BLOCKCHAIN

TÜRKİYE

CRYPTO ASSET STORAGE REPORT

Crypto Service Providers Working Group

MARCH 2025

TURKEY INFORMATION TECHNOLOGY FOUNDATION

BLOCKCHAIN
TÜRKİYE

CRYPTO ASSET STORAGE
REPORT

Crypto Service Providers Working Group

TURKEY INFORMATION TECHNOLOGY FOUNDATION

CRYPTO ASSET STORAGE
REPORT

MARCH 2025

DISCLAIMER

This report, prepared by the "Crypto Service Providers Working Group" of the Blockchain Turkey Platform operating under the Turkish Informatics Foundation, consists of an examination of blockchain technology in terms of current personal data protection legislation and practices; it has been published for the purpose of understanding the legal aspects of the technology It does not constitute binding advice or opinion for individuals or institutions. This report contains information obtained from publicly available sources, and the accuracy or completeness of such information is not guaranteed. All information and opinions provided in this report are subject to change over time. In this context, the author assumes no responsibility or liability to readers of this report or any third party.

Kripto Hizmet Sağlayıcıları
Çalışma Grubu

FOREWORD

Digital assets and their storage have become one of the most dynamic and critical components of the financial world, especially in recent years. Technological advances, the proliferation of blockchain-based assets, and the need for integration between traditional financial systems and the digital ecosystem have made the secure storage of digital assets more important than ever. In this context, this comprehensive report, prepared by the Crypto Service Providers Working Group, addresses the latest developments in the sector, regulatory dynamics, and projections for the future.

Globally, digital asset custody services have begun to play a critical role for the financial sector, with major financial institutions and technology companies making significant investments in this area. Regulations are becoming clearer in various regions of the world, the legal status of digital assets is becoming more defined, and a safer environment is being created for institutional investors. Different countries have adopted various technical and legal approaches for digital asset custody solutions. This diversity provides an important picture of how the global digital asset ecosystem is taking shape.

Interest in digital assets and custody services is also growing in our country. In recent years, significant regulatory measures have been implemented for crypto asset service providers, and the framework for digital asset custody services has become clearer. The new regulations cover the definition of crypto assets, the licensing of digital asset custody institutions, and secure custody standards.
The regulations issued in this area in Turkey ensure that digital asset custody services become more reliable, while also contributing to the sector's growth within a legal framework.

This report is the first of its kind on digital asset custody and is the most comprehensive study in the sector, covering technical infrastructure, legal regulations, and examples from around the world. Our study also provides a comprehensive examination of the different technologies used in custody services. Various approaches have been evaluated, ranging from cold storage and hot storage solutions to advanced security technologies such as multi-signature and MPC (multi-party computation). These innovative solutions adopted to ensure security in digital asset storage are transforming the methods investors and financial institutions use to protect their assets.

All these developments have led to digital assets being viewed not only as an investment vehicle but also as an integral part of financial systems. As the transition between traditional financial institutions and decentralized finance applications accelerates, collaboration between regulatory bodies and market actors has become inevitable. Technical developments and legal regulations concerning digital asset custody form the most important building blocks of this transformation process.

This report aims to provide valuable guidance to industry leaders, regulators, and investors by thoroughly examining the current local and global landscape, risks, and legal framework in the field of digital asset custody. With the advancement of technology and regulations, the secure custody of digital assets will become an integral part of the financial ecosystem.

I invite you to enjoy reading our report, which contains the latest information and analysis in this field.

Yasin Oral
Founder and CEO of Paribu

ABBREVIATION LIST

- MPC - Multi-Party Computation
- Multi-sig - Multi-signature
- HSM - Hardware Security Modules
- SGX - Software Guard Extensions
- AML - Anti-Money Laundering
- CFT - Countering the Financing of Terrorism
- KYC - Know Your Customer
- HTTPS - Secure Hypertext Transfer Protocol
- PGP - Pretty Good Privacy
- ECDLP - Elliptic Curve Discrete Logarithm Problem
- EdDSA - Edwards-Curve Digital Signature Algorithm
- IoT - Internet of Things
- NIST - National Institute of Standards and Technology
- FIPS - Federal Information Processing Standard
- SHA - Secure Hash Algorithms
- SHAKE - Scalable Output Functions
- TSS - Multiparty Signing Algorithm
- DSA - Digital Signature Algorithm
- ZK - Zero-Knowledge Proof
- TRNG - True Random Number Generators
- RBAC - Role-Based Access Control
- DeFi - Decentralized Finance
- RWA - Tokenization of Real-World Assets
- ETF - Exchange-Traded Fund
- CBDC - Central Bank Digital Currency
- DLT - Distributed Ledger Technology
- IMF - International Monetary Fund
- FATF - Financial Action Task Force
- IOSCO - International Organization of Securities Commissions
- TradFi - Traditional Finance
- SPK - Capital Markets Board
- MASAK - Financial Crimes Investigation Board
- BDDK - Banking Regulation and Supervision Agency
- SerPK - Capital Markets Law
- MiCA - European Union Crypto Asset Legislation
- CASP - Crypto Asset Service Provider
- FINMA - Swiss Financial Markets Supervisory Authority
- FCA - Financial Conduct Authority
- BaFin - German Federal Financial Supervisory Authority
- KWG - German Banking Act
- FIU - German Financial Intelligence Unit
- VARA - Virtual Assets Regulation Authority, Dubai Virtual Assets Regulatory Authority
- ICO - Initial Coin Offering
- SEC - Securities and Exchange Commission, U.S. Securities and Exchange Commission
- CFTC - U.S. Commodity Futures Trading Commission
- SSS - Shamir's Secret Sharing
- DDoS - Denial of Service
- Pen-Test - Penetration Test
- MFA - Multi-Factor Authentication
- SAR - Suspicious Activity Reporting
- STR - Suspicious Transaction Reporting
- TÜBİTAK - Scientific and Technological Research Council of Turkey
- SOC - Security Operations Center
- ISAE - International Standards on Assurance Engagements
- ISO - International Organization for Standardization
- CCSS - Common Core State Standards
- PoR - Proof of Reserve
- PoL - Proof of Liability
- AUC - Assets Under Custody
- ML - Machine Learning
- AI - Artificial Intelligence
- DAO - Decentralized Autonomous Organizations
- RegTech - Regulatory Technology

CONTENTS

CRYPTO ASSET STORAGE REPORT

A.

The Concept of Storage

Custody services ensure the security and integrity of the financial system by safeguarding investors' assets. Investors are provided with both accessibility and liquidity through the professional management of their assets. Furthermore, compliance with regulatory requirements ensures that investors are protected within the legal framework and guarantees that processes are conducted transparently.
In our country, during a period when legal regulations for crypto assets are gaining momentum, the legal framework for crypto assets has also become clearer with the publication and entry into force of Law No. 7518 on Amendments to the Capital Markets Law in the Official Gazette. This regulation strengthens the legal steps taken to protect investors' crypto assets and ensures that crypto assets are now subject to legal protection just like traditional assets. Today, with the increasing importance of both crypto assets and traditional digital assets, the role of custody services has also become increasingly critical. Custody services not only ensure asset security but also minimize investors' risks through advanced infrastructures and technologies, thereby supporting long-term capital growth potential. With the adoption of digital assets and the increase in institutional demand, the requirements for custody services in terms of professionalism, scalability, and security have also significantly increased.

e Custody in Traditional Finance

In traditional financial systems, custody services are a critical service that enables investors to securely store and manage their securities, cash, and other financial assets.

These services, provided by banks, investment firms, or independent custodial institutions, include important functions such as recording investors' assets, managing settlement and reconciliation processes, and ensuring the payment of dividends and interest. In this context, Takasbank plays a central role in custody and settlement services in Turkey. Takasbank is an important clearing and custody institution established for the purpose of clearing securities and futures and options contracts in Turkey. It contributes to the development of capital markets in Turkey and enables financial transactions to be carried out safely and efficiently. Takasbank securely clears a wide range of financial instruments, including stocks, bonds, government bonds, corporate bonds, repo and reverse repo transactions, futures and options contracts. These clearing operations are conducted by establishing a secure bridge between buyers and sellers, thereby contributing to the stability of the financial system.
Takasbank also provides securities custody services, ensuring the physical protection and transfer of these securities. Today, these transactions are carried out electronically thanks to modern technology, and investors' securities are stored securely.

The operation of custody and clearing services enables investors to trade safely and efficiently in capital markets. These services not only safeguard investors' securities but also increase market liquidity by streamlining transaction processes. Institutions such as Takasbank reduce the operational burden on investors and increase the reliability of the financial system while providing custody and transfer of securities.

Functions of Custody Services

1. Recording and Tracking of Assets:
Custodian institutions record all assets in investors' portfolios and track their current values. The recording of securities and other financial assets safeguards investors' ownership rights. Furthermore, these records can be used as legal evidence in the event of any dispute regarding the ownership of assets. Securities and cash-like assets in investors' portfolios are continuously updated and valued.

2. Settlement and Reconciliation Transactions:
Custody services ensure that asset settlement transactions are carried out smoothly. Securities or cash transfers are executed through a settlement system within defined rules. For example, in stock trading, custody service providers act as a secure bridge between the buyer and seller throughout the settlement process, ensuring the transaction is completed. Similarly, reconciliation processes are also performed by custody service providers, which means that the parties reach an agreement and the transactions are verified. These processes increase liquidity in the financial system and ensure trust among market participants.

3. Dividend and Interest Payments:
Custodian institutions regularly track dividend and interest payments earned by investors from their securities and transfer them to investors' accounts. This service ensures that investors receive their passive income smoothly and guarantees that these payments are made on time. Dividend payments are particularly critical for stockholders, while interest payments are crucial for bondholders.
Custody service providers reduce investors' operational burden by ensuring these revenues are transferred to accounts correctly and on time.

4. Account Management and Reporting:
Custody service providers offer detailed account management and reporting services by monitoring investors' assets. These reports regularly show investors changes in their portfolios, gains, dividends, and interest payments. Reporting services help investors make healthier portfolio management decisions. Thanks to these reports, investors can see how much profit they have made from which assets and which of their assets have lost value.

Traditional Custody Service Providers

In traditional financial systems, custody services are typically provided by three main institutions:

1. Banks:
Banks offer comprehensive infrastructure to securely store investors' cash and securities. Major banks provide extensive custody services for investors operating in national and international markets. Banks contribute to the creation of a secure financial environment through the custody
services they offer to their customers, they also contribute to the creation of a secure financial environment.

2. Investment Firms:
Investment firms provide custody services, particularly for large investment funds and asset management companies. These firms securely store assets and execute settlement transactions during the portfolio management process for investors. Investment firms also support portfolio management by providing investors with various financial analyses.

3. Independent Custody Institutions:
Independent custodial institutions are private companies that operate independently of banks or investment firms and provide solely custodial services.

These institutions provide impartiality and independence for investors. Independent custodial institutions are often preferred by large fund managers or international investors because they ensure the secure custody of securities and manage transactions transparently.

e Custody in the Crypto Asset Sector

In the crypto asset sector, custody refers to services that enable the secure storage and management of crypto assets. These services include the secure storage of private keys, the tracking of assets on a ledger, the secure execution of transfer transactions, and providing investors with fast and easy access to their assets. Crypto custody services aim to minimize the risk of digital assets being lost or stolen through methods such as cybersecurity measures and multi-signature technologies. As in traditional finance, they provide investors with legal assurance and transparency by complying with regulatory requirements. As the crypto asset sector continues to grow rapidly, the secure storage and management of these digital assets is critically important. Crypto asset custody services are indispensable, especially for large-scale investors and institutions, to ensure the security of their assets and protect them against cyber threats. Protecting crypto assets is one of the greatest security challenges of the digital age. This challenge is particularly significant given that cryptocurrencies are based on irreversible transactions. For example, the loss or theft of a private key can result in the irreversible loss of assets.

The Importance of Storage Services and the Benefits of

Custody services play a critical role for investors by providing security, liquidity, and professional management for both traditional financial assets and crypto assets. These services minimize the risk of theft, loss, or damage to assets, ensuring that investors can store their assets in a secure environment. With the proliferation of digital assets, the importance and scope of custody services are increasing. With the introduction of regulations, these services are being developed to meet specific security standards and enable investors to manage their assets professionally. Crypto asset custody services aim to reduce the risk of investors' assets being lost or stolen by ensuring that digital assets are stored in a secure environment. Storage on devices that are not connected to the internet, such as cold wallets, prevents assets from being exposed to online attacks, while hot wallets offer the advantage of fast transactions. These two storage methods are used by institutions and individual users in different scenarios, depending on the balance between risk and speed.

One of the most fundamental components of crypto asset custody services is the secure storage of private keys. A private key is a digital key that grants an investor access to their wallet and provides full control over their assets. If this key is compromised, malicious individuals may transfer or steal the assets. Storage services use advanced encryption technologies, multi-signature (Multisig), and multi-party computation (MPC) methods to ensure the security of private keys. Multisig provides a structure where multiple keys are required to approve a transaction, while MPC distributes the private key among multiple parties, preventing any single individual from gaining control of the key.

Compliance of crypto custody services with regulatory frameworks helps investors protect their assets in a secure environment. This compliance not only provides security for investors but also brings transparency and accountability obligations. Standards such as KYC (Know Your Customer) and AML (Anti-Money Laundering) require crypto asset custody service providers to verify customer information and take measures against illegal activities.

However, the cybersecurity measures of crypto asset custody services are also of great importance as part of legal requirements.
In the event that investors' digital assets are stolen or lost, insurance policies and recovery mechanisms offered by custody service providers can help compensate investors for their losses.

c Mechanisms Required for Storage

Today, the security of digital data is one of the most critical issues in the world of information technology. Various cryptographic mechanisms are used to ensure the secure transmission, storage, and protection of information from unauthorized access. Cryptography is essential for the secure storage, monitoring, and management of digital assets. This section will discuss the most widely used and critical cryptographic mechanisms in the modern digital world.

Public Key (Asymmetric) Encryption

Today, many different encryption methods with various algorithms are used to ensure the secure transmission, storage, and confidentiality of data. These encryption methods can be divided into two categories: symmetric and asymmetric (public key).

Symmetric encryption is a method where the same key is used for both encryption and decryption, and this structure has certain advantages and disadvantages. While it can be advantageous for encrypting large data sets due to its fast and efficient operation, using the same key for encryption and decryption can create a security vulnerability. If unauthorized individuals or systems obtain the key of the recipient or sender, a security breach may occur. In this case, encrypted data may be compromised. Asymmetric encryption, unlike symmetric encryption, uses two different keys. One key is the public key used to encrypt the data, and the other is the private key used to decrypt it. This encryption method provides greater security, and while the public key can be distributed, the private key remains only with the owner. Asymmetric encryption also allows the sender's identity to be verified through digital signatures, ensuring that only authorized individuals have access to the data.

Asymmetric encryption is a fundamental technology for ensuring privacy and security in today's digital communications. This encryption method allows users to securely share confidential information and uses two keys to accomplish this: a public key and a private key.

Public and Private Keys

Public-key cryptography systems are based on a structure where two different keys complement each other. These keys are mathematically linked, but it is practically impossible to derive one key from the other. One of these keys (the public key) is shared with everyone, while the other (the private key) is kept secret.

• Public Key: Can be used by anyone, and messages encrypted with this key can only be decrypted by the corresponding private key.

This allows a person to receive messages securely; the sender encrypts the message using the recipient's public key, but only the recipient can decrypt it.

• Private key: This key belongs solely to its owner and is not shared with others. This key is used to decrypt messages encrypted with the public key. If someone obtains this private key, they can access encrypted messages, so the security of this key is critical.

How Public Key Encryption Works

Public key encryption uses complex mathematical algorithms to ensure security. The basic working principle of this system is as follows:

1. Key Pair Generation: The user generates a pair of keys: a public key and a private key. The public key can be shared with anyone; the private key is stored securely.

2. Encryption: The sender encrypts a message using the recipient's public key. This process renders the message unintelligible to anyone other than the recipient.

3. Decryption: The recipient decrypts the encrypted message using their private key and accesses the original content.

This process ensures secure information sharing, as only individuals possessing a specific private key can decrypt the encrypted messages.

e Usage Areas

Public-key encryption is used in many different areas:

• Email Security: Systems such as PGP (Pretty Good Privacy) enable the encryption of email content.

• SSL/TLS Protocols: They enable secure communication over the internet, allowing websites to offer secure connections using HTTPS.

• Digital Signatures: Used to verify the integrity and origin of data.

Public-key cryptography is a critical tool for ensuring security in the digital world. Thanks to the two-key system, users can securely share information and verify identities. This encryption method plays a fundamental role in ensuring internet security and is indispensable in today's digital world.

Elliptic Curves

Elliptic Curve Cryptography (ECC) is an advanced cryptography method that meets today's digital security needs. ECC is based on the mathematical structure of elliptic curves used in public-key cryptography systems. Compared to traditional systems such as RSA, it offers the same level of security with smaller key sizes, making it an attractive option, especially for devices with limited processing power.

Mathematical Foundations of ECC

Elliptic curves are defined by the equation $y^2 = x^3 + ax + b$. The solution to this equation relies on the Elliptic Curve Discrete Logarithm Problem (ECDLP), which poses a significant challenge in cryptography. ECC is built on the difficulty of solving this problem. This difficulty forms the basis of the high security offered by ECC, as it provides strong security without the need for large key lengths.

e Advantages of ECC

Elliptic Curve Cryptography (ECC) stands out in cryptography due to its many advantages. One of its biggest advantages is that it requires smaller key sizes to provide the same level of security. For example, a 256-bit ECC key provides equivalent security to a 3072-bit RSA key. This feature makes ECC an ideal cryptographic solution, especially for mobile devices and other systems with limited processing power or energy capacity.

In summary, ECC has the following characteristics:

1. More Efficient Computation: Thanks to smaller key sizes, ECC is more efficient in terms of both computation time and memory usage. This enables lower energy consumption and faster processing times.

2. Bandwidth and Storage Savings: ECC saves bandwidth in data transmission by using smaller keys and digital signatures. It also minimizes storage requirements.

3. High Security: With shorter key sizes, it offers the same or higher level of security compared to classic algorithms such as RSA and DSA. The Elliptic Curve Discrete Logarithm Problem (ECDLP) is considered a very difficult problem to solve without requiring large key lengths.

4. Low Power Consumption: Small keys and an efficient computation structure make ECC an excellent choice for devices requiring low power consumption. It is widely used to extend battery life, particularly in IoT applications and mobile devices.

Application Areas and Standards ( )

ECC offers a wide range of applications for various cryptographic operations and protocols. It is effectively used in fundamental security operations such as digital signatures (e.g., ECDSA), key exchange (e.g., ECDH), and data encryption. These application areas ensure that ECC is preferred in many industries thanks to the high security and low resource usage it provides.

• Elliptic Curve-Based Digital Signatures (ECDSA/EdDSA):

Elliptic curve-based digital signatures are used to verify the identity of digital documents and ensure their integrity. ECDSA is widely used in areas such as online transactions, email security, and blockchain. ECC's low computational and memory costs have led to its widespread use in many areas today, from cryptocurrency wallets, primarily Bitcoin, to secure communication protocols.

• Elliptic Curve Diffie-Hellman (ECDH) Key Exchange:

It enables two parties to securely establish a shared key. ECDH is a preferred key exchange method in secure communication protocols such as public-key cryptography and SSL/TLS.

• Data Encryption:

ECC provides efficient data encryption operations even on devices with low processing power. It is a powerful encryption solution, especially for environments with limited resources such as mobile devices and IoT systems.

With the widespread adoption of ECC, various standards have been developed to create secure and compatible systems. NIST has defined several key standards for ECC-based algorithms:

• FIPS 186-4:

A standard for elliptic curve-based digital signature algorithms (ECDSA). This standard specifies the requirements for securely creating and verifying digital signatures.

• SP 800-56A/B:

This standard provides guidelines for key exchange protocols. SP 800-56A defines elliptic curve-based key exchange protocols (ECDH), while SP 800-56B sets rules for other public-key cryptography applications of ECC.

Security and Cryptographic Robustness

ECC has gained an important place in the modern digital security world by combining high security and efficiency. However, the security of ECC largely depends on the correct selection of the elliptic curve used and the correct implementation of these curves. Errors in elliptic curves or weak curve selections can compromise the security of ECC. In particular, to ensure the security of elliptic curves
, the mathematical properties of the selected curve must be carefully examined and the application must be performed correctly.

Hash Functions

Hash functions are one of the most fundamental building blocks of modern cryptography and are used in many critical security applications. Frequently used in areas such as ensuring data integrity, creating digital signatures, and password storage, hash functions also play an important role in wallet infrastructures that ensure the security of crypto assets. These functions are mathematical functions that convert input into a fixed-size hash value. For example, whether a few letters or a long text is entered into a hash function, a fixed-length value is produced as output. In this process, hash functions are expected to possess certain security properties. Cryptographic wallets utilize various cryptographic mechanisms such as hash functions.

Basic Properties of Hash Functions

A hash function must meet certain security properties. These are critical for cryptographic robustness and data integrity:

1. Pre-image Resistance: It should be difficult to find the input corresponding to a given hash value, i.e., to reverse engineer it. This property makes it difficult to derive the original data from its encrypted form.

2. Second Pre-image Resistance: Finding another input that produces the same hash value as a given input should be very difficult. This prevents data from being altered and manipulated with a fake hash value.

3. Collision Resistance: It must be nearly impossible to find two different inputs that produce the same hash value. Since collisions in a hash function can create security vulnerabilities, this feature is critically important.

These properties make hash functions reliable and ensure that crypto wallets are secure.
In crypto wallets, users create digital signatures to verify their transactions, and this process relies on hash functions. In addition, the private keys of wallets are protected by hash functions to ensure they are stored securely.

The Role of Hash Functions in Cryptocurrency Wallets

Cryptocurrency wallets operate based on hash functions to securely manage digital assets, particularly Bitcoin, Ethereum, and others. The primary uses of hash functions in cryptocurrency wallets can be listed as follows:

1. Key Management: Cryptocurrency wallets securely store the private keys that allow users to access their assets. These keys are made secure by processing them with hash functions. For example, a wallet password or PIN code is stored via a hash function and can only be decrypted when the correct inputs are provided.

2. Address Generation: Addresses created in crypto wallets to make a transaction or send an asset are usually generated based on hash functions.

In cryptocurrencies such as Bitcoin and Ethereum, a wallet address is created using a hash function based on a public key. For example, Bitcoin addresses are typically generated using hash algorithms such as SHA256 and RIPEMD160.

3. Digital Signatures: In crypto wallets, a digital signature is required for users to perform transactions. Digital signatures are created using hash functions to approve and verify the user's transactions. A transaction is signed using the user's private key with the help of a hash function, thereby ensuring the accuracy and source of the transaction.

4. Blockchains and Data Integrity: Hash functions form the basis of blockchains. Each block contains the hash value of the previous block, thereby preserving the integrity of the blockchain. The slightest change in a block affects the hash value of all subsequent blocks, causing the chain to break. This demonstrates how critical hash functions are in the secure storage of crypto assets.

Security Threats and Current Algorithms

Legacy hash algorithms have become vulnerable to various attacks over time due to security flaws. For example, algorithms such as SHA1 have proven weak against collision attacks and are no longer considered a reliable option in modern cryptography. Due to these security vulnerabilities, more secure hash algorithms such as SHA256 and SHA3 are preferred today. SHA256 is one of the fundamental hash functions used in crypto asset wallets such as Bitcoin. In the Bitcoin blockchain, each block is hashed using SHA256 and linked to the previous block, thus preserving the integrity of the chain. This structure ensures the security of blockchains and prevents tampering with transactions.

SHA3, a newer algorithm, was standardized by NIST in 2015. Designed to meet evolving needs in cryptography, SHA3 is a slightly modified and optimized version of the Keccak algorithm. One of SHA3's most significant innovations is its data processing technique, known as sponge construction. This structure works by "absorbing" the data like a sponge and then "compressing" the digest, making SHA3 more resistant to certain types of attacks. SHA3 has a security level compatible with SHA2 but is structurally different, providing additional protection against certain attacks.

SHA3 is used in various applications, particularly secure data storage, digital signatures, and identity verification. Additionally, functions derived from SHA3, such as SHAKE (Extendable-Output Functions), can meet specific application needs with flexible output lengths. Extensible output functions like SHAKE offer the ability to adjust the length of hash values according to requirements, making it more flexible for a wide range of cryptographic applications.

Digital Signing Algorithms

Digital signature algorithms are cryptographic protocols used to verify the integrity and origin of a message. These algorithms are based on mathematical foundations and play a critical role in proving the authenticity of data and providing security to the recipient. This section will examine the RSA, DSA, ECDSA, EdDSA, Schnorr, and Threshold Signature Scheme (TSS) algorithms.

RSA Signature Algorithm

The RSA digital signature algorithm relies on the difficulty of factoring large prime numbers.

Key Generation: In the RSA algorithm, two large prime numbers p and q are selected, and their product $N = p.q$ is calculated. Then, the Euler totient function $\phi(N) = (p-1)(q-1)$ is calculated. The encryption key e is selected such that $1 < e < \phi(N)$, and e and $\phi(N)$ are coprime. The private key d is calculated such that $e \cdot d = 1 \pmod{\phi(N)}$.

Signing: The message m is hashed using the hash function, yielding $H(m)$, and the signature is constructed as follows:

$$s = H(m)^d \bmod N$$

Verification: The recipient uses the following equation to verify the signature:

$$H(m) \stackrel{?}{=} s^e \bmod N$$

If the equality holds, the signature is considered valid.

DSA (Digital Signature Algorithm)

DSA is based on the ElGamal signature scheme and relies on the difficulty of the discrete logarithm problem.

Key Generation: A prime number p and a prime factor q (such that $q|p-1$) is selected. A number g is selected such that $g^q = 1 \bmod p$. The user's private key x, $1 \leq x \leq q-1$, and the public key is defined as $y = g^x \bmod p$.

Signing: The message m is hashed using the hash function $H(m)$. A random k, $1 \leq k \leq q-1$, is selected and the signature is constructed as follows:

$$r = (g^k \bmod p) \bmod q$$

$$s = k^{-1}(H(m) + x \cdot r) \bmod q$$

The signature pair is (r, s).

Verification: The recipient uses the following equations to verify r and s:

$$w = s^{-1} \bmod q$$
$$u_1 = H(m) \cdot w \bmod q$$
$$u_2 = r \cdot w \bmod q$$
$$v = (g^{u_1} \cdot y^{u_2} \bmod p) \bmod q$$

If $v = r$, the signature is considered valid.

ECDSA

ECDSA relies on the difficulty of the discrete logarithm problem over elliptic curves.

Key Generation: On the elliptic curve E, a point G is selected and the user's private key becomes d. The public key is $Q = dG$.

Signing: The message m is hashed using the hash function $H(m)$. A random k is selected and $kG = (r, \_)$ is calculated. The signature is formed as follows:

$$s = k^{-1}(H(m) + dr) \bmod n$$

The signature is a pair (r, s).

Verification: The recipient follows these steps to verify r and s:

$$w = s^{-1} \bmod n$$

$$u_1 = H(m) \cdot w \bmod n$$

$$u_2 = r \cdot w \bmod n$$

$$(x_1, y_1) = u_1 G + u_2 Q$$

If $x_1 = r \bmod n$, the signature is valid.

EdDSA (Edwards-Curve Digital Signature Algorithm)

EdDSA operates on Edwards curves and is optimized for performance.

Key Generation: A secret key *a* is generated, and the corresponding $A = aB$ is calculated.

Signing: Message *m* is hashed using a hash function $H(m)$. A random value *r* is determined as $r = H(a \| m)$, and $R = rB$ is calculated. The signature is formed as follows:

$$s = r + H(R||A||m) \cdot a \bmod n$$

The signature pair is (R, s).

Verification: The recipient verifies the signature using the following equation:

$$sB = R + H(R||A||m) \cdot A$$

Schnorr Signature Algorithm

The Schnorr algorithm relies on the difficulty of the discrete logarithm problem and has smaller signature sizes.

Key Generation: The private key is *x*, and the public key is $y = g^x \bmod p$.

Signing: A random *k* is selected and $r = g^k \bmod p$ is calculated. With the hash function:

$$e = H(m \| r)$$

and the signature is formed as follows:

$s = k - xe \bmod q$ The signature pair is (e, s).

Verification: The recipient calculates $r' = g^s \cdot y^e \bmod$ and verifies the following equation:

$$e \stackrel{?}{=} H(m \| r')$$

(Threshold Signature Scheme (TSS)

TSS relies on a threshold value ***t*** for n signers to create a signature. t signers must cooperate for the signature to be valid.

Key Generation: TSS divides the secret key among ***n*** signers, distributing a portion to each.

Signing: Each signer creates a partial signature using their own private key share. The partial signatures are combined using Lagrange interpolation to produce a full signature.

Verification: The complete signature is verified using the system's public key. The signing process provides privacy and distributed security for the signers.

Multi-Party Computation (MPC)

MPC is a cryptographic technique that enables secure computation in distributed systems. MPC allows a group of participants to perform a joint computation without revealing their private data. The goal of MPC is to process data and obtain computational results without compromising privacy among participants. This technique plays a critical role, particularly in secure data sharing, encryption key distribution, and processing confidential data. In cybersecurity and cryptography, MPC is becoming increasingly important for the secure processing of confidential and sensitive data.

Mathematical Foundations of MPC

MPC is essentially a set of cryptographic protocols that enable data to be processed securely without a trusted third party.

Throughout the computation process, each party protects its own secret inputs. No information leakage occurs between parties when the results are computed.

In MPC, computations are performed according to the following principles:

• Privacy: Each participant's input remains confidential and is not shared with other participants.

• Accuracy: The computation is performed correctly, and all participants arrive at the correct result.

• Reliability: The system must continue to produce reliable results even if one or more participants act maliciously.

These features are provided using methods such as Shamir's Secret Sharing.

Shamir's Secret Sharing

Shamir's Secret Sharing is one of the fundamental methods used in MPC and relies on sharing data using polynomials. This technique allows a secret to be divided among ***n*** participants of the SSS and enables the secret to be recovered only when a specific number of participants combine their shares.

• Secret Sharing: The secret is divided into ***n*** parts by creating a polynomial ***f(x)***. The constant of this polynomial***, f(0),*** represents the secret ***S***. The other participants receive shares ***distributed as f(1), f(2),.***

• Recovery of the Secret: When at least ***t*** participants gather, the original secret (SSS) can be recovered using Lagrange interpolation.

Thanks to this method, it is impossible to obtain the secret if fewer than t participants cooperate. This provides a high level of security for MPC.

's Application Areas

MPC is used in many different areas. The following areas are the most common applications of MPC in the world of cryptography:

• Confidential Data Analysis: Companies and organizations can perform joint analyses without revealing each other's data using MPC. For example, running fraud detection algorithms while maintaining the confidentiality of transaction data between banks.

• Key Management: Secure creation and sharing of cryptographic keys can be achieved through multi-party collaborations using MPC. For example, algorithms such as Threshold Signature Scheme (TSS) provide secure signing using MPC.

• Crypto Wallets: MPC is an important technology for MPC wallets, which require multiple signatures and enable multiple parties to sign in order to enhance security. MPC wallets are wallets where no single party knows the entire private key, and the key is shared in pieces. These wallets secure the user's keys while allowing multiple parties to collaborate on transactions.

Zero-Knowledge Proofs

Zero-Knowledge Proofs (ZKP) are one of the most innovative and effective techniques in modern cryptography. This method allows the prover to prove to the verifier that a piece of information is true without leaking any additional information to the verifier. Thanks to this feature, ZKPs have become a critical tool for protecting data privacy and security at the highest level. ZKPs have a wide range of applications, from identity verification systems to cryptocurrency transactions.

The Three Fundamental Properties of Zero-Knowledge Proofs ( )

There are three fundamental properties that ZKPs must possess to be secure and functional:

1. Completeness: If the proven statement is true, an honest prover can convince the verifier of the truth of this statement. In other words, the proof process is successful and satisfies the verifier.

2. Soundness: If the proven statement is false, no fraudulent prover can convince an honest verifier that a false statement is true. This makes it impossible to validate false information.

3. Zero-Knowledge: While proving the statement's correctness to the verifier, the prover should not disclose any additional information about the statement itself. This allows the verifier to learn that the statement is correct, but does not leak any other information to the verifier.

1. Interactive Zero-Knowledge Proofs (Interactive ZKPs): These require an interactive process between the prover and the verifier. During this process, the verifier asks the prover various questions and receives correct answers. The most classic example is the "Cave Metaphor," where the prover attempts to prove to the verifier that they know the location of a secret passage in the cave, but does not reveal where the passage is. Interactive ZKPs provide high security in some use cases, but can pose challenges for use in decentralized systems.

2. Non-Interactive Zero-Knowledge Proofs (Non-Interactive ZKPs): This is a type of proof that works without any interaction between the prover and the verifier. The prover presents a single proof, and the verifier uses this proof to reach a conclusion. They are well-suited for blockchain applications because they enable transactions to be performed without interaction in decentralized systems. Non-interactive ZKPs offer advantages in terms of efficiency and scalability.

3. zkSNARK (Succinct Non-Interactive Arguments of Knowledge): zkSNARKs are one of the most popular and widely used versions of non-interactive zero-knowledge proofs. They are used specifically in blockchain technology to solve transaction privacy and scalability issues. zkSNARKs produce short proofs and can be verified quickly. These features make ZKPs highly effective in large data sets and transaction-intensive systems.

4. zkSTARK (Zero-Knowledge Scalable Transparent Arguments of Knowledge): zkSTARKs work similarly to zkSNARKs but with one key difference: they do not require a trusted setup. zkSTARKs offer higher scalability and transparency. They produce faster and more secure results, especially when verifying large datasets.

5. Bulletproofs: A technique used to reduce the size of ZKPs and lower transaction costs. Bulletproofs produce smaller proofs compared to zkSNARKs and accelerate verification processes. This increases transaction efficiency in blockchain systems and prevents network congestion by reducing transaction sizes.

Zero-Knowledge Proofs offer a wide range of applications as a technology that directly addresses today's digital security requirements:

• Cryptocurrency Transactions: ZKPs are widely used to ensure the privacy and security of cryptocurrency transactions. Particularly in privacy-focused cryptocurrencies such as Zcash, verification can be performed without revealing users' identities or transaction details.

• Identity Verification: ZKPs allow a user to log into a system without revealing their identity. For example, a user can prove they are registered in a biometric database without revealing their biometric data.

• Data Privacy and Sharing: ZKPs are used to prove the accuracy of sensitive data such as health or financial data. Verification can be performed without sharing the data, which ensures data accuracy while maintaining privacy.

• MPC and ZKP Combination: Multi-Party Computation (MPC) and ZKPs can be used together to perform secure computations in distributed systems. This strengthens the balance between privacy and security by enabling confidential data to be processed without being shared.

Homomorphic Encryption

Homomorphic encryption is one of the most innovative approaches in modern cryptography and allows data to be processed in its encrypted form. This means that various operations can be performed on the data even while it is encrypted, and the results are meaningful and accurate when decrypted. This feature is particularly critical for crypto wallets integrated with MPC because these wallets rely on multi-party computation techniques to maximize privacy and security.

Mathematical Foundations of Homomorphic Encryption

Homomorphic encryption is an encryption function ***Enc()*** and provides the ability to perform operations on this function. Certain mathematical operations can be applied to encrypted data without the need to decrypt it. The fundamental principle of Homomorphic Encryption can be summarized as follows:

Let the data be m_1 and m_2.

Let these data be given in their encrypted form as $Enc(m_1)$ and $Enc(m_2)$.

When an operation is performed on the encrypted data, $Enc(m_1)$ and $Enc(m_2)$ are the encrypted form of the value obtained as a result of this operation: $Enc(m_1 \circ m_2)$

In this process, the result of the operation $m_1 \circ m_2$ can be obtained directly without decrypting m_2.

The encryption function $Enc(x)$ and the decryption function $Dec(x)$ have the following properties:

$Dec(Enc(m_1).\ Enc(m_2)) = m_1 \circ m_2$

This feature allows certain operations to be performed on encrypted data, and the result yields the correct result when decrypted.

ic Encryption in Cryptocurrency Wallets:

1. Key Management: In MPC-based wallets, private keys must be shared among multiple parties and processed securely. Homomorphic encryption allows these keys to be computed in an encrypted form. While the keys remain encrypted, correct computations are performed, and secure keys can be generated as a result of the operation.

2. Transaction Signing: When a transaction is to be performed, the parties in the MPC wallet can sign transactions in an encrypted manner. Thanks to homomorphic encryption, signature operations can be performed in an encrypted manner, and the validity of the signature can be verified without revealing the private keys of the parties who signed it.

3. Privacy Protection: Cryptocurrency wallet users may wish to keep their transactions private. Homomorphic encryption ensures this privacy by keeping transaction details encrypted. Wallet users can securely conduct transactions without revealing transaction information. Especially in transactions requiring multi-party signatures, conducting transactions with encrypted data enhances privacy.

e Advantages of Homomorphic Encryption

Homomorphic encryption enhances the security and privacy of MPC-based crypto wallets, but it also offers several other significant advantages:

• Ability to Process Encrypted Data: Transactions can be performed while data remains encrypted, eliminating the need to share data with third parties. For example, a user's wallet address or transaction details remain encrypted throughout the transaction, and no one can access this information.

• Security of Multi-Party Computations: When combined with MPC, homomorphic encryption enables highly secure computations between parties. This plays a critical role in key management and transaction security in wallets.

• Data Integrity and Privacy: Data integrity is preserved during transactions, and the data obtained as a result of operations performed on encrypted data is consistent with the original data. This maximizes the security of wallet transactions.

Challenges of Homomorphic Encryption and Limitations of

Although homomorphic encryption offers significant advantages in MPC-based wallets, there are also some challenges:

• Computational Cost: Homomorphic encryption requires more computational power and time compared to other encryption methods. Especially in fully homomorphic encryption systems, processing time and resource usage are quite high.

• Efficiency: In systems requiring real-time transactions, such as crypto wallets, the slowness of homomorphic encryption can negatively impact system performance. Therefore, hybrid systems can be used to improve performance.

• Key Management: The security and management of keys used with homomorphic encryption also pose an additional challenge. Keys must be properly distributed and protected.

e Wallet Categories

Wallets used in the cryptocurrency world are essential tools that enable the secure storage and management of digital assets. They are divided into different categories based on security requirements, transaction speeds, and user needs. These categories are generally known as hot wallets, cold wallets, and warm wallets. Each category offers different approaches in terms of cryptography and security.

Single-Signature Wallets

Single-signature wallets represent the simplest form of cryptocurrency wallets. Known as traditional digital wallets, they typically rely on a single private key to access assets.

Essentially, these wallets operate on a simple principle: A private key provides full control over the associated funds. This key acts as the sole signature required to move the funds, making these wallets easy to use but also creating certain vulnerabilities:

• Single Point of Failure: Since these wallets rely on a single private key, if that key is compromised, the entire wallet balance is at risk. In other words, this approach creates a single point of failure, leaving the wallet vulnerable if the private key is lost, stolen, or compromised. While traditional financial systems offer backup options and fraud protection, in single-signature wallets, if the private key is lost and no backup has been made, it is usually impossible to recover the funds.

• Lack of Shared Access: Single-signature wallets do not have the ability to share access or control. Therefore, they are not suitable for organizations or groups that require joint financial management.

While useful for individual users with small funds, the inherent risks and lack of flexibility of these wallets make them inadequate for institutions or scenarios requiring greater security.

Wallets enable the creation of digital (cryptographic) signatures (e.g., ECDSA, EdDSA, BLS) through the signing process, which is primarily performed using a secret (private) cryptographic key. Digital signatures form the basis of all decentralized infrastructures. When a transaction is signed by its owner, it is sent to the decentralized network. The network's nodes verify the signature using the sender's public key, which ensures the transaction's validity.
Trust in decentralized systems is as important as ensuring the security of private keys.

However, current key management solutions fall short of meeting the desired availability, security, and privacy requirements. The protection of private signing keys is entirely up to the users themselves. Current traditional wallet technologies face the following issues:

1. Identity Exposure: Signers are publicly known and traceable on the blockchain (pseudonyms are not sufficient to conceal identities). Therefore, attackers can target a specific signer based on publicly available information on the blockchain network. If the identity of a user holding a large amount of funds is obtained, this could even put the user's life at risk. Furthermore, any system holding private keys could be a prime target for cyberattacks.

2. Cyber Threats: Since each individual has only one private key (this key is physically stored on mobile devices, desktop computers, hardware tokens, or USB drives), it is difficult to securely protect these keys against complex cyber threats, making them vulnerable to single point of failure attacks.

3. Internal Threats: Preventing internal threats within a business is not easy. Therefore, if an employee becomes malicious, corporate funds may be at risk. One way to prevent this is to establish a distributed structure that prevents any single person from accessing the funds.

Hot Wallets ( )

Hot wallets are wallets that are constantly connected to the internet and used for instant transactions. From a cybersecurity perspective, hot wallets strike a balance between security and speed. Key pairs are typically generated using elliptic curve-based algorithms such as ECDSA or EdDSA. The user creates digital signatures using their private key, and transactions are carried out with these signatures.

However, being constantly connected to the internet can make them vulnerable to attacks such as Man-in-the-Middle (MITM) and key logging.

When modeling hot wallets algebraically, assume that an elliptic curve defined over $\boldsymbol{Z_p}$(the set of integers modulo $\boldsymbol{p}$) is used, where $\boldsymbol{p}$ is a prime number. The user's private key is $\boldsymbol{d}$ and the public key is $\boldsymbol{P}$ = dG, where $\boldsymbol{G}$ is a generator point on the elliptic curve. During a transaction, the user creates a digital signature using the private key $\boldsymbol{d}$. However, the system's protection against replay attacks and side-channel attacks may be insufficient. Therefore
hot wallets, while suitable for actively using small amounts of cryptocurrency, should not be preferred for transactions requiring high security.

Cold Wallets (Cold Wallets)

Cold wallets store your private key entirely offline to ensure the security of your cryptocurrency. This makes it impossible for hackers to access your private key over the internet, eliminating security risks.

significantly reduces security risks. Hardware wallets are the most popular type of cold wallet and can be considered "air-gapped"
systems. In other words, your private key
(d) never comes into contact with the online environment. When you want to make a transaction, the hardware wallet performs the necessary calculations to generate the signature, but never exposes your private key outside the device.

Hash-based cryptography and multi-factor authentication further enhance the security of cold wallets.
For example, a strong hash function such as SHA256 or Blake2b is used to securely hash transaction data. This hash is then sent to the hardware wallet, where the signing process is performed without the private key ever leaving its secure environment.

Additionally, advanced techniques like Zero-Knowledge Proofs (ZKP) enable verifying the transaction's validity without revealing the private key. The biggest disadvantage of cold wallets is their difficulty of use. The device must be brought online for each transaction, which can slow down the process and negatively impact the user experience. However, the superior security they provide makes this disadvantage worthwhile, especially when storing large amounts of cryptocurrency.

Warm Wallets (-Warm Wallets)

Warm wallets strike a balance between hot and cold wallets. They are typically stored offline but can be quickly brought online when needed. Mathematically, warm wallets often enhance security using threshold signature or multisig algorithms.

Such protocols ensure that a transaction is only valid when a specific number of users sign it.

For example, the Shamir Secret Sharing protocol is an ideal security mechanism for such wallets. This protocol allows the private key to be split into different parts and distributed. Mathematically,

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1}$$

A polynomial is created, and when t points of this polynomial are known, $a_{(0)}$, i.e., the private key,
can be recalculated. This method can be used by warm wallets to
.

This type of wallet is often preferred by corporate users who want both security and ease of access. However, putting the wallet online can pose some security risks; therefore, multi-signature or similar additional security measures are recommended.

e Wallets

Multisig wallets have a structure that requires signatures from multiple parties for a transaction to be valid. Mathematically, these wallets are modeled using threshold cryptography. Suppose that at least n signatures are required for a transaction to be approved. In this case, each signature data is used for verification, and the transaction is only successful when the specified threshold is met.

The algebraic model of a Multisig wallet could be as follows: Suppose there are n private keys ***d1, d2, ...,*** dn on an elliptic curve ***E. .....dn***. Each
The user's public key P_i is defined as $d_i.G$.
Here, ***G*** is the generator point on the elliptic curve.
For transaction verification, at least ***t*** people must create digital signatures using d_i that meet this threshold value. This mechanism increases security by making it difficult to complete a transaction even if a single person's private key is accessed.

These structures are particularly preferred for corporate wallets, exchanges, and secure transfers. From a cybersecurity perspective, Multisig significantly increases security because even if one person is attacked, they cannot approve the transaction alone.

How Do Multisig Wallets Work?

The m-of-n principle forms the basis of multisig wallets. This principle defines the minimum number of signatures (m) required for a transaction to be considered valid, out of a total of n keys. For example, a 3-out-of-5 multisig wallet allows a transaction to occur after receiving signatures from any three of the specified five keys. This mechanism not only enhances security but also reduces risks associated with lost private keys.

Transactions can be executed as long as the required threshold number of signatures is obtained. Multi-signature (Multisig) technology is a method developed to enhance the security of digital assets. This technology is typically used by joint accounts or organizations to authorize and execute a transaction that requires approval from multiple parties. It is also particularly suitable for situations requiring collective decision-making, such as joint funds, business partnerships, or financial operations. While transactions in traditional single-signature wallets can be verified with just one private key signature, multi-signature wallets require signatures from multiple keys. This approach provides greater security and control over transactions.

Multi-signature wallets are managed through smart contracts on the blockchain network. These smart contracts enhance security and provide decentralization by defining the necessary conditions and participants to validate a transaction. Thus, multi-signature eliminates a single point of failure and creates an additional layer of security by preventing unauthorized transactions.

cryptography Behind Multi-Signature (Multisig)

a) Threshold Signatures

Threshold signatures are the fundamental concept that enables multisig wallets to function securely. The threshold value m determines how many signatures out of the total number of signers (n) are required to authorize a transaction. For example, in a 2-out-of-3 multisig wallet:

- Each of the three individuals or organizations has their own private key.
- To initiate a transaction, at least two of these three private keys must be signed.
- The transaction is considered valid once the required number of signatures (in this case, two) is obtained.

This mechanism means that even if one of the private keys is compromised, the attacker cannot transfer funds without the cooperation of the other signers.

b) Security Measures

When implementing multi-signature wallets, it is important to follow best practices to ensure maximum security:

1. Geographic Distribution: Ensuring signers are geographically dispersed reduces the risk of a single location being compromised.

2. Regular Key Rotation: Regularly changing private keys reduces the risk of long-term key exposure.

3. Cold Storage: Storing some private keys offline (cold storage) protects them from online attacks.

4. Audit Logs: Keeping detailed audit logs of wallet activities is important for monitoring and tracking suspicious actions.

5. Use of Different Platforms: Using different platforms (such as Windows, Linux, iOS) together can reduce the risk of a potential zero-day attack affecting the entire system. This diversity provides extra security by preventing platform-specific vulnerabilities from compromising the entire wallet structure in a single attack.

Advantages of Using Multi-Signature

1. Increased Security: Multi-signature wallets offer greater security compared to single-signature wallets. Since multiple private keys are required to authorize a transaction, the risk of unauthorized access or fraud is significantly reduced. This method provides additional security by preventing a single point of failure.

2. Risk Reduction: Since multiple parties are required to approve a transaction, the risk of losing funds due to a single person's error, mistake, or malicious intent is significantly reduced. This is a major advantage, especially for organizations.

3. Shared Control: Multi-signature wallets, ideal for shared accounts or organizations, allow multiple users to jointly manage funds. This ensures that decisions regarding transactions are made in a more transparent and democratic manner.

4. Fraud Prevention: The requirement for multiple signatures reduces unauthorized transactions and potential fraud attempts. Since multiple parties must approve any transaction, the likelihood of malicious transactions decreases.

5. Customizable Security Levels: Multi-signature wallets allow the number of signers required to execute a transaction to be customized. This provides flexibility between security and usability.

e Disadvantages of Using Multi-Signature

1. Complexity: Setting up and managing a multi-signature wallet is more complex than traditional single-signature wallets. It requires coordination between multiple parties and an understanding of how the multi-signature system works.

2. Risk of Access Loss: If one of the authorized parties loses their private key or it becomes unusable, access to funds may be blocked. This can be a major problem, especially when critical transactions are involved.

3. High Setup Costs: Creating and maintaining a multi-signature wallet can sometimes require higher initial costs due to its complexity and additional security measures.

4. High Transaction Fees: Since multi-signature transactions have larger signature data, they require higher transaction fees than single-signature transactions. This extra cost can be a significant disadvantage for users, especially on congested blockchain networks.

5. Transaction Delays: Transactions may experience delays compared to single-signature transactions because they require multiple signatures. Delays can occur especially when one of the signers is unavailable.

6. Dependency on Signers: The functionality of a multi-signature wallet may be compromised if one of the required signers fails to respond, potentially causing transaction bottlenecks.

Understanding these advantages and disadvantages can help individuals or organizations determine whether a multi-signature wallet is the right choice for their cryptocurrency storage and transaction needs.
In summary, a multi-signature wallet prevents any single person or organization from having full control over the assets stored within it, thereby enhancing security and providing shared control among multiple authorized users.

MPC ( ) Wallets

Multi-Party Computation (MPC) is an advanced technique used to enhance the security of digital assets. MPC is a revolutionary cryptographic technique that enables multiple parties to perform joint computations without revealing their individual input data. MPC ensures secure, joint computation while protecting private data. In the context of wallets, MPC splits a private key into parts and distributes them among multiple parties.

This increases security by reducing the risk of a single point of failure. MPC wallets offer more flexibility than traditional Multisig wallets.

MPC enables multiple parties to perform a joint computation without disclosing their private data. This method is based on the Shamir Secret Sharing (SSS) protocol. In this method, a secret key is divided into multiple parts, with each part distributed to different parties. This ensures that the secret key cannot be revealed unless a certain threshold number of parts are brought together.

The security of MPC is based on two fundamental properties:

1. Privacy: The private information held by the parties cannot be learned by other parties while the protocol is being executed.

2. Correctness: Even if some parties attempt to deviate from the protocol or share information, MPC prevents these attempts from affecting the correct result or leaking the information of honest parties.

3. Threshold Signing and Robustness: MPC's threshold feature ensures that only a certain number of parties need to participate for the transaction to be executed.

This feature increases the system's robustness, ensuring that the transaction is successfully completed even if some parties cannot participate in the protocol or act maliciously. This makes MPC reliable and more resistant to attacks.

MPC eliminates the "single point of failure" because it does not require the creation of a single private key. MPC-based solutions provide operational flexibility compared to multi-signature solutions. For example, the number of signers in an MPC wallet can be increased or decreased, and these changes do not cause any disruption to operational processes. Furthermore, MPC has a wider range of applications because it is more compatible with different blockchain protocols.

One of the most significant innovations of MPC in digital asset security is the continuous renewal of the private key (key refresh). This feature means that an attacker has only a few minutes to seize all key shares; after this period, the shares are renewed, and the attacker must start over. This method strengthens the security layer, providing additional protection against cyberattacks.

MultiSig and MPC wallets offer security mechanisms that address this vulnerability by distributing control and increasing protection against unauthorized access. Below, we examine the unique features, similarities, and limitations of these technologies, focusing on MultiSig and MPC wallets.

MPC and MultiSig : Similarities

Although MPC and MultiSig wallets have different mechanisms, they share some common similarities for institutions seeking to enhance the security and control of digital assets:

• Distributed Control: Both technologies have the ability to distribute wallet access and control among multiple parties or organizations.

This enables institutions to make collective decisions on transactions and minimizes the risk of unauthorized transactions or internal fraud.

• Strong Security and Robustness: MPC and MultiSig wallets maintain the overall security of the system as long as there are enough participants or signatures remaining, even if some participants or keys are compromised. This security layer has a much more robust structure than single-key solutions.

• Minimum Trust: MPC and MultiSig reduce the need for trust between participants by distributing control and using cryptographic algorithms. This is particularly valuable when working with complex corporate structures or external partners.

• Flexibility: Both MPC and MultiSig can be customized to suit specific security needs and operational processes. Organizations can determine the number of signers required for transaction authorization and the preferred cryptographic algorithms.

e Advantages of MPC Wallets

MPC (Multi-Party Computation) wallets are becoming an increasingly popular option for managing digital assets by addressing many of the limitations encountered in MultiSig wallets. Here are some key advantages of MPC wallets:

• Flexible Multi-Chain Support: MPC wallets have a blockchain-agnostic structure and can support many blockchains that use ECDSA, EdDSA, and BLS signing algorithms. Unlike MultiSig wallets, a single MPC wallet can manage assets on multiple blockchains.

• Advanced Privacy: MPC wallets only require a single private key signature to be broadcast to the blockchain for transaction approval. All other computations occur off-chain, and sensitive information remains hidden from public view. This makes MPC wallets ideal for privacy-focused organizations.

• Key Recovery Mechanisms: MPC wallets offer key recovery mechanisms, allowing for the recovery of lost or compromised keys. This feature provides a security net that is often lacking in traditional MultiSig solutions.

• Low Gas Fees and Increased Transaction Speed: MPC wallets can significantly reduce gas fees associated with blockchain transactions.

Since complex computations occur off-chain, the transaction published to the blockchain for confirmation is smaller.

This reduces the transaction size, leading miners to prioritize these transactions and result in faster transaction confirmations.

Limitations of MultiSig Wallets

While MultiSig wallets enhance security compared to single-key wallets, they also present certain limitations:

• Not Protocol Agnostic: MultiSig wallets are not compatible with every blockchain protocol and may require different implementations for each blockchain. This necessitates the use of multiple wallet solutions to manage different crypto assets.

• Operational Complexity: As organizations grow, tasks such as changing the number of signers or adding or removing keys can become difficult. Since MultiSig wallets are typically pre-configured, making such changes is inflexible.

• Transparency Issues: The public nature of transactions on the blockchain allows MultiSig signatures and approval thresholds to be tracked. This can attract the attention of malicious actors and create potential targets for attack.

• High Transaction Costs: Since every transaction in MultiSig wallets is created on the chain, a transaction fee must be paid for each wallet creation, address creation, and signature. This results in high transaction costs for transactions requiring multiple signatures.

To summarize briefly, the general benefits of the MPC solution can be listed as follows:

• System-Level Threshold Security

• Support for Threshold ECDSA, Threshold EdDSA, and Threshold BLS

• Shared Responsibility

• Preventing financial losses from cryptocurrency exchanges

• Ensuring the privacy of signers

• Separation of the signing process and signature requests

• Improving availability and eliminating single points of failure

• Lower transaction fees

• Multi-party approval

• Multi-factor authentication

• Creating a whitelist for hot wallets (as an additional security layer)

• Mobile app support for iOS and Android platforms (to ensure ease of use and increased usability)

• No need for a central trusted party to generate public-private key pairs (trustless setup)

• Cloud services participating in the signing process for a single user

• Unique communication between connected services

• Non-repudiation between services

• Threshold asset key management with cloud services for end users

• Third-party audits

Blockchain and cryptocurrency technologies offer innovative solutions for storing and securely managing digital assets. Techniques such as multi-signature usage, cold storage, HSM/TPM/SGX procedures, and MPC have been developed to enhance the security of digital assets and are of critical importance, especially for cybersecurity experts. The operational flexibility, protocol independence, and high security that MPC provides compared to multi-signature methods make this technology a more advanced solution for digital asset security.

Custodial ( ) Wallets

Custodial wallets are a more centralized type of wallet where the user's private keys are managed by a third party. In these wallets, cryptographic control is typically held by the service provider rather than the user.
Users securely manage service provider keys when using the service provider's APIs to perform their transactions.

Mathematically speaking, custodial wallets are primarily protected by the service provider's encryption infrastructure and access control models. Encryption algorithms are used for keys stored in the service provider's data centers. Access control mechanisms, such as Role-Based Access Control (RBAC), form the core security components of these wallets. This type of wallet is commonly used on centralized exchanges and facilitates transactions on behalf of users. However, since users are not the actual owners of the keys, it is considered a weaker model in terms of security.

-Free (Non-Custodial) Wallets

Non-custodial wallets are wallets where the user has full control over their own private keys.

In these wallets, no third party can access the user's assets or private keys. Cryptographically speaking, each user possesses their own wallet's key pair, and these keys are typically generated and protected using secure elliptic curve algorithms such as ECDSA.

The fundamental cryptographic security of non-custodial wallets relies on the secure storage of the user's private key. HD Wallets (Hierarchical Deterministic Wallets) are a technology that enables the secure generation of multiple private keys using a single seed. Mathematically, HD wallets operate with child keys derived from a master key, and these keys are calculated deterministically.

ic Wallets

Fully non-custodial wallets allow users to have complete control over their assets. Private keys are stored entirely by the user, and no third party can access these keys. Cryptographically, the wallet owner's authority is verified using digital signatures for each transaction. These wallets offer high security and privacy, but user errors (e.g., key loss) can lead to serious consequences.

-Supported Non-Custodial Wallets

Supported non-custodial wallets provide users with full control over their private keys while also offering a certain level of third-party support. For example, third parties may only be involved in recovery mechanisms. These wallets typically work with social recovery mechanisms. Cryptographically, while the user retains full control over the key, additional security measures (e.g., multi-signature or recovery keys) are provided.

This type of wallet offers the advantages of non-custodial wallets while also standing out with security measures that protect against user errors.

Paper Wallets

Paper wallets are a simple and low-cost method used by users to store their digital assets offline. A paper wallet typically contains the user's private and public keys for their crypto assets in the form of a QR code or written text. Since they are not connected to the internet, they eliminate the risk of cyber attacks. The biggest advantages of paper wallets are their low cost and the fact that they give users complete control. However, they carry risks such as physical damage, loss, or becoming unreadable(12). Therefore, special precautions must be taken to protect paper wallets. Transacting with paper wallets can be more complex than with digital wallets. To transfer or spend, you must transfer the keys to a software wallet. In conclusion, paper wallets offer a low-cost and secure offline solution, but they should be used with caution due to physical risks and usage difficulties.

e Wallets

Voice wallets provide offline protection by storing the private keys of digital assets as encrypted audio files. These files are stored on physical media such as CDs or vinyl records, offering strong protection against cyber attacks. Although audio wallets are an innovative security method, they can be difficult to use due to the technical knowledge required and the risk of damage to physical media. Therefore, they are more suitable for users with more technical knowledge who are seeking innovative security solutions.

e Wallets

A Brain Wallet is a type of storage technique created by users using a password or phrase (usually a passphrase) that allows them to remember the private keys of their digital assets. With brain wallets, users do not need any physical or digital storage device to access their wallets. They are created through deterministic crypto address generator services such as Brainwallet.io (13).

One of the biggest advantages of memory wallets is that they allow you to protect your assets without the need for a physical wallet. Additionally, access to your assets is only possible with a password known only to you, which enhances privacy. However, memory wallets also have some significant disadvantages. If you forget your password, you may lose access to your digital assets completely. Furthermore, using simple or predictable passwords increases the risk of your wallet being compromised and can jeopardize your security. Therefore, it is crucial for those considering using a memory wallet to choose strong passwords that are difficult to forget.
Memory wallets may be a suitable option for those seeking an innovative and minimal approach to storing their digital assets, but users must be careful about creating strong passwords.

-Based Smart Contract Wallets

Smart contract-based wallets refer to wallets where digital assets are stored as smart contracts, or in other words, at a contract address. Users' transfer transactions are carried out on the smart contract. Compared to traditional cryptocurrency wallets controlled by a single private key, smart contract-based wallets differ in terms of increased security, automation, and functionality.

Smart contract-based wallets offer an advanced solution that manages your digital assets within a framework of automated processes and rules. Unlike traditional wallets, these wallets are managed by smart contracts that activate when specific conditions are met, rather than relying on a single private key. This automates the management of your crypto assets and enhances security.
For example, Gnosis Safe is a smart contract-based wallet used for transactions requiring multiple signatures. Argent serves as an Ethereum wallet by providing an interface. ERC4337 stands out as a solution that provides smart contract-based account abstraction standards on the Ethereum network. One of the most important advantages of smart contract-based wallets is that they offer programmable transactions. Complex transactions such as automatic payments and time-locked transactions can be easily performed with these wallets. Additionally, the extra security layers provided by smart contracts play a significant role in protecting digital assets. However, using these wallets can be more complex than traditional wallets and may require technical knowledge (14).

Additionally, if smart contracts are misconfigured, irreversible transactions may occur, meaning that it is not possible to reverse erroneous transactions. Therefore, while smart contract-based wallets offer a secure and flexible solution for users with technical knowledge
users a secure and flexible solution, but they require careful configuration and use.

e Wallets

Software wallets are applications that allow users to securely store and manage their digital assets; they can be downloaded and installed on a computer, run online via the cloud, or run on a smart device via a mobile application.

Users can protect their private keys through software wallets and use these private keys to communicate with other blockchains and perform cryptocurrency transactions.

Software wallets typically allow users to create cryptocurrency wallet addresses, send and receive cryptocurrency, view their current balances, and in some cases, purchase or exchange cryptocurrency. They can also enable users to perform various financial transactions using DeFi (Decentralized Finance) services.

There are many examples of software wallets, such as Paribu Self, Metamask, Phantom, Keplr, Temple, TrustWallet, myEtherWallet, and Guarda.

Software wallets are susceptible to cyber attacks because they are online. Users should minimize these risks by using strong passwords. It is also crucial to update the security features of software wallets and download the application from reliable sources (10). Additional measures such as strong passwords, two-factor authentication, and regular backups are necessary to ensure security. Since the security of software wallets is directly linked to the security of the device used, these precautions are vital.

Hardware Wallets

Hardware wallets are physical devices used to secure digital assets by storing users' private keys offline. Since hardware wallets are not connected to the internet, they provide additional protection against cyber attacks.

Therefore, hardware wallets are an important option, especially in situations requiring high security and for long-term investments.

Unlike software wallets, hardware wallets require physical access and may also have additional tamper-resistant features.
For example, they stand out with physical security measures such as PIN codes and fingerprint recognition, as well as tamper-resistant features. However, using these devices can be more complex than software wallets, and the setup process may take more time. Using hardware wallets can involve certain difficulties, such as backup and hardware failure. There is also the possibility of losing the device. Despite these disadvantages, hardware wallets are the preferred solution for providing a high level of protection for the security of digital assets. Today, there are many hardware wallet providers such as Trezor, KeepKey, BitBox, CoolWallet S, ELLIPAL Titan, and Tengem (11).

Cold Storage - HSM Procedures

Cold storage methods rely on keeping cryptocurrencies offline, providing the highest level of protection against online threats. Although cold storage methods for crypto assets carry certain security risks, they can be secured using Hardware Security Modules (HSM).

Cold Storage and HSM ( ) Usage

The cold storage method involves storing private signing keys offline, providing effective protection against cyberattacks over the internet. However, the use of cold storage solutions also brings some operational challenges.

Storing, processing, and transferring crypto assets may require multi-step, time-consuming procedures. At this point, the use of HSMs plays a critical role in keeping private keys in a secure environment and ensuring that transactions involving these keys are performed securely.
HSMs are specially designed cryptographic processors that ensure private keys are stored in a secure environment and that encryption, authentication, and signing operations performed with these keys are executed with a high level of security. With these features, the use of HSMs in cold storage systems provides multi-layered protection for private keys by combining both offline and physical security layers.

HSM Procedures and Technical Details

1. Key Management and Key Generation

• HSMs are used to generate and store the private keys of cryptographic assets. During key generation, HSMs use Hardware Random Number Generation (HRNG) to maximize the level of randomness. This makes it extremely difficult to predict or regenerate the keys.

2. Key Storage and Physical Protection

• HSMs feature a tamper-resistant design to physically protect private keys. If a physical tampering attempt is detected, the HSM automatically erases all private keys and sensitive data stored within it. This feature prevents private keys from being physically compromised in any way.

3. Cryptographic Operations and Authentication

• HSMs perform cryptographic operations directly within themselves and ensure that private keys never leave the device.

For example, when a transfer transaction is to be performed, the relevant private key is signed using the HSM, and since this transaction is performed only within the HSM, complete protection against external threats is ensured.

4. Policy-Based Security and Authorization

• In HSM-based cold storage methods, additional security policies can be applied to transactions. For example, parameters such as specific transfer limits, whitelisted wallet addresses, and spending limits can be defined during HSM setup. This ensures that each transaction is checked for compliance with these policies, and non-compliant transactions are rejected.

Cold Storage - HSM Integration and Usage Challenges

HSM integration can be a complex process requiring technical expertise during integration into the existing infrastructure. The following steps should be followed for successful HSM integration:

• Planning and Compatibility: Detailed planning should be carried out for HSM integration, taking into account the company's existing infrastructure and operational requirements.

• Testing and Validation: After HSM installation, all processes must be tested to ensure they work compatibly. This phase involves rigorously testing HSMs and resolving any incompatibilities.

• Security and Maintenance: Periodic maintenance and firmware updates should be performed to protect HSMs from security vulnerabilities.

• Physical Security Measures: HSMs must be stored in a secure environment and access must be restricted to authorized personnel only. Physical security vulnerabilities are critical in preventing devices from falling into the hands of unauthorized individuals.

• Access Controls and Authorization: Access to HSMs must be controlled. Only individuals with the necessary permissions should have access. Otherwise, a malicious administrator could misuse HSMs to gain access to critical funds or sensitive data. Therefore, determining and managing authorization levels is of great importance.

Threats and Challenges Encountered During the Storage Process

The rapid proliferation of digital assets presents significant opportunities for financial institutions, but it also creates new challenges and threats. Safeguarding these assets extends beyond technical infrastructure and security measures to encompass a broad range of areas, including regulations, the human factor, and technological risks. Institutions must understand and manage the complex challenges and increasing threats they face in protecting digital assets. There is no single solution to this process; reliable approaches require a balanced combination of technology and procedures.

In the processes of storing digital assets, multiple control points should be implemented at every stage, such as using cryptographic techniques to ensure ownership and control of assets, enabling secure interaction with smart contracts, and providing support for tokenized securities. Technical security measures must be implemented to protect against external attackers, internal threats, or accidental failures, including safeguarding private keys; ensuring data integrity, key recoverability, and audit trails; and addressing software vulnerabilities and exploits. Furthermore, security assumptions such as the determination of security protocols (multi-party approval, single sign-on, disaster recovery), the use of trusted hardware, and the security level of cryptographic protocols should also be evaluated as part of procedural and technical security controls.

Regardless of the storage mechanism (hot, warm, or cold), the secure storage of seeds or private keys is of vital importance. One of the most important goals is to prevent unauthorized access to these seeds or keys, otherwise funds may be at risk. To prevent attempts to manipulate approval rules, an approval mechanism based on a certain majority vote is usually required. This mechanism should define actions such as whitelisting specific addresses, setting transaction amount limits, and determining the actions permitted in smart contracts. Legitimate users of the platform should sign transactions through the approval mechanism without directly accessing the private keys.

Backup operations must take place in a secure and controlled environment equipped with multi-layered access control to prevent unauthorized access. The backup process must be verifiable, and backup integrity must be regularly checked. Personnel involved in key generation and backup management must undergo comprehensive background checks and training to ensure full compliance with security protocols.
training to ensure full compliance with security protocols. Backup systems must be tested regularly, integrated with other controls, and integrated with disaster recovery plans and emergency procedures.

In addition to these challenges, user interface and user experience are of great importance in the dynamic world of cryptocurrency. These two factors directly influence customer preferences. Therefore, designs should be created that prioritize user security without negatively impacting the experience. While security affects the company's reputation risk, user experience will directly influence the adoption of the application.

Cybersecurity Threats and Risk Management

Cybersecurity threats in blockchain-based systems vary, including unauthorized access, phishing attacks, distributed denial of service (DDoS) attacks, and smart contract vulnerabilities. When it comes to storing digital assets, the compromise of private (secret) keys and vulnerabilities in security architectures pose serious threats.

• Unauthorized Access: Brute force attacks targeting storage wallets and attacks exploiting security vulnerabilities provide direct access to digital assets. Weak key management systems are particularly targeted by attackers in decentralized wallets.

• Phishing Attacks: These are social engineering attacks that aim to deceive users into revealing their private keys or wallet access information. Advanced URL spoofing and Evil Twin (fake wireless access point (Wi-Fi) attack) techniques are used to target corporate access points.

• DDoS Attacks: Storage organizations' API access points or network infrastructure are targeted by coordinated botnet attacks, reducing system performance and causing service interruptions.

Risk management requires multi-layered security strategies that include the early detection of cyber threats and immediate response processes. Storage organizations should use the following techniques, integrated with proactive security protocols, to minimize threats
techniques to minimize threats:

Penetration Testing (Pen Testing): Simulated attacks conducted to identify security vulnerabilities in the storage infrastructure.	White Box Testing: Analyses of internal system architecture and code structures. Black Box Testing: Testing external access points from an attacker's perspective. Gray Box Testing: Security testing based on partial information.
Zero-Day Attack Analysis Behavior-based anomaly detection and threat intelligence should be used to detect attacks that exploit unknown security vulnerabilities. Artificial intelligence and machine learning algorithms play an important role in detecting zero-day threats.	Real-time data analysis should be provided using Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS). Sandboxing: Threats are detected immediately by analyzing code containing security vulnerabilities in isolated environments.
Real-Time Threat Detection Continuous monitoring and log analysis systems are used to identify unusual activities in the system.	SIEM (Security Information and Event Management): Integrated solutions that detect potential threats by analyzing log data in real time. Anomaly Detection: Performs anomaly analysis on network traffic, transaction behaviors, and system accesses.

Advanced risk analysis consists of methods that continuously assess cybersecurity threats and increase system resilience. Some of the techniques used to increase the security level of storage organizations are as follows:

• Threat Modeling: An approach that systematically analyzes potential security risks. Each layer of the storage infrastructure is evaluated in detail:

  • Stride Model: Classification of threats based on Identity Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service (DDoS), and Elevation of Privilege risks.

• Cryptographic Security: The security and robustness of cryptographic algorithms and protocols in storage solutions play a critical role in risk analysis:

• Post-Quantum Cryptography: Solutions must be developed that are resistant to the risk of quantum computers breaking traditional cryptographic algorithms.

• Advanced Key Management: Key rotation, multi-signature (Multi-Sig) protocols, and distributed key management techniques (e.g., Shamir Secret Sharing) should be implemented.

DREAD Analysis: DREAD Analysis is a framework used to assess security risks. Developed by Microsoft, this method classifies threats and enables a more systematic analysis of their impact.
DREAD performs risk assessment based on 5 fundamental criteria, and its name is formed from the initial letters of these criteria:

DREAD ANALYSIS	
Damage Potential	How much damage can an attack cause to the target system? For example, if the database is compromised, will sensitive information be leaked? Or will the system be completely disabled? To prevent this, multi-layered security measures must be implemented on critical systems (e.g., access controls, data encryption).
Reproducibility	The ease with which the attack can be repeated is analyzed. For example, does an attack method yield successful results every time it is attempted? To address this issue, security vulnerabilities in the system must be regularly identified and patched (e.g., penetration tests and security patches).
Exploitability	This indicates how easy it is to carry out the attack. For example, does the attack require complex technical knowledge or special hardware, or can even low-level attackers do it? This requires the implementation of multi-factor authentication (MFA) systems, access authorization, and software security standards.
Affected Users	It indicates how many users or systems could be affected by the attack. For example, is it a small group of users or a wide-ranging impact? Therefore, the potential impact of damage should be limited through segmentation and permission-based access controls.
Discoverability	It assesses how easily the security vulnerability can be discovered. For example, is the vulnerability visible to everyone, or can it only be discovered through complex analysis? To prevent this, threats must be detected in advance using security vulnerability scanning tools and continuous monitoring systems.

1.

• Custodial institutions must protect entrusted assets and customer rights from loss and misuse, particularly in the event of bankruptcy.

• Operational controls, cyber resilience, and storage policies that minimize risks should be established.

• Accurate and up-to-date records of customer assets must be maintained, and these records must clearly show the customers' assets.

2. Segregation and Reuse of Assets

• Segregation: Entrusted crypto assets must be kept completely separate from the custodial institution's own assets.

• Reuse and Transfer of Ownership: The transfer of ownership or reuse of customer assets may only be carried out with the customer's prior explicit consent and comprehensive prior disclosure.

3. Outsourcing and Additional Risk- e Management

• If custody services are outsourced, similar security measures must be implemented, and customers must be informed accordingly.

• Additional risk management mechanisms must be implemented.

4. e Provision Transparency

Custody institutions must ensure transparency regarding the rights and obligations arising from custody agreements, security regulations, outsourcing, the use of omnibus accounts (accounts combining the assets of multiple clients), regulations concerning the reuse of client assets, and issues related to the risks that may arise from these practices.

5. e Measures for Multi-Functional Service Providers

• Organizations that provide custody services and other crypto asset services must identify, disclose, and manage conflicts of interest.

• The functions must be mandatorily separated or the business lines must be completely segregated.

6. Customer Protection and Financial Guarantee

• The protection and segregation of customer funds are required by regulators.

• Custodial institutions must have additional capital reserves or participate in guarantee mechanisms to provide compensation in the event of loss or theft of customer assets.

• They must provide insurance coverage to ensure the security of assets.

7. Emergency and Account Agreement

• IMF Recommendation: Custody institutions must establish an effective liquidation plan.

• IOSCO Recommendation: On-chain and off-chain reconciliations must be performed regularly and accurately.

8. Blockchain Network Security

The consensus algorithm and smart contract controls in the blockchain network where the custody infrastructure operates should be reviewed regularly, as updates may occur.

9. Zero Trust Architecture

Every access point must be continuously verified through authentication mechanisms. User, device, and application security must be controlled separately.

10. Artificial Intelligence-Powered Predictive Analytics

Cybersecurity threats should be predicted, and risks minimized using data-driven decision mechanisms.

A multi-layered approach is necessary to ensure the security of digital assets. This approach includes both technical security measures and the continuous evaluation of operational processes.

1. Security Metrics and Assessment

• Measurable security metrics are used in risk management. For example:
• System uptime ratio
• Update speeds against zero-day attacks
• Penetration test results
• Accuracy rate of anomaly detection systems

2. Continuous Security Assessment

• Security vulnerabilities in storage platforms should be regularly assessed and penetration tests should be performed.

• The system's security vulnerabilities should be continuously tested using methods such as Red Team and Blue Team exercises or Bug Bounty Programs. Under these programs, system owners offer rewards to white hat hackers (Ethical Hackers) to find and report security vulnerabilities. This way, vulnerabilities are closed and the security level is increased.[1]

3. Reporting and Addressing Vulnerabilities

• Weaknesses are proactively identified using attack simulations and predictive analysis systems.

• The remediation of these vulnerabilities is integrated with security models such as Zero Trust Architecture.

' Risk Management Policies for Storage Organizations

The risk management policies of custodial institutions consist of comprehensive strategic frameworks developed to ensure the security of digital assets, reduce operational disruptions, and enhance resilience against various threats. The risk management policies include:
1. Building block,
2. Risk identification,
3. Measurement,
4. Control and Monitoring
These processes are detailed to address technological, operational, legal, and market risks.

Technological Risks

Technological risks are risks directly related to the security of digital assets and are shaped primarily by the protection of private keys, the security of blockchain networks, and vulnerabilities in environmental infrastructure. Since control of digital assets depends on the integrity of private keys, security breaches in this area can lead to significant financial losses. Possible solutions and applications to ensure this are listed below.

1. Key Management Protocols

• Hardware Security Modules (HSM): Offline HSMs are used for the physical security of private keys. These devices protect keys from unauthorized access and automatically destroy data if tampered with.

• Multi-Signature (Multi-Sig) and MPC: Storing private keys in fragments and requiring approval from multiple authorized parties for transactions eliminates a single point of failure.

2. Two-Way Signing Systems and Time-Stamped Transactions

• Mutual Authentication: Secure communication between systems is ensured with mutual authentication, and third-party (man-in-the-middle) attacks are prevented.

• Multi-factor authentication (MFA): Used as an additional security layer in key management, reducing the risk of unauthorized access.

• Time-Stamped Transaction Approvals: Specific time intervals are defined for users to verify transaction details, and transaction monitoring mechanisms are integrated to enhance security.

3. Blockchain Security

• Smart Contract Audits: Smart contracts must undergo comprehensive security audits during the development phase. This process involves:

  • Code Review: Errors and vulnerabilities should be identified using manual and automated code analysis tools (e.g., Slither, MythX, Manticore).

  • Audit: Detailed smart contract audits should be performed by independent security firms.

  • Testing on Testnet: The security and performance of contract functions should be tested on the testnet before deployment to the main network.

  • Gas Optimization and Audits: High gas fees can sometimes be exploited in smart contract attacks; therefore, optimization should be performed.

• Zero-Day Attack Analysis: Proactive security measures should be taken to respond quickly to newly discovered vulnerabilities.

  • Upgradeable contract structures, such as proxy contracts, can be preferred to enable smart contract updates.

  • When security vulnerabilities are detected, emergency actions can be implemented using multi-signature (multisig) authorization mechanisms.

• Secure Distribution Processes: Before smart contracts are distributed to the blockchain, the security of the contract owner's keys must be ensured and unauthorized access risks must be eliminated.

Operational Risks

Operational risks arise from factors such as human error, process deficiencies, and system outages. These risks typically emerge due to weak corporate procedures and insufficient automation. Solution methods and applications can be listed as follows.

1. Automated Verification and Monitoring Systems

• Automated verification systems that minimize manual approval of transactions significantly reduce the error rate.

• Machine learning-based systems that detect suspicious transaction activities (Anomaly Detection) prevent potential operational errors with real-time alerts.

2. Role-Based Access Controls (RBAC)

• Each employee is only allowed to access information within their authorized scope on the system. Authorization levels are regularly reviewed and updated. Users should only have the permissions necessary to perform their duties.

3. Business Continuity and Emergency Plans

• Emergency response plans are activated in cases such as system outages or cyberattacks. Backup mechanisms ensure the availability of assets.

Legal Risks

Legal risks are risks arising from uncertainties and non-compliance during the process of complying with standards set by regulatory bodies.
The digital asset ecosystem is subject to different regulations around the world, making these risks unavoidable for custodial institutions. Below, we will list some solution methods and applications.

1. Compliance with Anti-Money Laundering (AML) and Counter-Terrorism Financing (CFT) Policies

AML stands for anti-money laundering. It encompasses policies, procedures, and regulations aimed at preventing criminal proceeds from entering the financial system through legal channels. CFT stands for countering the financing of terrorism. It refers to measures that detect, prevent, and punish money flows intended to finance terrorist activities. When used together, these two concepts refer to the legal compliance frameworks that financial institutions and digital storage service providers implement to prevent money laundering and terrorist financing. AML/CFT policies are particularly important in the field of crypto assets and digital storage services. In this context, processes such as customer identification procedures (KYC), suspicious activity reporting (SAR), suspicious transaction reporting (STR), and continuous monitoring of financial transactions are implemented.

• Know Your Customer (KYC): Custody platforms use robust KYC processes to verify customer identities and comply with AML/CFT policies.

• Suspicious Activity Reporting (SAR): Real-time analysis is performed using systems that detect potential money laundering activities, and reports are submitted to regulatory authorities. Financial institutions are required to report certain suspicious activities to the relevant authorities.

• Suspicious Transaction Reporting (STR): Detailed analyses are performed using systems that detect potential money laundering and terrorist financing activities, and suspicious transactions are reported to regulatory authorities. Financial institutions are required to report certain suspicious transactions to the competent authorities in a timely manner.

2. Risk Transfer

• Risk transfer agreements made with insurance providers to reduce legal risks provide compensation in the event of cybersecurity breaches or operational losses.

3. Compliance Programs with the Regulatory Framework

• Internal control mechanisms are established in line with regional regulations (e.g., MiCA, SEC, FCA)[2], and regular checks are carried out by independent audit firms.

Market Risks

Market risks include price fluctuations and liquidity risks arising from the highly volatile nature of digital assets. Rapid price changes in crypto asset markets may expose custodial institutions to the risk of value loss. Some solutions for this are listed below.

1. Dynamic Asset Valuation Methods:

• The market values of digital assets can be continuously monitored using real-time data streams and AI-powered analysis tools.

2. Portfolio Diversification:

• Custodial institutions can offer different types of digital assets in their clients' portfolios to balance volatility.

3. Hedging Strategies:

• Derivative products and option contracts can be used to hedge against market fluctuations.

4. Stress Tests and Simulations:

• Stress tests are conducted regularly to measure the impact of potential market shocks. These tests can assess the resilience of institutions during a crisis.

AML/CFT

Anti-Money Laundering (AML) and Counter-Terrorist Financing (CFT) controls in crypto custodial institutions are crucial for preventing illegal activities, ensuring international compliance, and adhering to local regulations. These controls require strict procedures and policies to manage financial and technological risks. In this sense, the main AML and CFT controls that can be implemented in crypto custodians begin with the implementation of know your customer (KYC) procedures. Under KYC, customer identity and address verification processes are carried out, risk levels are assessed, and risk profiles are created. A risk-based approach is adopted, whereby customer segmentation is determined, transactions from high-risk countries or regions are closely monitored, and additional investigations are conducted for high-risk transactions.

To track transactions, blockchain analysis tools and software are used to detect suspicious transactions through automated transaction monitoring systems, and reporting of these suspicious transactions to legal authorities is ensured. Additionally, compliance with international sanctions lists (OFAC, FATF, etc.) and blacklist checks are ensured. Applications that analyze transactions on the chain to detect illegal activities can be provided. In this regard, crypto custodians must also ensure that support service providers and business partners comply with AML/CFT standards.

In summary, implementing these controls at crypto custodians is critical both to ensure compliance with legal obligations and to enhance customer and market confidence. Crypto custodians must invest in both technology and competent, experienced compliance staff to meet AML and CFT requirements.

1. val (KYC) and Continuous Monitoring

KYC processes form the basis of AML/CFT policies. KYC involves custody service providers verifying customer identities and regularly updating this information:

• Identity and Address Verification: Digital storage institutions use technologies such as biometric verification and optical character recognition (OCR) to verify users' identity documents (passport, driver's license, national ID card, etc.) and address information.

• Risk-Based Assessment: Customers are classified as low, medium, or high risk based on their activities and transaction history. This classification is supported by real-time monitoring of customer behavior and risk scoring systems.

It should be noted that KYC processes are not a one-time application. Customer profiles and transaction activities are regularly analyzed to detect suspicious transaction patterns.

2. Detection of Suspicious Transactions with Blockchain Analysis Tools

Blockchain analysis tools enhance transparency in digital asset transfers and detect illicit activities by establishing the technical dimension of AML/CFT controls:

• Transaction Monitoring and Pattern Analysis: Blockchain-based analysis software (e.g., Chainalysis, Elliptic, and CipherTrace) monitors digital asset transfers in real time to detect abnormal transaction patterns.

• Risk Address and Blacklist Control: Transfers associated with risky or blacklisted addresses on the blockchain are automatically flagged, and the necessary reporting mechanisms are triggered.

• Detection of Fragmented Transfers: Microtransfers made using techniques such as "smurfing" for money laundering purposes are analyzed, and these transactions are examined as a combined model on the chain.

These tools provide effective solutions against threats such as "dark web" links, risky exchanges, and the use of fake identities.

3.

Digital asset custodians continuously evaluate customer activities using automated risk scoring systems as part of their AML/CFT policies:

• Risk Scoring Algorithms: Artificial intelligence and machine learning algorithms analyze customer transaction histories to generate dynamic risk scores.

• Suspicious Transaction Reporting (SAR/STR): Transactions deemed high-risk or suspicious are reported to regulatory authorities. The SAR (Suspicious Activity Reporting) mechanism is used in accordance with international AML standards.

4. International Regulatory Compliance (FATF Standards)

The effectiveness of AML/CFT policies is measured by compliance with international regulatory standards. In particular, the rules established by the FATF (Financial Action Task Force) provide a global framework:

• Travel Rule: The Travel Rule established by the FATF requires the collection and sharing of sender and recipient identity information in digital asset transfers. This prevents transfers from remaining anonymous, thereby limiting illegal activities.

• Regular Audits: Custody service providers are subject to periodic audits conducted by regulatory agencies. These audits assess the effectiveness of AML/CFT compliance policies.

5.

While implementing AML/CFT controls, data privacy must also be considered:

• Compliance with the Personal Data Protection Law (KVKK), General Data Protection Regulation (GDPR), and Other Data Protection Legislation: Customer data must be collected and stored in accordance with global data protection legislation.

• Transparency and Authorized Access: Data leaks and unauthorized access are prevented by ensuring that only authorized personnel can access customer information.

The assessments conducted by independent audit firms for digital asset custody services are based on internationally recognized standards.
The most commonly used ones include:

1. SOC 1/SOC 2 Reporting:

• SOC 1 (Service Organization Control 1): Tests the effectiveness of controls over financial reporting. This report provides assurance, particularly regarding the integration of digital asset custody services into financial systems.

• SOC 2 (Service Organization Control 2): Covers the auditing of technical elements such as security, access control, system integrity, confidentiality, and data protection. This report plays a critical role in evaluating the security of the infrastructure used to store digital assets.

2. ISAE 3000 (International Standard on Assurance Engagements): Based on International Assurance Standards, ISAE 3000 provides in-depth reviews in terms of data security, process accuracy, and compliance. The cybersecurity protocols and operational risk management of digital asset storage services are evaluated within the framework of this standard.

3. ISO 27001 Certification: Ensures the standardization of information security management systems. Under ISO 27001, digital asset storage service providers' data security policies, encryption techniques, and access control mechanisms are examined in detail.

4. Smart Contract Security and Code Review: Independent audit firms use code reviews and formal verification techniques to ensure smart contract security. The error tolerance, logical consistency, and resilience against cyber attacks of smart contracts used on blockchain-based platforms are analyzed. This process contributes to the elimination of security vulnerabilities and the sustainability of systems.

ic Areas Focused on During the Audit Process

Independent audit firms focus on the following areas when evaluating digital asset storage services:

• Cybersecurity Protocols: The accuracy of encryption methods, penetration testing, and network security assessments are performed.

• Operational Controls: Business continuity plans, system backup and recovery protocols are analyzed.

• Compliance Management: AML/CFT policies are implemented, KYC processes and data protection standards are monitored.

• Risk Management: We identify vulnerabilities, evaluate the effectiveness of risk mitigation strategies, and assess the adequacy of incident response plans.

In terms of security standards, the custodial institution utilizes the latest cybersecurity measures such as cold (offline) storage, multi-signature wallets, multi-party computation (MPC), biometrics, and hardware security modules. Protocols such as proof of reserves undergo regular audits. Additional layers of protection can be provided through insurance coverage. Security certifications such as ISO, SOC, and CCSS can also be considered important documents to obtain. Advanced cybersecurity measures include penetration testing, data encryption, defense against distributed denial-of-service (DDoS) attacks, and continuous monitoring activities to prevent breaches and data loss.

An independent audit is conducted to evaluate the processes, controls, and information systems that form the basis for the accuracy, integrity, and reliability of financial statements in custodial institutions.

In these audit procedures, it should also be noted that Proof of Reserves (PoR) alone is not sufficient to prove an institution's solvency or demonstrate that customer funds have not been misused, and that PoR must be supported by Proof of Liabilities (PoL), which shows the amount owed to depositors. Proof of Reserves (PoR): When considered as a mere snapshot, it can be manipulated. For example, funds can be borrowed immediately before the snapshot and returned to their actual owners afterwards. PoR must be fully audited and include continuous monitoring of blockchain addresses. This can be addressed by introducing minimum standards (e.g., audits) for PoR across the industry or by taking snapshots simultaneously (with the same timestamp) for all platforms.

Proof of Liabilities (PoL): It is important for measuring total customer deposits. However, it does not highlight off-chain or off-balance sheet liabilities, and these liabilities may remain hidden. Appropriate audits conducted by financial auditors can help resolve this issue, but there are limits to what an audit can achieve. Therefore, appropriate regulation and oversight are necessary as additional safeguards.

The following practices could be adopted in the name of asset management and transparency with potential regulations:

• Assets Under Custody (AUC): Crypto platforms can publish their assets under custody (AUC). Regulators can request access to AUC down to the individual account level and access the internal records of crypto platforms.

• Disclosure of Wallets on the Chain: CTPs can disclose their wallets on the chain, as many platforms do today. This information can be reconciled to determine whether the number of assets on the chain matches internal records.

Areas of Focus in Oversight Processes

1. Financial Reporting and Transparency: Regulatory bodies audit the financial condition and operational processes of custodial institutions at specific intervals. Periodic financial reports ensure transparency, accountability, and trust. Regulators, who analyze the financial condition of institutions in detail, determine the necessary actions to minimize the risk of bankruptcy.

2. Asset Segregation: Custodial institutions must keep customer assets separate from their own operational assets. This practice protects customer assets in the event that service providers encounter financial difficulties and prevents loss of trust.

3. AML/CFT Controls: AML (Anti-Money Laundering) and CFT (Countering the Financing of Terrorism) controls play a critical role in regulatory oversight processes. Custody service providers perform risk-based controls using KYC, suspicious transaction reporting (SAR/STR), and blockchain analysis tools.

4. Technological Surveillance and Risk Management: Regulatory agencies require automated monitoring systems, penetration tests, and real-time transaction audits. In this process, instant risk assessment tools are used to detect and prevent potential threats.

5. Licensing and Continuous Monitoring: Storage service providers must meet certain legal standards in order to operate. Regulatory bodies ensure the sustainability of service quality by implementing licensing processes as well as continuous monitoring and oversight mechanisms.

The Importance of Regulatory Oversight and the Impact of

Regulatory oversight ensures that digital asset custody services become more reliable, transparent, and sustainable. Strict oversight by regulatory bodies strengthens the climate of trust in the sector and allows investors to store their assets more securely. In particular, licensing and periodic compliance audits support sustainable growth in the sector by raising the quality standards of service providers.

Regulatory oversight also plays a role in promoting technological innovation. For example, regulators setting strict requirements in areas such as smart contract audits, blockchain security, and data privacy standards encourages service providers to develop more secure and innovative solutions.

Additional Security Measures

Ensuring the security of digital assets cannot be limited to basic security measures alone.
In today's world, multi-layered security measures play a vital role in countering increasing cyber threats and evolving attack techniques. Additional security measures include advanced encryption techniques, physical security, anomaly detection, predictive analytics, and verifiable encryption. These solutions work together to protect the confidentiality, integrity, and availability of digital assets.

Anomaly Detection

Anomaly detection is a security method used to identify abnormal behavior in digital asset systems. Unauthorized access, fraud, and security breaches are detected early, particularly through machine learning algorithms and big data analysis.

Technical solutions can be summarized as follows:

1. Machine Learning (ML) Algorithms: These analyze user transaction patterns to detect anomalies. For example, large amounts of asset movements or transactions made from different IP addresses are flagged.

2. Threshold-Based Detection: By defining threshold values such as transaction volume and geographic location, transactions that exceed certain criteria can be automatically stopped or require manual verification.

3. Real-Time Monitoring: System logs are analyzed in real time, and rapid intervention is provided when anomalies are detected.

4. Blockchain Analytics: Systems that track address movements on the blockchain are used to detect fraud or money laundering (AML/CFT) activities.

Predictive

Predictive analysis uses big data analytics and AI-based algorithms to anticipate potential risks and security threats in advance. Technically, possible threats can be neutralized using these technologies.

1. Big Data Analytics: Future threats are predicted by analyzing past transaction data. Risky addresses are identified by monitoring anomalous movements on the blockchain.

2. Behavioral Analysis: User behavior patterns are learned to detect anomalies. For example, a user who consistently accesses the system from the same IP address but then accesses it from another country is flagged as exhibiting risky behavior.

3. Dynamic Risk Scoring: A dynamic risk score is created for user wallets and transactions, and high-risk transactions require additional verification.

4. Proactive Security Measures: AI-based prediction systems analyze risky scenarios in advance, enabling security measures to be proactively implemented.

The Future and Development of Storage Solutions e Areas

As the adoption rate of digital assets increases, it is inevitable that storage services will keep pace with this trend. Storage solutions that are considered reliable in traditional financial systems are being redefined by the innovations brought about by blockchain technology. User needs in terms of security, ease of access, and operational costs will play a critical role in the design of future storage solutions. In this context, new technologies and solutions are expected to be developed to meet the demands of both individual and corporate users.

Areas of Development

1. User-Friendly Storage Solutions

With the proliferation of digital assets, existing storage methods that require technical knowledge remain limited in terms of accessibility to the general public. Therefore, storage solutions that improve the user experience and reduce technical barriers will increasingly come to the fore.

• Automatic Key Management: Solutions will be developed that securely store users' private keys and minimize the risk of loss through automatic backup mechanisms.
Splitting keys into parts and distributing them across different security levels will offer both ease of use and security.

• Social Recovery Mechanisms: Social recovery solutions that enable users to recover access through friends, family members, or trusted third parties in the event of key loss will become widespread.

• Biometric Authentication: Biometric authentication technologies such as fingerprint, retina scanning, or facial recognition, instead of traditional passwords, will increase security while providing users with easy access to their digital assets.

• Cross-Chain Compatibility and Integration: The need for compatibility between different blockchain networks is becoming increasingly important. Users are turning to wallets that allow them to manage various digital assets, from Bitcoin and Ethereum to new altcoins, in a single interface.

• AI and Machine Learning Integration: The use of artificial intelligence (AI) and machine learning technologies in crypto wallets is increasing. AI-powered analysis tools enhance the user experience by providing investment insights, risk analysis, and automated trading recommendations.

2. Scalability

Scalability, one of the biggest challenges of blockchain technology, is also a critical area of development for storage services.
Innovative technologies are being developed to enable current storage solutions to cope with increasing user numbers and transaction volumes.

• MPC: Instead of storing private keys in a single location, splitting them into different parts and distributing them geographically has the potential to provide scalable security. MPC-based solutions enable transaction approval by processing key fragments on different sides.

• Layer-2 Solutions: Layer-2 solutions (e.g., rollup technologies) will be used to increase the scalability of blockchain networks. These solutions will enable fast and low-cost transactions by reducing the transaction load on the main blockchain.

• Hybrid Storage Structures: Hybrid solutions, which combine both on-chain (on the blockchain) and off-chain (outside the blockchain) data storage methods, will increase fast access and scalability without compromising security.

3. e Storage Solutions for Enterprises

Institutional investors' interest in the digital asset market is increasing demand for reliable and compliant custody services. Institutional custody solutions designed specifically for large-scale investors prioritize operational efficiency and risk management.

• Risk Management and Compliance: AML/CFT controls and KYC processes are strictly enforced in institutional custody services. Custody service providers must develop audit mechanisms and reporting systems to ensure regulatory compliance.

• Insured Custody Solutions: The insurance of digital assets creates an element of trust for large-scale investors. Institutional solutions will offer risk transfer mechanisms against potential losses by integrating with third-party insurance providers.

• Programmable Security and Smart Contracts: Implementing automated security policies with smart contracts will reduce operational costs and make risk management more effective in corporate custody services. For example, multi-signature mechanisms can be used to approve transactions according to different levels of authority.

4. Decentralized Custody Initiatives

As an alternative to traditional centralized custody solutions, decentralized custody models embrace the principle of decentralization, one of the fundamental principles of blockchain technology.

While traditional custody services rely on a centralized structure, decentralized solutions operate with distributed and trustless systems. This allows users to have full control over their assets while eliminating single points of failure.

Future Expectations for Decentralized Custody ( )

The rapid growth of decentralized finance (DeFi) and Web3.0 ecosystems is increasing demand for decentralized storage solutions for managing digital assets. This development will enable individual and corporate users to turn to more secure, accessible, and intermediary-free solutions. Decentralized technologies will bring significant innovations in terms of security and flexibility while offering users full control over their assets.

1. Self-Custody Platforms

Self-custody platforms are storage solutions where users manage their own private keys. Since central intermediaries are eliminated in these systems, security risks are significantly reduced.

• Users store and control their private keys through their own wallets. Hardware wallets and software wallets form the basis of self-custody solutions.

• Enhancing the security of keys through multi-factor authentication (MFA) and split key management elevates self-custody solutions to a higher level.

This allows users to have full control over their assets and eliminates the risk of centralized attacks.

2. e Storage Based on DAO

Decentralized autonomous organizations (DAOs) allow users to manage storage services through community-based decision-making mechanisms. DAO-based storage solutions combine a collective security approach with a democratic management model.

• In a DAO structure, decision-making processes for storing digital assets are automated through smart contracts. Security is ensured using multi-signature mechanisms and MPC technologies.

This eliminates single points of failure and enables transparent community control.

3. -Splitting of Cryptographic Keys

Cryptographic key splitting techniques enhance the security of private keys by eliminating the risk of attack from a single point.

• Using mechanisms such as Verifiable Shamir Secret Sharing (SSS), keys are split into multiple parts and stored in different locations. Access to the entire key requires combining a specific number of parts.

• While ensuring decentralization, this prevents individual losses. For example, configurations such as 3 out of 5 (combining three out of five pieces) can be implemented.

In self-custody platforms and institutional storage solutions, storing keys in geographically distributed secure systems makes this method more effective.

The Impact of Legal Regulations on Storage Services

The rapid growth of the digital asset market and the transformation of the financial ecosystem have made it imperative for regulatory bodies to strictly supervise custody services. International regulations establish new obligations and operational standards for service providers.
While regulations aim to enhance the security of digital assets, they also require service providers to adopt high standards in terms of transparency, risk management, and consumer protection.

1. Transparency Requirements

Transparency is a requirement strictly demanded by regulators. Custodians must periodically report on the status of customer assets and undergo transparent financial audits.

Technical Requirements:

• Reporting Standards: International reporting frameworks (SOC 1/SOC 2, ISAE 3000) and independent audits require custodial services to present their financial and operational status to regulators.

• Blockchain-Based Verification: Real-time proof of reserves solutions on the blockchain can be used for transparency. This allows for continuous monitoring of the accuracy of customer assets.

• Impact: Transparency requirements necessitate that custody service providers automate their regular reporting processes and upgrade their technological infrastructure. This enhances service quality and strengthens customer trust.

2.

Regulations require that customer assets be completely segregated from the custodial service provider's operational accounts. This practice ensures that customer assets are protected in the event that the service provider experiences financial difficulties.

Technical Applications:

• Segmentation and Tracking: Customer assets are tracked separately on the blockchain through different wallets or sub-accounts. This method both reduces operational risks and ensures transparent management of customer assets.

• Smart Contracts: Using self-custody or DAO-based solutions, customer assets are automatically and verifiably segregated.

• Digital Identity and Traceability: Customer asset movements are recorded in detail, ensuring KYC/AML compliance.

• Impact: Asset segregation enhances customer security while enabling service providers to establish a more robust infrastructure in terms of operational transparency and legal compliance.

3. Insurance and Risk Management

Regulations require custody service providers to provide financial guarantees and offer insurance coverage to customers. These practices are vital, especially for minimizing the risks of institutional investors.

Technical Solutions:

• Cyber Insurance Policies: Insurance coverage is provided for storage services against cyber attacks or key loss situations.

• Risk Transfer Mechanisms: Service providers share financial risks by entering into agreements with third-party insurance companies and risk management platforms.

• Dynamic Risk Scoring: Using machine learning and big data analytics, dynamic risk scoring is performed for customer accounts, and risky transactions are automatically detected.

• Impact: Insurance solutions prevent potential financial losses while providing institutional investors with a secure entry into the market.

4. al Integration of Regulatory Compliance

The regulatory compliance process requires custody service providers to make their technological infrastructure compliant and flexible.

• RegTech Solutions: Regulatory technology (RegTech) applications automate AML/CFT controls and streamline suspicious transaction reporting (STR) and compliance reporting processes.

• Smart Audit Systems: Blockchain-based verifiable encryption and traceable verification mechanisms enable regulators to review transactions transparently and in real time.

• AI and Predictive Analytics: AI-powered risk analysis and anomaly detection systems are integrated to ensure regulatory compliance.

B. LEGAL FRAMEWORK FOR CRYPTO ASSET STORAGE PROCESSES

The crypto asset market has focused on one particular crypto asset service over the past year: crypto asset custody. Stablecoins, CBDCs (Central Bank Digital Currencies), the tokenization of real-world assets (RWAs) such as stocks, bonds, commodities, and real estate, and new innovative use cases such as ETFs (Exchange Traded Funds) have increased institutional interest in digital assets across banking and financial institutions.
The adoption of Bitcoin and Ether ETFs, in particular, has triggered increasing acceptance in the mainstream financial sector. Although the current crypto custody market is still relatively small, the sector is reported to be growing at an annual rate of 30%. All these developments have increased institutional demand for regulated, secure, and resilient custody services.
.[1]

1. The Importance of Defining the Legal Framework in Crypto Asset Custody Processes

Custody is a concept that generally refers to the process of holding assets on behalf of third parties and often includes managing them. The custodian is responsible for securely holding the assets entrusted to them and ensuring legal certainty over them.

In many cases, custodial institutions do more than just safeguard assets; they also manage the accounts or transactions of the depositor, including activities such as dividend collection, regulatory compliance, and lending.[2] In traditional finance, custodial institutions have held assets electronically or physically on behalf of end users since the 1940s. However, the dynamics of emerging decentralized finance (DeFi) are quite different from traditional finance and the mechanisms used there.

The storage of crypto assets is one of the current issues in the regulation of DLT (Distributed Ledger Technology)-based transactions. New regulations on storage are rapidly developing in Turkey and around the world. There is no globally and uniformly defined regulatory legal framework for crypto assets. Therefore, the services offered by crypto asset storage wallet providers and even the scope of the concept of crypto asset storage can vary greatly. In countries with regulations, the rules in force regarding storage
[3] In particular, crypto
Before discussing the current situation in countries where asset activities are booming and the custody regulations in these countries, it would be appropriate to explain why it is important to address the issue of crypto asset custody in the legal sphere:

Since Bitcoin entered our lives, the crypto asset world has witnessed periods of ups and downs at various times.

1 *Carlo R. W. De Meijer, Traditional financial custodians enter the crypto market (October 21, 2024) https://www.finextra.com/blogposting/27059/traditional-financial-custodians-enter-the-crypto-market#:~:text=The%20growing%20institutional%20interest%20across,institutional%20demand%20for%20regulated,* ure **2** *World Federation of Exchanges, Crypto-Asset Custody: A Blueprint for Regulatory and Operational Excellence (August 28, 2024), https://www.world-exchanges.org/storage/app/media/Cally%20Billimore/Custody%20of%20Crypto-Final.pdf, p. 3.*

3 *World Federation of Exchanges, p. 2.*

In particular, the losses incurred during the period between 2021 and 2023, which led to the "crypto winter" and amounted to millions of dollars, have shaken confidence in crypto assets and distributed ledger technology. The malfunctions and losses experienced with crypto assets are actually closely related to the storage of crypto assets.

In a jurisdiction where there are no regulations on the storage of crypto assets, crypto asset service providers are free to use different methods to store their customers' assets. While some providers prefer hot and cold wallets under their own control, others can increase security levels by working with third-party storage companies that produce storage solutions that do not create operational problems, and may even resort to insurance solutions for customer assets.

The International Monetary Fund (IMF) highlights the weaknesses that contributed to the FTX scandal in a policy paper, drawing attention to the lack of legal regulations for custody services or their inadequacy: "The multifunctional and
activities (such as brokerage, trading, and custody services) are not subject to regulation and oversight. In the case of FTX, these integrated offerings led to leveraged lending to customers, liquidity mismatches, and subsequently higher withdrawal requests ."[4]

A recent study conducted in 2024 identified some fundamental issues related to custody activities that have shaken the confidence of crypto asset investors.

Accordingly, organizations offering crypto asset custody services have failed to prevent the loss of their customers' private keys. Furthermore, they have failed to develop adequate custody policies against threats such as cyber risks, misstatements, and internal and external theft. In addition, crypto asset custody services have been combined on the same balance sheet with risky activities such as brokerage, investment, and lending by cryptocurrency exchanges, leading to widespread conflicts of interest and jeopardizing the stability of crypto asset custody services.
Another important point to consider is that institutions providing custody services are unable to prevent the assets of many customers from becoming mixed with their own assets, and the identity of the owner of these assets has become undeterminable. Finally, custodial service providers have used customer assets for trading on their own accounts or on the accounts of an affiliated entity. They have offset particularly high losses with the assets entrusted to them for safekeeping. Even today, many custodial service platforms reserve the right to reuse assets entrusted to them for their own investment or business purposes.
.[5]

The events that have occurred in the crypto asset ecosystem, some of which have reached the scale of global scandals, have revealed the following realities: If customer assets are not adequately protected within the scope of custody activities, significant losses may occur. During the period we have mentioned, developments regarding the legal nature of crypto assets and the legal rules to be applied to them under enforcement and bankruptcy law were still taking shape. The rules regarding the determination of rights over crypto assets, which are lacking in most jurisdictions but are developing, and the rules to be applied in the event of bankruptcy have fallen short in providing adequate special protection for token holders.

4 *IMF, Elements of Effective Policies for Crypto Assets (February 13, 2023), https://www.imf.org/en/Publications/Policy-Papers/Issues/2023/02/23/Elements-of-Effective-Policies-for-Crypto-Assets-530092, p. 39.*

5 *Dirk Zetzsche, Julia Sinnig, Areti Nikolakopoulou, Crypto custody, Capital Markets Law Journal, Volume 19, Issue 3, July 2024, Pages 207–229, https://doi.org/10.1093/cmlj/kmae010, p. 209*

For this reason, international policymakers and legislators have turned their attention to creating regulations for crypto asset custody platforms. Indeed, as of 2022, organizations such as the IMF, IOSCO, and FSB have put crypto asset custody under the microscope and identified issues requiring greater sensitivity, calling for them to be prioritized:

The IMF emphasizes the importance of crypto asset service providers operating in a licensed or authorized manner. It is stated that institutions offering activities such as the storage, transfer, exchange, and safekeeping of reserves and assets should be subject to rules similar to those applied to financial service providers, along with additional requirements appropriate to new business models (such as combined exchanges and wallets).[6]

The IMF Fintech Notes 2022 highlights some important points regarding custody services provided by wallet providers. Accordingly, the provision of custody services by wallets is a critical element, particularly for the unbacked crypto **asset** ecosystem, and it is important that they are positioned in a robust manner from a regulatory perspective. In this context, unlike single-function crypto exchanges, they will need to take some additional measures, and thus stricter regulations may be required. In this regard, the IMF emphasizes the need to keep funds and crypto assets separate from the institution's own funds and assets.

Without the explicit consent of customers and unless an appropriate compensation procedure is established, the reuse of customer assets and funds or their use in lending activities should not be permitted. In this context, users' wallet addresses must be different from the platform's own wallet addresses. In addition, platforms must have established an effective emergency management procedure. The reporting of operational or cyber incidents must be timely and accurate to ensure market integrity. When cyber or operational processes are outsourced to third parties, the wallet provider should be responsible for any incidents that occur. Wallet providers should share changes in their assets with their users upon request or at regular intervals. Platforms must comply with the AML/CFT standards set forth by the FATF. In addition, regulatory frameworks may include provisions regarding insurance coverage in the event of a cyber attack, with the aim of reducing risks for consumers. Furthermore, the IMF notes that the proper segregation of customer funds can reduce customer losses in the event of a firm's bankruptcy, and that working with third-party providers and maintaining critical information technology infrastructure are also important. Finally, it emphasizes the importance of prioritizing user interests, especially when the platform performs different functions, and of explaining this to customers within the framework of transparency and information obligations when a conflict of interest arises.
IMF, Policy Paper- Elements Of Effective Policies For **Crypto Assets, February** 2023, p. 22.

6 *IMF, Policy Paper- Elements Of Effective Policies For Crypto Assets, February 2023, p. 22.*

7 *Unbacked crypto assets are crypto assets that are not backed by any physical asset or collateral processed on distributed ledger technology. These assets are generally designed to be transferable and used as a means of payment. The best-known examples are Bitcoin and Ether.*

8IMF Fintech Notes: Regulating the Crypto Ecosystem The Case of Unbacked Crypto Assets Parma Bains, Arif Ismail, Fabiana Melo, and Nobuyasu Sugimoto, 2022

In Section 7 of its Recommendations prepared at the end of 2023, IOSCO provides suggestions and supporting guiding principles regarding risks related to the safekeeping of customer funds and assets. It is stated that these risks particularly relate to the segregation of assets, their reuse, and issues concerning liability and ownership. The IOSCO Recommendations also address the control mechanisms that must be implemented by crypto asset service providers and the principles governing the custody of crypto assets within this scope.

Recommendation 12 highlights that custody platforms that have been attacked in the past and/or have lost access tools to customer assets they are responsible for protecting must ensure the proper custody of customer assets. This depends on the strength of a platform's policies, procedures, and controls, including access tools such as private keys and wallets. A platform offering custody services should organize sufficient policies, procedures, and regulations around the risks associated with different wallet types (e.g., hot and cold) to minimize the risk of customer assets being lost, stolen, or inaccessible. Therefore, regulatory authorities should assess whether a platform can compensate its customers for their losses in accordance with applicable laws in the event of theft or loss of customer assets, and how it can do so.
Regulators must require that a CSD ensure the adequate protection of customer assets, including when they are placed with a third party selected by the platform, with the aim of minimizing the risk of loss or misuse at all times.

As with traditional financial assets, regulatory authorities should require accurate and up-to-date records and accounts that determine the amount, location, and rights status of customer assets. Consequently, sufficient, reliable, and transparent information should be provided to customers and third parties (e.g., the authority conducting insolvency proceedings, regulatory authorities, and courts) to ensure that customers can exercise their rights regarding their assets, particularly to recover the assets they have deposited or their equivalent value.[10]

Recommendation 13 concerns the segregation of customer assets by platforms offering custody services from their own proprietary assets and from the assets of any affiliates or service providers they incorporate into their operations. With this recommendation, IOSCO highlights the importance of a platform specifying how customer assets are protected against loss or misuse and how such assets are segregated as customer assets that are not subject to the claims of the platform's creditors. It is stated that in order for the platform to be able to use customer assets for purposes such as lending, the customer must be informed in a language they can understand and their explicit consent must be obtained, ensuring that they understand the risks involved.[11]

Recommendation 14 indicates that if a crypto asset service provider enters into a sub-custody relationship with a third party, the terms of the contractual arrangements for this sub-custody relationship and the additional risks they may pose to the customer must be specified in detail.[12]

9 *The Board of the International Organization of Securities Commissions (IOSCO), Policy Recommendations for Crypto and Digital Asset Markets Final Report (November 16, 2023), pp. 33-39*

10 *The Board of the International Organization of Securities Commissions (IOSCO), Policy Recommendations for Crypto and Digital Asset Markets Final Report (November 16, 2023), p. 33.*

11 *IOSCO, p. 34.*

12 *IOSCO, p. 35.*

The FSB highlights the following point: As seen in cases such as TerraUSD/LUNA, Celsius Network, and FTX, most failed market participants have undertaken functions quite similar to those in traditional finance (TradFi). These functions, carried out without appropriate governance structures or regulatory compliance, created vulnerabilities identified by the FSB. In light of these lessons learned, the FSB states that it has strengthened both sets of high-level recommendations in three areas. The first relates to the protection of customer assets. Financial service providers that hold or control customer assets must ensure that these assets are effectively segregated from their own assets. Secondly, the FSB states that authorities must have certain requirements in place to address risks associated with conflicts of interest. In this context, crypto asset service providers, including affiliated entities that combine multiple functions and activities, should be subject to appropriate regulation, oversight, and supervision or be brought into compliance. This includes the legal separation of certain functions where appropriate. Finally, the FSB points out that crypto asset issuers and service providers may seek to avoid regulation and oversight by moving to jurisdictions with less stringent regulation. Therefore, the FSB's high-level recommendations include the level of compliance for activities spread across multiple jurisdictions, particularly those in jurisdictions that do not apply international standards.
has been strengthened in terms of information sharing, including.[13]

The World Federation of Exchanges, in its 2024 study, states that the fundamental problem in the storage of crypto assets is determining whether the crypto assets stored by the storage platform belong to the platform itself or to the customer (the actual or legal person storing them) in cases where the storage platform fails. In this context, the study examines how the concept of custody has evolved from the past to the present and makes recommendations on the legal framework that regulatory authorities should establish. In the event of the bankruptcy of platforms offering crypto asset custody services, it is crucial that customer assets are segregated. In fact, customer assets should be excluded from bankruptcy, meaning they should be kept separate from the real or legal person's assets. Cyber risks must be prevented by establishing a well-thought-out technology architecture and implementing mature cybersecurity programs. Existing or potential conflicts of interest must be managed adequately and effectively. Risks existing for customers must be explained to them in a clear and understandable manner. It is important that insurance policies are adequate and communicated to customers in a clear and understandable way. Finally, requesting independent audits from reputable and reliable auditors to ensure the evaluation of financial statements, processes, and controls can prevent significant losses in the future·

13 *FSB Global Regulatory Framework for Crypto-Asset Activities Umbrella public note to accompany final framework (July 17, 2023) https://www.fsb.org/uploads/P170723-1.pdf pp. 5–6.*

14 *World Federation of Exchanges, pp. 5-11.*

Based on policy documents prepared by organizations such as the IMF, FSB, and IOSCO, and the regulations proposed in MiCA regarding custody, some authors **have concluded** that regulations on custody activities are essential in the following areas:

• Entities engaged in custody activities must take measures to protect the assets entrusted to them for custody and the rights of their customers against the risk of loss and misuse, particularly in the event of insolvency.

• Organizations engaged in storage activities must implement the necessary control mechanisms to minimize operational and cyber resilience risks.

• Accurate and up-to-date records of customer assets must be maintained.

• Crypto assets must be kept separate from the custodian's own assets.

• Arrangements for the transfer of customer assets and the reuse of customer assets require the customer's prior explicit consent and the fulfillment of the obligation to provide information on this matter.

• When custody activities are outsourced, the same safeguards and risk management measures must still be implemented.

• The institution engaged in custody activities must be transparent regarding the rights and obligations arising from the custody agreement.

• Cryptocurrency service providers that perform multiple functions, including custody, must identify, disclose, and manage any conflicts of interest.

Following this general information on the custody of crypto assets, this part of our study will provide information on the current situation regarding the steps taken in Turkey and around the world, particularly in countries that are leaders in the crypto asset ecosystem.

2. 's Situation in Turkey

The fundamentals of storing crypto assets in Turkey, as in many countries, are based on the custody agreement, which is applied in traditional finance and particularly in banking law. According to Article 561 of the Turkish Code of Obligations, a custody agreement is a contract whereby the custodian undertakes to keep a movable property entrusted to them by the depositor in a safe place. The depositary may charge a fee if this is expressly stipulated or if the circumstances and conditions so require. According to Article 568 of the same Code, even if a third party claims a right in rem over the deposited item, the depositary is obliged to return it to the depositor unless it is seized or a claim for recovery is brought against the depositary. The safekeeping of money and valuable documents is further regulated in Article 570 of the Code, titled "Safekeeping of fungible items." Accordingly, if it has been expressly or implicitly agreed that the custodian shall return the money entrusted to them in kind without being obliged to return it in the same amount, the benefit and loss of that money shall belong to them. Money left unsealed and open is considered an implied agreement. The depositary may not dispose of other fungible items or valuable documents entrusted to them unless expressly authorized by the depositor.

15 *Dirk Zetzsche, Julia Sinnig, Areti Nikolakopoulou, Crypto custody, Capital Markets Law Journal, Volume 19, Issue 3, July 2024, Pages 207–229, https://doi.org/10.1093/cmlj/kmae010, p. 211 ff.*

While the Law of Obligations establishes the fundamental principles of custody agreements, more detailed and sometimes differing practices regarding custody agreements exist, particularly in the context of banking transactions.

As in many countries around the world, Turkey is evolving from traditional finance towards decentralized finance. Cryptocurrency exchanges operating in Turkey not only enable users to buy and sell cryptocurrencies but also offer custody services. Local exchanges use various security protocols and technological solutions to ensure users can store their cryptocurrencies securely. In addition, independent storage service providers are companies that specialize in the secure storage of crypto assets. These companies use cold wallets, multi-signature protocols, and other security measures to securely store users' assets. There are companies operating in this field in Turkey that offer services that comply with international standards.

Until July 2024, there was no legal framework regulating crypto asset custody activities, nor had this been addressed in any previous legislation. The custody of crypto assets was covered under Article 4/2 of the Regulation on the Non-Use of Crypto Assets in Payments, which came into force in 2021, as one of the activities that payment and electronic money institutions could not engage in: Payment and electronic money institutions cannot act as intermediaries for platforms offering crypto asset purchase, sale, custody, transfer, or issuance services or fund transfers made through such platforms. The meaning of the term "custody" used here was not specified.

However, some studies on custody activities offered recommendations in line with the sector's needs. For example, a report published by the Turkish Banks Association in 2022 stated: "The storage of digital assets by licensed custody institutions and the establishment of institutional counterparties in the market will have a positive impact on investors in terms of reducing complex processes and risks and increasing reliability. On the other hand, banks starting to provide custody services, which will enable them to become active players in the digital asset market, will contribute to their gaining new customers at an increasing rate, reaching young customer groups, designing new or hybrid products with traditional banking products, and gaining a competitive advantage through technology. In addition, custody services and integration into the crypto ecosystem are likely to add value to banks in numerous areas, including new customer acquisition, growth, visibility, innovative brand image, and many others. On the other hand, the same report also highlights the risks and challenges that may arise if banks provide this service: "The main ones are: the complex and multi-stage nature of the processes, KYC/AML processes, traceability, and Disagreement issues, volatility in transaction volumes, the risk of becoming a target for attacks due to the large value of assets held in custody, ensuring cybersecurity, increased costs arising from risk control and insurance, etc., and the absence/uncertainty of regulations (how to ensure the security of assets and the classification of assets, etc.) can be listed as examples.

The legal framework for crypto asset custody services in Turkey is shaped by regulations set by the Capital Markets Board (CMB), the Banking Regulation and Supervision Agency (BRSA), and the Financial Crimes Investigation Board (MASAK).

16 *Turkish Banks Association, Overview of Banking in Relation to Digital Assets, Potential Business Models, and Legal Assessment of Digital Assets (07.02.2022), p. 23*

The Capital Markets Board (CMB) has been granted the authority to supervise and regulate the activities of crypto asset custody service providers under Law No. 6362 on the Capital Markets, as amended by Law No. 7518 on Amendments to the Capital Markets Law, which entered into force on July 2, 2024. The CMB sets the necessary standards and obligations regarding the custody and management of crypto assets, and also aims to ensure the legality of these services and market transparency.

The Capital Markets Law (CML) Article 3 defines the concepts of crypto asset service provider, crypto asset custody service, and platform. Accordingly, crypto asset service providers include platforms, institutions providing crypto asset custody services, and other institutions designated to provide services related to crypto assets, including the initial sale or distribution of crypto assets, in regulations to be issued based on this Law. The same article also provides a definition of what is meant by a crypto asset custody service. In this context, a crypto asset custody service refers to the storage, management, or other custody services to be determined by the Capital Markets Board of the crypto assets of platform customers or the private keys that grant the right to transfer these assets from the wallet.

According to Article 35B/4 of SerPK, the procedures and principles regarding the purchase and sale of crypto assets through platforms, the initial sale or distribution of crypto assets, the exchange, transfer, and custody of crypto assets are regulated by the Board.

According to SerPK 35C/6, it is essential that platforms hold their customers' crypto assets in their own wallets. The custody service for crypto assets that customers prefer not to hold in their own wallets must be provided by banks authorized by the Board in accordance with the regulations to be issued by the Board and deemed appropriate by the Banking Regulation and Supervision Agency, or by other institutions authorized by the Board to provide crypto asset custody services, and customers' cash must be held in banks. Crypto assets held at banks and customer cash within this scope are not subject to the provisions on deposit and participation fund insurance set forth in Article 63 of Law No. 5411. The Board is authorized to establish separate principles for custody for each crypto asset or based on their underlying technological features or the nature and quantity of crypto assets.

Pursuant to SerPK Article 35/C/7, customers' cash and crypto assets are separate from the crypto asset service providers' assets, and records are kept in accordance with this provision. Under no circumstances may the cash and crypto assets held by crypto asset service providers on behalf of customers be seized, pledged, included in the bankruptcy estate, or subject to precautionary measures, even if such assets are subject to public claims due to the debts of the crypto asset service providers or the debts of the customers. The provisions of paragraphs 7 and 8 of Article 46 of this Law regarding the holding of customer cash in banks by crypto asset service providers shall also apply to crypto asset service providers.

With the entry into force of the law amending the Capital Markets Board (CMB), the CMB has published a series of guidelines, statements, and policy decisions and has collected applications from companies currently operating in the crypto asset ecosystem and those wishing to operate in it.

The Capital Markets Board (CMB) has published a list on its website for the purpose of informing the public about institutions that have declared they will operate in accordance with Provisional Article 11 of SerPK. In this context, as of March 2025, the organizations listed do not necessarily mean that they are authorized under the relevant legislation, but there are eleven organizations with "custody application" written next to their application.

Following the amendments to the Law, the CMB has continued to regulate the crypto asset ecosystem through policy decisions and announcements. In this context, the Capital Markets Board Decision Body's Policy Decision No. i-SPK.35.B.1 (dated 19/09/2024 and numbered 1484) contains points that also concern custody:

• Article 35/C of the Capital Markets Law
Paragraph 6 stipulates that customer cash must be held in banks; paragraph 7 of the same article stipulates that customer cash and crypto assets are separate from the crypto asset service provider's assets and that records must be kept in accordance with this provision. Paragraph 7 of Article 46 of the Law stipulates that customer cash held at banks must be tracked in a separate account opened for platform customers, separate from the platform's own cash assets. In this context, cash transfers of platform customers must be carried out through banks or institutions authorized for this purpose in accordance with the relevant legislation. Platforms cannot accept customer cash in person, deliver it to the customer in person, or store it in any way on their premises.

• Except for the environments or methods deemed appropriate in Article 2, such as the purchase and sale of crypto assets, initial sale or distribution, exchange, transfer, storage operations required for these, or the conversion of customers' crypto assets into cash or cash into crypto assets, etc., shall be considered as commercial or professional activities within the scope of Articles 99/A and 109/A of the Law.

• The provisions outlined in Section 7/b(a) also apply under capital markets legislation. Considering that the custody infrastructure and reserve proof mechanisms for crypto assets are not yet operational, prior to the Authority issuing regulations regarding the issuance of capital market instruments as crypto assets in accordance with Article 13 of the Law, Capital market instruments defined in Article 3 of the Law and indices determined in relation to capital market instruments, baskets combining various asset groups (including crypto assets), precious metals, and crypto assets based on the underlying assets regulated in VII-128.3 on Warrants and Investment Institution Certificates, cannot be issued as crypto assets or listed on platforms.

• If crypto assets are not stored in customers' own wallets, control over the keys to the wallets where crypto assets held in customer accounts are stored must be maintained on the platforms by no later than November 8, 2024. Any practices contrary to this provision shall be evaluated under Article 110/A of the Law.

Currently, companies that undertake to provide crypto asset storage services must apply to the CMB and submit certain documents. This application is not a license application for crypto asset storage, but rather a commitment to engage in such activity.

Within the scope of this application, certain documents pertaining to partners, board members, the CEO, and deputy CEOs shall be submitted. These documents shall cover the information systems infrastructure used by the applying Company, processes and tools related to the protection of customer assets, processes related to the recording of transactions in the blockchain system, and documentation related to AML/CFT systems or reporting to public authorities, etc. integration with internal and external systems, operational and reporting processes, documents related to the functioning of risk management processes, the functioning of the custody system for crypto assets and customers' cash assets, services used for the custody of crypto assets, and the wallet technologies used for custody processes.
The documents must be submitted.[17] Thereafter based on the evaluation to be conducted by the CMB, the relevant Company may be permitted to be included in **the list of** entities engaged in custody services.

Communication on the Establishment and Operating Principles of Crypto Asset Service Providers (III-35/B.1), published in the Official Gazette on March 13, 2025, Communication on the Working Procedures and Principles of Crypto Asset Service Providers (III-35/B.2), Communication on Independent Audit of Information Systems (III-62.2.b), and the Circular on Procedures and Principles Regarding Information Systems Management (VII-128.10) issued by the Capital Markets Board contain the most comprehensive and detailed regulations on custody to date in Turkey.
The regulations, which contain rules, principles, and fundamentals for various institutions such as banks providing custody services and crypto asset service providers, have been quite explanatory in terms of understanding the scope of custody activities. The purpose of the Communiqué on the Establishment and Operating Principles of Crypto Asset Service Providers (III-35/B.1) is to regulate the procedures and principles regarding the establishment, commencement, operation, and suspension of operations of crypto asset service providers.

Article 4 of the Circular defines crypto asset custody activities as "the storage, management, or other custody services determined by the Board, which provide the right to transfer customers' crypto assets or the private keys associated with these assets from the wallet." Articles 5, 6, and 7 of the Communiqué specify the conditions for companies that will provide crypto asset custody services, while Articles 9 to 19 specify the conditions required to engage in crypto asset custody activities.

Crypto asset custodians must include the names of the platforms they have agreements with on their websites, list the crypto assets for which they provide custody services, and keep this information up to date. This allows for transparent oversight of which companies utilize crypto asset custodians.

According to Provisional Article 1 of the Communiqué, custody institutions listed on the CMB's website under the "List of Active Institutions" as of March 13, 2025, i.e., the date of publication of the Communiqué, and custody institutions that have submitted an application in advance on the date of publication of this Communiqué must apply for an operating license by June 30, 2025.

Communication on the Working Procedures and Principles of Crypto Asset Service Providers and Capital Adequacy (III-35/B.2) clearly stipulates the services and activities that crypto asset service providers may offer, the principles related to these, the listing principles for crypto assets, the settlement system, and the principles and rules regarding their capital and capital adequacy. Article 5 of the same regulation, titled "Services and Activities of Crypto Asset Service Providers," specifies the activities that fall within the scope of custody:

17 *https://spk.gov.tr/data/668412388f95db0c2c4e36d5/Ek-1%20Duyuru-Talep%20Edilen%20Belgeler.pdf*

18 *https://spk.gov.tr/kurumlar/kripto-varlik-hizmet-saglayicilar/faaliyette-bulunanlar-listesi*

a) Receiving and executing orders related to crypto assets, their exchange, transfer, and the storage services required for these activities, and c) The storage, management, or other storage services determined by the Board for crypto assets or the private keys related to these assets. Each storage institution engaged in these activities must obtain permission from the Capital Markets Board.

The third section of Circular (III-35/B.2), titled "Principles Regarding Platform Activities," first regulates the activities and general principles of platforms and then lists the obligations to which platforms are subject in order to create a trading environment, execute customer orders as the counterparty, and establish a price monitoring system. Communication (III-35/B.2) clearly grants platforms the authority to provide custody services, stating in Article 17, titled "Custody of Customers' Crypto Assets by Platforms," that platforms may collectively store their customers' crypto assets in one or more wallets, provided that such storage complies with the limitations set forth in the capital adequacy requirements.

Communication (III-35/B.2) states in Article 24 of Section 5, titled "Custody Services and Transfer Principles," that crypto asset custody services are defined as "the storage, management, or other custody services determined by the Board for crypto assets or private keys related to such assets that platform customers do not prefer to keep in their own wallets."
However, custody institutions are permitted to provide custody services directly to customers other than platform customers.

However, providing wallet services where full control of the private key is left to the investor is not considered a custody service. Article 25 of the Communiqué (III-35/B.2) states that institutions that may provide custody services are banks authorized to provide crypto asset custody services in accordance with this Communiqué and deemed appropriate by the BDDK, or other institutions authorized by the Capital Markets Board to provide crypto asset custody services.

Custody institutions are required to store customers' crypto assets collectively on behalf of the platform, separately from their own accounts. Subject to the provisions of Law No. 5549 and related legislation, platforms are not required to have their customers sign an external contract with the custody institution. If custodial institutions provide direct custody services to customers within the scope of the second paragraph of Article 24 of the Communiqué (III-35/B.2), the custodial institution must enter into a separate agreement with these customers regarding the service in question and ensure that the risks arising from this service are communicated to customers in a clear and detailed manner. All keys and components used by the custodian to control customer assets must be stored in secure hardware modules in accordance with the principles set out in the TÜBİTAK Infrastructure Criteria.

A written procedure must be established, which includes matters related to the provision of custody services in accordance with the principles set forth in this Circular (III-35/B.2), and which will enter into force by a decision of the custody institution's board of directors. This procedure must be reviewed at least once a year to ensure its validity. Custody institutions are expected to ensure that the size of the hot wallets in which they store crypto assets does not exceed 5% of the total customer assets.

The management and access to assets and mechanisms such as private keys, the mechanisms used in the generation of private keys, and the keys used in the backup process by crypto asset service providers must comply with the principles set forth in the TÜBİTAK Infrastructure Criteria. If private keys are split into parts using mechanisms such as multi-party threshold cryptography, each part and the mechanisms in which the key parts are used, including their backups, must be kept in Turkey, and control over them must remain with the crypto asset service providers.

Pursuant to Article 31 of Circular (III-35/B.2), a service agreement must be signed between platforms and custodial institutions. This agreement shall cover the processing of transactions by custodial institutions in the distributed ledger network system, how the costs incurred in operating the distributed ledger network system will be reflected, and the rights and obligations of the parties in the event of termination of the agreement. If the custodian institution loses the conditions required in this Communiqué (III-35/B.2), platforms must sign an agreement with another custodian institution. The custody institution that was a party to the old contract remains liable until the new contract enters into force. The minimum capital of custody institutions must be at least 500,000,000 Turkish Lira, as required by Article 34 of Circular (III-35/B.2).

Pursuant to Article 41 of the Circular (III-35/B.2) titled "Storage Limits and Liquidity Reserve Obligation," at least 95% of the crypto assets that customers choose not to hold in their own wallets must be stored at the custodian specified in Section B.2 of this Circular (III-35/B.2). The maximum 5% portion not held by the custodial institution shall be held in wallets on the platform in accordance with the principles set forth in Article Article 26 of the relevant Circular.

3. Current Legal Framework in Other Countries at the Forefront of the Crypto Asset Ecosystem

3.1 The Crypto Asset Storage Process in the European Union and MiCA Regulation (Markets in Crypto Assets Regulation - MiCAR) Regulations

The entry into force of MiCA in the European Union is also considered a significant milestone for countries outside the EU. By introducing detailed regulations in areas such as crypto-asset service providers (CASP) and custody services, MiCA establishes a standard not only within the European Union but also in global crypto-asset markets. MiCA's comprehensive regulatory framework is considered a reference point for companies operating in the crypto asset market
, it is thought that it may also prompt other countries to review their own digital finance strategies and develop a framework compatible with MiCA.

MiCA lists the specific services that crypto asset service providers may offer. MiCA licenses crypto asset service providers offering the crypto asset services listed under Article 3(1)(16) and subjects them to certain other financial obligations. These listed crypto asset services include the custody and management of crypto assets on behalf of customers (crypto asset custody services).[19]

19 *Article 3(16) of MiCA, titled "Definitions," defines "crypto asset service" (crypto assets
service) or activities related to crypto assets, specifically mentions a service type described as "providing custody and management of crypto assets on behalf of customers." Furthermore, the same regulation's Article 17
, "providing custody and management of crypto assets on behalf of customers" is defined as "providing custody and management of crypto assets on behalf of customers."
it is stated that "it shall mean the storage or control of crypto assets or tools for accessing these crypto assets, in the form of private cryptographic keys, where applicable.*

Depending on the services they provide and due to the specific risks associated with each type of service, providers of crypto asset custody services should be subject to requirements specific to these services.

The obligations and security measures related to custody services provided by MiCA may reshape the operational processes and compliance policies of companies offering these services. Therefore, it is also expected that crypto asset service providers in countries outside the EU will develop similar regulations incorporating the fundamental principles of MiCA or make additions to their domestic laws to align with MiCA.

MiCA also requires a specific license for CCPs to provide the services mentioned above, including custody services.[20] In this context, pursuant to MiCA Article 59, a crypto asset service provider is defined as a legal entity or organization that, due to its profession or occupation, provides one or more crypto asset services to third parties in a professional manner and is authorized to carry out such activities.[21] Therefore, entities wishing to operate as CAVPs must have an office registered in an EU Member State.[22] To this end, a formal application must be made to the competent authorities in the EU Member State.[23]

In general, when examining licensing requirements for KVHSs, these requirements vary depending on the services they will provide. However, they include (i) a requirement to maintain a certain minimum capital, (ii) organizational requirements (partnership structure, personnel employed, etc.) and (iii) business conduct requirements (acting honestly, fairly, professionally, and prioritizing customer interests, etc.).[24]

According to MiCA Article 83, Crypto Asset Service Providers (CASP) that provide custody and management of crypto assets on behalf of customers must sign a contract with their customers containing certain mandatory provisions and must establish and implement a custody policy that must be provided in electronic format upon customer request. Accordingly, CCPs must specify the nature of the service in the contract they will conclude with their customers electronically, which may include the holding of crypto assets belonging to customers or access tools to such crypto assets. In this case, the customer must have the ability to keep control of the crypto assets under their own supervision. Alternatively, crypto assets or the means of accessing them may be transferred to the full control of the crypto asset service provider.
Crypto asset service providers holding customers' crypto assets or the means to access these crypto assets must ensure that these crypto assets are not used for their own accounts.
Crypto asset service providers must continuously ensure that all crypto assets they hold are not subject to any obligations or restrictions.

20 *MiCA Article 63, titled "Assessment of the Application for Authorization and Grant or Refusal of Authorization," contains detailed provisions on the criteria for evaluating the license processes of KVHSs how the process will be assessed in terms of which criteria.*

21 *MiCA Art. 3/f. 1 (15)*

22 *ÇETİN, Müge: "Crypto Assets from the Perspective of Capital Markets Law," On İki Levha Yayıncılık, 1st Edition, Istanbul, 2023, p. 103; to access the relevant work electronically: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4346795 (S.E.T.: 10/09/2024)*

23 *ANNUNZİATA, Filippo: "The Licensing Rules in MiCA," Fintech Regulation and the Licensing Principle," (Ed: Moura Vincente, Diogo Pereira Duarte, and Catarina Granadeiro, European Banking Institute, 2023.*

24 *ÇETİN, p. 103*

These crypto asset service providers should also be held liable for any loss arising from an incident related to information and communication technology ("ICT"), including an incident resulting from a cyberattack, theft, or any malfunction. However, as understood from the content of the provision, the liability of KVHSs for such potential damages is regulated as strict liability.

It is particularly worth noting that one of the most important provisions imposing detailed obligations on CCPs in relation to crypto asset custody services is Article 75 of MiCA. Upon examining the content of the relevant provision, the first paragraph of the article stipulates that crypto asset service providers who store and manage crypto assets on behalf of customers must enter into a **contract25** with their customers to define the scope of their duties and responsibilities. The contract in question must: (a)
the identity of the parties; (b) the nature of the crypto asset service provided and a description of this service; (c) the custody policy; (d) the means of communication between the crypto asset service provider and the customer, including the customer's identity verification system; (e) a description of the security systems used by the crypto asset service provider; (f) the fees,
costs, and expenses applied by the crypto asset service provider; (g) the applicable law.

Another noteworthy aspect of MiCA regarding custody is the requirement that Crypto Asset Service Providers (CASP) maintain separate records for each customer, corresponding to their rights and assets in crypto assets, on behalf of their customers.**26** Thus, crypto-asset service providers are obliged to record any action following their customers' instructions as soon as possible. MiCA ensures that such records are supported by internal procedures and that any action affecting the record of crypto-assets is tracked and evidenced by a transaction regularly processed in the customer's position record. In addition, the relevant CASS must establish a custody policy **27** containing internal rules and procedures for storing or controlling such crypto assets or providing access tools to crypto assets. A summary of the custody policy will be provided to customers in electronic format upon request.

In addition, MiCA imposes another important regulatory requirement on CSDs that provide custody and management of crypto assets: they must provide their customers with a position statement of the crypto assets recorded on their behalf at least once every three months and upon the customer's request. **28**

25 *As in Turkish law, there is no legal requirement in European Union law that a contract must be in writing; contracts between platforms operating in a digital environment, such as CSDs, and their customers are often concluded as electronic contracts in a digital environment.*
For detailed information on this subject, see MARYKE, Silalahi Nuth: "Electronic Contracting in Europe Benchmarking of National Contract Rules of United Kingdom, Germany, Italy and Norway in Light of the EU E-Commerce Directive", Universitet i Oslo, Complex nr. 2/2008, p. 33 ff.; For electronic access to the relevant work, see https://www.jus.uio.no/ifp/forskning/om/publikasjoner/complex/2006-2011/complex-2008-02.pdf (S.E.T.: 09.10.2024)

26 *The register referred to in MiCA Art. 75/f. 2 is described as a register of positions.*

27 *The storage policy to be prepared by the aforementioned CCPs is intended to minimize the risk of customers losing their crypto assets or rights related to these crypto assets or means of access to crypto assets due to fraud, cyber threats, or negligence. See MiCA, Art. 75/para. 2/c. 3*

28 *The statements of position of the CSDs are referred to in MiCA Art. 75/f. 5 as "statement of position of the crypto-assets".*

It is stated that the aforementioned position record will be prepared electronically and will specify the relevant crypto assets, their balances, values, and crypto asset transfers made during the relevant period.Another prominent issue for KVHSs providing custody services is that KVHSs are expected to separate the crypto assets they hold on behalf of their customers from their own assets and to ensure that their customers' means of access to their crypto assets are clearly defined.[30] Stored crypto assets are legally separated from the KVHS's assets in accordance with applicable regulations, in the interest of the KVHS's customers, so that the KVHS's creditors, particularly in the event of bankruptcy, cannot claim the crypto assets stored by the KVHS. The KVHS will ensure that stored crypto assets are operationally separated from the crypto asset service provider's assets.

Finally, MiCA stipulates a minimum capital requirement of €125,000 for CSDs wishing to provide transfer services for crypto assets, including custody services.[31]

MiCA's custody regime provides a comprehensive framework for crypto-asset service providers in the European Union, aiming to ensure security and protect customer rights within the sector. This regulation, considered a turning point in the digital finance sector in the EU, imposes significant requirements across a wide range of areas, from licensing conditions to the transparency of internal procedures. Furthermore, the requirement for service providers to keep customer crypto assets and the means of accessing these assets separate from their own assets enhances customer security and ensures the protection of crypto assets. With MiCA coming into full effect by the end of 2024, crypto asset markets within the EU are expected to become safer, more transparent, and more regulated.

Whether the principles established by MiCA, particularly in the context of crypto asset custody, are appropriate for the sector's balances and MiCA's objectives is also a matter of debate in European countries. It is stated that MiCA's focus is on "institutional resilience." Institutional resilience means ensuring that the custody service provider is well-organized, well-managed, and does not reuse its customers' assets for its own account.

29 *MiCA Art. 75/para. 5/c. 2*

30 *MiCA Article 75/f. 7 essentially reflects the segregation rule envisaged in MiCA and also reflected in Turkey's Capital Markets Law No. 6362, whereby the assets belonging to the customers of CSDs (cash and crypto assets) are segregated from their own assets. Thus, again referring to the relevant MiCA regulation, this means that in the event of, for example, bankruptcy, creditors will apply directly to the CSDs for their claims, and creditors will have no recourse against customers.*

31 *Services defined as Class 2 under the heading Annex IV in MiCA*

• Providing custody and management of crypto assets on behalf of customers;

• Exchange of crypto assets for funds;

• and/or exchange of crypto assets for other crypto assets, and it is stated that the minimum capital amount that CSDs must provide for these services is 125,000 euros. In Turkey, Law No. 7518, which envisages important regulations regarding crypto assets and CSDs, and the subsequent principle decisions published by the CMB (see CMB's Principle Decision No. SerPK.35.B (dated 08/08/2024 and numbered 42/1259)), the minimum capital and equity capital amount for CSDs applying for an operating license in Turkey must have a minimum capital and equity amount of at least 50 million TL.

According to MiCA, all CSDs providing custody services are subject to all rules, such as governance, conflicts of interest, segregation of assets, and operational risk obligations. However, it is noted that MiCA has shortcomings regarding "asset resilience." Asset resilience refers to the ability of the custodial institution, third parties, token issuer, or DeFi application to provide safeguards in the event of difficulties, regardless of the circumstances. According to authors who hold this view, this deficiency stems partly from the nature of DLT and partly from MiCA's failure to include regulations on private law and, in particular, insolvency proceedings related to crypto assets. Although product regulations for ARTs and EMTs partially compensate for this gap, it is noted that other crypto asset holders are left unprotected. In this context, it is stated that MiCA lags behind TradFi regulation in ensuring asset resilience, as it does not play a much stronger role in providing protection through explicit powers that allow for the supervision of custodians and other service providers and the representation of customers' interests in legal proceedings against third parties.[32]

3.2. Switzerland

Switzerland, as one of the countries that has embraced blockchain technology and hosts the "crypto valley," has an active ecosystem for blockchain and crypto asset ventures. Thanks to the pragmatic and inclusive approach of the Financial Market Supervisory Authority (FINMA) and timely legal regulations, Switzerland is able to quickly adapt to technological developments in the crypto asset ecosystem.

Since 2018, FINMA **has** distinguished between payment, service, and asset tokens in its ICO Guidelines. A legal framework regulating digital assets has been established in Switzerland, specifically to facilitate the issuance processes of "asset tokens" and to provide higher protection to customers using wallet providers and digital asset service providers. The "Federal Act on the Amendment of Federal Laws to Take Account of Developments in Distributed Ledger Technology," which came into force in 2021 and is known as the "DLT Act" for short, has made the issuance of digital assets a more easily applicable process by providing for amendments to many different existing laws.

With the entry into force of the DLT Act, a specific legal basis has been established under Article 16/1 of the Banking Law for the segregation of payment tokens held for customers as part of custody services in the event of insolvency. To ensure the segregation of custody accounts and avoid capital requirements, banks are obligated to maintain payment tokens in custody accounts for their customers at all times. If banks do not hold crypto assets themselves, they must ensure that their customers are protected under insolvency law in the event of the sub-custodian's insolvency, either under Swiss law or through a similarly secure legal basis abroad.

Switzerland has also become one of the leading countries in the field of digital asset custody. This success is believed to have been achieved thanks to the creation of a regulatory framework that encourages innovation and diversity.

32 *Dirk Zetzsche, Julia Sinnig, Areti Nikolakopoulou, Crypto custody, Capital Markets Law Journal, Volume 19, Issue 3, July 2024, Pages 207–229, https://doi.org/10.1093/cmlj/kmae010, p. 221 ff.*

33 *FINMA, Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs) Published February 16, 2018, https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/wegleitung-ico.pdf*

The report prepared by FINMA in February 2023 states that approximately CHF 6 billion worth of crypto assets are covered by custody services. It also reveals that most institutions operating in the crypto asset sector offer custody services but use third-party custody service providers, such as other banks and securities companies, for this service.[34]

The June 2023 Swiss Digital Asset Custody Report examined the digital asset custody environment in the country in terms of the services offered by service providers, their licensing status, and the types of custody they use, and identified 57 companies offering custody services in Switzerland. These companies 44.1% are banks or institutions with equivalent licenses. These institutions include retail and online banks such as Swissquote, private banks such as Maerki Baumann, universal banks such as Credit Suisse, crypto banks such as Sygnum, and regional banks such as Hypothekarbank Lenzburg.[35]

The 2024 **report** of the same name highlights three key risks for organizations offering crypto asset custody services: (i) operational risks such as user errors; (ii) cybersecurity risks such as hacking or social engineering; and (iii) legal uncertainties related to licensing and bankruptcy processes. Furthermore, it is noted that while ensuring transactions are user-friendly, securely storing private keys is the biggest challenge for organizations offering crypto asset custody services.

All banks in Switzerland offering digital asset custody services hold customer assets off their balance sheets, thereby protecting them in the event of bankruptcy. FINMA closely monitors whether this protection is provided. This practice is considered an increasingly important security feature for both corporate clients and wealthy private clients.

Among providers offering custody services in Switzerland support NFTs. These are typically crypto asset service providers or banks specializing in this area.

Financial institutions in Switzerland are insured against loss or theft. Along with the increase in the number of banks offering custody services, the number of insured crypto asset service providers has also risen from 41.2% in the previous year to 50%.

Another feature of the digital asset custody service offered by Swiss banks is the data privacy protection provided under the Swiss Bank Secrecy Act. Sixteen of the custody service providers, or 44.4% of all providers, comply with Swiss banking secrecy standards as a legal requirement.
44.4% of all providers, comply with Swiss banking secrecy standards as a legal requirement.

The aforementioned report also assesses how MiCA, which will come into full effect at the end of 2024, will affect crypto asset service providers offering custody services in Switzerland. MiCA imposes strict obligations on service providers offering custody services, such as licensing requirements, segregation of customer assets, robust governance structures, proper record-keeping, and maintaining sufficient financial resources.

34 *FINMA, Resolution Report 2020, https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/finma-publikationen/resolution-bericht/20200225-resolution-bericht-2020.pdf?sc_lang=en&hash= CCE986A47FCDE3D13A8DD4A748BC12DF'*

35 *Swiss Digital Custody Report 2023, https://static1.squarespace.com/static/6641b46de2c26a6478ff8f6e/t/666b18cdfb4ce0015152d037/1718294737562/Swiss+Digital+Asset+Custody+Report+2023.pdf*

36 *Swiss Digital Asset Custody Report 2024, https://static1.squarespace.com/static/6641b46de2c26a6478ff8f6e/t/668323ba60d1d203f76fff68/1719870411796/Swiss_+Digital_Asset_Custody_Report_2024.pdf, p. 36.*

It is noted that MiCA is much stricter than the current custody regulations in Switzerland. Therefore, Swiss-based digital asset custody institutions aiming to provide services within the EU have two options, regardless of whether they are licensed or subject to AML regulations: establish an EU-based subsidiary to achieve full compliance with MiCA, or use the "reverse solicitation"[37] exemption to provide services without actively marketing to customers upon their request. If the first option is chosen, Liechtenstein is considered a good choice for establishing a subsidiary. [38]

3.3 United Kingdom

In the United Kingdom, in order to provide services related to crypto assets, it is necessary to apply to the FCA for registration under the Money-Laundering Regulations (MLRs) covering such services. The registration requirement is set out in Articles 8 and 9 of the MLR. Article 14/A of the relevant Act defines which crypto asset services are subject to anti-money laundering regulations.

Currently, businesses wishing to offer crypto asset custody services, including those already registered or authorized by the FCA for other services (e.g., electronic money institutions, payment institutions, and firms authorized under the Financial Services and Markets Authority), must also register with the FCA.

Companies wishing to provide custody services in the United Kingdom are expected to meet certain criteria in addition to registering with the FCA. These criteria are detailed below.

First and foremost, the FCA will assess whether the activity is conducted as an active business in the United Kingdom based on the specific circumstances. The following factors will be considered in this assessment:

• Commercial Element: It will be assessed whether the person or entity advertises, operates, or presents itself as conducting business related to crypto-asset services.

• Commercial Benefit: It will be assessed whether the individual or entity derives direct or indirect benefit from this service.

37 *Reverse solicitation: This is a practice mentioned in Article 61 of MiCA. Although it is often referred to as a "reverse solicitation exemption," it is actually a prohibition: It is a regulation that prohibits third-country firms from providing crypto asset services to customers established or located within the European Union, unless it is at the customer's own request and initiative.*

38 *38 Swiss Digital Asset Custody Report https://static1.squarespace.com/static/6641b46de2c26a6478ff8f6e/t/668323ba60d1d203f76fff68/1719870411796/Swiss_+Digital_Asset_Custody_Report_2024.pdf, p. 35. In this context, establishing a subsidiary in Liechtenstein could be advantageous given the country's progress in implementing MiCA and its efficient processes for converting existing licenses into MiCA licenses. Thus, obtaining the necessary license would likely be faster. Furthermore, thanks to Liechtenstein's proximity to Switzerland, companies offering custody services can ensure that the content requirements stipulated by the Liechtenstein authorities are met through offices in Zurich or Zug. Such a move could allow the use of the same content for both the Swiss parent company and the subsidiary in Liechtenstein , streamline operations, and maximize efficiency.*

• Relevance to Other Activities: Crypto asset services may constitute only a part of the overall business activities. The relevance of these services will be assessed by evaluating their relationship with other services.

• Regularity/Frequency: The frequency with which the crypto asset service is performed will be assessed to determine whether it is performed as a business.

Each application should be assessed on its own merits, taking into account the nature of the work being carried out and the business model. When determining whether the work is carried out in the United Kingdom, the following factors will be considered:

• Presence of an Office in the United Kingdom: If the business has an office or headquarters in the United Kingdom, this may indicate that the service is being carried out in the United Kingdom (Article 9). If the office is not a registered office or headquarters, the type of service provided by this office and whether the existence of this office means that business is conducted in the United Kingdom will be assessed.

• No Office or Activity in the United Kingdom: If a business has no office or other activity in the United Kingdom but only a customer in the United Kingdom, it may be concluded that the business is not carried on in the United Kingdom. For example, if a CSD is registered in a jurisdiction outside the United Kingdom and has no office or representative in the United Kingdom, but still allows UK customers to open trading accounts, buy and sell crypto assets, or store them, this does not automatically mean that business is being conducted in the United Kingdom.

Companies wishing to provide crypto asset custody services are required to submit certain information and documents when applying for registration with the FCA:

• The specific crypto asset services to be offered by the business must be explained within the framework of the activity program.

• The business's objectives, customers, employees, management structure, plans, and projections must be included in the regulatory business plan. Sufficient detail must be provided to demonstrate that the proposal has been carefully considered, taking into account the adequacy of financial and non-financial resources. It should include information on transaction volume and value, number and types of customers, pricing, main income and expense items, and any additional products or services planned to be offered in the future.

• The description of how the business is organized (including the company structure chart, related parties, and group assets) is expected to be presented in the organizational structure chart. If there are any outsourcing arrangements, their description should be included.

• Details of the systems to be used to carry out the business's operations, security policies, and procedures must be provided.

• Current information about the business and the individuals involved in its organization must be provided.

• The manager and other persons responsible for the management of the business have an obligation to demonstrate that they have a good reputation and possess the appropriate knowledge and experience. As part of the organizational chart, this section must include details of the roles and responsibilities of key persons.

• A person responsible for compliance with anti-money laundering procedures must be designated. The AML/CTF framework must be defined, including policies, procedures, and training materials designed to ensure compliance with the anti-money laundering legislation in force.

• Details regarding senior management's responsibilities, oversight, organizational structure, budget estimates, and financial statements and business continuity arrangements for the first three fiscal years must be provided.

• The risks inherent in the nature of the business must be assessed, and information and documentation regarding the impact and likelihood of these risks occurring must be provided. The methodology used to develop the risk assessment must be outlined.

• The details of the financial promotion policy must be explained, including the systems, controls, and processes used to ensure that promotions comply with relevant UK legislation and are fair, clear, and not misleading.

• It should include details of the policies and procedures that define how the requirements of anti-money laundering regulations will be met when obtaining and transmitting recipient and sender information when transferring crypto assets, and the technology solutions that will be used to support this.

• All crypto asset addresses over which the business has control and which it uses in its business activities must be reported.

Although the United Kingdom has announced plans to introduce more detailed regulations in the near future, it is still unclear how the situation will progress following the change of government.

3. 4 Germany

The German Banking Act (KWG-Kreditwesengesetz) Section 1/11 sentence 4 defines crypto assets. According to this, crypto assets are digital representations of value that are not issued or guaranteed by a central bank or public institution, do not have legal tender status, but are accepted by natural or legal persons as a medium of exchange or for investment purposes.

Crypto assets can be transferred, stored, and traded electronically. Crypto assets are considered financial instruments under Section 1(11) sentence 1 no. 10 of the KWG.

In Germany, **the law** implementing the regulation amending the Fourth EU Anti-Money Laundering Directive (AMLD4) has added the custody of crypto assets as a new financial service under the KWG. This law has been in force since January 1, 2020, and requires companies wishing to offer such services to obtain a license from BaFin ("Bundesanstalt für Finanzdienstleistung") before commencing operations. However, transitional provisions are in place for companies that were already carrying out these activities as of the date the law came into force.

BaFin regularly publishes information on its website regarding the legal status of the legal framework for crypto assets, and this site is constantly updated. In addition, BaFin has published various guides and manuals specifically related to the crypto custody business. These guides include a guide on the definition of the crypto custody business, **a guide** on the interpretation of Section 64/y of the KWG, guides for authorization applications, and guides on anti-money laundering requirements.

39 *Federal Law Gazette I, p. 2602, dated December 19, 2019, Gesetz zur Umsetzung der Änderungsrichtlinie zur Vierten EU-Geldwäscherichtlinie – GwRLÄndG*

40 *BaFin is the abbreviation for the Federal Financial Supervisory Authority (Bundesanstalt für Finanzdienstleistungsaufsicht), Germany's financial regulatory authority. Established on May 1, 2002, BaFin is the German It is responsible for ensuring the safe and orderly functioning of the financial sector. BaFin supervises banks, insurance companies, and securities markets, ensuring the soundness, integrity, and stability of these institutions.*

41 *https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Auslegungsentscheidung/BA/ae_Hinweise_zur_Auslegung_64y_KWG_en.html;jsessionid=46D99BD1E20DC2DEC63AAA39C118ED20.internet001?nn=19578884*

i. Definition of Crypto Custody Services in German Law

According to Section 1 (1a) sentence 2 no. 6 of the German Banking Act (KWG), the business of crypto asset custody is defined as the custody, management, and protection of crypto assets or private cryptographic keys used to store, hold, or transfer crypto assets for others.

In this context, custody refers to the safekeeping of crypto assets as a service offered to third parties. Therefore, this specifically covers service providers that hold their customers' crypto assets collectively, without their customers having knowledge of the cryptographic keys used.

Management refers to the fulfillment of rights arising from crypto assets.

Protection refers to both the digital storage of private cryptographic keys provided as a service to third parties and the storage of the physical data medium (e.g., a USB drive or a piece of paper) on which these keys are stored. Merely providing storage space, such as services provided by web hosting or cloud storage providers, will not meet the definition unless these providers explicitly offer services for the storage of private cryptographic keys.[42]

ii. Application to BaFin

BaFin aims to minimize both national and international risks to the German financial system, ensure that financial processes in Germany continue to function properly, and safeguard their integrity. Anyone wishing to conduct crypto asset custody business on a scale requiring commercially organized business operations in Germany must obtain prior written permission from BaFin in accordance with the regulation in KWG 32/1 sentence 1. For the majority of financial services covered by Article 1/1a of the KWG, companies authorized to provide a specific financial service may also provide this service in relation to crypto assets. However, this does not apply to the custody of crypto assets. This is because those already authorized to provide financial services require additional authorization to engage in the business of storing crypto assets.[43]

The application for a crypto asset custody license requires documentation of various requirements, such as a minimum initial capital of 150,000 euros, reliable founders, and qualified managers.
A business plan must also be included with the application. This plan should include the balance sheets and income statements for the first three fiscal years, the company's organizational structure, and internal control mechanisms. In addition, the plan must comply with relevant accounting and financial standards. Businesses must have an appropriate business organization and provide information about their IT strategies and security.

42 *https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Merkblatt/mb_200302_kryptoverwahrgeschaeft_en.html;jsessionid=46D99BD1E20DC2DEC63AAA39C118ED20.internet001?nn=19578884*

43 *https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Merkblatt/mb_200302_kryptoverwahrgeschaeft_en.html?nn=19578884*

Adequate IT security is an integral part of a sound business organization within the meaning of Section 25a of the KWG. The requirements of MaRisk [44] and BAIT [45] must be implemented as part of the risk management system. BaFin expects detailed information on IT systems and processes. For applications for crypto asset custody licenses, the security of cryptographic keys must be a priority.

The documents to be submitted as part of the application include the security strategy, management of security incidents, and risk assessment. Depending on the company's business model, it must be explained how crypto assets are technically stored (e.g., "hot wallet," "cold wallet") and whether the assets are held in separate or collective wallets.
The main points of the information that must be submitted with the application can be listed as follows:
The business strategy related to the planned activity; long-term IT strategy; comprehensive definition of IT system architecture; security strategy and encryption methods; information on significant outsourcing and cloud solutions; risk assessment and measures taken; detailed definition of the cryptography concept; access roles and security concept for sensitive data and cryptographic keys; definition of monitoring procedures. This information should be presented taking into account the principle of proportionality and the specific circumstances of the company.
Founders must be qualified and trustworthy in accordance with Article 25c (1) of the KWG and must have sufficient time to perform their duties. This also applies to those engaged in the custody of crypto assets. Founders who do not possess sufficient qualifications may result in the authorization application being rejected.

A founder must possess sufficient theoretical and practical knowledge and management experience in the relevant business areas.

In the crypto asset custody business, BaFin will consider the size and structure of the business, as well as the fact that crypto custody is a new financial service. Therefore, special importance will be given to the founder's technical expertise. In particular, they will be required to have training and practical experience in IT security matters.

Applications must include a handwritten and signed resume to prove the founders' qualifications and reliability, a certificate of good standing submitted to the competent authority, and a document obtained from the Trade and Industry Register. BaFin has published a checklist specifying the documents required for the application.

BaFin will recognize activities in the field of crypto custody as practical experience at the relevant hierarchical level. Additionally, founders are expected to develop any areas of expertise they lack during the transition period. In special cases, BaFin will also assess whether a founder has the human resources and organizational structure to temporarily compensate for any lack of expertise. These assessments will be made individually for each business based on its size and structure.

If an institution only stores crypto assets within the meaning of **Section** 1/11 of **the** KWG, the appointment of only one founder is generally sufficient. However, if the relevant crypto assets also fall under another category of financial instruments or if the company engages in other types of business, the situation may be different.

44 *MaRisk is an abbreviation referring to the minimum requirements for risk management applicable in Germany; it is a circular issued by the German Federal Financial Supervisory Authority that provides concepts for risk management for banks, insurance companies, and other companies conducting financial transactions in Germany.*

45 *Similar to the Minimum Risk Management Requirements in MaRisk, BAIT also specifies the legal requirements of Section 25a of the German Banking Act. BAIT explains how financial institutions should establish appropriate technical and organizational resources for their IT systems in accordance with the supervisory authority's catalog of requirements.*

46 *KWG 1(11) "The issuance of prepaid cards for payments, provided that the issuer of the card is not simultaneously the service provider and therefore the recipient of the payment made with the card (prepaid card transactions)."*

BaFin may indicate that the appointment of more than one founder may be necessary in certain cases. If, due to the size of the institution and the scope of its business activities, a proper business organization cannot be ensured with a single founder, the dual control principle must be applied. This will be examined separately by BaFin in each case based on the documents submitted during the application process. Therefore, an organizational chart showing the responsibilities of the management board must also be included in the authorization process. In addition, documents demonstrating that the institution has sufficient human resources and technical and organizational structure must be submitted. Founders must devote sufficient time to their duties.

iii. Prevention of Money Laundering

The GwG (Geldwäschegesetz) requires economic actors operating in Germany to participate in efforts to prevent money laundering and terrorist financing. Institutions engaged in the custody of crypto assets are among the obligated institutions under Section 2 of the GwG.

The three pillars of anti-money laundering are defined within the framework of Germany's Anti-Money Laundering Act (GwG). First, Section 4 of the GwG requires obligated institutions to have an effective risk management system in place; this system must analyze the risks of money laundering and terrorist financing and establish appropriate internal controls. Second, GwG
Article 10 sets out customer due diligence obligations; accordingly, institutions must verify the identity of customers, identify beneficial owners, and assess the purpose of the business relationship. Finally, Article 43 of the GwG requires the reporting of suspicious transactions and specifies that these reports must be made to the Financial Intelligence Unit (FIU); at the same time, obligated institutions must register with the FIU. These three pillars are critical to ensuring effective combating of money laundering and terrorist financing within the scope of custody activities.

3. 5 United Arab Emirates (UAE)

The UAE aims to grow the crypto asset custody services sector while also introducing oversight to the sector through a comprehensive licensing process designed to minimize risks in this area. This is intended to provide a secure operating environment for international investors and businesses. Crypto asset custody services encompass service providers that securely store and manage users' digital assets. To offer these services, businesses must meet specific financial and security standards. They are also required to comply with anti-money laundering and counter-terrorist financing regulations.

Article 121 of the United Arab Emirates Constitution permits the establishment of free zones.
Federal Law No. 8 of 2004 allows for the establishment of regions known as financial free zones, which are a subset of free zones. According to the relevant regulation, the basic elements of a financial free zone are as follows: They are exempt from federal civil and commercial laws but are subject to criminal laws, including AML. There are two free economic zones in the United Arab Emirates: Abu Dhabi Global Market (ADGM) and Dubai International Financial Centre (DIFC).
This section of our report will outline ADGM, DIFC, and other regulations pertaining to crypto asset custody services within the UAE.

3. 5.1. Under the Virtual Asset Regulatory Authority (VARA)

On March 9, 2022, the Dubai Virtual Asset Regulatory Authority (VARA) was established in Dubai by Law No. 4 2022/4. On February 7, 2023, the VARA Regulation was published.

Under VARA Regulations, the licensing regime for a Virtual Asset Service Provider (VASP) depends on the type of service the VASP offers. VARA defines seven distinct categories of virtual asset activities that overlap to determine the scope of services a VASP can offer. A VAS may apply for multiple activities and consolidate them under a single general license. Generally, the seven activity categories include: advisory services; brokerage services; custody services; exchange services; lending and borrowing of virtual assets; payment and remittance services for virtual assets; and virtual asset management and investment services.

In addition to the main regulation concerning crypto asset custody services, there is also a Rulebook (Custody Services Rulebook) that institutions must comply with.[47] The rules contained herein have been published in accordance with the Virtual Assets and Related Activities Regulation 2023 and form part of this
part of that regulation. It also applies to all service providers licensed by VARA to conduct Custody Services in the Emirate.

A CSD wishing to carry out one or more of these activities must apply to VARA for a license. Application fees, renewal fees, and annual audit fees are applied at various rates.

A consultancy services license comes with an application fee of AED 40,000 and an annual audit fee of AED 80,000, while the equivalent stock exchange services license fees are AED 100,000 and AED 200,000, respectively.

In August 2023, VARA published a revised Custody Services Rulebook regarding staking activities. Accordingly, KVHSs with a custody services license can now provide staking services to their customers from the same legal entity without obtaining a separate license for the Virtual Asset Management and Investment Services activity category, provided they obtain additional approval from VARA.

3. 5.2. Dubai Financial Services Authority (DFSA)

Dubai has rapidly emerged as a hub for crypto asset custody services and is attracting the attention of major players in this field. The Dubai Financial Services Authority (DFSA), located in the DIFC, has established the "Crypto Token Regime" for the regulation of crypto assets. This regime expands the scope of many existing financial services activities related to the provision of crypto token-related products and services.

On March 8, 2024, DIFC enacted the Digital Assets Law. Immediately afterwards, DIFC published the DIFC Amendments Law, which introduced changes to the Law of Obligations, Trust Law, and Companies Law to align them with the nature of digital assets.

The Digital Assets Act recognizes and defines the following as digital assets:

(a) the active operation of software by a network of participants and the combination of data sampled by the network

47 *https://rulebooks.vara.ae/rulebook/custody-services-rulebook*

as a conceptual unit of quantity; (b) existing independently of any specific person or legal system; and (c) things that cannot be duplicated and whose use or consumption by one person or a specific group of persons necessarily prevents one or more other persons from using or consuming that thing.[48]

The Digital Assets Law establishes a framework for the control of a digital asset, the establishment of ownership rights over it, the transfer of ownership, and the recovery of possession.

3. 5.3. Abu Dhabi Laws

Abu Dhabi has updated and renamed the Crypto Asset Framework, which was implemented in 2018, to the Virtual Assets (VA) Framework. The Financial Services Regulatory Authority (FSRA), a separate financial regulator within the Abu Dhabi Global Market (ADGM), **has published** Guidance on the Regulation of Crypto Asset Activities. This Guide should be considered in conjunction with the Guide previously prepared by the FSRA regarding regulations on ICOs/ITOs and Virtual Currencies. The ADGM Regulations, together with the FSRA rules and Guide regulating the use of virtual assets, are referred to as the "Virtual Asset Framework."

The FSRA defines virtual assets as the digital representation of a value that can be bought and sold digitally and functions as a medium of exchange and/or a unit of account and/or a store of value, but does not have legal tender status in any jurisdiction.
Virtual assets are not issued or guaranteed by any jurisdiction and perform the above functions solely by agreement within the virtual asset user community and are distinct from Fiat Currency and E-money.

The application process for obtaining a crypto custody service license includes discussions with the FSRA, a thorough application submission, in-principle approval, final approval, and operational launch testing. Applicants must demonstrate robust management, systems, and control mechanisms for the custody of virtual assets and customer funds.
An individual wishing to operate as a broker, dealer, or custodian in the traditional sphere will need to apply for and obtain FSRA approvals applicable to the specified traditional investments or financial instruments, in addition to obtaining approval to conduct regulated activities related to virtual assets.
and obtain them.[51]

FSRA operates on the basis that there are three types of custody methods for virtual assets: hosted, unhosted, and outsourced. FSRA acknowledges that other alternative virtual asset custody models may exist or emerge in the future. Organizations aiming to offer such alternative models and uncertain about the regulatory obligations they may incur are advised to contact FSRA as soon as possible.

48 *Digital Asset as a thing that:*
"(a) exists as a notional quantity unit manifested by the combination of the active operation of software by a network of participants and network-instantiated data; (b) exists independently of any particular person and legal system; and (c) is not capable of duplication and use or consumption of the thing by one person or specific group of persons."
necessarily prejudices the use or consumption of that thing by one or more other persons.

49 *https://www.adgm.com/documents/legal-framework/guidance-and-policy/fsra/guidance-virtual-asset-activities-in-adgm-20231218.pdf*

50 *https://www.adgm.com/documents/legal-framework/guidance-and-policy/fsra/guidance-icos-and-crypto-assets_20180625_v11.pdf*

51 *https://en.adgm.thomsonreuters.com/sites/default/files/net_file_store/Guidance-Regulation_ofVirtual_Asset_Activities_in_ADGM_(VER05.181223).pdf*

3. 6 The Process of Storing Crypto Assets in the US and SEC Regulations

The legal relationship between an organization providing a crypto asset custody service in the United States and its customer is primarily governed by state laws, although federal regulations and licensing requirements also apply. This relationship may also be affected by the legal and regulatory requirements applicable to state-regulated and supervised cryptocurrency custody service providers, such as banks, investment advisors, trust companies, and broker-dealers, depending on the specific circumstances. Federal law requires investment advisors and broker-dealers that conduct high-value cash or securities transactions to hold the assets subject to the transaction in institutions that meet certain qualifications.[52]

The Custody Rule, as set forth in Rule 206(4)-2 [17 CFR 275.206(4)-2] of the Investment Advisers Act, applies to investment advisers registered with or required to register with the Securities and Exchange Commission (SEC), to comply with certain obligations to protect these assets from loss, theft, misuse, embezzlement, and adverse effects, including the investment advisor's financial difficulties or bankruptcy. These obligations include the custody of the relevant assets by a "qualified custodian."

This rule applies to all investment advisors who directly or indirectly hold their clients' funds or securities. The Custody Rule defines a qualified custodian as certain banks, broker-dealers, futures commission merchants, and foreign financial institutions.[53] Trust companies and registered broker-dealers may qualify, but each must have the ability to securely and separately store their clients' crypto assets. In this context, it is mandatory for these institutions to meet certain reliability and security standards.

However, it should be noted that there is debate among entrepreneurs as to whether the recent rules on custody are compatible with the flexibility and innovation requirements of the crypto asset sector.

In corporate markets, the custody relationship is generally established between the holder and the relevant securities intermediary as governed by Uniform Commercial Code (UCC) Article 8 in the form in which it came into force in the relevant state.[55] If the held asset qualifies as a "financial asset," this custody relationship may be assessed under UCC Article 8.

Pursuant to the June 2019 Agenda Decision of the International Financial Reporting Standards Interpretations Committee, crypto assets should not be classified as "financial assets" because they are not cash or an entity's equity instrument.[56] In some cases, crypto assets may grant their owner certain rights related to the asset they represent.

52 *Clifford Chance, "Custody of Cryptoassets: Moving Towards Industry Best Practice" June 2023, 34: https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2023/06/custody-of-cryptoassets.pdf*

53 *https://www.ecfr.gov/current/title-17/chapter-II/part-275*

54 *Sidley Austin LLP, "Crypto-Focused Private Fund Adviser Settles with U.S. SEC for Custody Rule and Other Violations," September 2024, https://www.sidley.com/en/insights/newsupdates/2024/09/crypto-focused-private-fund-adviser-settles-with-us-sec-for-custody-rule-and-other-violations..*

55 *Uniform Commercial Code, Article 8, "Investment Securities," American Law Institute and Uniform Law Commission.*

56 *International Monetary Fund, "Recording Crypto Assets in Macroeconomic Statistics," June 2022, : https://www.imf.org/external/pubs/ft/gfs/gfsac/pdf/Recording_Crypto_Assets_MacroStats_July_22.pdf.*

Examples of such assets include commodities such as gold or oil, intellectual property rights, or real estate.[57] Some asset-backed tokens provide a direct right to the asset, while others do not offer the possibility of redeeming the asset they represent. A crypto asset can be classified as a financial asset if it provides the right to receive cash equivalent to the value of the asset it represents. Currently, according to the IRS (Internal Revenue Service), crypto assets are classified as "digital assets" and are therefore taxed as property. However, it should be noted that Article 8 of the UCC also covers securities and, furthermore, any property held by a securities broker in a "securities account" for a customer, provided that the securities broker and the customer have agreed that the property will be treated as a financial asset. Therefore, for crypto assets to be treated similarly to financial assets under UCC Article 8, the custody agreement must explicitly include the relevant provision.

Reference should be made to **Article 58**. If the custody relationship is subject to UCC Article 8, an institution providing crypto asset custody services as a securities broker has the obligation to hold sufficient assets to cover the customer's securities and to comply with the customer's instructions. It is also subject to certain prohibitions, such as not paying interest on assets without the customer's consent. In general, unless the parties agree otherwise, the crypto asset custody service provider is obligated to exercise due care.

It should be noted that UCC Article 8, while stipulating that a securities broker does not have ownership rights over the assets it holds, emphasizes that each rights holder has an ownership right proportional to all interests in the specific types of financial assets held by the securities broker on behalf of the rights holder.

A custodial relationship may also be established as a bail or trust relationship under state law. Although a written agreement is not required to establish a bail or trust relationship under state law, the court may determine that such a relationship exists based on the specific circumstances of the case. In practice, especially in a corporate context, typical custody agreements for the custody of crypto assets are widely used. If the contract does not contain provisions indicating the existence of such a relationship between the organization providing the crypto asset custody service and the customer, a bail or trust relationship cannot be established. If the custody service provider is considered the customer's bail or trustee, there is a duty of care, diligence, and loyalty in the custody of the property. The legal relationship between the crypto asset custody service provider and the customer may also take other forms.

can be established.[59] For example, a debt relationship that imposes no special obligations on the organization providing the crypto asset custody service

may involve a debt relationship where no specific obligations are imposed on the entity providing the service, a typical debt relationship established between the debtor and creditor, or a contractual relationship where the customer has an unsecured monetary claim solely related to the entity's bankruptcy, without any claim on the actual stored assets.

57 *PwC, "About the Crypto Assets Guide," https://viewpoint.pwc.com/dt/us/en/pwc/accounting_guides/crypto-assets-guide/crypto_assets_guide/aboutthecryptoassets.html.*

58 *Clifford Chance, "Custody of Cryptoassets: Moving Towards Industry Best Practice," 35.*

59 *Clifford Chance, "Custody of Cryptoassets: Moving Towards Industry Best Practice," 35.*

On February 15, 2023, the SEC proposed amendments to the Custody Rule and new, comprehensive obligations for registered investment advisors that hold assets on behalf of clients.The proposal aims to reduce the risk of customer asset loss and ensure assets are properly segregated by expanding the types of assets subject to custody safeguards beyond funds and securities.
Therefore, digital assets are also covered. The proposal requires investment advisors who hold customer assets to keep these assets separate from their own property. Investment advisors are subject to certain reporting and compliance requirements, including the obligation to inform customers about their practices regarding the custody of customer assets. Under the proposal, investment advisors must enter into a written agreement with a qualified custodial institution. These agreements must include reasonable safeguards, such as requiring qualified custodial institutions to undergo annual audits conducted by public auditors for the protection of clients and to make relevant records available to the public upon request. This situation brings about a change in the current market practice of investment advisors. Indeed, advisors are not always a party to the custody agreements between the custodian and the client. Thus, the SEC's enforcement will extend to the activities of banks and other custodial institutions over which the SEC does not have direct regulatory authority.

It is stipulated that a qualified bank or foreign financial institution offering custody services must hold customer assets in an account that will protect them from the bank's creditors in the event of bankruptcy.

In addition, institutions providing authorized crypto asset custody services must be transparent about where and how customer assets are stored and provide customers with sufficient information on this matter. Pursuant to the proposal, customer assets must be recorded in the customer's name or otherwise held for the customer's benefit and must not be commingled with the assets of the advisor or persons associated with the advisor. Furthermore, except where the customer has given written consent or authorization, the advisor shall not be entitled to claim any rights, fees, security interest, lien, or claim in favor of related persons or creditors.
The proposal also introduces regulations regarding compensation obligations for the loss of customer assets caused negligently or intentionally by the provider of the crypto asset custody service. This aims to prevent the misuse or mismanagement of customer assets. However, this proposal has not yet been adopted and is expected to be adopted in the coming period.

Furthermore, Staff Accounting Bulletin No. 121 (SAB 121)[61], published by the SEC in 2022, requires organizations providing custody services for crypto assets to hold these assets on their balance sheets. While this regulation brings significant costs and risks for banks, it also provides greater transparency for investors and crypto
It aims to guarantee the protection of customer assets in the event of a company's bankruptcy. On the other hand, the relevant regulation limits banks' ability to offer crypto asset custody services and causes these services to shift to non-banking institutions. The U.S. House of Representatives **passed** H.J. Res. 109 on May 8, 2024, to remove these restrictions, but President Biden vetoed the bill, and this veto has not been overridden.

60 *Proskauer Rose LLP, "Regulation in the Post-FTX Environment: SEC's Proposed Enhanced Custody Rule and Its Effects on Crypto," February 2023: https://www.proskauer.com/blog/regulation-in-the-post-ftx-environment-secs-proposed-enhanced-custody-rule-and-its-effects-on-crypto.*

61 *SEC. Staff Accounting Bulletin No. 121, March 31, 2022. https://www.sec.gov/regulation/staff-interpretations/accounting-bulletins/old/staff-accounting-bulletin-121*

62 *https://blockchain.bakermckenzie.com/2024/05/13/u-s-house-passes-bill-to-undo-sec-guidance-that-limited-ba nks-ability-to-custodian-crypto-assets/*

SAB 121 therefore **remains** in effect. However, the SEC has granted exemptions to some large banks to comply with this regulation by ensuring the protection of customer assets. In the US, providers of crypto asset custody services must comply with rules established not only by the SEC but also by other federal regulatory agencies such as the Commodity Futures Trading Commission and the Financial Crimes Enforcement Network. These agencies require crypto asset custody service providers to have robust security protocols in place to protect digital assets. However, crypto asset custody service providers must also comply with relevant laws and regulations, including Know Your Customer (KYC) and Anti-Money Laundering (AML) rules. In the US, some local custody initiatives have been established specifically to protect digital assets. Although these initiatives have not yet been approved by the SEC, they are technically qualified as custodians.
The entities were registered as state-based limited-purpose trust companies by utilizing the definition of "bank" under the Investment Advisers Act of 1940 and the Investment Company Act, and met the definition of a custodial institution under both laws.

On September 3, 2024, the SEC imposed its first enforcement action for violations of the Custody Rule relating to digital assets. The agency found that a registered investment adviser within its jurisdiction failed to hold "crypto assets offered and sold as securities" held by a private fund client in a qualified custodial institution, as required by Rule 206(4)-2 of the Investment Advisers Act.

As determined by the SEC, the advisor held certain crypto assets belonging to the fund in accounts on digital asset trading platforms such as FTX Trading Ltd., which are not qualified custodians. The fund lost approximately half of its assets following the collapse of the relevant platform. However, the SEC found that the advisor did not adequately inform investors about withdrawal periods and compliance deficiencies. As a result, the advisor **agreed to** pay a $225,000 penalty to be distributed to fund investors affected by the custody rule violation.
As a result, the current financial market infrastructure in the United States is not designed to accommodate cryptographically encoded assets. Integrating crypto assets into existing systems requires significant financial resources and human capital. In particular, those providing custody services must take effective and significant measures in the field of cybersecurity and strengthen their technological infrastructure to protect customer assets from cyberattacks.

Investment advisors in the United States may encounter various compliance challenges when managing digital assets in their clients' portfolios. The first of these is the ongoing uncertainty regarding whether digital assets fall within the definition of "securities" under **the** Securities **Act** of 1933. The SEC has previously stated that a blockchain token alone does not constitute a security.
However, the SEC **is** actively **involved** in various litigation processes, arguing that tokens and other digital assets are offered and sold as securities under the investment contract test established by the U.S. Supreme Court in SEC v. W.J. Howey, Co.

63 *https://blockchain.bakermckenzie.com/2024/07/16/house-fails-to-override-veto-of-bill-to-undo-sec-guidance-that-limits-banks-ability-to-custodian-crypto-assets/*

64 *Sidley Austin LLP, "Private Fund Adviser Settles with SEC over Custody Rule".*

65 *https://www.sec.gov/files/rules/final/2009/ia-2968.pdf*

66 *Sidley Austin LLP, "Private Fund Adviser Settles with SEC over Custody Rule"*

Another challenge is that, due to the large number and variety of digital assets, qualified custodial institutions are not available for all digital assets. This situation prevents advisors from fully complying with the custody rule for these assets, even when it is assumed that the assets in question are "offered and sold as securities." Taking these uncertainties and challenges into account, it is recommended that all advisors, including investment advisors focused on digital assets, review their asset protection policies and procedures in light of the SEC's ongoing oversight and enforcement-focused approach to compliance with the custody rule.

It should be noted that the changes proposed by the SEC could reduce the number of qualified custodial institutions storing crypto assets and force investors to withdraw their funds from platforms that already implement strong protection procedures. The proposed changes are also criticized for making it more costly for hedge funds, private equity funds, and pension funds to invest in crypto assets and store them, thereby making crypto inaccessible as an asset class for advisors who do not want to take on additional compliance obligations. Critics worry that this situation will drive investors and firms toward less regulated offshore services, potentially creating conditions similar to those that led to the collapse of FTX.
they are aware.[67] On the other hand, the SEC argues that expansion of the rule's scope will reduce the risk of customer asset loss, the status of assets that must be held by qualified custodians, and legal uncertainties regarding custody regulations. On this basis, the SEC argues that such steps could increase investment opportunities in crypto assets and the accessibility of advisory services.

67 *Proskauer Rose LLP, "Regulation in the Post-FTX Environment".*

REFERENCES

ANNUNZİATA, Filippo: "The Licensing Rules in MiCA", Fintech Regulation and the Licensing Principle", (Ed: Moura Vincente, Diogo Pereira Duarte, and Catarina Granadeiro, European Banking Institute, 2023.

Atlantic Council CBDC Report, https://www.atlanticcouncil.org/blogs/econographics/a-report-card-on-chinas-central-bank-digital-currency-the-e-cny/

Bank of England CBDC Design Proposal 2024, https://www.bankofengland.co.uk/research/digital-currencies

Ben-Sasson, E., et al. (2014). "Zerocash: Decentralized Anonymous Payments from Bitcoin."

BIS Annual Economic Report 2024, https://www.bis.org/about/bisih/topics/cbdc/mcbdc_bridge.htm

BIS Environmental Impact Study, https://www.bis.org/publ/othp82.pdf

BIS mBridge Project Documentation, https://www.bis.org/publ/othp59.htm

Blum, M., Feldman, P., & Micali, S. (1988). "Non-interactive zero-knowledge and its applications."

Boneh, D., & Shoup, V. (2020). A Graduate Course in Applied Cryptography.

Bünz, B., et al. (2018). "Bulletproofs: Short Proofs for Confidential Transactions."

Carlo R. W. De Meijer, Traditional financial custodians enter the crypto market (October 21, 2024)- https://www.finextra.com/blogposting/27059/traditational-financial-custodians-enter-the-crypto-market#:~:text=The%20growing%20institutional%20interest%20across,institutional%20demand%20for%20regulated%2C%20secure

China's Progress Towards CBDC, https://www.csis.org/blogs/new-perspectives-asia/chinas-progress-towards-central-bank-digital-currency

Clifford Chance, "Custody of Cryptoassets: Moving Towards Industry Best Practice" June 2023, 34: https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2023/06/custody-of-cryptoassets.pdf.

ÇETİN, Müge: "Crypto Assets from the Perspective of Capital Markets Law," On İki Levha Yayıncılık, 1st Edition, Istanbul, 2023, p. 103; to access the relevant work electronically: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4346795

Digital Yuan Technical Overview, http://www.pbc.gov.cn/en/3688110/3688172/4157443/4293696/2021071614584691871.pdf

Dirk Zetzsche, Julia Sinnig, Areti Nikolakopoulou, Crypto custody, Capital Markets Law Journal, Volume 19, Issue 3, July 2024, https://doi.org/10.1093/cmlj/kmae010

Eli Ben-Sasson, et al. (2018). "Scalable, transparent, and post-quantum secure computational integrity."

REFERENCES

FINMA, Guidelines for inquiries regarding the regulatory framework for initial coin offerings (ICOs) Published February 16, 2018, https://www.finma.ch/en/~/media/finma/documents/documentscenter/myfinma/1bewilligung/fintech/guidelines-ico.pdf

FINMA, Resolution Report 2020, https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/finma-publikationen/resolution-bericht/20200225-resolution-report-2020.pdf?sc_lang=en&hash=CCE986A47FCDE3D13A8DD4A748BC12DF

FSB Global Regulatory Framework for Crypto-Asset Activities Umbrella public note to accompany final framework (July 17, 2023) https://www.fsb.org/uploads/P170723-1.pdf pp. 5–6.

F. Yan, Y. Gu, Y. Wang, C. M. Wang, X. Y. Hu, H. X. Peng, et al., "Study on the interaction mechanism between laser and rock during perforation," Optics and Laser Technology, vol. 54, pp. 303-308, Dec 2013.

Goldreich, O. (2001). Foundations of Cryptography: Volume 1, Basic Tools.

Goldwasser, S., Micali, S., & Rackoff, C. (1985). "The Knowledge Complexity of Interactive Proof Systems."

IMF Central Bank Survey 2024, https://www.imf.org/en/Publications/digital-money-research

IMF, Elements of Effective Policies for Crypto Assets (February 13, 2023), https://www.imf.org/en/Publications/Policy-Papers/Issues/2023/02/23/Elements-of-Effective-Policies-for-Crypto-Assets-530092.

IMF Fintech Notes: Regulating the Crypto Ecosystem The Case of Unbacked Crypto Assets Parma Bains, Arif Ismail, Fabiana Melo, and Nobuyasu Sugimoto, 2022.

International Monetary Fund, "Recording Crypto Assets in Macroeconomic Statistics," June 2022, https://www.imf.org/external/pubs/ft/gfs/gfsac/pdf/Recording_Crypto_Assets_MacroStats_July_22.pdf .

Lindell, Y., & Katz, J. (2014). Introduction to Modern Cryptography.

PWC CBDC Implementation Guide, https://www.pwc.com/it/it/publications/assets/docs/central-bank-digital-currency.pdf

Project Dunbar Technical Framework, https://www.bis.org/about/bisih/projects/dunbar.htm

Proskauer Rose LLP, “Regulation in the Post-FTX Environment: SEC’s Proposed Enhanced Custody Rule and Its Effects on Crypto”, February 2023: https://www.proskauer.com/blog/regulation-in-the-post-ftx-environment-secs-proposed-enhanced-custody-rule-and-its-effects-on-crypto.

PwC, "About the Crypto Assets Guide," https://viewpoint.pwc.com/dt/us/en/pwc/accounting_guides/crypto-assets-guide/crypto_assets_guide/aboutthecryptoassets. html.

REFERENCES

SEC. Staff Accounting Bulletin No. 121, March 31, 2022. https://www.sec.gov/regulation/staff-interpretations/accounting-bulletins/old/staff-accounting-bulletin-121

Sidley Austin LLP, “Crypto-Focused Private Fund Adviser Settles with U.S. SEC for Custody Rule and Other Violations,” September 2024, https://www.sidley.com/en/insights/newsupdates/2024/09/crypto-focused-private-fund-adviser-settles-with-us-sec-for-custody-rule-and-other-violations.

Swiss Digital Custody Report 2023, https://static1.squarespace.com/static/6641b46de2c26a6478ff8f6e/t/666b18cdfb4ce0015152d037/1718294737562/Swiss+Digital+Asset+Custody+Report+2023.pdf

Swiss Digital Asset Custody Report 2024, https://static1.squarespace.com/static/6641b46de2c26a6478ff8f6e/t/668323ba60d1d203f76fff68/1719870411796/Swiss Digital Asset Custody Report 2024.pdf

The Board of the International Organization of Securities Commissions (IOSCO), Policy Recommendations for Crypto and Digital Asset Markets Final Report (November 16, 2023)

Turkish Banking Association, Overview of Banking in Relation to Digital Assets, Potential Business Models, and Legal Assessment of Digital Assets (February 7, 2022)

Uniform Commercial Code, Article 8, "Investment Securities," American Law Institute and Uniform Law Commission

World Federation of Exchanges, Crypto-Asset Custody: A Blueprint for Regulatory and Operational Excellence (August 28, 2024), https://www.worldexchanges.org/storage/app/media/Cally%20Billimore/Custody%20of%20Crypto%20-%20Final.pdf

https://blockchain.bakermckenzie.com/2024/05/13/u-s-house-passes-bill-to-undo-sec-guidance-that-limited-banks-ability-to-custodian-crypto-assets/https://blockchain.bakermckenzie.com/2024/07/16/house-fails-to-override-veto-of-bill-to-undo-sec-guidance-that-limits-banks-ability-to-custodian-crypto-assets/

Sidley Austin LLP, “Private Fund Adviser Settles with SEC over Custody Rule”.

https://www.sec.gov/files/rules/final/2009/ia-2968.pdf

https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Auslegungsentscheidung/BA/ae_Hinweise_zur_Auslegung_64y_KWG_en.html;jsessionid=46D99BD1E20DC2DEC63AAA39C118ED20.internet001?nn=19578884
https://blog.arksigner.com/blokzinciri-teknolojisi/web-3-0-doneminde-regulasyon-avrupa-birliginin-mica-tuzugu

https://blockworks.co/news/what-are-smart-contract-wallets

https://brainwallet.io/

https://en.adgm.thomsonreuters.com/sites/default/files/net_file_store/Guidance-Regulation_ofVirtual_Asset_Activities_in_ADGM_(VER05.181223).pdf

REFERENCES

https://www.adgm.com/documents/legal-framework/guidance-and-policy/fsra/guidance-icos-and-crypto-assets_20180625_v11.pdf
https://www.adgm.com/documents/legal-framework/guidance-and-policy/fsra/guidance-virtual-asset-activities-in-adgm-20231218.pdf

https://www.ecfr.gov/current/title-17/chapter-II/part-275

https://www.investopedia.com/terms/p/paper-wallet.asp

https://www.kaspersky.com.tr/resource-center/definitions/what-is-a-hardware-wallet

https://www.liminalcustody.com/knowledge-center/understanding-digital-asset-custodians/

https://rulebooks.vara.ae/rulebook/custody-services-rulebook

https://spk.gov.tr/data/668412388f95db0c2c4e36d5/Appendix-1%20Announcement%20Requested%20Documents.pdf

https://spk.gov.tr/kurumlar/kripto-varlik-hizmet-saglayicilar/faaliyette-bulunanlar-listesi

https://www.world-exchanges.org/our-work/articles/crypto-asset-custody-blueprint-regulatory-and-operational-excellence

CONTRIBUTORS

• Dr. Alpaslan Burak Eliaçık
TÜBİTAK

• Dr. Mustafa Takaoğlu
TÜBİTAK

• Dr. Taner Dursun
TÜBİTAK

• Assoc. Prof. Dr. Mehmet Sabir
Kiraz De Montfort University

• Dr. Süleyman Kardaş
Batman University

• Dr. Pınar Çağlayan Aksoy

• Ahmet Mesut Şahinoğlu
Paribu Custody

• Aysu Düz
Paribu

• Cem Sağlam
Paribu Custody

• Nergis Nurcan Karababa
Paribu Custody

• Meva Öztürk
Paribu

• Deniz Parlaöz
BCTR

• Merve Öztürk Günaltay
BCTR

• Ozan Ege
Web3 Meta Hub

• İlayda Aydın
Web3 Meta Hub

• Bekir Yenidoğan
KPMG Turkey

• Bartu Kaan Ertuğrul
KPMG Turkey

• Gizem Koçak
PwC

• Reşat Uğur Ulu
Togg

• Hasan H. Yaşar
Kolcuoğlu Demirkan Koçaklı Law Firm

• Sinem Nilsu Bayazıt
Kolcuoğlu Demirkan Koçaklı Law Firm

• Irem Cansu Demircioğlu Mercan
Kolcuoğlu Demirkan Koçaklı Law Firm

• Yağmur Gündoğdu
Akıncı Law Firm

• Murat Yılmaz
Akbank

• Onur Çakır
Halkbank

• Cemal Araalan
CBC Law Firm

• İzel Beliz Taylan
Defy

• Suat Özkan
Defy

BLOCKCHAIN
TÜRKİYE

CRYPTO ASSET STORAGE
REPORT

Crypto Service Providers Working Group

TBV
TURKEY INFORMATION TECHNOLOGY FOUNDATION