future internet

MDPI

Article

Shared-Custodial Wallet for Multi-Party Crypto-Asset Management

Yimika Erinle [1,2], Yebo Feng [3,*], Jiahua Xu [1,2], Nikhil Vadgama [1,2] and Paolo Tasca [1,2]

[1] Centre for Blockchain Technologies, University College London, London WCIE 6BT, UK; yimika.erinle.21@ucl.ac.uk (Y.E.); jiahua.xu@ucl.ac.uk (J.X.); nikhil.vadgama@ucl.ac.uk (N.V.); p.tasca@ucl.ac.uk (P.T.)
[2] DLT Science Foundation, London WC2H 2JQ, UK
[3] College of Computing & Data Science, Nanyang Technological University, Singapore 639798, Singapore
* Correspondence: yebo.feng@ntu.edu.sg

Abstract: Blockchain wallets are essential interfaces for managing digital assets and authorising transactions within blockchain systems. However, typical blockchain wallets often encounter performance, privacy and cost issues when utilising multi-signature schemes and face security vulnerabilities with single-signature methods. Additionally, while granting users complete control, non-custodial wallets introduce technical complexities and security risks. While custodial wallets can mitigate some of these challenges, they are primary targets for attacks due to the pooling of customer funds. To address these limitations, we propose a chain-agnostic Multi-Party Computation Threshold Signature Scheme (MPC-TSS) shared-custodial wallet with securely distributed key management and recovery. We apply this solution to create a wallet design for wealth managers and their clients, consolidating the management and access of multiple cryptocurrency tokens and services into a single application interface.

Keywords: cryptocurrency wallet; crypto assets; multi-party computation; wallet security; wallet design; key management; key recovery

Academic Editor: Xuebin Ren

Received: 28 October 2024
Revised: 10 December 2024
Accepted: 19 December 2024
Published: 31 December 2024

Citation: Erinle, Y.; Feng, Y.; Xu, J.; Vadgama, N.; Tasca, P. Shared-Custodial Wallet for Multi-Party Crypto-Asset Management. *Future Internet* **2025**, *17*, 7. https://doi.org/10.3390/fi17010007

1. Introduction

Distributed Ledger Technology (DLT) emerges as a disruptor exhibiting a transformative potential that extends across a multitude of industries (e.g., supply chain management, banking, and healthcare [1–4]). DLT has a decentralised structure that offers enhanced data integrity, making it resistant to manipulation or tampering by any individual or group. To achieve this, the systems employ a combination of private and public keys. These keys protect the data from unauthorised alterations and enable signer authentication.

The unprecedented growth in DLT has catalysed a parallel surge in digital asset investment [5]. The unique characteristics of these assets, which preclude their integration into conventional banking infrastructure, have given rise to specialised institutional custodial services that provide secure wallet solutions. In this context, Multi-Party Computation (MPC) wallets represent a promising avenue for enhancing asset security for custodial institutions. These specialised wallets use threshold signatures, a cryptographic technique that disperses a private key among multiple stakeholders [6]. The key can only be reconstructed when a predetermined quorum of stakeholders collaboratively generates a signature. In doing so, MPC wallets address the vulnerabilities associated with single points of failure, amplifying the security and reliability of digital asset management.

As the complex landscape of cryptocurrencies continues to expand, attracting an increasingly diverse array of investors, the need for a tailored, secure, efficient, and reliable custodian solution that meets the nuanced needs of wealth managers and their clients has never been more pressing. Our wallet design fills this gap with a MPC-based wallet streamlined for wealth managers overseeing high-net-worth investors' digital assets. We also integrate a decentralised key recovery design to ensure all wallet operations including key generation, transaction management and key recovery are distributed. Our work presents profound opportunities for wealth management firms, equipping them with a comprehensive solution to the challenges associated with crypto asset management.

2. Background

2.1. Multi-Party Computation

MPC is a cryptographic technique developed in the 1980s by Andrew Yao [6,7]. It was initially designed to allow multiple parties to compute functions of their combined inputs without revealing their corresponding inputs to one another or any other party. Consider a scenario in which m individuals want to calculate the value of a function, $f(x_1, x_2, x_3, \ldots, x_m)$, which is an integer function of m integer variables, x_i, with a bounded range. Initially, a person P_i knows the value of x_i but no other values of x. Individuals can calculate the value of f by communicating with each other without revealing any information about the values of their variables.

In traditional single-signature wallets, a single key is utilised to enable one authenticated owner to sign and broadcast transactions to the blockchain [8]. Therefore, it must be kept secret and secure at all times [9], which poses a security threat in case the key is compromised. MPC wallets represent a new approach to address the security vulnerabilities of traditional cryptocurrency wallets. Rather than having a single private key, MPC wallets divide the key into "shards" or "key shares" and distribute them among multiple parties, which are then used to sign the transaction.

2.2. Threshold Cryptography

Blakely [10] and Shamir [11] introduced and formalised the concept of secret sharing. One of its most well-known applications is threshold cryptography [12], a method of key or secret distribution among several independent systems. Authenticating messages between non-trusting parties requires effective key management solutions, making threshold cryptography particularly valuable. To generate signatures in our solution, we implement threshold signature scheme (TSS), a component of threshold cryptography. For instance, an organisation should have one public key instead of many individual keys for each employee. However, the authority to sign on behalf of the organisation must be distributed to avoid misuse. Threshold cryptography achieves this in a wholly digital way [13].

The transaction signing is a multi-step process that starts with key share generation and ends with a single signed message as the output (see Figure 1). We propose the signature scheme discussed by Lindell and Nof [14] for this purpose. This efficient implementation of the threshold Elliptic Curve Digital Signature Algorithm (ECDSA) scheme can be used for our MPC-TSS solution.

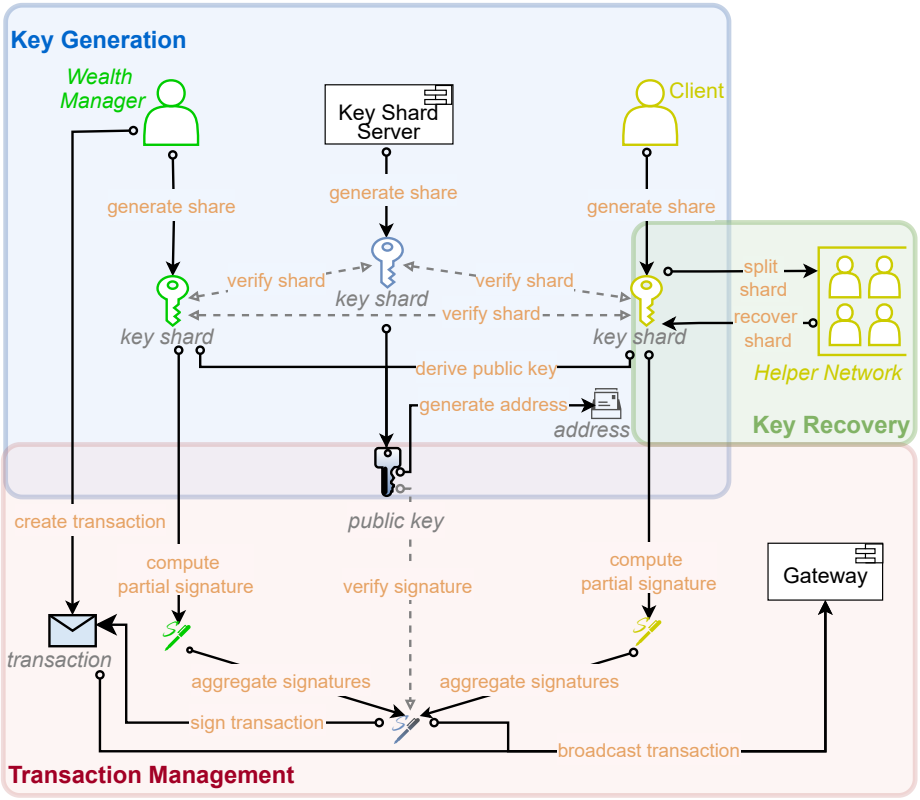

Figure 1. Operational design of the system showing Section 4.1, Section 4.2 and Section 4.3.

3. System Architecture

Our system is designed to achieve crypto-asset security while providing a seamless user experience. We utilise a 2-of-3 threshold MPC scheme involving three key participants: the Client User, the Wealth Manager User and the Custody System. Our proposed solution uses an MPC functionality to manage the private keys of the wealth manager and the clients. A rationale for choosing the MPC-based wallet is that MPC can incorporate thresholds into its cryptographic operations, meaning that certain services can only be executed if a minimum number of parties out of a pool of available parties provide their key shares. We leverage these properties of the MPC-based wallets to design a secure and efficient shared-custodial solution which requires signatures from two out of the three parties to process the transaction within the pre-defined transaction policy.

3.1. Roles in the System

Our system comprises five main entities, as depicted in Figure 2; the Client User, the Wealth Manager User, the Custody Platform, the Blockchain System and the Centralised Exchange (CeX). Each entity is crucial in ensuring the system's security, functionality and usability.

3.1.1. Client User

This user owns the crypto assets and controls a private key share generated through the Distributed Key Generation (DKG) protocol (see Section 4.1). The client's private key share is stored encrypted in the "key shard store" component of the client-controlled device (see Figure 2), utilising secure hardware features such as secure enclave on iOS devices. The Client User must authenticate successfully to perform actions within the system, which include:

1. Wallet Creation: Initiates the creation of a wallet, participating in the DKG process alongside the Wealth Manager and the Custody System to generate the key shares and establish a joint public key.
2. Key Share Management: Securely stores their private key share locally, manages it and can initiate recovery in case of loss, as described in Section 4.3.
3. Transaction Policy Management: Accepts policies defined by the wealth manager such as withdrawal limits and whitelisted accounts which are cryptographically enforced into the MPC protocol. This limits funds loss in several attack scenarios (see Section 5.1).
4. Transaction Initiation: Initiates transactions for sensitive transactions such as on-ramp/off-ramp operations or transfers to non-whitelisted addresses.
5. Transaction Signing: Participates in the MPC protocol to sign transactions, in conjunction with the Wealth Manager or Custody Platform, depending on the transaction type and predefined policies.
6. Key Recovery Initiation: Initiates the recovery, if their key fragments are lost, as shown in Figure 1.

3.1.2. Wealth Manager User

The Wealth Manager User is a trusted financial advisor or institution that assists the Client User in managing their crypto assets. The Wealth Manager holds a private key share generated through the DKG process and associated with the Client User's wallet address. The two main components associated with this user are the key shard store used for secure key management and the frontend employed to perform the following capabilities:

1. Client Portfolio Management: Manages crypto assets on behalf of the Client User, overseeing one or more of these users.
2. Key Share Management: Securely stores their private key share and utilises decentralised recovery mechanisms (see Section 4.3) in case of key shard loss.
3. Transaction Initiation and Signing: Initiates and signs transactions within the limits of the Client User's authorisation policies, participating in the MPC protocol with the Client User and/or the Custody Platform.
4. Transaction Policy Management: Defines policies such as withdrawal limits and whitelisted accounts on account creation.
5. Compliance and Reporting: Ensures that all transactions comply with relevant regulatory requirements and provides necessary reporting to the Client User as needed.

3.1.3. The Custody System

The Custody System serves as the facilitator and coordinator of the platform, providing the infrastructure necessary for secure key management, transaction processing, policy enforcement and communication between parties. The Custody System holds a private key share generated through the DKG process and participates in the signing process if necessary. However, as a security measure, the Custody System cannot initiate transactions under any circumstances. The system operations are carried out by the following components:

- Backend: Ensures connectivity to the components within and outside the custody systems by making requests, fetching and providing data.
- Database: Stores mostly nominal data records on wealth managers and clients, as well as a history of transactions and public addresses of users.
- Key Store Server: Participates in the secure generation of key shards, manages its key shard generated and engages in transaction signing without exposing private keys.

By facilitating communication between the components above, the custody system enables a flexible and secure environment for the client and wealth manager. The functions performed by the system include:

1. Key Management Coordination: Facilitates the coordination of the DKG protocol during wallet creation, providing the necessary infrastructure and communication channels between the platform, and the participating parties. All parties independently generate and exchange public commitments of their key shares securely (see Figure 1). The system does not access or control the private key shares of other parties.
2. Key Share Management: Securely stores and manages the controlled key shard which cannot initiate transactions.
3. User Authentication Support: Facilitates secure user authentication by providing interfaces and protocols for the Client User and Wealth Manager to authenticate themselves.
4. Communication Interface: Provides interfaces for interactions between the Client User and Wealth Manager, facilitating seamless operation and user experience (see Section 4.4).
5. Transaction Verification and Policy Enforcement: Verifies transactions comply with predefined policies set by the Wealth Manager.
6. System Monitoring: Monitors system activities to detect and prevent unauthorised access or fraudulent transactions, ensuring compliance with security standards and regulatory requirements.
7. Transaction Confirmation: Sends transaction updates, transaction confirmations and other notifications to the users.

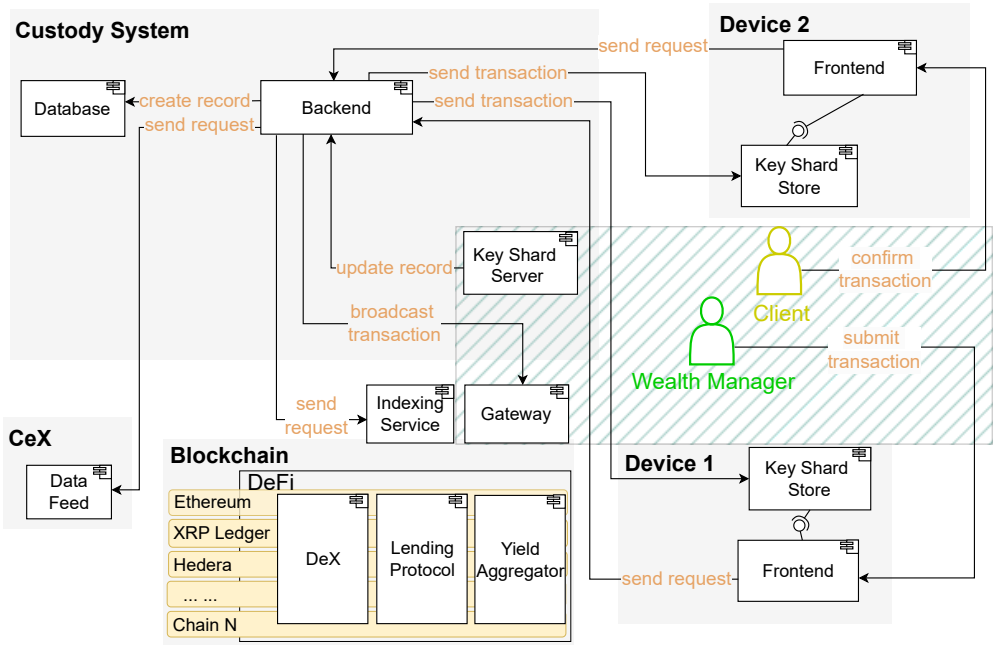

Figure 2. System architecture of our 2-of-3 MPC-TSS wallet. The area with hatch highlight is elaborated on in Figure 1.

3.1.4. Blockchain System

The Blockchain System represents the distinct blockchain networks that the wallet solution interacts with. Components such as decentralised exchange (DeX), lending protocols and yield aggregators provide Decentralised Finance (DeFi) services to users. The system connects to blockchain networks via two critical components:

- Blockchain Gateway: Handles the broadcasting of signed transactions to the blockchain network, ensuring proper transaction formatting and adherence to network protocols.
- Indexing Service: Retrieves and indexes blockchain data relevant to the wallet operations, such as transaction confirmations, account balances, and network status, providing up-to-date information to the users.

3.1.5. Centralised Exchange (CeX)

This is primarily employed to periodically retrieve token prices via an API integration via the "data feed" component. This may also serve other functionalities to users such as on/off ramp services.

4. System Operation

This section provides an overview of the primary operations within our multi-party shared-custodian solution. These operations are designed to ensure the secure management, transaction handling, and recovery of digital assets.

4.1. Key Generation

As shown in Figure 1, we employ Distributed Key Generation (DKG) to produce cryptographic key shards for the client, wealth manager, and the system. Key shards are generated locally for all users and are never exposed to one another, effectively eliminating any single point of failure. If a malicious actor compromises one of the shares, the client's funds cannot be spent because no single shard provides access to the private key.

The process begins with each participant independently generating their own key shard. These shards are collaboratively verified using cryptographic commitments to ensure consistency and integrity. Once verification is complete, the shards are mathematically combined to derive a public key. This public key is then used to generate a shared wallet address for the wealth manager and the associated client.

Unlike traditional Verifiable Secret Sharing (VSS), DKG eliminates the need for a trusted centralised party [15]. Instead, each participant runs their own VSS instance, distributing pieces of their share to the other participants. At the end of the sharing phase, these pieces are verified for consistency using cryptographic commitments. This decentralised approach ensures that no single entity ever has access to the full private key, enhancing both security and trust among participants [16].

The resulting setup is a 2-of-3 MPC-TSS wallet, requiring the collaboration of at least two parties (e.g., the client and wealth manager, the wealth manager and system, or the client and system) to generate a valid transaction signature. This distributed approach ensures that the private key is never fully reconstructed, thereby protecting against compromise and maintaining system security.

4.2. Transaction Management

Our solution allows the client and wealth manager to conduct various transactions, including on/off-ramp transactions, token swaps, and other DeFi transactions. As illustrated in Figure 3, the transaction flow is designed to maintain security and efficiency at every step.

The process begins after an authenticated wealth manager user logs in. The wealth manager interacts with the frontend to create a transaction message specifying the transaction details. On submission of the transaction request, the backend generates the transaction, creates a record in the database, and sends the transaction to the wealth manager's key shard store. The wealth manager is required to sign the transaction for further process-

ing. Following transaction authorisation, a partial signature is generated by the wealth manager's shard.

The backend confirms that the transaction has been signed and sends a transaction authorisation message to the client. If the client or system generates a second partial signature, the signatures are aggregated to form the final valid signature. The transaction is successful if either the client or the system signs the transaction request message. However, an unsigned transaction message or a declined request from the client or system results in transaction failure. Following approval, the backend broadcasts the transaction to the blockchain via the "gateway" component, as shown in Figure 2. The wealth manager user is then updated on the transaction status.

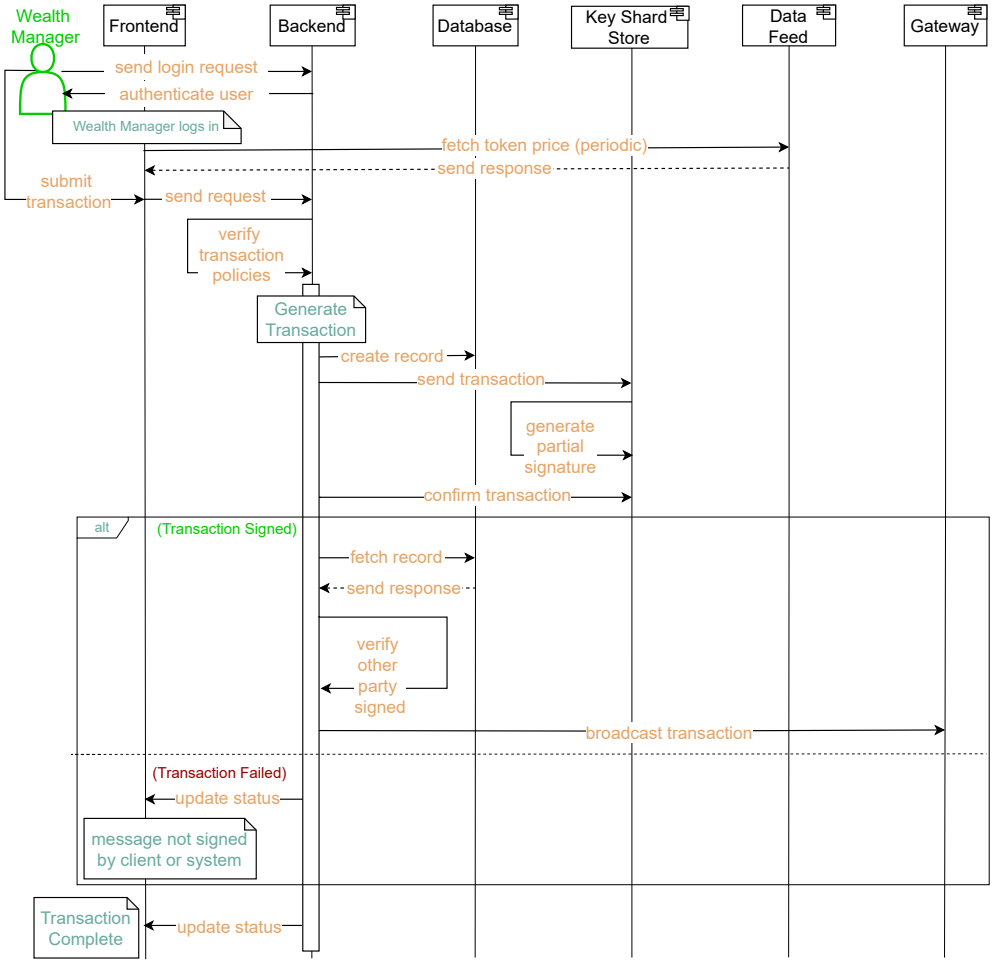

Figure 3. Typical transaction generation process (Section 4.2) by the wealth manager user.

4.3. Key Recovery

Key recovery is a critical component of our system, ensuring that client and wealth manager users can regain access to their assets in case of device loss or theft. We integrate the Decentralised Recovery (DeRec) protocol [17] into our system to enable secure key shard recovery for users. The key operations of the protocol are described below:

4.3.1. User and Helper Pairing

This involves a trusted setup where the user and each helper exchange cryptographic keys to establish secure communication. Pairing is facilitated using a secure channel where each message is signed and encrypted, ensuring authentication and integrity. For instance, during an in-person pairing, users may exchange public keys via QR codes. The pairing

protocol also includes a unique nonce to prevent replay attacks and ensure each session's authenticity. After pairing, both parties possess each other's public keys and can securely exchange messages linked to a specific secret ID.

4.3.2. Share Distribution

The wealth manager and client users are required to distribute their encrypted private key shards to a selected group of recovery agents. Both users' key shards are encrypted using distinct Key Encryption Key (KEK), with each split into multiple shares using Verifiable Secret Sharing (VSS). This threshold scheme dictates a specific minimum number of shares, known as the recovery threshold, which must be amalgamated to reconstruct each KEK. Additionally, a selected group of recovery agents receive an encrypted form of the key shard. No recovery agent has both the KEK and the encrypted shard, as KEK is distributed among a total number of recovery agents.

4.3.3. Share Versioning

To maintain consistency and avoid share corruption, each helper's share is annotated with a version number. When the secret or helper set changes from adding or removing helpers, updated shares are generated and transmitted to all helpers. Older versions are securely deleted after confirmation of successful propagation. These measures ensure synchronisation across helpers and reduce the risk of recovery failure due to outdated shares.

4.3.4. Periodic Verification

To maintain the recovery system's reliability, the user periodically verifies that helpers retain correct shares. This is achieved through a challenge-response mechanism, where the user sends a random challenge nonce to the helper, who responds with a hash of their retained share and the nonce. The protocol ensures that corrupt or non-cooperative helpers are identified and excluded. By enforcing periodic verification, the system mitigates the risk of data loss or tampering and ensures the availability of sufficient uncorrupted shares during recovery.

4.3.5. Share Recovery

Users can initiate the recovery process via the custody system's user interface in case of device or key shard theft. Recovery agents are required to authenticate the user to ensure legitimacy. Following successful authentication, the system retrieves the encrypted key shard and KEK shards from helpers. The user applies a merkle tree-based majority-rule mechanism to determine the correct commitment for the received shares, ensuring malicious or corrupted shares are excluded. Afterwards, verified shares are combined using Shamir's reconstruction algorithm to derive the original KEK, which decrypts the encrypted key shard. This process restores access to the private key while maintaining the integrity and confidentiality of the recovery operation.

4.3.6. Security Assumptions

While the DeRec protocol is designed to mitigate many security risks, certain assumptions underpin its operation, as detailed below:

1. Integrity of Cryptographic Schemes: The protocol assumes that cryptographic primitives are computationally secure against adversaries.
2. Secure Communication Channels: The protocol assumes that communication between sharer and helpers occurs over cryptographically secure channels using signed and encrypted messages.

3. Non-Collusion Among Helpers: The protocol assumes that helpers do not collude to compromise the sharer's shard without authorisation. This risk is minimised, as the identity of helpers and details such as the total number and threshold are private, with helpers oblivious to each other's existence and unable to communicate.

4.4. User Interface

The application is designed to simplify the management of wallets, policies, and transactions, to ensure enhanced usability for wealth managers and clients while maintaining the highest security standards.

4.4.1. Wallet Configuration

The wealth manager employs the wallet mobile app to initiate wallet setup and shares access details with the client. Once the wealth manager and client are authenticated, the DKG protocol is initiated. During this process, private key shards are securely generated and distributed among the participating parties, enforcing threshold logic such as the 2-of-3 signing requirement.

As part of the DKG process, the wealth manager and the client collaboratively define transaction policies, including approval thresholds, withdrawal limits, and whitelisted addresses. These policies are cryptographically embedded into the MPC protocol by associating them with the generated public key and are shared between all parties.

Subsequent modifications to these policies require explicit multi-party approval. The system ensures that changes are cryptographically tied to the MPC protocol, requiring collaborative signing by all stakeholders to securely update the cryptographic state of the wallet to ensure no single party can alter the policies unilaterally.

4.4.2. Transaction Approval

Our application provides a highly flexible approval based on the wealth manager and client's preferences. Clients can also delegate approval to the custody system or define transactions that require their approval. Transaction approval is managed using the 2-of-3 MPC-TSS model, ensuring secure and distributed approvals. Once a transaction is initiated, our application shows the status of each required signature. If a transaction violates established policies, such as exceeding a withdrawal limit or targeting a non-whitelisted address, it is not processed, ensuring compliance and security.

4.4.3. Transaction Notifications

Notifications are triggered at key milestones, such as transaction submission, approval completion, and blockchain confirmation. For example, when a transaction is approved by one party but not approved by another party, the system sends updates to notify all relevant participants of the pending status. In addition, if a transaction fails, participants receive notifications to this effect, including the reason for the failure.

4.4.4. Transaction History

This interface allows users to review operations by viewing past transactions. Transactions are categorised by type, such as token swaps, on-ramp and off-ramp transfers, and status.

5. Threat Model

In this section, we present a threat model for our 2-of-3 MPC-TSS wallet solution. The primary security goal of our system is to safeguard users' funds from unauthorised access and transactions while protecting the integrity of the client shard, wealth manager shard and system key shard server. We identify potential threats, assess their impact, and outline

mitigation strategies to ensure the security and integrity of the crypto assets managed within the system.

5.1. Attack Scenarios

Client and Wealth Manager Users are expected to act in their best interests; however, these users may be susceptible to attacks from an adversary. We elaborate on individual and joint-party compromise in the following:

5.1.1. Individual Party Compromise

Our solution eliminates single points of failure by distributing risk across multiple parties and mitigating device losses through key recovery agents (Section 4.3). In the event of a wealth manager's key shard compromise, unauthorised transactions still require the client's or system's partial signatures. Similarly, a client shard compromise allows transaction initiation but remains insufficient without additional signatures. A compromise in the custody system shard prevents the initiation of the transaction entirely due to design constraints of the system, as shards held by the system cannot initiate transactions (Section 3.1). Finally, a helper shard compromise does not compromise the system as periodic verification using a challenge-response mechanism (Section 4.3.4) alerts clients to potential breaches.

5.1.2. Joint Party Compromise

In a 2-of-3 MPC configuration, the compromise of two user shards will inevitably lead to the system being compromised, as two compromised shards are sufficient to authorise transactions. Acknowledging this inherent limitation, the system has been carefully designed to minimise potential fund losses in such scenarios through cryptographically enforced policy rules. These rules, which include whitelisted addresses, withdrawal limits, and multi-party approvals for policy modifications, are collaboratively defined during the wallet setup process.

For instance, if the key shard server and the wealth manager's shard are compromised, the adversary can sign transactions. However, any unauthorised actions are restricted by predefined policies. Transactions must comply with withdrawal limits and whitelisted address constraints, preventing significant asset loss unless all parties explicitly approve policy changes. Similarly, if the key shard server and the client shard are compromised, adversaries cannot execute unrestricted transfers or modify transaction policies without the wealth manager's approval. If both the client and the wealth manager's shards are compromised, transactions still adhere to the established policy rules, with changes such as increasing withdrawal limits or altering whitelisted addresses requiring system involvement. In scenarios where multiple helpers are compromised, their impact remains limited unless the user-defined helper threshold is exceeded, as helpers alone cannot directly authorise transactions.

5.2. Defence Implementations

We mitigate the risk of attacks with several diverse implementations. Our approach combines time-based, role-based and operation-based mitigations, to ensure the client's funds are secured.

5.2.1. Operation-based Mitigations

These implementations are integrated into the operations of our solutions and include:

1. Fully Distributed Operations: All operations within the system, including key generation, user authentication, transaction signing and key recovery are distributed to prevent single points of failure.

2. Distributed Key Generation: To mitigate against attacks which aim to compromise cryptographic elements of the wallet at the key generation stage, we employ distributed key generation.
3. Multi-factor Authentication (MFA): Incorporating MFA limits attacks such as brute force, dictionary attacks, identity spoofing, and other authentication-related attacks employed in isolation. A combination of these techniques is required to bypass authentication.
4. 2-of-3 MPC-TSS: By distributing shards between multiple parties, more than one party needs to be compromised to threaten the system. Additionally, full signatures are generated by an interactive signing process and key shards are never assembled.
5. Decentralised Recovery: Integrating the decentralised recovery protocol delegates recovery to the users and prevents various attacks.

5.2.2. Role-Based Mitigations

Our design limits the functionality of the custody system by ensuring the custody key shard can not initiate transactions. A similar implementation exists in the Zengo wallet [18]. The key share held by our system primarily acts as a secondary approval mechanism in cases where the client has delegated rights to the custody system. The wealth manager and an associated client can define cryptographically enforced transaction policies to prevent malicious activities.

5.2.3. Time-Based Mitigations

We implement time-based defence measures [19–23] such as periodic key shard updates and periodic helper shard validation. Updating key shards periodically provides proactive mitigation of attacks by enabling parties jointly generate new key shards. Therefore, an adversary cannot initiate transactions if using a client's old shard and a wealth manager's new shard. Additionally, periodic shard validation of each user's helpers ensures helper availability.

5.2.4. Legal Mitigation

To enhance accountability and protect clients from potential malicious actions by wealth managers, we propose the adoption of binding legal agreements aligned with established frameworks and regulatory standards. These agreements ensure that wealth managers are legally responsible for any breach of trust or unauthorised actions. By clearly defining the rights and obligations of both parties, such agreements provide clients with a contractual basis to seek legal recourse in the event of misconduct, thereby offering protection against potential exploitation. Additionally, adherence to these agreements fosters transparency and trust, as clients are assured that wealth managers are operating within a legally binding framework that prioritises their interests.

For instance, in the UK, the Financial Conduct Authority (FCA) mandates that firms providing investment services enter into written agreements with their clients [24]. These agreements must outline the rights and obligations of both parties and be provided in a durable medium before any service is rendered. This requirement ensures transparency and accountability, offering clients a clear understanding of the terms governing their relationship with the wealth manager.

6. Business Model

Our platform offers a blockchain-agnostic MPC-based wallet solution that integrates a range of crypto-asset services into a single, user-friendly platform. By addressing the challenges of blockchain network fragmentation and enhancing security, we provide clients and wealth managers with a secure and efficient way to manage crypto assets.

6.1. Value Proposition

Our value proposition centres on delivering a seamless and secure crypto-asset management experience by combining advanced cryptographic technologies with a broad array of financial services. The key elements of our value proposition include:

6.1.1. Shared Custodial Model

Our shared custodial model offers a balanced approach to crypto asset management by combining the security and control of non-custodial wallets with the convenience and services of custodial wallets. The values provided in the shared custodial model over traditional wallet models are as follows:

1. User Empowerment and Control: In fully custodial wallets, users must trust the custodian entirely, often sacrificing control over their assets. In contrast, our shared custodial model ensures that users retain control over their assets and transaction authorisations. Our solution cannot initiate transactions without the user's explicit consent, aligning with the principles of user sovereignty.
2. Decentralised Recovery Mechanisms: Traditional non-custodial wallets place the entire key management responsibility on the user, risking permanent loss of assets if keys are lost or forgotten. In addition, users are required to protect seed phrases in addition to private keys. Our platform integrates decentralised recovery mechanisms, allowing users to securely recover their key shares without relying on a central authority or exposing their private keys.
3. Mitigation of Single Points of Failure: Most traditional wallets present a single point of failure, making them vulnerable to certain attacks. Our model's distributed architecture mitigates this risk by requiring collaboration among multiple parties for critical operations, enhancing overall system resilience.
4. Diverse Service Offerings with Private Key Control: Users benefit from convenient accessibility to various financial services such as staking, lending, and wealth management tools, while controlling the private key.

6.1.2. Unified Platform for Diverse Crypto Assets

We offer access to several crypto assets and services from multiple blockchain protocols within a single platform. This eliminates the need for users to manage multiple wallets or navigate different DeFi protocols, addressing the issue of blockchain network fragmentation.

6.1.3. Wealth Management Optimisation

By empowering wealth managers with tools to efficiently manage client portfolios, including AI-powered portfolio optimisation, transaction monitoring, and compliance support, we enhance their ability to deliver value to clients and differentiate their services.

6.2. Revenue Streams

Our platform generates revenue through listing, transaction, management, and performance fees, as shown in Figure 4. By aggregating various crypto-asset services, we create multiple monetisation streams.

6.2.1. On/Off-Ramp Listing Fees

Third-party service providers are charged a fee for listing their on-ramp (fiat-to-crypto) and off-ramp (crypto-to-fiat) services on our platform. This provides users with convenient access to these services directly in our application, improving their experience while generating revenue from service providers.

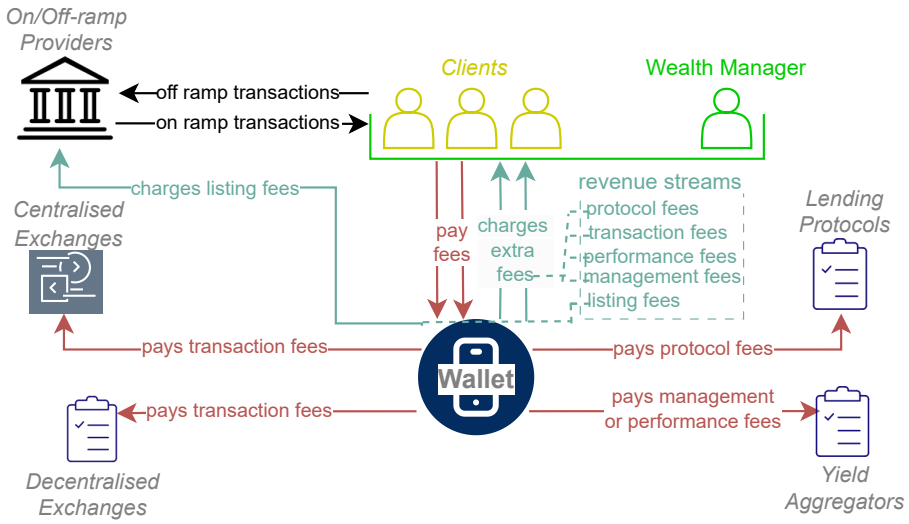

Figure 4. Revenue model detailing diverse revenue streams (Section 6.2) and user incurred costs.

6.2.2. Transaction Fees

Users are charged a small fee for facilitating transactions on our platform. By integrating decentralised exchange services such as token swaps and centralised exchanges, we charge an additional fee to conduct these transactions.

6.2.3. Management and Performance Fees

Management fees are charged based on the client's assets under management (AUM). These fees compensate wealth managers for their services providing revenue to the platform and offering advanced tools such as AI-aided portfolio optimisation. We also implement performance-based fees for investment and portfolio management services that exceed predefined benchmarks. This aligns the interests of wealth managers with those of their clients and rewards successful asset growth and portfolio optimisation.

6.2.4. Staking and Lending Services

Rewards or interest generated from staking and lending protocols employed through our platform are included in our revenue model. Similarly, Metamask charges a 10% fee on user staking rewards [25]. Clients benefit from passive income opportunities, while our platform shares in the generated returns.

6.3. Competitive Advantage

Our business model leverages key competitive advantages that differentiate us in the market. Unlike generic wallet services that take a one-size-fits-all approach, we specialise in meeting the specific needs of high-net-worth clients and their wealth managers. This focus enables us to provide tailored solutions for portfolio optimisation and advanced asset management. By combining the benefits of both custodial and non-custodial wallets, we deliver the security and control that non-custodial users expect, while offering the convenience of a familiar Web2-style user experience. This premium, bespoke service appeals to high-value clients seeking seamless, secure, and efficient crypto-asset management.

6.4. Risk Management

Our risk management strategy addresses the core risks associated with managing crypto assets. We have structured our approach into four primary categories: security, regulatory and operational risk.

6.4.1. Security Risk

By decentralising the key management and recovery process, we significantly mitigate the risk of private key loss or single points of failure within our system. With decentralised key generation, management and recovery, and multi-factor authentication, we significantly reduce the attack surface area associated with traditional wallets.

6.4.2. Regulatory Risk

Ensuring compliance with legal and regulatory frameworks is critical to our platform's operations. We aim to explore Zero-Knowledge KYC (ZK-KYC) [26] to meet KYC and AML requirements while preserving the privacy of clients. Additionally, we incorporate Know Your Transaction (KYT), which enables continuous transaction monitoring to identify suspicious activity and reassess historical transactions in light of new risk indicators, such as associations with sanctioned entities or financial crimes [27]. Our platform complies with global data protection regulations, ensuring secure handling and storage of user information to minimise the risk of breaches or non-compliance penalties.

6.4.3. Operational Risk

Third-party audits are conducted regularly to assess system integrity and identify potential vulnerabilities. Additionally, clients are provided with customisable security policies, including transaction limits and pre-defined transaction requirements, to provide control over asset management and reduce operational risks.

7. Related Work

Single-signature wallets, the most traditional form of digital asset custody, rely on a single private key for transaction authorisation. While widely adopted, these wallets have significant vulnerabilities. Loss or theft of the private key results in irrevocable loss of assets. Academic work such as Igboanusi et al.'s Pure Wallet [28] explored enhancements to single-signature wallets by incorporating offline transaction capabilities and smart contract support. However, these designs lack fraud detection and scalability mechanisms in high-demand environments. Similarly, Ebrahimi et al. [29] examined cold wallet solutions but focused mainly on transaction security without addressing the issues of recovery or dynamic use cases. These shortcomings underscore the limitations of single-signature models in modern applications. To overcome the limitations of single-signature wallets, multi-signature wallets emerged as an alternative. Unlike single-signature wallets, multi-signature wallets distribute control across multiple parties, enhancing security by requiring multiple cryptographic signatures for transaction authorisation [8]. Despite these advancements, multi-signature wallets often increase transaction validation time and require blockchain protocol modifications or smart contract integrations [30].

Unlike multi-signature models, MPC wallets employ threshold cryptographic techniques to enable decentralised signing processes without revealing private keys to any single participant [11]. Threshold signature schemes offer superior efficiency by generating a single signature compatible with existing blockchain protocols, avoiding the need for protocol modifications required by multi-signature wallets [10]. Nicola et al. [31] highlighted the promise of MPC for balancing security and usability in custodial applications. Notable advancements in this area include Lindell's two-party threshold Elliptic

Curve Digital Signature Algorithm (ECDSA) protocol [32], which leverages conventional Paillier encryption, and Doerner et al.'s extension to t-out-of-n threshold settings [33], employing Shamir's secret sharing to enhance flexibility and security. In blockchain ecosystems, Blokh et al. [34] advanced MPC-based ECDSA protocols for cold storage, reducing attack vectors by leveraging non-interactive pre-signing modes. More recently, Han et al. [30] integrated MPC with Bloom filters to enhance transaction validation and participant privacy. However, these studies often focus on generic key management use cases and do not elaborate on the key recovery mechanism. Diverse key management approaches also exist in the industry, showcasing a landscape of major institutional custody providers (see Table 1). These approaches include hardware security modules (HSMs), specialised hardware devices that securely generate, store, and process cryptographic keys while protecting against tampering [35]. This diversity highlights the range of available solutions in key management techniques, blockchain support, and compliance measures.

Our design addresses academic gaps and builds upon these industry observations by proposing a blockchain-agnostic MPC-TSS wallet tailored for wealth managers, combining decentralised key management, securely distributed recovery, and efficient transaction management.

Table 1. Survey of major institutional custody providers. M-Sig—Multi-sig (●: include, ○: not include).

Name	Key Management			Chains Supported							Compliance		
	MPC	M-Sig	HSM	Bitcoin	Ethereum	XRP Ledger	Solana	Cardano	Stellar	Hedera	KYC	KYT	AML
Copper [36]	●	○	○	●	●	●	●	●	●	●	●	○	○
Gemini Custody [37]	●	○	○	●	●	○	●	○	○	○	●	○	○
Fireblocks [38]	●	○	○	●	●	●	●	●	●	●	●	○	○
BitGo [39]	●	●	○	●	●	●	●	●	●	●	●	○	○
Genesis Custody [40]	●	○	○	●	●	●	○	○	●	○	●	○	○
Ripple Custody [41]	●	○	●	●	●	●	●	●	●	●	●	●	●
Tangany [42]	●	○	●	●	●	●	●	●	●	●	●	●	●
Prosegur Crypto [43]	●	●	○	●	●	●	○	○	○	○	○	○	○
DLT Finance [44]	●	○	○	●	●	●	●	●	●	○	●	●	●
Hex Trust [45]	○	○	●	●	●	●	●	●	●	●	●	●	●
BitPanda [46]	○	●	●	●	●	●	●	●	●	○	●	○	●
GK8 [47]	●	○	○	●	●	●	●	●	●	●	○	○	○
DigiVault [48]	○	●	●	●	●	○	○	○	○	○	○	○	○
Cybavo by Circle [49]	●	○	○	●	●	●	●	●	●	○	●	●	●
Bitcoin Suisse [50]	○	●	●	●	●	●	●	●	○	○	○	○	○
Cobo [51]	●	○	●	●	●	●	●	●	●	○	●	●	●

8. Conclusions

This paper introduces a blockchain-agnostic MPC-TSS wallet specifically tailored for wealth managers and their clients, addressing critical gaps in existing custodial and non-custodial wallet solutions. Leveraging threshold cryptography and decentralised key recovery, our design mitigates single points of failure, enhances transaction security, and reduces the risks associated with key mismanagement.

By integrating compliance-focused features and user-friendly interfaces, our solution not only meets the technical and regulatory demands of wealth management but also simplifies the complex landscape of digital asset management. Addressing adversarial risks such as individual or joint-party compromise, the design ensures secure recovery and protection against asset loss within a decentralised framework. We envision this wallet as a transformative step towards secure and efficient crypto-asset management, paving the way for broader institutional adoption.

Author Contributions: Conceptualisation, Y.E., J.X., N.V. and P.T.; methodology, Y.E., Y.F., J.X., N.V. and P.T.; investigation, Y.E. and J.X.; data curation, Y.E. and J.X.; writing—original draft preparation, Y.E., Y.F. and J.X.; writing—review and editing, Y.E., Y.F., J.X., N.V. and P.T.; visualisation, Y.E. and J.X.; supervision, Y.F., J.X., N.V. and P.T.; project administration, J.X., N.V. and P.T. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The data presented in this study are available within the article. Further inquiries can be directed to the corresponding author.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Baur, A.W.; Bühler, J.; Bick, M.; Bonorden, C.S. Cryptocurrencies as a disruption? Empirical findings on user adoption and future potential of bitcoin and co. In Proceedings of the Conference on e-Business, e-Services and e-Society, Delft, The Netherlands, 13 October 2015; pp. 63–80.
2. Queiroz, M.M.; Telles, R.; Bonilla, S.H. Blockchain and supply chain management integration: A systematic review of the literature. *Supply Chain. Manag. Int. J.* **2020**, *25*, 241–254. [CrossRef]
3. Linn, L.A.; Koo, M.B. Blockchain for health data and its potential use in health IT and health care related research. In Proceedings of the ONC/NIST Use of Blockchain for Healthcare and Research Workshop, Gaithersburg, MD, USA, 26–27 September 2016; ONC/NIST; pp. 1–10.
4. Hassani, H.; Huang, X.; Silva, E. Banking with blockchain-ed big data. *J. Manag. Anal.* **2018**, *5*, 256–275. [CrossRef]
5. Alzahrani, S.; Daim, T.U. Analysis of the cryptocurrency adoption decision: Literature review. In Proceedings of the 2019 Portland International Conference on Management of Engineering and Technology (PICMET), Portland, OR, USA, 25–29 August 2019; pp. 1–11.
6. Yao, A.C. Protocols for secure computations. In Proceedings of the 23rd Annual Symposium on Foundations of Computer Science (SFCS 1982), Chicago, IL, USA, 3–5 November 1982; pp. 160–164.
7. Yao, A.C.C. How to generate and exchange secrets. In Proceedings of the 27th Annual Symposium on Foundations of Computer Science (SFCS 1986), Toronto, ON, Canada, 27–29 October 1986; pp. 162–167.
8. Erinle, Y.; Kethepalli, Y.; Feng, Y.; Xu, J. SoK: Design, Vulnerabilities, and Security Measures of Cryptocurrency Wallets. *arXiv* **2023**, arXiv:2307.12874. [CrossRef]
9. Thompson, S. The preservation of digital signatures on the blockchain. *See Also* **2017**, *3*. [CrossRef]
10. Blakley, G.R. Safeguarding cryptographic keys. In Proceedings of the 1979 International Workshop on Managing Requirements Knowledge (MARK), New York, NY, USA, 4–7 June 1979; p. 313.
11. Shamir, A. How to share a secret. *Commun. ACM* **1979**, *22*, 612–613. [CrossRef]
12. Desmedt, Y.G. Threshold cryptography. *Eur. Trans. Telecommun.* **1994**, *5*, 449–458. [CrossRef]
13. Desmedt, Y. Some recent research aspects of threshold cryptography. In Proceedings of the Information Security: First International Workshop, ISW'97 Tatsunokuchi, Ishikawa, Japan, 17–19 September 1997; Proceedings 1; Springer: Berlin/Heidelberg, Germany, 1998; pp. 158–173.

14. Lindell, Y.; Nof, A. Fast secure multiparty ECDSA with practical distributed key generation and applications to cryptocurrency custody. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, Toronto, ON, Canada, 15–19 October 2018; pp. 1837–1854.
15. Kate, A.; Huang, Y.; Goldberg, I. Distributed Key Generation in the Wild. *Cryptology ePrint Archive* **2012**, *2012*, 377.
16. Pedersen, T.P. Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing. In *Proceedings of the Annual International Cryptology Conference*; Springer: Berlin/Heidelberg, Germany, 1991; pp. 129–140.
17. DeRec. 2023. Available online: https://github.com/derecalliance/protocol/blob/main/protocol.md (accessed on 26 July 2024).
18. Zengo. What is Zengo's Recovery Kit? 2024. Available online: https://help.zengo.com/en/articles/2603673-what-is-zengo-s-recovery-kit (accessed on 2 July 2024).
19. Thyagarajan, S.A.K.; Bhat, A.; Malavolta, G.; Döttling, N.; Kate, A.; Schröder, D. Verifiable Timed Signatures Made Practical. In Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security, Virtual, 9–13 November 2020.
20. Abadi, A.; Kiayias, A. Multi-instance Publicly Verifiable Time-Lock Puzzle and Its Applications. In Proceedings of the Financial Cryptography, Virtual, 1–5 March 2021.
21. Rivest, R.L.; Shamir, A.; Wagner, D. *Time-Lock Puzzles and Timed-Release Crypto*; Massachusetts Institute of Technology: Cambridge, MA, USA, 1996.
22. Malavolta, G.; Thyagarajan, S.A.K. Homomorphic Time-Lock Puzzles and Applications. In Proceedings of the IACR Cryptology ePrint Archive, Santa Barbara, CA, USA, 18 August 2019.
23. Kavousi, A.; Abadi, A.; Jovanovic, P. Timed Secret Sharing. Cryptology ePrint Archive. 2023. Available online: https://eprint.iacr.org/2023/1024 (accessed on 3 February 2024).
24. Financial Conduct Authority. Client Agreements (MiFID, Equivalent Third Country or Optional Exemption Business). FCA Handbook: Conduct of Business Sourcebook (COBS), COBS 8A.1. Available online: https://www.handbook.fca.org.uk/handbook/COBS/8A/1.html (accessed on 6 December 2024).
25. Metamask. Does MetaMask Charge a Fee for Validator Staking? 2024. Available online: https://support.metamask.io/metamask-portfolio/move-crypto/stake/validator-staking/other/validator-staking-fee/ (accessed on 1 December 2024).
26. zkPass. 2023. Available online: https://zkpass.gitbook.io/zkpass/overview/use-cases/zkkyc (accessed on 23 October 2024).
27. Chain Analysis Team. How Continuous Cryptocurrency Transaction Monitoring Gives Compliance Teams Peace of Mind. 2021. Available online: https://www.chainalysis.com/blog/kyt-continuous-monitoring/ (accessed on 14 September 2024).
28. Igboanusi, I.S.; Dirgantoro, K.P.; Lee, J.M.; Kim, D.S. Blockchain side implementation of pure wallet (pw): An offline transaction architecture. *ICT Express* **2021**, *7*, 327–334. [CrossRef]
29. Ebrahimi, S.; Hasanizadeh, P.; Aghamirmohammadali, S.M.; Akbari, A. Enhancing Cold Wallet Security with Native Multi-Signature Schemes in Centralized Exchanges. *arXiv* **2021**, arXiv:2110.00274. [CrossRef]
30. Han, J.; Song, M.; Eom, H.; Son, Y. An efficient multi-signature wallet in blockchain using bloom filter. In Proceedings of the 36th Annual ACM Symposium on Applied Computing, Virtual, 22–26 March 2021; pp. 273–281.
31. Di Nicola, V.; Longo, R.; Mazzone, F.; Russo, G. Resilient Custody of Crypto-Assets, and Threshold Multisignatures. *Mathematics* **2020**, *8*, 1773. [CrossRef]
32. Lindell, Y. Fast Secure Two-Party ECDSA Signing. *J. Cryptol.* **2021**, *34*, 44. [CrossRef]
33. Doerner, J.; Kondi, Y.; Lee, E.; Shelat, A. Threshold ECDSA from ECDSA Assumptions: The Multiparty Case. In Proceedings of the 2019 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 19–23 May 2019; pp. 1051–1066.
34. Blokh, C.; Makriyannis, N.; Peled, U. Efficient Asymmetric Threshold ECDSA for MPC-based Cold Storage. Cryptology ePrint Archive, Paper 2022/1296, 2022. Available online: https://eprint.iacr.org/2022/1296 (accessed on 1 May 2023).
35. Mavrovouniotis, S.; Ganley, M. Hardware security modules. In *Secure Smart Embedded Devices, Platforms and Applications*; Springer: Berlin/Heidelberg, Germany, 2013; pp. 383–405.
36. Copper. 2023. Available online: https://copper.co/products/digital-asset-custody (accessed on 14 April 2023).
37. Gemini Custody. 2023. Available online: https://www.gemini.com/custody (accessed on 5 January 2023).
38. Fireblocks. 2023. Available online: https://www.fireblocks.com/ (accessed on 6 February 2023).
39. BitGo. 2023. Available online: https://www.bitgo.com/products/custodial-wallets/ (accessed on 5 February 2023).
40. Genesis. 2022. Available online: https://genesistrading.com (accessed on 18 July 2022).
41. Ripple Custody. 2024. Available online: https://ripple.com/solutions/digital-asset-custody/ (accessed on 2 August 2024).
42. Tangany. 2023. Available online: https://tangany.com/ (accessed on 18 January 2023).
43. Prosegur Crypto. 2023. Available online: https://www.prosegurcrypto.com/en (accessed on 10 January 2023).
44. DLT Finance. 2023. Available online: https://dlt-finance.com/ (accessed on 2 March 2023).
45. Hex Trust. 2023. Available online: https://hextrust.com/services/hex-trust-custody (accessed on 25 February 2023).
46. BitPanda. 2023. Available online: https://custody.bitpanda.com/ (accessed on 18 January 2023).
47. GK8. 2023. Available online: https://www.gk8.io/solutions/ (accessed on 4 January 2023).

48. DigiVault. 2022. Available online: https://cointelegraph.com/news/digivault-launches-permanently-live-cryptocurrency-custody (accessed on 4 September 2022).
49. Cybavo by Circle Company. 2024. Available online: https://www.cybavo.com (accessed on 4 August 2024).
50. Bitcoin Suisse. 2023. Available online: https://www.bitcoinsuisse.com/vault (accessed on 10 February 2023).
51. Cobo. 2023. Available online: https://www.cobo.com (accessed on 4 January 2023).