2024

Deciphering Crypto Risks: Crypto asset risk management requirements for financial service providers

Christian Zeiß
Julius-Maximilians-Universität Würzburg, Germany, christian.zeiss@uni-wuerzburg.de

Konstanze Lang
Julius-Maximilians-Universität Würzburg, Germany, konstanze.lang@stud-mail.uni-wuerzburg.de

Axel Winkelmann
Julius-Maximilians-Universität Würzburg, Germany, axel.winkelmann@uni-wuerzburg.de

Recommended Citation

Zeiß, Christian; Lang, Konstanze; and Winkelmann, Axel, "Deciphering Crypto Risks: Crypto asset risk management requirements for financial service providers" (2024). *Wirtschaftsinformatik 2024 Proceedings*. 28.
https://aisel.aisnet.org/wi2024/28

Deciphering Crypto Risks: Crypto asset risk management requirements for financial service providers

Research Paper

Christian Zeiß[1], Konstanze Lang[1], and Axel Winkelmann[1]

University of Würzburg, 97070 Würzburg, Germany
{christian.zeiss,konstanze.lang,axel.winkelmann}@uni-wuerzburg.de

Abstract. The emergence of decentralized finance and crypto assets has fundamentally changed the financial world and offers new potential to private investors and financial service providers. Despite the benefits, it is essential to face the risks. While initial regulation is already in place for risk management, financial service providers are often left to implement these measures on their own. This paper aims to identify the requirements for crypto assets risk management for financial service providers that go beyond implementing individual regulations. Guided by our research approach, we derive requirements from an academic and practical knowledge base. Accordingly, we evaluate the final requirements with a mixed-methods approach to receive feedback from portfolio managers, financial advisors, and blockchain experts. Finally, we will provide a comprehensive framework for financial service providers to effectively manage and mitigate crypto asset risks.

Keywords: Crypto Asset, Risk management, DeFi, Financial Service Provider

1 Introduction

A financial system that offers services and products with low transaction costs, high returns, and transparency (Gramlich et al. 2023, Schär 2021) - at first glance, it sounds like an ideal situation. But is it? Crypto assets have recently experienced enormous demand and are developing into financial products for the masses (Piñeiro-Chousa et al. 2022, Litterscheidt & Streich 2020). Initially, crypto assets were a niche product held only in the portfolios by a small target group despite their high-profit potential (Voskobojnikov et al. 2021). As the number of financial products available and the number of websites providing them has increased rapidly, decentralized finance (DeFi) and cryptocurrencies are becoming widely available to the general public (Rehman et al. 2020, Zeiß, Straub, Schaschek & Winkelmann 2024).

Despite this, fraud and a lack of regulation are plaguing crypto assets (Conti et al. 2018, Chalmers et al. 2022), leading to cases such as Cryptoqueen[1] and FTX[2] attracting media attention. Accordingly, it is crucial for all players in the crypto market to be aware of these risks and to understand them fully (Valeonti et al. 2021). This heightened level of threat that requires appropriate risk management accompanies the novelty of crypto

[1] https://edition.cnn.com/2023/01/22/business/ruja-ignatova-cryptoqueen-fbi-most-wanted-cec/index.html

[2] https://edition.cnn.com/2023/11/02/business/ftx-sbf-fraud-trial-verdict/index.html

19th International Conference on Wirtschaftsinformatik
September 2024, Würzburg, Germany

assets (Ferreira & Sandner 2021). By this, financial service providers (FSP) need to identify, measure, and minimize threats to ensure private as well as institutional investors can safely participate in the crypto market (Rehman et al. 2020, Barbereau et al. 2022). Currently, FSP encounter significant challenges in fulfilling this role partly due to a dearth of specific knowledge among organizational and individual level (Zeiß, Straub, Hahn, Lang, Schaschek, Tomitza & Winkelmann 2024). Additionally, FSP operating in the crypto market must adhere to new fundamental standards (Ferreira & Sandner 2021). However, there are various regulation standards for FSP for crypto assets, but their consolidation and embedding in the organization still need to be clarified (Maia & dos Santos 2021). The multifaceted landscape of occurring challenges and regulatory demands highlights the critical need for robust research into efficient and effective risk management strategies for FSP in the crypto ecosystem.

The problems briefly described lead us to our research question:
RQ: *What are the requirements for establishing and improving risk management for crypto assets for financial service provider?*

To answer this question, we apply a design science research approach to develop requirements by conducting a structured literature review and supplementing this with interviews with practitioners to derive provider expectations. With our results, we contribute to blockchain governance, security management in FinTech, and DeFi risk management.

The paper is structured as follows: We briefly examine the role of FSP in DeFi and risk management (Chapter **2**). Next, we describe our research design (Chapter **3**) and present the requirements (Chapter **4**). Further, we evaluate the requirements mixed-methods (Chapter **5**). In Chapter **6**, we discuss our research, concluding with limitations, further research, and implications (Chapter **7**).

2 Research Background

Financial Service Provider in Decentralized Finance. Crypto assets are tokenized assets comprising objects traded as digital representations of physical or virtual assets (Schwiderowski et al. 2023). Tokenization describes the digital securitization of virtual and physical rights and goods. Supply chain traceability (e.g., Pytel et al. 2023) have primarily used this tokenization. Nevertheless, many applications have emerged in developing the DeFi and crypto ecosystems (Whitaker & Kräussl 2020). Payment, utility, and asset tokens separate those crypto tokens (Schwiderowski et al. 2023). These assets include cryptocurrencies, non-fungible tokens, and tokenized assets such as fractionalized real estate or art (Piñeiro-Chousa et al. 2022, Hartwich et al. 2023). With the upcoming blockchain technology and as a reaction to the economic crisis, a decentralized financial system emerged (Schär 2021, Zetzsche et al. 2020). This DeFi ecosystem emphasizes the role of transparency and trust and develops new innovative business models (Chen & Bellavitis 2020). Contrary to DeFi, centralized finance relates to the traditional financial system, and investment opportunities typically comprise stocks, funds, or commodities (Wurgler 2000). Transactions require an intermediary, usually in the form of a central authority such as an FSP (Thakor 2020).

Technical innovations, new regulations, or increasing customer demands are changing the financial ecosystem and driving to a competitive environment (Qin et al. 2021, Thakor 2020). With the advent of DeFi, the formerly very powerful intermediaries, e.g., FSP, typical of the underlying blockchain technology and its pure peer-to-peer communication, have no longer been part of the system (Schär 2021). Banks were becoming considerably less influential, losing their customers and money (Gramlich et al. 2023). However, due to re-intermediation, DeFi is now softening, and new FSP are gathering in the DeFi ecosystem where technology eliminated the old players (Chen & Bellavitis 2020). For example, numerous crypto exchanges, trading platforms for tokenized assets, and service providers for custody exist (Whitaker & Kräussl 2020, Zeiß, Straub, Schaschek & Winkelmann 2024). Consequently, the new FSP have gained power. Finally, traditional FSP need to strengthen their resilience to guard their position in the ecosystem and better resist future changes (Mishra et al. 2023). As DeFi and crypto market participants, FSP requires appropriate risk management to avoid total exposure to potential dangers and risks (Ferreira & Sandner 2021, Conti et al. 2018).

Risk Management in the Financial Sector. Risk management plays a fundamental role in identifying, analyzing, and categorizing threats within an organization (Hopkin 2018). It aims to minimize risk by appropriately allocating economic resources (Stulz 2008). In the financial sector, risk management aims to maintain profitability, security, and liquidity ratios while managing assets and liabilities (Chornous & Ursulenko 2013). Investing in crypto assets will likely involve higher financial and non-financial risks, so rigorous management is essential (Jeegers 2023).

Managing non-financial risk is challenging for companies as historical data from other industries or even from the early stages of the crypto market often does not accurately reflect current risks. The crypto industry faces unique risks such as regulatory uncertainty, technological vulnerabilities (e.g., hacks, smart contract bugs), and market manipulation (Jeegers 2023). However, increasingly sophisticated measurement techniques are being used to assess these uncertainties accurately (Kaiser 2023). Quantifying non-financial risks is often challenging, so the appropriateness of different threat assessment frameworks may differ depending on the type and size of the organization, its regulatory environment, as well as best practices (Ma et al. 2021). Scenario analysis has recently emerged as an essential method of risk assessment, particularly for FSP using advanced measurement approaches for operational risk (Kaiser 2023).

The financial risks associated with crypto assets are higher than those associated with traditional assets (Chimienti et al. 2019). Financial risks can be divided into credit, liquidity, and market risks. Value at Risk (VaR), Expected Shortfall, and stress testing are methods and strategies to assess these risks (Jeegers 2023). VaR measures the expected loss on investment at a given probability and over a given time (Jorion 1996). Expected shortfall measures the severity of losses in an adverse scenario and is used to accurately estimate scenarios beyond a certain probability (Jorion et al. 2007, Jeegers 2023).

3 Methodology

Examining and validating requirements is a common research objective (Tomitza et al. 2023, Verlande et al. 2023). In order to derive our requirements for the risk management of crypto assets for FSP, we proceeded in four steps (Figure 1). Since the risk management of crypto assets is a dynamic topic, we placed great importance on findings from practice. Therefore, we considered theoretical and practical perspectives when elaborating our requirements. We evaluated these requirements employing a mixed-methods approach (Bryman 2006).

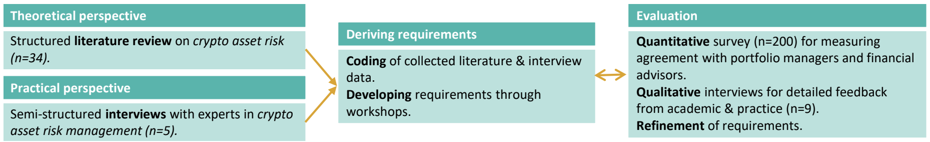

Theoretical perspective
Structured literature review on crypto asset risk (n=34).
Practical perspective
Semi-structured interviews with experts in crypto asset risk management (n=5).
Deriving requirements
Coding of collected literature & interview data.
Developing requirements through workshops.
Evaluation
Quantitative survey (n=200) for measuring agreement with portfolio managers and financial advisors.
Qualitative interviews for detailed feedback from academic & practice (n=9).
Refinement of requirements.

Figure 1. Research approach for deriving requirements for crypto asset risk management.

Step 1: We conducted a structured literature review following vom Brocke et al. (2009) focusing on crypto asset risk management for including the scientific knowledge bases. For this review of scientific literature dealing with the risk management of crypto assets in the financial sector, we searched for relevant literature using the databases *ACM Digital Library, Web of Science, and Science Direct*. Including criteria was on peer-reviewed relevant articles. For exclusion, we removed paper without digital access and duplicates (Figure 2). The literature search operated at the full-text level with the broadest possible scope using the following query string, which we adapted for each database: *("crypto asset" OR "digital asset" OR "cryptocurrency" OR "cryptocurrencies") AND "risk"*

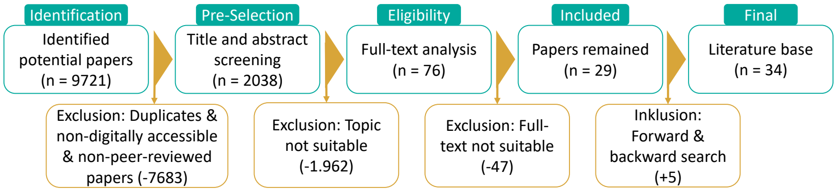
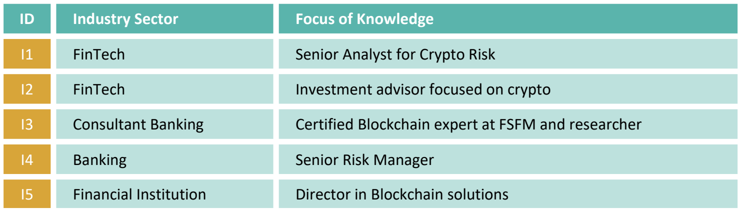

Identification
Identified potential papers (n = 9721)
Pre-Selection
Title and abstract screening (n = 2038)
Eligibility
Full-text analysis (n = 76)
Included
Papers remained (n = 29)
Final
Literature base (n = 34)
Exclusion: Duplicates & non-digitally accessible & non-peer-reviewed papers (-7683)
Exclusion: Topic not suitable (-1.962)
Exclusion: Full-text not suitable (-47)
Inklusion: Forward & backward search (+5)

Figure 2. Reduction of literature review with inclusion and exclusion.

Step 2: We performed in-depth interviews with practitioners to gain insights and expand our knowledge base for deriving our crypto asset risk management requirements. As the interviews were semi-structured, we prepared open-ended guiding questions, discussed to steer the participant toward a specific topic (Qu & Dumay 2011). As we emphasized the role of practical insights in our research approach, we selected experts with risk management experience and deep knowledge of the current trends in crypto assets, digital currencies, and the financial sector. Representatives from five FSP took part in the interviews, all of whom are experts with extensive experience in leadership positions within the company or ecosystem. The FSP surveyed all operate business models and provide risk management services within the crypto asset ecosystem. In addition, certain experts also serve as instructors at renowned academic institutions. The following figure provides a brief introduction to each interviewee (I1-I5).



ID	Industry Sector	Focus of Knowledge
I1	FinTech	Senior Analyst for Crypto Risk
I2	FinTech	Investment advisor focused on crypto
I3	Consultant Banking	Certified Blockchain expert at FSFM and researcher
I4	Banking	Senior Risk Manager
I5	Financial Institution	Director in Blockchain solutions

Figure 3. Overview of experts for interviews (I1-I5).

Step 3: For elaborating our requirements, we summarized the data collected from the literature review and the expert interviews. First, the research team read the identified relevant papers and coded them. Second, we evaluated the interview data with the qualitative content analysis by Mayring (2020). In three workshops, our research team designed and formulated requirements for managing risks associated with crypto assets.

Step 4: The evaluation consists of a quantitative survey and qualitative interviews (Bryman 2006). Using the platform Prolific, the survey is aimed at 200 portfolio managers and financial advisors, as these professional groups can provide valuable insights based on their work experience in risk management. The participants' age range was 19 to 60 (30,1 on average), and the gender-balanced audience mainly consisted of individuals from the UK, Germany, and the US. We start our study with a topical introduction. The next section of our survey presents the elaborated requirements with their titles and descriptions, each with a seven-point Likert-scale of agreement for the participants (Tomitza et al. 2023). Participants can also contribute ideas if anything needs to be added. After conducting the survey, we analyze the responses and qualitative feedback to refine the requirements. Further, we evaluate our requirements for crypto asset risk management through nine semi-structured interviews with experts from academia and practice in crypto assets as well as risk management, which we obtain through our social environment. In these interviews, we explain our research objective, approach, and final requirements and gather their qualitative feedback on the requirements for refinement. During the evaluation process, we hold several workshop sessions with the research team to refine the requirements and continuously supplement them with feedback.

4 Requirements for Crypto Asset Risk Management

Categorizing risk management requirements for FSP of crypto assets into *Assessment, Strategy, and Control* dimensions offers a clear and structured approach to effectively managing crypto asset risks. Each dimension addresses specific meta-aspects within the risk management process, while the identified requirements examine each dimension in detail. In Figure 4, we show the dimensions and requirements (REQ1-10) elaborated from literature and interviews (I1-I5) for crypto asset risk management from an FSP perspective:

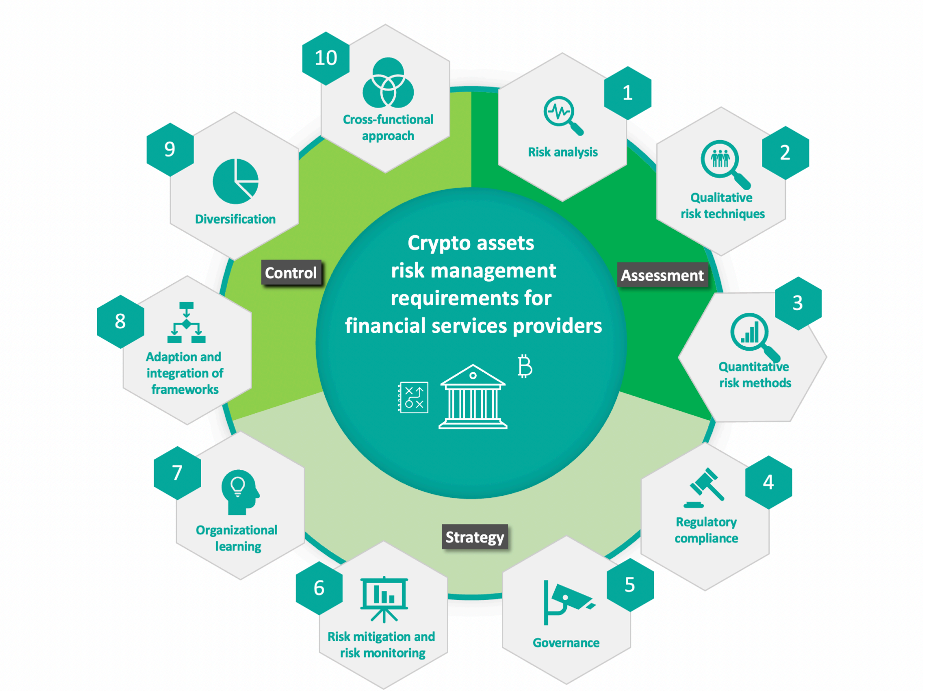

10
Cross-functional approach
1
Risk analysis
9
Diversification
2
Qualitative risk techniques
Control
Crypto assets risk management requirements for financial services providers
Assessment
8
Adaption and integration of frameworks
3
Quantitative risk methods
7
Organizational learning
4
Regulatory compliance
Strategy
6
Risk mitigation and risk monitoring
5
Governance

Figure 4. Dimensions and requirements for crypto assets risk management.

Assessment: The systematic identification and evaluation of risks is necessary to understand the nature, extent, and impact of various factors on the FSP. Use qualitative and quantitative techniques to estimate risk events' likelihood and potential impact.

REQ1: **Risk analysis** of crypto assets is crucial in their risk management due to the unique threats arising from volatility and the ever-changing regulatory environment (I1-5). "*Looking at the history, crypto assets or crypto instruments have a significantly higher volatility than traditional*" (I2). FSP should consider specific hazards regarding crypto activities, e.g., market, counterparty default, or operational risks (Hsieh & Brennan 2022). When dealing with tokenized assets, organizations should be aware of issuer risk (I1, I3). The token is introduced with a promise, such as interest payments, dividends, or service delivery. That claim's credibility determines the token's corresponding value (Schär 2021). Furthermore, cyber and technical troubles (Hacibedel & Perez Saiz 2023) align with awareness (I1-5) of the risks of decentralized protocols, cyber criminals, and technological progress (Apostolaki et al. 2017). Additionally, the lack of an appropriate corporate strategy is indicative of the entire organization (I2, I4). Risk management for crypto assets must recognize the interdependence of multiple threats (I1-5).

REQ2: **Qualitative risk techniques** are a vital aspect of managing crypto assets. It involves evaluating subjective risks that depend on market conditions, regulations, or technical limitations (I1-5). Qualitative risk techniques are crucial for estimating risks through self-executing smart contracts (Basel Committee on Banking Supervision 2022). The Financial Action Task Force (FATF) recommends using qualitative risk techniques to manage crypto assets threats (Financial Action Task Force 2019). This approach helps organizations identify and assess risks associated with crypto assets (I2). It should identify and evaluate the money laundering and terrorist financing risks (I1-5). In the United States, FSP are required by the Securities and Exchange Commission (SEC) to conduct a risk assessment before investing in or managing crypto assets (U.S. Securities and Exchange Commission 2019). Recently, major banks have adopted scenario analysis, which has become a crucial tool to employ advanced measurement approaches for operational risks, as mandated by supervisory authorities (I3, I4). It helps estimate and account for model risks that have not yet occurred or have only ensued to a limited extent (Kaiser, 2023). Scenario analysis is a technique for analyzing qualitative risks in traditional finance and applies to crypto assets (I4). "*To assess the risks, I would develop a list of criteria. Above all, I would have a look at the scenario calculation. In other words, I ask myself the question: what could actually go wrong*" (I4)?

REQ3: **Quantitative risk methods** employ mathematical and statistical tools (I2, I3, I4) to support FSP in making informed decisions to manage risks for crypto assets and estimate those threats (Ma et al. 2021). This approach enables organizations to consider the level of risk they are willing to accept when investing in crypto assets. The Basel Committee on Banking Supervision (BCBS) suggests that quantitative risk methods should be employed to establish the capital level financial institutions should maintain to cover the risks associated with crypto assets (Basel Committee on Banking Supervision 2022). According to the International Organization of Securities Commissions, assessing risks quantitatively can help FSP identify, evaluate, and prioritize crypto asset hazards and develop suitable strategies to manage them (International Organization of Securities Commissions 2023). In addition, quantitative risk methods can assist organizations in complying with regulatory requirements related to crypto assets (I1, I3). The Fifth Anti-Money Laundering Directive (5AMLD) in the European Union mandates financial institutions to evaluate the risks linked with crypto assets and establish suitable measures to alleviate those threats (European Union 2018). As crypto assets are a novel asset class with new and different risks (Gramlich et al. 2023, Ferreira & Sandner 2021), the application of quantitative methods used in traditional finance should be explored when measuring crypto asset risks (I2, I3, I4, I5). We consider VaR, Monte Carlo simulations, and Economic Capital Models to be appropriate methods (I1-I5). All statistical methods can be used for crypto assets without limitations (I2, I3, I5). However, not all of them are currently used in practice (I5). "*VaR comes with certain weaknesses that do not work well in practice [...] VaR requires calibration for each asset class. This is very tedious*" (I2). "*It is relatively difficult to carry out something like a conventional VaR calculation with a 99.9 percent confidence level, simply because of the lack of data*" (I3). "*In traditional finance, we have credit scoring models, behavioral and application scoring. None of this exists yet and has therefore not been adapted to current and future market conditions*" (I5). A further option for quantitative measurement is Bayesian structural break analyses. An advantage of this approach is that it can be applied across all asset classes (I2). Nevertheless, the advantages and disadvantages of individual measurement methods regarding crypto asset risk management are still uncertain (I3).

Strategy: This dimension involves developing and planning strategies and measures to manage, minimize, or avoid assessed risks. These strategies must address legal and compliance issues, as well as organizational resource sharing. Overall, it is crucial to consider the FSP's objectives and align the risk strategy with the corporate strategy.

REQ4: When considering risk management for crypto assets, it is advisable to thoroughly examine the applicable **regulatory compliance** (Mikhaylov 2023). Compared to traditional finance assets, there is still regulatory uncertainty (Ferreira & Sandner 2021). Nevertheless, the experts agree that regulation gives FSP security and can foster risk mitigation (I1-5). "*We need some kind of an alignment in global regulators. This alignment will provide more certainty in the space asset tracing and recovery asset tracing*" (I1). Crypto asset service providers that perform critical functions should be licensed and authorized (Bains et al. 2022, Ferreira & Sandner 2021). This includes companies that provide transfer, exchange, settlement, and custody services (Bains et al. 2022). New regulations, such as 'Markets in Crypto-Assets' (MiCAR), control the market more strictly (I1, I2). Organizations' requirements for crypto assets could be more extensive (I3). Regulatory risks can also vary by country, and it is a challenge presently that we need to align regulations globally (I1, I5). BCBS 239 is a standard that governs threat reporting by financial institutions. It requires FSP to limit Group 2 crypto assets to less than 1 percent of their Tier 1 capital for risk management purposes. The decision to enter into such transactions (I2, I4) must be entirely consistent with the FSP's risk appetite and strategic objectives, as determined and approved by the bank's board of directors (I2). In addition, financial institutions' stress testing analyses must include crypto transactions (Basel Committee on Banking Supervision 2022).

REQ5: Unclear and inconsistent **governance** structures and processes can pose risks to investors, financial institutions, and the broader financial system. Governance encompasses various factors, including transparent decision-making processes, efficient risk management practices, and robust internal controls (Brown et al. 2009, Basel Committee on Banking Supervision 2022). By prioritizing governance as a requirement for risk management, organizations can better manage the unique hazards of crypto assets and build trust with stakeholders (I3, I5). Consensus-oriented governance models in crypto assets allow stakeholders to develop assets, enabling innovative risk management and achieving political goals. However, these models also pose challenges in determining responsibility for damages. The decentralized nature of decision-making makes it difficult to determine who is accountable for any harm that may arise (Elliott & De Lima 2018).

REQ6: To assess newly emerging threats promptly, it is necessary to **continuously monitor** the crypto asset market and its interconnectedness with the broader financial system (I2, I4). The implementation of regulations such as the EU proposal MiCAR is required to **mitigate already identified risks**. Due to the rapid pace of developments in the crypto market and the potential for influential players to accelerate adoption, continuous monitoring is necessary to identify critical exposures should they arise (Zeiß, Straub, Schaschek & Winkelmann 2024). Monitoring crypto assets' use on any crypto market presents a significant challenge. While conducting a comprehensive analysis of direct and indirect exposures is difficult, it is still possible to gain valuable insights (I3, I5). Official statistics are already helpful in shedding light on aggregated indirect exposures of the main economic sectors to crypto assets (International Monetary Fund 2023). For instance, the European Securities and Markets Authority has published a risk monitoring framework for the crypto asset market, which covers stablecoins, crypto asset service providers, and decentralized financial services (European Securities and Markets Authority 2022).

REQ7: By fostering a culture of **continuous learning for organizations**, FSP can ensure that their staff is up-to-date with the trends, threats, and best practices in the industry (Gephart et al. 1996). This culture can help organizations stay informed on the latest developments in the crypto asset market and adjust their risk management strategies accordingly (I3, I5). Organizational learning is essential for risk management in crypto assets, as the market is rapidly evolving, and new threats and opportunities are constantly emerging (Zetzsche et al. 2020, Zeiß, Straub, Hahn, Lang, Schaschek, Tomitza & Winkelmann 2024). By promoting ongoing education, organizations can build a more knowledgeable and skilled workforce, which can help them better manage risks and stay ahead of the curve in the rapidly evolving crypto ecosystem (Mishra et al. 2023). Organizations can provide training and development opportunities for their staff (I1-5). Additionally, organizations can encourage their staff to stay informed by reading publications (I1, I3) and attending events (I1, I3, I5).

Control: Implementing specific control measures and procedures involves ongoing monitoring and adjustment of risk management measures to ensure effectiveness and keep threat exposure within acceptable limits. Effective risk control necessitates a continuous assessment of the risk landscape and the effectiveness of the implemented controls, as well as inter- and intra-organizational resource sharing.

REQ8: FSP should have a **clear and robust risk management framework** appropriate to the threats of their crypto asset exposures and services (I2, I5). Given the anonymity and limited regulatory oversight of crypto assets, banks should fully **integrate** their risk management framework for cryptos into their overall risk management processes (I5), including those related to anti-money laundering and countering the financing of terrorism and sanctions evasion and increased fraud monitoring (The Bank for International Settlements 2019, Basel Committee on Banking Supervision 2022). One way to manage these risks is to integrate frameworks into existing processes (KPMG 2022). FSP should assess whether they adequately incorporate the features of these mostly new and untested markets into their risk frameworks. In the longer term, methodologies and calibrations will likely need to be adjusted (Bank of England 2023).

REQ9: The highly volatile and decentralized nature of crypto assets makes them particularly risky (Piñeiro-Chousa et al. 2022, Schär 2021). Therefore, a lack of **diversification** can lead to significant losses. "*It is essential to differentiate between the banking perspective, which involves holding cryptos on its books with the intention of selling them to customers, and the investment perspective*" (I5). Most crypto assets must provide diversification benefits to investors. Smart Contracts, Proof of Work coins, Proof of Stake coins, and Masternodes are the best out-of-sample diversifiers. They consistently outperform the benchmark portfolio (Kajtazi & Moro 2019). The diversification benefits of crypto assets must be less beneficial for risk-averse investors (I1, I3, I5). During uncertain economic environments, crypto assets offer similar diversification benefits to traditional assets (Platanakis et al. 2018). There is a need to consider not only the number of different assets but also their specific characteristics (I1-5). A diversified portfolio could include assets with varying market capitalization, trading volume, and risk profiles (Trimborn et al. 2020). Banks must adhere to strict credit risk standards when valuing crypto assets and cannot exploit diversification benefits. "*Holding Bitcoin and Ether will not allow me as a bank to claim any diversification benefits from a credit risk perspective. Unless the investment is hedged, the bank has to hold one euro in capital reserves for every euro it invests in ether. Similarly, for every euro invested in Bitcoin, the bank is required to hold a corresponding capital reserve for every euro invested. This is an additional burden on the bank*" (I2).

REQ10: A **cross-functional approach** enables looking at risks from different perspectives, thereby conducting a more comprehensive assessment. Through the collaboration of experts, potential risks can be identified early and managed appropriately (I1-5). Crypto assets risks are of particular concern due to their high volatility, lack of regulation, and cybersecurity concerns (Arner et al. 2019). In addition, a cross-functional approach can help increase transparency and accountability in risk management of crypto assets (I3, I5). Organizations that adopt an interdisciplinary approach can better demonstrate that they have taken appropriate measures to minimize potential risks (Mizrak 2023).

5 Evaluation

We evaluate our requirements mixed-methods (Bryman 2006) by a quantitative survey and qualitative insights from expert interviews. First, we proceeded with the survey, measuring the degree of agreement for each requirement, including keywords and descriptions, with a 7-point Likert scale. We interviewed 200 portfolio managers and financial advisors at asset and wealth management firms. Figure 5 shows an average agreement of 87.3% on all requirements. We recognize the highest values for the risk analysis (REQ1), the quantitative risk methods (REQ3), and organizational learning (REQ7). On the contrary, the participants perceive the minimum agreement for the cross-functional approach (REQ10) and diversification (REQ9).

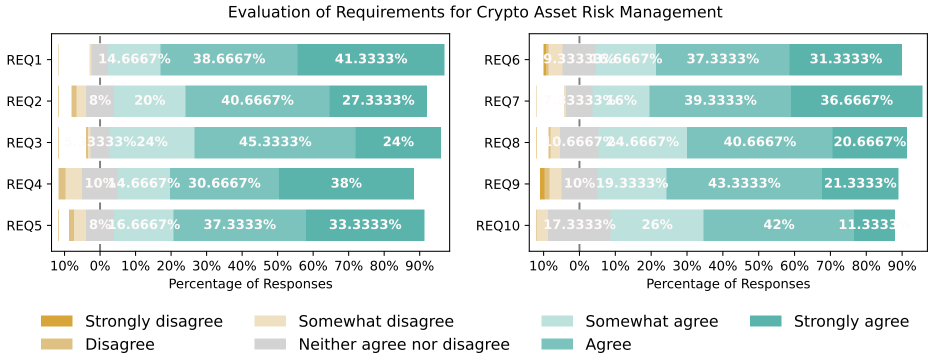


Figure 5. Quantitative evaluation of the requirements with a survey. (n=200)

In addition, we conducted semi-structured interviews with nine highly qualified experts from academia and practice who specialize in risk management, crypto finance, or organizational adaptation. We presented the elaborated dimensions and requirements.

Regarding understandability, the experts mention a high degree (IE1, IE4, IE9) as the requirement, including the high-level abstraction in Figure 4, and the descriptions and explanations (IE2) support each other. The experts really like the focus of the requirements, as it combines risk assessment and mitigation with organizational aspects of learning and integration (IE1, IE3, IE6). The scope of the requirements is rated quite well. Some experts might add ethical perspectives, fairness, or other aspects (IE1, IE2, IE5, IE8, IE9). In addition, the experts appreciate the aspects of governance and integration of frameworks, organizational learning, and cross-functional approach, as these points are most lacking in reality (IE1, IE2, IE6). Finally, the requirements could enrich the common understanding of crypto assets as well as the awareness of crypto assets and specific risk management across the organization. The requirements highlight components for implementing their risk management processes and structures (IE6, IE9). Summarizing the results of the twofold evaluation, the study participants and the experts from the interviews underline the importance of combining qualitative and quantitative risk assessment. As a discrepancy, the experts emphasized inter- and cross-organizational integration (REQ8, REQ10) and governance.

6 Discussion

By developing requirements for establishing and improving risk management of crypto assets for FSP, we aim to boost their stability, ensuring they remain unshaken in turbulent markets. Risk factors and their management in crypto assets are complex and require a multidisciplinary approach. FSP must, therefore, not only navigate the intricate regulatory landscape but also develop robust internal systems to monitor and manage risks.

Both traditional financial assets and crypto assets are subject to a range of risk factors. However, there are notable differences between the two. Crypto assets, for instance, often display higher volatility and a paucity of historical data for risk assessment (Jeegers 2023, Zeiß, Straub, Schaschek & Winkelmann 2024). This complicates the application of quantitative models based on data and necessitates a more comprehensive approach that entails the incorporation of qualitative factors (Leo et al. 2019), (I1-5). Qualitative methods and expert judgment are particularly important in regulatory uncertainty, which presents a significant challenge in developing appropriate risk management strategies. Large banks have begun to employ scenario analysis for the risk management of crypto assets in a manner similar to that observed for traditional financial assets (I4). Clear and coherent regulation is crucial for enhancing risk management (European Securities and Markets Authority 2022, Ferreira & Sandner 2021). Coupled with diversification strategies, the implementation of clear and consistent regulatory frameworks can mitigate risks in the crypto asset market. However, the high correlation among these assets, particularly Payment Tokens, limits diversification's efficacy. Compared to Payment Tokens, managing risks associated with so-called Utility Tokens is focused on understanding and evaluating the adoption and usage of the underlying protocol, as the value of these tokens is less influenced by market speculation (I3).

Although technological challenges can be scary, they are solvable with further research and development. However, legal and regulatory risks are more complex. The regulatory landscape is trying to keep up with the pace of digital innovation within the crypto market but requires harmonized global efforts (Teng et al. 2023). Frameworks such as the MiCA, GDPR, or AML regulation provide decision-making platforms, but the complexity of compliance requires continued efforts by FSP (I1). Market risks from extreme volatility and changes in sentiment emphasize the need for modern financial instruments and infrastructures. Overall, monitoring the crypto asset space and taking appropriate measures to manage the risks and capitalize on the opportunities is crucial.

7 Conclusion

Summary. This research paper examined the requirements for crypto asset risk management for financial service providers. In particular, it focused on elements of strategy, assessment, and control, which provide a comprehensive and organizational approach that extends beyond the mere implementation of legal requirements. We used a literature review and interviews with experts in assessing and managing crypto risks as a knowledge base. For evaluation, 200 participants, focusing on portfolio managers and financial advisors, completed our questionnaire and rated the requirements. Additionally, we conducted nine interviews with experts from academia and practice to obtain more profound qualitative feedback for refinement. In total, we collected ten requirements.

Limitations and Further Research. Our approach's rigid structure and implementation were both advantages and limitations. Using a structured literature review and semi-structured interviews to gain knowledge encountered obstacles such as conceptualizing the proper search string, selected databases, or the experts' and study participants' quantity and profile. Further insights can be gathered by integrating focus groups or empirical surveys. Including different FSP types and sizes as well as different crypto assets offered, promising research can be initiated based on our results. Furthermore, adopting emerging technologies, such as artificial intelligence, has immense potential to enhance risk management by facilitating improved decision-making. Nevertheless, further research needs to address data privacy, cybersecurity, and quality control challenges.

Implications. We contribute to the knowledge base of blockchain governance, security management in banking, and DeFi risk management. Our requirements should form the foundation for creating organization-specific, robust risk management frameworks that consider the correlation between different crypto assets, the impact of market volatility, and regulatory changes. Our results contribute to the IS research field and address the financial sector. For practical implications, FSP can adapt our requirements by creating new or modifying their existing risk management frameworks based on their type of FSP service offer or size. Comprehensive risk management does not depend solely on the further development of regulations. With our requirements, we deliver many aspects that FSP must proactively address to compete in the crypto asset ecosystem in the long term.

8 Acknowledgements

This work has been developed in the project InKryBa and is partly funded by the DZ-Bank-Stiftung under grant number FRFMM-788/2022. The authors are responsible for the content of this publication.

References

Apostolaki, M., Zohar, A. & Vanbever, L. (2017), Hijacking bitcoin: Routing attacks on cryptocurrencies, *in* '2017 IEEE symposium on security and privacy (SP)', IEEE, pp. 375–392.

Arner, D. W., Zetzsche, D. A., Buckley, R. P. & Barberis, J. N. (2019), 'The identity challenge in finance: from analogue identity to digitized identification to digital kyc utilities', *European business organization law review* **20**, 55–80.

Bains, P., Ismail, A., Melo, F. & Sugimoto, N. (2022), *Regulating the crypto ecosystem: the case of stablecoins and arrangements*, International Monetary Fund.

Bank of England (2023), Prudential Regulation Authority Annual Report 2022-23, Technical report. Accessed: 2024-03-01.

Barbereau, T., Sedlmeir, J., Smethurst, R., Fridgen, G. & Rieger, A. (2022), Tokenization and regulatory compliance for art and collectibles markets: from regulators' demands for transparency to investors' demands for privacy, *in* 'Blockchains and the Token Economy: Theory and Practice', Springer, pp. 213–236.

Basel Committee on Banking Supervision (2022), 'Prudential treatment of cryptoasset exposures'. `https://www.bis.org/bcbs/publ/d545.pdf`.

Brown, I., Steen, A. & Foreman, J. (2009), 'Risk management in corporate governance: A review and proposal', *Corporate Governance: An International Review* **17**(5), 546–558.

Bryman, A. (2006), 'Integrating quantitative and qualitative research: how is it done?', *Qualitative research* **6**(1), 97–113.

Chalmers, D., Fisch, C., Matthews, R., Quinn, W. & Recker, J. (2022), 'Beyond the bubble: Will nfts and digital proof of ownership empower creative industry entrepreneurs?', *Journal of Business Venturing Insights* **17**, e00309.

Chen, Y. & Bellavitis, C. (2020), 'Blockchain disruption and decentralized finance: The rise of decentralized business models', *Journal of Business Venturing Insights* **13**, e00151.

Chimienti, M. T., Kochanska, U. & Pinna, A. (2019), 'Understanding the crypto-asset phenomenon, its risks and measurement issues', *Economic Bulletin Articles* **5**.

Chornous, G. & Ursulenko, G. (2013), 'Risk management in banks: new approaches to risk assessment and information support', *Ekonomika* **92**(1), 120–132.

Conti, M., Kumar, E. S., Lal, C. & Ruj, S. (2018), 'A survey on security and privacy issues of bitcoin', *IEEE Communications Surveys Tutorials* **20**, 3416–3452.

Elliott, D. J. & De Lima, L. (2018), 'Crypto-assets: their future and regulation', *Oliver Wyman* pp. 1–14.

European Securities and Markets Authority (2022), 'Crypto-Assets and Financial Stability', `https://www.esma.europa.eu/sites/default/files/library/esma50-165-2251_crypto_assets_and_financial_stability.pdf`. Accessed: 2023-03-15.

European Union (2018), 'Regulation (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018', `https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L0843`. Accessed: 2023-03-15.

Ferreira, A. & Sandner, P. (2021), 'Eu search for regulatory answers to crypto assets and their place in the financial markets' infrastructure', *Computer Law and Security Review* **43**, 105632.

Financial Action Task Force (2019), 'Guidance for a risk-based approach to virtual assets and virtual asset service providers'. https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html.

Gephart, M. A., Marsick, V. J., Van Buren, M. E., Spiro, M. S. & Senge, P. (1996), 'Learning organizations come alive', *Training & Development* **50**(12), 34–46.

Gramlich, V., Guggenberger, T., Principato, M., Schellinger, B. & Urbach, N. (2023), 'A multivocal literature review of decentralized finance: Current knowledge and future research avenues', *Electronic Markets* **33**.

Hacibedel, B. & Perez Saiz, H. (2023), 'Assessing macrofinancial risks from crypto assets'.

Hartwich, E., Ollig, P., Fridgen, G. & Rieger, A. (2023), 'Probably something: A multi-layer taxonomy of non-fungible tokens', *Internet Research* **34**(1), 216–238.

Hopkin, P. (2018), *Fundamentals of risk management: understanding, evaluating and implementing effective risk management*, Kogan Page Publishers.

Hsieh, S.-F. & Brennan, G. (2022), 'Issues, risks, and challenges for auditing crypto asset transactions', *International Journal of Accounting Information Systems* **46**, 100569.

International Monetary Fund (2023), '11th statistics forum: Session iv - Urszula Kocha'nska', https://www.imf.org/-/media/Files/News/Seminars/2023/11th-stats-forum/session-iv-urszula-kochanska.ashx. Accessed on 2024-03-02.

International Organization of Securities Commissions (2023), Report on Financial Technologies (Fintech), Innovation, Regulation and Sustainable Growth, Technical report, IOSCO. Accessed: 2024-03-01.

Jeegers, T. (2023), Cryptoasset taxonomies, *in* 'Understanding Crypto Fundamentals: Value Investing in Cryptoassets and Management of Underlying Risks', Springer, pp. 121–137.

Jorion, P. (1996), 'Risk2: Measuring the risk in value at risk', *Financial analysts journal* **52**(6), 47–56.

Jorion, P. et al. (2007), *Financial risk manager handbook*, Vol. 406, John Wiley & Sons.

Kaiser, T. (2023), *Praxis des Non-Financial Risk Managements im Finanzsektor*, Springer.

Kajtazi, A. & Moro, A. (2019), 'The role of bitcoin in well diversified portfolios: A comparative global study', *International Review of Financial Analysis* **61**, 143–157.

KPMG (2022), 'Cryptoassets: A Risk Management Perspective', https://kpmg.com/xx/en/home/insights/2022/04/cryptoasset-risk.html. Accessed: 2024-03-08.

Leo, M., Sharma, S. & Maddulety, K. (2019), 'Machine learning in banking risk management: A literature review', *Risks* **7**(1), 29.

Litterscheidt, R. & Streich, D. J. (2020), 'Financial education and digital asset management: What's in the black box?', *Journal of Behavioral and Experimental Economics* **87**, 101573.

Ma, C., Colon, L., Dera, J., Rashidi, B. & Garg, V. (2021), ‘Caraf: crypto agility risk assessment framework’, *Journal of Cybersecurity* **7**(1), tyab013.

Maia, G. & dos Santos, J. V. (2021), ‘Mica and defi (’proposal for a regulation on market in crypto-assets’ and ’decentralised finance’)’, *SSRN Electronic Journal* .

Mayring, P. (2020), *Qualitative Forschungsdesigns*, Springer Fachmedien Wiesbaden, pp. 3–17.

Mikhaylov, A. (2023), ‘Understanding the risks associated with wallets, depository services, trading, lending, and borrowing in the crypto space’, *Journal of Infrastructure, Policy and Development* **7**(3).

Mishra, R., Singh, R. K., Kumar, S., Mangla, S. K. & Kumar, V. (2023), ‘Critical success factors of blockchain technology adoption for sustainable and resilient operations in the banking industry during an uncertain business environment’, *Electronic Commerce Research* .

Mizrak, F. (2023), ‘Integrating cybersecurity risk management into strategic management: a comprehensive literature review’, *Research Journal of Business and Management* **10**(3), 98–108.

Piñeiro-Chousa, J., Ángeles López-Cabarcos, M., Sevic, A. & González-López, I. (2022), ‘A preliminary assessment of the performance of defi cryptocurrencies in relation to other financial assets, volatility, and user-generated content’, *Technological Forecasting and Social Change* **181**.

Platanakis, E., Sutcliffe, C. & Urquhart, A. (2018), ‘Optimal vs naïve diversification in cryptocurrencies’, *Economics Letters* **171**, 93–96.

Pytel, N., Zeiß, C. & Winkelmann, A. (2023), ‘Enabling utxo-based backwards and forwards traceabilty’, *ECIS 2023 Research Papers* **319**, 5–11.
URL: *https://aisel.aisnet.org/ecis2023*$_{r}p/$319

Qin, K., Zhou, L., Afonin, Y., Lazzaretti, L. & Gervais, A. (2021), ‘Cefi vs. defi – comparing centralized to decentralized finance’, *arXiv:2106.08157v2* .

Qu, S. Q. & Dumay, J. (2011), ‘The qualitative research interview’, *Qualitative Research in Accounting Management* **8**, 238–264.

Rehman, M. H., Salah, K., Damiani, E. & Svetinovic, D. (2020), ‘Trust in blockchain cryptocurrency ecosystem’, *IEEE Transactions on Engineering Management* **67**, 1196–1212.

Schär, F. (2021), ‘Decentralized finance: On blockchain-and smart contract-based financial markets’, *FRB of St. Louis Review* .

Schwiderowski, J., Pedersen, A. B. & Beck, R. (2023), ‘Crypto tokens and token systems’, *Information Systems Frontiers* .

Schär, F. (2021), ‘Decentralized finance: On blockchain- and smart contract-based financial markets’, *Fed. Reserve Bank St. Louis Rev.* **103**.

Stulz, R. M. (2008), Rethinking risk management, *in* ‘Corporate Risk Management’, Columbia University Press, pp. 87–120.

Teng, H.-W., Härdle, W. K., Osterrieder, J., Baals, L. J., Papavassiliou, V. G., Bolesta, K., Kabasinskas, A., Filipovska, O., Thomaidis, N. S., Moukas, A. I. et al. (2023), ‘Mitigating digital asset risks’.

Thakor, A. V. (2020), ‘Fintech and banking: What do we know?’, *Journal of Financial Intermediation* **41**, 100833.

The Bank for International Settlements (2019), ‘Statement on crypto-assets’. https://www.bis.org/publ/othp14.htm.

Tomitza, C., Schaschek, M., Straub, L. & Winkelmann, A. (2023), ‘What is the minimum to trust ai?—a requirement analysis for (generative) ai-based texts’, *Wirtschaftsinformatik 2023 Proceedings* .

Trimborn, S., Li, M. & Härdle, W. K. (2020), ‘Investing with cryptocurrencies—a liquidity constrained investment approach’, *Journal of Financial Econometrics* **18**(2), 280–306.

U.S. Securities and Exchange Commission (2019), ‘Framework for "Investment Contract" Analysis of Digital Assets’, https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets. Accessed: 2023-03-15.

Valeonti, F., Bikakis, A., Terras, M., Speed, C., Hudson-Smith, A. & Chalkias, K. (2021), ‘Crypto collectibles, museum funding and openglam: Challenges, opportunities and the potential of non-fungible tokens (nfts)’, *Applied Sciences* **11**, 9931.
URL: *https://www.mdpi.com/2076-3417/11/21/9931*

Verlande, L., Rudel, S. & Lechner, U. (2023), ‘Requirements for a federated learning system to strengthen it security in human resource management’, *Wirtschaftsinformatik 2023 Proceedings* .

vom Brocke, J., Simons, A., Niehaves, B., Riemer, K., Plattfaut, R. & Cleven, A. (2009), ‘Reconstructing the giant: On the importance of rigour in documenting the literature search process’, *17th European Conference on Information Systems* **o. A.**, 1–12.

Voskobojnikov, A., Wiese, O., Koushki, M. M., Roth, V. & Beznosov, K. K. (2021), The u in crypto stands for usable: An empirical study of user experience with mobile cryptocurrency wallets, *in* ‘Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems’, ACM, pp. 1–14.
URL: *https://dl.acm.org/doi/10.1145/3411764.3445407*

Whitaker, A. & Kräussl, R. (2020), ‘Fractional equity, blockchain, and the future of creative work’, *Management Science* **66**, 4594–4611.

Wurgler, J. (2000), ‘Financial markets and the allocation of capital’, *Journal of Financial Economics* **58**, 187–214.

Zeiß, C., Straub, L., Hahn, V., Lang, K., Schaschek, M., Tomitza, C. & Winkelmann, A. (2024), *Designing for Banking Resilience: A DeFi E-Learning Solution*, Vol. 14621, Springer, Cham, pp. 325–338.

Zeiß, C., Straub, L., Schaschek, M. & Winkelmann, A. (2024), The obscure world of digital assets - design principles for user-centered platforms, *in* ‘ECIS 2024 Proceedings’, Vol. 4, pp. 1–16.
URL: *https://aisel.aisnet.org/ecis2024/track16*$_{f}intech/track16_{f}intech/4$

Zetzsche, D. A., Arner, D. W. & Buckley, R. P. (2020), ‘Decentralized finance’, *Journal of Financial Regulation* **6**, 172–203.