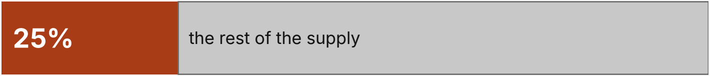
A quarter of all Bitcoin has its public key exposed

Exposed means visible on the blockchain, not currently at risk. Deriving a private key from a public one needs a quantum computer that does not exist. Bitcoin is unusual in that anyone can audit this and count it.



about 4 million BTC, with the public key visible on the chain

Source: Deloitte, Quantum computers and the Bitcoin blockchain. LaMarr Labs, lamarrlabs.com/resources