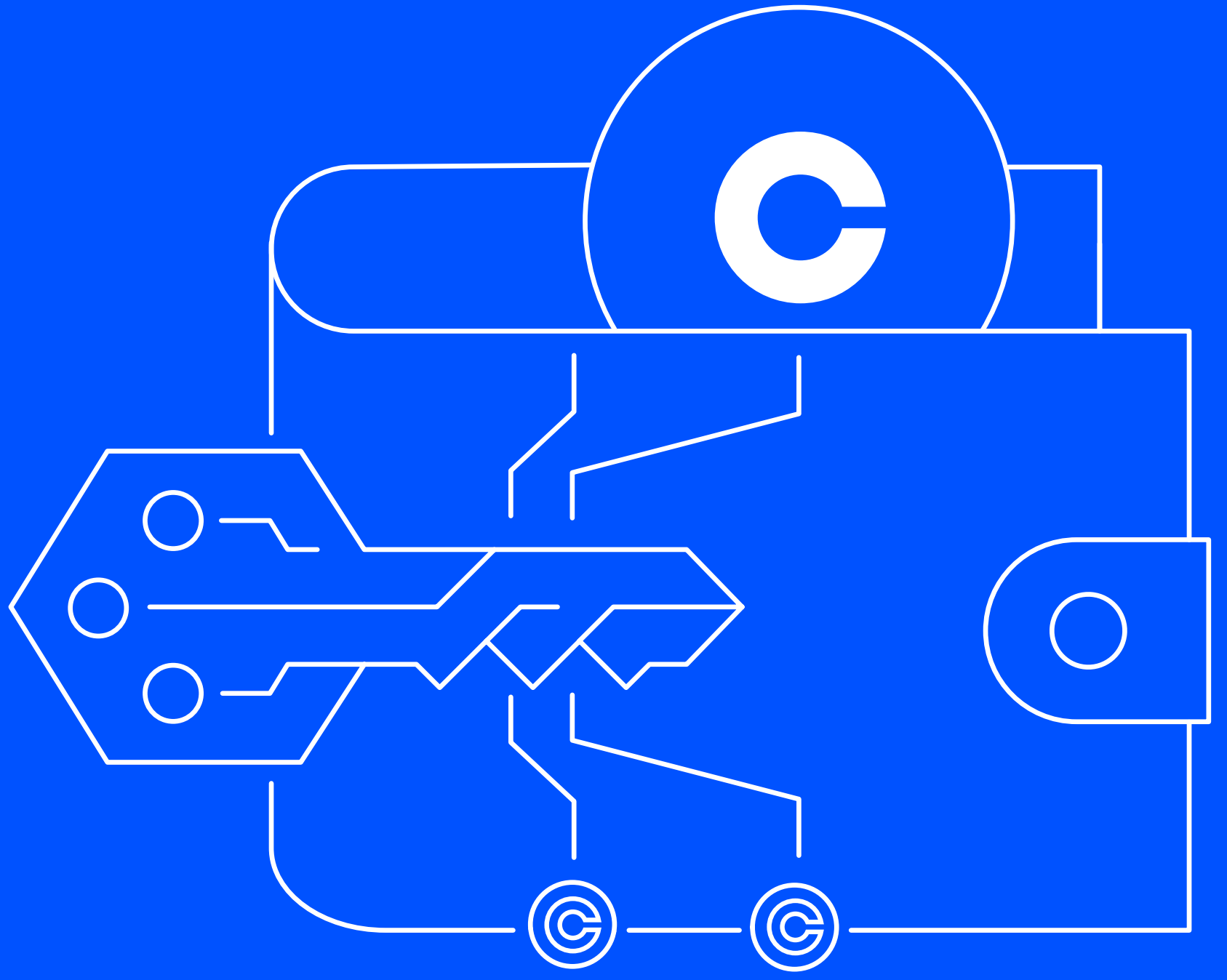
2026 Q3

coinbase **INDEPENDENT ADVISORY BOARD** ON QUANTUM COMPUTING AND BLOCKCHAIN

Post-Quantum Migration and Abandoned Coins

Authored by the **Coinbase Independent Advisory Board on Quantum Computing and Blockchain**



Date of publication: June 2026

Post-Quantum Migration and Abandoned Coins

Prof. Scott Aaronson
(UT Austin),

Prof. Dan Boneh
(Stanford),

Justin Drake
(Ethereum Foundation),

Prof. Sreeram Kannan
(Eigen Labs and University of Washington),

Prof. Yehuda Lindell
(Coinbase and Bar-Ilan University),

Prof. Dahlia Malkhi
(UCSB)

As we outlined in our **position paper,** quantum computers are not a threat to blockchains today. However, exact timelines are unknown, and we believe that the debate should not revolve around predictions as to when they will be. Rather, the blockchain community needs to take action to begin preparing for a post-quantum reality, and that preparation should begin now.

There are two very different questions that need to be addressed to ready a blockchain for a post-quantum reality. The first is a purely technological question, and that is how to migrate so that all cryptography is post-quantum secure. There are technical challenges with this, primarily due to public-key and signature sizes, and these are discussed in detail in the aforementioned position paper. The second is a governance question – what do we do with coins that are abandoned, and not transferred to new post-quantum addresses? In this blog, we will discuss this dilemma in depth.

Background

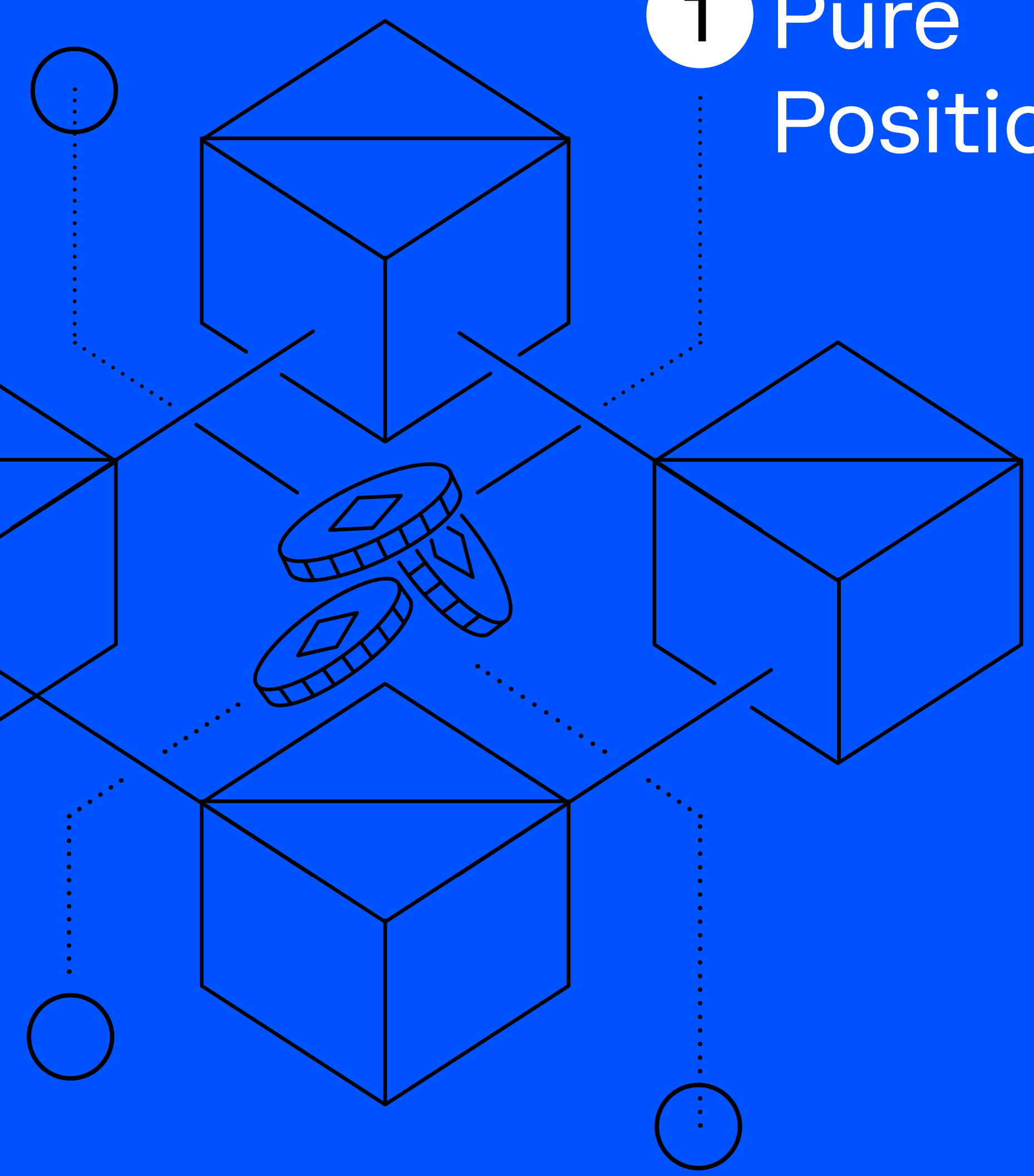
Before presenting the positions, we will provide some background, specifically as it relates to Bitcoin.

Although this is a question that all blockchains will need to address, it is particularly significant for Bitcoin given the large number of coins for which the existence of an owner is unclear (a.k.a., the Satoshi coins). In more detail, in the early days of Bitcoin, addresses were of the type P2PK – pay to public key – where the public-key itself is the address. These coins are all vulnerable to a cryptographically-relevant quantum computer (CRQC) since public keys are exposed. There are approximately 1.7 million Bitcoin spread across about 20,000 public keys that are of this form. Many if not most of these are assumed to belong to Satoshi (whose status is of course unknown) and to owners who have lost their keys.

There is no way to confirm exactly how many of these have active owners or not (we do know of some tens of thousands of Bitcoin whose owners have declared losing their keys, or whose keys have been intentionally destroyed, but this is just a drop in the ocean). In contrast to P2PK outputs, P2PKH outputs commit to a hash of the public key. If the corresponding public key has never been revealed, the coins are not directly vulnerable to Shor-style quantum attacks, because an attacker would first need to find a public key matching the hash. This does assume that the public key was not revealed in some other way, which would not be unusual since public keys are in general treated as public. In any case, once a P2PKH output is spent, the public key is revealed, and any remaining or future coins sent to the same public-key hash are then blatantly vulnerable to a quantum attacker. In addition to the above, there are other address types with exposed public keys in Bitcoin, like Taproot. According to Project11, the number of bitcoins that are vulnerable due to address reuse is currently about 5 million.

Most of these are assumed to belong to active users and are not lost. (Again, this is conjecture and there is no way to actually measure it. However, large numbers belong to large cold wallets belonging to known exchanges, or have seen recent activity. For these the assumption is well grounded.) The discussion below is relevant for all blockchains, but we will focus on Bitcoin. The reason for this is a combination of it being the largest crypto-asset, and the significant number of bitcoins that are assumed to be lost and vulnerable.

1 Pure Positions



1: Pure Positions- Burn Vulnerable Coins or Do Nothing

Position 1 – burn abandoned assets at a determined deadline:

After a blockchain transitions to enable post-quantum signatures, a deadline can be given with the statement that after that deadline quantum-vulnerable signatures (e.g., ECDSA/EdDSA/Schnorr) will no longer be accepted. This means that all address owners who do nothing until the deadline will permanently lose all assets under those addresses.

The primary technical argument for this position is that blockchains are like all other cryptographic systems – when a cryptographic algorithm becomes no longer secure, it is deprecated and replaced. Specifically in this case, the ability to cryptographically sign constitutes a proof of ownership. Once the cryptography is broken, this is no longer the case. Thus, allowing quantum-derived private keys to spend abandoned coins would effectively transfer value to entities that were never the legitimate owners. It is also important to note that asset owners are given a long window of time to move their coins; if they do not, then it is reasonable to assume that they have been abandoned.

Another argument in favor of burning abandoned assets is to prevent a sanctioned state actor (like the DPRK) from obtaining very large amounts of bitcoin, potentially tainting market confidence, creating sanctions-compliance problems, and undermining Bitcoin's legitimacy as a global currency.

From an economics perspective, a large number of lost or dormant coins that could be recovered through quantum attacks may cause a large increase in the effective circulating supply of Bitcoin, potentially causing a sharp decline in the price of bitcoin. If such a supply increase were due to legitimate users deciding to sell, that would be fine. However, if it is due to lost coins being retrieved because legacy cryptography has been broken, then this is not a reasonable result for all other bitcoin owners. In that case, the coins are not entering the market because their rightful owners chose to sell; they are entering the market because the old mechanism for proving ownership has failed.

In general, leaving a large number of quantum-vulnerable assets in circulation is a threat to the economic viability of Bitcoin. It threatens legitimate asset owners who have behaved responsibly and moved their assets to post-quantum-safe addresses. This is an important argument: asset owners who have lost their private keys do not need protection, since they have already lost practical control over their coins. The real concern from an ethical-ownership perspective is asset owners who have not lost their private keys, but who nevertheless did not move their coins before the migration deadline.

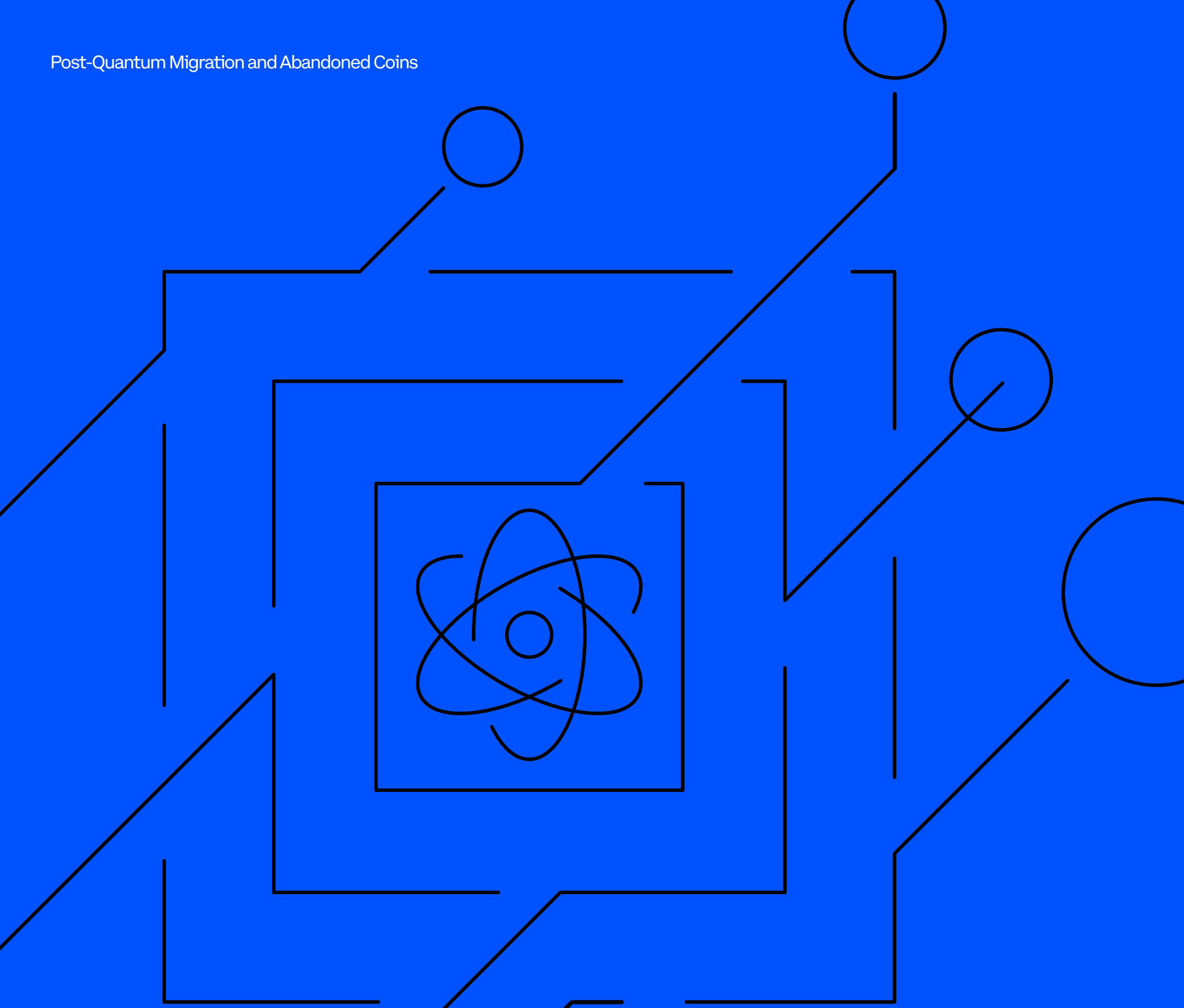
The question is on what basis it is legitimate to effectively deprive those owners of their assets. It is not strictly confiscation, since no one else receives the coins, but the effect is still that the owner loses the ability to spend them. The answer, according to this position, is that entities choosing not to move their assets are not merely taking a risk for themselves. They are endangering all responsible owners who have updated their addresses to be post-quantum safe. Their inaction creates a systemic risk and a negative externality for the rest of the network. As a result, there is a moral basis for saying that, after sufficient notice and a reasonable migration period, entities that do not move their assets should lose the ability to spend them.

Position 2 – enable post-quantum addresses but otherwise do nothing:

According to this position, post-quantum addresses need to be enabled on the blockchain, but nothing else should be done beyond that. If I, as an owner of Bitcoin, wish to take the risk that my funds are stolen by a quantum attacker, then that is my right. The fundamental principle of Bitcoin is that it is not controlled by any single entity, and owners' property rights are absolute. Fundamentally, there is no difference between burning coins and reversing the blockchain if funds have been stolen. There is of course a technical difference: determining if funds are stolen or not requires a process to reach that conclusion, and such processes can never be perfect. However, in principle, it is the same – it is allowing external factors to influence ownership, rather than the rules set down in Bitcoin. Once this precedent is set, does this mean that the network will begin to sanction owners at the network level? Indeed, bitcoins tied to terrorists and criminals have been confiscated in the past. However, this is very different from "confiscating at the network level". But once the Bitcoin network has demonstrated willingness to do this (for post-quantum security), then government and law enforcement pressure to do it again (for other reasons) can increase.

Beyond the above, the question remains as to whether it is "right" to deny asset owners access to their assets. There is no reliable way to determine whether an asset owner has been negligent. They may be unable to transfer their funds to post-quantum addresses – they may be in prison, they may have temporarily lost access to their keys, they may inherit bitcoin but only locate the actual private keys too late, and so on.

Another argument is that everyone understands that burning coins is a radical step. As such, it should be done only when it is absolutely necessary. However, it is impossible to know when that would be. Thus, a weaker variant of the "do nothing" position is "do nothing until a quantum computer actually breaks addresses". There is of course significant risk in that a quantum attacker could already break thousands of addresses and quietly transfer them to post-quantum addresses. In particular, since we cannot unequivocally say which coins are lost and which are just dormant, we may not necessarily know if a quantum attack is taking place. Thus, this position actually means "do nothing until a public quantum computer at a large-enough scale to break elliptic-curve cryptography is demonstrated". This argument is also in response to the argument regarding proof of ownership being broken as a reason to burn coins. This can only be accepted after quantum computers are actually demonstrated to break elliptic-curve cryptography. Until that point, the proof of ownership provided by existing digital signatures is still valid.



2 Intermediate Positions

2: Intermediate Positions

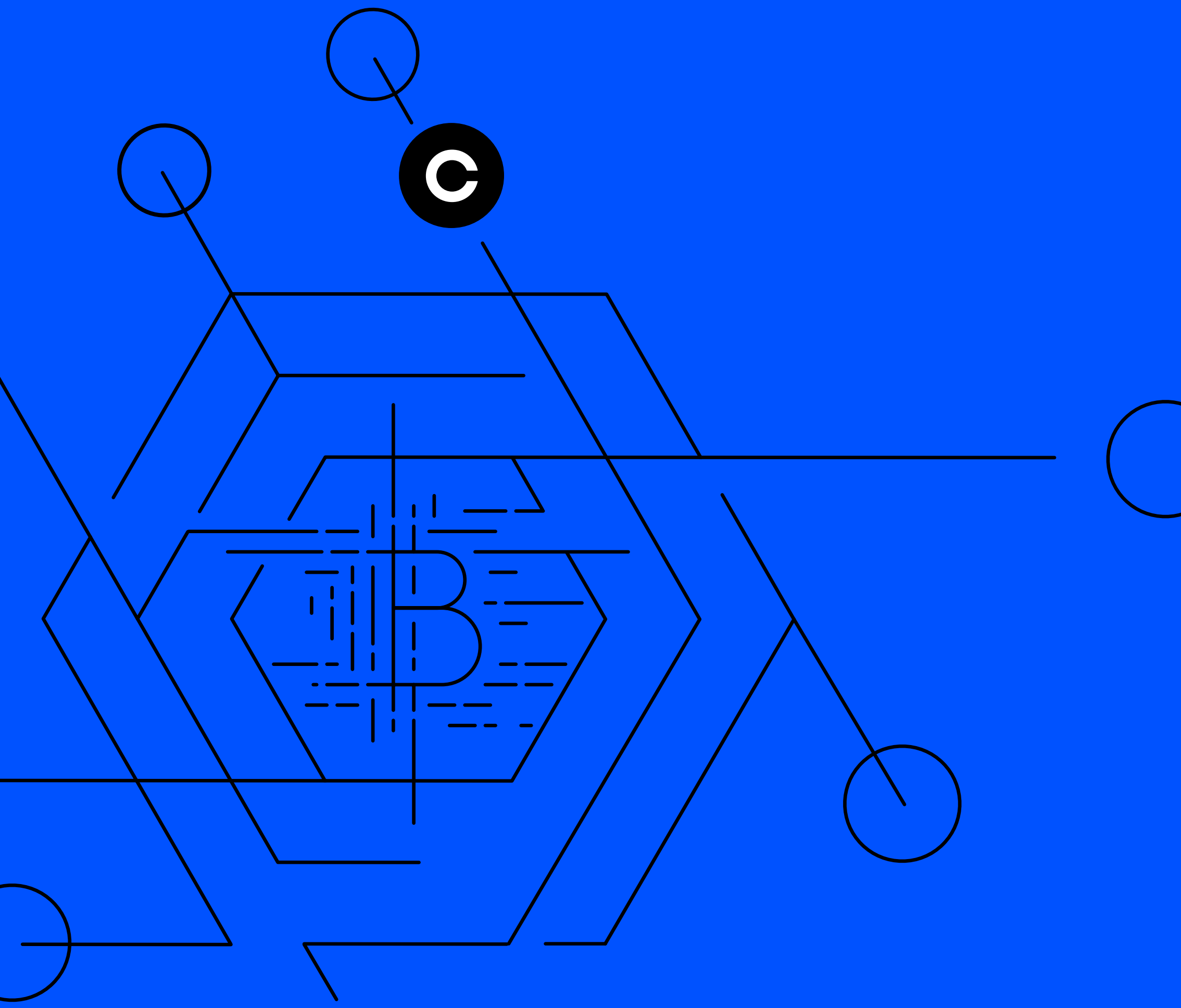
Above, we have described two "pure" positions on abandoned assets - burn them all or do nothing. We have described a possible compromise to the position of "do nothing" which is "do nothing until quantum capabilities are publicly demonstrated". We will now describe other proposals that take intermediate positions that attempt to navigate this challenging question.

1. **The Hourglass proposal:** This proposal limits the number of bitcoin from P2PK addresses that can be spent per block. The aim of this is to address the potential issues that arise with a sharply-increased supply of bitcoins that are made available due to P2PK addresses being broken by a quantum computer. Stated simply, if it is only possible to spend 1 bitcoin per block, then the P2PK addresses – even if broken – will not result in a crash in the price of Bitcoin, since there will not be a supply glut. The other side of this is that unlike the "pure burn" proposal, this does not completely take away a user's ability to obtain their bitcoin back. Under the assumption that the vast majority of P2PK addresses are lost and before quantum computers break P2PK addresses and compete for hourglass spending, legitimate users still holding P2PK addresses will be able to transfer their funds at a reasonable rate.

2. **BIP-361:** This proposal sets a time at which ECDSA/Schnorr will not be allowed anymore. However, after that time, it will still be possible to use a ZK-proof (e.g., a post-quantum SNARK) to prove that you know a hash preimage of the private key. Such a proof is resistant to quantum attacks, since although a CRQC can learn the private key from the public key, it cannot invert the hash to find the hash preimage under the private key. This is relevant for all keys generated from mnemonics, or HD wallet seed phrases as proposed in BIP-32, since keys in this case are generated by hashing a value to get the private key. This means that such users indeed know such a preimage and can provide the required ZK proof. Note that BIP-32 dates back to 2012, and thus earlier P2PK addresses (and likely many addresses after as well) were not generated using a seed phrase, making this solution not relevant for them.

3. **PACTs:** This proposal addresses a different issue, which is that legitimate owners of P2PK or otherwise-vulnerable addresses may not wish to publicly move their bitcoins now (possible because it incurs transaction fees and possibly for other reasons). The idea here is that users can use Bitcoin's timestamp feature in order to generate a hash (commitment) of a transaction generated using a vulnerable key, transferring the funds to a quantum-safe address. This commitment is posted on the Bitcoin blockchain today. Importantly, since this transaction is generated before quantum attacks become feasible, it is valid and can be accepted even when vulnerable ECDSA/Schnorr signatures are no longer allowed. Thus, the user merely needs to open the commitment to the transaction, and the assets are transferred to the given post-quantum address. This method allows users to protect their funds without publicly moving them today. They do, however, need to act and create that commitment before a given deadline.

We stress that the above proposals are compatible with each other; there is no reason to not adopt more than one or all of them, since each has its own advantages.



3

Recommendations

3: Recommendations

We refrain from providing any specific recommendation. Indeed, there is no correct answer here, and the Bitcoin community needs to be the one to decide. Having said that, there are two very clear recommendations that we can make.

Recommendation 1 :

Start technical planning and migration now:

The question of what to do with abandoned assets is objectively hard. However, it is orthogonal to the task of adding support for post-quantum signatures. This technical task should be addressed immediately. Of course, we don't mean migrating tomorrow, since the right way to migrate needs to be studied, researched, and discussed. This is not a decision to run into too fast, without appropriate preparation. Thus, the time to begin this planning is now. Once post-quantum addresses are available, users can decide to begin transitioning their funds, as they wish. In parallel, the community can discuss abandoned assets, but this should not prevent work on post-quantum signing migration.

Recommendation 2:

Clarity:

A serious problem in any economic system is a lack of clarity. The lack of government clarity around cryptocurrency law has been an obstacle to adoption, and fortunately, this is improving. In a similar way, many users are concerned because they don't know what the bitcoin community is planning to do. Is the problem going to be ignored? Is there a timeline by which the community will make a decision? What are the community's plans? This is hard since, by design, the Bitcoin community is distributed and decentralized. Nevertheless, a clear statement by a large portion of the community that this issue is being taken seriously and will be addressed is important to allay users' fears.

Summary

Abandoned assets are a major challenge in any blockchain, but are particularly challenging for Bitcoin.

In this blog we have described the main positions and their rationale, as well as some intermediate proposals that attempt to find some balance. We hope that the discussion around this topic increases, with the aim of finding a resolution that everyone can live with. Irrespective of this topic, we strongly recommend that the technical work to incorporate post-quantum signatures begin now, as this is orthogonal to the more difficult question of abandoned assets. In addition, we recommend that the Bitcoin community – and other blockchains – strive for clarity regarding plans on this topic, so that users' fears that it will go unaddressed are put to rest.