocol is hacked and still maintains prior approvals, it can result in unauthorized transactions and losses for the impacted user.

3. WORKING WITH SPECIALIST VENDORS

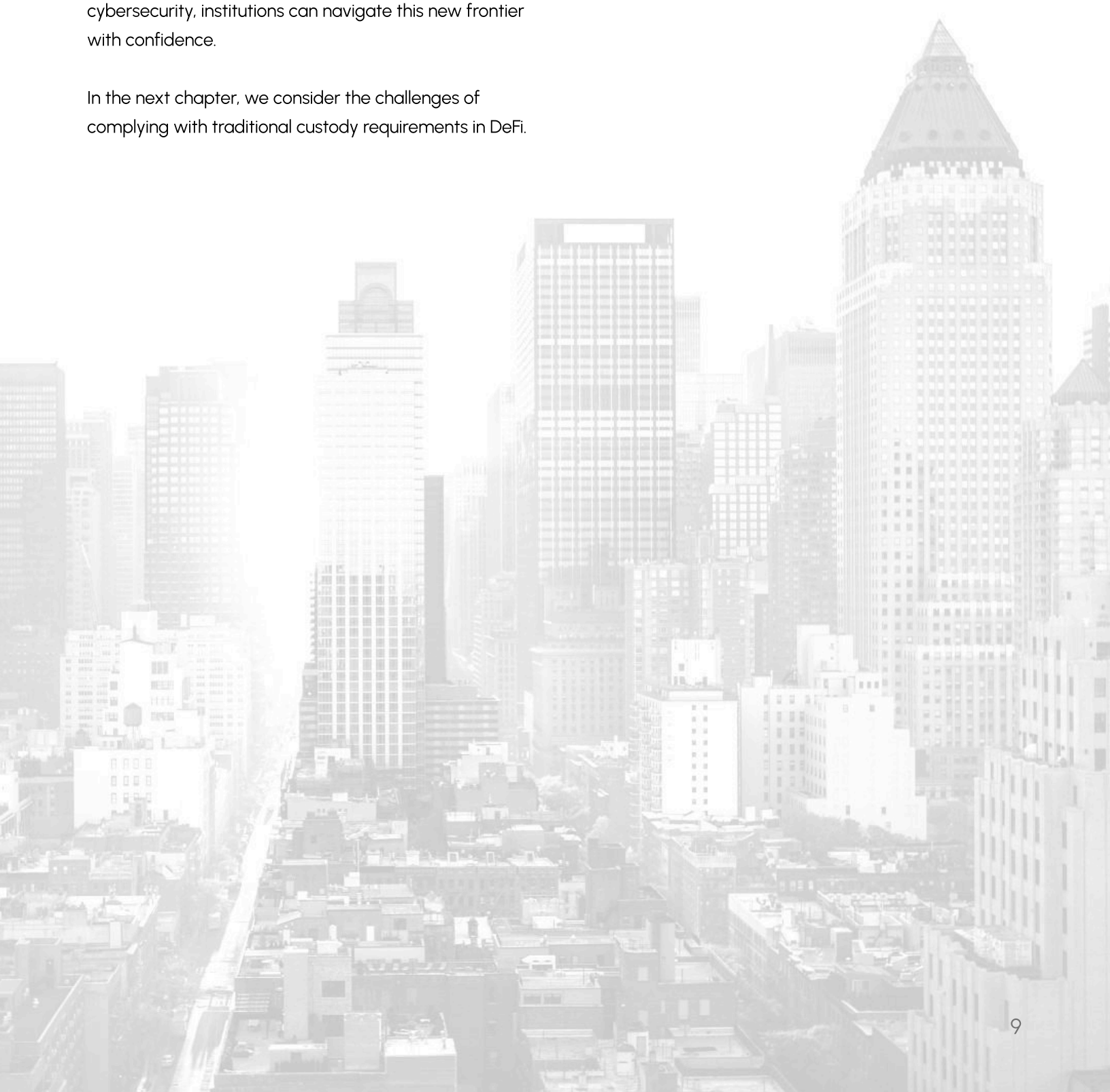
Institutions that successfully engage with DeFi protocols often do so by leveraging the expertise of specialized vendors. A number of cybersecurity specialists offer cutting-edge solutions designed to address the unique challenges of decentralized finance. From enhanced monitoring tools, to sophisticated threat detection systems, these vendors can help mitigate the risk of hacks and unauthorized access.

Many of our institutional clients have found success by working with trusted vendors who offer DeFi-specific cybersecurity solutions. Talos maintains relationships with some of the most reputable cybersecurity specialists in the industry and can help connect institutions with specialized partners to support safe interactions with the DeFi ecosystem.

Conclusion

The cybersecurity challenges facing financial institutions in DeFi are significant, but not insurmountable. By selectively engaging with protocols, leveraging multiple wallets, and working with trusted vendors who specialize in DeFi cybersecurity, institutions can navigate this new frontier with confidence.

In the next chapter, we consider the challenges of complying with traditional custody requirements in DeFi.



03

Custody Challenges in DeFi: Navigating Compliance for Institutions

Custody Challenges in DeFi: Navigating Compliance for Institutions

For institutions managing assets on behalf of clients, the path to DeFi is marked by significant hurdles—particularly when it comes to complying with existing custody regulations. Regulatory frameworks present a significant challenge in an ecosystem where assets are often held in self custody wallets rather than by traditional custodians.

Institutional DeFi is inherently at odds with the Custody Rule

The SEC's Rule 206(4)-2 (the "Custody Rule") requires private fund managers in the US to maintain client assets with a qualified third-party custodian, ensuring that assets are protected in the event of insolvency, fraud, or other events. However, the decentralized nature of DeFi complicates compliance with this regulation. In DeFi, assets are typically stored in decentralized wallets or locked in smart contracts rather than held by a custodian.

The recent case of Galois Capital is a prime example of the challenges institutions face. After a two-year investigation, Galois Capital, formerly an SEC-registered investment advisor, settled with the SEC for $225,000 due to failures to comply with the Custody Rule while managing crypto assets. This case marked the first action taken against an institution for custody violations involving crypto assets and signals the need for institutions to carefully consider custody requirements in the DeFi space.

Institutions interested in DeFi must reconcile traditional custody rules with a decentralized framework that operates outside the conventional financial system. Unlike traditional custodians that meet regulatory definitions, smart contracts and decentralized wallets do not easily fit the mold of "qualified third-party custodians". Without a clear path to compliance, how can institutions mitigate the risk of regulatory scrutiny and keep assets secure while still benefiting from the advantages of DeFi?

Solutions for custody compliance in DeFi

Despite these challenges, institutions can adopt several strategies to reduce the risk of regulatory actions and safeguard digital assets. Through our experience working with institutional clients in DeFi, we've identified several potential solutions:

1. SELECTING AN INSTITUTIONAL-GRADE CUSTODY SOLUTION

Institutions must be proactive in choosing a custody solution that balances DeFi's decentralized nature with the security and oversight expected by regulators. One option is to opt for an enterprise-grade self-custody solution from reputable providers that help ensure that assets are secure both in custody and during transfer. Institutional-grade custody solutions also offer features to support a firm's internal controls, such as multiple approvals or different levels of approvals depending on the size of the transaction. These solutions can help bridge the gap between DeFi best practices and traditional custody requirements.

2. MAKING TRANSPARENT DISCLOSURES

Disclosure is key when managing DeFi investments on behalf of clients. Institutions must clearly disclose the risks associated with their chosen custody solution as well as the risks inherent in DeFi itself. Proper disclosure not only helps fulfill regulatory requirements, but also builds trust with clients by informing them of potential risks.

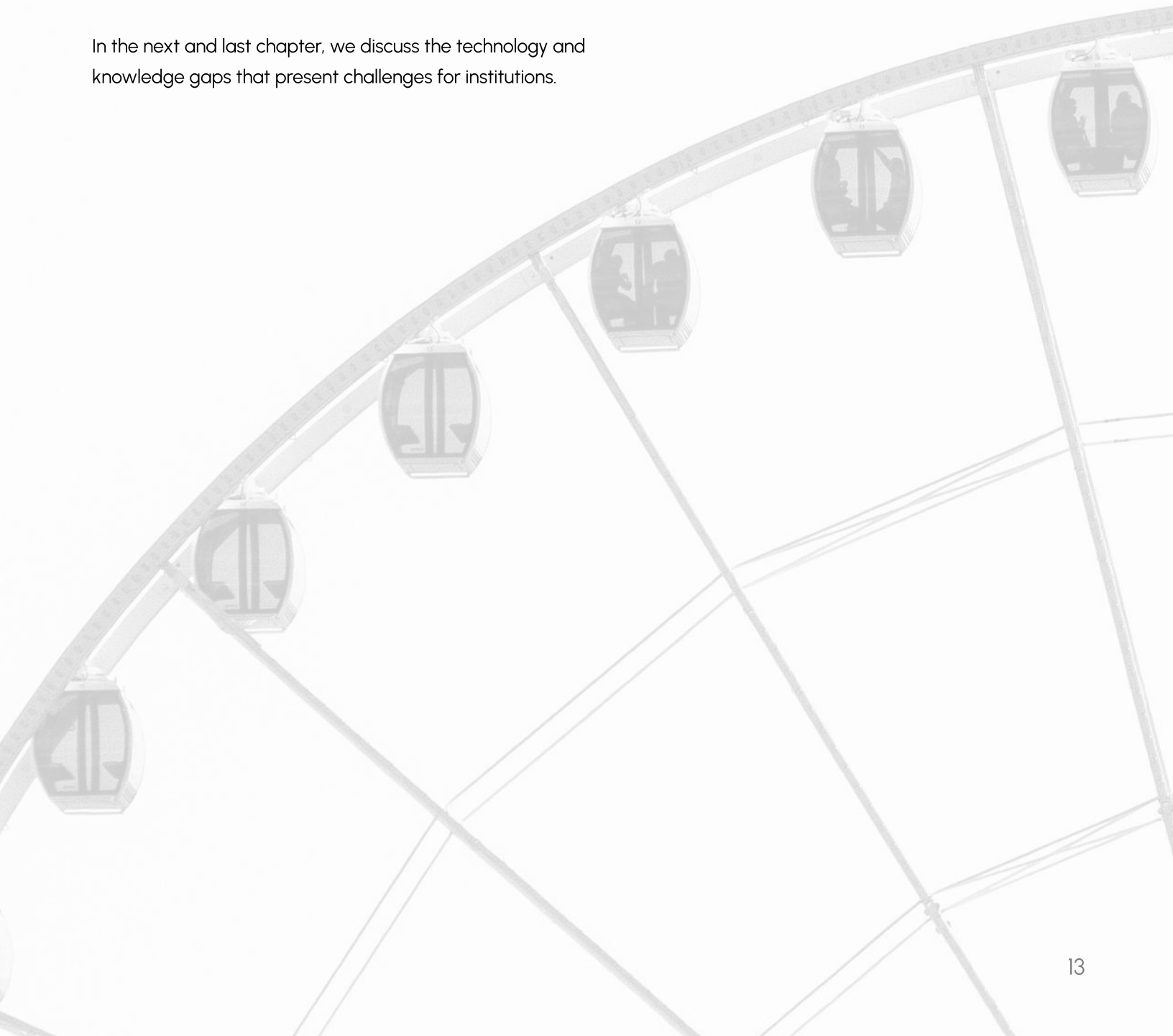
3. SECURING INSURANCE COVERAGE

DeFi protocols often lack the comprehensive insurance coverage that traditional third-party custodians offer. However, working with the right insurer can help institutions secure coverage to mitigate the risks associated with self custody. Some even provide specific coverage for smart contract failures and hacks, which institutions can use to hedge against risks associated with DeFi smart contracts.

Conclusion

While full compliance with custody regulations may not always be possible when transacting in DeFi, institutions can adopt smart solutions to minimize risks and safeguard assets. From selecting the right custody and insurance partners, to managing disclosures and security, there are ways for institutions to responsibly engage with DeFi while minimizing regulatory concerns and potential risks around custody.

In the next and last chapter, we discuss the technology and knowledge gaps that present challenges for institutions.



04

Technology Challenges and Knowledge Gaps in DeFi: Partnering for Success

Technology Challenges and Knowledge Gaps in DeFi: Partnering for Success

As financial institutions begin exploring the DeFi landscape, many are realizing that their legacy systems and existing workflows are not compatible with blockchain technology. Interacting with decentralized protocols and automated market mechanisms can feel like an entirely new world – one where the rules of traditional finance (TradFi) don't apply.

Technology challenges: Interoperability and Irreversibility

Financial institutions are accustomed to working with highly customized legacy systems designed to operate within the parameters of traditional, centralized finance. DeFi, by contrast, is decentralized, with no intermediaries to broker trades, maintain order books, or manage custodial services. This creates a significant interoperability issue – getting legacy systems to communicate with blockchain protocols is complicated.

For example, while transaction data is available on chain, parsing that data into institutional-grade reports, audit trails, and compliance documents requires sophisticated tools and expertise. This can be a headache for investment advisors that must routinely provide clients with detailed account statements and portfolio breakdowns from custodians. Without the right technology, it is difficult to generate a unified report that captures assets stored on chain across multiple wallets and protocols.

Another challenge inherent in DeFi technology is the irreversibility of transactions, which can make mistakes both costly and permanent. In TradFi, by contrast, there is often a centralized intermediary to contact to help parties unwind transaction errors. If a transaction is mistakenly submitted to a DeFi protocol, there is nobody to call to reverse it.

Knowledge gaps: Understanding the Idiosyncracies of DeFi

In addition to technological hurdles, many institutions may lack knowledge about how DeFi operates. This can cause operational challenges, such as failing to understand why a trade on a certain digital asset failed. For example, in DeFi, assets can be upgraded or updated, with ticker symbols and contract addresses changing in ways unfamiliar to those used to CeFi. So a simple mistake, like attempting to trade a "dead coin", may lead to errors and confusion.

Failing to understand Miner/Maximum Extractable Value (MEV) risk is another example of an area where a lack of knowledge can result in significant slippage on transactions. MEV is a set of strategies employed by arbitrageurs to maximize their profits by reordering or censoring transactions in a blockchain network. This is possible because pending smart contract transactions are held in the network's publicly visible waiting area, or mempool, where they sit until a miner or validator confirms the next block in the network chain. If institutions are unaware of MEV risk, they may unknowingly be allowing arbitrageurs to front-run their transactions.

Addressing the technology challenges and knowledge gaps

The good news is that solutions to these challenges exist. By partnering with the right technology provider, institutions can gain access to tools that help them confidently manage DeFi transactions – reducing the risk of a mistaken trade becoming permanently enshrined on the blockchain. Institutions should look for a technology provider that can also help to aggregate DeFi liquidity, manage trades, automate reporting and provide other information needed to operate their business in DeFi.

With the right platform, institutions can manage all of their DeFi transactions in one place, avoiding the need to piece together information from multiple blockchains and protocols. The result is a more streamlined, efficient workflow that reduces operational friction and allows institutions to focus on strategy rather than technology.

Lastly, the right partner will have deep knowledge of both CeFi and the unique nuances of DeFi, helping institutions to bridge the gap between the two worlds. A good provider will help clients understand the mechanics of DeFi: how to interact with decentralized exchanges, manage liquidity pools and avoid common pitfalls.

Conclusion

DeFi is on the cutting edge of both finance and technology, offering institutions unprecedented opportunities for innovation and growth. However, as with any frontier, it comes with a novel set of challenges, particularly for institutions dependent on legacy systems and traditional methods of operation.

A key to success in DeFi is partnering with the right technology provider, one who can bridge both the technology and knowledge gaps.

Talos has helped numerous institutions navigate DeFi's complexities. Contact us to explore how we can support your institution in overcoming these challenges to unlock the potential of DeFi.

[1]See US Dep't of the Treas., AMLA: The Department of the Treasury's De-Risking Strategy, 22 (2023), https://home.treasury.gov/system/files/136/Treasury_AMLA_23_508.pdf

[2]Rebecca Rettig, Michael Mosier & Katja Gilman, Genuine DeFi as Critical Infrastructure: A Conceptual Framework for Combating Illicit Finance Activity in Decentralized Finance, (2024), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4607332

[3]55 Dep't of the Treas., A Framework for OFAC Compliance Commitments, https://ofac.treasury.gov/media/16331/download?inline (last visited Jan. 23, 2024); Dep't of the Treas., Sanctions Compliance Guidance for the Virtual Currency Industry, (2021), https://ofac.treasury.gov/media/913571/download?inline

[4]Joseph Burleson, Michele Korver & Dan Boneh, Privacy-Protecting Regulatory Solutions Using Zero-Knowledge Proofs, a16z crypto, (2022), https://a16zcrypto.com/posts/article/privacy-protecting-regulatory-solutions-using-zero-knowledge-proofs-full-paper/

[5]Funds Stolen from Crypto Platforms Fall More Than 50% in 2023, but Hacking Remains a Significant Threat as Number of Incidents Rises, Chainalysis (Jan. 24, 2024), https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2024/

[6]Press Release, SEC Charges Crypto-Focused Advisory Firm Galois Capital for Custody Failures, U.S. Securities and Exchange Commission (Sept. 3, 2024), https://www.sec.gov/newsroom/press-releases/2024-111

talos.com