# Quantum computing and Bitcoin



Quantum computers are computers which exploit quantum mechanics to do certain computations far more quickly than traditional computers. A sufficiently large quantum computer would cause some trouble for Bitcoin, though it would certainly not be insurmountable.

*Note that the abbreviation* QC *can stand for either* quantum computer(s) *or* quantum cryptography*.*

## QC attacks

The most dangerous attack by quantum computers is against public-key cryptography. On traditional computers, it takes on the order of $2^{128}$ basic operations to get the Bitcoin private key associated with a Bitcoin public key. This number is so massively large that any attack using traditional computers is completely impractical. However, it is known for sure that it would take a sufficiently large quantum computer on the order of only $128^3$ basic quantum operations to be able to break a Bitcoin key using Shor's Algorithm. This might take some time, especially since the first quantum computers are likely to be extremely slow, but it is still very practical.

For symmetric cryptography, quantum attacks exist, but are less dangerous. Using Grover's Algorithm, the number of operations required to attack a symmetric algorithm is square-rooted. For example, finding some data which hashes to a specific SHA-256 hash requires $2^{256}$ basic operations on a traditional computer, but $2^{128}$ basic quantum operations. Both of these are impractically large. Also, since quantum computers will be massively slower and more expensive than traditional computers for decades after they are invented, quantum attacks against symmetric crypto seem unlikely to be especially common. If quantum computers grow in speed and shrink in price over time, then their inherent per-operation advantage in mining might allow them to out-compete classical computers in Bitcoin mining at some point, probably far in the future; this is comparable to the historic move from CPUs to GPUs to ASICs in Bitcoin's past, and would not be an issue.

### Timeline / plausibility

Creating a quantum computer is a *massive* scientific and engineering challenge. As of 2019, the largest general-purpose quantum computers have fewer than 100 qubits, have impractically-high error rates, and can operate only in lab conditions at temperatures near absolute zero. Attacking Bitcoin keys would require around 1500 qubits. Humanity currently does not have the technology necessary to create a quantum computer large

enough to attack Bitcoin keys. It is not known how quickly this technology will advance; however, cryptography standards such as ECRYPT II tend to say that Bitcoin's 256-bit ECDSA keys are secure until at least 2030-2040.

There is a company called D-Wave which claims to produce quantum computers with over 2000 qubits. However, this claim has not been universally accepted, and even if it is true, this is a *special-purpose* "annealing quantum processor" incapable of attacking crypto.

## Mitigations

Bitcoin already has some built-in quantum resistance. If you only use Bitcoin addresses one time, which has always been the recommended practice, then your ECDSA public key is only ever revealed at the one time that you spend bitcoins sent to each address. A quantum computer would need to be able to break your key in the short time between when your transaction is first sent and when it gets into a block. It will likely be decades after a quantum computer first breaks a Bitcoin key before quantum computers become this fast.

All of the commonly-used public-key algorithms are broken by QC. This includes RSA, DSA, DH, and all forms of elliptic-curve cryptography. Public-key crypto that is secure against QC does exist, however. Currently, Bitcoin experts tend to favor a cryptosystem based on Lamport signatures. Lamport signatures are very fast to compute, but they have two major downsides:

- The signature would be quite large, at least several kB (40-170 times larger than now). This would be very bad for Bitcoin's overall scalability, since bandwidth is one of the main limiting factors to Bitcoin's scaling. Advances in scalability such as Segregated Witness (the signature is part of the witness) and Lightning will be helpful.
- At the time that you create each keypair, you would need to set some finite maximum number of times that you can sign with this key. Signing more than this number of times would be insecure. Increasing the signing limit increases the size of each signature even more. Since you are only really supposed to use addresses once, this may not be a huge problem for Bitcoin.

There is also some ongoing academic research on creating quantum-safe public-key algorithms with many of the same properties as today's public-key algorithms, but this is very experimental. It is not known whether it will end up being possible.

A new public-key algorithm can be added to Bitcoin as a softfork. From the end-user perspective, this would appear as the creation of a new address type, and everyone would need to send their bitcoins to this new address type to achieve quantum security.