

What Splitting the Keys Changes

28 October 2026

In the script-based form of a two-of-three bitcoin wallet, holding two of the three recovery phrases is not always enough to spend. The network releases the coins only if the spender presents the full spending script, which lists all three public keys, and it matches exactly [9][10][14]. If one key is lost and the record of the wallet's configuration is lost with it, the two surviving keys can be left unable to act. Shared control reduces some risks. It also creates new ones, and the Law Commission treats the question of who controls a holding separately from the question of who owns it.

The question

When control of bitcoin is split across several keys and several people, what risks does that reduce, what new risks and burdens does it create, and how does English law currently think about who controls, and who owns, a jointly controlled holding? And how does this bear on a family that wants more than one person to be able to act if the holder cannot?

Method and sample window

We read the Property (Digital Assets etc) Act 2025 and the Bill's explanatory notes [1][4]; the Law Commission's Digital assets: Final report in full official text, concentrating on its glossary and chapters 2 and 5, with its project page for dates [2][3]; and three pages of HMRC's Cryptoassets Manual [5][6][7]. We read chapter 7 of the FCA's policy statement PS26/11 and its made rule on back-up keys [20]. For how multi-signature works, we read eight Bitcoin Improvement Proposals (BIPs), Bitcoin's published technical standards [8]–[15]. The UK Jurisdiction Taskforce's Report on Control of Digital Assets (March 2026) is released by LawtechUK through a download form; we did not review its full text. We read LawtechUK's pages on it and three briefings on it, by two law firms and a barristers' chambers [16]–[19][21]. All sources were accessed on 28 October 2026. The scope is England and Wales.

How we weigh the sources. Legislation sets the framework. Law Commission reports explain the reasoning of the statutory law reform body; they are not law. HMRC's manual states HMRC's view for tax purposes. FCA rules apply to firms. The BIPs are cited only for how the technology works. Briefings are commentary, used only to report what a document covers. We do not summarise court judgments. Where we found nothing on a point, we report a gap in the record, not a gap in the law.

A note on terms. A private key is the secret used to authorise a transaction; a public key is generated from it [5]. A signature is the proof, made with a private key, that a transaction is authorised. A recovery phrase (or seed phrase) is a list of words from which a wallet's keys are generated, which can be written on paper [15]. A wallet is the interface in which the private key is stored [6].

1. A multi-signature arrangement is defined by its threshold

A multi-signature wallet requires a set number of signatures, from a larger set of keys, before coins can move. The Law Commission's glossary calls these M-of-N arrangements, with M the number of signatures or keys required and N the total [2]. The required number is called the threshold, or quorum. BIP 11, assigned in October 2011, proposed "M-of-N-signatures required transactions" as a standard type, with examples including a two-of-three escrow between buyer, seller and a dispute agent [8].

Multi-signature is not the same as splitting a single key. The Law Commission's glossary separately describes "sharding of keys": splitting one key into pieces, some subset of which can be recombined to recover and use it [2]. In the script-based multi-signature examined here, each key produces its own signature, and nothing is recombined [8][14].

2. The wallet configuration is part of what must be kept

In the script-based forms of multi-signature set out in BIP 16 and BIP 141, coins are locked to a hash (a fingerprint) of a script, not to the script itself. To spend, the spender must supply the script, and validation fails if its hash does not match [9]. The script contains the threshold and every public key in the arrangement [14]. The newer Segregated Witness form works the same way [10].

BIP 380, which specifies output script descriptors, notes that, typically, "backups have consisted of solely the private keys", and that given only those, a restored wallet cannot know which scripts and addresses to produce [13]. A descriptor is a short, readable record of the exact scripts and keys a wallet uses, including how keys are derived [13]. In this article we call that record the wallet configuration.

A two-of-three holding therefore needs enough keys to meet the threshold and the public details of every key, including any lost key. A lost recovery phrase takes its public key with it unless that public key was recorded elsewhere. The configuration carries no spending power on its own, but it is enough to set up a watch-only wallet [13], and it is not optional.

3. Splitting control moves risk; it does not remove it

In a two-of-three arrangement, any one key can be lost and the coins can still move. Any one key can be stolen and the thief still cannot move them [8][14]. The same arithmetic shows the new exposures. Two keys lost together means the coins cannot move. Two keys reached by the same person, whether by theft, coercion or collusion, means they can, given the configuration. The protection depends on the keys failing independently. Keys stored in one building, or held by two people who travel together, may not.

A third party holding one key introduces a dependence on that party. BIP 11's example of a two-of-two wallet with a protection service (WPS) carried a side note about copies of the service's keys, "so that their coins can be spent even if the WPS goes out of business" [8].

The FCA's new rules for firms address one version of this. In PS26/11, respondents asked how its custody rules apply where control "may be distributed or shared", such as multi-party computation (MPC), where keys are split across systems so no single party can move the asset (para 7.13) [20]. The FCA introduced an exception from its trust requirement where a firm holds a back-up key and the client "retains full control of the cryptoasset and can act independently"

(chapter 7, response to question 29; CASS 17.3.12R) [20]. It notes remaining risks, including "misuse or theft of the cryptoassets by virtue of the firm having a back-up key", and keeps such firms subject to CASS 17.2 and 17.4 and barred from appointing third parties [20]. Its Diagram 1 shows that a firm holding a key, or part of one, may or may not fall within its safeguarding rules, depending on the arrangement [20].

4. Shared control is a standing coordination burden

Every multi-signature transaction must be assembled, passed to enough signers, and combined. BIP 174 defines a standard format for this, the partially signed bitcoin transaction (PSBT) [12]. It allows a signer to be offline, because the transaction carries the information needed to sign [12]. It also allows a signer to show the addresses, amounts and fee as "a confirmation of intent" [12]. Each signer can be a separate check. That is a safeguard and a cost: every transaction needs enough of the right people, with their devices, available. Routine use favours keeping keys close at hand; protection against a single event favours keeping them apart.

5. The Law Commission describes control as a fact and declines to define it

The Property (Digital Assets etc) Act 2025, dated 2 December 2025, provides that a thing, "including a thing that is digital or electronic in nature", is not prevented from being the object of personal property rights merely because it is neither a thing in possession nor a thing in action [1]. It does not mention bitcoin, control or multi-signature [1]; the explanatory notes leave wider matters "to development by the common law" [4].

The Law Commission's final report, published on 28 June 2023 [3], sets out its approach in chapter 5. It describes, "but do[es] not define", the factual concept that best captures the ability to exclude or permit access to such a thing and to put it to its uses (para 5.2) [2]. It calls control "highly complex, composable and multi-faceted" (para 5.3) [2]. It does not recommend a statutory definition, concluding that "the common law is best placed" to develop the concept (para 5.12) [2].

Multi-signature runs through that reasoning. The report records multi-signature arrangements as "the most obvious and most-cited area of complexity" raised by consultees (para 5.14) [2]. It lists them among the ways users currently "manipulate control", alongside hardware wallets and intermediated holding (para 5.69) [2]. These are the Commission's descriptions and conclusions. They are not law.

6. The Law Commission expects shared control, and separates control from title

The report has a short section on shared control. In some situations, it says, "multiple parties might share control, no single party might have control, or control might be split in a variety of different ways" (para 5.94) [2]. It does "not think these issues are insurmountable for the law" (para 5.95) [2]. Where parties share control, it expects intention to help, and says intention "can readily be inferred by analysing the contractual and other arrangements between the parties", including the laws of agency (para 5.96) [2].

It compares a warehouse door with several keys held by different people, but says the analogy "can only go so far" (para 5.98) [2].

On ownership, the report states: "Almost all consultees agreed that superior legal title and control over a digital object can be separated" (para 5.74) [2]. It gives multi-signature arrangements as an example of technical conditions that "regulate how a particular crypto-token can be controlled" (para 5.75) [2]. It concludes that factual control "(plus intention) can found a legal proprietary interest", which in certain circumstances can be separate from, and inferior to, "a superior legal title" (para 5.104) [2].

The report does not apply this to families. It treats holding a key as a question of control, and leaves to the courts how control and intention bear on competing interests (paras 5.95–5.98, 5.104) [2].

7. The guidance that followed is recent, non-binding and contextual

The Law Commission recommended an expert panel to give "non-binding guidance" on control (para 5.4) [2]. LawtechUK states that the UK Jurisdiction Taskforce's Control Panel was set up following that recommendation and "is chaired by Justice Zacaroli" [16]. Briefings by a law firm and a barristers' chambers report that the panel's Report on Control of Digital Assets was published on 19 March 2026 [17][18]; Mayer Brown describes it as "non-binding, practical guidance" [19].

According to those briefings, the report covers multi-party control. 3VB lists "direct, multi-party, smart contract-based, delegated, and layered forms of control" among its use cases [18]. DLA Piper lists shared and multi-party control, including "multisignature wallets requiring multiple keyholders to authorise a transaction", among its examples, and reports that control is to be assessed "on a context-specific, system-by-system basis" [17]. LawtechUK's page for the report states its purpose: to give guidance on how digital assets are controlled in practice, "in order to assist in the identification of the legal or equitable owner(s) of digital assets or of an interest in them" [21].

We did not review the report's full text, so we do not state its conclusions on multi-signature holdings. The briefings did not set them out [17][18][19].

What the record does not say

None of the three HMRC pages we read mentions multi-signature or shared control. CRYPTO10350 frames keys around one pair: "Any person who knows the public and private keys can authorise transactions" [5]. HMRC states that misplacing a key "does not count as a disposal", and that a negligible value claim could be made where there is no prospect of recovery [7]. We found no HMRC guidance on losing one key of several where the threshold can still be met.

We found no official source that sets out a rule for family members who each hold a key. The FCA's rules govern firms; the parts we read do not address keys held among family members [20].

If the holder cannot act

Alderlux's Foundations piece, [A Will Cannot Reach Bitcoin](#), sets out why legal ownership and practical access are separate. Our forthcoming investigation, *Losing Capacity, Not Life*, examines an attorney's authority under a lasting power of attorney.

Multi-signature can give a second person a key. Whether they can act without the holder depends on the threshold. If others together hold enough keys to meet it, they can, and so could anyone who reached their keys. If not, they cannot. Holding a key is a technical position; authority to act for another person is a separate legal question.

Questions a holder can ask

- What is the threshold, how many keys exist, and could the people other than the holder meet it together?
- Who holds each key, and could two of them be lost, or reached, in the same event?
- Where is the wallet configuration recorded, and would it survive the loss of any single key?
- Does any key depend on a firm or service, and what happens to that key if the firm stops operating?
- How long would it take to gather enough signers, and does each understand what they are approving?
- Is there a written understanding of who owns the coins, separate from who holds the keys?
- If a key holder could no longer act, who would decide what happens to their key?

The case for the opposing view

It can fairly be argued that multi-signature is mature: the core standard dates from 2011, and later standards address key order, configuration and coordination [8][11][12][13]. On this view the risks above are design choices with technical answers. The lack of a statutory rule is also deliberate: the Law Commission chose to leave control to the common law (para 5.12) [2].

Both points have force. Neither decides, for a particular family, who holds what, where it is recorded, or who owns the coins.

Conclusion

Multi-signature replaces one point of failure with a threshold. A two-of-three arrangement tolerates the loss or theft of any single key, but depends on the configuration being kept, the keys failing independently, and enough signers being available. It changes where the risk sits rather than removing it.

The Law Commission treats control as a fact, capable of being shared and separable from title, and leaves the rest to the courts. The guidance that followed is non-binding. For a family, holding a key, having authority to act, and owning the coins are three separate questions. A multi-signature wallet answers only the first.

Limitations

- England and Wales only.
- The UK Jurisdiction Taskforce report was not reviewed in full. Its content is reported only as described by LawtechUK, two law firms and a barristers' chambers.
- Law Commission report: glossary and chapters 2 and 5 read closely; later chapters searched, not read in full.
- The Law Commission's 2024 supplemental report and draft Bill were not reviewed.
- PS26/11: chapter 7 and CASS 17.3.12R–17.3.13G read; other chapters and policy statements not.
- The LawtechUK report page [21] was read; the report itself was not.
- Taproot-based multi-signature forms were not examined.
- No court judgments are summarised.
- The sources we read contain no data on how many holders use multi-signature or how often arrangements fail.

Sources

1. Property (Digital Assets etc) Act 2025 (c. 29), as enacted, 2 December 2025. legislation.gov.uk
2. Law Commission, Digital assets: Final report, Law Com No 412, HC 1486 (June 2023), glossary and chapters 2 and 5
3. Law Commission, Digital assets (project page)
4. Property (Digital Assets etc) Bill [HL], Explanatory Notes, HL Bill 31–EN (11 September 2024). UK Parliament
5. HMRC, Cryptoassets Manual, CRYPTO10350: Introduction to cryptoassets: public and private keys (updated 28 November 2025)
6. HMRC, Cryptoassets Manual, CRYPTO10375: Introduction to cryptoassets: wallets (updated 28 November 2025)
7. HMRC, Cryptoassets Manual, CRYPTO22400: Cryptoassets for individuals: Capital Gains Tax: losing private keys (updated 28 November 2025)
8. BIP 11, M-of-N Standard Transactions (assigned 18 October 2011). Bitcoin BIPs repository
9. BIP 16, Pay to Script Hash (assigned 3 January 2012)
10. BIP 141, Segregated Witness (Consensus layer) (assigned 21 December 2015)
11. BIP 67, Deterministic Pay-to-script-hash multi-signature addresses through public key sorting (assigned 8 February 2015)
12. BIP 174, Partially Signed Bitcoin Transaction Format (assigned 12 July 2017)
13. BIP 380, Output Script Descriptors General Operation (assigned 27 June 2021)
14. BIP 383, Multisig Output Script Descriptors (assigned 27 June 2021)
15. BIP 39, Mnemonic code for generating deterministic keys (assigned 10 September 2013)
16. LawtechUK, Reports
17. DLA Piper (law-firm briefing), The UK Jurisdiction Taskforce (UKJT) Report on Control of Digital Assets (17 April 2026)
18. 3VB (barristers' chambers briefing), UKJT Report on Control of Digital Assets published (20 March 2026)
19. Mayer Brown (law-firm briefing), UK Jurisdiction Taskforce Publishes Report on Control of Digital Assets (22 May 2026)
20. Financial Conduct Authority, PS26/11: Crypto Regime – Regulated Cryptoasset Activities (June 2026), chapter 7 and Appendix 1 (FCA 2026/42, CASS 17.3.12R–17.3.13G)
21. LawtechUK, Report on Control of Digital Assets (report page; the report itself was not read)

Alderlux provides education and information only. We do not provide regulated financial advice, investment recommendations, legal or tax advice. Alderlux is not authorised by the Financial Conduct Authority.