

# Taproot: Explaining Bitcoin's Biggest Upgrade in Four Years

IMPROVED SECURITY, PRIVACY, & THROUGHPUT RATE

Greg Cipolaro

GLOBAL HEAD OF RESEARCH

Ethan Kochav

RESEARCH ANALYST



# Introduction

---

On November 14th, block number 709,632, Bitcoin will undergo its most significant technical upgrade in over four years as a series of technology updates collectively known as “Taproot” becomes part of Bitcoin’s code. Originally proposed by Gregory Maxwell in 2018 and developed by Pieter Wuille, Taproot is designed to improve Bitcoin’s security, privacy, and throughput rate while reducing fees and laying a foundation for future upgrades.

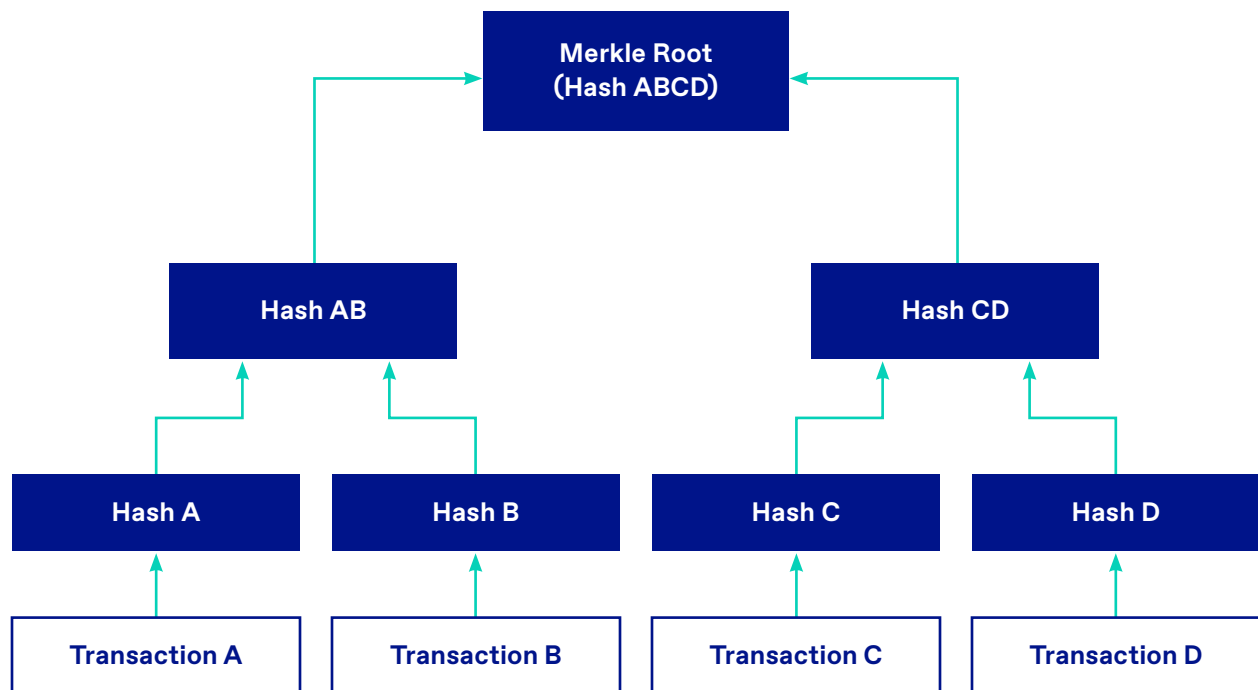
Taproot joins two technologies that have long been contemplated in the Bitcoin developer universe, Merklized Abstract Syntax Trees (MAST) and Schnorr signatures. In the following report, we introduce both technologies and explain how they improve the Bitcoin network. Like previous foundational updates, such as SegWit in 2017, we expect the adoption of Taproot to grow over time. Taproot is being deployed via a soft fork, meaning users, nodes, and miners can choose to adopt the technology but are not forced to do so. Taproot enjoys near-universal acceptance amongst the community, as opposed to SegWit, which was wrapped up in the scaling debate, but Taproot is more complex to implement than SegWit and SegWit provided a much more dramatic transaction fee reduction for most transaction types. Still, the deployment of Taproot is an important milestone for Bitcoin and one that continues to expand its use cases, while making it more secure and private.

# Merkalized Abstract Syntax Trees (MAST)

## Improves Privacy and Reduces Data Storage

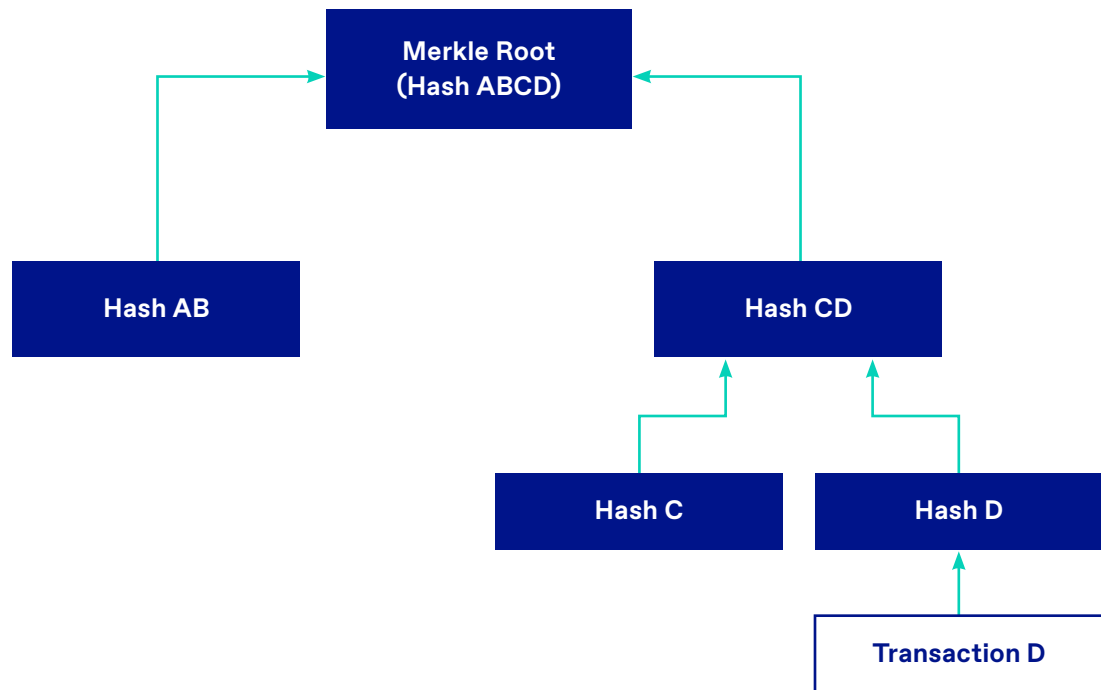
The discussion of Bitcoin technology is often focused on hash algorithms, digital signatures, mining, and blockchains. However, an equally important but often overlooked feature is something called a Merkle Tree. Patented by computer scientist Ralph Merkle in 1979, Merkle Trees are a way to prove that a single item exists in a data structure, such as whether a transaction has been included in a previous block, with a very limited amount of information. Merkle Trees are essential for the functioning of light clients or Simple Payment Verification (SPV) wallets. They are wallets that run on resource-constrained devices like smartphones. With the use of Merkle Trees, light clients can make bitcoin transactions without having to hold the +370 Gb of blockchain data in a Bitcoin full node.

Merkle Trees work by organizing a large set of data, in this case, transactions in a block, in a binary tree format that visually looks like a March Madness bracket. The top of the tree is an important element — a crucial element called the Merkle Root. The Merkle Root is included in a block header, publicly visible data that is encoded at the beginning of every block.






The Merkle Root is computed by combining each of the matchups all the way up the tree and hashing them together. To prove that a transaction is in the tree, a full node only needs to provide to a light client the set of hashes that would be combined with that transaction to create the Merkle Root. This is much less data than providing all the transactions in a block. Without this mechanism, the SPV would not be able to interact with the blockchain.



It is also worth noting that the hashes used as proof are fingerprints of transactions (in the first “round”) or fingerprints of fingerprints (in later “rounds”), so the proof data reveals no transaction information. While this feature is less important in this context, since transactions are easily viewable on the blockchain, it becomes more relevant when we apply this technology to digital signatures through something known as a “Merkelized Abstract Syntax Tree” (MAST).

MAST is an extension of the Merkle Tree concept except that it is applied to advanced transaction types or conditional payments. The possible conditions that can define a payout are organized in a Merkle Tree as above. To spend a bitcoin that is tied to these conditions, the spender only needs to show the specific condition that leads to a spend, along with the hashes of each of its “match-ups” on the tree. Currently, the spender needs to show the blockchain entirety of potential conditions to spend a transaction, which can be a comparatively large amount of data. MAST, therefore, improves privacy by hiding some of the conditions of a spend from the public — remember, the matchups on the tree are fingerprints, not actual conditions — which has the knock-on effect of reducing the amount of space taken on the blockchain and thus the fees that will be incurred.



# Schnorr Signatures are an Improved Digital Signature Scheme

---

Bitcoin would not work without digital signatures. A signature is what allows users to send (spend) bitcoins and for nodes to verify that transactions are valid. Bitcoin's current signature system uses Elliptic Curve Digital Signature Algorithms (ECDSA), a secure technology but one that today is inferior to alternatives. At the time that Satoshi Nakamoto wrote the code for Bitcoin, Schnorr signatures, named after its creator, German mathematician and cryptographer Claus Schnorr, existed but had just come off patent protection and were not implemented in the open-source codebases used to write Bitcoin Core. Today, Schnorr signatures have gained greater acceptance after a decade of having been battle-tested, and their enhancements over ECDSA can be utilized.

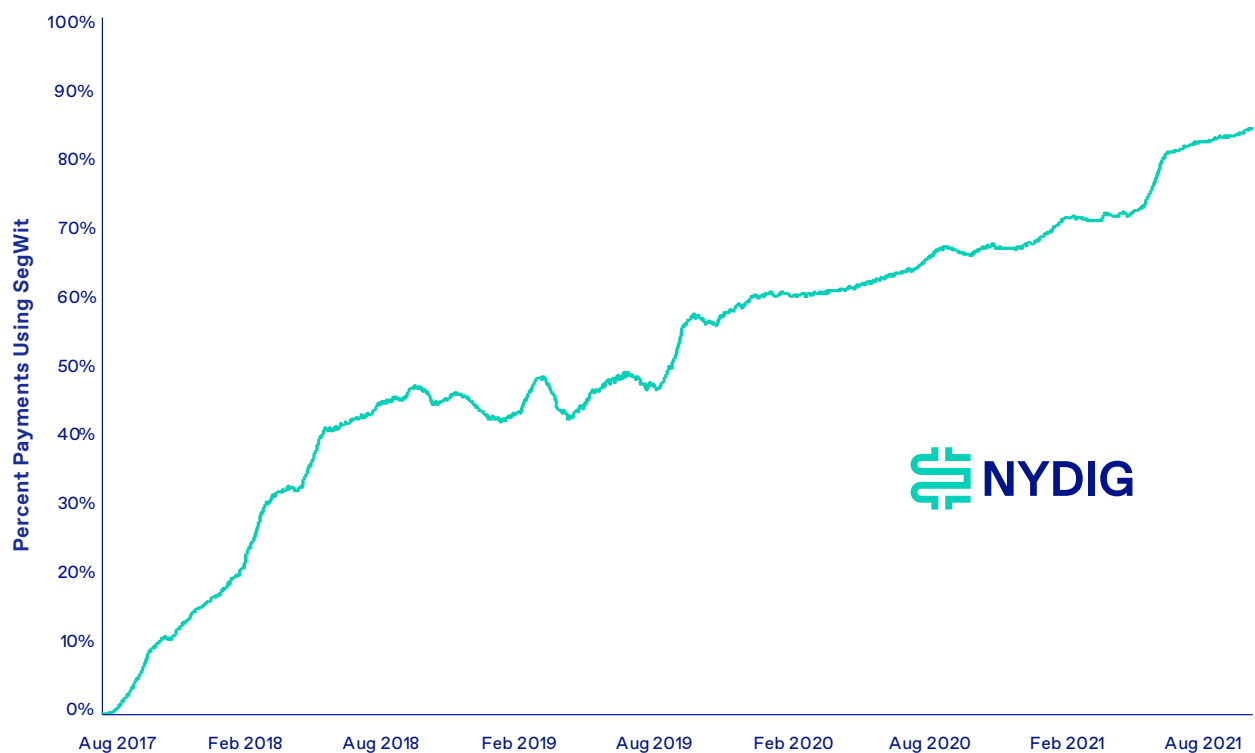
Schnorr signatures are mathematically simpler than ECDSA signatures. This means that it is easier to formally prove its security, one big advantage in the cryptographic community (though an ECDSA signature has never been successfully forged). Schnorr also allows for linear combinations of public/private keys, allowing two parties to efficiently combine their signatures. In ECDSA, to create a multi-signature address, one must write a script that requires both parties to provide their signatures separately. In Schnorr, one only needs to provide a single combined public key. Much like MAST, this can create significant space savings and improve privacy, though it does so in a completely different way. The linearity also allows for something called "batch verification." Instead of verifying one signature at a time, nodes can add up the public keys, add up the signatures, and confirm that the combined signature is valid. This can considerably speed verification of transactions and syncing the blockchain, provided a significant amount of the network adopts Taproot.

Although we have discussed Schnorr and MAST as separate technologies, Schnorr is also able to interact directly with MAST in one interesting way. To encumber a transaction with a MAST script, a transactor uses its Merkle Root in the unlocking script (as described in the previous section). Because of the linearity of Schnorr signatures, one can sum their public key with the Merkle Root to create a new public key. A transaction can be spent by providing either a public key (or multiple public keys) or the solution to the MAST script. This further improves the space savings and privacy brought by MAST.

# How Quickly Will the Network Adopt Taproot?

The best parallel to Taproot is SegWit, which was activated in fall 2017. In the four years that followed, SegWit has finally reached an adoption rate of nearly 85% of transactions.

## SegWit Adoption Has Reached 85%



Source: [transactionfee.info](https://transactionfee.info)

It is difficult to know whether the uptake of Taproot will follow a similar trajectory to SegWit. On one hand, Taproot is a much less controversial upgrade than SegWit. SegWit was lumped into a rancorous scaling debate within the Bitcoin community, and so a large part of the community rejected SegWit on ideological grounds. Taproot does not nearly engender the same political disagreement. On the other hand, SegWit provided instant fee savings on nearly all transactions. Nodes could find immediate and tangible monetary savings by switching to SegWit. Taproot only provides such savings on complex scripts that not all users may employ. In addition, the technology may also be more difficult to implement by wallet providers.

# Conclusion

---

We understand that wading into the technical underpinnings of Bitcoin can often be a complex exercise for most investors. It is important to realize that while we often analogize Bitcoin with digital gold, at its core, Bitcoin is still software tied together through economic incentives and social bonds throughout the community. This software continues to improve, becoming more efficient and introducing new features, as it does with Taproot. The two innovations encompassed by Taproot, MAST and Schnorr signatures, act in somewhat separate and sometimes interlinking ways to accomplish the joint goal of improving security and privacy while reducing space taken on the blockchain and thus fees. Both concepts have been long contemplated in the Bitcoin community, and unlike the previous major update, SegWit, were much less controversial. The enhancements that they make to the network may also improve layer two solutions such as the Lightning Network. Their long-awaited inclusion into Bitcoin has been met with optimism. Not only will Taproot improve the network in the short term, but it provides the foundation for new features.

## DISCLOSURES

This report has been prepared solely for informational purposes and does not represent investment advice or provide an opinion regarding the fairness of any transaction to any and all parties nor does it constitute an offer, solicitation or a recommendation to buy or sell any particular security or instrument or to adopt any investment strategy. Charts and graphs provided herein are for illustrative purposes only. This report does not represent valuation judgments with respect to any financial instrument, issuer, security or sector that may be described or referenced herein and does not represent a formal or official view of New York Digital Investment Group or its affiliates (collectively, “NYDIG”).

It should not be assumed that NYDIG will make investment recommendations in the future that are consistent with the views expressed herein, or use any or all of the techniques or methods of analysis described herein in managing client accounts. NYDIG may have positions (long or short) or engage in securities transactions that are not consistent with the information and views expressed in this report.

The information provided herein is valid only for the purpose stated herein and as of the date hereof (or such other date as may be indicated herein) and no undertaking has been made to update the information, which may be superseded by subsequent market events or for other reasons. The information in this report may contain projections or other forward-looking statements regarding future events, targets, forecasts or expectations regarding the strategies, techniques or investment philosophies described herein. NYDIG neither assumes any duty to nor undertakes to update any forward-looking statements. There is no assurance that any forward-looking events or targets will be achieved, and actual outcomes may be significantly different from those shown herein. The information in this report, including statements concerning financial market trends, is based on current market conditions, which will fluctuate and may be superseded by subsequent market events or for other reasons.

Information furnished by others, upon which all or portions of this report are based, are from sources believed to be reliable. However, NYDIG makes no representation as to the accuracy, adequacy or completeness of such information and has accepted the information without further verification. No warranty is given as to the accuracy, adequacy or completeness of such information. No responsibility is taken for changes in market conditions or laws or regulations and no obligation is assumed to revise this report to reflect changes, events or conditions that occur subsequent to the date hereof.

Nothing contained herein constitutes investment, legal, tax or other advice nor is it to be relied on in making an investment or other decision. Legal advice can only be provided by legal counsel. NYDIG shall have no liability to any third party in respect of this report or any actions taken or decisions made as a consequence of the information set forth herein. By accepting this report in its entirety, the recipient acknowledges its understanding and acceptance of the foregoing terms.