

Bitcoin's Taproot Upgrade Explained

August 19, 2026 · Document #361 · bip39-phrase.com



Photo by [Pierre Borthiry - Peiobty](#) on [Unsplash](#)

Bitcoin's Taproot upgrade, activated in November 2021 at block 709,632, represents the most significant protocol improvement since SegWit in 2017. The upgrade bundles three Bitcoin Improvement Proposals—BIP 340, 341, and 342—that collectively enhance privacy, efficiency, and smart contract functionality on the Bitcoin network.

Enhanced Privacy Through Schnorr Signatures

Taproot introduces Schnorr signatures, replacing Bitcoin's original ECDSA signature scheme for new transaction types. Schnorr signatures enable key aggregation, allowing multiple signers in a multisig transaction to combine their public keys and signatures into single values. This makes complex multisignature transactions indistinguishable from standard single-signature payments on the blockchain. The result is meaningful privacy gains: an observer cannot determine whether a transaction involved one person or a coordinated group, whether it executed a Lightning Network channel close or a simple payment.

Lower Fees and Better Scalability

Schnorr signatures are mathematically smaller and faster to verify than ECDSA signatures. Multisignature and other complex transactions that previously required exposing multiple public keys and signatures on-chain can now present aggregated data, reducing the transaction size by up to 30 percent in some cases. Smaller transactions mean lower fees for users and more transactions per block, improving Bitcoin's overall throughput without changing the block size limit.

MAST and Flexible Smart Contracts

Taproot integrates Merkelized Alternative Script Trees (MAST), a technique that allows a transaction to commit to multiple spending conditions but reveal only the one actually used. Prior to Taproot, all possible spending paths in a script had to be exposed on-chain, even those not executed. With MAST, only the branch taken becomes public, hiding unused conditions and saving block space. This makes complex contracts—such as time-locked inheritances, atomic swaps, or escrow arrangements—cheaper and more private. It also opens design space for more sophisticated applications on Bitcoin's base layer.

Adoption and Long-Term Impact

Taproot adoption has been gradual. As of mid-2023, Taproot-enabled transactions account for a growing but still minority share of Bitcoin activity, as wallets and services integrate support. The upgrade's full impact will unfold over years as developers build applications leveraging its privacy and efficiency properties. Taproot does not introduce radical new functionality, but it refines Bitcoin's existing capabilities in ways that align with the network's goals: preserving user privacy, lowering costs, and enabling flexible scripting without compromising security or decentralization.

[Read more articles: bip39-phrase.com/bitcoins-price-go-up/](https://bip39-phrase.com/bitcoins-price-go-up/)

SEED PHRASE ARCHIVE

The archive section of this document contains 60 generated word sequences illustrating the BIP39 format.

1) head drill earn science gasp immune law snap scrub creek scale crash

— Part 2 of 4 —

SEED PHRASE ARCHIVE

- 2) math foster erosion odor guilt cluster patch absurd shock square feed field
- 3) rabbit giraffe brisk mimic vehicle cool girl accuse picnic yellow material input
- 4) public cute possible degree barrel extra sick surge alert vault isolate credit
- 5) change general radio reduce tiger fatal stay carbon topic dutch pyramid violin
- 6) shrimp gauge marine suffer replace below allow common space slot wolf insect
- 7) shuffle neither whale spoon mimic asthma soul chef post illegal road aerobic
- 8) rally zero bonus machine umbrella void insect glad link coin apple ticket
- 9) there process river print legend law actual swift exist forget riot elbow
- 10) glide spirit school text appear little expose cousin dynamic ancient fiction solve
- 11) agree recipe wreck leaf clinic turtle bunker dutch fruit width upon mercy
- 12) call setup lazy round palace hat sure dentist tobacco quantum smart diary
- 13) rotate stay trophy bachelor original estate dice scatter flame base plastic nerve
- 14) glimpse parade language drum conduct sound east flag depth cereal bachelor captain
- 15) blossom gown rib rain gift end embrace puppy have exist survey only
- 16) property require system jacket library crystal lucky enjoy bike sunset salmon cheap
- 17) story army alarm use treat tongue right work bus birth six federal
- 18) find torch jelly nurse cream stairs proud game shrug naive pact orchard
- 19) off vague marriage learn captain embark ginger great project bounce canal bracket
- 20) help similar jewel wreck define exercise kit genuine elevator crucial shop oblige
- 21) glare lion fragile library execute topple make casino replace pet hood evil
- 22) excuse smile fossil assist chest auto dizzy powder door other level work
- 23) adjust fit garage paddle image sleep gorilla hero thought during violin oblige
- 24) cream juice matter duck cherry upon accident jacket olive rug regular release
- 25) mistake urge mom left print stick payment enrich embrace fan engage vehicle
- 26) crew board joke pill install like poem vocal frost expire matter diesel
- 27) innocent usual settle ticket rich crop slab elegant legal jacket august vendor
- 28) hen vacuum tip tourist tide obscure trash teach much delay hover plunge
- 29) sail heavy scrap space actor thumb cancel flash truth aunt noodle axis
- 30) remind hospital mail bundle nasty pull polar gate hospital jar gauge this
- 31) adapt dirt parent ramp sister theory surface rival wife just actor early
- 32) permit series mass sword load stay wage problem member enjoy profit seed
- 33) measure leaf order figure labor light laptop animal athlete dirt practice card
- 34) make slim dad notice item scale nerve oblige broom subway long swear
- 35) cabbage appear funny quantum attitude glance piano move trash wedding frozen grocery
- 36) problem biology joke impose salt palm flower festival cruel metal sad unaware
- 37) melody cook narrow rich material excite letter choice nest mercy section north
- 38) always kite dice hundred pipe satisfy arena mad era uncle worry injury
- 39) element mind pear joke engine salmon anger reunion sadness noise theory pluck
- 40) other solar focus menu work dentist wine power area advice arch ribbon
- 41) cricket achieve rival cupboard false choose hundred rebel else trip month pyramid
- 42) rack before space old party inquiry rather palm ten artefact april piano
- 43) category flame curious sniff issue bundle author lake host also bottom stairs
- 44) donate ostrich lamp glove piece question saddle cash swallow method ethics virtual
- 45) finger piano strategy hire romance spin box tourist galaxy half flower cage

— Part 3 of 4 —

SEED PHRASE ARCHIVE

- 46) fit soup poet harvest boil illegal road loud wreck siren symptom bid
- 47) method basic zero zebra supply rude neck never account cherry panic sentence
- 48) flee gown banana warfare repeat parrot during sight police cram shoot family
- 49) toast example hospital hint country sand loud must fuel fee seed cage
- 50) good such side jaguar fancy nerve hurry rotate depth cancel reward sugar
- 51) refuse report before soda leg gesture image question social resource expose swamp
- 52) flock ship permit young soccer clerk team funny steak lab answer pretty
- 53) glad transfer desk divert erupt green twice say inhale bomb traffic cancel
- 54) vanish claw offer joy demise lesson cycle chaos unfair later apology access
- 55) mirror prison warfare coach sting float bunker diamond rookie rival orphan advance
- 56) upgrade lottery vintage media rifle donate citizen detect ancient armor pizza ride
- 57) awake float trade rifle sudden spy save issue athlete stairs victory struggle
- 58) sister photo list assault help eight sniff wolf today memory obtain better
- 59) onion corn reunion stadium cook arrow caution finish witness bean travel squeeze
- 60) pudding mad select multiply world tank near among beach embody volcano current

SEE ALSO

- [Bitcoin's Taproot Upgrade Explained — BIP39 Seed Phrases \(August 11, 2026\)](#) (2026-08-11)
- [Bitcoin's Taproot Upgrade Explained — BIP39 Seed Phrases \(June 12, 2026\)](#) (2026-06-12)
- [Accepting Crypto Payments as a Merchant: A Modern Business Move — BIP39 Seed Phrases \(May 30, 2026\)](#) (2026-05-30)
- [Debunking Myths About Bitcoin's Energy Consumption — BIP39 Seed Phrases \(April 01, 2026\)](#) (2026-04-01)

Educational examples only. Randomly generated, not valid wallet phrases - never use them to store funds. Details:

bip39-phrases.com/security/

— Part 4 of 4 —