KPMG

KPMG Blockchain Report 2024

January 2025

KPMG Switzerland

DLT The Foundation of Digital Trust

1 Introduction

KPMG's Blockchain Report 2024 provides you with a comprehensive analysis with valuable insights into the current state and future prospects of Distributed Ledger Technology (DLT) in Switzerland. The first chapter introduces the transformative potential of DLT and the adoption of DLT within the Swiss financial sector.

Subsequent chapters provide a detailed overview of the regulatory landscape, including key developments and their impact on the industry. We also examine the tax implications of staking for financial institutions and individuals, offering a thorough analysis of the challenges and opportunities in this area. The report concludes with an outlook on the future of DLT, supported by expert insights and recommendations, to help you navigate the evolving financial ecosystem.

For example, the Swiss Bitcoin Association is currently in talks with Swiss politicians to revive and strengthen Switzerland's role in the cryptocurrency sector. Although Switzerland already has well-established regulatory foundations and a clear framework for crypto activities, there is a growing concern that other countries are rapidly catching up. To maintain its competitive edge and leadership position, Switzerland needs to take proactive measures so as not to fall behind. These discussions aim to explore new strategies and policies that will not only reinforce the existing regulatory clarity but also lay a solid foundation to support innovation and growth in the crypto industry. In doing so, Switzerland can continue to attract and retain top crypto companies and talent, thereby securing its status as a global hub for cryptocurrency and blockchain technology.

Moreover, the current bull run in the cryptocurrency market remains stable, largely due to the expectation that the new US administration will adopt a more lenient stance on crypto regulations. This expectation has fostered a sense of optimism among investors and market participants, who believe that favorable regulatory policies could further stimulate growth and innovation within the sector.

Furthermore, the potential for a regulatory environment that supports rather than stifles the development of cryptocurrencies and blockchain technology is seen as a significant positive factor. As a result, confidence in the market has been bolstered, contributing to the sustained upward momentum of the bull run. This stability is critical for attracting new investment and encouraging the continued expansion of the crypto ecosystem.

2
DLT Adoption

2.1 Financial Sector in Switzerland

Banks' & Big4's DLT service offering

Despite recent claims by crypto startups to completely revolutionize the financial system, traditional financial institutions in Switzerland are increasingly aware of the robust capabilities of the underlying technology and the efficiency gains achieved by digital asset innovators. Especially institutional investors are recognizing that despite the market setbacks during the crypto winter, the long-term technological advantages prevail and market adoption of DLT continues.

With their extensive experience in preventing and mitigating such issues, these institutions are well-positioned to capitalize on the current wave of industry consolidation. This presents opportunities for them to acquire new technologies, skilled professionals or even entire companies, thereby strengthening their digital asset offerings.

Moreover, many Swiss banks and asset managers have established dedicated internal functions and teams that actively drive and expand crypto-related projects and product offerings for traditional financial clients.

Looking at the years ahead, the Swiss financial sector and its participants would be wise to prepare for a market structure that prioritizes blockchain's core aspects, such as Distributed permissionlessness, interoperability, transparency, and immutability with less middle-men. Regulation, not least through the election of an openly crypto-friendly US administration, is likely to follow in the coming years, making any crypto-related project or product offering less uncertain from a legal perspective.

Similarly, the EU's current efforts to create a digital Euro, or various bank's initiatives for seamless trading infrastructures, will also lead to a more crypto-ready market structure that will allow customers to become more familiar with these concepts. Eventually, newer generations of customers may grow up expecting and demanding such services and products from their bank or wealth manager.

Most large consulting agencies have identified crypto and blockchain-related services as one of the future growth areas. To this end, especially Big4 consulting firms are already engaged in crypto-related services for their clients, primarily providing advisory, licensing, tax and legal services. However, a growing number of assurance engagements can also be observed over the last couple of years.

Supported by various publications, studies and blog articles that create additional awareness and demand among existing financial market participants in Switzerland (especially banks and asset managers), most advisory engagements tend to be related to the following areas:

1. Risk management
2. Cryptoassets custody and trading
3. Technology & cyber
4. Tokenization of real-world assets
5. Fraud prevention and AML assistance
6. Stablecoins and payment infrastructures

Source: Corporate Websites of Big4 Firms & CVVC Top 50 Report 2023

2.2 Crypto Valley

Venture funding & valuation

According to the CVVC Top 50 Report 2023, global venture funding totaled USD 344.5 billion across 22,718 deals. This represents a 35% decrease in funding and a 34% decrease in the number of deals compared to 2022. Crypto Valley (i.e. Zurich, Zug, and Geneva) experienced a similar trend, with a 36% decrease in venture funding compared to its peak in 2022. The region raised USD 2.97 billion through 255 venture deals.

The Crypto Valley accounted for approx. 5.1% of European venture funding and had 6 large deals, representing 7.1% of European large deals, 1.1% of global large deals.

The top 50 projects have a total valuation of USD 373.45 billion. Notably, 18 of these companies are based in Zug, accounting for 97% of the total valuation. Similarly, the 25 privately traded blockchain companies have a combined valuation of USD 9.48 billion. Twelve of these companies are based in Zug, accounting for 59% of the total valuation. Thus, the Crypto Valley (specifically the city of Zug) still has a very large lead over any other region when it comes to Blockchain and DLT-related businesses worldwide.

Despite challenging global economic conditions, the resilience and adaptability of Crypto Valley's blockchain sector remains strong. The region's commitment to the promotion of emerging blockchain technologies and startups also remains at a high level. The Crypto Valley continues to be a hub for innovation and development in the blockchain industry.

The Crypto Valley participated in 20.4% of all European blockchain-related venture deals and secured 12.3% of the total funding in those deals.

This is an all-time high figure and shows the continued importance of the Crypto Valley and Switzerland as one of Europe's most active blockchain and crypto hubs.

The most active quarter in 2023 in terms of blockchain-related deals was Q1, with a total of USD 160.3 million raised. While Zug and Zurich contributed a total of 81% of all such deals throughout the year, with 17 and 10 deals respectively, Geneva was not far behind, with 8 deals in 2023.

In terms of the size and nature of crypto deals in Europe in 2023, it is important to note that most interest seems to have been generated in seed and early-stage investments, with 31 deals out of a total of 49 deals falling into this category. A further 10 deals were late-stage investments, while only 8 deals were pre-seed or below.

Overall, there are 13 Blockchain unicorns (companies with >USD 1 billion in market capitalization) in the Crypto Valley in Switzerland. 3 of those unicorns are privately operating companies, while 10 of them are blockchain platforms that operate publicly traded cryptocurrencies. Thus, given the substantial market capitalization in Switzerland, the crypto sector should warrant significantly more attention from financial market participants than it currently seems to receive.

Source: CVVC Top 50 Report 2023

3 Regulatory Overview

3.1 Regulatory developments

Key regulatory developments in 2024

In 2024, the Swiss Financial Market Supervisory Authority (FINMA) made significant strides in providing clarity and regulatory guidance within the rapidly evolving cryptocurrency landscape. Two major announcements were particularly noteworthy: one on the staking of cryptoassets announced in December 2023 and the other on the 'stablecoins' use case. These guidelines are central to shaping the operational and compliance framework for businesses engaged in these activities, ensuring that Switzerland continues to maintain robust regulatory standards. However, the response from the industry has not always welcoming.

In a nutshell, institutions must carefully limit counterparty and operational risk. This can be achieved through rigorous due diligence, which serves as a safeguard against potential pitfalls in the staking process. It is also imperative for institutions to ensure that third-party providers, who play a crucial role in the staking ecosystem, are not only authorized but also hold withdrawal keys. These providers must have robust risk management practices in place to prevent any adverse outcomes.

For institutions choosing direct staking and managing staking keys themselves, the emphasis on transparency remains paramount. They must provide clear risk disclosures and have measures in place to mitigate operational risks. An essential component of this approach is the preparation of a Digital Asset Resolution Package (DARP), which outlines the protocols for asset management in various scenarios.

Staking guidance

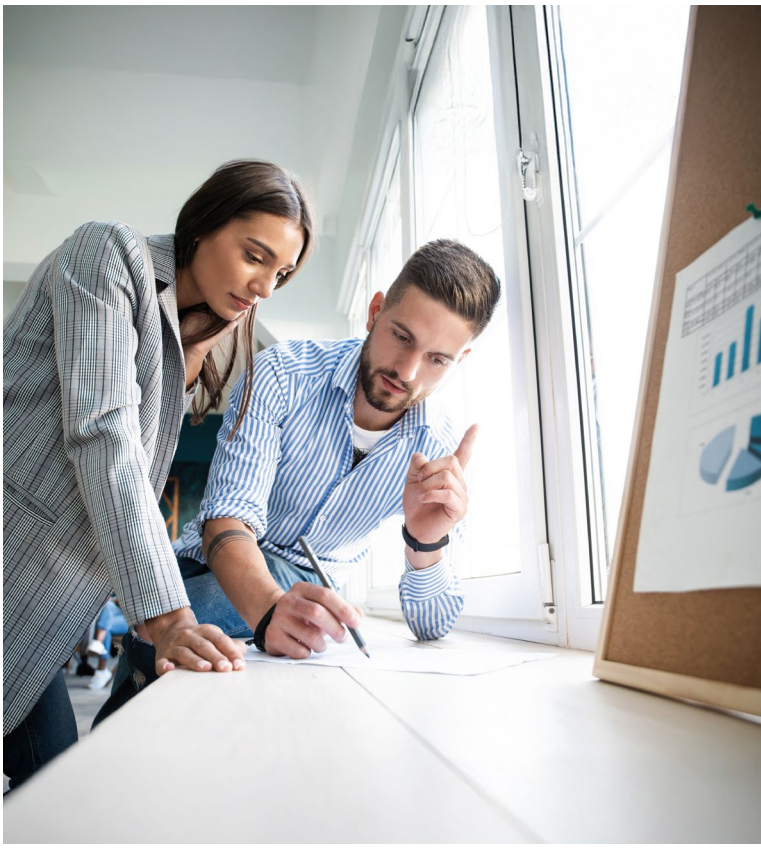
FINMA provided much-needed clarity on staking services, addressing custody, operational risks and regulatory requirements, thus dispelling earlier licensing concerns.

Background

The DLT Act of 2021 established a legal framework for cryptoasset custody, protecting customers in case of custodian insolvency. The growing prominence of staking services, coupled with Ethereum's transition to proof of stake, prompted FINMA to issue its guidance 08/23 on 20 December 2023 to reduce regulatory uncertainty.

Key Regulatory Insights

Guidance 08/23 addresses staking chain delegation, direct staking as well as unlicensed participants in staking.



3.1 Regulatory developments

The staking landscape also includes unlicensed participants, which presents its own set of challenges and considerations. Unlicensed entities offering custodial staking services are not necessarily required to obtain a banking license, provided that they conduct individual custody and are part of a self-regulatory organization for anti-money laundering (AML) supervision. This ensures that they operate within a framework that promotes accountability and adherence to financial regulations. However, the situation changes when it comes to collective custody of payment tokens, as this often requires a banking or fintech license due to the increased risks and regulatory scrutiny.

In summary, whether through staking chain delegation or direct staking, institutions must navigate a complex regulatory environment with diligence and transparency. By establishing clear fiduciary agreements, conducting thorough due diligence, and complying with regulatory requirements, institutions can effectively manage the risks associated with staking. For unlicensed participants, the path forward involves individual custody and regulatory compliance through self-regulation or obtaining the necessary licenses for collective custody. As the staking ecosystem continues to mature, these practices will be instrumental in fostering trust, stability and growth within the industry.

Stablecoin guidance

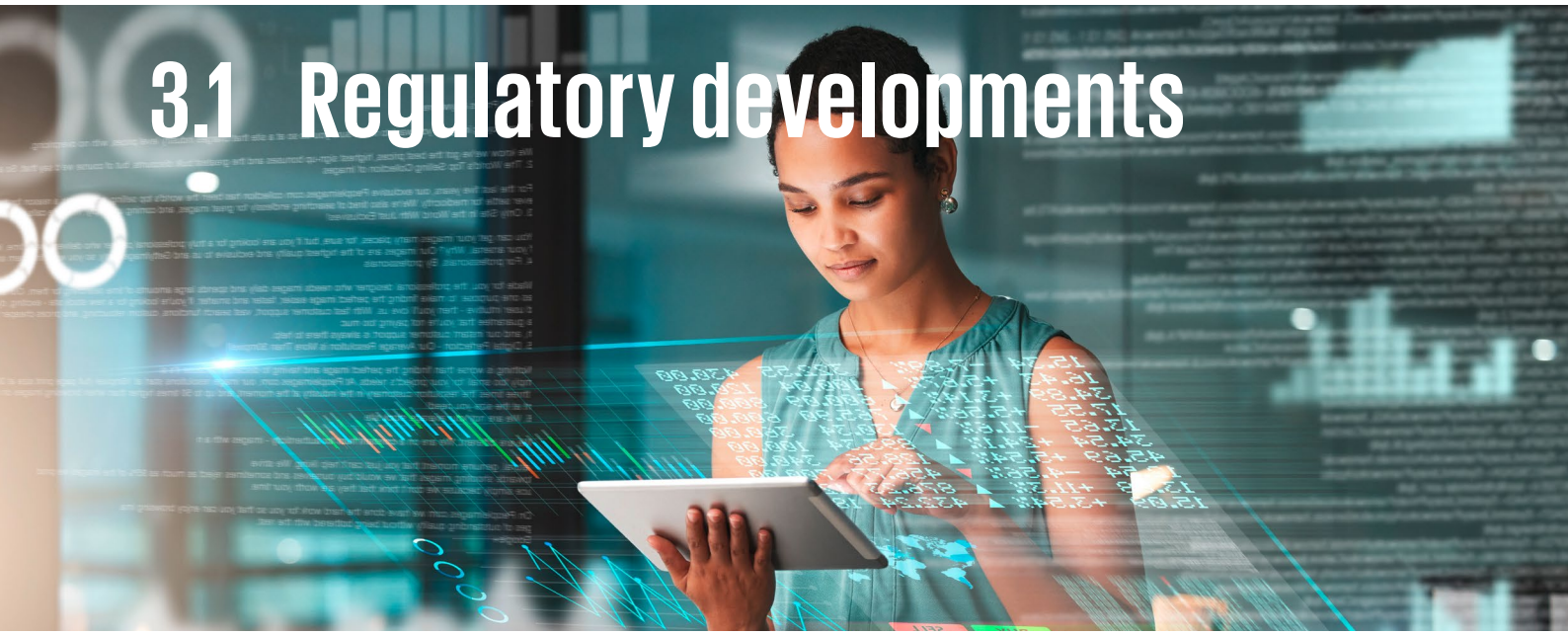
Guidance 06/2024 issued in July 2024 outlines regulatory measures to address the growing role of stablecoins in the financial ecosystem, emphasizing legal, operational, and financial stability requirements.

In most use cases, stablecoins fall into two distinct categories when it comes to their legal classification: they are either subject to banking law or to collective investment scheme regulations. This distinction depends on the specific methodologies used to manage the underlying assets.

As stablecoin issuers assume the role of financial intermediaries, they inherit the obligation to comply with anti-money laundering (AML) regulations. This compliance includes the identity of holders and identifying beneficial owners to ensure the integrity of financial transactions.

In scenarios where stablecoin issuers opt to use bank guarantees as a means to circumvent the need for licensing, they must adhere to stringent requirements. These include ensuring that customers have individual claims against the guaranteeing bank in the event of the issuer's bankruptcy, guarantees that provide full coverage for public deposits and accrued interest, and easy access for customers to claim these guarantees when needed. Additionally, banks are limited to asserting only those defenses that are permitted by law.

3.1 Regulatory developments



Banks that extend these guarantees also face potential reputational risks. Should the issuers fail to meet their AML obligations, banks could be exposed to claims from fraudulent holders and bear the brunt of increased legal costs.

The Federal Council's report underscores the critical importance of preventing the misuse of default guarantee exceptions as a loophole to bypass licensing requirements. This measure is key to ensuring the stability of the financial market and the protection of its participants.

While the guidance provides clarity on how to interpret the applicable law for stablecoin projects, the industry did not agree with all of FINMA' interpretations. In particular, the Swiss Blockchain Federation expressed its concerns in a communication dated August 2024. The SBF highlights more stringent AML requirements compared to foreign jurisdictions, resulting in a regulatory framework that Hinders competitive business models in Switzerland versus abroad.

In conclusion, FINMA's guidance brings regulatory clarity to the industry. However, this may also lead to innovative new business ideas becoming more scrutinized.

How we can assist you regarding DLT regulations

- Navigate trends/developments in the regulatory landscape important for strategic decision-making
- Evaluate proposed activities against applicable laws/regulations
- Lend support during the license application process with the regulatory authority from an advisory or license application audit perspective
- Assess tokens against applicable regulations (i.e. FINMA ICO Guideline)
- Assist with compliance with DLT-specific regulatory requirements
- Assist in the selection, training and oversight of specific DLT service providers
- Educate Board, Management and/or other staff on DLT regulations

Romano Feuerstein
Director, Financial Services, Assurance and Regulations
KPMG Switzerland

+41 58 249 56 98
rfeuerstein@kpmg.com

3.2 Prudential treatment of crypto exposures

Current FINMA treatment of crypto exposure

Since 2018, FINMA has been one of the first national regulators to impose specific capital and liquidity requirements on cryptoassets. To date, FINMA has established its regulatory practice largely through bilateral letters and communications with affected banks and financial institutions. In October 2018, FINMA summarized these requirements in its letter to EXPERTsuisse's expert commission banking audit.

Risk-based capital requirements

For on-balance sheet cryptoassets, and to account for both market and credit risk from such assets, FINMA has imposed a risk-weight of 800% on the fair value of all unnetted long positions. It does not require banks and financial institutions to add a specific surcharge to account for operational risk.

For structured products, FINMA requires a risk weight of 700% on the net position as well as of 100% on the matched position per cryptoasset. For credit, settlement and operational risk, the treatment should be the same as for non-crypto-related products.

For derivative exposures with cryptoassets as underlyings, accepted approaches for determining capital requirements include conservative adjustments to established approaches for counterparty credit risk without recognition of netting. Likewise, established approaches without netting are used for market risk.

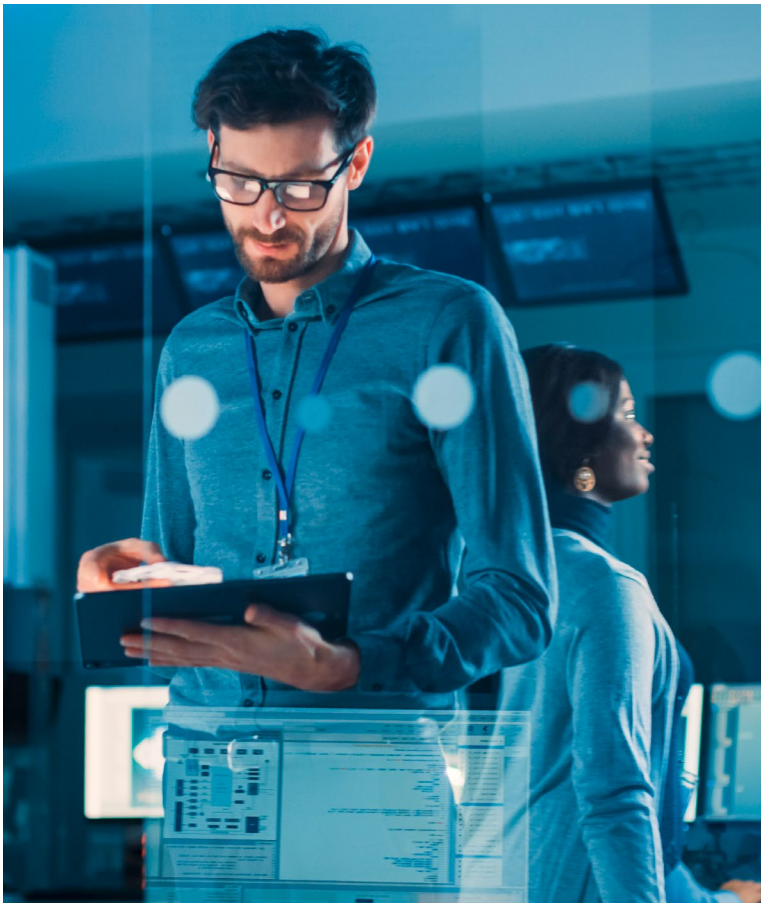
Large exposure

FINMA has highlighted an expectation of more stringent risk concentration rules for cryptoassets but has not yet enforced specific requirements.

FINMA requires supervised institutions to ensure appropriate internal limits.

Liquidity

FINMA has clarified with banks and financial institutions subject to quantitative liquidity requirements that cryptoassets may not be considered as High Quality Liquid Assets (HQLA) and that flows in or related to cryptoassets (e.g., via derivatives) may only be considered as outflows and not as inflows in the Liquidity Coverage Ratio (LCR).



3.2 Prudential treatment of crypto exposures

Upcoming BCBS prudential standards

In response to the potential risks that crypto exposures may pose to the financial stability and the banking system the BCBS has finalized its standards for the prudential treatment of exposures in this asset class in 2024, which are generally more conservative than the current FINMA treatment. The BCBS standards cover all pillars of the Basel Framework and are expected to be adopted by 1 January 2026.

Swiss financial market regulation has generally adopted BCBS standards consistently and comprehensively in the past. It should be noted, though, that several industry representatives have pointed out that a further strengthening of the regulatory approach could represent a fundamental change in the Swiss strategy regarding crypto assets. Regardless of whether the BCBS standards are fully or partially implemented, a consistent, national, and published set of regulatory requirements for the treatment of cryptoassets is needed.

For Group 1 cryptoassets, BCBS is considering an infrastructure risk add-on to Risk-Weighted Assets (RWA) based on observed weaknesses in the infrastructure on which the cryptoassets are based. The previously proposed fixed add-on of 2.5% of the exposure value for all Group 1 cryptoassets was removed from the final version of the prudential standard in favor of a more flexible treatment. This is intended to incentivize banks to actively address infrastructure vulnerabilities.

For Group 1b cryptoassets, a specific redemption risk test must be conducted to ensure that only stablecoins issued by regulated entities with robust redemption rights and governance are eligible.

Pillar 1 requirements

Given the diverse nature of cryptoassets and the variety of risks associated with them, the BCBS has established a classification system that defines the prudential treatment of cryptoassets for banks.

The classification system divides cryptoassets into two broad categories:

- Group 1 cryptoassets: tokenized assets (Group 1a) and cryptoassets with effective stabilization mechanisms (Group 1b).
- Group 2 cryptoassets: unbacked cryptoassets, tokenized traditional assets and stablecoins that do not meet the criteria associated with Group 1 cryptoassets. Group 2 is split into cryptoassets that meet (2a) or do not meet (2b) hedge recognition criteria.

Pillar 1 requirements

a) Risk-based capital

For Group 1 cryptoassets, banks can determine the necessary capital requirements based on the risk levels of the underlying assets according to the Basel Framework. However, they must also account for additional risks, such as risks associated with the infrastructure of such assets. Group 2 cryptoassets are subject to more stringent capital requirements. Group 2 is subject to a risk weight of 1250%, with Group 2a eligible for hedge recognition.

b) Leverage ratio

Cryptoassets are included in the exposure measure according to their value for financial reporting purposes.

c) Large exposure

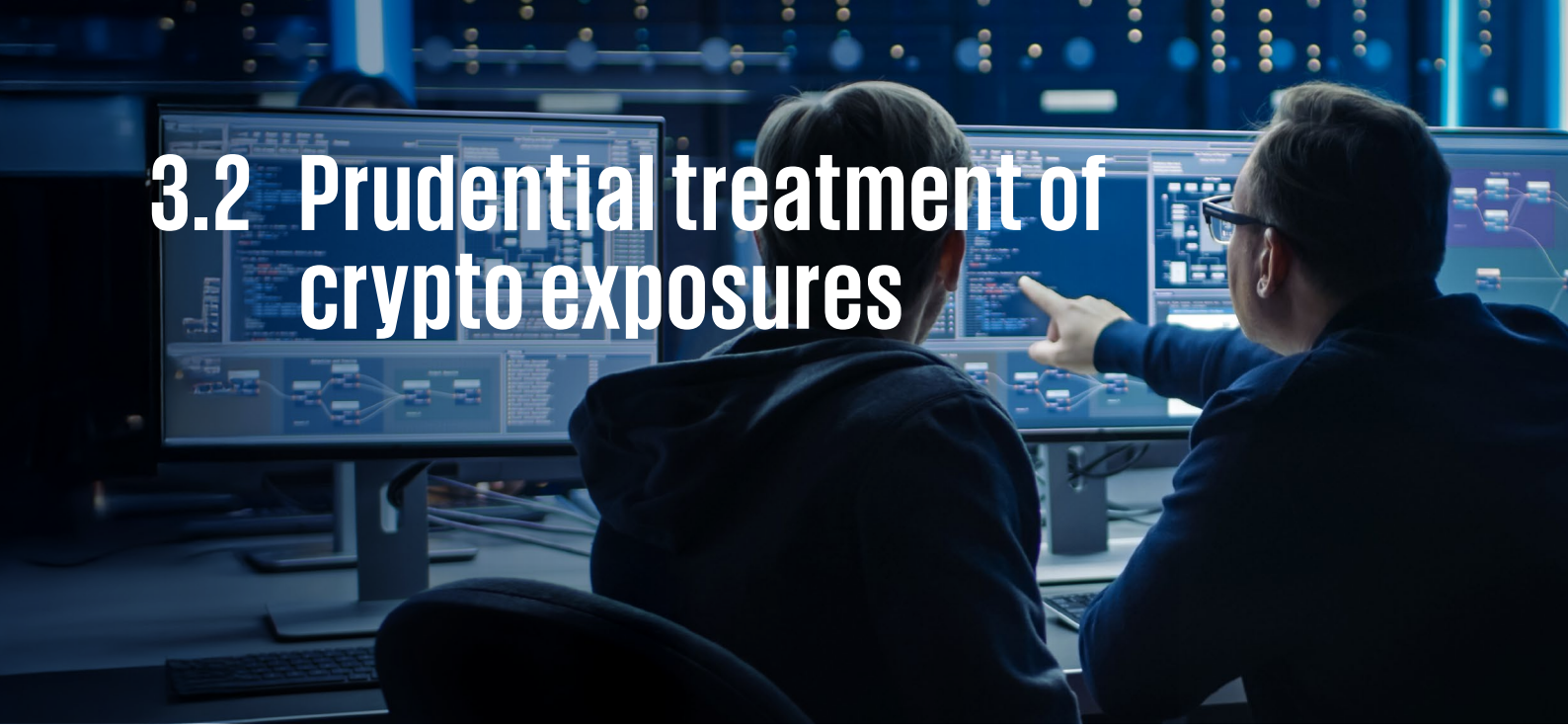
For Group 1 cryptoassets, banks are subject to the same exposure limits as in the large exposure standard. For Group 2 cryptoassets, dedicated limits apply.

d) Liquidity

Liquidity requirements for cryptoassets generally follow existing treatments for traditional exposures with similar risks – subject to potential adjustments. Group 1a cryptoassets with underlying assets qualifying as HQLA may also qualify as HQLA.

e) Asset class limit

Group 2 cryptoassets are subject to an asset class limit. Supervised institutions may not hold cryptoassets in excess of 2% of their Tier 1 capital. The regulator is already notified when cryptoassets reach 1% of Tier 1 capital.



3.2 Prudential treatment of crypto exposures

Pillar 2 requirements
Maintaining resilience to the direct and indirect risks associated with cryptoassets requires comprehensive risk management practices. Banks must develop and implement robust policies and procedures to continuously identify, assess and mitigate risks arising from cryptoasset exposures or related services.

Pillar 3 requirements
The BCBS disclosure principles also apply to banks' cryptoassets and cryptoliabilities. The qualitative and quantitative disclosure requirements include an overview of a bank's involvement in cryptoasset activities, the risks associated with these activities and how these risks are managed. In addition, banks are required to disclose material information on their cryptoasset exposures in three dedicated disclosure tables covering the following information:

a) Cryptoasset exposures and capital requirements;
b) Accounting classification of exposures to cryptoassets and cryptoliabilities; and.
c) Liquidity requirements for exposures to cryptoassets and cryptoliabilities.

How we can help you with the prudential treatment of your crypto exposures

- Navigate trends/developments in the regulatory landscape important for strategic decision-making
- Assist in compliance with crypto-specific regulatory requirements, especially including impact assessments as part of new business initiatives
- Evaluate the proposed activity against applicable laws/regulations
- Educate the Board, Management and/or other staff on crypto-specific regulations

Halvor Ruf
Director, Financial Services, Consulting
KPMG Switzerland

+41 79 561 68 57
hruf@kpmg.com

4 Tax Overview

4.1 Staking: Swiss Tax Implications for Financial Institutions

As Switzerland's financial sector increasingly embraces cryptocurrencies, even traditional financial institutions are entering the cryptoasset space. In 2024, several major Swiss banks expanded their banking services to offer custody and trading for cryptoassets. One of Switzerland's largest financial institutions started offering Bitcoin and Ethereum trading and storage through its e-banking and mobile platforms. This move reflects broader trend among some cantonal banks which also began offering cryptocurrency services.

Some Swiss financial institutions have gone even further, offering additional services such as staking – a move that represents another step towards adapting their product offerings to compete with popular trading platforms and keep their services attractive. However, this expansion of services also brings additional challenges, such as ensuring compliance with tax regulations. In this article, we aim to highlight some of the tax challenges associated with staking for financial institutions in Switzerland.

Recap: What is staking?

Staking means locking tokens for a certain period to help secure and support the operations of a Proof of Stake blockchain. Validators who contribute their tokens to this process receive rewards in return. Typically, this includes the so-called block reward (newly created units of the respective cryptocurrency or token) and/or a transaction fee.

In many cases, validators operate staking pools, while multiple participants, known as delegators, combine their tokens.

Joining a staking pool makes it easier to participate and earn rewards, even with a small number of tokens. Delegators entrust their tokens to a validator, who manages the staking process on their behalf. The rewards generated by the staking activities – which can be seen as a form of passive income – are then distributed to the delegators depending on how many tokens they contributed to the pool. This allows delegators to earn rewards without having to directly manage a validator node.

4.1 Staking: Swiss Tax Implications for Financial Institutions

Tax Implications of Staking for Individuals

For financial institutions offering staking services to their clients, it's crucial to understand the tax implications of staking for individuals. This knowledge is essential not only to answer client inquiries effectively but also to produce accurate tax reports.

Wealth tax

Cryptocurrencies, including those that are staked, are subject to wealth tax. At the end of the tax year, the value of staked tokens is considered part of the taxpayer's total assets. The wealth tax is then calculated based on the combined value of all assets, including the staked tokens. This means that even if the tokens are locked up and not immediately accessible, their value is still considered for wealth tax purposes.

Income tax

According to Swiss tax law, stakingrewards are not considered tax-free capital gains, but are generally considered taxable income from movable property. Staking rewards must be reported in the tax return at their market value at the time of receipt, converted into Swiss francs.

Attention: Under certain circumstances, the Swiss tax authorities may regard an individual's activity as self-employment. In this case, the earnings from staking, including rewards, would be taxed as income from self-employment and would be subject to social security contributions. Additionally, reclassifying staking activities as self-employment means that any future sale of cryptocurrencies or staking rewards will be subject to income tax.

How we can help you with DLT tax issues

- Clarify the correct VAT treatment and data requirements for all banking services around cryptoassets (custody, trading, staking etc.)
- Assist with the issuance of tokens (Profit tax, Withholding tax, Stamp transfer tax, VAT)
- Assist with the qualification of tokens for Swiss tax purposes
- Assess whether transactions involving cryptoassets are subject to stamp transfer tax or withholding tax
- Provide solutions with regard to cryptoassets / transactions tax reporting & account statements
- Evaluate tax treatment of investments in cryptoassets by individuals
- Support the readiness for information exchanges on cryptoassets
- Provide tax support for the establishment of crypto funds

Sabrina Leutert
Senior Manager,
Financial Services, Tax
KPMG Switzerland

+41 58 249 53 99
sleutert@kpmg.com

Thomas Brotzer
Partner, Financial Services, Tax
KPMG Switzerland

+41 58 249 21 00
tbrotzer@kpmg.com

4.1 Staking: Swiss Tax Implications for Financial Institutions

Tax Implications of Staking for Financial Institutions

For financial institutions involved in staking, the tax situation becomes more complex. In this section, we'll look at various tax areas, such as direct taxes, Swiss value added tax ("VAT"), Swiss withholding tax ("WHT") and Swiss stamp transfer tax ("SSTT"), explaining how each one applies to staking activities. Financial institutions need to be aware of how each tax affects them.

Direct taxes

In Switzerland, the tax treatment must generally follow the accounting treatment ("Massgeblichkeitsprinzip"), which is based on the rules of the Swiss Code of Obligations and the accounting rules for banks. No separate tax accounts need to be prepared, but there are some tax adjustments that need to be considered in the tax return.

Staking rewards (when staking for own benefit) are considered part of the business income, so they need to be included in the overall profit. Staking rewards are typically initially recorded at their fair market value at the time they are received. Any fees charged to clients for the provision of the staking service (delegated staking) are also considered part of the business income. Businesses can reduce their taxable income by deducting expenses related to staking if these are commercially justified.

Swiss VAT

VAT is arguably the most complex tax when it comes to staking activities. The treatment of staking rewards therefore requires careful consideration. However, it helps that the Swiss Federal Court ruled on a significant case in 2023 that clarified some of the open questions regarding the VAT treatment of staking activities.

The VAT treatment of staking services provided by a financial institution to its customers varies depending on the specific design of the service offering. Due to the complexity of VAT legislation and practice and the different VAT treatments depending on contract structures and blockchain protocols, only a general overview is provided below. This should not be considered a complete or directly applicable guide, as the actual VAT treatment may differ based on specific circumstances and requires an individual analysis in each case.

a) Financial Institution acts as the Validator itself

A customer can stake their assets on a validator node managed by the financial institution. From a VAT perspective, the financial institution acts as the service provider (validator) to the protocol, so it is generally entitled to the total amount of rewards distributed by the protocol for validation services. This can lead to challenges, depending on how the transactions are recorded in the books, as staking fees may either be billed off-chain or directly deducted from the staking rewards on-chain, depending on the blockchain's protocol.

Validation itself – the creating of new blocks and the "packaging" of transactions – is considered a taxable electronic service. The way the service is provided depends on the consensus mechanism used by the protocol, and whether it is considered a collective entity (e.g. DAO) or a protocol organization. If the recipient of the service is identifiable, there is a service relationship, and the payment is subject to Swiss VAT if the recipient is located in Switzerland/Liechtenstein. If the protocol doesn't clearly identify the recipient, such as in cases where no specific organization controls the protocol, the Swiss Federal Tax Administration ("SFTA") may classify the rewards as non-remuneration ("Nicht-Entgelt").

4.1 Staking: Swiss Tax Implications for Financial Institutions

If the validator receives a transaction fee, there is a taxable service relationship between the validator and the initiator of the transaction. The transaction fee is subject to VAT if the initiator is located in Switzerland/Liechtenstein. This creates challenges, as the validator often does not know the identity of the transaction initiator.

Finally, when part of the reward is passed on by the financial institution to the delegators, it may not be deducted from the gross amount. The SFTA may consider this as a separate service provided by the client to the validator, triggering Swiss input VAT or Swiss reverse charge VAT consequences at the level of the validator.

b) Staking services are provided via third-party validator

The financial institution collaborates with third-party validators. Customers may stake their tokens directly to the third-party while using the financial institution's platform, whereas assets are not moved out of the institution's wallets. The tax treatment depends on the specific protocols, agreements with the third parties or customers and the external representation. There may be a three-party relationship with two service relationships, or the delegator may provide a taxable service directly to the validator. This can be very complex because the way it is recorded in the accounts often doesn't match the way it needs to be treated for VAT purposes.

Swiss withholding tax ("WHT")

Swiss withholding tax generally does not apply to staking rewards, as they are generated by blockchain networks. Swiss withholding tax itypically applies to income such as dividends and interest paid by Swiss entities, which does not include staking rewards.

However, for cross-border staking activities, Swiss residents should be aware of potential international tax responsibilities, especially with increased global tax transparency initiatives such as the OECD's Crypto-Asset Reporting Framework. Although Switzerland doesn't impose WHT on staking rewards, residents are required to declare these rewards on their tax returns to ensure compliance and avoid penalties.

Swiss stamp transfer tax ("SSTT")

For Swiss stamp tax purposes, a company domiciled in Switzerland qualifies as a securities dealer if its assets consist of more than CHF 10 million in taxable securities or if its activity consists exclusively or to a significant extent of trading taxable securities.

In general, staking is not subject to Swiss stamp transfer tax. However, financial institutions holding cryptocurrencies must be cautious about qualifying as securities dealers for SSTT purposes. Where cryptoassets are considered securities for SSTT purposes, then an SSTT will apply on the trading of such tokens. Therefore, it's crucial for financial institutions to evaluate whether their cryptoassets fall within this category.

Conclusion

It's exciting to see more and more Swiss banks and other financial institutions entering the world of cryptoassets, blending traditional finance with new technologies.

As this trend continues, it will be interesting to see how the tax rules will adapt to support this growth while remaining in line with global standards.

It feels like we're just at the beginning of what could be a fascinating journey for cryptoassets in Switzerland and beyond.

4.2 Outlook CARF

CARF: tax transparency for crypto-assets

Background on CARF

In 2014 the OECD first published the Common Reporting Standard ("CRS") for an Automatic Exchange of Information in Tax Matters ("AEoI"). In Switzerland, the AEoI has been in place since 2017. Since then, Crypto-Asset have largely developed as a new asset class. At the same time, they have created new ways for taxpayers to hide their income and assets from the view of tax authorities.

As the CRS was written with traditional financial institutions and assets in mind, cryptoassets have in most cases been outside the scope of CRS. To keep up with the fast development of the crypto world and to address the tax evasion and avoidance risks created by the increased use of cryptoassets, the OECD has published the Crypto-Asset Reporting Framework ("CARF"), alongside a comprehensive revision of the CRS.

Currently more than 60 jurisdictions (incl. Switzerland and, from 2027, the USA) have committed to implementing CARF. The Swiss Federal Council has published draft legislation that is expected to become effective from 1 January 2026, so the first exchange of data can take place in June 2027. In the following we provide a selection of the most relevant new rules and what affected entities can do to prepare.

Wide definition of "Crypto-Asset"

Building on the same principles as the CRS, CARF introduces extensive due diligence and reporting obligations for Reporting Crypto-Asset Service Providers ("RCASP").

An RCASP is any individual or entity that, as a business, provides the service of executing crypto-asset exchange transactions for or on behalf of customers, including by acting as a counterparty, or as an intermediary or by making available a crypto-asset trading platform. The term therefore covers most crypto-asset brokers, dealers, custodial wallet providers, Crypto ATMs, exchange service providers and potentially also banks (as outlined further below).

The term crypto-asset is broadly defined to include any digital representation of value that relies on a cryptographically secured distributed ledger or similar technology to validate and secure transactions. In this context, a "digital representation of value" means that a Crypto-Asset must represent a right to value which can be traded or transferred to others in a digital manner.

Broad definition of "Crypto-Asset"

The following exemptions are foreseen, which are not considered relevant cryptoassets and are therefore not reportable:

a) Central Bank Digital Currencies and Specified Electronic Money Products (both will be reportable under the amended CRS and are therefore excluded under CARF to avoid double reporting); and

4.2 Outlook CARF

b) cryptoassets that cannot be used for payment or investment purposes (i.e. certain cryptoassets that can only be exchanged or redeemed within a fixed network or environment for specified goods and services, such as tokens for food, books, travel, restaurant vouchers, digital music, games, etc.).

It is important to note that the term RCASP hinges on the definition of a crypto-asset. The broad definition of a crypto-asset means that the term will not only cover cryptocurrencies such as Bitcoin, Ethereum, etc. but also digital bonds/ warrants/futures, tokenized precious metals or other cryptoassets, as long as they can be transferred via a distributed ledger technology.

The above means that CARF will not only concern crypto-asset brokers, dealers, and exchange service providers. Also, a bank may be considered an RCASP if the bank offers any of the above-mentioned products to its customers. Offering one in-scope product is sufficient and the bank would need to implement adequate systems, policies and procedures to comply with the CARF due diligence and reporting obligations from 1 January 2026. Swiss banks should therefore make good use of 2025 to perform a detailed analysis of their product offering to determine whether any of them are seen as relevant cryptoassets that would make the bank an RCASP from 2026.

Extensive Due Diligence requirements

Very similar to the rules for Financial Institutions ("FI") under CRS, CARF requires that RCASPs perform due diligence procedures so as to identify any of their customers that are reportable crypto-asset users, i.e. clients that are resident in a CARF reportable jurisdiction. As part of these due diligence procedures, RCASPs need to:

- For individual users: obtain a self-certification from each crypto-asset User, stating the user's residence for tax purposes;
- For users that are entities: obtain a self-certification from the crypto-asset user, stating the entity's status and residence for tax purposes, and the entity's Controlling Persons (except where the entity is an Active Entity or an Excluded Person such as a Financial Institution);
- Confirm the reasonableness of such self-certification based on the information obtained by the Reporting Crypto-Asset Service Provider, including any documentation collected pursuant to AML/KYC Procedures.

An RCASP that is also an FI under CRS will largely be able to rely on the self-certifications already obtained for CRS purposes. However, the following important differences should be noted:

- CARF requires a look-through to the Controlling Persons of all entities that are Passive NFEs or Professionally Managed Investment Entities ("PMIE") (under CRS this is only required for Passive NFEs and PMIE in a Non-Partner Jurisdiction).
- Unlike CRS, CARF requires a self-certification from all clients, including pre-existing crypto-asset users (an electronic indicia search is not sufficient under CARF). For pre-existing crypto-asset users, RCASPs are given one year to obtain a self-certification.

RCASPs will need to ensure that they obtain the required self-certifications from their new and pre-existing customers in time. Entities that are already FIs under CRS (such as banks) should perform an analysis of their customer base with regards to the above. Specifically, these entities must ensure that they obtain a self-certification from all controlling persons of PMIEs and from any pre-existing crypto-asset users by 31 December 2026.

4.2 Outlook CARF

Transaction-based reporting requirements will bring new challenges

Starting from 2027, RCASPs will be required to annually report certain information with respect to their crypto-asset users (incl. name, address, jurisdiction(s) of tax residence, TIN, date and place of birth, type of entity and details of controlling persons of certain entities). This contrasts with CRS, which requires reporting of year-end balances and certain payments.

CARF will require reporting of the aggregate fair market value of outward and inward crypto-asset rransactions, number of units and number of relevant transactions, separated by transaction and type of crypto-asset. Specifically, RCASPs will need to report:

- The aggregate gross amount paid/received, the aggregate number of units and the number of relevant transactions with respect to acquisitions/disposals of relevant cryptoassets;
- The aggregate fair market value, the aggregate number of units and the number of Reportable Retail Payment Transactions;
- The aggregate fair market value, the aggregate number of units and the number of relevant transactions, subdivided by transfer type (where known by the RCASP).

These new transaction-based reporting requirements will pose significant challenges for IT systems. RCASPs that have not been FIs under CRS so far will need to implement a new appropriate reporting infrastructure. Entities that have already been FIs under CRS (such as banks) will only be able to leverage their existing CRS reporting systems to a limited extent and will need to review and amend their infrastructure to ensure it captures and reports the data required under CARF.

How we can assist you with CARF

- Conduct an impact assessment to determine whether an entity (e.g. a bank) is a Reporting Crypto-Asset Service Provider based on its product offering
- Provide support with implementing a CARF operating model, incl. due diligence and reporting processes
- Draft CARF policies & procedures setting out an RCASP's due diligence, reporting and compliance obligations under CARF
- Provide training tailored to different audiences (e.g. board members/executive management, CARF SMEs, etc.)
- Provide hotline support for any CARF-related technical questions as and when required

Stefan Keglmaier
Senior Manager, Tax & Legal, Banking
KPMG Switzerland

+41 58 249 7861
stefankeglmaier1@kpmg.com

5 Innovation in Audit

5.1 Innovation in Audit

DLT in Audit: Revolutionizing Assurance Services with Cutting-Edge Technology

DLT's technical aspects

DLT refers to a digital system for recording information (i.e. the transaction of assets) in which the transactions and their details are recorded in multiple places at the same time. Unlike traditional databases, DLT has no central data storage or administration functionality. This innovative technology is the backbone of various transformative applications, including:

- Cryptocurrencies such as Bitcoin, Ethereum and Solana
- Central Bank Digital Currencies (CBDCs), representing digitized fiat currencies issued by central banks
- Tokenized assets encompassing equity, debt or property rights
- Diverse use cases in identity verification, logistics, geodata tracking and secure communication

The inherent strengths of DLT – decentralization, transparency, security, and immutability – offer significant potential to improve the operational efficiency, reliability and trustworthiness of a wide variety of systems. For auditors, it is imperative to understand the complexities of DLT so as to fully assess its impact on clients' operations and to tailor audit procedures that ensure robust and reliable audit evidence, ultimately leading to well-founded audit opinions.

Focus on cryptocurrencies: identifying & addressing audit risks

In the realm of financial statement audits, the emergence of cryptocurrencies requires a bespoke approach to risk assessment.

Auditors must delve deeply into the unique business activities, operational frameworks and protocols of clients engaged in the cryptocurrency market. The spectrum of cryptocurrency-related services is broad and includes, but is not limited to the following:

- Custodial services for the secure management of private keys
- Payment services facilitating on-chain transactions and other payment solutions
- Decentralized finance (DeFi) offerings, such as staking, liquidity provision and decentralized lending

Each service category carries its own set of risks and complexities, requiring auditors to have specialized technical knowledge and an understanding of the required infrastructure. A detailed analysis of these services uncovers a range of risks in cybersecurity, data integrity, operational efficiency and governance. Auditors must deploy sophisticated responses, including general IT controls testing, IT application controls and software audit tools, tailored to the client's internal control framework and automation level.

5.1 Innovation in Audit

a) Custody Services Risks

- Cybersecurity Risk: the risk of unauthorized access to the cryptoassets is paramount. This includes both external threats from hackers and internal threats from potentially malicious employees. Robust security protocols and regular security audits are essential to mitigate this risk.
- Data Integrity Risk: the risk that the data will be tampered with or corrupted, either intentionally or accidentally. This requires the implementation of stringent controls to ensure data integrity at all times.
- Availability Risk: the risk that clients' assets may not be accessible when needed due to technical issues or system failures. This requires a comprehensive disaster recovery and business continuity plan to ensure asset availability.
- Operational Risk: the risk of loss resulting from inadequate or failed internal processes, people or systems. This requires a clear segregation of duties and process automation to reduce human error.
- Governance Risk: the risk associated with the lack of a proper governance framework to oversee the custody operations. This requires ensuring compliance with regulatory requirements and implementing best practices for asset custody.

b) Payment Services Risks

- Regulatory Risk: the risk of non-compliance with rapidly evolving regulations governing blockchain transactions. Staying abreast of regulatory changes and ensuring compliance is critical.
- Anti-money laundering (AML) risk: the risk of facilitating illegal money transfers. Crypto payment services must have robust AML procedures in place to detect and prevent such activities.
- Settlement risk: the risk associated with the finality of transactions and the reconciliation between blockchain records and the general ledger. Ensuring accurate and timely settlement is crucial.
- Revenue recognition risk: the risk of inaccurately recognizing revenue, especially when transaction fees or rewards are involved. This includes accounting for transaction fees such as gas fees on the Ethereum network.
- Right of disposal risk: the risk that the customer does not have the necessary access to private keys to perform transactions, which could lead to disputes or loss of assets.

5.1 Innovation in Audit

c) Distributed Finance (DeFi) Services Risks

- Smart contract risk: the risk of flaws or vulnerabilities in smart contract code, which could be exploited, leading to loss of funds.
- Protocol risk: the risk associated with the underlying protocol of DeFi services, including potential for systemic failures or attacks.
- Liquidity risk: the risk that a particular asset may not be easily convertible to cash without significant loss in value, especially in volatile market conditions.
- Compliance risk: the risk of failing to adhere to legal and regulatory standards, which can be particularly challenging given the decentralized nature of DeFi services.
- Counterparty risk: the risk that the other party in a transaction may default on their obligations, which is higher in a decentralized environment where counterparties are often anonymous.

KPMG Chain Fusion: Pioneering Audit Technology for DLT

- In anticipation of the unique risks posed by DLT, KPMG has developed KPMG Chain Fusion, a state-of-the-art software audit tool designed to extract information directly from blockchains, thereby enabling automated and efficient audit procedures. KPMG Chain Fusion offers a suite of functionalities that address critical audit concerns, such as confirming the existence of assets, verifying transaction details, verifying wallet ownership, assessing token supply, evaluating liquidity pool balances, and assisting in the accurate valuation of digital asset holdings.
- The tool's design requires minimal client input, relies on publicly available yet pseudonymized data and is equipped with bulk upload features to streamline the audit process. KPMG Chain Fusion currently supports over 60% of the top 100 cryptocurrencies, with plans for continued expansion.

How we can assist you in DLT-related audit engagements

- Support you with a state-of-the-art audit approach by the use of software audit tools
- Leverage the new technologies to increase efficiencies and minimize manual audit procedures
- Act as a sparring partner and bring a broad industry know-how into the discussion
- Provide two-way communication including valuable insights gained throughout the audit
- Tailor our audit approach to your needs as a startup or as a global company by accessing our international network
- Help you navigate DLT complexities and the application of new required audit procedures

Romano Feuerstein
Director, Financial Services, Assurance and Regulations
KPMG Switzerland

+41 58 249 56 98
rfeuerstein@kpmg.com

6 Your Contacts

Our Swiss team of DLT experts is always available for you

KPMG AG
Badenerstrasse 172
PO Box
CH-8036 Zurich

Romano Feuerstein
Director, Financial Services,
Assurance and Regulations
KPMG Switzerland

+41 58 249 56 98
rfeuerstein@kpmg.com

Petrik Leutert
Director, Financial Services,
Accounting and Assurance
KPMG Switzerland

+41 58 249 42 07
pleutert@kpmg.com

Sabrina Leutert
Senior Manager,
Financial Services, Tax
KPMG Switzerland

+41 58 249 53 99
sleutert@kpmg.com

Halvor Ruf
Director, Financial Services,
Consulting
KPMG Switzerland

+41 79 561 68 57
hruf@kpmg.com

kpmg.ch