

Bitcoin's Taproot Upgrade Explained: Schnorr, MAST and Tapscript

October 06, 2026 · Document #406 · bip39-phrased.com

Taproot is a Bitcoin protocol upgrade that activated on November 14, 2021, at block height 709,632. It bundled three Bitcoin Improvement Proposals: BIP 340 for Schnorr signatures, BIP 341 for Taproot outputs, and BIP 342 for Tapscript. Miners signaled support during a three-month Speedy Trial window in 2021 before the rules locked in. It was the network's first major consensus change since SegWit in 2017, and its goal was to make complicated spending conditions cheaper to use and harder to identify.

Schnorr signatures and key aggregation

Before Taproot, Bitcoin used ECDSA signatures. BIP 340 added Schnorr signatures, which rest on a simpler security proof and always produce 64-byte signatures. Their key property is linearity: separate signatures can be added together into one. A 3-of-3 multisig spend under ECDSA publishes three public keys and three signatures. With MuSig-style aggregation, the participants combine their keys into a single public key and produce a single signature. The on-chain footprint becomes identical to an ordinary single-signer payment, so observers cannot learn how many parties had to agree, what threshold applied, or which addresses belong to the same wallet.

Hiding the script with MAST

A Taproot output looks like any other single-key output. The output key is a tweaked version of the participants' aggregated key, and the tweak commits to a Merkle tree of alternative scripts. Spending can then take one of two paths. A key-path spend uses one signature and reveals nothing else; it is the cheapest and most private option. A script-path spend is used when the participants cannot or do not want to sign cooperatively, and it reveals only the executed script plus a short Merkle proof that the script was among those committed to. Unexecuted branches stay hidden, which matters for escrows, timelocks, and Lightning channels where only one of several possible outcomes ever occurs.

Tapscript and what it enables

Tapscript changed the rules underneath these spends. It replaced OP_CHECKMULTISIG with OP_CHECKSIGADD, which fits Schnorr's batch verification, lifted the 10,000-byte limit on standard script size, and made signature validation versioned so new opcodes can be introduced without altering the rules for existing scripts. The practical payoff shows up in Layer 2: cheaper channel opens and closes, point time locked contracts, and Discreet Log Contracts are all easier to build when spending conditions can be hidden. Adoption was gradual, with only a small share of transaction outputs using Taproot in its first year, but wallet and exchange support spread steadily.

A soft fork, with tradeoffs

Taproot was deployed as a soft fork, so it remains backward compatible: nodes that never upgraded still validate Taproot blocks and simply treat those outputs as anyone-can-spend under the old rules. The cost is complexity. Aggregation schemes such as MuSig2 require careful key management and strict nonce handling, and a nonce reused across two signatures leaks the private key outright. Taproot did not change Bitcoin's supply schedule or block size; it reworked how spending conditions are proven, moving the network closer to scripts that are powerful to use and invisible to everyone else.

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

Contents: Article (p.1) -> Seed Phrases (pp.2-4) -> Related Documents (p.5)

SEED PHRASE ARCHIVE

The following pages list 75 example seed phrases assembled from the 2048-word BIP39 dictionary.

1. draw bounce six bar chalk label box gloom toss appear clump tonight
2. lazy anchor rocket until child sponsor cricket switch tribe rally butter priority
3. apple catalog fog major country chair section harsh tilt air start across
4. grass injury unable sauce tooth cry interest receive north imitate popular recall
5. innocent burden enrich twice tired child device object oak favorite female opinion
6. hurry spray whale artwork shrug era tomorrow panel crew rather slim print
7. absurd armed roast decline cruel quarter address skin glare arm output fire
8. receive capable wet flame various news cheap wish discover nature buzz mule
9. fantasy item message winter warfare dinosaur off solve viable prosper come crystal

#406 — 2/5

SEED PHRASE ARCHIVE

10. drill mutual token rug father volume wish post damage tumble business solar
11. crash female illegal charge repeat palm person loud galaxy bird average venture
12. screen tower improve toast thing correct advice gravity flee spare bone winter
13. chicken solution output cliff lonely crop sea grit valve load devote bird
14. spoon evoke fluid ketchup can burger fee pause ship urban lobster oil
15. diesel physical item leopard slender rally inquiry draw whale spawn deposit six
16. cloud tool laundry choice cry local airport post pottery winter struggle cause
17. near nephew vapor civil spirit beauty gown follow hurt negative park age
18. above uncle broom canoe moment inch vivid law lock wrestle margin prosper
19. filter shield already nest spy door until broom citizen april pupil bundle
20. they almost action proud solar antenna rubber index system essence barrel bamboo
21. curve truth find plastic become depart drip surround unit together body pond
22. diesel stereo view truck illegal destroy cook floor runway devote segment inside
23. useful apple drift notable hero blame velvet orient portion breeze humble fame
24. muscle casino decrease empower knock will pool glare vehicle spread flower torch
25. city mistake buzz bless curtain drama shallow equal service shell hen daring
26. survey profit regular wheel fashion board brick ghost fluid motor code caution
27. globe certain two cake suggest hurdle perfect gloom crystal design globe term
28. soldier noise again jealous amused flee target assist weekend tortoise wall air
29. sorry noise annual bomb once rally cage feed employ eagle club trumpet
30. carbon twelve hero second squirrel dust client grocery liar name palm cinnamon
31. strike lumber bid bread device visit spider pudding coast birth any evidence
32. fiber napkin into van street galaxy double cable add produce turkey clip
33. chalk arena devote neck fit earth improve just boss grit detect provide
34. post dream oppose pretty satoshi sure scale hollow slide express planet tell
35. window clip super approve soul stuff gate west fabric priority flag illness
36. ceiling chicken stay hire hat endless garden sting scout genius rely rose
37. token neither oak task flip sting pool acid science ship magic harsh
38. exclude travel romance fox devote ticket donor vacuum various awkward rack toss
39. save region alpha auto excess science merry hurdle couple auto maid pond
40. wise lemon dilemma job tackle scare smoke swamp dove pear artist february

#406 — 3/5

SEED PHRASE ARCHIVE

41. lady behind angle another dizzy bread rapid picnic bean leader coil express
42. potato industry doll plastic region wood follow emotion april pyramid cement raven
43. hospital spread jeans evoke lumber wool purchase rebuild gun able cloud undo
44. laptop volcano seven material boil motion blame honey correct now winner goose
45. kidney keen wife always panic hidden scout wine lava venue brass warrior
46. goat punch relief rhythm girl section limb reject burger nose critic gadget
47. trouble bike gauge aunt boy hand arrange icon bomb piano raven cute
48. rate inquiry harsh lesson man pony distance bicycle flash expire picnic decorate
49. wage stool dutch when field employ barrel dress debate few sting essay
50. leopard cradle stone tortoise wrist broom bonus around reduce head rebel spike
51. coin comfort lion alone edge judge pole obscure inhale horn annual train
52. addict nephew outside eye toe culture solar keen chase sheriff earn balcony
53. ankle case fragile gather rebuild brisk used fault poet fantasy minimum prize
54. rich field olive accuse fury brush rabbit rib eager rebel screen slight
55. purpose trip aspect swamp heart melt private captain floor approve return shield
56. range ghost whale cake audit social stock blush margin village toward tortoise
57. school pulp avoid author color they village slow arm boost head goddess
58. client trash stage shallow often brother answer balcony party path car range
59. spot pact athlete rally belt roast smile empower bracket glove twin sentence
60. cruel fly shuffle copy palace antique supreme filter elder base over tattoo
61. silk reunion oxygen very close sail minimum weasel key record riot conduct
62. embrace zoo lonely second again want seat grid enough gaze march glass
63. tonight congress bone auction crop joy way truly weekend canoe quit dune
64. you segment attract apple much success source loop goddess actress broccoli cactus
65. person spike upper peace convince section attract gain train decorate burden found
66. burger insane matrix unusual forget seat crucial okay rigid bean yellow toe
67. devote clean bicycle negative essay verify all margin burger will receive rigid
68. found vast mask entry lava shiver fiscal grape island gun trade worry
69. town month caution fine clutch spy clown tackle earth glance tortoise happy
70. team ginger detail thunder page sting erupt sad source dry screen used
71. save label bonus cactus clock sunset mercy kite teach between cart famous
72. bomb twice glass tone jazz together disease almost wait join model tip
73. kiwi knife idea patient copy stereo wonder screen fiction limit ball analyst

#406 — 4/5

SEED PHRASE ARCHIVE

74. detail depart rate oxygen miss guard sustain snake snow alcohol promote citizen

75. marine essay pill maple staff ocean promote ethics execute empty pond climb

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 \(September 18, 2026\) \(2026-09-18\)](#)
- [Bitcoin's Taproot Upgrade Explained — BIP39 Seed Phrases \(June 12, 2026\) \(2026-06-12\)](#)

Educational examples only. Randomly generated, not valid wallet phrases - never use them to store funds. Details: bip39-phrases.com/security/
#406 — 5/5