There is a certain (relatively high) probability that quantum computers capable of breaking the elliptic curve digital signature algorithm will be built within our lifetimes. These computers will be capable of deriving the private key from the public key of an ECDSA key pair. In relation to this, virtually every blockchain will struggle with the question of what to do with addresses that have not been migrated to quantum-resistant ones.

The community will face the crucial question of what to (not) do with such addresses. In the past months, I directly contacted many developers and researchers, and unfortunately the vision of what to do in such a situation differed roughly 50/50 between the two main options (described later). After further consideration, I thought it might be beneficial to open such a discussion here. I am not bringing any new proposal to save vulnerable addresses, but I would like to read more arguments for one option or the other. Or maybe someone can present a new choice. I appreciate any response as this might be a systemic risk in the future.

Assumptions for the consensus choice:

- quantum computers with enough physical qubits to crack the discrete algorithm will not be available within this decade
- we will have indications of reaching the scale of a quantum computer that might be capable of breaking the ECDSA a couple of years in advance
- Ethereum will be technically equipped for the post-quantum era on all fronts: quantum-resistant signature mechanisms are available for use in account abstraction wallets, STARKs everywhere, post-quantum secure signature aggregation schemes are implemented, etc.
- secure mechanisms for migrating from quantum-vulnerable addresses to quantum-resistant addresses can be easily used
- the research will show that tens of percents of the entire supply still remain not migrated and vulnerable (in 2019, Pieter Wuille calculated that for BTC approx. 37 % of supply is at risk). For ETH, the number can be similar or maybe even worse (reusing addresses).

What is considered safe

: addresses from which a transaction has never been sent (and the public key has not been revealed on the blockchain), contract addresses with owners (EOAs) who have never sent any transaction (e.g. Safe wallets where we add addresses with no sent txs as the owners).

What can be done

:

1. Do nothing

The easiest way is to do nothing and not touch vulnerable addresses. After a number of years, when QCs have sufficient performance, these addresses will be broken and the owner of such a QC (probably a state/military actor or a large corporation) will get the funds.

no need to make a controversial consensus choice

the fundamental premise of the blockchain remains: whoever presents a valid private key has access to the funds

it will be impossible to know who in fact has spent the funds from a given address (the real owner / quantum adversary?)

in case of insufficient distribution of powerful QCs, a large percentage of ETH supply can fall into the hands of a single entity

the possibility of unexpected inflation if the QC attacker decides to sell

1. Lock them

We can lock/burn/freeze vulnerable addresses. I liked the idea from Justin Drake:

“What is the most palatable way to destroy such coins?”. My strategy (which strives for maximum fairness) would be to setup a cryptoeconomic quantum canary (e.g. a challenge to factor a mid-sized RSA Factoring Challenge composite) which can detect the early presence of semi-scalable quantum computers, ideally a couple years before fully-scalable quantum computers appear. If and when the canary is triggered all old coins which are vulnerable automatically get destroyed. Of course there will be complications and bike shedding around what constitutes a good quantum canary, as well as exactly which coins are quantum vulnerable

vulnerable coins out of circulation

everyone will have enough time to migrate

it is difficult to create the line and distinguish between vulnerable and invulnerable addresses (especially in the account

abstraction world: we assume that in a couple of years most users will be using a smart contract wallet where they choose the spending conditions (including the signature mechanism which could eventually be quantum-resistant but also vulnerable ECDSA)

most activity will be on rollups anyway

2b. Lock them but with a recovery operation

Basically the second method with the following exceptions:

a)

If an address has not been used, it's safe, and if quantum computers come we would be able to make a hard fork that lets you move those funds into a quantum-safe account using a quantum-proof STARK that proves that you have the private key (vbuterin, Reddit - Dive into anything)

b)

We completely ban the use of ECDSA but allow spending coins from addresses with revealed public key if the user presents a ZK proof that the key was derived from the mnemonic seed (we assume the seeds to be quantum resistant as they are "behind" the hash).

we will enable the recovery of the maximum amount of coins

complexity, hard to find consensus for this

TL;DR: having them frozen or having them stolen?