www.gsr.io
gsr@gsr.io

COTW: What's on Tap for Taproot?

With Bitcoin's biggest upgrade in years set to go live in November, we explore what Taproot means for the network and its users.

- ***Upgrading Bitcoin:*** While Bitcoin has already had a profound impact on the world, its technology is not a finished product, and as such, it continues to evolve and improve. Such improvement is formally encompassed in the Bitcoin Improvement Proposal (BIP) process, where anyone in the world can table proposals to improve the protocol or provide information to the community. BIPs can cover a major change to the network like block size or transaction verification (called Standard BIPs), describe or record general information about the Bitcoin ecosystem such as design issues (Informational BIPs), or propose a change to a process outside the core Bitcoin protocol (Process BIPs). A BIP typically starts with socializing an informal proposal via the Bitcoin development mailing list, chat boards, and messaging apps to solicit feedback and generate support. From there, the author(s) will formally write-up and recirculate the BIP adhering to certain formatting, content, and quality requirements, before submitting to the BIP editor who then rejects or accepts it and posts it to the Bitcoin Core GitHub BIP Repository. The community at large then discusses the proposal, additional changes based on feedback are implemented, and developers write, test, and implement the necessary code. The community then chooses the process for activating a finalized BIP, which can vary, but in general requires a vote with a high threshold of community buy-in. The BIP process is intentionally slow, onerous, and conservative to ensure vast stakeholder support and a successful roll out.
- ***Taproot Overview:*** Proposed in 2018 by Bitcoin Core developer Greg Maxwell, Taproot is a soft fork upgrade to the Bitcoin protocol designed to make transactions more private, secure, and scalable. Taproot is actually composed of three BIPs, Schnorr Signatures (BIP 340), Taproot (BIP 341), and Tapscript (342), with the three collectively referred to as Taproot. At a high level, Taproot integrates smaller and more secure Schnorr digital signatures, introduces a new script type for spending Bitcoin, and updates the opcodes to implement Schnorr signatures and the Pay-to-Taproot script type. Specifically:
    - Schnorr Signatures (BIP 340): As detailed in our in-depth primer How Bitcoin Works, Bitcoin uses a digital signature scheme to prove Bitcoin ownership and allow the network to authenticate transactions. Bitcoin inventor Satoshi Nakamoto chose the Elliptic Curve Digital

Signature Algorithm (ECDSA) as its signature scheme given its security, familiarity, and the fact that it is open source. However, the Schnorr Digital Signature Scheme (SDSS), which was under patent until 2008, has certain security, simplicity, and efficiency benefits compared to ECDSA. For example, the SDSS is theoretically more secure than ECDSA as it is provably secure with fewer assumptions, and is also non-malleable, meaning a signature can't be altered prior to confirmation as is the theoretical case with ECDSA (this could lead to a double spend attack). In addition, Schnorr public keys and signatures are slightly shorter than those of ECDSA, leading to space savings. And perhaps most importantly, unlike the current system where relatively complex transactions such as multisig require multiple public keys and signatures to be validated and stored by the network, SDSS enables public keys and signatures to be aggregated and for just one public key and one signature to be processed by the network. This materially improves computation efficiency, storage, and privacy, as such complex transactions appear on-chain as a normal single-signature transaction.

- Taproot (BIP 341): Bitcoin Script is Bitcoin's simple programming language enabling the processing of transactions. It essentially gives Bitcoin's software, Bitcoin Core, instructions on how coins in an unspent transaction output (UTXO) can be spent, defining the spending conditions under which a transaction is valid. Scripts contain data, such as the digital signature and public key, as well as operation codes (opcodes for short) that are simple commands specifying what operation to perform. Most transactions require simple scripts, such as the Pay-To-Public-Key-Hash (P2PKH) that sends a UTXO to an address (~75% of all Bitcoin transactions are P2PKH), though other transactions such as those enabling multisig or time-locks use more complex scripts.

  Taproot introduces a new script type (i.e., a new way to define spending conditions) called Pay-to-Taproot (P2TR), allowing users to send a UTXO to a Schnorr public key or to the Merkle root of a variety of other scripts. At a high-level, P2TR uses a Merkelized Alternative Script Tree (MAST), which summarizes a large number of possible spending scripts into a Merkle tree. Then, the UTXO can be unlocked and spent by either the owner of the private key or anyone who can satisfy the requirements of any script within the Merkle tree. This allows for the spender to only reveal the script they used (only the satisfied spending condition), rather than all of the scripts (all possible conditions for spending an output), makes the transaction output on the blockchain look the same for all transaction types (single-sig, multisig, time-lock, etc.), and makes many chain analysis heuristics unusable, enhancing privacy and efficiency of the network.

  We show our understanding of Taproot functionality with example spending conditions in **Exhibit 1** below. Here, a UTXO is locked into what appears to be a single public key, but which is actually an aggregation of a simple public key and a MAST-based public key. The UTXO can then be unlocked and spent by publishing a signature for the simple public key or by satisfying any one of the scripts in the MAST. For example, the simple public key can actually be a multisig thanks to Schnorr signature aggregation, while the scripts can allow an individual party to unlock the UTXO by themselves after a certain amount of time has passed. This would allow for the Bitcoin to be unlocked by an individual party after a certain

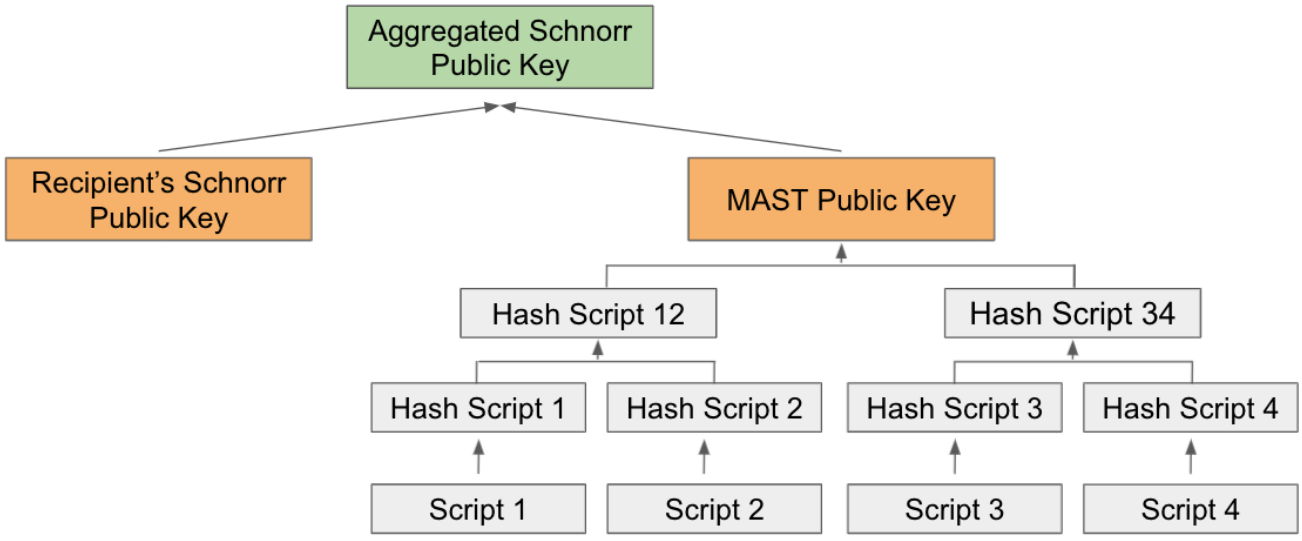
period of time should the multisig users be unable to come to agreement or if some of the associated private keys are lost. Importantly, it's impossible to tell that the simple public key was actually a multisig setup and only the spending condition used to unlock the UTXO is revealed.

- Tapscript (BIP 342): Tapscript implements Taproot by defining the semantics of the initial scripting system under BIP 341. To do so, it adjusts several existing opcodes and adds new ones to verify P2TR scripts and Schnorr signatures.

After disagreement around which activation method to use, community members compromised on a "Speedy Trial," requiring that 90% of the blocks mined signaled support for the upgrade by sending data via "signal bits" over any ~two week difficulty period beginning in May. The upgrade reached consensus at the end of the third signalling period in mid-June at block 687,284, and Taproot is expected to activate at block 709,632 on November 16th, 2021.

- ***Benefits:*** Taproot is the biggest upgrade to the Bitcoin network since SegWit in 2017. It's Schnorr signatures and related key aggregation attribute bring about significant security and efficiency benefits by making all transaction types look the same. Moreover, Taproot defines new spending conditions that when combined with Schnorr signatures and MAST, provides for more complex spending conditions while requiring less information to be revealed on-chain. And Tapscript will update Bitcoin Script to enable Schnorr signatures and Pay2TR. Benefits of Taproot are likely to initially be limited, since, as a soft fork, most Bitcoin wallet providers will continue to use ECDSA and as such, blocks will continue to have both Schnorr and ECDSA signatures. That said, Taproot should encourage greater use of multisig transactions and Lightning Network channels given its cost and privacy benefits. And Taproot's key aggregation should make Bitcoin more attractive for building DeFi upon. And of course, this key upgrade improves privacy, security, and scalability as detailed above to enhance Bitcoin as both a medium of exchange and store of value.

Exhibit 1: Pay-To-Taproot (P2TR) Example Spending Conditions



Source: River Financial, GSR

Author: Brian Rudick, Senior Strategist

Sources Used

- Bitcoin Github: BIP 340 Schnorr Signatures for secp256k1
- Bitcoin Github: BIP 341 Taproot: SegWit version 1 spending rules
- Bitcoin Github: BIP 342 Validation of Taproot Scripts
- Kraken Intelligence: Taproot Primer, An Upgrade for the Ages
- Coinmonks: An Introduction Guide on Bitcoin TAPROOT
- Coinmonks: Schnorr Signatures Bitcoin 101
- River Financial: What Is Taproot and How Will It Benefit Bitcoin?
- River Financial: What Do Schnorr Signatures Do for Bitcoin?
- River Financial: Pay-to-Taproot (P2TR)
- Binance: What Is Taproot and How It Will Benefit Bitcoin
- Bitcoin.it: BIP 0001
- Komodo Platform: Bitcoin Script
- River Financial: What is a Bitcoin Improvement Proposal
- Clark Moody: Bitcoin Dashboard

About GSR

GSR is a global leader in digital asset trading, market making, OTC derivatives, and investments. We operate in a culture of excellence and leverage our first-rate reputation, deep relationships and proprietary trading technology to move swiftly and capitalize on market opportunities.

GSR's experienced team brings together decades of institutional trading expertise, while our industry-leading proprietary technology stack anchors everything we do.

Our main service areas are: market making; proprietary and algorithmic trading; client execution; structured products; risk management solutions; and portfolio investments.

For more information or if we can help with anything, please see gsr.io or contact us at gsr@gsr.io.

Required Disclosures

This material is a product of the GSR Sales and Trading Department. It is not a product of a Research Department, not a research report, and not subject to all of the independence and disclosure standards applicable to research reports prepared pursuant to FINRA or CFTC research rules. This material is not independent of the Firm's proprietary interests, which may conflict with your interests. The Firm trades instruments discussed in this material for its own account. The author may have consulted with the Firm's traders and other personnel, who may have already traded based on the views expressed in this material, may trade contrary to the views expressed in this material, and may have positions in other instruments discussed herein. This material is intended only for institutional investors. Solely for purposes of the CFTC's rules and to the extent this material discusses derivatives, this material is a solicitation for entering into a derivatives transaction and should not be considered to be a derivatives research report.

This material is provided solely for informational purposes, is intended for your use only and does not constitute an offer or commitment, a solicitation of an offer or comment (except as noted for CFTC purposes), or any advice or recommendation, to enter into or conclude any transaction (whether on the indicative terms shown or otherwise), or to provide investment services in any state or country where such an offer or solicitation or provision would be illegal.

Information is based on sources considered to be reliable, but not guaranteed to be accurate or complete. Any opinions or estimates expressed herein reflect a judgment made as of the date of publication, and are subject to change without notice. Trading and investing in digital assets involves significant risks including price volatility and illiquidity and may not be suitable for all investors. GSR will not be liable whatsoever for any direct or consequential loss arising from the use of this Information. Copyright of this Information belongs to GSR. Neither this Information nor any copy thereof may be taken or rented or redistributed, directly or indirectly, without prior written permission of GSR. Not a solicitation to U.S. Entities or individuals for securities in any form. If you are such an entity, you must close this page.