

SoK: Cryptographic Key Recovery for Cryptoasset Custody and Financial Technologies

Francisco Javier Becerra Sanchez  

University of Luxembourg, Luxembourg

Antonio Ken Iannillo  

University of Luxembourg, Luxembourg

Radu State  

University of Luxembourg, Luxembourg

Abstract

Cryptoasset systems often bind cryptographic key control to financial control: losing a wallet seed, custody share, hardware device, or smart-account credential can remove spend authority, while compromised recovery can enable theft. Existing work treats recovery through separate vocabularies—key backup, secret sharing, account recovery, credential re-issuance, social recovery, and asset migration—making mechanisms and tradeoffs difficult to compare.

This paper presents a Systematization of Knowledge (SoK) on cryptographic key recovery for cryptoasset custody and financial technologies. Starting from a 118-paper systematic-review discovery corpus, we derive a 77-paper synthesis corpus and code each retained system in a master matrix covering recovered objects, recovery semantics, mechanisms, enrollment and storage, authorization, trust placement, failure events, post-recovery state, validation evidence, deployment status, privacy, usability, and limitations. The matrix supports an axis-first taxonomy that separates secret-restoring, hybrid, control-restoring, forensic/extractive, and framework-oriented recovery.

Our central observation is that recovery is not a single operation: systems may reconstruct an original secret, regenerate a seed, restore a share, reissue a credential, migrate signing authority, restore account control, move assets, or extract forensic artifacts. We derive a generalized construction model, check it against production-facing designs, and identify six findings: recovery semantics are heterogeneous; recovery shifts trust; liveness improvements create abuse paths; post-recovery lifecycle management is uneven; protocol evidence outpaces user evidence; and recovery metadata remains underprotected. These gaps motivate a research agenda for recovery-aware financial technologies.

2012 ACM Subject Classification Security and privacy → Key management

Keywords and phrases Cryptoasset Custody, Key Recovery, Wallet Security, Smart Accounts, Threshold Cryptography, Secret Sharing, Decentralized Identity, Secure Hardware

Digital Object Identifier 10.4230/LIPIcs.AFT.2026.3

Related Version *Full Version*: <https://arxiv.org/abs/2608.07104>

Supplementary Material

Collection (Reproducibility Package): <https://github.com/franciscobecerra97/Cryptographic-Key-Recovery-for-Financial-Technologies/tree/aft-2026-artifacts> [86]

Funding This research was funded in part by the Luxembourg National Research Fund (FNR), grant NCER22/IS/16570468/NCER-FT, and by FinnovationHub, funded by the Ministry of Finance of the Government of Luxembourg.

Acknowledgements The authors thank colleagues and reviewers for helpful feedback.



© Francisco Javier Becerra Sanchez, Antonio Ken Iannillo, and Radu State; licensed under Creative Commons License CC-BY 4.0

8th Conference on Advances in Financial Technologies (AFT 2026).

Editors: Aggelos Kiayias and Maria Kyropoulou; Article No. 3; pp. 3:1–3:28

Leibniz International Proceedings in Informatics



LIPICs Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

1 Introduction

In cryptoasset systems and related financial technologies, control of a cryptographic key can become control of financial value: loss may remove access to funds or services, while compromised recovery may transfer that control to an attacker. Key recovery is therefore part of the security boundary for systems that rely on cryptographic authorization [110, 92, 8, 95].

Recovery must balance two goals that pull against each other. It should prevent legitimate users and institutions from being permanently locked out after loss, unavailability, or operational failure. At the same time, it must not create a weaker path for theft, coercion, surveillance, insider abuse, or unauthorized transfer. This tension is the core reason recovery remains difficult: the mechanisms that improve availability also introduce new actors, records, and decisions that must be secured.

Existing work proposes many mechanisms, but uses incompatible vocabulary. Recovery may mean restoring cryptographic material, changing account control, moving value, reissuing identity credentials, repairing custody roles, or extracting forensic artifacts. Comparisons can therefore obscure what is actually restored and what risks remain after recovery.

This paper addresses that fragmentation through a Systematization of Knowledge (SoK) focused on cryptographic key recovery for cryptoasset custody and financial technologies. We center the paper on financial control, while including adjacent identity, data-protection, governance, and secure-hardware work when it contributes a recovery pattern that can transfer to financial systems.

Recovery is not one operation. A useful comparison must ask what control is restored, who authorizes it, what failure it handles, and what state remains afterward.

1.1 Contributions

This Systematization of Knowledge makes the following contributions:

- **Financial-technology corpus and scope.** We construct a 118-paper discovery corpus on key backup, recovery, and restoration, with auditable queries, screening flow, exclusion reasons, snowballing rounds, QA threshold, and manually verified LLM-assisted screening. We then derive a 77-paper synthesis corpus scoped around financial technologies while retaining transferable recovery patterns from identity, hardware, and data-protection systems.
- **Recovery semantics for financial control.** We distinguish secret-restoring recovery from control-restoring recovery and show why this distinction matters for financial systems. This clarifies when a system restores the same secret and when it instead restores financial control through a changed control relationship.
- **A 77-system master matrix and codebook.** We code every retained system using a controlled vocabulary for financial context, recovery semantics, mechanism family, enrollment and storage, failure events, authorization, trust placement, adversary model, post-recovery state, validation evidence, deployment status, privacy, usability, post-quantum relevance, and limitations. The full version provides the complete per-system matrix, while the reproducibility package provides the machine-readable matrix and its codebook.
- **Evaluation vocabulary, taxonomy, and construction model.** We organize mechanisms by whether they restore secrets, restore control, combine both, perform forensic extraction, or define requirements. We define adversary classes and recovery-specific safety, liveness, and privacy properties, then derive a seven-stage construction model.

- **Production practice checks and research agenda.** We check the taxonomy against six production or standards-facing recovery designs and tie six findings to matrix counts and examples, including sparse user-study evidence, under-specified post-recovery hygiene, metadata leakage, custody boundaries, recovery economics, inheritance, and post-quantum migration.

1.2 SoK Framing and Novelty

Motivation for systematization

The goal is not only to summarize prior mechanisms. We define comparable recovery semantics, code every retained system into the master matrix provided in the full version, and separate secret reconstruction from restored financial control. A threshold wallet that reconstructs an old seed, a smart account that rotates ownership, and a recovery service that moves assets are all recovery systems, but they leave different post-recovery states and abuse paths.

Novelty relative to closest related work

Prior work usually studies one slice of the problem: cryptocurrency protocols and DeFi, wallet protocols and attacks, threshold recovery, deterministic or hardware-wallet designs, smart-account recovery, identity recovery, or forensic extraction. This SoK contributes a cross-domain comparison centered on recovery semantics rather than mechanism names. Its novelty claims are: (i) secret-restoring and control-restoring recovery should be evaluated separately; (ii) post-recovery state is a first-class security property for financial systems; and (iii) recovery evidence must connect cryptographic mechanisms with operational controls, metadata exposure, production practice, and human behavior. Table 1 compares the closest prior-work clusters.

2 Background and Scope

This paper uses the term *cryptographic key recovery* broadly, but not without distinction. In the corpus, recovery may mean reconstructing an original private key, regenerating a deterministic seed, restoring a key share, reissuing a credential, transferring signing authority, recovering account control, or moving assets to a new control path. These operations differ in what they restore and in the risks they introduce.

The primary scope is financial technology: systems in which cryptographic material authorizes assets, transactions, account access, custody operations, or credentials used by financial infrastructure. This includes blockchain wallets, smart-contract accounts, custody systems, decentralized applications, decentralized identity, and secure hardware when they support financial control or transferable recovery patterns.

The paper also considers non-financial work when it contributes a mechanism relevant to financial systems. Examples include identity-management recovery, data-protection recovery, governance-related recovery, and hardware-enforced recovery. These systems are included because financial technologies often reuse the same primitives and operational patterns: secret sharing, threshold reconstruction, deterministic derivation, secure elements, trusted authorities, biometric or physical anchoring, and delegated recovery.

■ **Table 1** Closest related-work clusters and this paper’s added recovery-semantics focus.

Prior work	Scope	Recovery semantics	se-	Financial-control treatment	Corpus or evidence	This paper adds
Cryptocurrency and DeFi SoKs [6, 97, 107]	Protocols, DeFi primitives, risks, and incidents	Mostly indirect: key management, incidents, rescue windows, or mitigation		Protocol and market-level financial control	SoK syntheses and incident datasets	Recovery-specific matrix for wallets, custody, smart accounts, identity, and forensics
Wallet taxonomies and security surveys [56, 46, 45, 24]	Wallet definitions, protocols, factors, attacks, and defenses	Recovery is a feature or fallback, not the organizing axis		Wallets as transaction interfaces and attack targets	Taxonomies, SLR evidence, and incident analysis	Recovered objects, secret/-control axis, post-recovery state, and life-cycle evidence
Custody and key-management work [103, 95]	Dynamic access structures, threshold custody, HSMs, and operations	Access update, backup restoration, share reconstruction, or signer continuity		Central: assets must stay live without weakening controls	Formal constructions, prototypes, benchmarks, and cases	Cross-family comparison with regulation, economics, inheritance, production cases, and users
Web3 account recovery [110, 17, 5, 79, 22, 12, 58]	Guardians, fallback signatures, passkeys, pre-signed transfers, and composition	Concrete control-restoring mechanisms		Direct wallet and smart-account asset control	Mechanism papers, simulations, gas costs, and composability	Shows how control restoration differs from secret restoration and exposes hygiene/-metadata gaps
Identity and WebAuthn recovery [92, 93, 59, 94, 34, 60]	SSI wallets, DID backup, backup authenticators, credential reissue, and share restoration	Credential or identity-control recovery		Transferable to regulated payments and account access	Prototypes, benchmarks, and formal analyses	Separates identity restoration from asset-control recovery and maps transfer to finance
Usability and key-management studies [98, 63, 88, 90]	Human coordination, wallet mental models, memory cues, seed phrases, and factor loss	User-facing ceremonies and factor handling		Often implicit through wallet access	Three retained user-study rows plus adjacent usability evidence	Conservative user-evidence table and agenda for stress, death, phishing, and accessibility

3 Review Methodology and Corpus Construction

The contribution of this paper is the systematization, not the review protocol itself. We nevertheless used a systematic literature review (SLR) workflow as an auditable discovery process and then narrowed the final synthesis around recovery in cryptoasset custody and financial technologies.

■ **Table 2** Database search audit. The table separates library exports from normalized screening input so reviewers can trace the corpus before snowballing and SoK-stage filtering.

Database	Exported	Normalized	Syntax and filter note
Scopus	218	129	TITLE-ABS-KEY logical query; Computer Science, English, article/conference filters
IEEE Xplore	462	434	All-metadata logical query; English conference/journal records exported in BibTeX
ACM Digital Library	1,542	1,506	Full-record or metadata logical query; ACM BibTeX batch exports
ScienceDirect	2,100	2,075	Title/abstract/keywords logical query; ScienceDirect BibTeX batch exports

3.1 Guiding Questions

The review was guided by four questions: **RQ1:** What object or control relationship is recovered? **RQ2:** What cryptographic primitives, system architectures, and operational procedures enable recovery? **RQ3:** What safety, liveness, privacy, usability, and trust tradeoffs are reported? **RQ4:** What open challenges remain for wallets, smart accounts, custody systems, decentralized identity, secure hardware, and related financial infrastructure?

3.2 Discovery Corpus

We searched Scopus, IEEE Xplore, the ACM Digital Library, and ScienceDirect for peer-reviewed English-language computer-science papers on cryptographic key backup, recovery, and restoration. The search was run and exported on 14 October 2025. The logical query was:

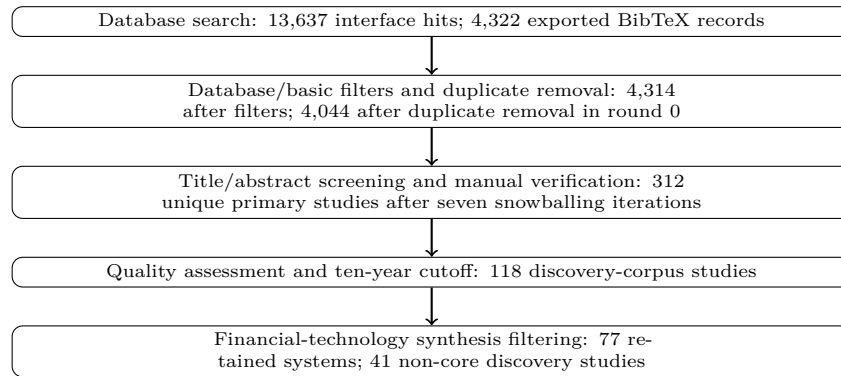
(“key” OR “private key” OR “cryptographic key”) AND (“recovery” OR “backup”) AND
 (“public key infrastructure” OR blockchain OR cryptocurrency OR wallet OR “self-sovereign
 identity” OR “decentralized identity” OR “identity management” OR “digital identity”).

The same logical query was adapted only for database field syntax and export format. Table 2 reports the database-specific search surface and counts. The SLR log records 13,637 initial database-interface hits before database-side filters; the local export audit contains 4,322 BibTeX records and 4,144 normalized records. The round-0 screening log contains 4,314 records after basic filters and 4,044 after duplicate removal.

The initial title-and-abstract screening used a Large Language Model through an API as a decision-support tool: **gpt-5** for title/abstract screening and **gpt-5-mini** for basic filtering of snowballing references. Each prompt included the candidate title and abstract, inclusion and exclusion criteria, and a request for an accept/reject verdict plus justification. Outputs were recorded as status and comments fields. Both LLM-assisted inclusions and exclusions were manually verified, and accepted records were reconciled into the round-level BibTeX files before quality assessment. The model scaled screening; it did not make final inclusion decisions.

Backward and forward snowballing were applied until convergence: a final iteration produced no new snowballing references and left the retained primary-study count unchanged at 312. Table 3 reports the round-level counts.

Table 4 summarizes grouped exclusion reasons. Title/abstract reasons were rule-coded from the manually verified decision comments. The final SoK-stage exclusions were coded from the full-text extraction rows.



■ **Figure 1** Auditable corpus-construction flow. The key transition is from broad SLR discovery to a 77-system synthesis corpus used for taxonomy, matrix counts, and findings.

■ **Table 3** Screening and snowballing counts. Round 7 provides the stopping rule. RA = research articles or candidate references; BF = after basic filters; RD = after duplicate removal; IE = cumulative retained records after inclusion/exclusion screening; BS = new backward/forward snowballing references.

Round	RA	BF	RD	IE	BS
0	13,637	4,314	4,044	129	1,820
1	1,949	1,147	817	230	1,390
2	1,620	849	623	281	668
3	950	594	478	303	208
4	511	401	360	308	67
5	375	331	321	311	21
6	332	321	315	312	5
7	317	314	313	312	0

■ **Table 4** Grouped exclusion reasons. The table distinguishes title/abstract screening exclusions from full-text SoK-stage exclusions, showing why records left the evidence base.

Title/abstract exclusion reason	Count	SoK-stage exclusion reason	Count
Cryptographic security or authentication, but no recovery	2,119	Transferable non-financial background only	28
Adjacent domain, but no recovery mechanism	1,866	Financial-adjacent but not core comparable recovery	9
Review or non-primary literature	434	Requirements or background only	4
Unrelated application or out of scope	359		
Key generation/protection, not recovery of an existing key	279		
No cryptographic private-key or ownership context	108		
Insufficient or missing abstract	15		

3.3 Quality Assessment and Discovery Corpus

After snowballing convergence, 312 primary studies were retained for quality assessment. Each study was scored using five criteria: evidence and validation; cryptographic foundations and techniques; security analysis and limitations; proposed solution or contribution; and open problems or future directions. Each criterion was scored as yes (1.0), partial (0.5), or no (0.0).

■ **Table 5** Two-stage corpus construction. Reviewers should read the 118 papers as the discovery corpus and the 77 retained papers as the evidence base for the SoK’s comparative claims.

Stage	Role in the paper	Result
SLR discovery	Identify peer-reviewed work on cryptographic key backup, recovery, and restoration through database search, manual verification, and snow-balling.	118 papers
Financial-technology ex- traction	Retain papers with concrete recovery semantics and direct or transferable relevance to wallets, custody, smart accounts, decentralized identity, secure hardware, or financial infrastructure.	77 papers

Applying the QA threshold retained 194 studies with score at least 4.0. Of these, 76 were pre-2016 foundational papers and are used as background where appropriate, while 118 had score at least 4.0 and publication year at least 2016. Those 118 studies form the discovery corpus used for full-text extraction and SoK narrowing.

3.4 Financial-Technology Synthesis Corpus

The 118-paper discovery corpus was intentionally broader than the final SoK needed to be. It included direct wallet and custody papers, but also adjacent work on generic key management, authentication, identity, hardware, cloud backup, and data protection. For the final synthesis, we therefore performed a second filtering step after full-text extraction.

Each extracted paper was coded for recovered object, secret/control recovery axis, mechanism family, enrollment and storage, recovery trigger, failure-event class, authorization, trust placement, adversary model, post-recovery state, financial-technology context, validation evidence, deployment status, privacy, usability, post-quantum relevance, and limitations. We retained papers that described a concrete recovery, backup, restoration, transfer, re-issuance, or extraction mechanism; were directly financial or clearly transferable to financial control; and contained enough detail to compare recovery semantics and tradeoffs. We excluded papers where recovery was peripheral, generic without a financial-technology transfer, or not comparable along the SoK dimensions.

This filtering reduced the corpus from 118 discovery papers to 77 synthesis papers. The excluded 41 papers were not treated as irrelevant; rather, they informed boundary-setting and background but were not used as core evidence for the taxonomy, counts, and cross-cutting findings. Figure 1 summarizes the full flow, while Table 5 summarizes the final two-stage construction.

4 Corpus Overview

The 77-paper synthesis corpus is the evidence base for the taxonomy, mechanism comparison, and cross-cutting findings. It is narrower than the 118-paper discovery corpus because the goal is to systematize mechanisms that restore cryptographic or financial control, not to catalog every paper that mentions key recovery. The retained studies are concentrated in self-custody and blockchain wallet settings, with additional evidence from institutional custody, permissioned blockchains, smart-contract accounts, decentralized identity, secure hardware, and forensic recovery. Categories are non-exclusive.

■ **Table 6** Non-exclusive corpus facets. Counts can exceed 77 within a facet when a study belongs to multiple categories.

Facet	Largest extracted groups
Financial context	Self-custody wallets (57), payment or permissioned blockchains (14), transferable non-financial patterns (15), institutional custody (11), DeFi or smart-contract applications (10), smart-contract accounts (9), decentralized identity for finance (8), secure hardware for financial infrastructure (8).
Recovered object	Original private keys (34), signing authority (20), account control (19), seed or root secrets (15), asset ownership or transfer paths (13), key shares (10), recovery keys (5), credentials (3), forensic artifacts (3).
Validation evidence	Prototypes (56), benchmarks (50), formal proofs (28), simulations (17), security games (11), case studies (9), gas-cost measurements (7), user studies (3), no evaluation in the extracted evidence (6), operational deployment evidence (1).

The venue and validation mix affects how the counts should be read. The corpus is recent-heavy: 7 of the 77 synthesis rows are from 2016–2018, while the remaining rows are from 2019 or later, with 43 conference or symposium papers, 32 journal articles, and 2 workshop or CEUR papers. This makes the evidence strongest for mechanism comparison, protocol feasibility, and engineering validation. It is weaker for deployment prevalence, recovery under stress, and operational or user outcomes, which is why we report user-study and deployment evidence separately instead of treating prototype, proof, benchmark, and deployment rows as equivalent. Table 7 reports the confidence tiers used to interpret the venue and validation mix.

The master matrix gives each retained system one auditable row covering the comparison dimensions, evidence fields, limitations, and SoK relevance. Table 8 compresses that matrix by the paper’s primary organizing axis. The reproducibility package provides the complete machine-readable matrix, its codebook, summary tables, and audit artifacts.

■ **Table 7** Venue and evidence confidence tiers used to interpret corpus counts. The tiers affect confidence in claims drawn from the counts, not whether a retained row is counted in the matrix.

Confidence tier	Rows	Count interpretation
Higher for protocol soundness	28	Strongest for cryptographic claims, safety arguments, and mechanism feasibility; weaker for deployed prevalence or user behavior.
Higher for external validity	5	Stronger support for user, forensic, or operational observations, but still narrow relative to the breadth of wallet and custody practice.
Medium engineering evidence	40	Useful for comparing implemented prototypes, benchmarks, and design tradeoffs; not enough to infer production reliability.
Lower or contextual evidence	4	Included for requirements, boundary-setting, or conceptual relevance; used cautiously and not as strong evidence for mechanisms.

■ **Table 8** Compressed view of the 77-system master matrix by recovery axis.

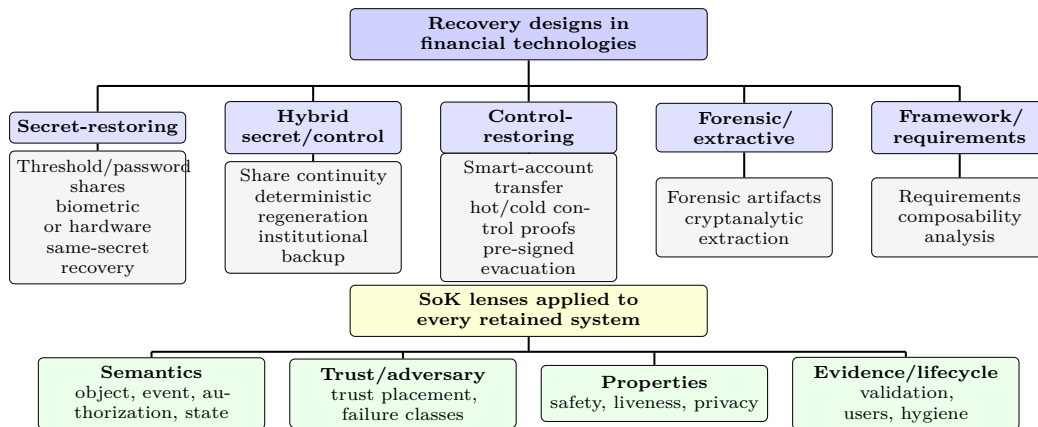
Recovery axis	Rows	Dominant mechanisms	Typical post-recovery state	Studies
Secret-restoring	38	Threshold reconstruction, password/factor-protected recovery, biometric or fuzzy regeneration, TEE/HSM-assisted recovery	Same or equivalent secret available; occasional share refresh or credential reset	[52, 98, 108, 53, 100, 43, 3, 47, 82, 92, 73, 91, 67, 80, 93, 35, 89, 66, 65, 106, 61, 88, 85, 81, 74, 55, 51, 104, 41, 105, 101, 48, 72, 10, 33, 9, 11, 18]
Hybrid secret/control	16	Deterministic regeneration, threshold continuity, institutional backup, social or guardian recovery	Secret material is restored while signing authority, custody participation, or account control may also change	[42, 70, 23, 7, 54, 68, 57, 79, 102, 59, 87, 95, 34, 78, 60, 20]
Control-restoring	16	Smart-contract control transfer, fallback or ownership proof, passkey/backup authenticator recovery, pre-signed asset evacuation	New owner, credential, signing path, or asset-control relation replaces the failed path	[110, 103, 109, 19, 17, 13, 8, 5, 4, 71, 21, 22, 96, 94, 90, 58]
Forensic/ extractive	5	Forensic artifact recovery and cryptanalytic key extraction	Artifact, credential, or key is extracted from device, backup, memory, nonce failure, or investigation evidence	[16, 62, 44, 49, 50]
Framework/ requirements	2	Requirements analysis and composability modeling	No single post-recovery state; evaluates recovery obligations or composed mechanisms	[77, 12]

5 Recovery Semantics and Evaluation Vocabulary

Recovery mechanisms in the corpus do not all recover the same thing: some reconstruct a private key or seed, some repair a threshold role, some rotate account control, and some extract artifacts after an incident. We therefore compare each design using four recovery-semantics dimensions: the *recovered object*, the *failure event*, the *authorization path*, and the *post-recovery state*. These dimensions describe what is restored, why recovery is invoked, what evidence or actors authorize it, and what control relation remains afterward. The adversary classes and recovery properties at the end of this section are supporting evaluation lenses, not additional parts of the four-part framework.

5.1 Recovered object

Recovery may reconstruct an original private key or seed, restore a share or signing role, restore account control or asset ownership, or extract forensic artifacts. Mechanisms include password-protected shares, threshold reconstruction, deterministic regeneration, biometric or physical



■ **Figure 2** Roadmap of the SoK taxonomy and lenses. The top tree groups recovery designs by the promise they make; the bottom lenses are applied to every retained system in the matrix and used in the tradeoff analysis.

regeneration, hardware-assisted retrieval, contracts, fallback keys, backup authenticators, pre-signed transactions, and ownership proofs. Table 8 lists retained studies by recovery axis, the full version provides the complete row-level coding, and Table 9 gives representative mechanism examples.

5.2 Failure event

The corpus covers several failure modes: loss of a local key, seed, device, mnemonic, or share; unavailability of threshold participants or custody roles; loss or compromise of smart-account owners; failed identity-wallet migration or backup restoration; and post-incident forensic recovery. Table 10 summarizes how these failure modes map to adversary classes. A recurring limitation is that many designs focus on loss but give less detail for compromise, coercion, malware, or malicious recovery helpers.

5.3 Authorization path

Recovery is authorized by different evidence of legitimacy. Depending on the family, authorization may require enough shares or servers, a memorized or factor-derived credential, retained root material, biometric helper data, guardian approval, contract timeouts and challenges, pre-authorized transactions, organizational procedures, hardware controls, or custody roles. The authorization basis matters because it determines who can approve recovery, who can block it, and what evidence remains after the event.

5.4 Post-recovery state

The post-recovery state is often under-specified. Some protocols return the same secret and continue with unchanged keys [52, 108]; some repair or refresh shares while preserving threshold signing authority [70, 59]; some restore access by rotating credentials or moving control to a new key [110, 22]; and some transfer assets away from a failing account [71, 58]. For financial technologies, this distinction is material: a user, exchange, or smart account that rotates ownership after recovery has a different audit and dispute problem from one that reconstructs the old private key.

5.5 Supporting adversary vocabulary

We also normalize the threat vocabulary used across papers, because terms such as “lost key,” “recovery,” and “compromise” otherwise mix different financial risks. We distinguish eight recurring classes. *Loss* means the legitimate party no longer has usable access to a key, seed, credential, device, share, passkey, or signer. *Compromise or theft* means that the material may be copied, stolen, malware-exposed, or attacker-controlled. *Coercion* means that a user, guardian, provider operator, or institutional signer is pressured to approve recovery or disclose recovery material. A *malicious helper* is a guardian, shareholder, trustee, server, or custody participant who deviates from the recovery protocol alone or in collusion. *Server or provider abuse* covers wallet providers, cloud backup services, identity verifiers, recovery providers, HSM operators, and infrastructure services that misuse their role or metadata. An *institutional insider* is an organizational actor such as an administrator, treasurer, support agent, compliance role, or recovery officer who misuses delegated recovery authority. *Unavailability* means that a user, helper, server, blockchain, signer, network, device, or institution cannot participate when needed. A *forensic adversary* attempts to extract wallet artifacts, keys, backups, traces, or evidentiary control material from devices or services.

5.6 Recovery-specific properties

Finally, we evaluate each design through three recovery-specific properties. *Safety* means unauthorized parties cannot trigger recovery, reconstruct a secret, rotate control, evacuate assets, or exploit recovery metadata to steal financial control. *Liveness* means a legitimate claimant can complete recovery after loss, participant churn, device replacement, institutional outage, or disaster without relying on a single fragile actor. *Privacy* means the recovery process does not unnecessarily reveal helper relationships, provider choices, account linkage, recovery attempts, identity-proofing material, device replacement, or forensic traces.

6 Taxonomy of Key Recovery Mechanisms

Table 9 is axis-first: mechanism families are nested under the recovery semantics they primarily realize. This avoids grouping systems once by cryptographic primitive and again by design family. The primary recovery axis is mutually exclusive and assigned by the final recovery promise and post-recovery state recorded in the master matrix. Mechanism families remain non-exclusive because some systems combine mechanisms, such as threshold reconstruction inside a hardware wallet or backup-authenticator recovery inside a smart account. Citation columns are representative; the full version provides exhaustive row-level coverage.

The primary split is between *secret-restoring* and *control-restoring* recovery. Secret-restoring mechanisms preserve the old control relation by reconstructing or regenerating the same key, seed, or share. Control-restoring mechanisms intentionally create a new control relation, for example by moving an account owner, registering a backup authenticator, executing a pre-signed transaction, or proving ownership to migrate assets. Hybrid systems combine both promises, such as restoring a share while also preserving institutional signing authority or social-account control. Control-restoring designs are not weaker merely because they do not reconstruct the original secret; they make a different promise and need different post-recovery checks. Figure 2 summarizes the taxonomy spine and the lenses applied to each retained system.

■ **Table 9** Axis-first taxonomy and design comparison. Mechanisms that reconstruct a secret, rotate control, move assets, or extract evidence make different recovery promises.

Axis	Mechanism family	What recovery restores	Enrollment or storage pattern	Examples
Secret-restoring	Threshold, password-protected, and factor-assisted reconstruction	Same key, seed, mnemonic fragment, or share	Distributed shares, password/factor material, protected server shares, backup fragments	[52, 98, 108, 53, 100, 66, 55, 105, 101, 10]
Secret-restoring	Memory-based, biometric, fuzzy, and hardware-assisted regeneration	Same or equivalent wallet-control secret	Memory artifact, helper data, biometric source, secure element, HSM, or TEE	[82, 73, 65, 88, 51, 48, 72, 33]
Hybrid secret/control	Share continuity, social/delegated recovery, biometric helper-key regeneration, and institutional disaster recovery	Secret material plus signing role, custody role, account access, or wallet-governance authority	Committees, guardians, biometric helper keys, organizational media, custody procedures, or DID backup stores	[42, 70, 7, 79, 59, 95, 34, 78, 60]
Control-restoring	Deterministic hot/cold signing-authority recovery	Future signing authority after hot-key compromise, without reconstructing the compromised hot key	Cold-wallet seed or master state, derivation path, and synchronized wallet state	[19]
Control-restoring	Smart-contract transfer, fallback signing, passkey recovery, credential re-issuance, and ownership proof	Account owner, signer, backup credential, ownership proof, or control path	On-chain state, fallback keys, backup authenticators, challenge windows, re-issuance, or proofs	[110, 103, 17, 13, 5, 21, 22, 96, 94]
Control-restoring	Asset evacuation and pre-authorized transfer	Value or asset-control relation moved away from a failed path	Pre-signed transactions, emergency controls, provider state, or encrypted transfer material	[71, 58]
Forensic/extractive	Forensic artifact recovery and crypt-analytic extraction	Wallet artifacts, credentials, keys, or evidentiary traces	Device access, backups, memory, nonce failures, investigation workflow, or seized evidence	[16, 62, 44, 49, 50]
Framework/requirements	Requirements and composability analysis	No single recovered object; compares obligations or composed mechanisms	Requirements model, key-person analysis, or formal composition model	[77, 12]

The taxonomy also separates *cryptographic trust distribution* from *operational trust distribution*. Threshold systems distribute cryptographic material but still need participant governance, refresh, authentication, and availability. Hardware systems reduce software exposure but concentrate trust in devices, attestation, or recovery artifacts. Social recovery and smart contracts reduce single-custodian dependence but add guardian, metadata, liveness, and irreversibility risks.

7 Mechanism-Family Tradeoff Analysis

Using the master matrix provided in the full version and the axis-first taxonomy, we compare safety and liveness surfaces, post-recovery hygiene and metadata privacy, and validation evidence. Table 9 gives the axis-level mechanism comparison, Table 10 adds the adversary lens, and Table 11 summarizes the obligations that follow after recovery. The family tables are cross-cutting lenses rather than primary-axis reclassifications; each cited system keeps the canonical axis assigned in the master matrix.

Table 10 Family-by-adversary comparison. Actors who improve liveness can also become collusion, coercion, provider, insider, or metadata surfaces.

Family	Loss / unavailability	Compromise / theft	Coercion / malicious helpers	Provider, insider, or forensic exposure	Examples
Threshold and password-protected reconstruction	Lost keys, shares, or passwords when enough shares/servers remain live	Exposed shares, weak passwords, or stale fragments can reconstruct	Collusion or coercion crossing the threshold	Server contact, helper membership, and recovery attempts may leak; hosted shares add provider trust	[52, 98, 108, 53, 100, 61, 55, 105, 101, 59]
Deterministic, biometric, and hardware recovery	Device, seed, mnemonic, signer, or factor loss when source material remains available	Restored seeds, helper keys, or cold-wallet authority may preserve attacker access unless old paths are quarantined	Biometrics, memories, devices, or support flows can be coerced	Vendors, attestation, HSMs, helper data, and identity checks become trust/privacy points	[19, 82, 73, 65, 88, 51, 48, 72, 33, 78, 11]
Social, guardian, and smart-account transfer	Lost owners, passkeys, or signers when guardians, fees, and windows are available	Compromised guardians, fallback signers, modules, or passkeys can rotate control	Vote buying, social engineering, recoverer abuse, and guardian collusion	On-chain proposals, guardian sets, and signer rotations can reveal distress and relationships	[110, 103, 17, 13, 7, 5, 71, 79, 21, 22, 96, 94, 90, 12, 58]
Institutional custody and disaster recovery	Signer churn, lost institutional devices, outages, and disasters	Compromised operator devices, HSM credentials, backups, or policy engines can move funds	Collusion or coercion of officers can satisfy dual-control policies	Administrators, recovery officers, compliance roles, logs, and drills expose insider/metadata surfaces	[109, 77, 102, 95, 60]
Forensic and extractive recovery	Inaccessible devices, backups, memory, nonce failures, or investigation evidence	The same extraction path can be abused by attackers or overbroad investigators	Coercion may compel device access, backup disclosure, or support escalation	Forensic traces are often the recovered object; chain-of-custody and privacy risks are intrinsic	[16, 62, 44, 49, 50]

The first comparison axis is *safety*: who can cause unauthorized recovery? Threshold systems bound exposure by shares or servers but depend on enrollment, participant independence, and refresh; smart-account and guardian systems avoid custodial key storage but add vote-buying, social-engineering, coercion, and challenge-window risks; hardware designs isolate secrets but depend on device, attestation, backup, or HSM assumptions. The second axis is *liveness*: threshold, contract, biometric, memory-based, and institutional systems can all fail when helpers, fees, inputs, terminals, or policies are unavailable. The third axis is *evidence*: the corpus validates feasibility and performance more often than recovery under stressful, high-value conditions.

■ **Table 11** Post-recovery hygiene and metadata/privacy obligations by mechanism family.

Family	Post-recovery hygiene	Metadata/privacy exposure	Common gap	Examples
Threshold and password-protected reconstruction	Rotate/rekey if compromise is possible; revoke stale fragments; refresh shares; audit helpers/servers	Helper linkage, server contact, timing, and repeated use can reveal distress or linkage	Old-secret reconstruction often lacks rotation, revocation, or dispute handling	[52, 98, 108, 53, 100, 61, 55, 105, 101, 59]
Deterministic, biometric, and hardware recovery	Revoke backups/helper data; reset authenticators; quarantine lost devices; migrate funds or rotate control if old material may still authorize value	Device replacement, helper data, vendor contact, identity checks, and account linkage expose context	Many designs lack a decision rule for continued use of restored material or retirement of old authority	[19, 82, 73, 65, 88, 51, 48, 72, 33, 78, 11]
Social, guardian, and smart-account transfer	Revoke old owners/passkeys; refresh guardians; review delays/cancellation; audit final owner state	Guardian relationships, proposals, signer rotations, challenge windows, and module state reveal attempts	Guardian reset, cancellation, rollback, and dispute handling are uneven	[110, 103, 17, 13, 7, 5, 71, 79, 21, 22, 96, 94, 90, 12, 58]
Institutional custody and disaster recovery	Rotate signer/AP-I/HSM credentials and policy roles; preserve logs; quarantine affected devices	Approver graphs, provider contacts, audits, drills, KYC, insurance, and legal holds reveal operations	Governance, notification, and disputed-instruction workflows are less uniform	[109, 77, 102, 95, 60]
Forensic and extractive recovery	Move funds or rotate keys; revoke recovered credentials; maintain chain-of-custody; quarantine devices/secrets	Device images, backups, artifacts, clusters, investigator actions, and asset movement are metadata-rich	Legitimate recovery and adversarial extraction share tooling, so authority boundaries matter	[16, 62, 44, 49, 50]

8 Generalized Construction Model

Across the taxonomy, recovery designs can be described by a common construction model. It is not a protocol template; it is a checklist of design obligations that recur across wallets, custody systems, identity wallets, and smart accounts.

1. **Control material.** The system identifies what is at risk: a private key, seed, key share, recovery key, credential, signing role, account owner, or asset-control relation.
2. **Enrollment.** The system creates recovery material before failure, such as secret shares [98, 108, 66], masked password-protected shares [52, 53, 80], deterministic seeds [19, 23, 48], biometric helper data [51, 72, 78], hardware-wrapped secrets [82, 65, 33], guardians [42, 17, 79], backup authenticators [21, 94, 11], or pre-signed transactions [71, 58].
3. **Storage and governance.** Recovery material is placed with the user, helpers, servers, institutions, smart contracts, secure hardware, cloud providers, or forensic evidence stores. This step determines whether the design is non-custodial, threshold-custodial, institutionally governed, or provider-assisted.
4. **Failure trigger.** Recovery begins after loss, unavailability, compromise, migration, death, device replacement, identity-wallet restoration, or investigation. The trigger may be user-initiated, contract-triggered, institutional, or forensic.
5. **Authorization and checks.** The system verifies that the recovery claimant is legitimate. Authorization can be cryptographic, social, institutional, on-chain, biometric, hardware-backed, or evidentiary. Strong designs separate authorization from mere possession of backup data.

6. **Recovery action.** The system reconstructs a secret, regenerates a derived key, repairs a share, reissues a credential, rotates ownership, transfers assets, or extracts an artifact.
7. **Post-recovery hygiene.** The system should decide whether to rotate keys, invalidate stale shares, revoke old authenticators, refresh guardians, record an audit event, or migrate funds. Many retained studies do not fully specify this stage, which is a central gap for financial deployments.

This construction model explains why apparently similar mechanisms differ in financial risk. A threshold wallet that reconstructs the old seed [108, 105, 101] exposes the recovered secret after completion. A smart-account recovery protocol that rotates ownership [110, 103, 22] avoids exposing the old key but must secure the transfer process. A pre-signed evacuation mechanism [71, 58] may preserve asset value while abandoning the old account. The full version walks four representative systems through all seven stages to show where their post-recovery hygiene obligations diverge. These semantics should not be evaluated under a single “key recovery” label.

9 Production Recovery Designs

The 77-paper synthesis corpus remains the peer-reviewed evidence base for this SoK. Deployed wallet and custody systems are nevertheless useful practice checks: they are not counted as corpus rows, but they show whether the taxonomy and construction model cover recovery semantics used by retail users, institutional customers, and smart-account developers. Table 12 classifies representative systems using official documentation.

Representative production recovery workflows

The seven-stage model separates production systems that all call themselves “recovery.” Ledger Recover restores seed-equivalent material through device-approved fragmentation, provider-held encrypted fragments, and identity verification. Safe{RecoveryHub} stores recoverer and delay state on-chain so a recoverer can propose owner or threshold changes unless current signers cancel. MPC custody restores a share or signer path across customer devices, provider infrastructure, passphrases, and policy. Passkey smart wallets add or replace a signer, after which stale passkeys and recovery phrases remain asset-control material.

10 Cross-Cutting Findings for Financial Technologies

10.1 Finding 1: Recovery semantics are heterogeneous

Recovery may mean reconstructing a key, regenerating a seed, restoring a share, recovering a recovery key, rotating credentials, restoring account control, transferring assets, or extracting forensic artifacts. The largest recovered-object groups are original private keys (34 studies), signing authority (20), account control (19), seeds or root secrets (15), asset ownership or transfer paths (13), and key shares (10). Counts are non-exclusive, but the design implication is clear: systems that restore account control should not be evaluated as if they reconstruct the original key.

10.2 Finding 2: Non-custodial recovery still moves trust somewhere

In this corpus, recovery mechanisms reduce or redistribute trust rather than eliminating it. Password-protected systems trust server independence and rate limiting; threshold systems trust participant diversity and share availability; hardware systems trust devices, attestation,

■ **Table 12** Production and standards-based practice checks outside the 77-paper corpus.

Design	Evidence source	Recovery axis and mechanism	Recovery action	Main SoK implication
Ledger Recover	Vendor product docs	Secret-restoring; secure-element export, encrypted fragments, HSM-backed providers	Identity checks release fragments to reconstitute seed entropy inside a Ledger secure element [64]	Restores seed-equivalent material; moves trust to identity proofing, firmware consent, providers, and HSMs
MPC custody	Vendor developer and help docs	Hybrid secret/-control; MPC share backup, signer reprovisioning, disaster recovery	Fireblocks and Coinbase Prime describe share/signer recovery through provider infrastructure, devices, passphrases, and policy [40, 39, 14]	Threshold cryptography still needs governance for passphrases, devices, signers, and disaster drills
Safe {Recovery-Hub} and modules	Safe documentation	Control-restoring; delayed recoverer module	A Recoverer proposes owner or threshold changes; signers can cancel during the delay [83, 84]	Smart-account recovery migrates control and exposes on-chain recovery metadata
ERC-4337 / EIP-7702	Standards and protocol docs	Control-restoring substrate; custom validation and EOA delegation	ERC-4337 supports custom account validation; EIP-7702 lets EOAs delegate to code using authorization tuples [26, 25, 27]	Account abstraction expands recovery design space; EIP-7702 leaves the EOA key as a bypass risk
WebAuthn/passkeys	W3C, FIDO, and product docs	Control-restoring; backup credential or passkey signer replacement	WebAuthn exposes backup state; Coinbase Smart Wallet uses a recovery phrase to create a new signer and passkey [99, 36, 15]	Passkey recovery depends on credential-provider recovery, fallback policy, and signer cleanup
Argent guardian recovery	Wallet support docs	Control-restoring; guardian social recovery with delay	Guardians approve recovery; Argent Vault recovery has majority approval and a 48-hour delay [2, 1]	Social recovery improves liveness but creates guardian availability, coercion, and relationship-metadata questions

or HSM boundaries; social recovery trusts guardians; and smart-contract recovery trusts public rules and challenge windows. In the trust and adversary fields, collusion appears in 22 rows, malicious actors in 20, server terms in 20, provider terms in 8, and insider terms in 8. These are conservative text-coded signals rather than a threat prevalence measure, but Table 10 makes the trust shift explicit. A useful recovery design should state where trust has moved.

10.3 Finding 3: Liveness improvements often create abuse paths

Adding helpers, backup authenticators, pre-signed transactions, cloud backups, or institutional procedures can prevent permanent loss while creating coercion, collusion, phishing, insider, or unilateral-transfer paths. Unavailability appears in 16 failure-event rows, while compromise or theft appears in 16 rows; the adversary text mentions collusion in 22 rows, malicious actors in 20, and coercion in 8. This tension appears across social recovery [42, 17, 79], smart-account transfer [110, 103, 5, 22], institutional custody [77, 95], and hosted or provider-assisted identity recovery [102, 94, 34]. Because coercion is rarely formalized, the observed coercion count is best read as a lower bound.

10.4 Finding 4: Post-recovery lifecycle is a common blind spot

Many studies explain how to recover but not what happens next: whether to rotate keys, refresh shares, revoke helpers, clear backup authenticators, audit the event, quarantine a device, migrate funds, or handle disputes. The post-recovery-state coding is dominated by same-or-equivalent secret restoration (46 rows), followed by new control relations or credentials (17), forensic extraction (4), operational access restored or rekeyed (3), analysis-only rows (3), asset movement (2), and share or committee refresh (2). Table 11 shows that same-secret systems need rotation or migration decisions, guardian systems need owner and helper reset, institutional systems need audit and policy cleanup, and forensic systems need chain-of-custody and authority boundaries.

10.5 Finding 5: User evidence lags behind protocol evidence

Formal proofs, prototypes, and benchmarks are common, but user-study evidence is rare. The extraction records 56 prototypes, 50 benchmarks, 28 formal proofs, 17 simulations, 11 security-game analyses, 9 case studies, 7 gas-cost measurements, and 6 rows with no evaluation in the extracted evidence. Only three retained studies include user-study evidence [98, 88, 90], and one forensic tool reports operational deployment evidence [50]. Because recovery is invoked under stress, device loss, death, institutional disruption, or suspected compromise, we treat usability claims without user data as claims, not as user evidence.

10.6 Finding 6: Recovery metadata is underprotected

Several designs protect key material while saying less about metadata: which guardians exist, which servers were contacted, whether a recovery attempt occurred, which device was replaced, which account is being migrated, or which institution is under stress. Privacy or private-state terminology appears in 51 privacy-discussion rows, but 52 rows also include limited, no-formal-analysis, not-stated, or out-of-scope caveats; metadata, contact, timing, log, linkage, trace, or surveillance terms appear in 33 rows. These counts reflect conservative coding of what papers report, not proof that every omitted discussion leaks data. The issue cuts across threshold servers [52, 61, 105], guardians [42, 79], smart accounts [103, 5, 22], identity wallets [59, 94, 34], and forensic tools [44, 50].

11 Financial, Regulatory, and Human-Factors Implications

Custody, compliance, and operational controls

Recovery becomes a regulated financial-technology concern when a provider holds, administers, restores, or can influence access to crypto-assets. MiCA-style custody rules, FATF virtual-asset guidance, and DORA operational-resilience obligations bring custody policy, client authentication, records, incident recovery, and provider duties into the design surface [32, 29, 37, 30]. This paper is not a legal analysis; the design point is that each mechanism should state whether recovery is self-custodial, provider-assisted, sub-custodial, institutional, or only a user-held backup. Obligations change depending on who verifies identity, sees recovery attempts, controls logs, and can block or reverse a disputed recovery [109, 77, 102, 95, 60].

Travel Rule metadata

Recovery designs that transfer assets, restore hosted access, or involve a crypto-asset service provider can also trigger Travel Rule information flows. FATF treats the Travel Rule as the virtual-asset application of Recommendation 16, requiring originator and beneficiary information to accompany covered transfers, while the EU implements parallel requirements for transfers of funds and certain crypto-assets in Regulation 2023/1113 and EBA guidelines [37, 38, 31, 28]. For recovery, the design implication is that identity proofing, beneficiary changes, emergency transfers, provider logs, and self-hosted-address interactions may become compliance metadata. Systems should therefore separate recovery authorization from Travel Rule reporting, minimize unnecessary recovery metadata, and state who can disclose records during disputes or investigations.

Economics and incentives

Recovery is also an incentive system. Guardians, shareholders, providers, support agents, and institutions may be unpaid, compensated, bonded, insured, or penalized; attackers can exploit those incentives through bribery, coercion, fee griefing, or collusion. Rational secret-sharing rows model some behavior [105, 101], composability work makes rational adversaries explicit [12], and pre-signed evacuation exposes fee drift and stale-UTXO issues [58]. Designs should specify who pays recovery fees, who absorbs disputed losses, and whether insurance or reimbursement changes diligence.

Inheritance and death or incapacity

Death and incapacity are not ordinary key-loss events: authority may shift to an heir, executor, trustee, provider, court, or pre-authorized beneficiary. The corpus contains only a small inheritance thread—key-person loss [77], biometric/heir wallet governance [78], re-registration recovery [18], and pre-signed recovery for owner disappearance or death [58]. Estate recovery therefore needs separate treatment for enrollment while alive, beneficiary changes, disputed claims, privacy, and post-transfer auditability.

Post-quantum migration

NIST finalized the first three post-quantum cryptography FIPS in 2024 and selected HQC for future standardization as a backup key-establishment algorithm in 2025 [75, 76]. Recovery material is migration-sensitive because wallet seeds, encrypted mnemonics, guardian secrets, recovery tokens, custody shares, and pre-signed emergency transactions may outlive active signing keys. Same-secret restoration can reintroduce classical ECDSA or Schnorr keys after

migration, so recovery should bind restored material to algorithm/version metadata and require re-derivation, fund migration, or key rotation when old material controls quantum-vulnerable addresses. Control-restoring recovery must update every path, not only the active signer: stale EOAs, guardians, fallback keys, passkeys, authorizations, and pre-signed transactions can remain bypasses. Institutional and forensic recovery also need crypto-agile policies for shares, approvals, HSM rules, audit signatures, and evidentiary records. The corpus has early signals [13, 48, 96, 94, 11], but no complete migration playbook for deployed wallets or custody systems.

■ **Table 13** User-study evidence in the retained corpus. Existing studies test tangible shares, memory cues, and multi-factor wallet recovery, but not high-stress, adversarial, estate, or broad-population recovery.

Study	Participants and task	Main finding	Main limitation for recovery claims
Offline secret sharing [98]	24-person form-factor survey; 18 completed field-study participants distributed five physical shares to 90 confidants and later retrieved enough shares for a 3-of-5 threshold	Physical share distribution and retrieval was practical, but recovery coordination could take days or weeks; paper versus plastic key tags did not dominate success	Student sample, one threshold configuration, simulated cryptographic reconstruction, and limited compliance checking
Reminisce [88]	51 participants/510 pictures for parameters, 105-person survey, and 20 wallet-experienced users who repeated picture-location recovery after one month	All 20 recovered successfully; 18 succeeded on the first attempt, with 1.10–8.29 minute recovery times and 2.56 minutes average	Repository security and authentication out of scope; fixed parameters; 20–40-year-old experienced wallet users; photo/location privacy leakage
Multi-factor key-derivation wallet [90]	27 United States participants compared custodial, conventional non-custodial, and MFKDF-based Ethereum wallet prototypes across creation, login, and recovery tasks	The MFKDF wallet reported 37% higher System Usability Scale (SUS) and 71% faster task completion than the conventional non-custodial wallet, with less seed-phrase handling	Small US-only and not gender-balanced sample; prototype fidelity limits; accessibility and marginalized populations not evaluated

Together, these studies show that tangible shares, picture-location memory, and familiar multi-factor workflows can work in controlled settings, but not how users behave under theft, grief, coercion, provider lockout, legal dispute, or market stress. Open questions include ceremony comprehension, stress errors, guardian coordination, inheritance, phishing, support escalation, accessibility, and recovery-metadata privacy.

12 **Open Problems and Research Agenda**

- **Standard recovery semantics.** Wallets, custody systems, and identity wallets need explicit terminology for original-key reconstruction, seed regeneration, share repair, credential re-issuance, control transfer, and asset evacuation. Without this, designs with different promises are difficult to compare.

- **Custody, regulation, and incentives.** Recovery mechanisms should declare whether they create self-custody, provider-assisted custody, sub-custody, or institutional obligations, and should model guardian availability, provider fees, Travel Rule metadata, reimbursement, insurance, fee drift, and collusion [105, 101, 12, 58, 32, 29, 37, 31, 30].
- **Inheritance and estate recovery.** Death and incapacity require different authorization semantics from ordinary loss, including beneficiary enrollment, revocation while alive, dispute handling, privacy, and auditability for heirs, executors, trustees, and providers [77, 78, 18, 58].
- **Composable recovery after loss or compromise.** Smart-account recovery increasingly combines guardians, backup authenticators, fallback signatures, timeouts, ownership proofs, and pre-signed transactions [103, 13, 21, 96, 58]. Research is needed on how these paths compose, and on recovery that rotates, revokes, audits, and disputes after compromise rather than only restoring after loss [52, 72, 9].
- **Privacy-preserving recovery coordination.** Recovery should hide helper relationships, server choices, attempts, and account linkage where possible, especially for threshold servers, guardians, identity wallets, and smart-contract metadata.
- **Human-centered recovery under stress.** Recovery ceremonies should be evaluated with users and operators under time pressure, grief, device loss, or fear of theft. Existing user evidence is useful but too sparse and controlled for the importance of the problem [98, 88, 90].
- **Operational threshold custody.** Threshold protocols need lifecycle support for lost shares, changing personnel, institutional disaster recovery, participant churn, and auditability [70, 59, 95].
- **Long-lived recovery material.** Wallet seeds, backup credentials, custody shares, and pre-signed recovery paths may survive for years. Post-quantum recovery is emerging [48, 94, 75], while forensic recovery raises privacy, chain-of-custody, and abuse questions [62, 44, 49, 50].

13 Ethics, Limitations, and Reproducibility

This SoK studies mechanisms that can restore or transfer financial control. The ethical risk is therefore not limited to confidentiality of keys. Recovery systems can enable theft, coercion, unauthorized transfer, insider abuse, account lockout, or exclusion from identity and financial services. For this reason, the taxonomy distinguishes what is recovered and who authorizes recovery; ambiguity in these two points can hide serious harms.

The review has methodological limitations. The search considered peer-reviewed journal and conference articles written in English and classified as computer science. The final synthesis retained 77 of the 118 discovery papers after full-text extraction and financial-technology-focused filtering. LLM assistance was used as a decision-support tool during screening, and all LLM-assisted decisions were manually verified. The resulting corpus is suitable for a focused SoK, but it does not exhaust gray literature, wallet documentation, standards drafts, or production incidents.

The extraction is also limited by the evidence reported in each paper. If a study did not state a deployment, user evaluation, privacy analysis, or post-recovery rotation procedure, we classify that evidence as absent rather than infer it. This conservative choice may understate properties implemented outside the paper, but it avoids giving recovery mechanisms credit for unstated guarantees.

For reproducibility, the paper reports the source databases, exact logical query, search/export date, database counts, de-duplication and screening counts, grouped exclusion reasons, snowballing rounds, QA threshold, retained-study count, and extracted comparison dimensions. The reproducibility package contains search-count summaries, screening-round summaries, the LLM screening protocol and prompts, exclusion-reason summaries, QA counts, extracted rows, the matrix codebook, count audits, venue/year confidence analyses, and the machine-readable 77-system master matrix. Copyrighted PDFs, raw library exports, private credentials, repository history, and private working materials are excluded from the package.

Generative-AI tools were used to support title and abstract screening and to assist with language and structural editing of the manuscript. All screening decisions and all AI-assisted manuscript content were reviewed and verified by the authors. The authors retained full responsibility for the extracted evidence, numerical counts, citations, interpretations, and final manuscript. Generative-AI tools were not treated as authoritative sources.

14 Related Work

Table 1 compares the closest external SoKs and surveys. Broad cryptocurrency and DeFi SoKs organize protocols, applications, attacks, and economic risk [98, 72, 69], while wallet-focused surveys organize protocols, authentication factors, attack surfaces, incidents, and defenses [54, 89, 35, 100]. These works establish the broader security context but do not use recovery semantics – what object or control relation is restored, who authorizes it, and what state remains afterward – as the primary unit of comparison.

The retained corpus connects bodies of work usually treated separately, including threshold reconstruction, factor- and hardware-assisted recovery, social and smart-account control transfer, decentralized-identity backup, institutional disaster recovery, and forensic extraction. This SoK makes these semantics auditable in a system-level matrix and distinguishes secret reconstruction from control restoration, signing-authority migration, credential re-issuance, asset evacuation, and forensic extraction. That distinction drives the taxonomy, construction model, and agenda.

15 Conclusion

Cryptographic recovery in financial technologies is broader than private-key backup. The retained corpus shows mechanisms for reconstructing secrets, regenerating wallet seeds, repairing shares, restoring credentials, delegating recovery, rotating account ownership, evacuating assets, and extracting wallet artifacts. A wallet that reconstructs a seed, a custody protocol that repairs a signing share, a smart account that rotates ownership, and a forensic tool that extracts artifacts are not making the same promise. Recovery-aware financial systems need explicit recovery semantics to compare safety, liveness, privacy, usability, and trust without creating new paths for theft, coercion, surveillance, or exclusion.

References

- 1 Argent. How to add a guardian to your argent ethereum wallet, 2025. Accessed: 2026-05-26. URL: <https://support.argent.xyz/hc/en-us/articles/360008013258-How-to-add-a-guardian-to-your-Argent-Ethereum-wallet>.
- 2 Argent. How to recover my wallet with guardians onchain, 2025. Accessed: 2026-05-26. URL: <https://support.argent.xyz/hc/en-us/articles/360007338877-How-to-recover-my-wallet-with-guardians-onchain-complete-guide>.

- 3 Soumya Basu, Alin Tomescu, Ittai Abraham, Dahlia Malkhi, Michael K. Reiter, and Emin Gün Sirer. Efficient verifiable secret sharing with share recovery in bft protocols. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, page 2387–2402. ACM, 2019. doi:10.1145/3319535.3354207.
- 4 Michele Battagliola, Alessio Galli, Riccardo Longo, and Alessio Meneghetti. A provably-unforgeable threshold schnorr signature with an offline recovery party. *CEUR Workshop Proceedings*, 3166:60–76, 2022. URL: <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85134323353&partnerID=40&md5=66337d80bb6e1705175aa7285cda93d4>.
- 5 Sam Blackshear, Konstantinos Chalkias, Panagiotis Chatzigiannis, Riyaz Faizullahoy, Irakliy Khaburzaniya, Eleftherios Kokoris Kogias, Joshua Lind, David Wong, and Tim Zakian. Reactive key-loss protection in blockchains. In *Financial Cryptography and Data Security. FC 2021 International Workshops*. Springer, 2021. doi:10.1007/978-3-662-63958-0_34.
- 6 Joseph Bonneau, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua A. Kroll, and Edward W. Felten. SoK: Research perspectives and challenges for bitcoin and cryptocurrencies. In *2015 IEEE Symposium on Security and Privacy*, pages 104–121. IEEE, 2015. doi:10.1109/SP.2015.14.
- 7 Micha Boro and Anna Kobusiska. Alternative authentication with smart contracts for online games. In *2021 IEEE 46th Conference on Local Computer Networks (LCN)*, pages 415–418, 2021. doi:10.1109/LCN52139.2021.9524886.
- 8 Florian Breuer, Vipul Goyal, and Giulio Malavolta. Cryptocurrencies with security policies and two-factor authentication. In *2021 IEEE European Symposium on Security and Privacy (EuroS&P)*, pages 140–158, 2021. doi:10.1109/EuroSP51992.2021.00020.
- 9 Syeda Tayyaba Bukhari, Muhammad Umar Janjua, and Junaid Qadir. Secure storage of crypto wallet seed phrase using ecc and splitting technique. *IEEE Open Journal of the Computer Society*, 2024. doi:10.1109/OJCS.2024.3398794.
- 10 Haewon Byeon, Aadam Quraishi, Praveen Thuniki, Ismail Mohamed Keshta, Mukesh Soni, and Mohammad Shabaz. Optimized security mechanism for publicly secret key sharing over cloud using blockchain. *CEUR Workshop Proceedings*, 3774:137–150, 2024. URL: <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85206453527&partnerID=40&md5=80d82f75bfa4de5397d86131d6d70b38>.
- 11 Bertrand Francis Cambou and Mahafujul Alam. Challengeresponse pair mechanisms and multi-factor authentication schemes to protect private keys. *Applied Sciences (Switzerland)*, 15, 2025. doi:10.3390/app15063089.
- 12 Panagiotis Chatzigiannis, Ke Coby Wang, Sunpreet Singh Arora, and Mohsen Minaei. A composability analysis framework for web3 wallet recovery mechanisms. *Proceedings - IEEE Symposium on Security and Privacy*, pages 1531–1546, 2025. doi:10.1109/SP61157.2025.00158.
- 13 David Chaum, Mario Larangeira, Mario Yaksetig, and William Carter. W-ots⁺ up my sleeve! a hidden secure fallback for cryptocurrency wallets. In *Applied Cryptography and Network Security*. Springer, 2021. doi:10.1007/978-3-030-78372-3_8.
- 14 Coinbase. How to secure your onchain wallet, 2026. Accessed: 2026-05-26. URL: <https://help.coinbase.com/en/prime/onchain-wallet/how-to-secure-your-onchain-wallet>.
- 15 Coinbase. Recover your smart wallet, 2026. Accessed: 2026-05-26. URL: <https://help.coinbase.com/en/wallet/getting-started/smart-wallet-recovery>.
- 16 Nicolas T. Courtois and Rebekah Mercer. Stealth address and key management techniques in blockchain systems. In *Proceedings of the 3rd International Conference on Information Systems Security and Privacy - ICISSP*. SciTePress, 2017. doi:10.5220/0006270005590566.
- 17 Weiqi Dai, Yan Lv, Kim-Kwang Raymond Choo, Zhongze Liu, Deqing Zou, and Hai Jin. Crsa: A cryptocurrency recovery scheme based on hidden assistance relationships. *IEEE Transactions on Information Forensics and Security*, 16:4291–4305, 2021. doi:10.1109/TIFS.2021.3104142.

- 18 Weiqi Dai, Yang Zhou, Xiaohai Dai, Kim-Kwang Raymond Choo, Xia Xie, Deqing Zou, and Hai Jin. Cr-dap: A comprehensive and regulatory decentralized anonymous payment system. *IEEE Transactions on Information Forensics and Security*, 20:3274–3286, 2025. doi:10.1109/TIFS.2025.3550821.
- 19 Poulami Das, Sebastian Faust, and Julian Loss. A formal treatment of deterministic wallets. In *CCS '19*, 2019. doi:10.1145/3319535.3354236.
- 20 Cristfol Daudn-Esmel, Jordi Castell-Roca, Alexandre Viejo, and Ignacio Miguel-Rodrguez. Multi-platform wallet for privacy protection and key recovery in decentralized applications. *Blockchain: Research and Applications*, 6:100243, 2025. doi:10.1016/j.bcra.2024.100243.
- 21 Varun Deshpande, Atharva Vijay Khade, Harish J, Gandhi Kishor Addanki, and Srivatsan Deenadayalan. A passkey based recovery mechanism for blockchain hardware wallets. In *2024 IEEE/ACM 17th International Conference on Utility and Cloud Computing (UCC)*, pages 276–281, 2024. doi:10.1109/UCC63386.2024.00046.
- 22 Varun M. Deshpande, J. Harish, and Atharva Vijay Khade. A practical recovery mechanism for blockchain hardware wallets. *IEEE Access*, 12:169928–169944, 2024. doi:10.1109/ACCESS.2024.3497302.
- 23 Adriano Di Luzio, Danilo Francati, and Giuseppe Ateniese. Arcula: A secure hierarchical deterministic wallet for multi-asset blockchains. In *Cryptology and Network Security*, 2020. doi:10.1007/978-3-030-65411-5_16.
- 24 Yimika Erinle, Yathin Kethepalli, Yebo Feng, and Jiahua Xu. SoK: Design, vulnerabilities, and security measures of cryptocurrency wallets. *Computer Networks*, 273:111691, 2025. doi:10.1016/j.comnet.2025.111691.
- 25 Ethereum Improvement Proposals. EIP-7702: Set code for EOAs, 2026. Accessed: 2026-05-26. URL: <https://eips.ethereum.org/EIPS/eip-7702>.
- 26 Ethereum Improvement Proposals. ERC-4337: Account abstraction using alt mempool, 2026. Accessed: 2026-05-26. URL: <https://eips.ethereum.org/EIPS/eip-4337>.
- 27 ethereum.org. Pectra 7702 guidelines, 2026. Accessed: 2026-05-26. URL: <https://ethereum.org/roadmap/pectra/7702/>.
- 28 European Banking Authority. Guidelines on information requirements in relation to transfers of funds and certain crypto-assets transfers under regulation (EU) 2023/1113, 2024. URL: <https://www.eba.europa.eu/activities/single-rulebook/regulatory-activities/anti-money-laundering-and-counteracting-financing-terrorism/guidelines-information-requirements-relation-transfers-funds-and-certain-crypto-assets-transfers>. Accessed: 2026-05-27.
- 29 European Banking Authority. MiCA article 75: Providing custody and administration of crypto-assets on behalf of clients, 2026. Accessed: 2026-05-26. URL: <https://www.eba.europa.eu/regulation-and-policy/single-rulebook/interactive-single-rulebook/17894>.
- 30 European Parliament and Council of the European Union. Regulation (EU) 2022/2554 on digital operational resilience for the financial sector, 2022. Accessed: 2026-05-26. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R2554>.
- 31 European Parliament and Council of the European Union. Regulation (EU) 2023/1113 on information accompanying transfers of funds and certain crypto-assets, 2023. Accessed: 2026-05-27. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R1113>.
- 32 European Parliament and Council of the European Union. Regulation (EU) 2023/1114 on markets in crypto-assets, 2023. Accessed: 2026-05-26. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R1114>.
- 33 Sebastian Faller, Tobias Handirk, Julia Hesse, Máté Horváth, and Anja Lehmann. Password-protected key retrieval with(out) hsm protection. In *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security*, pages 2445–2459. Association for Computing Machinery, 2024. doi:10.1145/3658644.3690358.

- 34 Mohammad Farhad, Gourab Saha, Masum Alam Nahid, Fairuz Rahaman Chowdhury, Partha Protim Paul, Mohammed Raihan Ullah, and Md Sadek Ferdous. Secure backup and recovery of ssi wallets using solid pod technology. In *2024 IEEE 48th Annual Computers, Software, and Applications Conference (COMPSAC)*, pages 1101–1111, 2024. doi:10.1109/COMPSAC61105.2024.00149.
- 35 Shahin Fatima and Shish Ahmad. Secure and effective key management using secret sharing schemes in cloud computing. *International Journal of e-Collaboration*, 2020. doi:10.4018/IJeC.2020010101.
- 36 FIDO Alliance. Synced passkey deployment: Emerging practices for consumer use cases, 2024. Accessed: 2026-05-26. URL: https://fidoalliance.org/wp-content/uploads/2024/05/Synced-Passkey-Deployment_-Emerging-Practices-for-Consumer-Use-Cases_2024-May-31.pdf.
- 37 Financial Action Task Force. Updated guidance for a risk-based approach to virtual assets and virtual asset service providers, 2021. Accessed: 2026-05-26. URL: <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html>.
- 38 Financial Action Task Force. FATF updates standards on recommendation 16 on payment transparency, 2025. Accessed: 2026-05-27. URL: <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/update-Recommendation-16-payment-transparency-june-2025.html>.
- 39 Fireblocks. Backup and recovery, 2026. Accessed: 2026-05-26. URL: <https://ncw-developers.fireblocks.com/docs/backup-recovery-1>.
- 40 Fireblocks. Backup and recovery overview, 2026. Accessed: 2026-05-26. URL: <https://developers.fireblocks.com/docs/perform-drs-process>.
- 41 Qianwen Gao and Yichi Tu. A blockchain wallet scheme with multi-factor authentication based on distributed system. In *2024 4th International Conference on Blockchain Technology and Information Security (ICBCTIS)*, pages 55–61, 2024. doi:10.1109/ICBCTIS64495.2024.00017.
- 42 Shuangyu He, Qianhong Wu, Xizhao Luo, Zhi Liang, Dawei Li, Hanwen Feng, Haibin Zheng, and Yanan Li. A social-network-based cryptocurrency wallet-management scheme. *IEEE Access*, 6:7654–7663, 2018. doi:10.1109/ACCESS.2018.2799385.
- 43 Xiaojian He, Jinfu Lin, Kangzi Li, and Ximeng Chen. A novel cryptocurrency wallet management scheme based on decentralized multi-constrained derangement. *IEEE Access*, 7:185250–185263, 2019. doi:10.1109/ACCESS.2019.2961183.
- 44 Arran Holmes and William J. Buchanan. A framework for live host-based bitcoin wallet forensics and triage. *Forensic Science International: Digital Investigation*, 44, 2023. doi:10.1016/j.fsidi.2022.301486.
- 45 Ivan Homoliak and Martin Perešíni. SoK: Cryptocurrency wallets: A security review and classification based on authentication factors. In *2024 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pages 1–8. IEEE, 2024. doi:10.1109/ICBC59979.2024.10634439.
- 46 Sabine Houy, Philipp Schmid, and Alexandre Bartel. Security aspects of cryptocurrency wallets: A systematic literature review. *ACM Computing Surveys*, 56(1):1–31, 2023. doi:10.1145/3596906.
- 47 Felix Hrandner and Christof Rabensteiner. Horcruxes for everyone – A framework for key-loss recovery by splitting trust. In *2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, pages 50–57, 2019. doi:10.1109/TrustCom/BigDataSE.2019.00017.
- 48 Mingxing Hu, Zhen Liu, and Yunhong Zhou. Efficient post-quantum secure deterministic wallet scheme. *Cybersecurity*, 7, 2024. doi:10.1186/s42400-024-00216-w.

- 49 Ah hyun Park, Hyejin Ryu, Woobeen Park, and Doowon Jeong. Forensic investigation framework for cryptocurrency wallet in the end device. *Computers & Security*, 2023. doi:10.1016/j.cose.2023.103392.
- 50 Lilita Infante, Roger A. Hallman, John Hays, Evelyn Cronnon, and Uri Stav. Recovery cat: A digital forensics tool for cryptocurrency investigations. In *2024 12th International Symposium on Digital Forensics and Security (ISDFS)*, pages 1–5, 2024. doi:10.1109/ISDFS60797.2024.10527279.
- 51 Olson Italis, Samuel Pierre, and Alejandro Quintero. Privacy-preserving model for biometric-based authentication and key derivation function. *Journal of Information Security and Applications*, 78:103624, 2023. doi:10.1016/j.jisa.2023.103624.
- 52 Stanislaw Jarecki, Aggelos Kiayias, Hugo Krawczyk, and Jiayu Xu. Highly-efficient and composable password-protected secret sharing (or: How to protect your bitcoin wallet online). In *2016 IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE, 2016. doi:10.1109/EuroSP.2016.30.
- 53 Stanisław Jarecki, Aggelos Kiayias, Hugo Krawczyk, and Jiayu Xu. Toppss: Cost-minimal password-protected secret sharing based on threshold oprf. In *Applied Cryptography and Network Security*, 2017. doi:10.1007/978-3-319-61204-1_3.
- 54 Farah Maath Jasim, Ali Makki Makki Sagheer, and Abdullah Mohammed Awad. Enhancement of digital signature algorithm in bitcoin wallet. *Bulletin of Electrical Engineering and Informatics*, 10:449–457, 2021. doi:10.11591/eei.v10i1.2339.
- 55 Woosung Jeong, Haesung Park, and Chanik Park. Keyscrub: A reliable key backup and recovery method for blockchain. *IEEE Access*, 11:91747–91755, 2023. doi:10.1109/ACCESS.2023.3308208.
- 56 Kostis Karantias. SoK: A taxonomy of cryptocurrency wallets. Cryptology ePrint Archive, Paper 2020/868, 2020. URL: <https://eprint.iacr.org/2020/868>.
- 57 Atharva Vijay Khade, Harsh Rajesh Patel, and Chirag Modi. Mnemonic phrase management and sim based two-factor authentication (2fa) for mobile wallets in blockchain. In *2023 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS)*. IEEE, 2023. doi:10.1109/ICBDS58040.2023.10346266.
- 58 Hyeonhak Kim and Sanjin Park. Cryptocurrency recovery framework using pre-signed transaction. *International Journal of Information Security*, 24, 2025. doi:10.1007/s10207-025-00994-5.
- 59 Jihwan Kim, Pyung Kim, Younho Lee, and Daeseon Choi. Key backup and recovery for resilient did environment. *Mathematics*, 12, 2024. doi:10.3390/math12060830.
- 60 Jihwan Kim, Younho Lee, and Daeseon Choi. Key-audit chain (kac): A resilient and reliable key management framework for did-based decentralized environments. *IEEE Access*, 13:141871–141885, 2025. doi:10.1109/ACCESS.2025.3597593.
- 61 Myungsun Kim, Sangrae Cho, Seongbong Choi, Young-Seob Cho, Soohyung Kim, and Hyung Tae Lee. A key recovery protocol for multiparty threshold ecdsa schemes. *IEEE Access*, 10:133206–133218, 2022. doi:10.1109/ACCESS.2022.3230683.
- 62 Ju-seong Ko and Jin Kwak. Private key recovery on bitcoin with duplicated signatures. *KSII Transactions on Internet and Information Systems*, 14:1280–1300, 2020. doi:10.3837/tiis.2020.03.020.
- 63 Katharina Krombholz, Aljosha Judmayer, Matthias Gusenbauer, and Edgar Weippl. The other side of the coin: User experiences with bitcoin security and privacy. In *Financial Cryptography and Data Security*. Springer, 2017. doi:10.1007/978-3-662-54970-4_33.
- 64 Ledger. What is ledger recover?, 2026. Accessed: 2026-05-26. URL: <https://www.ledger.com/academy/what-is-ledger-recover>.
- 65 Niko Lehto, Kimmo Halunen, Outi-Marja Latvala, Anni Karinsalo, and Jarno Salonen. Cryptovault – A secure hardware wallet for decentralized key management. In *2021 IEEE International Conference on Omni-Layer Intelligent Systems (COINS)*, pages 1–4, 2021. doi:10.1109/COINS51742.2021.9524133.

- 66 Guojia Li and Lin You. A consortium blockchain wallet scheme based on dual-threshold key sharing. *Symmetry*, 13:1444, 2021. doi:10.3390/sym13081444.
- 67 Guojia Li, Lin You, Gengran Hu, and Liqin Hu. Recoverable private key scheme for consortium blockchain based on verifiable secret sharing. *KSII Transactions on Internet and Information Systems*, 15:2865–2878, 2021. doi:10.3837/tiis.2021.08.009.
- 68 Zhen Liu, Guomin Yang, Duncan S. Wong, Khoa Nguyen, Huaxiong Wang, Xiaorong Ke, and Yining Liu. Secure deterministic wallet and stealth address: Key-insulated and privacy-preserving signature scheme with publicly derived public key. *IEEE Transactions on Dependable and Secure Computing*, 2022. doi:10.1109/TDSC.2021.3078463.
- 69 Amin Mahnamfar, Kemal Bicakci, and Yusuf Uzunay. Rostam: A passwordless web single sign-on solution mitigating server breaches and integrating credential manager and federated identity systems. *Computers & Security*, 139:103739, 2024. doi:10.1016/j.cose.2024.103739.
- 70 Sai Krishna Deepak Maram, Fan Zhang, Lun Wang, Andrew Low, Yupeng Zhang, Ari Juels, and Dawn Song. Churp: Dynamic-committee proactive secret sharing. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, pages 2369–2386. Association for Computing Machinery, 2019. doi:10.1145/3319535.3363203.
- 71 Natsume Matsuzaki, Masayuki Fukumitsu, and Yoshihiro Kita. Emergency button: Evacuation of crypto asset when key loss. In *2023 Eleventh International Symposium on Computing and Networking Workshops (CANDARW)*, 2023. doi:10.1109/CANDARW60564.2023.00048.
- 72 Ken Naganuma, Takayuki Suzuki, and Takatoshi Ohara. Leakable mnemonic phrase: A new orientation of wallets backup based on biometric-key. In *2024 International Symposium on Information Theory and Its Applications (ISITA)*, pages 325–328, 2024. doi:10.23919/ISITA60732.2024.10858205.
- 73 Ken Naganuma, Takayuki Suzuki, Masayuki Yoshino, Kenta Takahashi, Yosuke Kaga, and Noboru Kunihiro. New secret key management technology for blockchains from biometrics fuzzy signature. In *2020 15th Asia Joint Conference on Information Security (AsiaJCIS)*, 2020. doi:10.1109/asiajcis50894.2020.00020.
- 74 Vivek Nair and Dawn Song. Decentralizing custodial wallets with mfkdf. In *2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pages 1–9, 2023. doi:10.1109/ICBC56567.2023.10174998.
- 75 National Institute of Standards and Technology. Announcing approval of three federal information processing standards for post-quantum cryptography, 2024. Accessed: 2026-05-26. URL: <https://csrc.nist.gov/News/2024/postquantum-cryptography-fips-approved>.
- 76 National Institute of Standards and Technology. NIST selects HQC as fifth algorithm for post-quantum encryption, 2025. Accessed: 2026-05-27. URL: <https://www.nist.gov/news-events/news/2025/03/nist-selects-hqc-fifth-algorithm-post-quantum-encryption>.
- 77 Chan Nam Ngo, Daniele Friolo, Fabio Massacci, Daniele Venturi, and Ettore Battaiola. Vision: What if they all die? crypto requirements for key people. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 178–183, 2020. doi:10.1109/EuroSPW51379.2020.00032.
- 78 Saki Otsuki, Hiroto Tamiya, Kengo Mori, Toshiyuki Isshiki, ShinIchiro Matsuo, and Satoshi Obana. Biometrics enhances blockchain wallet governance. In *2025 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pages 1–9, 2025. doi:10.1109/ICBC64466.2025.11114682.
- 79 Allan B. Pedin, Nazli Siasi, and Mohammad Sameni. Smart contract-based social recovery wallet management scheme for digital assets. In *Proceedings of the 2023 ACM Southeast Conference*, pages 177–181, 2023. doi:10.1145/3564746.3587016.
- 80 Gyeongjin Ra, Chang-hyun Roh, and Imyeong Yeoung Lee. A key recovery system based on password-protected secret sharing in a permissioned blockchain. *Computers, Materials and Continua*, 65:153–170, 2020. doi:10.32604/cmc.2020.011293.
- 81 Avishka Rathnavibhushana, Tharinda Thamaranga, Sandaru Kaveesha, and Chandana Gamage. A social wallet scheme with robust private key recovery. In *2023 IEEE 17th International Conference on Industrial and Information Systems (ICIIS)*, pages 1–6, 2023. doi:10.1109/ICIIS58898.2023.10253598.

- 82 Hossein Rezaeighaleh and Cliff C. Zou. New secure approach to backup cryptocurrency wallets. In *2019 IEEE Global Communications Conference (GLOBECOM)*, pages 1–6, 2019. doi:10.1109/GLOBECOM38437.2019.9014007.
- 83 Safe. Account recovery with safe recoveryhub, 2026. Accessed: 2026-05-26. URL: <https://help.safe.global/articles/9622260218-account-recovery-with-saferecoveryhub>.
- 84 Safe. Safe modules, 2026. Accessed: 2026-05-26. URL: <https://docs.safe.global/advanced/smart-account-modules>.
- 85 Asia A. Salman, Nidaa Flaih Hassan, and Raghad Abdulaali Azeez. A secure private key recovery based on dna bio-cryptography for blockchain. *Iraqi Journal of Science*, 64:958–972, 2023. doi:10.24996/ij.s.2023.64.2.38.
- 86 Francisco Javier Becerra Sanchez, Antonio Ken Iannillo, and Radu State. Reproducibility Package: SoK Cryptographic Key Recovery for Cryptoasset Custody and Financial Technologies. Collection, version aft-2026-artifacts. (visited on 2026-09-16). URL: <https://github.com/franciscobecerra97/Cryptographic-Key-Recovery-for-Financial-Technologies/tree/aft-2026-artifacts>, doi:10.4230/artifacts.27945.
- 87 Aaliya Sarfaraz, Ripon K. Chakraborty, Saad Aslam, and Ahmad Sahban Rafsanjani. Optimized key recovery for blockchain wallets in sustainable supply chains. In *2024 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*, pages 343–347, 2024. doi:10.1109/IEEM62345.2024.10857165.
- 88 Jungwon Seo, Deokyeon Ko, Suntae Kim, Vijayan Sugumaran, and Sooyong Park. Reminisce: Blockchain private key generation and recovery using distinctive pictures-based personal memory. *Mathematics*, 10, 2022. doi:10.3390/math10122047.
- 89 Cheman Shaik. Securing cryptocurrency wallet seed phrase digitally with blind key encryption. *International Journal on Cryptography and Information Security*, 2020. doi:10.5121/ijcis.2020.10401.
- 90 Tanusree Sharma, Vivek C. Nair, Henry Wang, Yang Wang, and Dawn Xiaodong Song. I can't believe it's not custodial! usable trustless decentralized key management. *Conference on Human Factors in Computing Systems - Proceedings*, 2024. doi:10.1145/3613904.3642464.
- 91 Har Preet Singh, Kyriakos Stefanidis, and Fabian Kirstein. A private key recovery scheme using partial knowledge. In *2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, pages 1–5, 2021. doi:10.1109/NTMS49979.2021.9432642.
- 92 Reza Soltani, Uyen Trang Nguyen, and Aijun An. Practical key recovery model for self-sovereign identity based digital wallets. In *2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)*, pages 320–325, 2019. doi:10.1109/DASC/PiCom/CBDCom/CyberSciTech.2019.00066.
- 93 Reza Soltani, Uyen Trang Nguyen, and Aijun An. Decentralized and privacy-preserving key management model. In *2020 International Symposium on Networks, Computers and Communications (ISNCC)*, pages 1–7, 2020. doi:10.1109/ISNCC49221.2020.9297294.
- 94 Douglas Stebila and Spencer Wilson. Quantum-safe account recovery for webauthn. In *Proceedings of the 19th ACM Asia Conference on Computer and Communications Security*, 2024. doi:10.1145/3634737.3661138.
- 95 Yuto Takei and Kazuyuki Shudo. Pragmatic analysis of key management for cryptocurrency custodians. In *2024 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 2024. doi:10.1109/ICBC59979.2024.10634356.
- 96 Chen Wang, Zi Yuan Liu, and Masahiro Mambo. On the proof of ownership of digital wallets. *Cryptography*, 8, 2024. doi:10.3390/cryptography8040057.
- 97 Sam M. Werner, Daniel Perez, Lewis Gudgeon, Arian Klages-Mundt, Dominik Harz, and William J. Knottenbelt. SoK: Decentralized finance (DeFi). In *Proceedings of the 4th ACM Conference on Advances in Financial Technologies*, pages 30–46. ACM, 2022. doi:10.1145/3558535.3559780.

- 98 Oliver Wiese, Christoph Weinhold, Jan-Ole Malchow, and Volker Roth. I need this back, later! an exploration of practical secret sharing. In *Proceedings of the 34th Annual Computer Security Applications Conference*, pages 478–489. Association for Computing Machinery, 2018. doi:10.1145/3274694.3274729.
- 99 World Wide Web Consortium. Web authentication: An API for accessing public key credentials level 3, 2026. Accessed: 2026-05-26. URL: <https://www.w3.org/TR/webauthn-3/>.
- 100 Feng Xiong, Ruiyang Xiao, Wei Ren, Rongyue Zheng, and Jianlin Jiang. A key protection scheme based on secret sharing for blockchain-based construction supply chain system. *IEEE Access*, 7:126773–126786, 2019. doi:10.1109/ACCESS.2019.2937917.
- 101 Zhimei Yang, Changgen Peng, Chongyi Zhong, and Yangyang Long. Consortium blockchain private key protection scheme based on rational secret sharing and blockchain. *Computer Networks*, 242:110260, 2024. doi:10.1016/j.comnet.2024.110260.
- 102 Mert Yldz and erif Bahtiyar. A novel key management framework for secure and scalable decentralized identity systems. In *2024 17th International Conference on Security of Information and Networks (SIN)*, pages 1–8, 2024. doi:10.1109/SIN63213.2024.10871880.
- 103 Fan Zhang, Philip Daian, Iddo Bentov, Ian Miers, and Ari Juels. Paralysis proofs: Secure dynamic access structures for cryptocurrency custody and more. In *Proceedings of the 1st ACM Conference on Advances in Financial Technologies*, page 115. Association for Computing Machinery, 2019. doi:10.1145/3318041.3355459.
- 104 Yifang Zhang, Mingyue Wang, Yu Guo, and Fangda Guo. Towards dynamic and reliable private key management for hierarchical access structure in decentralized storage. In *Proceedings of the 32nd ACM International Conference on Information and Knowledge Management*, pages 3371–3380. Association for Computing Machinery, 2023. doi:10.1145/3583780.3615090.
- 105 Xingfan Zhao, Changgen Peng, Weijie Tan, and Kun Niu. Blockchain-based key management scheme using rational secret sharing. *Computers, Materials and Continua*, 79:307–328, 2024. doi:10.32604/cmc.2024.047975.
- 106 Wenbo Zheng, Kunfeng Wang, and Feiyue Wang. Gan-based key secret-sharing scheme in blockchain. *IEEE Transactions on Cybernetics*, 51:393–404, 2021. doi:10.1109/TCYB.2019.2963138.
- 107 Liyi Zhou, Xihan Xiong, Jens Ernstberger, Stefanos Chaliasos, Zhipeng Wang, Ye Wang, Kaihua Qin, Roger Wattenhofer, Dawn Song, and Arthur Gervais. SoK: Decentralized finance (DeFi) attacks. In *2023 IEEE Symposium on Security and Privacy*, pages 2444–2461. IEEE, 2023. doi:10.1109/SP46215.2023.10179435.
- 108 Xiuwen Zhou, Qianhong Wu, Bo Qin, Xinyi Huang, and Jianwei Liu. Distributed bitcoin account management. In *2016 IEEE Trustcom/BigDataSE/ISPA*, 2016. doi:10.1109/TrustCom.2016.0052.
- 109 Fangdong Zhu, Wen Chen, Yunpeng Wang, Ping Lin, Tao Li, Xiaochun Cao, and Long Yuan. Trust your wallet: A new online wallet architecture for bitcoin. In *2017 International Conference on Progress in Informatics and Computing (PIC)*, pages 307–311, 2017. doi:10.1109/PIC.2017.8359562.
- 110 Yanlin Zhu, Lirong Xia, and Oshani Seneviratne. A proposal for account recovery in decentralized applications. In *2019 IEEE International Conference on Blockchain (Blockchain)*, pages 148–155, 2019. doi:10.1109/Blockchain.2019.00028.