

Bitcoin's Taproot Upgrade Explained

August 11, 2026 · Document #353 · bip39-phrase.com



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

Bitcoin activated its Taproot upgrade at block 709,632 in November 2021, marking the most significant protocol change since SegWit in 2017. The upgrade bundled three Bitcoin Improvement Proposals — BIP340, BIP341, and BIP342 — each addressing distinct limitations in Bitcoin's scripting and signature systems.

Schnorr Signatures Replace ECDSA

At the core of Taproot is the shift from Elliptic Curve Digital Signature Algorithm (ECDSA) to Schnorr signatures, defined in BIP340. Schnorr signatures are mathematically simpler and have a key property: they are linearly composable. This means multiple signatures and public keys can be combined into a single signature that is indistinguishable from a standard single-key signature. For multisignature setups — wallets requiring approval from several parties — this collapses what used to be multiple on-chain signatures into one, reducing transaction size and fees. It also improves privacy, since a 2-of-3 multisig transaction looks identical to a single-party transaction.

Taproot and MAST Merge Script Flexibility with Privacy

BIP341 introduces the Taproot construction itself, combining Pay-to-Public-Key-Hash spending with a Merkelized Abstract Syntax Tree (MAST). MAST allows a transaction to commit to many possible spending conditions — time locks, multisig combinations, hash preimages — without revealing any of them on-chain unless they are actually used. Only the executed branch of the script is published; all other conditions remain private. In practice, if all parties in a contract agree, they can cooperate to spend using the key path, which looks like an ordinary payment and reveals nothing about the underlying contract. The script path is only exposed when cooperation fails, making complex smart contracts significantly cheaper and more private in the cooperative case.

Tapscript Updates the Scripting Language

BIP342 defines Tapscript, a revised version of Bitcoin Script designed for use in the script-path spending introduced by BIP341. Tapscript replaces the old OP_CHECKMULTISIG opcode with OP_CHECKSIGADD, which works cleanly with Schnorr's batch verification properties and removes the off-by-one quirk in the legacy opcode. It also introduces a new upgrade mechanism: leaf versions within the Merkle tree allow future script types to be added without requiring another network-wide soft fork for each change. This makes the scripting layer more forward-compatible than it was before Taproot.

Practical Impact on Bitcoin's Ecosystem

Taproot's immediate benefits are clearest in Lightning Network channels and complex custody arrangements. Lightning channels can now use Taproot outputs, making them indistinguishable from ordinary payments when closed cooperatively. Hardware wallet vendors and multisig custody providers began rolling out Taproot support through 2022 and 2023. The upgrade does not change Bitcoin's supply schedule or consensus rules around block rewards, but it lays groundwork for more expressive contracts, potentially including rollup-style constructions that researchers have explored as Layer 2 scaling paths. Wallet adoption has grown steadily, with Taproot output usage exceeding 50% of all Bitcoin transactions on several days in 2024.

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

Contents: Article (p.1) -> Seed Phrases (pp.2-5) -> Related Documents (p.6)

CRYPTOGRAPHIC SEED PHRASES

For reference, 90 sample BIP39-style phrases are printed below, each combining 12 words from the standard list.

1. collect hidden harvest east track wrap maximum poverty ritual clap trophy universe
2. bubble sing intact clock salmon shock team exclude improve inspire note link
3. tennis picnic must prevent want vault reform captain year segment island weapon
4. profit flavor breeze core saddle energy trim series matrix chaos risk invest
5. virtual myth creek stereo salad kite diary fade endless fox remind wing
6. error congress scrap bunker author blame quality bean impact vehicle abandon stamp
7. bright merge panther quantum edit arch price curtain valley street lava yellow
8. scout donate cabbage soul acoustic goddess skin evidence ride soda horror bulk
9. disorder spatial grocery amateur fringe stove alien kit vacant potato hamster color
10. shove roast fiction roof midnight radar duty grocery dynamic permit flip myself
11. hazard trumpet marine found normal smart clean tackle food own vacant raise
12. wrestle major mom claim visa rabbit local saddle horn season way uphold
13. expose shine cart valid fit say tired napkin tip clinic frog wall
14. capital elite stomach recall morning mixed raise success cloth dinosaur come rubber
15. debris someone naive subway thought essay tower join size desert boat demise
16. exhaust pause buyer boil language pledge cheap parent flee practice jealous arch
17. muscle gospel nerve million stay basket alpha thrive circle slogan water under
18. wild occur festival spin onion jacket happy make busy radar volume then
19. rookie undo outdoor surround stem idea equal duty unknown orange ten short
20. board infant water custom unfold make first sea clock gasp turn glance
21. puppy loud assist aspect truth fit veteran eyebrow kick slight easily buzz
22. weekend entire ready frame vessel audit pony you liar essay flush sibling
23. cream logic sunset undo public sphere now thrive enforce ramp toast universe
24. satoshi already salon word iron obscure sail online sunny quiz double feature
25. web moon nominee crane curious sound false call joy master random math
26. parade lumber clap jewel quarter regret awesome peasant expand slush acquire dismiss
27. play host brother remind try drum select winter project code smooth dove

— Part 3 of 6 —

CRYPTOGRAPHIC SEED PHRASES

28. miss december casual error syrup inflict infant barrel ancient swarm winter stereo
29. shuffle license stairs fury scorpion render puzzle shed climb panic aim act
30. glass weekend switch inside cactus install sell remind elegant candy giant resource
31. blind right echo thought much stove tower inner adapt cheap stock laundry
32. blade crawl lounge arrive unknown approve ceiling practice exclude dilemma project sell
33. cancel ceiling nothing damp trip scatter senior bitter blade seed solid dumb
34. crush olympic ask share slot scatter suspect decline real almost abstract have
35. lawn frame cream rabbit crack lens media coast live trust canoe program
36. custom mass debate east member salmon monster must whip figure someone august
37. fruit tide come misery refuse surface harvest congress surround review salute beyond
38. salad glove text girl retreat forest deny rebuild ugly mushroom busy dream
39. grace nose express ugly oyster accuse happy table possible face box antenna
40. chef dinosaur chapter turn aisle embrace physical follow enroll fun clog awesome
41. grid fitness permit pride slab rhythm emotion creek crater mimic polar anchor
42. frown symbol neutral cement swear inform side edit doctor immense dinosaur grief
43. unique nose deer actual cloth category orient survey total limb make damage
44. during dash smooth resist letter pilot talk across bus brick icon potato
45. auction marriage clock wrist mouse hire dilemma wealth gesture collect coach pepper
46. dolphin come fit index sight embody nest second chimney night praise month
47. clog fluid apart famous erase blouse exist remind mother asthma cat taste
48. price panic rotate army stereo place surprise grace usual enhance clog select
49. resource volcano avoid village water bleak join metal measure divert address physical
50. inflict upper avoid sphere wheat memory absurd inquiry weasel original number piano
51. olive entire area pudding garage high together girl leaf legal chair lesson
52. pilot element illegal flat menu mammal fantasy stand seminar attitude fire lesson
53. length wool glue milk drum sad iron country boost another magic cradle
54. tone wife silent trumpet wise shove assist cube nerve inside aware region
55. oven wood gas churn oyster put sing bike kiwi federal minute tiger
56. half diary more candy safe display humble brief organ census credit tiny

— Part 4 of 6 —

CRYPTOGRAPHIC SEED PHRASES

57. analyst kangaroo dizzy myself survey earn mosquito tackle wide patrol junior gun
58. spice purity enjoy output rough impose term claw black easily labor prison
59. rapid dove whip atom crucial remain work upon gravity deny foot media
60. corn glue crazy food stage denial demand mandate defy used ritual casual
61. ahead island pistol palace creek carry traffic bullet undo because engine soap
62. boost game auto gift float patch remain sponsor laptop involve tail engine
63. argue pigeon strong guide frost bird stay robot segment strike mesh domain
64. betray burden marine divorce recycle bulk frog save strong census sponsor hungry
65. stomach safe pizza episode smile nose win sleep decide figure brick wedding
66. carbon cable surprise mule enable there ladder car truth echo boat receive
67. lemon caught produce agree shoot retreat rice print army person motion average
68. phrase mosquito stone title domain lend long ranch trumpet course lumber obey
69. grief great payment cross copper domain immense ordinary boost sure pattern tenant
70. pizza analyst expand alley domain entire warrior wealth network such swamp rebuild
71. fancy icon metal purity praise describe invest point spell section cheese margin
72. amazing system romance woman muscle joy village canyon admit retire actor laundry
73. ginger zone wife demise judge pass tongue smart glide elder powder spot
74. phone age unveil obvious knee govern mask name slot genre physical right
75. amateur black pride curtain drift anger safe robot virtual tube solution desk
76. bird fresh final runway describe cost suffer scout dumb shine also armed
77. dose wagon insect mushroom rescue base repair antenna friend cheese tourist aim
78. cloth math ready place mistake harsh make north dinosaur twin slender wasp
79. bean culture remember voyage end beef service bus burden rookie reopen quantum
80. churn cousin begin grunt people consider spoon job motor lawn lizard permit
81. ring occur young illness legend surprise solution share laugh depth choice cool
82. kitten endless quick possible rain office fetch toss snake ski point friend
83. hold exact alien language source person connect angry rally fossil ordinary mean
84. naive knock body lab music sweet empower phrase sun fresh stand exit
85. input bless neglect vacuum produce coyote call frost gold viable ivory leave
86. across pause gloom advice peace pole labor cotton where just drum luxury

— Part 5 of 6 —

CRYPTOGRAPHIC SEED PHRASES

87. hold human saddle wreck devote ranch acid slush dismiss other voyage cycle
88. found obvious run find dignity camera car carpet mule afraid faint loud
89. tube jump rebel raven evidence say leopard month burst treat whisper axis
90. impact security detect grit arch ability upset express grief region visa
similar

SEE ALSO

- [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 \(April 01, 2026\) \(2026-04-01\)](#)
- [Understanding Bitcoin Ordinals and Inscriptions: A New Era for the Blockchain — BIP39 Seed Phrases \(May 26, 2026\) \(2026-05-26\)](#)

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

— Part 6 of 6 —