draft v2, 24 August 2026

FAQ: Bitcoin hard-fork 2026 “Blake2b”

1. **Will I need to update node software on my machine to continue connection with the Bitcoin network?**

   Yes. The current versions of node software (e.g. v29.4 of Bitcoin Knots) are not compatible with the updated protocol so node software update will be required for Bitcoin nodes.

2. **How will I know if my node software requires the update?**

   By checking your node software version, e.g. execute the command: “./bitcoind --version”. Version numbers 29.4 and lower will be obsolete and the future update will be needed. Also the so-called “Bitcoin Core” is obsolete. The new version will be at bitcoinknots.org.

3. **What is the difference between Bitcoin pre- and post- the hard-fork Blake2b? Why is the update needed?**

   The update is needed to improve security of Bitcoin and respond to the disruption caused by the coordinated attack (“98% attack” to indicate the share of the SHA-256d hashpower held by the attacker) carried out by SHA-256d oligarchs since the 8th of August 2026. At the date, SHA-256d oligarchs realized the threat of hampering the Bitcoin chain growth-rate. As a result it dropped from a block per 10 minutes to a block per 2 days (288 times slower). At the same time, the SHA-256d oligarchs launched their own copycat coin (so-called “SHA-256d-coin” or “bPedo” or “Bithereum”), faked the element of decentralization (by naming it “Bitcoin”), introduced an element of trust and central management of their SHA-256d coin.

   Beforehand, the same SHA-256d oligarchs had facilitated spam attacks, exploitation of known vulnerabilities, abused nodes for file store, sponsored troll farms and influencers, run smear campaigns against Bitcoiners to subvert their mission and culture, put the network in jeopardy by unblocking possibility to distribute CSAM instead of protecting the network against variety of threats, neglected cooperation to suspend transfers (i.e. mining certain transactions) of funds stolen/drained from ColdCard wallet victims (a week before the 98% attack, i.e. 30 June 2026).

   There will be hash-power more evenly distributed among independent sources, chain growth-rate will return to the average of a block per 10 minutes and the imminent threats of further disruptions from the SHA-256d hash-power domination attack vector will be avoided after the hard-fork Blake2b.

4. **Why not adjusting the difficulty instead of updating PoW algo?**

   Bad actors still control 98% of SHA-256d hashpower and could manipulate difficulty back higher. At the same time, they could substitute spam for transactions in blocks they mined, effectively blocking throughput of transactions in the network. Also, they could block competition from independent miners by replacing others’ blocks of transactions (chain reorganization).

5. **Will I have a realistic chance to mine a block on my PC like Hal Finney did?**

   Rather not. Personal computers are orders of magnitude less efficient at “mining” in comparison to a specific type of equipment (ASIC).

6. **Why is it insecure to send SHA-256d coins?**

   Sending SHA-256d coins may result in loss of bitcoins. For example, somebody sends SHA-256d coins to an address of exchange on the SHA-256d chain in order to sell them. The transaction details are shared publicly. An attacker could copy them and retransmit them to the Bitcoin thus causing unauthorized transfer of bitcoins (on the Bitcoin chain) to an exchange ("replay attack"). It stems from the fact that both SHA-256d-coin and Bitcoin share the same unlocking mechanisms. There will be a new mechanism ("sighash") unique to Bitcoin added as part of the hard-fork Blake2b.

7. **Will crypto-exchanges like e.g. Coinbase credit my account and allow withdrawals of both SHA-256d-coin and bitcoins?**

   Possible although they haven't made any statement about it yet (as far as I know).

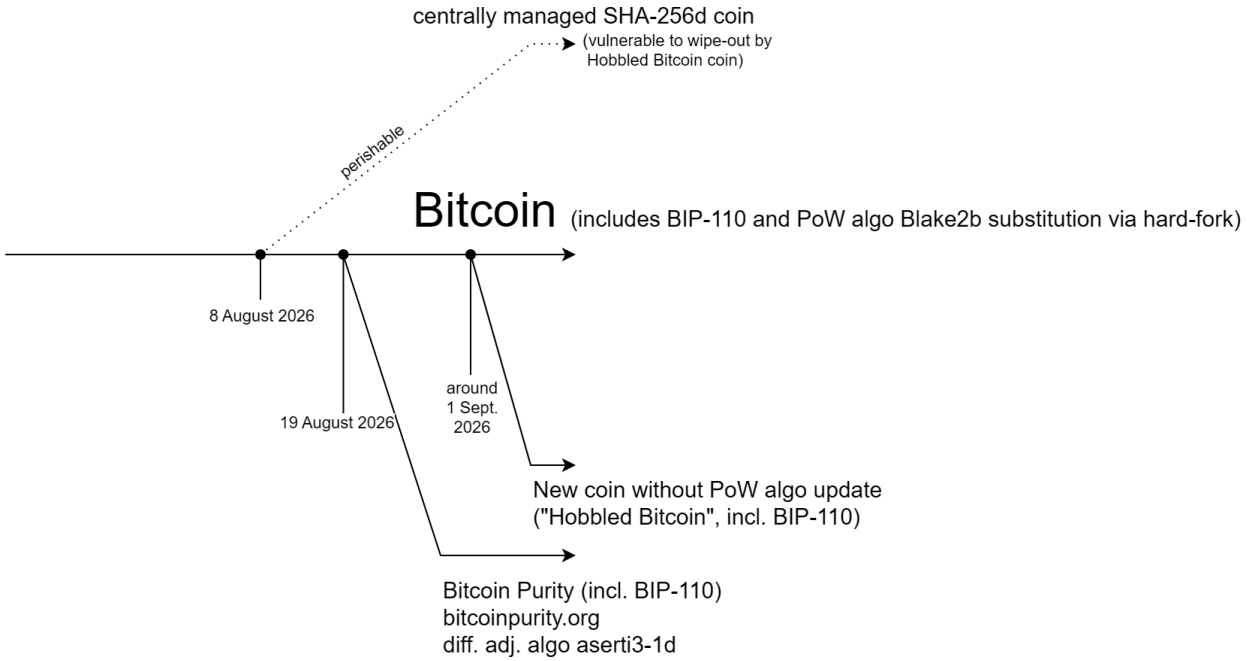
8. **Why should SHA-256d coin not be called Bitcoin?**

   Because Bitcoin is a decentralised system in contrast to SHA-256d coin which is a centrally managed one.

9. **Why did you choose Bitcoin and not SHA-256d-coin or Bithereum?**

   Because I need sound money.

Author: Greg Tonoski <greg.tonoski@gmail.com>.
Appendix: 1) diagram of the Bitcoin hard-fork



2) Visualization of the current status of the Bitcoin chain-tip

Source: mempool.guide