Bitcoin Policy
UNITED KINGDOM

Bitcoin Policy UK Response: FCA's GC26/7 on Decentralised Finance (DeFi)

Submitted by: Bitcoin Policy UK (BPUK)

Date: 12 November 2026

In response to: FCA's Guidance Consultation GC26/7 on Decentralised Finance (DeFi), published 21 October 2026.

Consultation deadline: 18 November 2026

Consultation contact: gc26-7@fca.org.uk

Consent: Bitcoin Policy UK responds as an organisation, does not request confidentiality, and consents to being named as a respondent and to its response being made public.

Executive Summary

Bitcoin Policy UK (BPUK) welcomes the FCA's proposed guidance on operational resilience and financial crime risks in decentralised finance (DeFi). We support the FCA's approach to assessing risk and the principle that firms remain responsible for the services they provide.

Bitcoin's base layer has demonstrated exceptional resilience since 2009, despite historical vulnerabilities and disruptions. Other blockchain networks have experienced significant outages, while many risks associated with Bitcoin arise from exchanges, custodians, bridges and applications rather than its underlying network. The FCA should distinguish between these different architectures and the risks they present, with practical examples showing how firms should assess them.

We also recommend stronger guidance on protecting customer information. Linking personal identities to wallet addresses can expose financial holdings and transaction histories, creating risks of fraud, theft and physical harm if those records are compromised.

Regulatory requirements should reflect the activities firms undertake, the technologies they use and the risks they can control. BPUK is not seeking preferential treatment for Bitcoin but proportionate regulation based on evidence.

Introduction and scope

Bitcoin Policy UK is a non-partisan, non-profit organisation providing research and policy expertise on Bitcoin in the United Kingdom.

This response should be read alongside our submission to CP26/36 of 27 October 2026[1], which addresses the regulatory perimeter issues discussed in Chapter 2 of the draft guidance.

[1] Bitcoin Policy UK, Response to the FCA's Consultation Paper CP26/36: Cryptoasset Perimeter Guidance, 27 October 2026.

Activities carrying comparable risks should meet comparable regulatory requirements. Where technologies introduce different risks, regulation should reflect those differences. Our position is not that Bitcoin should receive preferential treatment, but that regulatory requirements should be proportionate to the risks involved.

Question 1: Do you agree with our description of the operational resilience risks that may arise when firms provide financial services using DeFi? If not, please explain why.

The operational risks identified in paragraphs 1.6, 3.10 and 3.11 are relevant, but they differ significantly between blockchain networks and the applications built on them. The guidance does not clearly explain which risks apply to which technologies. Annex 2 already describes the different layers of the DeFi stack, and the FCA should use this framework to identify where specific vulnerabilities arise.

Different layers carry different risks. Many of the risks identified by the FCA arise from smart contracts, oracles, flash loans, administrator keys and protocol governance. Bitcoin's base layer does not support the complex smart contracts used by decentralised lending and trading platforms. Its scripting language is deliberately limited, reducing the potential for vulnerabilities associated with more complex applications.[2] Bitcoin also has no native price oracles, central administrator keys or committee controlling changes to its consensus rules.

Additional risks arise when Bitcoin is held or used through other networks and services. Wrapped Bitcoin (wBTC), for example, represents Bitcoin held in custody and issued as a token on another blockchain. Users depend on the custodian, the token's smart contracts and its governance arrangements, none of which form part of Bitcoin's base layer.

In 2024, changes to wBTC's custody arrangements prompted concerns about control of the underlying assets. Coinbase subsequently removed wBTC from trading, citing risks associated with the new arrangements.[3]

Bitcoin's Lightning Network also has its own operational risks, including channel liquidity and monitoring requirements. Federated sidechains depend on groups of signers to secure the Bitcoin backing their assets. These risks arise from the additional systems involved and should be assessed separately from Bitcoin's underlying network.

Different networks fail in different ways. Blockchain networks can experience different types of disruption depending on their design. In February 2024, Solana stopped finalising blocks for approximately five hours after a software fault affected validators running the same version of its software. Restoring the network required a coordinated restart.[4]

Ethereum experienced a different problem in May 2023, when disruptions to its consensus clients temporarily prevented blocks from reaching finality. Some blocks continued to be produced, and the network recovered without intervention.[5]

---

[2] Bitcoin Developer Guide, Transactions, section on Bitcoin Script. https://developer.bitcoin.org/devguide/transactions.html

[3] BitGo, "BitGo to Move WBTC to Multi-Jurisdictional Custody to Accelerate Global Expansion Plan", 9 August 2024 Coinbase Global Inc., opposition filing in BiT Global Digital Ltd v Coinbase Global Inc., 17 December 2024, pp. 8–9.

[4] Anza, "02-06-24 Solana Mainnet Beta Outage Report", 9 February 2024.

[5] Offchain Labs (Prysm), "Ethereum Mainnet Finality", Mainnet Postmortems, May 2023.

Bitcoin uses proof of work and has no equivalent mechanism for immediate finality. Instead, transactions become progressively harder to reverse as additional blocks are added. These differences affect how firms should assess network disruption, transaction settlement and operational resilience.

Bitcoin has demonstrated an exceptional record of operational resilience since its launch in January 2009. The independent Bitbo uptime tracker records approximately 99.99% availability, counting two major network disruptions in 2010 and 2013, with no further network downtime recorded by its methodology since then.[6]

In August 2010, a software flaw allowed a transaction to create more than 184 billion bitcoin, far exceeding the network's intended supply limit. Developers released a correction within hours, and the network adopted the corrected chain.[7] In March 2013, an incompatibility between Bitcoin software versions caused the blockchain to split temporarily. Mining pools voluntarily downgraded their software, sacrificing revenue to restore a single chain. The incident also resulted in a successful experimental double spend, documented in the developers' subsequent report.[8]

In September 2018, Bitcoin Core developers disclosed and patched another critical vulnerability that could have allowed the creation of additional bitcoin. They reported no known attempts to exploit it.[9] Bitbo's uptime figures measure major network disruptions rather than every software vulnerability or interruption experienced by individual users and services. Bitcoin was also a much smaller network during the incidents of 2010 and 2013. Its historical record does not guarantee future reliability, but it demonstrates that independently operated nodes, miners and developers have been able to respond to serious failures and restore normal operation without a central authority.

Recommendation 1: *The FCA should clarify in Chapter 3 that operational risks differ between blockchain networks and the applications built on them. Firms should assess the specific technologies they use, rather than applying the same assumptions to every network. The FCA should also use the framework in Annex 2 to identify which risks arise at each layer, with corresponding references in the risk tables at paragraphs 3.11 and 4.10.*

Question 2: Do you agree with our proposed guidance on how firms should assess and manage those operational resilience risks? Are there other risks or emerging practices we should consider?

BPUK supports the approach set out in paragraphs 3.16 to 3.42, particularly the distinction in paragraph 3.20 between the services firms provide to customers and the underlying protocols they use. Firms should remain responsible for the resilience of their services, while recognising the limits of their control over decentralised networks. We recommend four clarifications to help firms apply the guidance in practice.

Third-party arrangements. Paragraphs 3.39 to 3.41 address firms' responsibilities under SYSC 15A and, where outsourcing is involved, SYSC 8. A permissionless network such as Bitcoin has no central operator with whom a firm can negotiate contractual terms, audit rights or an exit plan. This differs from commercial providers such as custodians, hosted node services and bridge operators, which have identifiable operators and may be subject to outsourcing requirements. The FCA confirmed in PS26/13 that the use of permissionless distributed ledger technology should not be treated as outsourcing under SYSC 8.[10] The guidance should reflect this distinction consistently, while making clear that firms remain

[6] Bitbo, "Bitcoin Uptime Tracker", accessed October 2026
[7] Bitcoin Wiki, "CVE-2010-5139: Value overflow incident".
[8] Gavin Andresen, "BIP 50: March 2013 Chain Fork Post-Mortem", 20 March 2013.
[9] Bitcoin Core, "Disclosure of CVE-2018-17144", 20 September 2018.
[10] Financial Conduct Authority, PS26/13, Application of the FCA Handbook for Regulated Cryptoasset Activities, 30 June 2026.

responsible for assessing network dependencies, preparing for disruption and managing the resilience of their own services.

Recommendation 2: *Clarify that the use of a permissionless blockchain does not constitute outsourcing under SYSC 8, while retaining firms' responsibilities under SYSC 15A and applicable requirements for commercial service providers.*

Testing what a firm cannot control. Paragraph 3.40 recognises that firms have limited control over decentralised networks. Scenario testing should therefore assess how a firm would respond to network disruption, including whether it can suspend deposits and withdrawals, adjust confirmation requirements, communicate with customers and continue operating within its impact tolerances. The guidance should also recognise differences in network design. Bitcoin targets an average block interval of ten minutes, although individual blocks may take considerably longer.[11] Normal variations in confirmation times should not automatically be treated as network failures.

Recommendation 3: *The FCA should provide an example of scenario testing for a firm using a permissionless blockchain, focusing on the measures within the firm's control and how it would maintain its services during a network disruption.*

Independent verification and transaction confirmations. Firms using Bitcoin can reduce their reliance on external infrastructure by operating their own full nodes. These independently verify transactions and blocks against Bitcoin's consensus rules, rather than relying solely on information supplied by a commercial node provider.[12] This supports the FCA's emphasis on independent verification in paragraph 3.29. Firms should also adopt confirmation policies appropriate to the value and risk of each transaction. Bitcoin transactions become progressively harder to reverse as additional blocks are added, but no fixed number of confirmations guarantees finality. The 2013 chain split demonstrates why firms should consider the possibility of a temporary reorganisation when assessing settlement risk.

Recommendation 4: *The FCA should recognise independent node operation and proportionate confirmation policies as practical measures firms can take to reduce operational dependencies and manage settlement risk.*

A Bitcoin only worked example. The FCA's existing examples focus on firms with exposure to DeFi protocols and associated infrastructure. A contrasting example would help demonstrate how operational risks differ when firms use simpler blockchain arrangements. Consider Firm C, a regulated business providing Bitcoin custody and exchange services, settling transactions directly on Bitcoin's base layer without using smart contracts, bridges or oracles. Its operational assessment would focus on its own nodes, wallet infrastructure, private key management, banking partners and transaction settlement procedures. Scenario testing could include a temporary chain split, unusually high network fees or delays in transaction confirmation.

This example would not imply that ordinary Bitcoin custody and exchange activities constitute DeFi. It would demonstrate how a firm subject to applicable operational resilience requirements can assess its actual dependencies without attributing risks to technologies it does not use.

Recommendation 5: *The FCA should include a contrasting Bitcoin example to illustrate how firms can assess operational risks according to the networks, services and technologies they use, while making clear that activities outside DeFi remain subject to their applicable regulatory requirements.*

---

[11] Bitcoin Developer Guide, "Payment Processing", section on confirmations.
[12] Bitcoin.org, Running a Full Node, section "What Is a Full Node?"

Question 3: Do you agree with our description of the financial crime risks that may arise when firms provide financial services using DeFi? If not, please explain why.

BPUK agrees that DeFi can present significant financial crime risks, but the guidance should distinguish between technologies with different levels of transparency and traceability. We recommend four clarifications to help firms assess these risks accurately.

Transparency differs between networks. Bitcoin records transactions on a public ledger, allowing investigators to examine the movement of funds between addresses. However, identifying the people behind those transactions often requires additional information. Other networks are designed differently. Monero uses privacy features to conceal transaction amounts, senders and recipients, making conventional blockchain tracing considerably more difficult. Its Ring Confidential Transactions technology, which hides transaction amounts, became mandatory in September 2017.[13] Paragraph 4.10 groups privacy coins with mixers and bridges as methods of concealing transactions. The guidance should distinguish between these technologies and recognise that the ability to trace funds varies according to the network and services involved.

Tracing funds is not the same as identifying people. Bitcoin's public ledger allows investigators to follow transactions, but connecting a wallet address to an individual generally requires information obtained from other sources. The investigation into Zhimin Qian demonstrates how blockchain tracing can work alongside financial checks and conventional policing. Attempts to purchase expensive London properties were obstructed by questions about the source of the Bitcoin. According to the Crown Prosecution Service, investigators subsequently traced a £1.5 million transaction from a previously inactive cryptocurrency wallet to an address in York, where Qian was arrested. Police surveillance of her associate, Seng Hok Ling, also helped establish her whereabouts.[14]

Qian was sentenced to 11 years and eight months in November 2025, following an investigation that resulted in the seizure of more than 60,000 Bitcoin. The case illustrates how public blockchain records can assist investigators when combined with information gathered through regulated businesses and law enforcement.

Risk is not evenly spread across assets. Reliable estimates of illicit cryptoasset activity remain difficult to establish. Blockchain analytics depend on identifying addresses associated with criminal behaviour, while transactions involving unidentified addresses may fall outside those assessments. Different methodologies can produce significantly different estimates, making headline figures an unreliable basis for regulation without careful examination of their underlying assumptions.[15]

The FCA should assess financial crime risks according to the characteristics of individual assets, the services firms provide and the activities involved. Where quantitative estimates are used, their methodology, limitations and evidential basis should be transparent. Firms should not be expected to treat all cryptoassets as presenting identical risks simply because they use blockchain technology.

Tornado Cash sanctions status. Case Study 4 describes Tornado Cash as an entity designated by the US Office of Foreign Assets Control (OFAC). Although Tornado Cash was sanctioned in August 2022, the US Treasury removed it from the sanctions list on 21 March 2025.[16] The FCA should update Case Study

[13] The Monero Project, "Moneropedia: Ring CT", explaining the introduction and mandatory use of Ring Confidential Transactions.
[14] Crown Prosecution Service, "How we prosecuted Europe's biggest crypto money laundering case", case study.
Crown Prosecution Service, "Two people imprisoned for their key roles in a largescale money laundering case"11 November 2025.
[15] Basel Institute on Governance, *Assessing national risks related to virtual assets*, Basel AML Index, 8 December 2025.
[16] US Department of the Treasury, Office of Foreign Assets Control, "Cyber-related Designation Removal; North Korea Designation Update and Removal", 21 March 2025.

4 to reflect this change. The historical use of Tornado Cash in money laundering investigations remains relevant, but the guidance should accurately distinguish past sanctions from current restrictions.

Question 4: Do you agree with our proposed guidance on how firms should assess and manage those financial crime risks? Are there other risks or emerging practices we should consider?

BPUK supports the FCA's guidance on financial crime risk assessments, monitoring and suspicious activity reporting. However, two areas require greater precision.

Noncustodial wallets. Paragraphs 4.8 and 4.27 identify the potential use of noncustodial wallets to avoid Money Laundering Regulations (MLR) controls. While this risk exists, holding Bitcoin in a personal wallet is a legitimate practice that gives individuals direct control over their assets. Regulation 64G of the Money Laundering Regulations allows firms to request additional information about transfers involving unhosted wallets, but requires them to consider the risks associated with the transfer when deciding whether to do so.[17] The use of a personal wallet should not justify treating a customer or transaction as high risk.

Recommendation 6: *The FCA should clarify that transfers involving noncustodial wallets require an assessment of the actual risks involved, rather than an automatic presumption of heightened risk or routine collection of additional personal information.*

Privacy technologies. Paragraph 4.19 identifies the use of privacy technologies as a potential financial crime risk without adequately distinguishing their legitimate use from evidence of criminal activity. Financial privacy is a legitimate interest, and individuals should not be regarded as suspicious simply because they choose to protect their transactions from public scrutiny. Bitcoin's original whitepaper recommends using a new key pair for each transaction to reduce the ability to link transactions to an individual.[18] Fresh Bitcoin addresses, Lightning payments and other technologies that enhance privacy can serve legitimate purposes. The deliberate use of such technologies does not establish criminal intent.

The ability to conceal transaction information may be relevant to a firm's risk assessment, but it should be considered alongside other evidence and the circumstances of the transaction. Customers should not have to surrender their financial privacy merely to demonstrate that they have nothing to hide.

Recommendation 7: The FCA should clarify that the use of privacy technologies, including those deliberately designed to obscure transaction details, is not inherently suspicious. Firms should assess financial crime risks using relevant evidence and context, rather than treating a customer's decision to protect their financial privacy as an indicator of wrongdoing.

Question 5: Are there other risks or emerging practices related to DeFi which we should consider?

The security of customer data. The FCA's guidance addresses financial crime controls but gives insufficient attention to the risks created when firms collect and retain information linking customers to their cryptocurrency wallets. Such records can expose individuals to fraud, targeted theft and physical harm if compromised.

Bitcoin's public ledger makes these risks particularly serious. When someone's identity is linked to a Bitcoin address, anyone with access to that information may be able to examine associated transactions and identify holdings. As BPUK highlighted in its January 2025 commentary on the Cryptoasset Reporting

[17] The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, Regulation 64G, Requesting information: unhosted wallet transfers and cryptoasset businesses.
[18] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, Section 10, “Privacy”.

Framework,[19] collecting more information can create additional security risks for the people regulation is intended to protect. Unlike funds held in a conventional bank account, Bitcoin transferred to an attacker cannot ordinarily be recalled or frozen by a financial intermediary. Firms should therefore consider the consequences of exposing customer identity and wallet information, alongside their obligations to collect and retain it.

The risks are documented. In May 2025, Coinbase disclosed that criminals had paid customer support contractors or employees to obtain personal information from its internal systems. The compromised records included names, addresses, identity documents, account balances and transaction histories. Coinbase said it would reimburse eligible customers who were tricked into transferring funds as a direct result of the breach.[20]

Research published in 2024 by the University of Cambridge and University College London also documented physical attacks against cryptocurrency holders, including threats, kidnapping and violence. The researchers found that these attacks were underreported and warned that Know Your Customer requirements can create security risks alongside their intended benefits.[21] The Coinbase incident demonstrates the consequences of collecting sensitive financial information without sufficient safeguards. The academic research establishes that physical attacks against cryptocurrency holders are a concern, although it does not establish that these attacks generally originate from data breaches.

Recommendation 8: The FCA should provide explicit guidance on protecting customer information that links identities to wallet addresses, transactions and holdings. Firms should:

(a) collect only the personal information necessary to meet their legal obligations and respond to identified risks, consistent with the data minimisation principle in UK GDPR;[22]

(b) restrict and monitor access to records linking customer identities with cryptocurrency holdings, including access by contractors and external service providers;

(c) protect these records through appropriate security measures, including encryption, and delete personal information when the applicable retention period expires, subject to legal exceptions; and

(d) include the theft or unauthorised disclosure of customer identity and wallet information in their scenario testing, recognising the potential consequences for customers' physical safety.

These measures would help firms meet existing obligations while addressing the particular risks associated with identifiable cryptocurrency holdings. BPUK will raise the separate question of statutory data retention periods with HM Treasury.

BPUK also questions whether existing requirements to collect and retain personal information are proportionate to the risks they seek to address. Compliance with current law does not remove the need to examine whether those obligations expose individuals to unnecessary risks of fraud, theft or physical harm.

The FCA should consider these consequences when developing its guidance and identify where existing requirements may warrant review. BPUK recommends that HM Treasury reassess the necessity and

[19] Bitcoin Policy UK, *Commentary on the Cryptoasset Reporting Framework*, 16 January 2025.
[20] Coinbase Global Inc., Form 8-K, Material Cybersecurity Incident, filed 15 May 2025.
[21] Ordekian, M., Atondo-Siu, G., Hutchings, A. and Vasek, M., Investigating Wrench Attacks: Physical Attacks Targeting Cryptocurrency Users, Advances in Financial Technologies, 2024.
[22] UK General Data Protection Regulation, Article 5(1)(c), Data minimisation.
The Money Laundering Regulations 2017, Regulation 40, Record keeping.

proportionality of customer data collection and retention obligations, particularly where they link identifiable individuals to cryptocurrency holdings and transaction histories.

BPUK's Privacy Toolkit. BPUK's Privacy Toolkit provides practical guidance on protecting financial information and using Bitcoin privately, including personal wallets and direct transactions between individuals.[23] These are legitimate activities, and choosing to protect financial privacy should not create a presumption of wrongdoing. The Toolkit also encourages people to consider their personal security. Research by the University of Cambridge and University College London found that 25% of the physical attacks examined in their study occurred during transactions between individuals.[24] This reinforces the need for appropriate precautions when trading in person, without suggesting that such transactions are inherently suspicious.

BPUK supports compliance with existing legal obligations while questioning whether current requirements to collect and retain personal information are proportionate. Regulation should protect individuals from financial crime without unnecessarily increasing their exposure to theft, surveillance or physical harm.

Proportionality for smaller firms. Paragraph 1.10 states that the guidance clarifies existing requirements and therefore does not require a cost benefit analysis. However, the way firms interpret regulatory guidance can affect their compliance costs, particularly smaller businesses with limited resources. A firm using Bitcoin's base layer without exposure to lending protocols, bridges or oracles should not be expected to undertake the same assessments as a business operating across multiple DeFi protocols. Regulatory expectations should reflect the services firms provide, the technology they use and the risks they can control. Firm size may affect the resources available, but should not replace an assessment of actual risk.

Recommendation 9: *The FCA should clarify that operational resilience and financial crime expectations must be proportionate to a firm's activities, scale and technological exposure. Guidance intended to address complex DeFi arrangements should not impose unnecessary compliance burdens on firms that do not use those technologies.*

Question 6: Are there other steps that could be taken to reduce financial crime risks in DeFi? Are there other regulatory measures that we should consider to reduce the financial crime risks in DeFi?

Financial crime controls should focus on businesses providing regulated financial services, including exchanges and custodians. These businesses can identify customers, monitor transactions and respond to suspicious activity. Independent developers, node operators and miners do not necessarily have the same access to information or control over customer transactions.

We do not support extending financial crime obligations to independent software developers, Bitcoin node operators, miners or providers of personal wallet software merely because their technology can be used to transfer or hold Bitcoin. Regulatory obligations should reflect the activities undertaken and the control exercised, consistent with our response to CP26/36. The FCA should distinguish the provision of technology from the operation of a regulated financial service. Any additional measures should also be assessed for their impact on financial privacy and personal security. Requirements to collect or retain customer information must be justified by evidence and accompanied by appropriate safeguards, as discussed under Question 5.

---

[23] Bitcoin Policy UK, Privacy Toolkit, updated 20 June 2026.

[24] Marilyne Ordekian, $5 Wrench Attacks: When Cryptocurrency Crime Get Physical, University College London, 22 July 2025.

Conclusion

The FCA's proposed guidance would benefit from clearer distinctions between the risks associated with different blockchain networks, the services built on them and the responsibilities of regulated firms.

Our recommendations aim to ensure that regulation reflects the technologies firms use and the risks they can control. They also address the security consequences of collecting information that connects individuals to their cryptocurrency holdings. Financial crime prevention should not come at the expense of legitimate financial privacy or expose customers to unnecessary physical risks.

These changes would help firms apply the guidance proportionately while maintaining appropriate consumer protections. Bitcoin Policy UK would welcome further engagement with the FCA on these recommendations.

Submitted by the Bitcoin Policy UK Team
71-75 Shelton Street, Covent Garden, London, United Kingdom, WC2H 9JQ
Company number 14743706
contact@bitcoinpolicy.uk
https://www.bitcoinpolicy.uk/

END OF DOCUMENT