

Held for You, or Held by You

28 October 2026

From 25 October 2027, a firm safeguarding qualifying cryptoassets for customers in the UK must be authorised by the Financial Conduct Authority (FCA) [1][2]. The FCA does "not plan to extend FSCS cover" to these activities, so under its stated approach a custodian's failure would not open a route to Financial Services Compensation Scheme (FSCS) compensation [5]. Recovery would instead depend on how the coins were held, the legal arrangements around them and the circumstances of the failure [4]. The regime changes what custodians must do; it does not guarantee that customers get their coins back [2] [4].

The question

For a UK individual holding bitcoin, what does leaving it with an exchange or custody provider protect against and expose them to, compared with holding the keys themselves? And what does the new UK cryptoasset regime, which brings custody (in the legislation, "safeguarding") within the Financial Services and Markets Act 2000 from 25 October 2027, change and not change?

The regime applies to cryptoassets such as bitcoin that fall within the definition of "qualifying cryptoasset" in the 2026 Regulations [1]. A private key is the code that authorises a transaction. HMRC's manual describes it as "a randomly generated string", and states that any person who knows the keys can authorise transactions [9].

Method and sample window

We read SI 2026/102, the Cryptoassets Regulations [1]; the FCA's policy statements PS26/11 and PS26/13, including the client asset rules for cryptoassets (CASS 17) [4][5]; the FCA's overview and gateway pages [2][3]; its perimeter guidance PERG 18.6 and 18.12 [6][7]; five HMRC manual pages [8]–[12]; and an HM Treasury policy note [15]. All were accessed on 28 October 2026.

Legislation sets the boundary of what is regulated; FCA rules show how it will be applied. We use law-firm briefings only where the FCA text is silent: on the UK Jurisdiction Taskforce's 2024 insolvency statement, whose full text we did not review [13][14]. We do not summarise any court judgment.

1. The test is whether a firm can bring about a transfer, not who owns the coins

The 2026 Regulations create a regulated activity of safeguarding a qualifying cryptoasset on behalf of another person [1]. A firm is safeguarding if it has "control of the cryptoasset through any means that would enable" it "to bring about a transfer of the benefit of the cryptoasset to another person" [1]. Those means include holding or storing all or part of the "means of access", or appointing someone else to do so. "Means of access" includes "a private cryptographic key" [1].

Legal form does not take a firm outside the activity. "On behalf of another" includes cases where the customer has both legal and beneficial title, beneficial title only, or only "a right against" the firm "for the return of the cryptoasset" [1]. The FCA's guidance says safeguarding may be carried on "regardless of whether the cryptoasset is owned by the customer or the firm" [6]. The FCA explains its focus on control: such a firm can sign transactions "as if they were the owner, whether they have permission from the rightful owner to do so or not" [4].

Keys are central to the test, but the arrangement as a whole decides it [1][6]. The customer's legal title still matters if the firm fails, as finding 4 shows.

2. A firm's promise not to move the coins does not decide whether it holds them

The FCA's perimeter guidance frames the test as whether the firm "is, or could put itself, in a position to initiate a transfer" [6]. The ability merely to prevent a transfer is not enough [6]. A firm that "promises (eg, under a contract) not to exercise control but does actually have the requisite control" is still safeguarding [6]. Showing that a firm lacks "any means" to move a customer's coins "is likely to involve examining how the solution is engineered in technical detail" [6].

Shared arrangements depend on their design. A firm holding a single key "shard", a fragment of a key, may not have control on that basis alone; "the relevant threshold in that situation will be a case-specific matter" [6].

3. Holding your own keys sits outside the FCA custody rules

PS26/11 states it directly: "Self-custody models, where clients safeguard their cryptoassets themselves and firms do not have the ability to bring about a transfer, are not in scope of Article 9N and therefore the CASS rules do not apply" [4]. What falls away is the FCA custody regime, not the holder's other legal rights. HMRC, for example, treats the victim of a theft as still owning the asset, with "a right to recover it" [12].

No intermediary stands between the holder and the coins. But CASS 17 is built to ensure firms keep "accurate books and records", minimise "risk of loss or diminution", and protect "the means of access" [4]. In self-custody those tasks fall to the holder. Wallets and keys "can be duplicated" [10]. If a key was stored only on a computer that was later destroyed, the tokens "would be unreachable, although they would continue to exist" [9].

Self-custody is not one arrangement. A single device, a multi-signature set-up, backups held in separate places, or a recovery service holding a back-up key each carry different risks. What separates them is the wallet's design, how backups are kept, and whether any other party can initiate a transfer [4][6]. A firm holding a back-up key that would enable it to bring about a transfer is safeguarding, and is regulated though not as a trustee (finding 4); one holding a key or shard that cannot do so may fall outside the activity [4][6].

On tax, HMRC's guidance addresses lost keys and theft, not custodian failure. Misplacing a key "does not count as a disposal" for Capital Gains Tax. A negligible value claim may be possible "if it can be shown there is no prospect of recovering the private key or accessing the tokens", and has effect only "if HMRC accepts" it [11]. HMRC "does not consider theft to be a disposal", so "victims of

theft cannot claim a loss for Capital Gains Tax" [12]. We found no guidance, in the five manual pages we read, on coins lost in an exchange failure; nothing here implies the same treatment applies [8]–[12].

Whether anyone else could reach self-custodied coins if the holder could not act is the subject of our Foundations piece, [A Will Cannot Reach Bitcoin](#).

4. What a customer recovers on failure depends on how coins were held, and the failure rules are still to come

From 25 October 2027, a firm safeguarding cryptoassets must, "unless otherwise permitted", do so "as a trustee of the relevant cryptoasset" (CASS 17.3.3R) [4]. The FCA gives its reason: "the primary advantage of a trust is that it protects clients from competing claims to their cryptoassets in insolvency" [4]. Client coins must be "not co-mingled with, and ... identifiable separately from, any other assets" (CASS 17.3.17R(2)) [4].

The trust protects against competing claims. It does not guarantee that every coin comes back. The FCA notes that whether a creditor could claim client cryptoassets "will depend on the effect of applicable law, including under any future special insolvency regime" [4]. Where a shared trust falls short, its terms must say how the shortfall is allocated, and the FCA "would generally expect" it to be borne "pro rata" by the clients in that class (CASS 17.3.17R(3), 17.3.18G(3)) [4]. The trust terms must also state whether client cryptoassets may fund "the distribution costs of the trust on the failure of the trustee" (CASS 17.3.17R(4)) [4].

The trust has "targeted exceptions" [2]. Five were consulted on. Under them, coins may be held outside the trust or taken out of it, and the FCA states that these exceptions "reduce CASS protections" [4]:

- Lending (CASS 17.3.4R). Coins a client has engaged the firm to lend sit outside the trust while the lending service runs; the exception ends when the service ends [4].
- Settlement float (CASS 17.3.5R). Up to 2% of each client's cryptoassets, per cryptoasset class, may be held outside the trust to settle the client's trades on a UK trading platform run by the firm or its group. It needs prior informed consent, and the exception stops once a withdrawal of consent takes effect (CASS 17.3.11R(5)) [4].
- Services needing ownership (CASS 17.3.6R). Where the firm concludes a service requires it to own the coins, the firm takes ownership with prior informed consent and must record its reasons; the guidance gives staking as an example (CASS 17.3.7G) [4].
- Client instructions (CASS 17.3.8R). Coins leave the trust once moved on the client's "express and specific instruction"; a general discretionary mandate does not count (CASS 17.3.9G) [4].
- Debts (CASS 17.3.10R). The firm may take ownership of coins to discharge a debt the client owes it, under a written agreement [4].

The FCA added a sixth exception separately. A firm holding only a back-up key (or key shard), where the client has its own means of access, need not hold the coins on trust (CASS 17.3.12R) [4]. The client keeps control. The FCA's rationale is that if the back-up firm fails, the owner "continues to retain full control of their cryptoassets" [4]. The firm remains subject to CASS 17.2 and 17.4, and may not appoint third parties [4].

Where consent is required, the firm "must specifically and clearly explain to the client the risks to the client of the cryptoasset not being within a trust, including in the event of the firm's failure" (CASS 17.3.11R(3)) [4].

The UK Jurisdiction Taskforce's 2024 statement, which the FCA text does not cite, sets the background. As summarised by CMS, it concluded that digital assets "are capable of amounting to property for the purposes of English insolvency law", and that a recovery claim "could still be a proprietary claim, depending on the particulars of how the assets were held" [13]. Clifford Chance describes the statement as non-binding [14].

The rules for a custodian's failure are not yet written. The FCA has "committed to consulting on failure and distribution rules" for firms subject to CASS 17 [5]. Its overview states: "We will consult later this year on our proposed approach to managing cryptoasset firm failure" [2]. We did not find that consultation published in the searches we ran on 28 October 2026.

5. Authorisation brings complaints access and conduct rules, not compensation

PS26/13 confirms that most regulated cryptoasset firms will be subject to the Consumer Duty, conduct of business rules, "Dispute Resolution and access to the Financial Ombudsman Service", and CASS [5]. The Duty requires firms "to put consumer needs first and act to deliver good outcomes" [5].

Being able to complain is not the same as being compensated. Four steps are distinct. First, eligibility: the Ombudsman's compulsory jurisdiction covers eligible complainants, such as consumers with a relevant relationship with the firm (DISP 2.7.3R, 2.7.6R) [5]. Second, the outcome: a complaint "is likely to be upheld if the Financial Ombudsman finds that the firm has acted in a way that has caused loss" [5]. Third, redress: it is "unlikely" to be owed where a loss "has been caused by poor market performance" [5]. Fourth, payment: the FCA handles FSCS under the heading "Consumer compensation when firms are unable to meet liabilities", and does "not plan to extend FSCS cover" to these activities [5]. We found nothing in PS26/13 on how redress would be met by a failed firm that cannot pay.

The mandatory risk summary for qualifying cryptoassets will state that the FSCS "doesn't protect this type of investment" [5]. Firms that safeguard cryptoassets must instead explain "how any shortfall in trust property would affect clients in the event of firm failure" (COBS 6.1.7BR(3)(a)(ii)) [5].

Regulation also leaves the asset unchanged. The FCA states: "Cryptoassets are high risk investments and will remain high risk under our regime" [2]. It adds that consumers "could lose the entire value of their investment" [2].

6. Until 25 October 2027 custody is not yet a regulated activity, and two routes let some firms continue afterwards

The Regulations "come into force on 25th October 2027 (the 'full commencement day')", except that they took effect earlier for limited purposes such as FCA rule-making and applications [1]. The FCA's custody rules come into force on the same day [4]. Its application window "started on 30 September 2026 and will close 28 February 2027" [3].

Today, unauthorised exchange and custodian wallet providers must register under the Money Laundering Regulations [7]. Those registrations "will not convert automatically" [2].

Part 7 of the Regulations sets out two routes for firms that have applied but are not authorised when the regime starts [1]:

- Saving provision (regulation 53). It applies to a firm that applied "during the relevant application period", whose application has "not been determined" or has been refused but is "open to review" and which the FCA has not directed into the transitional route. For the activity applied for, the firm "is to be treated as if Parts 3 to 6 of these Regulations had not come into force". The provision ends two years after the full commencement day (regulation 53(3)) [1].
- Transitional provision (regulations 55 and 56). It applies to a firm that applied outside the window but before commencement, to an in-window applicant whose application has been refused (and is no longer open to review) or withdrawn, and to a firm the FCA directs into it [1]. The firm's exemption applies "solely to the extent ... necessary for the performance of a pre-existing contract", meaning one "entered into before the relevant day" (regulation 56(3), (4)) [1]. The FCA's gateway page puts it plainly: such firms "will not be able to enter into new contracts with existing UK customers or enter into new contracts with new UK customers" [3]. The firm must tell each counterparty that it "is not authorised by the FCA" for that activity (regulation 58) [1]. The FCA may cancel the exemption or impose conditions (regulation 59), and the provision ends two years after commencement (regulation 55(9)) [1].

Firms that have not applied must "run-off their UK cryptoasset business before the new regime commences" [3]. The saving route's wording treats the new regime as not yet in force for that firm's activity [1]; we found no FCA statement on how the custody rules apply to a firm relying on either route.

The trade-offs side by side

	FIRM HOLDS THE KEYS (EXCHANGE OR CUSTODIAN)	SHARED OR BACKUP-KEY ARRANGEMENTS	OWN KEYS ONLY
Who can move the coins	The firm with control [1][6]; for exchange wallets, "the platform holds and controls" the keys [10]	Depends on the design and the applicable rules; a firm may or may not have control [4][6]	Anyone who knows the keys [9]
FCA custody rules	CASS 17: trust, separate identification, reconciliation, key management, subject to exceptions [4]	A firm with control: CASS 17. A back-up key holder where the client has its own means of access: CASS 17.2 and 17.4, no trust [4]	"The CASS rules do not apply" [4]
If the firm fails	Trust protects against competing claims; outcome subject to applicable law; failure rules still to come [4][5]	Where only a back-up key is held, the owner "continues to retain full control"; otherwise as for a firm with control [4]	No custodian to fail
FSCS	Not planned [5]	Not planned [5]	Not applicable
Main dependency	The firm's arrangements and solvency [4]	The design and the parties holding keys [4][6]	The holder's own keys and backups [9][10]

What the record does not say

- How the FCA custody rules apply to a firm under the saving or transitional provision [1][3][4][5].
- How many UK holders use each model. We found no figure, and make no claim about which is more usual.

The questions that matter before you choose

CONTROL

- Who can initiate a transfer, alone or jointly with others [6]?
- Is the provider authorised for safeguarding, relying on the saving or transitional provision, or registered only under the Money Laundering Regulations [1][3][7]?
- How many copies of the keys exist, where are they, and who else could use them [10]?

RECOVERY

- What happens if a key, a device, a provider or a key-holder becomes unavailable [9]?
- Could someone else reach the coins if the holder could not be asked?

FAILURE

- Are client coins held on trust, under which document, and do any of the trust exceptions apply to this account [4]?
- How would a shortfall in trust property affect clients if the firm failed, and may client coins fund distribution costs [4][5]?

Where the trade-off sits

A provider can reduce the burden of managing keys, but it brings counterparty and custody risk: the firm's conduct, its arrangements and its solvency. Self-custody removes the custodian, but access, security and recovery then depend on the holder's own arrangements. Neither model is safer in every circumstance. The question is which set of risks the holder can understand and manage.

Limitations

- PS26/11, PS26/13 and the Regulations were read in full. The full text of the UK Jurisdiction Taskforce statement was not reviewed, and the FSCS was not consulted directly; its position is taken from the FCA.
- The UK Jurisdiction Taskforce statement addresses English law. Scottish and Northern Irish insolvency law were not examined.
- PS26/12 (prudential rules) was not examined, and only five HMRC manual pages were read.
- No court judgment is summarised or relied on.

Sources

1. The Financial Services and Markets Act 2000 (Cryptoassets) Regulations 2026, SI 2026/102, made 4 February 2026. legislation.gov.uk. Regulation 1; Regulated Activities Order article 9N as inserted by regulation 40(5); Part 7, regulations 51–59 (savings and transitional provision)
2. Financial Conduct Authority, Overview of our cryptoassets regime policy statements, published 30 June 2026
3. Financial Conduct Authority, Cryptoassets: How the gateway will operate, first published 8 January 2026, last updated 30 September 2026
4. Financial Conduct Authority, PS26/11, Crypto Regime: Regulated Cryptoasset Activities, June 2026, Chapter 7 (Safeguarding) and Appendix 1, Cryptoassets (Safeguarding) Instrument 2026 (FCA 2026/42), CASS 17

5. Financial Conduct Authority, PS26/13, Application of FCA Handbook for Regulated Cryptoasset Activities, June 2026, paras 1.2, 3.2, Chapter 5 and Chapter 12 (paras 12.1–12.34 and responses), and COBS 4 Annex 1R as amended
6. Financial Conduct Authority Handbook, PERG 18.6, Activity: safeguarding qualifying cryptoassets and relevant specified investment cryptoassets, last updated 16 September 2026
7. Financial Conduct Authority Handbook, PERG 18.12, Interaction with the Money Laundering Regulations, last updated 16 September 2026
8. HMRC, Cryptoassets Manual, CRYPTO10250, Introduction to cryptoassets: exchanges and exchange fees, updated 28 November 2025
9. HMRC, Cryptoassets Manual, CRYPTO10350, Introduction to cryptoassets: public and private keys, updated 28 November 2025
10. HMRC, Cryptoassets Manual, CRYPTO10375, Introduction to cryptoassets: wallets, updated 28 November 2025
11. HMRC, Cryptoassets Manual, CRYPTO22400, Cryptoassets for individuals: Capital Gains Tax: losing private keys, updated 28 November 2025
12. HMRC, Cryptoassets Manual, CRYPTO22450, Cryptoassets for individuals: Capital Gains Tax: being defrauded, updated 28 November 2025
13. CMS (law-firm briefing), Digital asset insolvency issues not insoluble for English law, 19 April 2024
14. Clifford Chance (law-firm briefing), Legal statement on digital assets and English insolvency law, 18 April 2024
15. HM Treasury, Draft statutory instrument amending the Financial Services and Markets Act 2000 (Cryptoassets) Regulations 2026: Policy Note, first published 21 April 2026, last updated 15 September 2026

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.