

The sword and the seal: Crypto asset recovery as quasi-legal mobilization under fragmented authority

AUTHORS: Ruoran Lai and Zehan Lin

SUMMARY: This article explores how legal intermediaries mobilize fragmented authority to recover stolen crypto assets post-hack. It introduces a four-task model of quasi-legal mobilization, focusing on the recovery process from 2016 to 2026, involving 468 major hacks. The study draws on 128 interviews and 4,775 public documents.

METHOD: The research employs a mixed-methods approach, combining qualitative interviews with quantitative data analysis. The sample includes 468 major crypto hacks from 2016 to 2026, providing a comprehensive timeline of recovery efforts.

KEY FINDINGS:

- Legal intermediaries classify harm, translate technical evidence, connect claims to enforcement actors, and sequence forums to facilitate recovery.
- Recovery processes are highly dependent on victims' access to institutional leverage and elite intermediaries.
- Quasi-legal mobilization reduces legitimacy ambiguity by producing recognition across public and private sites.

IMPLICATION FOR TRADING: Understanding the role of legal intermediaries in crypto asset recovery is crucial for traders and investors. This knowledge can help in formulating strategies to protect assets and navigate the complex legal landscape. Traders should be aware of the potential delays and dependencies on intermediaries, which can impact the speed and success of recovery efforts.

The sword and the seal: Crypto asset recovery as quasi-legal mobilization under fragmented authority

Ruoran Lai¹, Zehan Lin²

How are digital property rights protected when crypto assets move rapidly across borderless infrastructures, and when information and remedial capacity are fragmented across multiple public and private domains? To unpack this problem, this article develops a four-task model of quasi-legal mobilization under fragmented authority. We use recovery after crypto hacks as our primary case study. Drawing on 128 interviews, 4,775 public documents, and a dataset of 468 major crypto hacks from 2016 to 2026, we show how legal intermediaries characterize the wrong, substantiate claims with portable proof, authorize relief, and sequence forums. These practices offer an emerging institutional template for protecting property rights in the digital context. However, it may also make relief dependent on victims' access to institutional leverage and elite intermediaries. The article recasts legal intermediaries as central institutional actors and shows how second-order legal consciousness enables legality to travel across fragmented authority.

Keywords: legal mobilization; fragmented authority; legal intermediary; property rights; digital technology

1 Introduction

Crypto hacks pose a recurring challenge for law enforcement because on-chain assets can cross jurisdictions long before courts can grant enforceable relief. In 2025, hackers stole more than \$3.4 billion in cryptocurrency by exploiting vulnerabilities in wallets and decentralized finance (DeFi) smart contracts (Chainalysis Team 2025). However, more than 47% of the stolen assets were recovered in 2025, largely through on-chain freezes and blacklisting, which shows that there is quasi-legal enforcement proceeding recovery before courts or police could act. Victims seeking restitution relied on an ecosystem of exchanges, on-chain sleuths, protocol governors, stablecoin issuers, and other actors that controlled distinct points at which technical and institutional interventions could be imposed. This fragmentation raises a puzzle: how are digital property rights protected when the information and capacity needed to recover assets are dispersed across private and public actors, while formal legal intervention remains slow or unavailable?

We conceptualize post-hack recovery as quasi-legal mobilization under fragmented authority. Legal mobilization seeks to activate public authority through legal interpretation and institutional access (Vanhala 2018). Building on this, we defined quasi-legal mobilization as a related but less institutionally settled process: actors seek to activate dispersed public and private authority without a clear mandate from sovereign law. Post-hack recovery fits this model, since legal intermediaries turn a loss into a recovery by coordinating across different forums, and adapt legal categories and evidentiary forms to the legitimacy judgments anticipated in each forum, seeking remedies without direct sovereign command.

Existing research on legal mobilization shows that victims must name and claim their injuries (Black 1973; Felstiner, Abel, and Sarat 1980–81). Later work further shows that the process is extended beyond formal lawsuits, showing that legal meanings are often mobilized outside courts (McCann 2006). Yet much of this

¹ School of Law, Sun Yat-sen University, Email: lairr5@mail2.sysu.edu.cn.

² School of Philosophy, Wu Han University, Email: zehanlin9@gmail.com.

literature still assumes that a central authority can ultimately resolve the dispute. It offers less guidance for digital environments where the capacity to intervene is distributed across multiple platforms and private firms, while formal coercive power remains with state agencies. This separation between operational capacity and legal authority makes legitimacy ambiguous. dispute resolution practices suffer from both fragmented authority and ambiguous legitimacy. An intervention accepted by one forum as necessary recovery may be viewed by another as unauthorized control.

Blockchain's borderless architecture turns post-hack recovery into a form of quasi-legal mobilization. The legal meaning of a digital loss is rarely settled at the outset. An incident may be treated as theft or understood as an exploit. It may instead be attributed to faulty code or a failure of governance. These characterizations alter liability and the evidence required for intervention, opening or closing particular routes to recovery (McCann 2006). To activate fragmented authority, legal intermediaries first classify the harm and translate technical traces into evidence that can support action. They then connect claims with actors able to enforce them (Vanhala 2018). Legal consciousness makes these claims intelligible across fragmented forums (Ewick and Silbey 1998). Because private intervention often occurs outside formal adjudication, intermediaries must anticipate how others will judge its legitimacy. They frame intervention as fair and necessary to secure the recognition on which enforcement depends (Chua and Engel 2019). Quasi-legal mobilization reduces legitimacy ambiguity by producing legitimacy across public and private sites.

Prior research presents legal intermediaries as actors who put regulation into practice and monitor compliance (Kraakman 1986; Abbott, Levi-Faur, and Snidal 2017). Other studies examine how professionals interpret formal laws within organizations (Edelman, Uggen, and Erlanger 1999; Edelman et al. 2011). Our analysis extends this work to digital disputes, where legal intermediaries organize the protection of property rights. They translate digital losses into claims that relevant forums can recognize and connect those claims to actors capable of providing relief. Their role therefore lies in making recovery institutionally possible when no single authority controls the process.

Drawing on 128 interviews and 4,775 public documents, we analyze 468 major crypto hacks between 2016 and 2026. The analysis traces four linked processes of quasi-legal mobilization. Actors first characterize the wrong by deciding whether an ambiguous incident constitutes theft or an exploit. Some incidents are instead attributed to faulty code. This characterization shapes how they substantiate the claim, since on-chain traces must be translated into proof that other actors can use. They then seek to justify relief by establishing the legitimacy of interventions such as asset freezes. Recovery also depends on forum sequencing. Actors move between public authorities and private firms while engaging decentralized governance bodies to secure and enforce remedies. We argue that post-hack recovery is a form of quasi-legal mobilization dealing with how fragmented authority operates under ambiguous legitimacy. Distributed capable actors construct a form of legal consciousness from the bottom up, reframing claims into structures that diverse forums can recognize and act upon.

This article makes three contributions. First, it extends legal mobilization scholarship by showing how legal protection is assembled when authority is fragmented. In digital disputes, remedial action proceeds through networks of private and technical actors rather than through a single public court. Second, it specifies how legal intermediaries stabilize contested incidents. They classify ambiguous losses and turn digital traces into evidence that can support intervention. Third, it connects legal ambiguity to debates on legal consciousness

and digital property. Formal law alone does not confer legitimacy on private intervention. Legitimacy emerges as actors present their actions as lawful and fair while explaining why intervention is warranted to relevant audiences. These findings offer a broader model of property-rights protection for disputes in which remedial capacity is divided among actors who control different points of intervention.

2 Four-task framework of quasi-legal mobilization

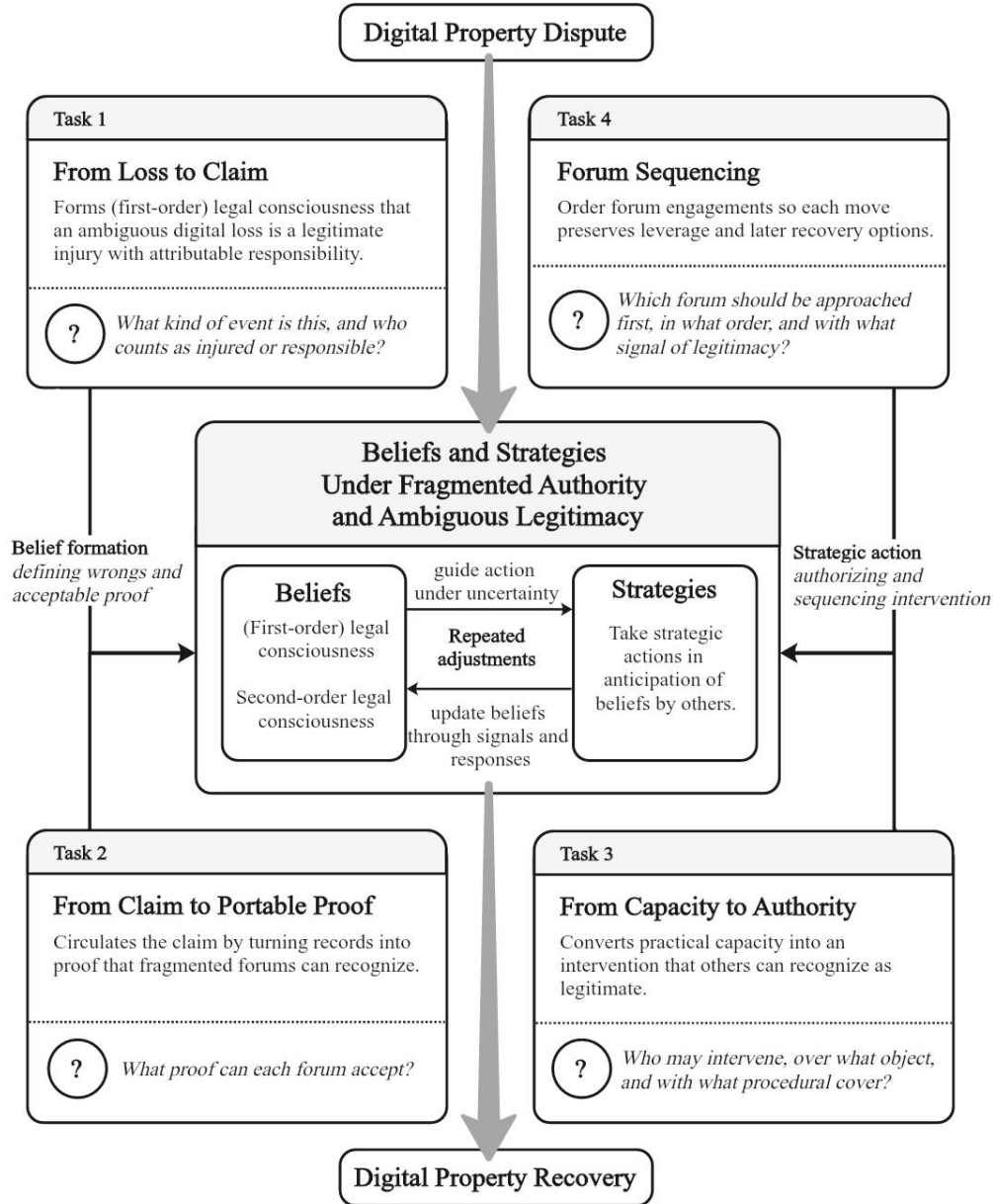
This article conceptualizes the primary task of post-hack asset recovery as making assets recoverable under fragmented authority (Ostrom 2010) and vague legitimacy. In established fields such as environmental activism, legal mobilization generally takes place within an institutional order in which actors can invoke recognized rights and procedures (Kim and Arrington 2023). Quasi-legal mobilization begins where evidentiary standards and sources of legitimacy remain unsettled. Actors develop and revise these standards as recovery proceeds. Across fragmented forums, they define the incident as a legally cognizable wrong and translate technical traces into acceptable proof. They must also establish why a proposed intervention constitutes legitimate relief (Kim and Arrington 2023). The resulting quasi-legal order is bottom-up and dynamic. It is produced and stabilized through the continuing governance of the incident (Ostrom 2010).

We develop a four-task model to further analyze the primary task involved in quasi-legal mobilization. The four tasks in our framework are linked by the interaction between belief and strategy under incomplete information (Figure 1). Beliefs refer to actors' subjective assessments of what has occurred and what law or fairness requires (Cooter 1998). They encompass legal consciousness and second-order legal consciousness. The latter concerns how actors expect others to judge legality and procedural propriety (Kreps and Wilson 1982; Headworth 2020). These expectations guide strategic choice. Actors select courses of action that preserve the prospect of asset recovery while reducing the risk that private intervention will be regarded as arbitrary or unlawful (Young 2014).

Strategies also reshape beliefs. In digital property disputes, each move sends a signal about the nature of the dispute and the claimant's credibility (McAdams and Nadler 2008). Other actors use these signals to judge whether intervention is warranted and what risks it may carry. This feedback operates throughout recovery. A strict legal framing may prompt formal action while narrowing the scope for private negotiation (McCann 2006). Evidence can move across organizations only when it meets their procedural requirements. A request for intervention likewise succeeds only when the recipient regards it as proper and justified (Sunshine and Tyler 2003). Each strategy therefore changes the conditions of subsequent action. It may support recovery by stabilizing expectations, or constrain later moves by making the request appear premature or illegitimate.

Thus, the primary task of Quasi-legal mobilization is unfolded through repeated adjustment between beliefs and strategies (Chua and Engel 2019). Claimants base their actions on how they expect others to view the law and evidence. Target audiences interpret these moves and update their own beliefs. In response, claimants must adjust their next steps (Lehoucq and Taylor 2020). Our four tasks model outline how actors organize this process. They move from a raw loss to a structured claim, turn that claim into portable proof, justify the exercise of authority, and sequence their forum choices. These are not separate steps in a linear path. They are deeply linked. Every move alters the playing field, determining whether the next strategy will actually be seen as credible and legitimate (Sunshine and Tyler 2003).

Figure 1. From digital loss to recovery: A four-task model of quasi-legal mobilization under fragmented authority



2.1 From loss to claim

The formation of legal consciousness begins with transforming a loss into a claim. As Black (1973) observes, legal systems do not automatically acquire cases. Raw injuries must first undergo a social transformation that can prompt institutional action. Felstiner et al. (1980–1981) show that harm must be named as an injury, blamed on an identifiable actor, and claimed through a demand for remedy. Quasi-legal mobilization therefore begins when a grievance is translated into a rights-based appeal to authority (Zemans 1983). We conceptualize the first task of asset recovery as this transition from loss to claim. Actors must stabilize an account of the incident that can support the production of proof and a subsequent request for authorized intervention.

Existing scholarship explains why recovery depends on coordination and how this process helps diffuse

legal consciousness among targeted actors, but offers less detail on how ambiguous incidents become actionable claims. Specialized actors use structural advantages to navigate legal institutions and sometimes reshape them (Galanter 1974; Barnes and Burke 2012). Strategic networks recast claims in forms that particular institutions can process (Vanhala 2018; Kahraman 2023; Jodoin and Wewerinke-Singh 2025). Legal intermediaries also connect dispersed evidence to formal authorities, thereby opening new routes for action (Savelsberg, LaBranche, and Philips 2025). This literature shows that mobilization depends on making a grievance institutionally legible before legal remedies can be pursued.

To prompt intervention, victims must frame the incident as a wrong and identify the actor or infrastructure to which responsibility attaches. Courts often struggle in dealing with pseudonymous wallets and jurisdictional gaps, so recovery extends across formal and quasi-legal forums (McCann 2006). Whether a harm becomes actionable also depends on the technical expertise and organizational capacity available to translate it into an institutional claim (Vanhala 2022). Where formal enforcement does not align with the decentralized infrastructure through which the loss occurred, quasi-legal practices provide the main routes through which recovery can proceed (Lehoucq and Taylor 2020).

In digital property disputes, claim-making begins by translating technical disruption into a recognizable wrong. Raw network data must be interpreted to distinguish an actionable violation from legitimate activity or system error. This framing defines the harm and attributes responsibility, while identifying the institutions from which intervention is sought. Because authority is fragmented, actors must adapt the claim to the forum they approach (Ostrom 2010). Each forum recognizes different grounds for action and may require a different account of the same incident. Claim-making therefore links the characterization of the wrong to the remedy requested. As recovery proceeds, actors revise this account to preserve its institutional legitimacy and strengthen their bargaining position.

In blockchain networks, an asset transfer is initially a neutral technical event. It becomes a claim when recovery actors interpret the outflow as a malicious exploit and assign responsibility for the loss. This account must distinguish the incident from legitimate activity or a systemic failure. Once the loss is framed as an actionable wrong, actors must substantiate the claim with evidence that independent institutions can verify.

2.2 From claim to portable proof

Claims can move across institutions only when they are expressed as evidence that each forum can assess. This requirement creates legitimacy ambiguity because forums do not share a common standard for what counts as sufficient proof. Research on organizational mediation shows how professionals manage such uncertainty by translating unsettled expectations about proper conduct into institutionally recognizable forms (Edelman 1992; Edelman and Suchman 1997; Gray and Silbey 2014). Building on this insight, we define the second task of recovery as the transition from claim to portable proof. Once the event has been characterized, actors must assemble evidence that can secure recognition across forums despite the absence of common evidentiary standards.

Existing scholarship shows that evidence is produced rather than simply discovered. Quasi-legal mobilization therefore depends on knowledge production, as actors must present claims in forms that institutions can treat as actionable (Kim and Arrington 2023). Research on organizations and regulation likewise shows how professionals mediate ambiguous legal mandates through established procedures and interpretive work (Edelman 1992; Abbott, Levi-Faur, and Snidal 2017). However, these studies largely

examine evidentiary interpretation within bounded institutional relationships. They offer less insight into how proof travels across fragmented forums, where recognition depends on multiple institutions with different evidentiary requirements.

In digital property disputes, portable proof is created by turning dispersed technical traces into an evidentiary bundle that institutions can assess. Transaction records and platform communications must be organized into an account that links the available evidence to an unauthorized loss or transfer. The bundle must also establish the claimant's standing and identify a specific object of intervention, such as an account or infrastructural node. It is then adapted to the forum in which relief is sought. Platforms apply their own procedural requirements, while courts and governance bodies may demand different forms of proof.

Portability refers to the capacity of evidence to move across forums while preserving the claim it supports. Once technical traces are organized into a coherent package, public and private authorities can assess their relevance to the disputed loss. However, private interventions may not guarantee universal institutional recognition. Evidence may establish the basis of the claim and identify an object against which action can be taken, but each institution remains bound by its own procedures and authority. The next task is therefore to turn recognized proof into justified relief.

2.3 From capacity to authority

Portable proof makes a claim recognizable, yet action still requires authorization. Claimants must connect a substantiated claim to an intervention that other participants regard as legitimate. Existing research shows how gatekeepers use expertise and institutional position to shape legal outcomes (Galanter 1974; Kraakman 1986; Barnes and Burke 2012). Under fragmented authority, technical control over an asset does not itself confer a right to exercise that control. Other actors must accept the proposed action as a limited and justified form of relief. We therefore define the third task of recovery as the transition from capacity to authority. This transition requires an authorization script that links the available proof to a specified intervention and explains why the actor may carry it out.

In a quasi-legal order, legitimacy depends on whether private intervention can be rendered legally recognizable. Second-order legal consciousness provides the practical framework through which actors judge what constitutes fair and appropriate conduct (Ewick and Silbey 1998). The progression from first-order to second-order legal consciousness occurs when beliefs are translated into strategic action. Digital disputes often develop before state authorities can respond, leaving private actors to intervene without a direct legal mandate. They seek legitimacy by aligning their actions with established legal forms. This alignment allows institutional audiences to interpret the intervention as justified and procedurally intelligible when it is later reviewed (Chua and Engel 2019).

This legitimacy is state-referential, although it is not conferred directly by the state. Private actors use law as a shared language through which intervention can acquire bottom-up legitimacy. They present the measure as a limited act of preservation and anticipate the possibility of later review by public authorities. This expectation shapes how the intervention is designed, even when formal authorities never become involved. The measure must remain compatible with subsequent legal proceedings (Sunshine and Tyler 2003). Standardized compliance records and targeted procedural requests support this compatibility. They connect the exercise of private control to a form of relief that other institutions can recognize as authorized (Edelman 1992; Edelman et al. 2011).

The authorization process relies on organizational forms of legitimacy. When law is ambiguous, institutions use compliance structures and established procedures to make their obligations manageable (Edelman et al. 2011; Gray and Silbey 2014). In digital settings, these routines turn external requests into formal institutional decisions. Once portable proof establishes the factual basis of a claim, actors must construct an authorization script. The script identifies the assets subject to intervention and sets the limits of the proposed relief. It also determines how the measure may later be reviewed or reversed. Its function is to convert established proof into a defined course of action.

Once an intervention is recognized as legitimate, actors must decide how to deploy it. Early moves can alter the prospects for later negotiation or formal legal action. The effect of authorized relief therefore depends on the forum in which it is pursued and its position within the wider sequence of recovery. This problem defines the final task: forum sequencing.

2.4 Forum sequencing

Actors without authority must decide which forum to approach first and anticipate the signal that this choice will send. The initial response may then expand or constrain the options available later. Sociolegal scholarship explains forum choice through resource constraints and procedural barriers (Vanhala 2018; Lehoucq and Taylor 2020). Other work emphasizes actors' expectations about how legal audiences will judge their claims (Ewick and Silbey 1998; Chua and Engel 2019). These accounts largely treat forum choice as a discrete decision. Under fragmented authority, engagement with one institution changes how subsequent moves are understood. It can alter both their credibility and their legitimacy. We therefore conceptualize the fourth task as forum sequencing.

Sequencing is the strategic process of preserving future options while acting before loss becomes irreversible. In digital property disputes, actors first identify the forums that can recognize a claim and the institutions capable of exercising control (Hoffmann 2003; Larson 2004). They then assess what each forum can deliver at a given moment and what is required to elicit a response. Actors stage their engagements so that recognition secured in one setting can support action elsewhere. An earlier move may strengthen the credibility of a later request or reduce the risks attached to intervention. Sequencing therefore depends on temporal fit. Claimants must approach a forum once the available evidence is sufficient to make it receptive, yet before delay deprives the remedy of practical value.

Forum sequencing requires actors to decide which institution to approach first and how to frame the request. This judgment depends on second-order legal consciousness, defined as actors' expectations regarding how other participants understand legality and how those understandings will shape their responses (Ewick and Silbey 1998; Chua and Engel 2019). Actors therefore bargain in the shadow of anticipated judgment, predicting how institutional audiences will classify the claim (Young 2014). Market routines and organizational settings gradually stabilize these expectations. Some strategies become viable, while others carry costs that make their use unlikely (Hoffmann 2003; Larson 2004). To move a dispute across fragmented forums, actors may combine a formal legal claim with a moral justification that remains intelligible to audiences operating under different standards.

In digital property disputes, claimants assess both the immediate effect of an action and how relevant audiences may interpret it (Cooter 1998). An asset preservation request may protect the disputed property while signaling a capacity to escalate. Private negotiation preserves flexibility, but may weaken the claim before

audiences that expect formal action. The viability of each move therefore depends on how it changes the reception of later interventions across forums (Vanhala 2018; Duan 2025). Sequencing is the practice of ordering those interventions in anticipation of such responses.

Legal intermediaries turn claims into actionable proof by organizing information in forms that institutional audiences can assess. Third parties interpret institutional expectations and relay relevant information through the governance system (Abbott, Levi-Faur, and Snidal 2017). Where state oversight is delayed or remote, professional service providers may assume governance functions that public authorities cannot perform promptly (O'Rourke 2003). This pattern is evident in blockchain ecosystems, where forensic firms and on-chain investigators often respond before state agencies can act. But their role extends beyond reporting existing legal requirements. They shape how organizations understand the legal risks attached to an incident and which forms of intervention appear available (Sytych and Kallapur 2025).

Drawing on this literature, we conceptualize digital asset recovery as four linked tasks of legal mobilization: moving from loss to claim, from claim to portable proof, from capacity to authority, and from forum choice to sequencing. Our analysis of crypto hacks shows that these tasks are recursive rather than discrete. Although they often follow a loose chronological order, new developments may require actors to revise an earlier claim, rework the available proof, or reconsider the sequence of forums.

3 Data and method³

This article uses a multi-source qualitative design to explain how post-hack asset recovery becomes actionable under fragmented authority. The analysis focuses on the practical work through which actors make recovery possible. It draws on 128 in-depth interviews and an archive of 4,775 public documents. We also compiled an original database of 468 major crypto hacks between 2016 and 2026. The interviews reveal how actors formulate claims and pursue redress. The documentary material reconstructs recovery episodes such as Poly Network and Nomad, while the database places these cases within broader patterns across the sector. Comparing these sources links actors' practical reasoning to observable recovery processes and their wider distribution. This triangulation allows us to assess whether the four tasks recur beyond the most visible cases. Parenthetical citations to original materials below identify the relevant interview transcripts, public-document corpus, or event database held by the authors.

The interview corpus comprises 128 semi-structured interviews conducted between July 2025 and April 2026 with participants in, and knowledgeable observers of, the recovery field (Appendix A). Because recovery decisions are sensitive and rarely visible to outsiders, we used purposive sampling supplemented by snowball recruitment. Sampling sought variation in the functions participants performed. Some constructed claims or assessed proof, while others controlled technical or organizational chokepoints or explained interventions to external audiences. Interviewees included on-chain investigators (n = 16), exchange employees (n = 17), and staff from stablecoin issuers (n = 10). The sample also covered cryptocurrency investors (n = 16), project team members (n = 22), key opinion leaders (KOLs) (n = 14), journalists (n = 16), lawyers (n = 13), and prosecutors (n = 4).

The interview guide followed the course of recovery from the initial classification of an incident to the

³ This study received approval from the relevant institutional review board. For anonymous review, the name of the institution and approval details are withheld and will be restored upon acceptance.

preparation of materials for third-party intervention. It also examined how actors assembled proof and decided when to engage adversaries. Respondents described the operational constraints they faced and the tactics used in negotiation. These accounts reveal second-order legal consciousness by showing how actors anticipated external responses. Such judgments are often absent from formal public accounts.

The public-document corpus reconstructs the visible record of post-hack recovery. We classified the 4,775 documents according to their role in the recovery process. Technical and forensic analyses informed incident characterization, while bounty pages and recovery guidelines documented proof-building. Real-time communications and governance updates captured negotiation. Regulatory notices, legal filings, and platform policies showed how actors sought authorized relief. The event database covers 468 major hacks between January 2016 and April 2026 and maps the wider field. For each event, we recorded when the incident became public and how disclosure developed. We also traced the production of evidence and changes in attribution confidence. Resolution coding identified whether actors negotiated or pursued enforcement and recorded the share recovered. Because these measures derive from public documents, the database captures visible recovery practices rather than private coordination. It places the focal cases within a broader empirical universe. (Public-document corpus; event database).

From the field map, we selected four cases to foreground different tasks in the recovery process. Poly Network illustrates characterization, while Nomad shows how root-cause analysis and data coordination substantiate a claim. Multichain foregrounds authorization through the construction of a defensible legal claim. Euler illustrates sequencing through legal threats and targeted communication. The database identifies scope conditions and broader patterns across the sector. The cases provide procedural detail that cannot be recovered from coded variables alone.

Analysis proceeded iteratively between event reconstruction and interpretation. Database coding was repeatedly checked against interview accounts and focal-case comparisons. For key incidents, we constructed timelines that followed the process from initial disclosure to resolution. Documentary evidence was then coded according to the four tasks. The analysis examined how an exploit became a public wrong and how supporting proof moved across institutions. It also traced the development of negotiation and enforcement, including which routes assumed primary or secondary importance in recovery.

Triangulation linked recurring patterns to the reasoning and processes that produced them. The database shows how often observable patterns recur, but cannot explain why actors select a particular proof bundle or sequence of forums. Interviews provide this reasoning by revealing how actors anticipate the responses of others. Focal cases then show how these expectations shape recovery over time as documentary records interact with private judgment and organizational practice. We retained an interpretation only when it was supported across these sources. (Interview transcripts; public-document corpus; event database).

Table 1 summarizes the four recurrent tasks that structure the analysis. The tasks may overlap and recur, although they often become salient in a loose temporal order.

Table 1. Four recurrent tasks of legal mobilization under fragmented authority

Task	Analytic question	Observable indicators	Failure mode
Characterizing the wrong	How is the event defined, and to whom are injury and responsibility attributed?	Initial narrative frame; timing of disclosure; disputes over classification; public labeling	The wrong remains unsettled, making later requests appear premature, contested, or strategically motivated.
Substantiating the claim	What evidence will the forum		Observable traces fail to become

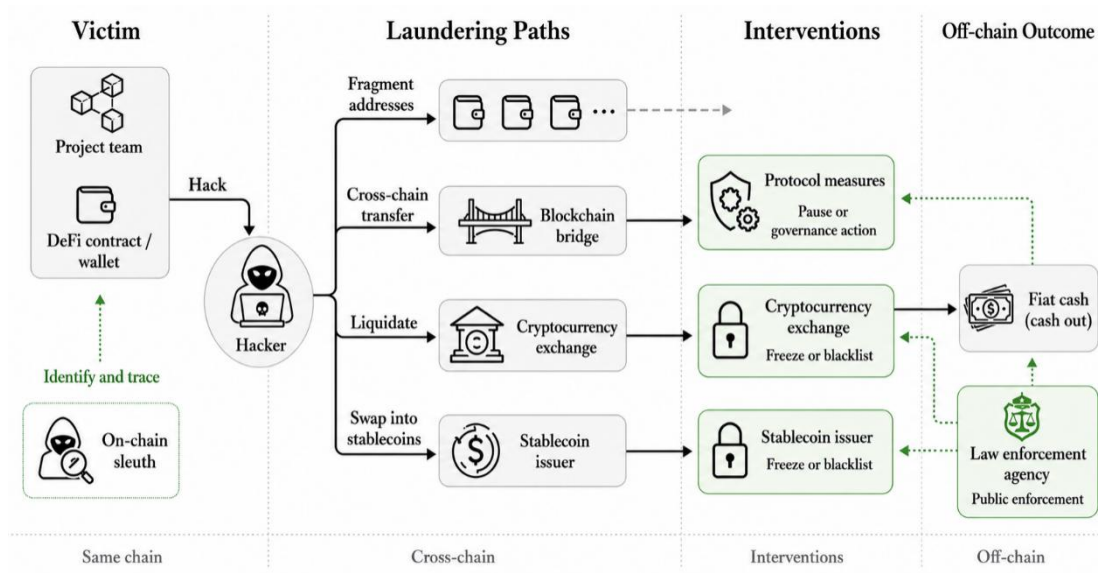
Task	Analytic question	Observable indicators	Failure mode
	accept, and what makes a recovery claim valid?	Root-cause findings; classification of relevant addresses; depth of tracing; confidence in attribution; instructions for asset return	actionable proof, leaving institutions unable or unwilling to process the claim.
Authorizing relief	Who may intervene, what may they control, and on what procedural basis?	Asset freezes or blacklisting; protocol pauses; identification of target addresses; designation of a recovery wallet; supporting legal or compliance records	Actors possess the capacity to intervene but lack recognized standing or a bounded justification, making the intervention appear arbitrary or difficult to sustain.
Sequencing forums	Which forum should be approached first, and how should later engagements be ordered?	Coordination across forums; timing of police reports; use of public pressure; private outreach; progression of negotiation	An otherwise viable move occurs at the wrong time and weakens subsequent cooperation, bargaining leverage, or legitimacy.

Given the sensitivity of this research, unwarranted disclosure could compromise ongoing investigations or disrupt platform operations. It could also expose victims to further harm. We therefore withhold non-public operational data and personally identifiable information. Undisclosed wallet addresses and proprietary compliance metrics are excluded, as are records of private negotiations. Interview excerpts were reviewed for consistency with consent protocols and edited only where necessary to protect participant confidentiality.

4 Empirical evidence

When a crypto hack occurs, hackers remove cryptocurrency from a wallet or DeFi smart contract and attempt to move it before the victim can respond (Figure 2). They may split the funds across addresses before routing them through cross-chain bridges. They may also liquidate the assets through exchanges or stablecoins. Each step creates a possible point of intervention, yet control and information remain dispersed across different actors. Project teams and on-chain investigators identify the incident and trace the assets. Exchanges or stablecoin issuers may then freeze accounts or restrict access to infrastructure, while state authorities provide coercive enforcement. Asset recovery begins as a race against asset dissipation and develops into a coordination problem under fragmented authority.

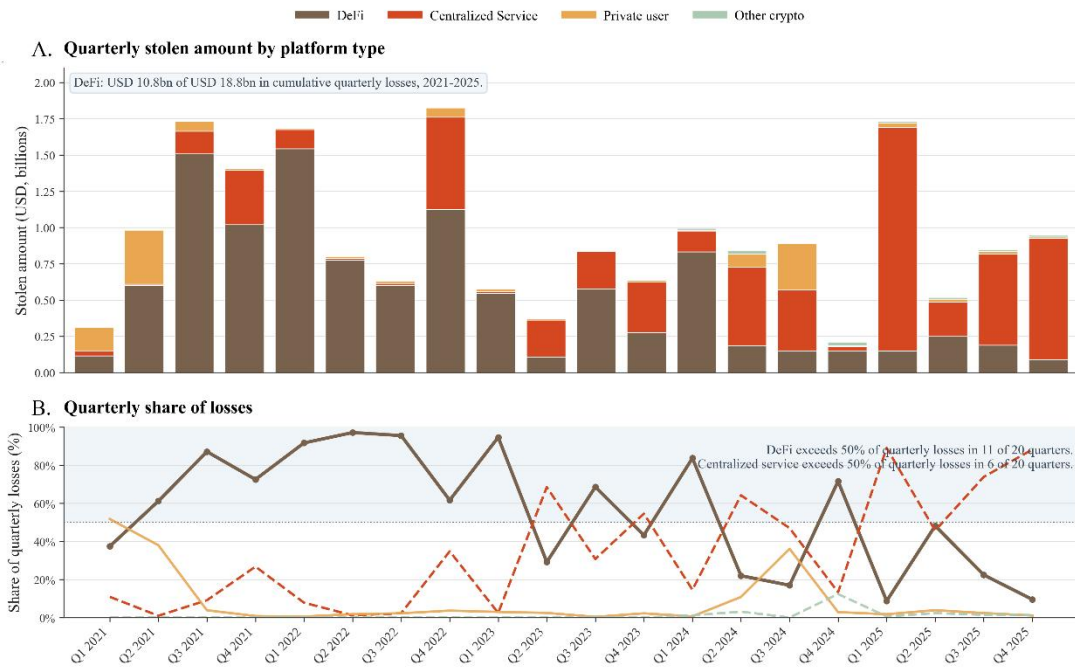
Figure 2 Laundering paths and intervention points in post-hack asset recovery.



Our findings show that post-hack asset recovery depends on coordination across forums. Poly Network foregrounds characterization, while Nomad highlights substantiation. Multichain centers on authorization, and Euler illustrates sequencing. All four tasks nevertheless recur across the cases. The broader dataset places these incidents within a field of 468 major hacks recorded between January 2016 and April 2026, with reported losses exceeding \$16.3 billion. DeFi protocols and centralized platforms account for 93% of incidents (event database; Figure 3). Once assets move beyond the victim’s direct control, it can pass rapidly through cross-chain bridges.

Consequently, the technical and legal capacities required for recovery are therefore distributed across multiple actors. No single institution has end-to-end authority over the process. One actor may trace the movement of assets, while another can freeze an account or impose a formal sanction. Quasi-legal mobilization unfolds across a dispersed field in which claimants must coordinate these partial capacities. Recovery becomes possible only when actions taken in different forums are connected into a pathway from loss to remedy.

Figure 3. Quarterly stolen amount and quarterly loss share by platform type, Q1 2021–Q4 2025.



Panel A shows stolen amount (USD billions); Panel B shows each type's share of total quarterly losses.

Source: DeFiLlama; authors' compilation.

The database shows that recovery requires more than detecting a hack or tracing funds. First, characterization is urgent but often unsettled. Although 83% of incidents ($n = 390$) were disclosed publicly within 48 hours, only 273 produced a shared account of what had occurred. Actors therefore often classify an incident before the underlying facts have stabilized. Second, traceability alone does not substantiate a claim. On-chain tracing reached cross-chain or multi-hop depth in 305 cases, but confidence in attribution was medium or high in only 91. Visible fund flows therefore do not by themselves constitute actionable evidence for a given forum. (Event database).

Third, authorization depends on persuading institutions that relief is warranted. Private remedial measures (e.g., freezes, blacklists, pauses) appeared in 69% of cases ($n = 321$), while state enforcement appeared in 25% ($n = 118$). Recovery therefore often relies on private entities validating a claim before or alongside state action. Finally, sequencing is common: 54% of cases ($n = 253$) visibly combined multiple forums or recovery routes. The problem is not simply whether to invoke law, but how to move among private and public forums in an order that preserves leverage, legitimacy, and the possibility of relief. (Event database).

4.1 Characterizing the wrong

Before seeking redress, victims must turn an injury into a claim by defining the harm and attributing responsibility (Felstiner, Abel, and Sarat 1980–81). This interpretive work is shaped by institutional context and by the narratives available to persuade relevant audiences (Olesen and Hammerslev 2023). Post-hack recovery complicates this process because the categories used to describe digital loss remain unsettled. Legitimacy ambiguity arises when the technical rules embedded in a protocol conflict with broader expectations of ownership (Edelman 1992; Frost and Schaaf 2024). Claimants must therefore stabilize the meaning of the wrong before recovery can proceed.

Post-hack recovery begins with a dispute over how the event should be understood. Some incidents are framed as malicious exploits, while others are attributed to failures of governance or presented as protective interventions. This classification assigns responsibility and shapes whether later intervention can be justified. In this field, an incident does not present itself as theft. As one interviewee noted,

“The exact same asset movement can be described in very different ways... It depends on who is telling the story... At the time (in the aftermath of a hack the interviewee has experienced), I saw it as a clearly illegal exploit. But hackers argued that they acted in good faith and were just helping the blockchain strengthen its security” (Interview transcript, Project-11).

The dispute centers on legal meaning and classification. Another interviewee stated:

“If we can’t call it theft, we can’t really step in to investigate... and say the hacker is in the wrong. These judgments can shape who felt responsible... it also determines if anyone even has the right to get involved” (Interview transcript, Sleuth-07).

The Poly Network case shows that the meaning of a digital wrong can change over time. The same fund outflow may be framed as a malicious exploit or governance failure, then later recast as a white-hat rescue as recovery strategies develop. Each characterization changes who is treated as injured or responsible and shapes which institutions can intervene without appearing arbitrary.

Poly initially framed the incident as a large-scale theft to restrict movement of the stolen funds. By presenting it as a cyberattack, Poly mobilized an industry-wide response. After identifying the assets and publishing the hacker’s addresses, it urged exchanges and token issuers to trace and freeze suspicious transactions. Miners were asked to monitor further transfers. This framing gave other actors grounds to intervene and turned an uncertain loss into a recognizable emergency. (Public-document corpus).

As communication continued and assets began to return, Poly revised its account. The project recast the attacker as “Mr. White Hat” and presented the exploit as an unconventional contribution to protocol security. It later offered a bug bounty. This conciliatory framing preserved the possibility of settlement and avoided fixing the attacker in an adversarial role. An on-chain investigator involved in the Poly case explained:

“At this stage, calling it this way (calling the hacker as ‘Mr. White Hat’) was about keeping open a way to calm things down. If the hacker could be presented as someone to negotiate with, rather than just a thief, then a private settlement became easier to defend to others watching the case” (Interview transcript, Sleuth-02).

This shift was a strategic recalibration in response to three recurring challenges. First, actors initially lack certainty about whether an event constitutes wrongful conduct or permitted code execution. Second, audiences respond to different narrative registers. Exchanges and issuers tend to act on allegations of theft, whereas bilateral negotiation requires more conciliatory language. Third, each label creates a trade-off. A strict classification may justify a freeze while narrowing the scope for negotiation. A more lenient account may

preserve bargaining space but weaken the case for third-party intervention.

Legal consciousness provides the forms through which harmful experiences become rights violations or actionable claims (Ewick and Silbey 1998; Chua and Engel 2019). Grievances may instead be minimized or diverted when framed outside legally cognizable categories (Duan 2025). In post-hack recovery, claimants anticipate how target audiences will interpret competing labels. This second-order legal consciousness shapes the vocabulary used to characterize the incident (Headworth 2020).

The database captures this process through disclosure timing and public framing. A public narrative appeared in 93% of cases ($n = 434$), but only 61% ($n = 286$) produced a coherent account. Disclosure was rapid: 83% of incidents ($n = 390$) were announced within 48 hours. Yet only 56% of cases ($n = 263$) combined rapid disclosure with a coherent narrative. Public scrutiny therefore often begins before the meaning of the incident stabilizes. The Poly Network case illustrates this problem: affected actors must frame an outflow as theft before external forums can treat the loss as actionable. (Event database).

Quasi-legal mobilization produces credible knowledge before the underlying facts are settled (Kim and Arrington 2023). Characterizing the wrong begins post-hack recovery, but provisional accounts must then gain recognition across institutions. This process is substantiation.

4.2 Substantiating the claim

Legitimacy ambiguity reappears at the stage of proof. Intelligence about wrongdoing must be translated into evidence that a given institution can assess. On-chain traces must be assembled into proof bundles, since evidence sufficient for one forum may not support action in another. As one interviewee said,

“Once the hack happened, the people around our protocol knew what was going on, because we understood the protocol logic well. But for an exchange, that was still not enough. They needed harder evidence and a more solid case before they could act. What seemed like obvious evidence to us was, in their eyes, still just a suspicion” (Interview transcript, Project-02).

An interviewee with five years of exchange experience confirmed this cautious approach to evidentiary thresholds, describing proof bundles as composite packages tailored to institutional demands (Interview transcript, Exchange-02).

A comprehensive proof bundle contains three layers. First, technical evidence anchors the claim on-chain. Exploit transactions and cryptographic hashes identify the relevant activity, while a post-mortem explains why the transfers were unauthorized. Second, tracing links the breach to assets or addresses that institutions can target. Victim confirmation establishes ownership, and a designated recovery address enables return. Third, actors convert these facts into institution-specific requests. For example, materials for law enforcement emphasize loss and attribution. Exchange requests focus on customer risk and the action sought, while submissions to stablecoin issuers invoke contractual authority and address indemnification (Interview transcripts, Exchange-12, Exchange-05, and Lawyer-04).

Regulation acquires practical meaning through institutional interpretation (Edelman 1992; Gray and Silbey 2014). Legal action similarly requires broad obligations to be translated into workable steps (Abbott, Levi-Faur, and Snidal 2017). Evidence in post-hack recovery follows the same logic. Although blockchain

ledgers are public, raw on-chain data must be assembled and assessed. As one lawyer put it, “Proof is made, not found” (Interview transcript, Lawyer-02).

Kim and Arrington (2023) describe legal mobilization as a form of knowledge production. Research on medical disputes likewise shows how contested terms such as “medical necessity” acquire practical meaning through insurance policies (Kirkland, Talesh, and Perone 2021). In crypto disputes, the category of “stolen funds” becomes actionable only when technical traces are translated into the institutional language of the forum asked to intervene.

The Nomad incident serves as a paradigm case because an unusually large copycat attack drew in more than 300 addresses and turned the breach into decentralized looting. Participants entered at different stages and followed divergent strategies. Some rapidly laundered funds, while others returned assets and sought white-hat recognition. These differences obscured roles on-chain, requiring Nomad to turn chaotic activity into an administrable claim. Root-cause analysis first traced the outflows to an implementation bug in the Replica contract, supporting their classification as unauthorized transfers. A public data repository then organized fragmented activity and distinguished malicious actors from TRM-verified responders. The bounty program formalized restitution by defining the conditions for amnesty and white-hat recognition. (Public-document corpus).

This process also served an accounting function (Maurer 2016). Nomad separated recoverable assets from slippage losses and distinguished legitimate post-hack transactions from malicious proceeds. It also treated substitute tokens differently from the original compromised assets and classified remaining holdings as distributable claims rather than assets eligible for direct return. This classification made the incident legible to other forums by clarifying which addresses mattered and which assets could be claimed. It also specified the terms of restitution. Actionable proof emerged through accounting and institutional translation. (Public-document corpus).

Nomad’s claim became actionable when the project organized a chaotic event into categories that other actors could process. The Head of Security at one interviewed project described this approach:

“When the evidence structure is this complicated, the important thing is not to get thrown off. We handled it almost like a hospital triage desk: we sorted and organized messy evidence from different sources and different actors, and kept working through it until we could build a complete and solid logical chain” (Interview transcript, Project-07).

Proof bundles organize social phenomena into forms that institutions can act upon. In post-hack recovery, this ordering often precedes formal judicial or regulatory intervention. By converting raw on-chain events into claims that can travel across forums, these bundles may generate institutional recognition. The next task is therefore to convert accepted evidence into authorized relief.

4.3 Authorizing relief

The primary barrier to digital asset recovery is institutional authority. To avoid the appearance of arbitrary private intervention, actors must convert technical control into legitimate relief. As one interviewee said,

“On the blockchain, different people hold different kinds of real control... So, it (post-hack asset recovery) happens when different actors intervene at different technical points of control. Whether it can move forward often depends on whether those forms of control can be activated in time and passed on from one to another...” (Interview transcript, Lawyer-04).

Another interviewee compared this mobilization to a “relay race” (Interview transcript, Sleuth-03). Recovery depends on activating different forms of practical control. Centralized platforms may freeze assets to slow their dissipation, while protocol teams can suspend smart contracts during an exploit. Forensic firms and on-chain investigators may also move vulnerable funds to safety. These interventions create technical capacity, but that capacity must still be recognized as legitimate relief.

Actors who deploy these controls function as de facto legal intermediaries. Exchanges and stablecoin issuers control bottlenecks that shape asset mobility and ledger visibility. Lawyers and on-chain investigators translate disputed events into directives that these institutions can execute. Yet no technical control point can authorize its own intervention. As one interviewee said,

“Whatever intervention we take, we must think about how others will see it. Every time I make a decision, I ask myself: how will the exchange view this? What will the stablecoin issuer think? Will the protocol operators, or people in their community, accept the way we are presenting it?” (Interview transcript, Lawyer-06).

This dynamic shows how second-order legal consciousness shapes authorization. Actors calibrate interventions to meet audience expectations of legitimacy (Headworth 2020; Chua and Engel 2019). Organizational routines and symbolic protocols turn abstract legality into actionable authority (Edelman 1992; Gray and Silbey 2014). Coercive action must appear both effective and procedurally bounded to affected audiences (Sunshine and Tyler 2003). In post-hack recovery, relief becomes authorized when audiences recognize it as a defensible exercise of power.

Institutional actors mobilize when claimants translate requests into established administrative forms (Edelman et al. 2011; Barnes and Burke 2012). Cooperation depends on three conditions. First, an authorized representative must have standing to act for those affected by the protocol. Second, the intervention must remain within defined technical and procedural limits. Third, compliance records and legal endorsements must provide a justification that can withstand later review. These conditions make internal organizational structures central to authorization.

The Multichain case separates technical capacity from authority. After large outflows from the bridge’s MPC wallets in July 2023, many assets were converted into stablecoins issued by Circle and Tether. Both firms could immobilize the tokens. Yet this capacity did not establish who could request intervention or which addresses could legitimately be targeted. An employee at a stablecoin issuer explained:

“Because we have the power to intervene, we need a clear and defensible reason for doing so. Otherwise, people may suspect that we are abusing that power or picking on weaker parties... If a freeze is imposed at a disputed point or on wallets that have not yet been clearly identified, people will naturally question it” (Interview transcript, Dealer-11).

Mobilizing these control points required a delimited object of relief. After the July 2023 outflows, claimants framed their requests around designated addresses and asset preservation. This confined the intervention to suspending specified stablecoin transfers during the initial investigation. The narrow scope allowed Circle and Tether to treat the freeze as a temporary protective measure rather than a broad exercise of discretion. Authorization thus arose by fitting the intervention into routine compliance procedures.

Multichain’s later trajectory reinforces this distinction. The initial USDC freeze could not determine ultimate custody or distribution. By late 2025, liquidators had secured a judicial mandate requiring Circle to maintain the freeze on designated wallets. This brought the assets within a structured liquidation process and prevented uncoordinated claims. Authorization therefore remained an institutional hurdle after the offense had been characterized and the evidence assembled. Even when hostile addresses were identified and the assets immobilized, sustained control required judicial backing and procedural form. Long-term relief became viable only when the technical freeze entered a recognized preservation regime. (Public-document corpus).

As actors characterize the wrong and substantiate the claim, they also consider whether a proposed intervention will be recognized as a responsible use of power. Actionable relief requires a clear mandate and a bounded target. It must also leave records that permit later review. These conditions allow the wider ecosystem to recognize private intervention as authorized preservation. They also introduce a strategic problem, since different remedies depend on different institutional audiences. The next task is sequencing engagement across decentralized forums under informational and jurisdictional uncertainty.

4.4 Sequencing forums under uncertainty

Successful recovery depends on the timing and sequence of engagement across forums. Similar incidents with comparable resources may produce different outcomes depending on how the response is ordered. Each intervention creates a trade-off. Public pressure can heighten scrutiny while prompting faster laundering. Contacting a stablecoin issuer may immobilize assets quickly, yet a premature request may fail compliance review. Negotiation can preserve the possibility of return, although users may interpret it as weakness or accommodation.

Actors therefore sequence forums under uncertainty, anticipating how each move will change the meaning of later moves. As one interviewee explained,

“It (when a theft happens and we start asking for help) feels a bit like making multiple emergency calls at the scene of a fire at the same time: calling the police, contacting building management, shutting off the power, evacuating people, and calling the hospital. The problem is not that you do not know whom to call. The problem is that you have to decide which call to make first and which to make later, because the step you take first will shape how others see the situation, whether they are willing to cooperate, and whether there is still time for them to act” (Interview transcript, Project-10).

Strategic legal mobilization depends on whether a forum is accessible and worth using, given its standing rules and attendant risks (Vanhala 2018). In post-hack recovery, access to different forums also changes over time. A forum becomes viable only after relevant audiences have received signals that warrant action. Sequencing therefore weighs available legal routes against anticipated audience responses.

The Euler case makes this sequencing visible. After the March 2023 exploit, the team imposed a communication blackout while using on-chain messages to demand the return of most funds. It also warned that formal proceedings could follow. When the hacker failed to respond, Euler escalated by proposing a public reward for information leading to arrest and full recovery. The reward sought both information and additional leverage. Meanwhile, the team restricted its social-media communication to a small number of prepared updates, despite criticism from observers seeking further explanation. (Public-document corpus).

Euler assessed how each move would reshape the options that followed. The relevant question was whether an available legal or technical step would preserve a viable path to recovery. These judgments reflect second-order legal consciousness: actors anticipate how others will interpret legitimacy and the proper exercise of authority (Headworth 2020; Young 2014). As one interviewee said,

“The same move can either help or backfire. What matters is not just the move itself, but when you make it and how other people interpret the signal it sends” (Interview transcript, Lawyer-07).

For example, silence could keep the hacker uncertain and preserve the possibility of return, but only if users viewed it as deliberate restraint rather than inaction. A legal threat could raise the cost of non-cooperation, but if made too early, it might harden the hacker’s position and reduce the scope for negotiation. Private contact could open a channel for restitution, yet without public pressure it might appear weak or overly accommodating. An on-chain sleuth with firsthand experience of hacker negotiations explained this sequencing logic:

“A police report can help, but sometimes only later. Filed too early, it slows everything down; filed at the right moment, it unlocks cooperation. Public pressure is for one audience; quiet outreach is for another. The sequence depends on whose reaction matters most at that stage” (Interview transcript, Sleuth-09).

Procedural justice helps explain why legitimacy in mediated settings depends on both outcomes and whether the process appears fair and properly ordered to those whose recognition is required (Sunshine and Tyler 2003).

Across these cases, we demonstrate that actors in quasi-legal domains can navigate fragmented authority. This dynamic links post-hack recovery to a broader socio-legal problem. In other fragmented settings, legal mobilizers combine institutional levels and opportunity structures to make law usable (Vanhala 2018). Post-hack recovery intensifies this problem because asset mobility shortens the time available for judgment. The order of intervention therefore carries legal meaning. The quasi-legal order of recovery is produced through these sequenced practices. (Interview transcripts; public-document corpus).

5 Discussion: When protection precedes adjudication

Our empirical analysis shows that recovering stolen crypto assets depends on quasi-legal mobilization under fragmented authority. Actors coordinate partial capacities while seeking institutional legitimacy. They translate

a technical loss into a recognizable claim and substantiate it with portable proof. They then justify private intervention and sequence engagement across forums according to anticipated audience responses. This process extends legal mobilization scholarship by showing how digital property protection is assembled across multiple institutional sites (Felstiner, Abel, and Sarat 1980–81; Lehoucq and Taylor 2020). It produces a quasi-legal order sustained by recognition across decentralized audiences. Legal intermediaries support this order by standardizing evidence and procedural signals so that claims remain intelligible across forums (Abbott, Levi-Faur, and Snidal 2017; Headworth 2020).

This quasi-legal order may also produce structural inequality. Because formal courts cannot respond at blockchain speed, recovery often depends on a victim's financial resources and institutional connections. Well-resourced victims can mobilize on-chain sleuths and exchanges quickly enough to preserve assets. This dynamic resembles Galanter's (1974) repeat-player advantage, although the relevant arena shifts from state courts to private chokepoints. Private recovery infrastructure may therefore reproduce disparities already observed in access to conventional justice (Sandefur 2015; Talesh 2015). Alternative recovery routes remain unevenly accessible and tend to favor claimants with the resources to activate them (Taylor 2025).

Post-hack recovery also raises procedural justice concerns because intervention often precedes legal judgment (Sunshine and Tyler 2003). Blacklisting and asset freezes may preserve funds without formal adjudication. This reversal places private entities in the position of authorizing and executing relief before affected parties can seek review. Protective measures may therefore appear arbitrary when no immediate appeal is available. Similar concerns arise in platform governance, where private systems enforce detailed rules under limited external accountability (Klonick 2018). Research on outsourced regulation likewise shows that private monitoring complements state enforcement only when supported by transparency and institutional accountability (O'Rourke 2003).

Policymakers should bring private recovery networks within a clearer procedural framework. Our findings show that private actors possess the technical expertise and speed required in digital environments. The policy challenge is to introduce accountability without undermining that capacity. A polycentric model should preserve the agility of market actors while reducing victims' dependence on elite connections or public pressure (Ostrom 2010). Standardized safeguards could turn ad hoc rescue efforts into a more reliable system of property protection (Abbott, Levi-Faur, and Snidal 2017). This requires clear evidentiary thresholds and formal channels for submitting claims. Once assets are frozen, fixed time limits and transparent review procedures should apply. These safeguards distinguish legitimate emergency preservation from arbitrary private control and support more consistent responses to fast-moving digital disputes (Klonick 2018; Taylor 2025).

6 Conclusion

Using post-hack asset recovery as a focal case, this study shows how digital property rights are enforced through quasi-legal mobilization under fragmented authority and ambiguous legitimacy (Ostrom 2010; Kim and Arrington 2023). Victims and their allies must often act before any court can validate the evidence or authorize relief. Recovery therefore develops through repeated adjustment between beliefs and strategies (Cooter 1998; Headworth 2020). Actors anticipate how target audiences will interpret the law and the available facts. Each move then signals a position to other participants, reshaping their expectations and the conditions for subsequent action (Kreps and Wilson 1982; McAdams and Nadler 2008).

The article develops a four-task framework for this process. First, characterization turns a raw technical loss into a recognizable wrong (Zemans 1983). Second, substantiation packages the claim as portable proof, allowing technical traces to move across forums (Edelman 1992; Gray and Silbey 2014). Third, authorization converts the practical capacity to intercept assets into legitimate authority. Claimants present intervention as a procedurally bounded form of relief (Sunshine and Tyler 2003). Finally, forum sequencing determines the timing and order of engagement. Actors anticipate how each move will signal intent and affect later recovery options (Vanhala 2018; Young 2014).

This article extends scholarship on legal intermediaries by identifying a decentralized mode of intermediation. Prior research largely examines intermediaries within established regulatory structures, where gatekeepers monitor conduct and professionals translate ambiguous law into organizational routines under recognized mandates (Kraakman 1986; Abbott, Levi-Faur, and Snidal 2017). Post-hack asset recovery operates under different conditions. Forensic firms and stablecoin issuers help create the institutional basis for authorization. They use law as a shared language through which a quasi-legal order develops from the bottom up (Edelman and Suchman 1997; Gray and Silbey 2014; O'Rourke 2003; Headworth 2020). In doing so, they connect dispersed technical capacities to forms of relief that other institutions can recognize.

A further contribution is to specify how legal consciousness operates under fragmented authority and incomplete information. Prior scholarship shows how understandings of law shape grievance identification and institutional mobilization (Ewick and Silbey 1998; Chua and Engel 2019). Post-hack recovery extends this account by showing how actors anticipate other audiences' judgments of proposed interventions (Headworth 2020; Young 2014). This second-order legal consciousness becomes especially important when validation is distributed across institutions. Claimants and intermediaries assess how each move will affect the credibility of later action (McCann 2006; Vanhala 2018; Lehoucq and Taylor 2020). The article thus connects legal consciousness to the temporal organization of quasi-legal mobilization, showing how legitimacy is tested and revised across fragmented audiences during recovery.

This framework also applies beyond crypto recovery to other fast-moving digital disputes. For instance, AI-generated deepfakes create similar conditions of fragmented authority, as synthetic media spreads faster than formal legal processes can respond. Victims must first translate the technical event into a legally cognizable wrong (Chesney and Citron 2019). The four-task model shows how they may seek relief before the harm becomes irreversible. They characterize the violation and assemble accessible proof, then pursue authorized intervention across platforms and regulatory bodies in a deliberate sequence (Klonick 2018). The framework therefore explains how legality is assembled where no single institution can provide an effective remedy.

Quasi-legal mobilization enables rapid protection when formal law is too slow, but may also reproduce inequality and weaken procedural accountability. Digital property recovery often depends on access to technical infrastructure and specialized expertise, giving well-resourced claimants a clear advantage (Galanter 1974; Sandefur 2015; Taylor 2025). Intermediaries may also freeze assets before courts issue final judgments. Emergency preservation can therefore develop into arbitrary private control when effective review is absent (Sunshine and Tyler 2003).

Future research should examine how private recovery networks can be made more accountable without reducing their speed. Policymakers could support this goal by developing a formal polycentric governance

framework (Ostrom 2010). Evidentiary thresholds and clear intake procedures should guide initial intervention. Once assets are frozen, fixed time limits and review mechanisms should apply (Abbott, Levi-Faur, and Snidal 2017; O'Rourke 2003). Bringing fragmented recovery capacities within a transparent framework could make digital asset recovery more predictable and accessible.

References

- Abbott, Kenneth W., David Levi-Faur, and Duncan Snidal. 2017. "Introducing regulatory intermediaries." *The ANNALS of the American Academy of Political and Social Science* 670 (1): 6–13.
- Barnes, Jeb, and Thomas F. Burke. 2012. "Making way: Legal mobilization, organizational response, and wheelchair access." *Law & Society Review* 46 (1): 167–198.
- Black, Donald. 1973. "The mobilization of law." *The Journal of Legal Studies* 2 (1): 125–149.
- Chainalysis Team. 2025. "North Korea drives record \$2 billion crypto theft year, pushing all-time total to \$6.75 billion." *Chainalysis*, December 18.
- Chesney, Robert, and Danielle K. Citron. 2019. "Deep fakes: A looming challenge for privacy, democracy, and national security." *California Law Review* 107: 1753–1819.
- Chua, Lynette J., and David M. Engel. 2019. "Legal consciousness reconsidered." *Annual Review of Law and Social Science* 15: 335–353.
- Cooter, Robert D. 1998. "Expressive law and economics." *Journal of Legal Studies* 27 (S2): 585–607.
- Duan, Jiahui. 2025. "Belittling grievances: Legal consciousness and strategic non-mobilization in Chinese workplace harassment." *Law & Society Review* 59 (3): 496–523.
- Edelman, Lauren B. 1992. "Legal ambiguity and symbolic structures: Organizational mediation of civil rights law." *American Journal of Sociology* 97 (6): 1531–1576.
- Edelman, Lauren B., and Mark C. Suchman. 1997. "The legal environments of organizations." *Annual Review of Sociology* 23: 479–515.
- Edelman, Lauren B., Christopher Uggen, and Howard S. Erlanger. 1999. "The endogeneity of legal regulation: Grievance procedures as rational myth." *American Journal of Sociology* 105 (2): 406–454.
- Edelman, Lauren B., Linda H. Krieger, Scott R. Eliason, Catherine R. Albiston, and Virginia Mellema. 2011. "When organizations rule: Judicial deference to institutionalized employment structures." *American Journal of Sociology* 117 (3): 888–954.
- Ewick, Patricia, and Susan S. Silbey. 1998. *The common place of law: Stories from everyday life*. Chicago: University of Chicago Press.
- Felstiner, William L. F., Richard L. Abel, and Austin Sarat. 1980–1981. "The emergence and transformation of disputes: Naming, blaming, claiming..." *Law & Society Review* 15 (3/4): 631–654.
- Frost, Lillian, and Steven D. Schaaf. 2024. "Citizenship in the shadow of law: Identifying the origins, effects, and operation of legal ambiguity in Jordan." *Law & Society Review* 58 (4): 573–606.
- Galanter, Marc. 1974. "Why the 'haves' come out ahead: Speculations on the limits of legal change." *Law & Society Review* 9 (1): 95–160.
- Gray, Garry C., and Susan S. Silbey. 2014. "Governing inside the organization: Interpreting regulation and compliance." *American Journal of Sociology* 120 (1): 96–145.
- Headworth, Spencer. 2020. "The power of second-order legal consciousness: Authorities' perceptions of 'street policy' and welfare fraud enforcement." *Law & Society Review* 54 (2): 320–353.

- Hoffmann, Elizabeth A. 2003. "Legal consciousness and dispute resolution: Different disputing behavior at two similar taxicab companies." *Law & Social Inquiry* 28 (3): 691–716.
- Jodoin, Sébastien, and Margaretha Wewerinke-Singh. 2025. "Legal mobilization in a global context: The transnational practices and diffusion of rights-based climate litigation." *Law & Society Review* 59 (1): 17–49.
- Kahraman, Filiz. 2023. "What makes an international institution work for labor activists? Shaping international law through strategic litigation." *Law & Society Review* 57 (1): 61–82.
- Kim, Claudia Junghyun, and Celeste L. Arrington. 2023. "Knowledge production through legal mobilization: Environmental activism against the U.S. military bases in East Asia." *Law & Society Review* 57 (2): 162–188.
- Kirkland, Anna, Shauhin Talesh, and Angela K. Perone. 2021. "Health insurance rights and access to health care for trans people: The social construction of medical necessity." *Law & Society Review* 55 (4): 539–562.
- Klonick, Kate. 2018. "The new governors: The people, rules, and processes governing online speech." *Harvard Law Review* 131: 1598–1670.
- Kraakman, Reinier H. 1986. "Gatekeepers: The anatomy of a third-party enforcement strategy." *The Journal of Law, Economics, and Organization* 2 (1): 53–104.
- Kreps, David M., and Robert Wilson. 1982. "Sequential equilibria." *Econometrica* 50 (4): 863–894.
- Larson, Erik W. 2004. "Institutionalizing legal consciousness: Regulation and the embedding of market participants in the securities industry in Ghana and Fiji." *Law & Society Review* 38 (4): 737–768.
- Lehoucq, Emilio, and Whitney K. Taylor. 2020. "Conceptualizing legal mobilization: How should we understand the deployment of legal strategies?" *Law & Social Inquiry* 45 (1): 166–193.
- Maurer, Bill. 2016. "Re-risking in realtime: On possible futures for finance after the blockchain." *Behemoth: A Journal on Civilisation* 9 (2): 82–96.
- McAdams, Richard H., and Janice Nadler. 2008. "Coordinating in the shadow of the law: Two contextualized tests of the focal point theory of legal compliance." *Law & Society Review* 42 (4): 865–898.
- McCann, Michael W. 2006. "Law and social movements: Contemporary perspectives." *Annual Review of Law and Social Science* 2: 17–38.
- O'Rourke, Dara. 2003. "Outsourcing regulation: Analyzing nongovernmental systems of labor standards and monitoring." *Policy Studies Journal* 31 (1): 1–29.
- Olesen, Annette, and Ole Hammerslev. 2023. "The dynamic and iterative pre-dispute phase: The transformation from a justiciable problem into a legal dispute." *Journal of Law and Society* 50 (1): 120–138.
- Ostrom, Elinor. 2010. "Beyond markets and states: Polycentric governance of complex economic systems." *American Economic Review* 100 (3): 641–672.
- Sandefur, Rebecca L. 2015. "Elements of professional expertise: Understanding relational and substantive expertise through lawyers' impact." *American Sociological Review* 80 (5): 909–933.
- Savelsberg, Joachim J., Jillian LaBranche, and Miray Philips. 2025. "Prosecutorial-NGO complex: New legal opportunity structures and the role of (I)NGOs in universal jurisdiction trials on Syria." *Law & Society Review* 59: 716–748.
- Sunshine, Jason, and Tom R. Tyler. 2003. "The role of procedural justice and legitimacy in shaping public support for policing." *Law & Society Review* 37 (3): 513–548.
- Sytch, Maxim, and Anusha Kallapur. 2025. "Legal and regulatory entrepreneurship: A review of organizational tactics and their consequences for organizations and the law." *Academy of Management Annals* online first. doi: 10.5465/annals.2024.0253.

- Talesh, Shauhin A. 2015. "Rule-intermediaries in action: How state and business stakeholders influence the meaning of consumer rights in regulatory governance arrangements." *Law & Policy* 37 (1–2): 1–31.
- Taylor, Whitney K. 2025. "The unintended consequences of increased access to justice." *Law & Society Review* 59 (4): 665–688.
- Vanhala, Lisa. 2018. "Is legal mobilization for the birds? Legal opportunity structures and environmental nongovernmental organizations in the United Kingdom, France, Finland, and Italy." *Comparative Political Studies* 51 (3): 380–412.
- Vanhala, Lisa. 2022. "Environmental legal mobilization." *Annual Review of Law and Social Science* 18: 101–117.
- Young, Kathryn M. 2014. "Everyone knows the game: Legal consciousness in the Hawaiian cockfight." *Law & Society Review* 48 (3): 499–530.
- Zemans, Frances Kahn. 1983. "Legal mobilization: The neglected role of the law in the political system." *American Political Science Review* 77 (3): 690–703.