**The Taproot Update: What Is It, How Will It Affect Bitcoin, And When Will It Launch?**

Within the coming months to a year, Bitcoin will receive the Taproot update, one that is much anticipated by a large portion of the community, as it will improve various aspects to the whole network and general experience.

This update, which we'll discuss in general sense without going too much into its technical details, is actually a bundle of three new implementations that's coming to Bitcoin:

● Taproot

● Schnorr Signatures

● TapScript

**What is Taproot?**

Taproot is a soft-fork that would improve Bitcoin's scripts, resulting in an improvement to its more complex contracts within the network, by bringing privacy to users.

It achieves this increased privacy by hiding the contents of a complex contract, like a multi-signature setup, perhaps with a time-lock function, and makes it appear as if it was a normal single transaction.

It's worth noting though that the initial sender's and the end receiver's address will still be known once the contract has been executed and completed, but other addresses that were used for signing would be hidden from the public.

**What is Schnorr Signatures?**

Schnorr Signatures is a different type of cryptographic signature scheme, that's both more simple and efficient in comparison to Bitcoin's Elliptic Curve Digital Signature Algorithm (ECDSA), because of its signature aggregation process.

That process will benefit users that are using a multi-signature setup, where instead of having to send out multiple transactions with two or more signatures, it will combine these signatures into one unique Schnorr signature to send.

**What is TapScript?**

Without getting technical, TapScript is basically an upgraded version of the current programming language Bitcoin has, which is called Script, which handles the spending policies.

It's considered to be a great addition added with this bundle of an upgrade, as it compliments both Taproot and Schnorr Signatures, as it improves Bitcoin's signature hashing, helping out to validate taproot scripts, brings in more flexibility to add new, what's termed as, opcodes (operation codes), which improves the capabilities of Bitcoin's smart contract, as well as modify or remove some resource limitations, like the current script size of 10,000 bytes, and removing the number of opcodes limit.

**What does this mean for Bitcoin?**

It means that users will benefit from increased privacy regarding Bitcoin's more complex transactions, a decrease in the amount of data that's being sent out and stored on the blockchain, even more transactions would be included per-block, which means less congestion within the in the network, a decrease on transaction fees as a result, and finally it would also help the development of the Lightning Network, as well as a possible increase in adoption of decentralised exchanges (DEX).

Generally speaking, the benefits for most people will be a simple enjoyment of paying less fees on their transactions, while the benefits for those who wish to indulge in more complex transactions, will enjoy a great deal of decreased fees, higher privacy, as well as an increase in the possibilities of building new applications.

**When will it get released?**

That depends. The Taproot update will launch sometime after the 'Speedy Trial' process has concluded, which is an attempt to see whether 90% of node operators within the Bitcoin network, will accept and adopt this upgrade or not, and if that threshold of adoption is reached, then we'll the release of the update soon after.

With all of that said, we're crossing our fingers for a smooth and successful launch of Taproot, considering all the great benefits it'll bring to Bitcoin and all of its users.