Taproot BIP Proposal

The proposal for Taproot, a long-anticipated technological change to bitcoin, is “nearly ready", a notable update that comes nearly two years after its introduction.

Taproot offers a new degree of privacy by making all transactions – no matter how complicated – appear the same to observers of blockchain data. The code adds what supporters call a much-needed feature to the network, and brings significant implications for scaling, fungibility and script innovation. Taproot is expected to be bundled together with Schnorr, a related upgrade that seeks to enable signature aggregation and make Taproot’s implementation possible. Right now, the Taproot/Schnorr soft fork is moving through the ecosystem feedback phase as developers recommend and review possible changes to the draft. The proposal moving forward is designed to save 30% to 75% in fee use and accelerate block validation by up to 2.5 times. It's a process that has attracted interest and excitement from different quarters of the crypto ecosystem.

Bitcoin relies on public-key cryptography to validate transactions. The current Elliptic Curve Digital Signature Algorithm has several shortcomings when it comes to privacy and fungibility, and the Taproot/Schnorr soft fork aims to fix them by hiding specific payment types from outside observers. Taproot is best explained using an example. Suppose there's an exchange featuring a hot key, a trusted 3rd party key, and a cold wallet emergency backup key. Conventionally, participants would need to broadcast all three keys as well as the two signatures used to spend the coins. The proposed upgrade will aggregate these keys into a single Schnorr signature, which would then be used to validate a Taproot output key that represents all the complexities involved. As a result, observers of the blockchain would simply see a single output without knowing which two keys were deployed to validate the transaction. This would reduce transaction size, save fees, and improve privacy. You can have a Lightning channel open or closed, a simple payment between two people, or a very sophisticated smart contract, and they sudenly became indistinguishable by spending Bitcoin using Taproot.

Taproot also opens the door for inscription innovation, as it allows for complicated arrangements of signatures and keys and eliminates limitations for how many scripts can be used to spend coins. The Taproot/Schnorr upgrade was the third-most popular write-in topic that industry participants said they are most excited to see in 2020. It will not only save fees and blockspace, but also enable new features and generate more interests to the network. It is also expected that Taproot will be incorporated by more wallets and more interesting features built for those who are securing their Bitcoin.

Now that it has been included as a Bitcoin Improvement Proposal (BIP), next step will be to make a request to Bitcoin Core with the proposed consensus rule changes, which will likely bring in another round of reviews around Taproot’s implementation. If that goes well, it will be merged, and discussion will start about how to activate it on the network. Finally, a release with the activation will be published, and if the conditions to activate it are met, it will go live.