Building the Record for Cryptocurrency in Divorce: Digital Assets in Classification, Discovery, Valuation, and Distribution

by
Shuxiang Zhuang*

I. Introduction: Cryptocurrency and the Divorce Record

A New York housewife, whom CNBC identified by the pseudonym "Sarita," suspected during her divorce that her husband, who earned roughly three million dollars a year, had not disclosed everything the couple owned. After spending six months on discovery and enlisting the help of a forensic accountant, she tracked down twelve bitcoins, then worth about half a million dollars, in a wallet he had never listed.[1] The concealment problem is familiar in a divorce proceeding, but the hiding place in this case is not. The incentive to hide marital wealth has not changed; what has changed is who holds the records that would reveal it.[2]

---

* PRC-Qualified Lawyer, Shanghai, China.

1 MacKenzie Sigalos, *A Husband Hid $500,000 in Bitcoin During a Divorce—and Got Busted by a Crypto Hunter*, CNBC (May 20, 2023), https://www.cnbc.com/2023/05/20/bitcoin-in-divorce-how-spouses-hide-assets-crypto-hunters-find-them.html (reporting that Sarita, who used a pseudonym, located twelve bitcoins in an undisclosed wallet after roughly six months of discovery assisted by a forensic accountant, and that her husband's reported assets did not match his approximately $3 million annual income). This Article uses the Sarita account as an introductory anecdote, not as legal authority.

2 *See* Stephanie L. Tang, *Cryptocurrency, NFTs, and the "Metaverse": Addressing the Expanding World of Virtual Assets in Divorce Proceedings*, 127 Penn St. L. Rev. 1, 6-8 (2022) (describing how a public blockchain, a pseudonymous wallet address, and a user-held private key replace the account records a bank or brokerage would otherwise keep).

Conventional dissolution practice often reconstructs marital wealth from financial records produced by the spouses or third parties. Bank records show deposits and transfers, brokerage statements show holdings and trades, payroll records show compensation, and tax returns provide an independent check on the other information.[3] Together, these sources create a financial record tied to the spouse's identity. When cryptocurrency is held through a centralized exchange, this process may still work because the exchange may keep account and transaction records linked to the holder's identity.[4] But self-custodied cryptocurrency breaks that chain. A holder who keeps her own private keys—the cryptographic credentials that authorize transfers from a blockchain address—can control and transfer the assets associated with that address without relying on a custodial intermediary. As a result, no intermediary necessarily maintains an authoritative account statement reflecting the holder's position, even though the relevant balances and transactions remain recorded on the blockchain. Rather than vanishing entirely, this financial evidence fragments across exchange logs, public ledger data, personal devices, and the cryptographic credentials necessary to establish control.[5]

Reported divorce disputes show why this fragmentation matters. They involve post-decree nondisclosure, equitable-distribution orders, fiduciary-duty claims, valuation fights, alleged

---

[3] *See* Richard West & Jonathan Fields, *A Divorce Practitioner's Bitcoin Primer*, 33 J. Am. Acad. Matrim. Law. 177, 184, 189 (2020) (explaining that conventional discovery devices "simply need to be tailored to use the new terminology of Bitcoin," but that subpoenas to peer-to-peer platforms "would be ineffective in most cases since the website would have no information on the transacting spouse").

[4] *See* West & Fields, *supra* note 3, at 183 ("[M]any of these exchanges have 'know your customer' requirements requiring identity verification."); 31 C.F.R. § 1022.210(d)(1)(i)(A) (2025) (requiring a money services business's anti-money-laundering program to include procedures for "[v]erifying customer identification"); Fin. Crimes Enf't Network, Fin-2013-G001, Application of Fincen's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies 3 (Mar. 18, 2013), https://www.fincen.gov/system/files/guidance/FIN-2013-G001.pdf (treating an "exchanger" of convertible virtual currency as a money transmitter subject to those requirements).

[5] *See* West & Fields, *supra* note 3, at 185, 189 (explaining that a bitcoin holder controls the asset through a private address, so that where no exchange holds the records a court can order the spouse personally to produce it); Tang, *supra* note 2, at 8 (explaining that the private key, held by the user, "grants the user access to their funds").

violations of automatic orders, and sanctions requests.[6] The assets have appeared in exchange accounts, self-custodied wallets, business holdings, hard drives, post-filing purchases, and token conversions.[7] Resolving these disputes may require counsel to collect evidence from several different sources and assemble it into a coherent record capable of supporting the relevant family-law claim or remedy. Assembling that record can also expose the cost of retrieving self-custodied assets, such as forensic data recovery, which a court may then have to allocate between the spouses.[8]

A few terms explain this fragmentation. A public blockchain is an open, decentralized ledger that records transactions in a permanent sequence of blocks, maintained by independent nodes rather than a single institution.[9] A private key is a cryptographic credential that authorizes transfers of assets associated with a blockchain address.[10] Blockchain transactions are pseudonymous, meaning that the transactions are visible but the address does not identify

---

6 *See In re* Marriage of DeSouza, 266 Cal. Rptr. 3d 890 (Cal. Ct. App. 2020); LaFond v. LaFond, 505 P.3d 406 (table), No. 82486-COA, 2022 WL 714430 (Nev. Ct. App. Mar. 9, 2022); Coe v. Rautenberg, 358 So. 3d 24 (Fla. Dist. Ct. App. 2023); Leonova v. Leonov, 242 A.3d 713 (Conn. App. Ct. 2020); Green v. Green, Nos. 3112 EDA 2024, 3239 EDA 2024, 3154 EDA 2024 & 3227 EDA 2024, 2026 WL 1309595 (Pa. Super. Ct. May 5, 2026) (non-precedential); *In re* Marriage of Seyl, 2026 IL App (2d) 240719-U (unpublished order under Ill. Sup. Ct. R. 23(b)); A.S. v. A.B., 88 Misc. 3d 1248(A), 2026 N.Y. Slip Op. 50471(U) (N.Y. Sup. Ct. Mar. 31, 2026).

7 *See DeSouza*, 266 Cal. Rptr. 3d at 892-94 (undisclosed bitcoin, fork-derived cryptocurrency, and wallet transfers); *Coe*, 358 So. 3d at 26 & n.1 (bitcoin stored on a damaged hard drive); *Leonova*, 242 A.3d at 732-37 (post-commencement purchase); *LaFond*, 2022 WL 714430, at *1-3 (concealed business entities and conversion of bitcoin into other tokens); *A.S.*, 2026 N.Y. Slip Op. 50471(U), at *7 (holdings across "US-based centralized exchanges, offshore centralized exchanges, decentralized exchanges, and various self-custody wallets").

8 *See Coe*, 358 So. 3d at 26 & n.1, 28 (reversing the trial court's failure to order the former husband to reimburse half of the $1,851.20 the former wife spent to recover data from the damaged hard drive holding the parties' bitcoin, a cost he had agreed at the final hearing to share).

9 Tang, *supra* note 2, at 6 (describing the blockchain as "an open, public, decentralized ledger that records transactions between parties in a permanent record" maintained by a network of nodes).

10 *Id.* at 7-8 (describing public-private key encryption and explaining that "[o]nly the user has access to their private key, which is similar to an account password or PIN and grants the user access to their funds").

the person behind it without additional evidence.[11] Once a transfer is confirmed on chain, no central authority can ordinarily reverse it.[12]

The same asset can generate several different kinds of proof, and no single subpoena collects them. Each source captures a different part of the record. A bank record shows fiat (traditional government-issued money) leaving a checking account for an exchange; the exchange's know-your-customer (KYC) records, the identity-verification records an exchange collects when it opens an account, tie the exchange account to a named person;[13] a blockchain transaction identifies the transfer to a self-custodied wallet, and a public explorer shows where the assets traveled next. A forensic examination of a phone may reveal the wallet application and sometimes a stored seed phrase.[14] Cluster analysis—a forensic

---

11 *Id.* at 6 (explaining that although the ledger is public, "users transact under a pseudonym (their virtual wallet address) so it is nearly impossible to trace trades back to the actual individual or entity without using more complex chain analysis tools").

12 *See* Consumer Fin. Prot. Bureau, Consumer Advisory: Risks to Consumers Posed by Virtual Currencies 5-6 (2014), https://files.consumerfinance.gov/f/201408_cfpb_consumer-advisory_virtual-currencies.pdf ("If you're not using a hosted wallet provider…, there's no mechanism for stopping the payment or getting the money back."); *cf.* West & Fields, *supra* note 3, at 193 (explaining that a confirmed transaction "is highly unlikely to be reversed").

13 On the identity-verification requirements that generate these records, see *supra* note 4. For a court's account of how a spouse's choice of platform affects the records available, see *A.S.*, 2026 N.Y. Slip Op. 50471(U), at *6 (crediting expert testimony that some offshore exchanges "do not require the same level of identity verification or reporting," rely on "self-authentication," and serve as "the platform of choice for individuals seeking to avoid tying their identity to any cryptocurrency ownership"); *id.* at *18-22 (awarding $300,000 in additional counsel fees and $125,000 in expert fees to trace holdings the husband had not disclosed).

14 A seed phrase (also called a recovery phrase or mnemonic phrase) is a human-readable sequence of words from which a compatible deterministic wallet can derive the seed used to generate cryptographic keys. Under BIP 39, valid mnemonic lengths are twelve, fifteen, eighteen, twenty-one, or twenty-four words, and a user may additionally protect the mnemonic with a passphrase. *See* Marek Palatinus et al., *BIP 39: Mnemonic Code for Generating Deterministic Keys*, Bitcoin Improvement Proposals (Sept. 10, 2013) https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki; Ronald Koch, *Cryptocurrency Basics for Litigators*, Colo. Law., Sept./Oct. 2024, at 18, 21. Possession of a usable seed phrase may therefore provide evidence of access or control and, depending on wallet configuration, may permit the holder to recover and transact with

technique that groups blockchain addresses likely controlled by the same person or entity—may associate several addresses with a common controller, which other evidence must then connect to a particular person.[15] The record in a crypto case is assembled from fragments like these, and the practitioner's task is to fit them into a single, coherent chain of proof.[16]

Once assembled, those fragments must connect the cryptocurrency to the facts that matter in the divorce. Exchange records and other identity evidence may link an account to a spouse, while device evidence, transaction history, and other off-chain evidence may help connect that spouse to a self-custodied wallet or public address. From there, the timing of transactions and the source of funds may bear on classification and tracing, undisclosed transfers may support a claim of concealment or nondisclosure, and market data may determine the value assigned to the asset. The same evidence also creates a practical problem in discovery. Private keys and recovery credentials may provide evidence of access or control, but disclosure of those credentials can also give another person the ability to move the assets. Discovery therefore must develop the record without unnecessarily exposing the means of control.[17]

---

the associated wallet; it does not, standing alone, establish legal ownership. *Cf.* Tang, *supra* note 2, at 8 (explaining that a private key grants the user access to funds).

15 *See* Sarah Meiklejohn et al., *A Fistful of Bitcoins: Characterizing Payments Among Men with No Names*, *in* Proc. 2013 Conf. on Internet Measurement 127 (2013) (developing heuristics for grouping bitcoin addresses under common control); Tang, *supra* note 2, at 7 (explaining that linking pseudonymous wallet addresses to individuals requires "more complex chain analysis tools"); Koch, *supra* note 14, at 21 (describing tools that visualize "clusters and connections between addresses"); *cf.* Ahlgren v. Ahlgren, 703 S.W.3d 378, 390-91 (Tex. App. 2023) (in a breach-of-trust action between father and son, describing a tracing expert's use of exchange records and the public blockchain to reconstruct one party's bitcoin holdings across hard forks and a CoinJoin mixer).

16 *See generally* Del Wright, Jr., A Short & Happy Guide to Bitcoin, Blockchain, and Crypto (2020); Koch, *supra* note 14.

17 *See* Koch, *supra* note 14, at 18 ("The cryptocurrency private keys (passwords) grant full control over one's wallet."); Tang, *supra* note 2, at 8; *A.S.*, 2026 N.Y. Slip Op. 50471(U), at *7 (noting expert testimony that for self-custody wallets there is no help desk or password recovery option, so the funds are inaccessible if the holder "refuse[s] to provide truthful statements regarding their

This Article proceeds in four Parts after this Introduction. Part II shows that courts already classify cryptocurrency under ordinary marital-property rules and explains why the difficulty lies not in the law but in the evidence, which is fragmented across exchanges, ledgers, devices, credentials, and human control. Part III sets out the six-stage record protocol. Part IV turns to what the record earns in court: sanctions where a spouse obstructs it, and a defensible valuation and distribution where the record holds. Part V collects drafting and litigation implications and concludes.

II. Ordinary Rules, Fragmented Evidence: Cryptocurrency as Divisible Property and the Record It Leaves

When courts reach the classification question, they generally treat cryptocurrency as property subject to the same marital-property rules that govern other assets.[18] The relevant questions therefore remain largely conventional: when the asset was acquired, what funds or property were used to acquire it, whether marital or separate property contributed to it, and how subsequent transactions affected its character or value. The introduction of digital assets leaves these core equitable inquiries intact, merely displacing the evidentiary trail required to satisfy them.

Unlike a conventional financial account, a cryptocurrency holding may leave relevant evidence across several sources. An exchange may preserve records identifying the purchaser and documenting deposits or trades, while the blockchain may record subsequent transfers without identifying the person behind an address. Assets moved into self-custody may require additional evidence from devices, wallet software, or other off-chain sources. Applying ordinary property rules to a cryptocurrency holding may therefore require reconstructing its acquisition and transaction history from these different parts of the record.

---

ownership"); *see also* West & Fields, *supra* note 3, at 185 ("If the private address is lost, the bitcoins are gone forever.").

18 *See* Tang, *supra* note 2, at 18-19, 26-30 (surveying property-division models and reported divorce decisions addressing cryptocurrency under existing frameworks); West & Fields, *supra* note 3, at 182-83 (discussing classification and valuation of bitcoin).

A. *Courts Apply Ordinary Marital-Property Rules to Cryptocurrency*

Reported decisions generally treat cryptocurrency within the same marital-property framework that governs other forms of property. Courts have looked to the timing and source of acquisition, applicable presumptions concerning marital contributions, valuation dates, settlement terms, and the ordinary principles governing division of the marital estate.[19] Although the underlying blockchain architecture complicates the evidentiary burden, traditional property principles remain firmly controlling.

These cases show that the same property-law framework carries through classification, valuation, and distribution. *In re Marriage of DeSouza* treated bitcoin acquired during the marriage as community property and divided it, together with related derivative cryptocurrency, under California's ordinary community-property framework.[20] *In re Marriage of Fial* applied Oregon's existing rules concerning contribution and tracing to cryptocurrency purchased during the marriage with funds drawn almost entirely from the husband's premarital retirement accounts.[21] Other courts have likewise addressed cryptocurrency through ordinary rules governing valuation and distribution. *Hull v. Hull*, for example, turned on the proper valuation date and the proof of the cryptocurrency's value at that date, while *Shteiwi v. Abdelmassih* and *Green v. Green* addressed the manner in which identified cryptocurrency holdings should be divided.[22]

---

19 *See* Tang, *supra* note 2, at 26-30; *see also* cases cited *infra* notes 20-22.

20 *DeSouza*, 266 Cal. Rptr. 3d at 892-94 (affirming a postjudgment order requiring the husband to transfer to the wife her share of community bitcoins, together with the bitcoin cash and bitcoin gold generated by forks, after the trial court had found the bitcoins purchased during the marriage to be community property and ordered them divided in kind).

21 *In re* Marriage of Fial, 591 P.3d 253, 255-57 (Or. Ct. App. 2026).

22 Hull v. Hull, No. 375462, 2026 WL 122187, at *5-7 (Mich. Ct. App. Jan. 15, 2026) (per curiam) (vacating the cryptocurrency award and remanding for proof of value as of the trial where the trial court had announced a trial-date valuation but used separation-date figures); Shteiwi v. Abdelmassih, 2025-Ohio-2901, ¶¶ 19, 61-64 (Ohio Ct. App.) (affirming equal division of the parties' cryptocurrency wallets by number of coins rather than by account value, where the parties submitted a joint stipulation identifying the wallets and their holdings); Green v. Green,

B. *Separate-Source Claims Survive When the Record Supports Them*

Difficulty of tracing does not relieve a court of the obligation to consider where the funds came from, and the same tools that expose concealment protect the spouse who supplied them. *In re Marriage of Fial* illustrates the point.[23] During the marriage the husband withdrew funds from premarital retirement accounts to buy cryptocurrency, which he held as a long-term investment and allowed to appreciate passively; the wife worked and served as primary homemaker and caretaker but played no role in the investment.[24] The trial court treated the cryptocurrency as a marital asset and, finding the husband had not rebutted Oregon's presumption of equal contribution, divided it equally. The Court of Appeals disagreed on the presumption. Because the account was nearly entirely traceable to the husband's premarital retirement funds and the appreciation had occurred passively, the husband had rebutted the presumption by a preponderance of evidence; the wife's contributions inside and outside the home, though real, did not equally contribute to the acquisition of that particular asset.[25] The court vacated and remanded for a "just and proper" division at the second step of the analysis, leaving room to weigh the parties' treatment of the funds as family money, and carved out a roughly $4,000 deposit possibly traceable to the wife's marital earnings.[26] The lesson runs both ways: whoever contends that cryptocurrency, like any other asset, was acquired with premarital or otherwise separately acquired funds must still put acquisition date, source of funds, marital contribution, and the active-or-passive character of appreciation into the record.

Nos. 3112 EDA 2024, 3239 EDA 2024, 3154 EDA 2024 & 3227 EDA 2024, 2026 WL 1309595, at *13 & n.22 (Pa. Super. Ct. May 5, 2026) (non-precedential) (finding the wife's challenge waived but noting that in-kind distribution of cryptocurrency was appropriate under 23 Pa. Cons. Stat. § 3502(a) where the trial court found the asset difficult to value).

23 *Fial,* 591 P.3d at 256-57 (describing the presumption of equal contribution and the "just and proper" inquiry under Or. Rev. Stat. § 107.105(1)(f)).

24 *Id.* at 254-56.

25 *Id.* at 256-57.

26 *Id.* at 257 & nn.1, 4; *see also Hull*, 2026 WL 122187, at *5 & n.3 (including in the marital estate a bitcoin that the husband claimed was premarital where he acknowledged he had no evidence to confirm premarital ownership).

C. *Classification Disputes Show That Discovery Cannot Stop at Account Ownership*

Classification disputes usually require transaction-level evidence. A wallet or exchange account may establish access, but the court still needs acquisition date, source of funds, marital or separate character, conversions into other assets, derivative coins or forks (units of a new cryptocurrency distributed to existing holders when a blockchain's protocol splits, as bitcoin cash and bitcoin gold were distributed to bitcoin holders in 2017), appreciation, and post-petition movement.[27] *DeSouza* illustrates why transfers and derivative cryptocurrency can matter to the remedy.[28] The same is true of tracing, conversions into other coins, missing coins, and valuation-date proof, each of which has been enough to move the classification or distribution analysis.[29]

For that reason, discovery must be directed to the facts needed for classification and distribution rather than to the existence of a particular account. Standard bank-and-broker discovery remains useful, especially where cryptocurrency was purchased through a centralized exchange, but it may capture only part of the relevant history. In a conventional portfolio case, a brokerage statement may identify the account holder, the assets held, the transaction history, and the value of the account in a single record. Cryptocurrency can separate those functions. An exchange may identify the purchaser and document the initial acquisition, while the blockchain records subsequent transfers, and evidence from a device or other off-chain source may be needed to connect those transfers to a particular spouse. No single source necessarily supplies the complete chronology.

---

27 *See DeSouza*, 266 Cal. Rptr. 3d at 892 (describing a fork as "an automatic process that generates dividends from bitcoin holdings in the form of new currency," there "bitcoin cash" and "bitcoin gold"); *Ahlgren*, 703 S.W.3d at 390-91 (describing the Bitcoin Cash and Bitcoin Gold coins a holder received "for each Bitcoin he held due to 'hard forks' in 2017").

28 *DeSouza*, 266 Cal. Rptr. 3d at 892-94.

29 *See Fial*, 591 P.3d at 256-57 (tracing to premarital funds); *LaFond*, 2022 WL 714430, at *1-3 (conversion of bitcoin into other digital assets and misrepresentation of value); *Hull*, 2026 WL 122187, at *5, *7 (cryptocurrency withdrawn shortly after filing and identified as "missing"; valuation-date proof); *DeSouza*, 266 Cal. Rptr. 3d at 892-93 (bitcoins rendered inaccessible by exchange bankruptcy).

Discovery therefore has to follow the record across the sources in which different parts of that chronology appear. Exchange records may establish identity, funding, trades, and withdrawals. Public-ledger data may establish the timing and path of later transactions but generally requires additional evidence to attribute an address to a person. Devices and wallet software may provide evidence of access or control, while testimony and other off-chain records may explain matters that the transactional record alone cannot establish. The sections that follow examine these sources separately because each contributes a different part of the evidentiary record and presents a different discovery problem.

D. *Centralized-Exchange Records Remain Reachable Through Ordinary Process*

When the asset passes through a centralized exchange, much of the traditional model still works. The exchange may hold KYC records, account-opening documents, linked bank accounts, deposits and withdrawals, trade histories, and acquisition dates. *Zietzke v. United States* shows both the reach and the limits of compulsory process against an exchange. The IRS summons there sought the taxpayer's Bitstamp records so that the agency could determine the number of his transactions, which cryptocurrency he used, and when and how he acquired it. The court rejected his petition to quash. It held, however, that the summons was overbroad for lack of a temporal limitation and ordered it narrowed before it could be enforced.[30] In *A.S. v. A.B.*, subpoenaed discovery revealed previously undisclosed cryptocurrency activity, and the court awarded pendente lite counsel and expert fees to permit further tracing in the divorce case.[31]

---

[30] Zietzke v. United States, 426 F. Supp. 3d 758, 764-66 (W.D. Wash. 2019) (denying the taxpayer's petition to quash an IRS summons served on the Bitstamp exchange, but holding the summons overbroad for lack of a temporal limitation and ordering it narrowed to the 2016 transactions under examination before it could be enforced). Like the *Coinbase* summons discussed below, *Zietzke* arose from a federal tax summons under 26 U.S.C. § 7602 rather than a matrimonial subpoena, so it illustrates what exchange records can contain more than what a family-law litigant can compel. *See infra* notes 32-34 and accompanying text.

[31] *A.S.*, 2026 N.Y. Slip Op. 50471(U), at *1.

One frequently cited authority deserves a caveat. *United States v. Coinbase, Inc.* is often invoked for the general proposition that exchange records are obtainable through legal process,[32] but the case involved an IRS "John Doe" summons under 26 U.S.C. § 7609(f), a federal tax-enforcement device rather than a matrimonial civil subpoena.[33] Even there, the summons was narrowed twice before enforcement.[34] The case therefore does not establish the scope of compulsory process available in a divorce proceeding. It is more useful in showing the kinds of records an exchange may possess and the need to tailor requests to the relevant period and transactions; the ordinary limits of possession, custody, control, relevance, proportionality, and privilege apply to those requests as they do to any other evidence.

E. *Public-Ledger Data Supports Tracing but Does Not Supply the Whole Record*

A public blockchain can preserve transaction history even when no intermediary maintains an account statement. It may show transfers between addresses, the timing and amount of transactions, forks, and other on-chain activity, but the ledger ordinarily does not identify the person behind an address.[35] Attribution therefore depends on evidence from outside the chain, such as exchange KYC records, platform logs, device evidence, admissions, tax records, or expert analysis.[36] *Ahlgren v. Ahlgren* illustrates

---

32 *See, e.g.*, West & Fields, *supra* note 3, at 189 (describing *Coinbase* as a case in which "the IRS successfully enforced a summons (subpoena) to obtain the records of Coinbase customers"); Tang, *supra* note 2, at 23-24 (citing *Coinbase* for a party's ability to obtain transaction information by subpoena to an exchange).

33 United States v. Coinbase, Inc., No. 17-cv-01431-JSC, 2017 WL 5890052, at *1 (N.D. Cal. Nov. 28, 2017); *see also In re* Tax Liabilities of John Does, No. 3:16-cv-06658-JSC (N.D. Cal. Nov. 30, 2016) (order granting an ex parte petition to serve a "John Doe" summons under 26 U.S.C. § 7609(f), which governs summonses that do not identify the taxpayer under investigation).

34 *Coinbase*, 2017 WL 5890052, at *5-7 (recounting the IRS's narrowing of the summons after intervention and further narrowing the categories of records subject to enforcement).

35 West & Fields, *supra* note 3, at 188 ("Blockchain transactions are not strictly anonymous, but rather pseudonymous, since they can be linked to a public address."). On forks, see *supra* note 27 and accompanying text.

36 Hadar Y. Jabotinsky & Michal Lavi, *Speak Out: Verifying and Unmasking Cryptocurrency User Identity*, 32 Fordham Intell. Prop. Media & Ent. L.J. 518, 528, 554-55 (2022) (explaining that on the public ledger "ownership is represented

how different sources can contribute to the same tracing record.[37] Although the case arose from a trust dispute rather than a dissolution proceeding, the trust's expert used exchange records to identify the initial Bitcoin acquisitions and later transaction and hard-fork evidence to reconstruct the subsequent holdings.[38]

Ahlgren also illustrates the limits of ledger-based tracing. The defendant son, whom the jury found to have withheld bitcoin belonging to the trust, later ran the traced bitcoin through a CoinJoin mixer—a privacy technique in which many users combine their transfers into a single joint transaction so that an observer cannot readily match the inputs to the outputs—to obscure the path of the traced assets.[39] The court held that this concealment did not defeat recovery: once a trustee commingles trust property so that it can no longer be identified, the tracing requirement ceases, and the last reliable evidence of holdings controls; here that evidence was testimony that the son still held "a couple thousand" bitcoin months before the demand, with no evidence he had sold them.[40] Both the methodology (exchange records, public-ledger data, and fork accounting) and the burden-shifting principle (a party may not manufacture an evidentiary gap and then exploit it) can inform a dissolution record where a spouse mixes coins or moves them to another blockchain through a cross-chain bridge after filing.[41]

---

by a set of letters and numbers indicating the user's public cryptocurrency address," and that de-anonymization depends on "operational and technical factors" external to the chain itself).

37 *Ahlgren*, 703 S.W.3d at 390-91.

38 *Id.* at 390-91 (testimony of asset-tracing expert Pamela Clegg identifying the initial purchases from exchange records and reconstructing later holdings from hard-fork distributions).

39 *Id.* at 391 (describing the trustee's use of a CoinJoin mixer to "wash" bitcoin and make it untraceable to its original source).

40 *Id.* (holding that the tracing requirement ceases once the trustee mingles trust property with his own so that it can no longer be identified, and relying on testimony that he still held "a couple thousand" bitcoin in the months before the demand, with no evidence of a sale).

41 Chainalysis, *Money Laundering Activity Spread Across More Service Deposit Addresses in 2023, Plus New Tactics from Lazarus Group*, Chainalysis Blog (Feb. 15, 2024), https://www.chainalysis.com/blog/2024-crypto-money-laundering/ ("Cross-chain bridges allow users to move funds from one blockchain to another."). Bridges are discussed further *infra* notes 54-55 and accompanying text.

These limitations become most consequential in civil discovery. Traditional discovery often assumes the existence of a third-party custodian—a bank, broker, or employer—whose identity-linked records can be obtained by subpoena. Cryptocurrency complicates that assumption because relevant evidence may be distributed across public ledgers, custodial platforms, personal devices, and multiple networks. The public ledger remains probative, but it may provide only one part of a record that must be reconstructed from both on-chain and off-chain evidence. Several features of the technology fragment the record further.

Self-custody. A holder who keeps the private keys in a software, hardware, or paper wallet can control the associated cryptocurrency without relying on a custodial intermediary; no institution necessarily maintains an account record to produce.[42] Possession of a usable private key can provide evidence of control and enables the holder to authorize transfers, but it does not by itself establish legal ownership.[43]

Fragmentation. Wallet evidence must be organized by network, not merely by address. On Ethereum and other EVM-compatible networks, one address can hold ETH and multiple tokens, and the same 0x address can appear across multiple EVM-compatible chains. A holder using bitcoin, ether, stablecoins, and Layer-2 networks may therefore require several network-specific queries rather than a single "wallet balance."[44]

---

[42] West & Fields, *supra* note 3, at 184-86, 195 (describing software, hardware, and paper wallet arrangements under which the holder, not an institution, controls the private keys). A wallet that keeps the private keys offline, such as a hardware device or a printed key, is commonly called a "cold wallet"or "cold storage"; this Article uses the terms in that sense. *See Crypto Glossary*, Gemini Cryptopedia, https://www.gemini.com/cryptopedia/glossary (last visited Aug. 22, 2026) (entries for "cold storage" and "cold wallet").

[43] *See* Tang, *supra* note 2, at 8 (explaining that the private key grants the user access to the associated funds); Koch, *supra* note 14, at 18 (explaining that cryptocurrency private keys grant control over a wallet). The distinction between cryptographic control and legal ownership is important because evidence that a person can authorize transactions does not necessarily resolve beneficial or marital ownership.

[44] *See Accounts*, Ethereum.org, https://ethereum.org/developers/docs/accounts/ (last visited May 20, 2026) (explaining that Ethereum accounts can receive, hold, and send ETH and tokens); Fabian Vogelsteller & Vitalik Buterin, *ERC-20: Token Standard*, Ethereum Improvement Proposals (Nov. 19, 2015), https://eips.ethereum.org/EIPS/eip-20 (specifying a token-contract interface

Change addresses. When a bitcoin transaction spends a UTXO, the full value of that UTXO must be assigned to transaction outputs or fees. If the selected inputs exceed the payment plus transaction fee, the transaction typically includes a change output returning the surplus to an address controlled by the sender, often a newly generated address.[45] A zero balance at one address therefore does not by itself establish that the sender no longer controls bitcoin; value may remain in other UTXOs or may have moved to a change address.

Mixers and privacy coins. Mixing services pool funds from many users and redistribute them, breaking the traceable path between addresses.[46] Privacy-focused assets can obscure transaction details, though the degree varies: Monero does so by default, while Zcash depends on whether shielded features are used.[47]

Jurisdiction. Peer-to-peer marketplaces that match buyers and sellers without taking custody often have no transactional

---

that returns the balance of an account address); Tao Yan et al., *Tracing Cross-Chain Transactions Between EVM-Based Blockchains: An Analysis of Ethereum-Polygon Bridges*, 10 Ledger 113, 115 (2025) (explaining that the same user address may be used on the source and target chains in EVM-based blockchain systems). A stablecoin is a token designed to hold a stable value, typically by being pegged to the U.S. dollar. *See Crypto Glossary*, *supra* note 42 (entry for "stablecoin").

45 John Tinkelenberg, *How Bitcoin Transactions Work: Addresses, UTXOs, and More*, Casa Blog (June 6, 2023), https://blog.casa.io/how-bitcoin-transactions-work/ (explaining that a UTXO cannot be partially spent and describing the use of a change address for remaining bitcoin).

46 West & Fields, *supra* note 3, at 189-90 (describing mixing services such as UltraMixer and CoinMixer as tools that "break the link between addresses"); *see also* Tang, *supra* note 2, at 47 (noting that Tornado.cash and Cashfusion have been used to obscure more than $8 billion in Bitcoin and Ethereum transactions).

47 West & Fields, *supra* note 3, at 189-90 (identifying Monero and Zcash as "private coins" that "make the trail hard to follow on the blockchain"); *About Monero*, Monero, https://www.getmonero.org/resources/about/ (last visited May 20, 2026) (describing ring signatures and RingCT and noting that all transactions are private by mandate); *Ring CT*, Moneropedia, https://www.getmonero.org/resources/moneropedia/ringCT.html (last visited May 20, 2026) (explaining that RingCT hides transaction amounts and became mandatory for all Monero transactions after September 2017); *Stealth Address*, Moneropedia, https://www.getmonero.org/resources/moneropedia/stealthaddress.html (last visited May 20, 2026) (explaining one-time stealth addresses and describing Monero as "private by default and optionally semi-transparent"); *What Is the Difference Between Shielded and Transparent Zcash?*, Zcash, https://z.cash/learn/what-is-the-difference-between-shielded-and-transparent-zcash/ (last visited May 20, 2026) (explaining that shielded addresses keep financial information private while transparent addresses make that information public).

record to produce; a subpoena returns nothing of value.[48] Offshore exchanges pose a related but distinct problem because obtaining records from a platform outside the United States may present additional enforcement obstacles, and some platforms may collect relatively little identity information to begin with.[49] Practitioners report that even domestic exchanges sometimes resist matrimonial discovery "as though they are a party to the case."[50]

Decentralized finance (DeFi) extends these problems. DeFi protocols run on smart contracts, code that executes automatically, and may lack the conventional customer records that discovery directed to a centralized intermediary would ordinarily seek.[51] Four mechanisms warrant attention.

Staking. In proof-of-stake networks, tokens are locked in a protocol in exchange for rewards, and many protocols impose lock-up or unbonding periods during which staked tokens cannot be transferred.[52] A spouse who asks only what tokens the other "holds" may miss a substantial position that is neither in a visible wallet nor presently liquid.

---

48 West & Fields, *supra* note 3, at 184 (observing, with respect to peer-to-peer marketplaces such as LocalBitcoins.com, that "issuing subpoenas would be ineffective in most cases since the website would have no information on the transacting spouse").

49 *See id.* at 197 (reproducing a discovery template that asks whether any crypto assets are "held by overseas exchanges"); *A.S.*, 2026 N.Y. Slip Op. 50471(U), at *6 (crediting expert testimony that some offshore exchanges "do not require the same level of identity verification or reporting").

50 Richard D. West, *Cryptocurrency—An Expert's View*, 46 Fam. Advoc., Spring 2024, at 14, 17 (interview with forensic expert Dorothy Haraminac) (observing that U.S.-based exchanges "are getting arrogant in their responses to discovery requests" and that, unlike traditional banks, "[c]rypto exchanges . . . may offer objections as though they are a party to the case").

51 Tang, *supra* note 2, at 7 n.26 (defining smart contracts as "digital agreements using computer code that automatically executes when the terms of the contract are met"); *see also* Brian Sanya Mondoh, Sara Adami-Johnson & Palesa Roza Gwele, *When Harry Leaves Sally: Digital Assets in Divorce and Succession*, Barrister Grp. (Apr. 22, 2025), https://thebarristergroup.co.uk/blog/digital-assets-in-divorce-and-succession (identifying DeFi as a distinct category of disclosable asset).

52 Jason Wright & Michael Detzel, *Staking Cryptocurrency in Marital Dissolution*, Stout (Sept. 8, 2025), https://www.stout.com/en/insights/article/staking-cryptocurrency-marital-dissolution (distinguishing direct, pooled, custodial, and liquid staking and noting that "access to rewards may be delayed by network-imposed lock-up or unbonding periods").

Liquidity pools. A depositor into an automated market maker is exposed to impermanent loss, a divergence between the withdrawal value of the pooled position and the value of holding the underlying tokens, so the ratio and identity of tokens returned on withdrawal may differ materially from those deposited.[53]

Cross-chain bridges. Cross-chain bridges allow users to move funds from one blockchain to another.[54] A wallet trace on the origin chain can miss the real location of the value. Bridge protocols received more than $743 million from illicit addresses in 2023—more than double the prior year.[55]

Wrapped assets. Wrapped Bitcoin (WBTC) is an Ethereum ERC-20 token backed one-to-one by bitcoin held in custody.[56] Value follows bitcoin; tracing starts on Ethereum. A spouse may hold economic exposure to bitcoin, value that rises and falls with bitcoin's price, without ever holding bitcoin itself.

F. *Credentials Can Be Both Evidence and a Means of Control*

Public-ledger evidence may establish the movement of cryptocurrency without establishing who could authorize those transactions. Evidence of control may therefore require closer attention to the credentials or devices used to access a wallet. Private keys and seed phrases are especially sensitive because possession of usable credentials may both support an inference of access or control and permit the assets to be transferred. Passwords and

---

53 Lioba Heimbach, Eric Schertenleib & Roger Wattenhofer, *Risks and Returns of Uniswap V3 Liquidity Providers*, *in* Proc. 4th ACM Conf. on Advances in Fin. Techs. 89, 92 (2022), https://doi.org/10.1145/3558535.3559772 (defining impermanent loss as "the loss in value of a liquidity position in comparison to holding the original assets as the price changes"). An "automated market maker" refers to a decentralized exchange mechanism that uses liquidity pools and a preset pricing formula, rather than matching buyers and sellers through a traditional order book. *See What Is an Automated Market Maker (AMM)?*, Coinbase Learn, https://www.coinbase.com/learn/advanced-trading/what-is-an-automated-market-maker-amm (last visited Apr. 17, 2026).

54 Chainalysis, *supra* note 41.

55 *Id.* (reporting that bridge protocols received $743.8 million from illicit addresses in 2023, up from $312.2 million in 2022).

56 *See* Coinbase, *Wrapped Bitcoin (WBTC) Price*, https://www.coinbase.com/price/wrapped-bitcoin (last visited Apr. 21, 2026) (describing WBTC as an ERC-20 token on Ethereum backed 1:1 by bitcoin held by custodians).

cold-storage devices may raise similar concerns depending on how the wallet is configured. Discovery of such material therefore implicates not only relevance and privacy, but also asset security.

The reported cases illustrate why discovery must distinguish between evidence of control and the credentials or devices that permit that control to be exercised. *Coe v. Rautenberg* shows that physical storage and recovery costs can become distribution issues when the asset depends on a hard drive.[57] *A.S.* describes the practical fragility of self-custody, where access may depend on a private key and no intermediary can restore lost credentials.[58] Compelled-decryption cases provide a further constitutional backdrop when discovery seeks passwords or comparable access information.[59] These concerns favor a staged approach to discovery: less intrusive records may establish ownership, transaction history, or control without disclosure of operational credentials, while requests for credentials can be reserved for circumstances in which those sources are insufficient. The aim is to develop the evidentiary record without unnecessarily exposing the means by which the assets can be moved.

III. The Record-Building Protocol: Preserve, Screen, Demand, Verify, Safeguard, Translate

A comprehensive record-building framework requires initial preservation and screening, followed by targeted discovery, verification of on-chain data, and the securing of private credentials. Existing treatments supply most of the individual components but leave them unordered. This Article organizes those tools into a

---

57 *Coe*, 358 So. 3d at 26-28 & n.1.

58 *A.S.*, 2026 N.Y. Slip Op. 50471(U), at *7.

59 *Compare* Commonwealth v. Davis, 220 A.3d 534, 548-51 (Pa. 2019) (holding that compelled disclosure of a computer password is testimonial and construing the foregone-conclusion exception as "one of limited application" that does not reach compelled password disclosure), *with* Commonwealth v. Gelfgatt, 11 N.E.3d 605, 614-16 (Mass. 2014) (permitting compelled decryption where the defendant's ownership and control of the computers, the fact of encryption, and his knowledge of the encryption key were already known to the Commonwealth and thus a "foregone conclusion"), *and* State v. Andrews, 234 A.3d 1254, 1273-75 (N.J. 2020) (applying the foregone-conclusion exception to cellphone passcodes where the State had established their existence, the defendant's ownership and operation of the phones, and the passcodes' self-authenticating character).

staged protocol, beginning with lower-cost sources and escalating to subpoenas, forensic work, or credential safeguards only when the existing evidence justifies the added expense.

It is designed to keep forensic cost tied to the record and to the amount at stake. Lower-cost indicators come first; subpoenas, device work, analytics, and credential safeguards follow only as the evidence justifies them. The order matters. Preservation fixes the evidentiary baseline before records vanish or coins move; screening then decides whether crypto is even likely enough to justify targeted requests. From there, the demand stage converts the technology into concrete discovery categories, verification checks the responding party's account against independent records, and the safeguard stage keeps production from doubling as a transfer mechanism. The final stage translates the technical record into the findings a family court actually rules on: classification, value, control, dissipation, nondisclosure, and remedy.

A. *Preserve: Fix the Baseline Before It Moves*

Everything downstream depends on getting here first, because crypto evidence is unusually easy to delete, move, or lose. A preservation letter should reach exchange records and communications, wallet applications and their logs, transaction histories and CSV exports, public addresses, emails and texts discussing wallets or exchanges, tax records, device data, hardware wallets and cold-storage devices, recovery materials, and records relating to seed phrases.[60] At this stage, the goal is to prevent the deletion or loss of evidence and to preserve a record of any subsequent asset movement, and to foreclose a later claim that the relevant records no longer exist. Production of a private key or seed phrase belongs, if at all, in a more controlled phase. The letter should also distinguish between preserving access evidence and disclosing spend authority. A spouse can be told to preserve a hardware wallet, wallet app, export file, seed-storage location, and transaction records without being ordered immediately to reveal a seed phrase to the other party. That distinction reduces the risk that preservation

---

60 *See* Tang, *supra* note 2, at 21 (recommending an early-case preservation letter); West & Fields, *supra* note 3, at 188.

itself creates a security incident. It also gives the court a cleaner record later: if a wallet app disappears, a device is wiped, or coins move after notice, the dispute is about conduct after a defined preservation obligation rather than about a vague duty to keep financial records.

Preservation has to come first because spoliation remedies often turn on whether a duty to preserve existed, whether relevant evidence was lost, and whether the responsible party had notice of that duty. *Seyl* illustrates what follows when assets move after filing and go undisclosed: one week after petitioning for divorce, the husband transferred roughly $840,000 in cryptocurrency to "cold wallet" storage and then omitted cryptocurrency from two financial affidavits and his interrogatory answers; the trial court awarded the wife an additional thirty-five percent of the cryptocurrency as a sanction, and the appellate court affirmed.[61] The nondisclosure, not cold storage by itself, supported the sanction.[62] *DeSouza* offers another example of undisclosed cryptocurrency information impairing the other spouse's community interest.[63] The general ESI cases support ordinary preservation consequences for electronic records.[64]

---

61 *Seyl*, 2026 IL App (2d) 240719-U, ¶¶ 9, 45, 70-71 (recounting the transfer of approximately $840,000 in cryptocurrency to cold wallet storage one week after the husband petitioned for divorce, the omission of the cryptocurrency from two financial affidavits and interrogatory answers, and the trial court's award to the wife of an additional 35% of the cryptocurrency as a sanction under 750 Ill. Comp. Stat. 5/501(a)(1)).

62 *Id.* ¶¶ 9, 71 (quoting the trial court's finding that the husband's conduct "amount[ed] to an intentional act designed to mislead Sandra, her counsel, and ultimately the Court," and its observation that "[f]inancial affidavits are the foundation of every divorce and family case").

63 *DeSouza*, 266 Cal. Rptr. 3d at 892-94.

64 *See, e.g.*, Freeman v. Giuliani, 732 F. Supp. 3d 30, 37-38 (D.D.C. 2024) (describing the court's earlier entry of default judgment on liability, under Federal Rules of Civil Procedure 37(b)(2)(A)(vi) and 37(e)(2)(C), as a sanction for the defendant's repeated failure to comply with basic preservation and production obligations); DeCastro v. Kavadia, 309 F.R.D. 167, 180-84 (S.D.N.Y. 2015) (imposing an adverse-inference instruction and a fee award for spoliation and willful nonproduction of electronic records); VOOM HD Holdings LLC v. EchoStar Satellite L.L.C., 939 N.Y.S.2d 321, 328-33 (N.Y. App. Div. 2012) (holding that a party must implement a litigation hold once it reasonably anticipates litigation and affirming an adverse inference for gross negligence in failing to do so). Together these decisions confirm that failure to preserve electronic records can support fee awards, adverse-inference instructions, or case-dispositive sanctions.

B. *Screen: Let Cheap Indicators Justify Expensive Discovery*

Before a case incurs the cost of forensics, low-cost indicators can tell counsel whether digital assets are likely in play and can lay the factual groundwork for a later concealment finding. Bank and credit-card statements frequently show transfers to exchanges such as Coinbase, Kraken, and Gemini, along with unexplained cash withdrawals ahead of large purchases and wires to payment processors tied to crypto acquisition.[65] Tax returns are a strong second signal: a "yes" answer to the Form 1040 digital-asset question is evidence of digital-asset activity, not necessarily current ownership; crypto-related tax items may appear across Form 8949, Schedule D, Schedule 1, Schedule C, information returns, and supporting worksheets; Form 1099-MISC can show mining or rewards income; and, beginning with covered transactions effected in 2025, certain U.S. custodial brokers generally report gross proceeds on Forms 1099-DA furnished in 2026; the form does not capture all foreign, decentralized, or self-custodied activity.[66] Device review and party communications may add wallet or exchange apps, emails or texts about wallets, or seed-phrase materials.[67]

The purpose of this screening is to turn general suspicion into actionable leads. Uncovering exchange transfers, tax anomalies, or digital footprint evidence can expose undisclosed holdings, post-filing purchases, or outright gaps in a spouse's financial disclosures. Once a centralized-exchange lead appears, the exchange's

---

65 West & Fields, *supra* note 3, at 189 ("[E]xamination of bank or credit card statements might reveal payments to Bitcoin exchanges . . . ."); *see also* Tang, *supra* note 2, at 46 (directing practitioners to review account statements for large, unexplained cash withdrawals and transfers to cryptocurrency-exchange sites).

66 Gross Proceeds and Basis Reporting by Brokers and Determination of Amount Realized and Basis for Digital Asset Transactions, 89 Fed. Reg. 56,480 (July 9, 2024) (to be codified at 26 C.F.R. pts. 1, 31, 301) (requiring custodial brokers to report gross proceeds on Form 1099-DA for digital-asset sales effected on or after January 1, 2025); IRS, *Digital Assets*, https://www.irs.gov/filing/digital-assets (last visited Sept. 1, 2026) (describing the Form 1040 digital-asset question and the forms on which digital-asset income and gains are reported); *see also* Tang, *supra* note 2, at 44-45 (describing IRS guidance on virtual currency and the Form 1040 virtual-currency question).

67 West & Fields, *supra* note 3, at 188-90; Tang, *supra* note 2, at 47-48 (discussing forensic protocols to identify use of wallet or exchange applications and, where possible, wallet addresses and keys).

own records can supply the count, type, dates, and manner of acquisition.[68]

C. *Demand: Ask for the Records Crypto Actually Generates*

Self-custodied cryptocurrency may leave no conventional monthly account statement, so a discovery request framed only in terms of "statements" may miss relevant records.[69] If "digital asset" is defined narrowly, a responding party can plausibly read the request to exclude altcoins, non-fungible tokens, governance tokens, staking rewards, lending and borrowing positions on DeFi protocols, mining proceeds, token swaps, and wrapped assets.[70] A definition that expressly reaches bitcoin, ether, and other altcoins, fungible and non-fungible tokens, and their DeFi analogues on any blockchain forecloses that move at the outset.[71]

Interrogatories should require the responding party to identify every exchange account opened, used, controlled, funded, or

---

68 *Zietzke*, 426 F. Supp. 3d at 764-66; *see also A.S.*, 2026 N.Y. Slip Op. 50471(U), at *5-7 (subpoenaed exchange records revealing undisclosed cryptocurrency activity).

69 *See supra* notes 42-43 and accompanying text.

70 This Article uses these terms in their ordinary industry sense. An altcoin is a digital asset other than bitcoin. A non-fungible token is a unique token recorded on a blockchain that may be associated with a specific asset. A governance token confers voting rights over a protocol's direction. Staking rewards are paid to participants who lock up assets to help secure a network. DeFi lending and borrowing positions involve lending and borrowing arrangements executed through self-executing smart contracts. Mining proceeds consist of newly minted block rewards and transaction fees awarded for validating transactions on a proof-of-work network. A token swap is the exchange of one token for another, commonly effected through an automated market maker. A wrapped asset is a token on one blockchain that represents an asset native to another. *See Crypto Glossary*, *supra* note 42 (entries for "altcoin," "staking," "block reward," and wrapped assets); Tang, *supra* note 2, at 9-11 (non-fungible tokens); *What Is a Governance Token?*, Coinbase Learn, https://www.coinbase.com/learn/crypto-basics/what-is-a-governance-token (last visited Sept. 5, 2026); *What Is an Automated Market Maker (AMM)?*, *supra* note 53 (token swaps); Wright & Detzel, *supra* note 52 (staking); *see also supra* notes 52-56 and accompanying text (staking, liquidity pools, bridges, and wrapped bitcoin).

71 Tang, *supra* note 2, at 37-38 (recommending a definitional section that expressly includes bitcoin, ether, other altcoins, and fungible and non-fungible tokens).

closed during the relevant period, together with any earlier account reasonably connected to assets at issue; every custodial and noncustodial wallet and associated public address; every transfer involving an identified account, wallet, or digital asset during the relevant period by date, amount, sending and receiving address, and purpose; every conversion between digital assets and fiat, goods, services, or other tokens; every staking, lending, mining, or yield arrangement; and the full circumstances of any claimed lost or destroyed access.[72] Requests for production should seek complete transaction histories and CSV exports rather than summary statements, transaction hashes for transfers, dated screenshots or exports of wallet balances, linked bank and card records, tax returns and related tax records, including Forms 1040 and 8949, Schedule D, relevant worksheets, and copies of information returns such as Forms 1099-DA and 1099-MISC with worksheets, records of movement from exchange custody to self-custody, and records of purchases made with crypto.[73] The drafting should ask for native exports where possible. A screenshot may show a balance, but a CSV export or exchange transaction history can show dates, counterparties, fees, basis information, and withdrawals to outside addresses. The requests should also cover closed accounts, because a spouse can close an exchange account after moving coins to self-custody while leaving a useful audit trail behind. Requests for admission should fix threshold facts cheaply, including that the party held an account at a named exchange during identified dates, controlled a specified address, or reported crypto activity on a return; a later denial contradicted by subpoenaed or on-chain evidence may, depending on the surrounding evidence, support an inference of nondisclosure or concealment.[74] Third-party subpoenas to domestic exchanges and to the banks and payment processors that funded purchases round out the demand, subject to the

---

72 *See* West & Fields, *supra* note 3, at 197 (App. B); Tang, *supra* note 2, at 40-42 (sample interrogatories addressing exchanges, wallet addresses, dates of acquisition, and transaction histories).

73 *See* West & Fields, *supra* note 3, at 197-98 (App. B); Tang, *supra* note 2, at 38-40 (listing recommended document requests, including complete transaction ledgers and records of linked bank and credit-card accounts).

74 *See* Tang, *supra* note 2, at 23 (noting that requests for admission in dissolution may seek admission or denial of whether a spouse has transacted in virtual currency or holds a wallet). The linkage between a denied request for admission and a later concealment finding reflects the author's analysis.

reachability limits already noted for offshore and decentralized venues.[75] The demand package should be written so each response can be checked against another source. A bank transfer to an exchange should correspond to an exchange deposit. An exchange withdrawal should correspond to a transaction hash or receiving address. A reported taxable event should correspond to account records or ledger movement. That cross-checking structure turns discovery responses into trial evidence.

One category should stay off the demand at this stage: seed phrases and private keys. Producing a key discloses credentials that confer spending authority and may enable activity outside the proper scope of the case, and a disclosed public address is ordinarily sufficient for a preliminary review of that address's public transaction history, although it may not reveal other addresses, chains, or assets controlled by the same person.[76] Compelled key production is an outer-boundary remedy, and it belongs in the safeguard analysis below, not in the first round of requests.

D. *Verify: Test the Disclosures Against Independent Records*

Party disclosures begin the verification work. Disclosed accounts can be reconciled against tax entries and bank records for internal consistency; free block explorers such as Etherscan and Blockchain.com can show activity on disclosed public addresses; subpoenaed exchange records can be laid against the party's own answers; and produced emails and texts may identify wallets or exchanges that did not appear in an interrogatory response. Counsel should build this baseline chronologically by first tracking fiat movements to and from centralized exchanges, and then matching subsequent trades and withdrawals to corresponding dates. Once specific public addresses are identified from the exchange records, on-chain movements can be cross-referenced against the

---

75 *See* Tang, *supra* note 2, at 43; West & Fields, *supra* note 3, at 189.

76 *See* West & Fields, *supra* note 3, at 189 (explaining that a court with personal jurisdiction over the other spouse may order production of a private address); Tang, *supra* note 2, at 42 n.311 ("It is unlikely that a party will simply agree to the disclosure of a private key, as it is similar to requesting a bank account password"; "having the wallet address should be sufficient for the preliminary task of looking up the cryptocurrency transactions a holder has performed"). The recommendation to reserve compelled key production for a later step reflects the author's proportionality and security analysis.

party's formal disclosures, tax returns, and testimony. Any material discrepancy in that baseline warrants further inquiry and, if unexplained, may support an inference of nondisclosure or concealment, and unresolved gaps determine whether the added expense of specialized analytics, device forensics, or a motion to compel is justified. Where those steps surface gaps, escalation to forensics is warranted: commercial analytics platforms such as Chainalysis and TRM Labs use clustering analysis to identify possible associations among addresses, forensic accountants reconcile crypto activity against the marriage's overall cash flow, and device examiners may recover deleted wallet apps and key material.[77]

This step is not a hunt for every wallet a spouse might theoretically have opened. It is a way to make each inference testable. A bank transfer to an exchange, a KYC file, a withdrawal hash, and a later wallet balance each prove different points; none alone proves the whole case. When those pieces align, the court can make ordinary findings about ownership and control. When they do not, the gap itself identifies the next narrow request. *Ahlgren* shows how expert analysis can combine exchange records and public-ledger data to reconstruct an asset history that no single source reveals.[78] The same work appears in other postures: tracing across centralized, offshore, decentralized, and self-custody holdings,[79] identifying marital crypto to support post-decree relief,[80] and untangling missing coins and evasive testimony on the way to an equitable award and a remand for valuation proof.[81] In *DeSouza*, the wallet transfers and derivative assets themselves shaped the remedy.[82]

---

77 TRM Labs, *Building Strong Cases with Blockchain Evidence: Admissibility, Chain of Custody, Experts, and Court-Ready Reporting*, TRM Insights (Feb. 27, 2026), https://www.trmlabs.com/resources/blog/building-strong-cases-with-blockchain-evidence-admissibility-chain-of-custody-experts-and-court-ready-reporting (describing clustering heuristics such as co-spend analysis and the corroboration of address attributions with independent records); *see also* Tang, *supra* note 2, at 24-25 (discussing retention of cryptocurrency-specialized experts and investigation providers).

78 *Ahlgren*, 703 S.W.3d at 390-91.

79 *A.S.*, 2026 N.Y. Slip Op. 50471(U), at *5-7, *18-22.

80 *LaFond*, 2022 WL 714430, at *1-3.

81 *Hull*, 2026 WL 122187, at *6-7.

82 *DeSouza*, 266 Cal. Rptr. 3d at 892-94.

Two cautions govern the verification stage. The first is proportionality. If the suspected concealed crypto is worth $50,000 and full forensics would cost $40,000, the investigation may consume the value it seeks to find. A tiered approach keeps cost tied to stakes: cheap review first, targeted subpoenas and focused device work next, and full forensics only where strong indicators justify them.[83] The second is legality. Counsel should not encourage self-help access to a spouse's accounts or devices. Depending on the source accessed, the existence and scope of authorization, and the method used, such access may implicate the Stored Communications Act, the Computer Fraud and Abuse Act, the Wiretap Act, state privacy law, or professional-responsibility rules. Civil liability, evidentiary consequences, and available remedies remain jurisdiction- and fact-specific.[84]

E. *Safeguard: Protect Credentials and Control*

Some forms of production hand over the ability to spend the asset, which is exactly why this stage has to preserve access to evidence without giving away control. Useful substitutes include public addresses, transaction hashes, read-only exports, exchange records, screenshots, neutral forensic inspection under a protective order, escrow, court-supervised transfer, and a small test transaction before any full in-kind transfer.[85] The physical-storage, self-custody, and compelled-decryption authorities point in the same practical direction: obtain verifiable access evidence first, and reserve credentials for a protective order or court-supervised process.[86] The

---

83 Tang, *supra* note 2, at 25 (cautioning that, where holdings are minimal, there is no pattern of nondisclosure, detailed tax filings exist, and both clients are amicable, "it likely is not worth seeking the additional analysis").

84 18 U.S.C. § 2701 (Stored Communications Act); *id.* § 1030 (Computer Fraud and Abuse Act); *id.* § 2511 (Wiretap Act); *see also* West & Fields, *supra* note 3, at 190.

85 *See* West & Fields, *supra* note 3, at 189-90 (recommending a stipulated forensic protocol and noting that ordinary rules on scope and protective orders continue to apply); *cf. DeSouza*, 266 Cal. Rptr. 3d at 894 (order directing transfer of a specified number of bitcoins and fork-derived coins). The escrow, test-transaction, and court-supervised transfer procedures described in the text reflect the author's recommendation.

86 *See Coe*, 358 So. 3d at 26-28 & n.1; *A.S.*, 2026 N.Y. Slip Op. 50471(U), at *7; *Davis*, 220 A.3d at 548-51; *Andrews*, 234 A.3d at 1273-75; *Gelfgatt*, 11 N.E.3d at 614-16.

order should also say who may view credential material, where it will be stored, whether counsel may retain a copy, whether an expert may image or inspect the device, how any test transaction will be documented, who bears network fees, and what happens if the receiving address is wrong or the transaction fails. These details are mundane, but they prevent the discovery process from becoming the source of the next dispute. The same concern appears at enforcement. A decree that says only to transfer cryptocurrency may leave the parties arguing about network, address, fee, timing, and confirmation rather than entitlement. The safeguard step reduces that risk by turning access into a supervised procedure. A court-supervised transfer can be staged in small steps: verify the address, send a nominal test amount, wait for confirmation, document receipt, and then transfer the remaining amount. That procedure is slower than handing over a seed phrase, but it better matches the family court's task of preserving value while deciding ownership.

F. *Translate: Turn a Discovery Record into a Distribution Record*

The final job is turning all of this into something a family court can act on. The record should answer the questions that distribution turns on: who controlled the asset, when it was acquired, what funds bought it, where it moved, what it was worth, whether it was disclosed, and whether it can be divided safely. The translation stage should avoid technical shorthand. The finding should not merely say that a wallet existed; it should say what evidence links the wallet to the spouse, what transactions show acquisition or movement, what date and source support value, and what practical steps make the remedy executable. That format also helps appellate review because it ties technical evidence to familiar findings. Those questions are what shape the remedy in practice—whether it ends in a fiduciary-breach finding, a tracing order, an in-kind split, an offset, an access order, a missing-asset charge, or reimbursement.[87]

---

87 *See DeSouza*, 266 Cal. Rptr. 3d at 892-94 (fiduciary-breach finding and in-kind transfer order); *Fial*, 591 P.3d at 255-57 (tracing to premarital funds and remand for a just and proper division); *Green*, 2026 WL 1309595, at *13 & n.22 (non-precedential) (in-kind distribution); *Coe*, 358 So. 3d at 27-28 (reimbursement of recovery costs); *LaFond*, 2022 WL 714430, at *1-3 (post-decree relief); *Hull*, 2026 WL 122187, at *6-7 (missing-asset charge and valuation remand); *Leonova*, 242 A.3d at 721-22, 732-37 (contempt for post-commencement

IV. From Record to Remedy: Concealment and Sanctions, Valuation and Distribution

Once the record exists, it does two kinds of work—it supports sanctions where a spouse has obstructed it, and it supports a defensible valuation and distribution where it holds. This Part takes each in turn. When a spouse hides crypto, courts draw on existing disclosure, fiduciary-duty, sanctions, dissipation, and fee-shifting doctrines. The remedy depends on the conduct and the record: omission, false disclosure, unauthorized transfer, deletion, refusal to comply, or violation of a court order. A sanctions record should identify the specific obligation in effect at the time of the misconduct (such as a statutory disclosure or fiduciary duty), the precise nature of the noncompliance (ranging from asset omission to the active deletion of records), and the resulting prejudice to the innocent spouse or the marital estate (such as inflated forensic costs or distorted settlement negotiations). Framed that way, the sanction rides on what the spouse did, not on a court's unease with the technology.

A. *Nondisclosure Can Breach Fiduciary or Statutory Disclosure Duties*

Nondisclosure can impair valuation, settlement, tracing, and trial preparation. *In re Marriage of DeSouza* illustrates how a crypto concealment record is built and why one asset can generate several distinct breaches.[88] Shortly after his wife Erica served him with a dissolution petition and California's automatic temporary restraining order in January 2013, Francis DeSouza used marital funds to acquire more than a thousand bitcoins through two proxies who bought on his behalf from the Mt. Gox exchange. He disclosed the aggregate holding — 1,062.21 bitcoins — on his preliminary and final schedules, but he did not disclose that he had used proxies, that roughly 499 of those coins remained trapped in Mt. Gox's bankruptcy, that the holding had generated bitcoin cash

---

cryptocurrency purchase in violation of automatic orders, offset against the husband's bonus); *A.S.*, 2026 N.Y. Slip Op. 50471(U), at *18-22 (fee award to fund tracing); *Seyl*, 2026 IL App (2d) 240719-U, ¶¶ 45, 70-71 (sanction for nondisclosure).

88 *DeSouza*, 266 Cal. Rptr. 3d at 892-94.

and bitcoin gold through 2017 forks, or that he had moved coins between wallets. Only after judgment, when Erica sought her half, did he reveal he could produce just 613.53 coins.[89] The Court of Appeal affirmed findings that Francis both violated the restraining order and breached his fiduciary duty under Family Code sections 721 and 1100, and that the breach impaired Erica's community interest under section 1101, which entitles the wronged spouse to fifty percent of any asset undisclosed or transferred in breach, plus fees.[90] Two holdings carry beyond California. On materiality, the court rejected the argument that Erica's general disinterest in the couple's finances during the marriage showed she would have done nothing had she known: her conduct during the marriage "sheds little if any light" on what she would do after retaining counsel, filing, and serving restraining orders.[91] On impairment, the court held that the success of one undisclosed investment does not offset the harm from a separate undisclosed transaction, because the disclosure policy "contains no exception for debts and assets that offset each other."[92] A spouse cannot launder a concealment by pointing to gains elsewhere.

B. *Courts Impose Adverse Equitable Consequences on the Spouse Who Hides or Controls the Asset*

When control or concealment affects the record, courts may assign the asset to the controlling spouse, award a larger share to the other spouse, order account access, shift fees, or otherwise adjust the estate. The sanctions cases show courts treating crypto concealment as ordinary litigation misconduct once the record establishes the conduct. In *In re Marriage of Seyl*, the husband moved roughly $840,000 in cryptocurrency to storage wallets a week after filing for divorce, then omitted it from two financial affidavits and

---

89 *Id.* at 891-93 (describing the January 2013 automatic temporary restraining order, the April 2013 proxy purchases through Mt. Gox, and Francis's post-judgment disclosure that only 613.53 of the 1,062.21 disclosed bitcoins remained available).

90 Cal. Fam. Code §§ 721, 1100, 1101; *DeSouza*, 266 Cal. Rptr. 3d at 894-95. Section 1101(g) authorizes an award of 50% of any asset undisclosed or transferred in breach of the fiduciary duty, plus attorney's fees and costs.

91 *DeSouza*, 266 Cal. Rptr. 3d at 896.

92 *Id.* at 897-98 (quoting *In re* Marriage of Feldman, 64 Cal. Rptr. 3d 29, 39 (Cal. Ct. App. 2007)).

his interrogatory answers; only after a court-appointed expert's team surfaced the accounts did he list more than $900,000 on a later affidavit.[93] The trial court rejected his claim that the omission was inadvertent and, invoking a statute requiring sanctions for an inaccurate or misleading financial affidavit, awarded the wife an additional thirty-five percent of the cryptocurrency, eighty-five percent in all, plus a $20,000 payment to charity as a sanction for perjury and discovery violations; the appellate court affirmed, quoting the trial court's explanation that the severity was deliberate because "[f]inancial affidavits are the foundation of every divorce and family case."[94] *Cohen v. Cohen* reaches dissipation on different conduct: there the husband bought $222,000 in cryptocurrency through concealed transactions funded with marital assets and loans, and the court found the losses a dissipation of marital assets which, together with his unpaid support, led it to award the wife the marital residence and any currency in his bitcoin or cryptocurrency accounts.[95] Together, *Seyl* and *Cohen* show the same limiting principle: the remedy follows the misconduct, not the fact that the property was digital.

C. *Automatic Orders, Post-filing Restraints, and the ESI Backdrop*

A purchase, sale, or transfer of crypto after the case begins can violate an automatic order or a restraint on disposing of marital property, and the asset's digital form does not make the transaction ordinary-course activity. The appellate court's reasoning in *Leonova* makes the point. The husband invested $39,000 in cryptocurrency after commencement and lost $22,000, and the Connecticut appellate court rejected his usual-course-of-business defense because he had never bought cryptocurrency before and had no accounts for doing so until after the action began;

---

93 *Seyl*, 2026 IL App (2d) 240719-U, ¶ 9. As a Rule 23(b) order entered after January 1, 2021, *Seyl* is nonprecedential but may be cited for persuasive purposes under Rule 23(e)(1); it is cited here as illustration.

94 *Id.* ¶¶ 7, 71; *see* 750 Ill. Comp. Stat. 5/501(a)(1).

95 Cohen v. Cohen, No. FBT-FA18-6079812-S, 2021 WL 12151633, at *4, *7, *10-11 (Conn. Super. Ct. June 23, 2021) (finding a $222,000 dissipation of marital assets through concealed cryptocurrency transactions and awarding the wife 100% of the marital residence and all cryptocurrency accounts); *see* Conn. Practice Book § 25-5 (2026) (automatic orders).

the remedy was an order that he pay the wife, out of his share of the estate, one-half of the loss.[96] The case turns crypto's volatility into an ordinary problem of risk allocation.

The ordinary sanctions framework governs when digital evidence is deleted, withheld, or never preserved, and cases such as *Freeman*, *DeCastro*, *VOOM*, *Holme v. Global Minerals & Metals Corp.*, *United States v. Rapower-3, LLC*, and *In re Heinz* establish the consequences of lost or withheld electronic financial records.[97] These decisions reinforce the preservation and sanctions principles above without establishing anything crypto-specific; they backstop the family-law authority rather than stand in for it.

D. *A Limiting Principle: Complexity Alone Is Insufficient*

Sanctions require more than difficulty in tracing or calculating crypto-assets. What is sanctionable is nondisclosure, false disclosure, a misleading affidavit, a refusal to comply, deletion, a breach of the duty to preserve, a violation of a court order, dissipation, or concealment.[98] Crypto's complexity bears on burden, proof, valuation uncertainty, and proportionality, but complexity is not itself a ground for sanctions. A spouse may hold crypto in a genuinely complicated form without doing anything wrong. The

---

[96] *Leonova*, 242 A.3d at 732-37 (rejecting a usual-course-of-business defense to a post-commencement cryptocurrency purchase where the husband had not previously purchased cryptocurrency or held accounts for doing so, and affirming an order that he pay the wife one-half of the $22,000 loss out of his share of the estate).

[97] *See* United States v. Rapower-3, LLC, 470 F. Supp. 3d 1232, 1237-38, 1251-53 (D. Utah 2020) (finding that contemnors discarded financial records responsive to a receivership order and barring them from relying on any document not produced by the court-ordered deadline); Lioce v. Heinz (*In re* Heinz), 501 B.R. 746, 758-59, 767-68 (Bankr. N.D. Ala. 2013) (drawing an adverse inference from the debtor's willful failure to preserve electronic accounting records and denying discharge under 11 U.S.C. § 727(a)(3) for failure to keep or preserve records); Holme v. Glob. Mins. & Metals Corp., 934 N.Y.S.2d 30, 31 (N.Y. App. Div. 2011) (affirming an adverse-inference charge for spoliation of electronic accounting and trading records); *see also* cases cited *supra* note 64.

[98] *See Seyl*, 2026 IL App (2d) 240719-U, ¶¶ 9, 68-72; *DeSouza*, 266 Cal. Rptr. 3d at 893-94; *Hull*, WL 122187, at *6-7; *Cohen*, 2021 WL 12151633, at *3-4, *10-11; *Leonova*, 242 A.3d at 732-37.

consequences attach when conduct obstructs the record or impairs the other spouse's rights. Keeping that line clear matters: sanctions should reach deceptive conduct, not the mere holding of a technically complex asset.

Once discovery produces the wallet and exchange records, the court still has to decide what the crypto is worth, when to value it, and how to divide it. The record built in Part III is what makes each of those choices defensible. Valuation and distribution should be treated as separate questions. A reliable value requires asset identity, quantity, valuation date, valuation time, price source, fees, and tax consequences. A workable distribution requires access, transfer mechanics, wallet competence, confirmation of receipt, allocation of failed-transfer risk, and a remedy if the asset has already moved. Those questions overlap, but they should not be collapsed. A court can accept a valuation while still choosing offset over transfer, or it can divide coins in kind while leaving tax-basis records and network-fee allocation to the order.

E. *Volatility Puts the Valuation Date and Method at the Center*

Crypto trades on multiple venues, and prices for the same asset can differ across platforms at the same time. The SEC has described investments in crypto asset securities as exceptionally volatile and speculative.[99] A valuation should disclose the date, time, source venue or index, quantity, and method. It should also identify whether the figure is a spot quote, a volume-weighted figure, an exchange-specific closing price, or a composite index, because those choices can matter in a fast-moving market. The valuation should also account for liquidity where the marital position may be too large to sell at the quoted price. For stablecoins, the valuation should identify any custody, redemption, or

---

[99] Sec. & Exch. Comm'n, Off. of Inv. Educ. & Advocacy, *Exercise Caution with Crypto Asset Securities: Investor Alert* (Mar. 23, 2023), https://www.investor.gov/introduction-investing/general-resources/news-alerts/alerts-bulletins/investor-alerts/crypto-asset-securities (describing crypto asset securities as "exceptionally volatile and speculative"); *see also* Sec. & Exch. Comm'n, Div. of Corp. Fin., *Crypto Asset Exchange-Traded Products* (July 1, 2025), https://www.sec.gov/newsroom/speeches-statements/cf-crypto-asset-exchange-traded-products-070125 (identifying "price differentials across crypto asset trading platforms" as a required disclosure topic).

network-specific considerations that materially affect the position. The valuation record should therefore show both the arithmetic and the assumptions behind it. *LaFond* demonstrates the consequences of relying on a materially inaccurate cryptocurrency valuation: because the husband misrepresented the initial value of the bitcoin, the court set aside the original property settlement years later and ordered an equal division of the actual, newly discovered cryptocurrency accounts.[100] The case does not, standing alone, prescribe a particular valuation date, exchange, index, or methodology.[101]

F. *In-kind Division Answers Volatility but Raises Access and Competence Problems*

In-kind division can let both spouses share future gains and losses, but it requires reliable transfer instructions, wallet access, technical competence, fee allocation, and confirmation of receipt. The order should specify the asset, network, quantity, sending wallet or exchange account if known, receiving address, timing, responsibility for fees, test-transaction procedure, and proof of completion. It should also address what happens if the recipient supplies an incorrect address, if the sender claims the wallet is inaccessible, if network congestion changes the fee, or if the transfer triggers tax reporting. *Green* is limited but useful: the court deemed the challenge waived and, alternatively, found no abuse of discretion in an in-kind split where the trial court credited testimony that a sale would force market timing and that cryptocurrency was difficult to value;[102] *Coe* shows that coin-level allocation must be arithmetically correct.[103] *DeSouza* and *Shteiwi* show what in-kind or coin-count treatment looks like in practice: the court awards each spouse a share of the coins themselves rather than a dollar figure fixed on a valuation date.[104] In *DeSouza* the trial court divided the community bitcoins in kind and the Court of Appeal affirmed a postjudgment order requiring transfer of the wife's share of the coins together with the fork-derived bitcoin cash and

---

100 *LaFond*, 2022 WL 714430, at *1-3.

101 *Id.*

102 *Green*, 2026 WL 1309595, at *13 & n.22 (non-precedential).

103 *Coe*, 358 So. 3d at 27-28.

104 *DeSouza*, 266 Cal. Rptr. 3d at 893-94; *Shteiwi*, 2025-Ohio-2901, ¶¶ 61-64.

bitcoin gold.[105] In *Shteiwi* the court affirmed an equal division of the parties' wallets by number of coins rather than by account value.[106] Because each spouse takes coins rather than cash, both share the risk of post-separation price movement.

G. *Offset and Equalization Work When One Spouse Controls the Asset or Transfer Is Unsafe*

Offset and equalization may be appropriate when one spouse controls the asset or direct transfer is unsafe. *Liu v. Chang* is an example: the trial court valued the bitcoin at $328,903, awarded that value to the husband, awarded the house to the wife because the court had no way to reach the coins, and produced a 55.41-to-44.59 property split.[107] Irreversibility supports the same caution around direct transfers.[108] *Coe v. Rautenberg*[109] supplies two concrete distribution points. The marital estate was primarily ten bitcoins; after the wife had already taken 1.2 of them from the husband's share to satisfy past-due child support, the trial court erroneously deducted that 1.2 from the whole estate before splitting the remainder, reducing her share. The appellate court corrected the arithmetic — the wife's share is computed from the original pool, the child-support conversion charged against the husband's half — and separately held the husband had to reimburse half the $1,851.20 the wife spent to recover the damaged hard drive that held the coins.[110] Coin-level allocation has to be done correctly, and the operational cost of reaching a self-custodied asset is itself a distribution item.

H. *Access Costs, Post-Decree Relief, and Tracing's Dual Role*

Crypto sometimes depends on a hard drive, a hardware wallet, forensic recovery, or expert help, and those costs are marital expenses, reimbursement claims, or allocation issues in their own right. *Coe,* discussed above, treated the hard-drive recovery cost

---

105 *DeSouza*, 266 Cal. Rptr. 3d at 893-94.

106 *Shteiwi*, 2025-Ohio-2901, ¶¶ 61-64.

107 Liu v. Chang, No. 78999-6-I, 2020 WL 1921123, at *2-3 (Wash. Ct. App. Apr. 20, 2020) (per curiam) (unpublished).

108 West & Fields, *supra* note 3, at 193.

109 *Coe*, 358 So. 3d at 26-28.

110 *Id.* at 27-28 (correcting the equitable-distribution arithmetic and requiring the husband to reimburse half of the $1,851.20 hard-drive recovery cost).

in exactly that way.[111] Distribution, in other words, includes the operational cost of getting to the asset, not merely the asset's value.

Post-decree relief may be available when a spouse misstates value, converts coins, omits accounts, or hides post-decree gains, but the applicable standard and time limits depend on state law and the decree. *LaFond* supports post-decree relief where a spouse misrepresented the value of bitcoin and converted bitcoin into other cryptocurrency, and expert tracing identified the marital crypto accounts; the wife proceeded by motion under Nevada's Rule 60(b), and the opinion does not address timeliness.[112] *DeSouza* supports post-dissolution relief for nondisclosure and fiduciary breach on a motion filed within weeks of the judgment.[113] The time limits vary. Rules modeled on Federal Rule of Civil Procedure 60(b) generally require a motion based on fraud or misrepresentation within one year of judgment, and Nevada allows six months, while California measures its one-year period for setting aside a family-law judgment for fraud or nondisclosure from the date the complaining spouse discovered or should have discovered it, and permits a fiduciary-breach claim raised in the dissolution proceeding itself without regard to the three-year limit that otherwise runs from actual knowledge.[114]

Tracing protects both spouses. It can expose concealment, but it can also prevent an overinclusive marital award by proving a separate-property source, passive appreciation, or a limited marital contribution.[115] *DeSouza* illustrates the offensive use of the same record: rather than defending a separate-source claim, the wife used the transaction and fork history to show that undisclosed purchases, transfers, and derivative assets had impaired

---

111 *Id.*

112 *LaFond*, 2022 WL 714430, at *1-3 (reviewing relief granted on a motion under Nevada Rule of Civil Procedure 60(b)(1) and (3)).

113 *DeSouza*, 266 Cal. Rptr. 3d at 893 (postjudgment motion filed in January 2018 following a December 2017 judgment).

114 *See* Fed. R. Civ. P. 60(c)(1) (one year for motions under Rule 60(b)(1)-(3)); Nev. R. Civ. P. 60(c)(1) (six months); Cal. Fam. Code § 2122(a), (f) (one year from the date the complaining party discovered or should have discovered the fraud or the failure to comply with disclosure requirements); *id.* § 1101(d)(1)-(2) (three years from actual knowledge, except that a claim may be brought in conjunction with a dissolution action without regard to that limit).

115 *Fial*, 591 P.3d at 255-57; *Ahlgren*, 703 S.W.3d at 390-91; *Hull*, 2026 WL 122187, at *6-7.

her community interest.[116] The tax treatment also matters: virtual currency is property for federal tax purposes, and section 1041 can carry basis consequences into divorce transfers.[117] Future tax consequences should be used only where the record gives a reasonable basis for estimating them.[118]

V. Drafting Implications and Conclusion

The framework also has practical consequences for settlement drafting, discovery definitions, valuation orders, and requests for expert or forensic fees. To reduce post-decree litigation, a settlement agreement should identify digital assets in detail. A schedule should cover exchange accounts, wallets, public addresses, asset types, quantities, valuation date and source, tax-basis records, forks, airdrops, staking rewards, wrapped assets, stablecoins, pending claims, lost-access claims, and post-valuation transfers. The agreement should also state what happens to later-discovered assets, derivative tokens, post-valuation rewards, and tax records needed by the recipient. Generic personal-property language may be too blunt for these issues. If one spouse keeps a business, the agreement should say whether business-held digital assets, exchange accounts, mining equipment, or wallet credentials are included. If the parties divide coins in kind, the agreement should include the transfer mechanics rather than leaving them to informal cooperation after judgment. *LaFond* and *DeSouza* show the need to address misrepresented value, converted assets, derivative coins, and wallet transfers in the decree or settlement record.[119]

---

116 *DeSouza*, 266 Cal. Rptr. 3d at 893-94, 897-98.

117 I.R.S. Notice 2014-21, 2014-16 I.R.B. 938 (treating virtual currency as property for federal tax purposes); 26 U.S.C. § 1041(a)-(b) (no gain or loss recognized on a transfer of property between spouses or incident to divorce; the transferee takes the transferor's adjusted basis).

118 *Cf.* Maurer v. Maurer, 623 N.W.2d 604, 607-08 (Minn. 2001) (permitting consideration of future tax consequences where the record supplies a "reasonable and supportable basis for making an informed judgment as to [the] probable liability").

119 *LaFond*, 2022 WL 714430, at *1-3; *DeSouza*, 266 Cal. Rptr. 3d at 893-94. An airdrop is a distribution of tokens to existing wallet holders without charge, typically to promote a new project or following a fork. *See Crypto Glossary*, *supra* note 42 (entry for "airdrop").

Discovery requests should define digital assets broadly enough to capture the ways value can change form. The definition should reach bitcoin, ether, altcoins, stablecoins, tokens, NFTs, governance tokens, staking rewards, mining proceeds, forks, airdrops, wrapped assets, DeFi lending and borrowing positions, liquidity-pool interests, exchange accounts, self-custody wallets, cold storage, hardware wallets, public addresses, and transaction histories. It should also cover accounts or wallets opened, used, controlled, accessed, funded, closed, or transferred during the relevant period. The reason is practical. Crypto value often changes form without leaving the economic estate. Coins can be swapped for other tokens, bridged to another chain, wrapped, staked, loaned, deposited into a liquidity pool, or moved from an exchange to self-custody. A request limited to "cryptocurrency accounts" may invite a narrow response that omits the record needed for classification, tracing, valuation, and enforcement. The definition should be paired with production formats. A party may need native CSV exports, complete transaction histories, account statements, tax forms, screenshots only as a backup, and public addresses or transaction hashes sufficient for independent review. For self-custody, the request should separate proof of control from production of spend authority, so the responding spouse can identify wallets and preserve records without immediately exposing a seed phrase. Derivative assets, multiple wallets, converted coins, tracing across accounts, and physical storage have all tripped up definitions that did not anticipate them—reason enough to name each one up front.[120]

A crypto valuation order should fix the asset, quantity, date, time, price source, exchange or index, network, wallet or exchange location, transaction fees, tax-basis record, and treatment of forks and rewards. An in-kind order should specify the receiving address, a test transaction, confirmation procedure, timing, fee allocation, and failed-transfer risk. If the court uses offset, the order should state why direct transfer is impractical or unsafe and should identify the asset used to equalize the award. If the court uses a sale, the order should state who sells, on what platform, by what deadline, who bears fees and taxes, and how slippage or market movement will be handled. If the court reserves jurisdiction, it

120 *DeSouza*, 266 Cal. Rptr. 3d at 892-94; *A.S.*, 2026 N.Y. Slip Op. 50471(U), at *5-7; *LaFond*, 2022 WL 714430, at *1-3; *Fial*, 591 P.3d at 255-57; *Coe*, 358 So. 3d at 27-28.

should say what future event triggers a return to court. The cases point toward orders that do the operational work: they should specify the transfer mechanics, use arithmetic that matches the coin count, fix the valuation date, and address derivative assets expressly.[121]

Where a spouse's control or concealment renders conventional discovery inadequate, a shifting of expert and forensic fees may be warranted. The request should be framed around need, proportionality, and allocation. A party seeking fees should identify the suspected asset, the cheaper discovery already attempted, the remaining gap, the proposed expert work, and the amount at stake. A party resisting fees should be required to say whether the objection is cost, privacy, relevance, access, or lack of foundation. That structure helps the court distinguish a speculative fishing expedition from a targeted effort to complete the record. It also creates a basis for fee shifting when one spouse's nondisclosure, refusal, or exclusive control made the forensic work necessary. Courts have allocated fees and costs for exactly this kind of work, including expert tracing of undisclosed cryptocurrency and hard-drive recovery.[122]

The reported cases do not establish a separate body of cryptocurrency-specific divorce law. They show that ordinary rules of classification, disclosure, valuation, sanctions, and distribution remain workable when the record identifies the asset, attributes control, traces acquisition and transfers, and supplies a defensible valuation. What cryptocurrency changes is where that record lives: identity, transaction history, and control can sit separately on exchanges, public ledgers, devices, and private credentials. Once the record is built, the cost of reaching a self-custodied asset—data recovery, forensics, expert access—stops being overhead and becomes one more item the court can allocate between the spouses.

---

121 *Green*, 2026 WL 1309595, at *13 & n.22 (non-precedential); *Coe*, 358 So. 3d at 27-28; *Hull*, 2026 WL 122187, at *6-7; *DeSouza*, 266 Cal. Rptr. 3d at 892-94; *Shteiwi*, 2025-Ohio-2901, ¶¶ 61-64.

122 *A.S.*, 2026 N.Y. Slip Op. 50471(U), at *18-22 (awarding pendente lite counsel and expert fees to fund tracing of allegedly undisclosed cryptocurrency); *Coe*, 358 So. 3d at 27-28 (requiring reimbursement of one-half of the cost of recovering the hard drive holding the parties' bitcoin). *LaFond* and *Ahlgren* illustrate the evidentiary value of expert tracing but did not address the allocation of expert fees in a dissolution proceeding.

For practitioners, the task is to build that record in a disciplined sequence.[123] Preservation comes before assets or records move; lower-cost indicators decide whether more intrusive discovery is warranted; party disclosures are checked against independent records; and access evidence is preserved without exposing spend authority. Followed in that order, the sequence leaves cryptocurrency presenting fewer new legal rules than new problems of proof.

---

123 *See DeSouza*, 266 Cal. Rptr. 3d 890; *Leonova*, 242 A.3d 713; *Cohen*, 2021 WL 12151633; *Coe*, 358 So. 3d 24; *Seyl*, 2026 IL App (2d) 240719-U; *Hull*, 2026 WL 122187; *LaFond*, 2022 WL 714430; *A.S.*, 2026 N.Y. Slip Op. 50471(U); *Fial*, 591 P.3d 253; *Green*, 2026 WL 1309595.