23 December 2021, 15:00 (EET)

What to Expect from Taproot – The First Bitcoin Update in 4 Years

On November 14th, 2021, Bitcoin activated the most significant update in four years at block 709,632, Taproot. The upgrade is designed to streamline transaction processing by making them faster and less expensive. The previous Bitcoin upgrade ended dividing the Bitcoin community, leading to the creation of a Bitcoin fork - Bitcoin Cash. Nevertheless, the Taproot upgrade was not contentious, signaling the beginning of a new Bitcoin era.

So, what is Taproot, and what can you expect from it? It is not only the benefits of the upgrade that are important. Taproot is essential as it reminds the world what Bitcoin is.

What is Taproot?

Taproot is Bitcoin's most recent and significant upgrade in four years. It consists of three primary updates – the BIP 340, BIP 341, and BIP 342. Generally, these updates address the Bitcoin network's privacy, scalability, and security concerns.

At the center of Taproot is a technique known as Schnorr Signatures that replaced the previous Elliptic Curve Digital Signature Algorithm (ECDSA). Satoshi Nakamoto, the anonymous Bitcoin creator, used ECDSA to create Bitcoin since Schnorr Signatures was still patented.

Taproot improves multi-signature and scripted transactions – special transactions signed with several keys. Previously, these transactions were not easily recognized by blockchain analytic companies. Taproot gives multi-sig and scripted transactions a custom wallet-to-wallet appearance, significantly improving their privacy and minimizing their size.

The blockchain upgrade also introduces some scripted conditions that must be achieved for transactions to be finalized and improves scalability. This means that more transactions are verified per block than they previously were. In other words, it is now easier to verify every node. This sounds well for the Bitcoin blockchain in the long term.

Besides, Taproot introduces a new address to the Bitcoin network. Previously, blockchain addresses started with 'bc1q,' but now they have a 'bc1p' initial. The upgrade also introduces Point Time-Locked Contracts (PTLC) to the blockchain network. These contracts streamline Lightning Network's privacy and reduce the cost of running a Lightning channel.

A Meaningful Step

The benefits above clearly show that Taproot is an essential Bitcoin update since the Segwet update, implemented in 2017. The presence of few Bitcoin updates illustrates one of its primary characteristics: It is robust.

Upgrading the Bitcoin protocol successfully is quite challenging. Remember, there is no central authority or individual to push changes through. The Bitcoin community is the one that gives consensus, and reaching consensus in a diverse and decentralized group of contributors is quite challenging. Therefore, even the simple fact that Taproot was unanimously backed shows its significance in the evolution of blockchain technology.

The Actual Benefit

Taproot upgrade improves Bitcoin's functionality and broadens its market. This sounds good, especially for those interested in Bitcoin prospects and valuation. However, the real benefit of Taproot for the investing community generally is that it reminds us that Bitcoin is an evolving technology.

Some crypto investors regard Bitcoin as a store of value, while others see it as a means of transferring value. These two groups of people overlook Bitcoin's most significant characteristic – Bitcoin is a new technology that is a work in progress. When you purchase precious metals like Silver, you don't even think how it will evolve ten years from now. Contrary to this, Bitcoin keeps on evolving.

Technological upgrades come with their own risks – the introduction of bugs and other unplanned consequences. This explains why Bitcoin upgrades are rare and far between since they must be carefully evaluated and tested. Additionally, a consensus is hard to achieve since there is no central authority or individual to approve upgrades solely.

However, a mutual consensus comes with its positives. Bitcoin has a market capitalization of almost $1 trillion, excluding the valuation of other businesses devoted to supporting the Bitcoin blockchain. Therefore, the risk must be reduced to almost nil.

Taproot demonstrates Bitcoin as a good store of value that can create good returns for investors. Bitcoin also offers an opportunity for investors to dive in early to a transformative technology investment. It can be compared to staking in a startup with a lot of potential but improved liquidity and no paperwork.

How Taproot Affects Bitcoin the Cryptocurrency

As the Bitcoin blockchain scales and becomes more effective at verifying transactions, it is more likely to become an efficient medium of exchange. Previously, Bitcoin's value was pegged on its utility as a store of value. Thus, it is likely for its value to increase as transactions become faster and more cost-effective.

Mining revenue will reduce significantly when all the 21 million Bitcoins are mined. Transaction charges will make up the majority of miner revenue. The Taproot upgrade brings this important step closer by reducing block sizes and enhancing the verification speed on the Bitcoin blockchain.

Final Thoughts

From the above discussion, we have seen that Taproot:

Enhances privacy: It makes complex processes, especially those that require multi and scripted signatures, indistinguishable from other on-chain transactions.

Minimizes fees: The upgrade reduces the data size of complicated transactions, minimizing the transaction costs further.

Better flexibility: The Taproot signature improves smart contract efficiency, making it ideal for users to introduce more complex requirements for a transaction.

Lightning boost: The upgrade makes Lightning Network transactions cost-effective, more flexible, and private.

Taproot not only enhances Bitcoin's usability, which will further broaden its market share and potentially its value in the long run. It reminds the world of Bitcoin's primary feature that seems to have been overlooked in the current market-based narratives. Bitcoin is still at its infancy stages, and its potential goes beyond its supply limit, inflation resistance, and decentralization.

Anyone who accepts cryptocurrency may present themselves globally and confirm their authenticity through BitcoinWide’s platform to improve their reputation by creating a profile.

Bitcoinwide