jesse@yourpersonalcryptoassistant.com

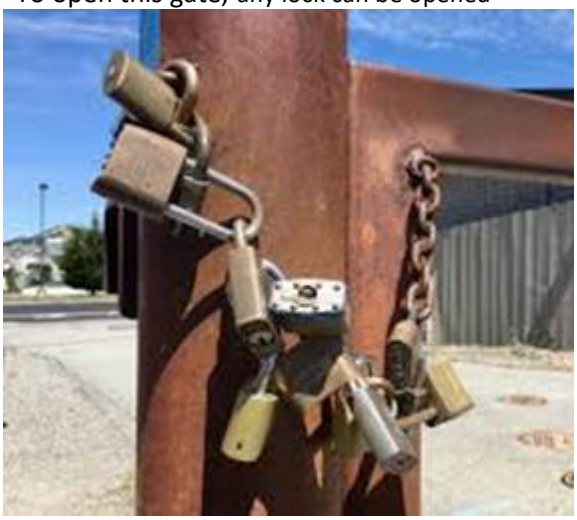
From: jesse@yourpersonalcryptoassistant.com
Sent: Wednesday, November 17, 2021 7:05 PM
To: jesse@yourpersonalcryptoassistant.com
Subject: Taproot is live - What's a taproot? and other thoughts - from Your Personal Crypto Assistant

Taproot is live - What's a taproot? It's taken four years, but the next big Bitcoin upgrade is now live. Called Taproot, this upgrade consists of 3 Bitcoin Improvement Proposals (BIP 340, 341, and 342). Does this impact you today? Probably not. This is really about increasing Bitcoin capabilities that wallets and exchanges can leverage. Until developers upgrade to leverage their products as an end user you can't do much on this… If all you care about is the price of Bitcoin and will it go up, the short answer is improving Bitcoin should help it's price in the long term, but short term who knows. Bitcoin is down about 10% as I write this… If you want to learn more about the changes and advantages that will come out of this (eventually) read the three detailed items below, or just skip ahead…

1. BIP 340 Schnorr signatures: Unless you are a cryptography geek the details on the math involved with the new type signatures are likely way beyond anything you care about. Same with the details on the current type signatures (ECDSA). There are three key advantages to the newer Schnorr signatures. First, they are a bit smaller which should reduce transaction costs slightly. Second, they are somewhat more secure than the earlier signatures. Third and most importantly, they allow for combo signature checks (see BIP 341). This also means that on chain a multi-sig looks the same as a single sig, improving privacy.
2. BIP 341 Taproot: There is a data structure called a Merkle tree (again not important unless you are a computer geek) that allows multiple conditions (signatures) to be combined and evaluated in one test. This is an oversimplification, but think of the multiple conditions like multiple padlocks on a gate.

To open this gate, every lock has to be opened

To open this gate, any lock can be opened



The tree structure allows many conditions and/or combinations of conditions (like locks in the picture above) to be combined as part of a Bitcoin transaction and validated easily (like the daisy chain picture on the right). Just like a tree in your back yard has a taproot that is the primary root and the smaller lateral branches extend from that, bitcoin transactions with many conditions (branches) can now be validated with just one check. Privacy is further enhanced since only the actual condition that was used to spend is revealed, the other conditions remain private.

3. BIP 342 Tapscript: This uses the above capabilities to provide new scripting options allowing Bitcoin to more easily support smart contracts as well as scripting options that will enable future enhancements to be added more easily.

Now that we are past the technical aspects, here are the three key takeaways I think you should know about the taproot upgrade.

1. Unlike the last major change, this one is very strongly supported by the Bitcoin community (everyone is on board to make it work).
2. Taproot and the new Tapscripts will help Bitcoin compete against Ethereum and other blockchains on smart contract implementation.
3. Bitcoin continues to improve and this increases the odds that it will maintain its current dominant position in crypto.

When I started drafting this email, Bitcoin was over $68,000 and my thought was with taproot in place it would go higher fairly quickly. Instead as I send this now, it's just under $60,000. I remain long term bullish and for me see this as a buying opportunity. I'm not quite ready to talk about it yet, but I think by my next email I'll have finished setting up Bitcoin in my IRA. When I do so, I'll share with you my thoughts on IRA crypto options, and let you know what I did.

What's next for you? you need to make your own call. If you are unsure start small, but please do continue learning and using crypto. As always you need to DYOR (Do Your Own Research) and invest wisely. For me, I enjoy explaining the technology and sharing what I know, that's what I do. I teach people about crypto. Call or email me and let me know how I can help…

I hope this has been interesting for you and it helps move you forward with crypto. Remember, this is only for your education, I don't offer financial, legal or tax advice. You need to evaluate your own situation and risk tolerance and DYOR (Do Your Own Research). Do not put any money into crypto that you are not willing to lose. I enjoy answering crypto questions, so feel free to email me or call me, I like to help. Personal instruction and assistance is my specialty – so if you or someone you know is looking for more than an email response to a question I also provide one on one and small group classes as well as personalized consulting.

Thanks,

Jesse

Jesse Markowitz
(407) 900-9453
Jesse@YourPersonalCryptoAssistant.com
https://YourPersonalCryptoAssistant.com
Helping you understand and excel with Bitcoin and other crypto technologies