

# Bitcoin's Taproot Upgrade Explained

September 18, 2026 · Document #390 · [bip39-pharse.com](https://bip39-pharse.com)



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

Bitcoin's Taproot upgrade activated on November 14, 2021, at block height 709,632. It was the most significant change to the Bitcoin protocol since the SegWit upgrade in 2017, bundling three separate Bitcoin Improvement Proposals — BIP 340, BIP 341, and BIP 342 — into a single soft fork.

## What Taproot Actually Changes

At its core, Taproot introduces a new signature scheme called Schnorr signatures, replacing the older ECDSA (Elliptic Curve Digital Signature Algorithm) that Bitcoin had used since its inception. Schnorr signatures are mathematically simpler, slightly smaller in data size, and allow multiple signatures to be aggregated into a single one. This last property is particularly important for multisignature transactions, which previously had to reveal every participating public key on-chain.

Alongside Schnorr, Taproot introduces a new scripting framework called Tapscript and a construction known as MAST — Merkelized Abstract Syntax Trees. MAST allows a transaction to commit to multiple spending conditions simultaneously while only revealing the specific condition that was actually used. A complex smart contract with ten possible outcomes only needs to expose the one path that was executed, not all ten.

## Privacy and Efficiency Gains

The combined effect of these changes is meaningful for both privacy and block space efficiency. Before Taproot, a two-of-three multisig transaction looked visibly different on-chain from a standard single-key payment. After Taproot, both can appear identical from the outside when the cooperative spending path is used. This makes it harder for blockchain analysis firms to distinguish between individual wallets, corporate treasury setups, and Lightning Network channel opens and closes.

For the Lightning Network specifically, Taproot enables a feature called Point Time-Locked Contracts (PTLCs), which replace the older Hash Time-Locked Contracts (HTLCs). PTLCs break the payment correlation that currently allows observers to potentially link the sender and receiver of a routed Lightning payment by spotting the same hash across multiple channel hops.

## Adoption and Limitations

Taproot adoption has been gradual. By mid-2023, roughly 1–2% of Bitcoin transactions were using Taproot outputs, with growth accelerating after the Ordinals protocol began using Taproot's expanded script capacity to inscribe data directly onto individual satoshis. Wallets including Sparrow, BlueWallet, and hardware signers like Coldcard added Taproot support throughout 2022.

The upgrade does not solve Bitcoin's base-layer throughput limitations. Block size remains constrained, and transaction fees still spike during periods of high demand. Taproot also does not enable sophisticated smart contracts comparable to Ethereum's EVM. What it does accomplish is more modest but technically precise: it makes certain complex transactions cheaper, less identifiable, and more flexible without requiring a hard fork or changes to Bitcoin's fundamental consensus rules.

Developers view Taproot as foundational infrastructure for future proposals, including those exploring covenant mechanisms and more expressive scripting capabilities that could expand Bitcoin's utility further.

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

---

## RANDOM MNEMONIC WORD SETS

---

This document continues with 70 machine-generated mnemonic word sequences for study and format reference.

- right grain wheat cushion sting vintage middle stuff entry equip thrive clog
- boss hurt humble avocado drive regret pledge salt salad right essence faculty
- ability walk quiz express plunge abstract armed forget wreck taste comic enough
- pink reflect off ahead pulp denial hire treat famous height cattle adult
- token dad million story marble trial husband gun finger unknown hidden river
- salad miracle reduce foot sail river hill author enroll apology track torch
- balance dog design movie egg obvious dilemma media shadow wedding speak doll
- twice detail drink actor knock village banner nothing festival option chapter domain
- same hawk aunt bachelor shoe zebra fabric icon ocean luxury leg hidden
- company mango awesome call inherit differ rib usage tag genius moment chef
- broccoli core actor picture boy close head cost raccoon outer enact purity
- bounce salon tomato inmate spray maze bamboo female teach pilot must once
- portion glue hunt warfare crisp federal sight coin must hint perfect bless
- valid stove unusual tiny cinnamon hen damage ghost fabric anger skate diagram
- chest voyage hamster law reflect dirt elegant question shuffle damage sleep believe
- talent wire host owner snack pupil income debate master wet close occur
- derive unable puppy general sense crystal absurd gauge fish feed gate grocery
- combine silent bacon focus crisp spring heavy field depth spot news coin
- then speed move style glad priority spirit arrest winter heavy pig slice
- silent long wide creek bless choose rebuild easily dish follow angle long
- antique valve juice lesson rookie violin note motor service toward bubble live
- fall field humor blur fever nature travel empty solve favorite olympic ginger
- deposit fan harsh bid scrap large vintage exit sure charge tower dentist
- tackle odor monster humble federal device buzz desk visit armor film frown
- endorse final fury chronic resource under lounge audit armed nasty mercy torch
- defense draft rabbit wrap ski loop omit praise immune more medal buffalo
- catalog regret matter pizza crunch badge win remove match seat stock verb
- abstract liberty account toy custom script office horror often spread remain iron
- camera venture hawk nothing wheat twelve bronze entire flee power exchange song
- coyote chest impose orchard ability never roof orbit boat laundry loyal deposit
- tree response invite upgrade pattern wire soldier buyer state lecture find music
- together vibrant violin food dinosaur metal mean nature common enable run obvious
- flight price era can room help plug legal wedding neck sure prevent
- matrix thank pole return frozen tree clap penalty useful meadow device staff
- winter labor baby employ garage inspire bubble fitness frozen process true wagon
- rural wild near blade indicate occur kingdom music gas dog seat damp
- fence once security slab glance will seat pluck example exhaust prize hunt
- impact buffalo stay arrow mercy face lunch cricket sock canyon chat intact
- ahead make blast start guilt picnic ripple next keen cabin era found
- solve blush crew firm vapor wool entry lunch apart near use hamster
- wrap immense job general month chair thank steak smart later deputy note
- frown game orbit slide doctor wrestle feel cradle clarify author jelly sugar
- pumpkin extra banner snack whisper jelly silk guide rice jewel viable horror

#390 — 3/4

---

## RANDOM MNEMONIC WORD SETS

---

- stock occur census brave flag hat path champion slush mosquito world muffin
- term liar scan cook skin empty able execute cute hood hub bracket
- eye suit merge shine just mule galaxy need section cross virtual iron
- volcano hair glad cage pledge scatter moment input museum oyster memory recall
- pilot daughter mother enrich state peace assist outside appear remind impact amused
- march kit fish blast inch between alley unusual come divert spot wink
- obvious demise shield unlock order aware army hair guess measure come liar
- check ecology olympic often juice slice party copper path crazy town enrich
- pattern artist middle cup crime nothing olive mesh maze river critic echo
- harbor runway stuff fruit error glory owner fat demand birth explain degree
- first uncover nothing arctic ramp near average toilet candy globe truth notable
- bulk inside blur bone episode welcome habit glass zoo indicate keep turkey
- delay path pattern number goddess castle tragic sibling love wreck spider come
- ranch plate fiction goat maid coffee student wheat ocean repair just tackle
- surround suit boring budget churn twenty mass prosper type bleak ecology labor
- shiver blame tone fly flock penalty jar scene van couple digital twin
- stage dust globe toss depend picture sign very second angry dentist assume
- melody purpose shrug jeans burst reflect naive faculty february dragon dog steak
- major heart trip day about success purse struggle dragon point empty sibling
- vicious run piano march truly duty luggage useless switch again vehicle tooth
- citizen summer earn toilet caution three gift conduct satoshi pony derive opinion
- embody mechanic myth rural clap coach slush open impulse dream choose ladder
- situate swap march stable inner much rack visual destroy olympic find banana
- south alarm patch deliver cabbage decrease effort exile wash witness panic submit
- notable private width remember venue around income infant anger spirit whale anxiety
- they degree cube wing secret month box deny daring fan face alone
- promote blood virus economy history conduct radio lucky quarter prevent skate such

## SEE ALSO

- [Bitcoin's Taproot Upgrade Explained — BIP39 Seed Phrases \(August 19, 2026\)](#) (2026-08-19)
- [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)

Educational examples only. Randomly generated, not valid wallet phrases - never use them to store funds. Details:  
[bip39-phrases.com/security/](https://bip39-phrases.com/security/)  
#390 — 4/4