bitcoin`s Sound Money Properties Series

#13: Secure & Scalable

with @SimplestBTCBook & @DJSATOSHI18

- PORTABLE, DURABLE, DIVISIBLE, FUNGIBLE
- TRULY SCARCE
- DISTRIBUTED & DECENTRALIZED
- CENSORSHIP RESISTANT & UNCONFISCATABLE
- IMMUTABLE & INCORRUPTIBLE
- EASILY VERIFIABLE & CAN'T BE COUNTERFEITED
- PERMISSIONLESS, FRICTIONLESS & PEER-TO-PEER
- NEUTRAL & VOLUNTARY
- TRANSPARENT, OPEN-SOURCE & AUDITABLE
- BORDERLESS
- PROVIDES SETTLEMENT FINALITY
- PSUEDONYMOUS & TRUSTLESS
- SECURE & SCALABLE
- DISINFLATIONARY/DEFLATIONARY

SECURE

Definition of secure

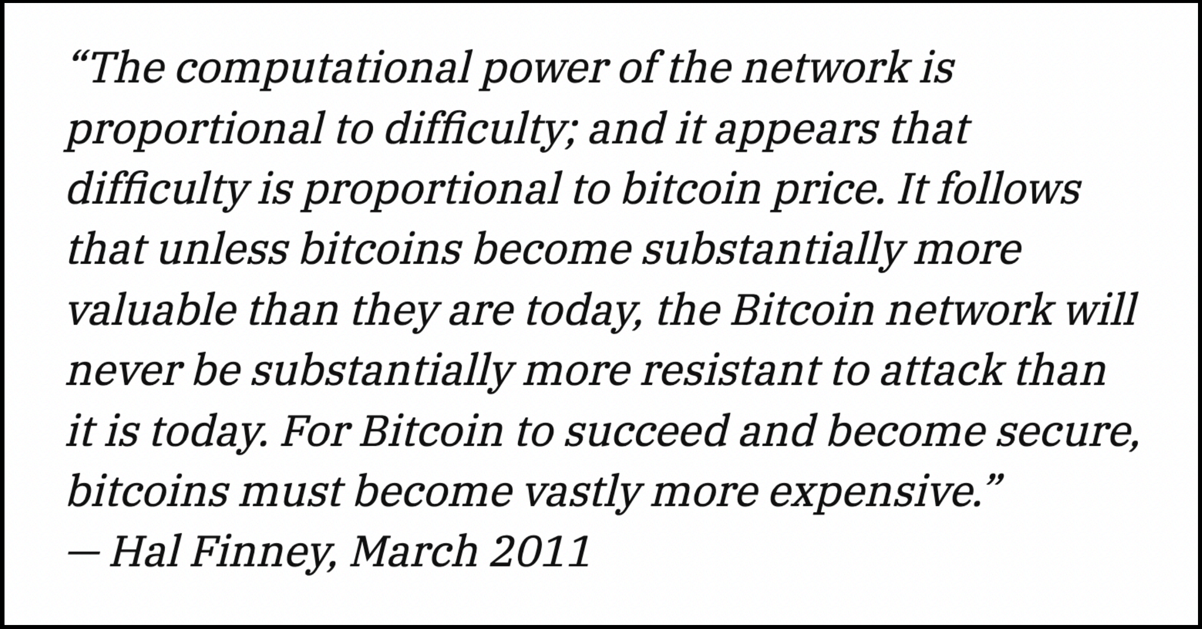
1 : free from danger

a : affording safety - a secure hideaway

b : trustworthy, dependable - a secure foundation

c : free from risk of loss

- merriamwebster.com



"The computational power of the network is proportional to difficulty; and it appears that difficulty is proportional to bitcoin price. It follows that unless bitcoins become substantially more valuable than they are today, the Bitcoin network will never be substantially more resistant to attack than it is today. For Bitcoin to succeed and become secure, bitcoins must become vastly more expensive."
— Hal Finney, March 2011

What Hal meant here, is that bitcoin's security is based on the amount of computational power being used by the network…

and this power increases as the mining difficulty increases…

and the mining difficulty increases as the price goes up, since the more valuable bitcoin is perceived to be, the more people will want to mine it…

and the more miners there are, the more the difficulty will increase, since the algorithm adjusts making it harder to mine, in order to keep the issuance of new bitcoins constant.

Bitcoin has increased in price by well over 2,000,000% since Hal made that comment in 2011.

I would venture to guess that he would agree that today, bitcoin is very, very secure!

BITCOIN IS SECURE

- What do we mean when we say bitcoin is secure?

- We mean that the bitcoin network, run by thousands of distributed nodes and miners all around the globe, is the most secure computer network in existence.

- The security is enabled both by the distributed nature of the network, which is 100% voluntary and ad hoc, and by the literal amount of computing power utilized by the nodes and miners.

- In addition, the bitcoin protocol is secured by cryptography:

Cryptography uses mathematical techniques to transform data and prevent it from being read or tampered with by unauthorized parties. That enables exchanging secure messages even in the presence of adversaries.

- nist.gov

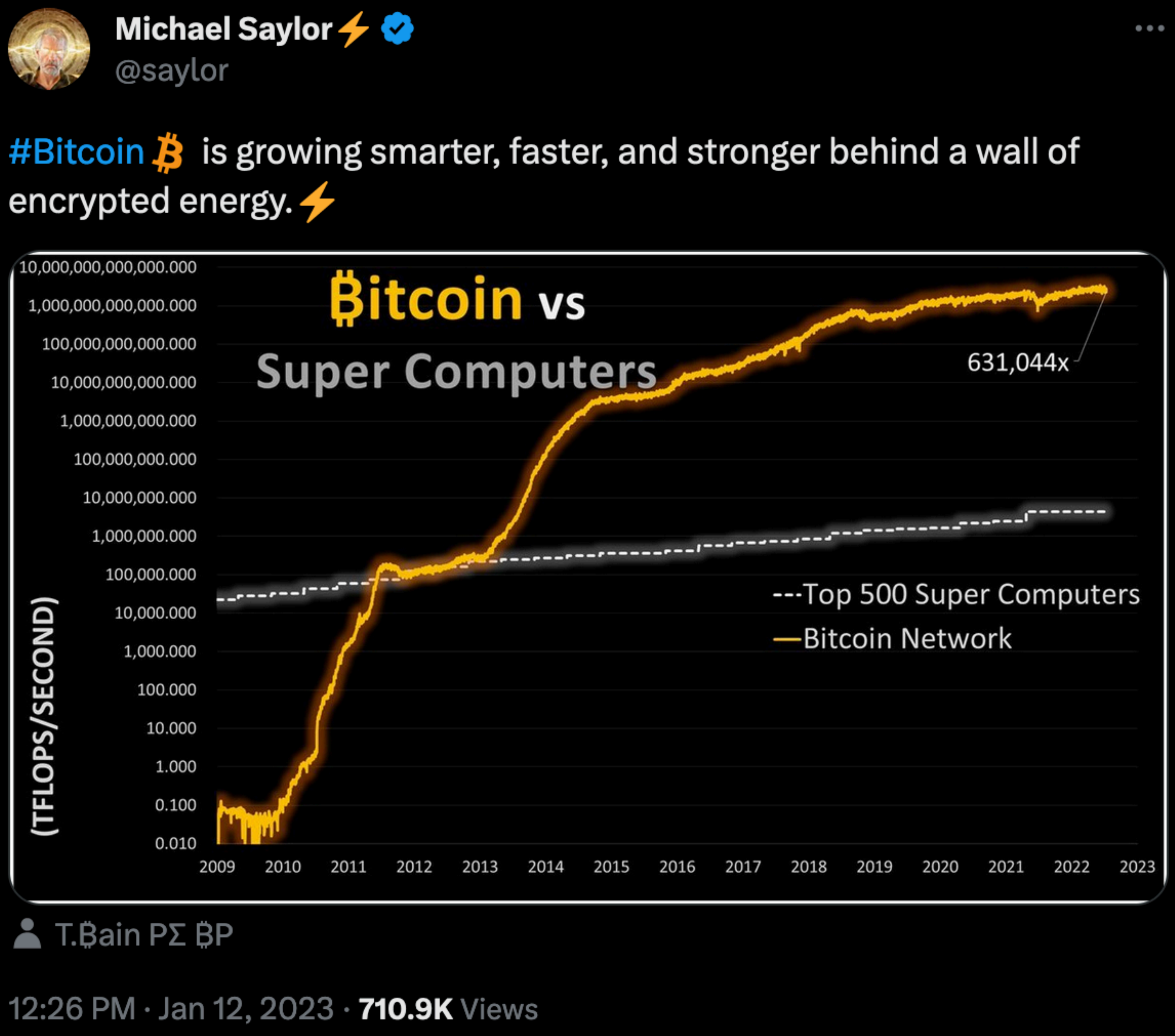
- Lastly, bitcoin is secure because it is immutable.

- As discussed in a previous episode, prior bitcoin transactions can never be altered.

- As each new block is appended to the tip of the timechain, the previous blocks become ever more cemented in by a wall of cryptographic energy.

- You can imagine a brick wall. As each new layer of brick is added, the ones lower down become more and more secure, it would take more and more time to ‘undo’ them and more and more expensive to rebuild, and all the while new bricks (blocks) are getting added to the top.

- Listen to the Michael Saylor clip discussing the incredible amount of energy backing bitcoin - https://twitter.com/BitcoinNewsCom/status/1670646136950996993



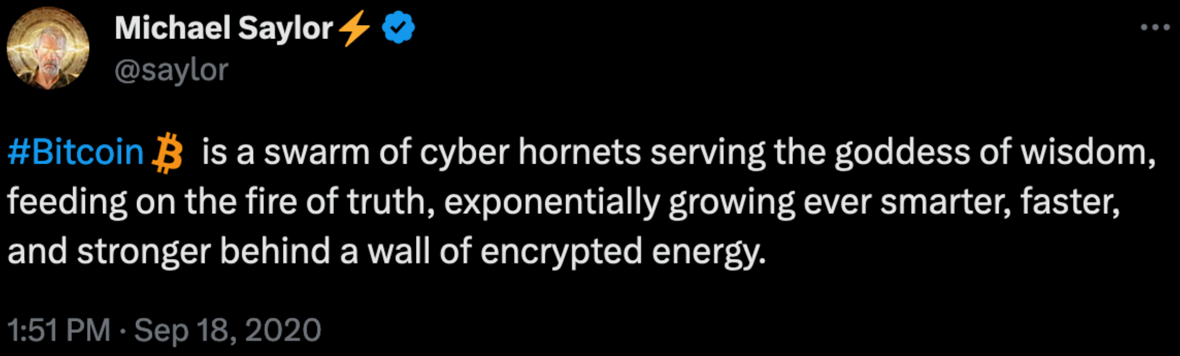
Michael Saylor⚡

@saylor

#Bitcoin ₿ is growing smarter, faster, and stronger behind a wall of encrypted energy.⚡

T.₿ain PΣ ₿P

12:26 PM · Jan 12, 2023 · **710.9K** Views

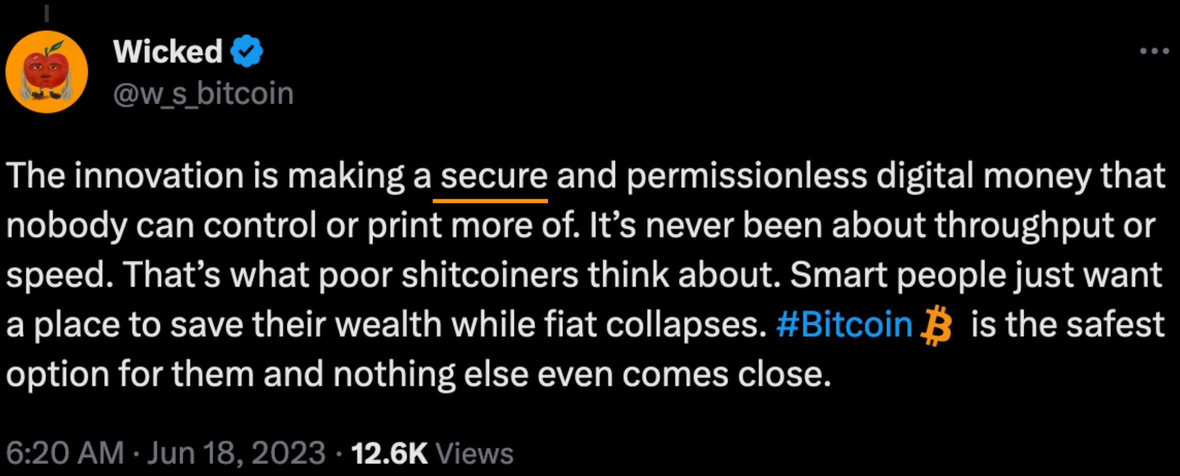


Michael Saylor⚡
@saylor

#Bitcoin ₿ is a swarm of cyber hornets serving the goddess of wisdom, feeding on the fire of truth, exponentially growing ever smarter, faster, and stronger behind a wall of encrypted energy.

1:51 PM · Sep 18, 2020

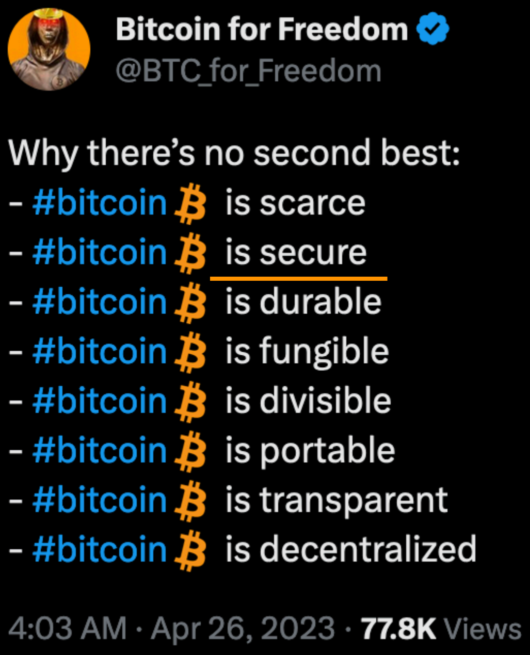
Bitcoin is Secure



Wicked
@w_s_bitcoin

The innovation is making a secure and permissionless digital money that nobody can control or print more of. It's never been about throughput or speed. That's what poor shitcoiners think about. Smart people just want a place to save their wealth while fiat collapses. #Bitcoin ₿ is the safest option for them and nothing else even comes close.

6:20 AM · Jun 18, 2023 · **12.6K** Views



Bitcoin for Freedom
@BTC_for_Freedom

Why there's no second best:
- #bitcoin ₿ is scarce
- #bitcoin ₿ is secure
- #bitcoin ₿ is durable
- #bitcoin ₿ is fungible
- #bitcoin ₿ is divisible
- #bitcoin ₿ is portable
- #bitcoin ₿ is transparent
- #bitcoin ₿ is decentralized

4:03 AM · Apr 26, 2023 · **77.8K** Views

SCALABLE

Definition of scalable

1: capable of being scaled

2 : capable of being easily expanded or upgraded on demand

- merriamwebster.com

What is Scalability?

- Scalability refers to the ability of a system to handle an increasing amount of work or load.

- In the case of Bitcoin, scalability refers to the number of transactions the network can handle at any given time.

- Transactions on the Bitcoin network are processed by nodes, and each node must validate the transaction before it is included in a block. The block is then added to the blockchain, which is a public ledger of all Bitcoin transactions.

The Current Scalability of Bitcoin

- On one hand, the number of transactions processed by the network has increased dramatically since its creation. In January 2009, the network processed just a handful of transactions per day.

- Fast forward to January 2021, and the network was processing an average of 330,000 transactions per day.

- From: btc.network/blog/how-scalable-is-bitcoin

- Roughly 6 blocks per hour x 24 hours = 144 blocks per day
- 144/day x 365 days a year = 52,560 blocks per year.

- So assuming an average of 2,500 transactions per block comes to an approximate total of 131,400,000 transactions per year on the base layer.

- As more people adopt Bitcoin there will be a higher demand for this limited block space on the base layer.

- Which is why layer 2 solutions like Lightning are helpful by providing faster and cheaper smaller transactions.

- @DJSATOSHI18

Scalability in the Traditional Financial World

- When comparing Bitcoin to the traditional financial world, it's important to keep in mind that Bitcoin is still a relatively new technology.
- Traditional payment systems like credit cards and wire transfers have been in use for decades and have had time to grow and scale to meet the demands of users.
- Credit card networks, for example, can process thousands of transactions per second.
- Wire transfers, on the other hand, can take several days to complete and are subject to high fees, especially for cross-border transactions.
- Despite the clear advantages of traditional payment systems in terms of scalability, they also have their own drawbacks. These systems are centralized, meaning that they are controlled by a single entity, such as a bank.
- This centralization can lead to issues such as censorship and security vulnerabilities.

- From: btc.network/blog/how-scalable-is-bitcoin

Improving the Scalability of Bitcoin

- To address the scalability issues facing Bitcoin, several solutions have been proposed. Some of the most promising include:

Segregated Witness (SegWit)

- SegWit is a protocol upgrade that was activated on the Bitcoin network in August 2017. The upgrade introduced several changes to the way transactions are processed, including increasing the block size limit from 1 MB to 4 MB. This has allowed the network to process more transactions per second, reducing wait times and lowering fees.

Lightning Network

- The Lightning Network is a second-layer solution that operates on top of the Bitcoin network. The network uses smart contracts to create payment channels between users, allowing them to transact without the need for each transaction to be confirmed on the blockchain. This has dramatically increased the number of transactions the network can handle, reducing wait times and fees.

- From: btc.network/blog/how-scalable-is-bitcoin

Conclusion

- The scalability of Bitcoin is an ongoing concern as the network continues to grow and gain popularity. However, it's important to keep in mind that Bitcoin is still a relatively new technology and that solutions are being developed to address the scalability issues.

- SegWit and the Lightning Network have already shown promising results… As the network continues to evolve, it's likely that new solutions will be developed, further improving the scalability of Bitcoin.

- In conclusion, while Bitcoin may not yet be as scalable as traditional payment systems *(yet!)*, its decentralized nature offers several advantages, including *censorship resistance and increased security. (Italics mine)*

- As the network continues to mature, it's likely that scalability will become less of an issue..

- From: btc.network/blog/how-scalable-is-bitcoin

BITCOIN'S CURRENT/POTENTIAL SCALING TECH

- Segwit - Segregated Witness
- Lightning
- Schnorr Signatures/Taproot
- Ark

SEGWIT BENEFITS

1. Malleability Fixes
2. Linear scaling of sighash operations
3. Signing of input values
4. Increased security for multisig via pay-to-script-hash (P2SH)
5. Script versioning
6. Reducing UTXO growth
7. Efficiency gains when not verifying signatures
8. Block capacity/size increase
9. Moving towards a single combined block limit

The “Block capacity/size increase” benefit is only in eighth place, as the main improvement is the Malleability Fixes, which permanently solves the problem of transaction malleability, offering efficiency and security to:

- Wallets that keep track of spent bitcoins;
- Anyone who spends unconfirmed transactions;
- Lightning Network;
- Anyone who uses the blockchain and smart contracts.

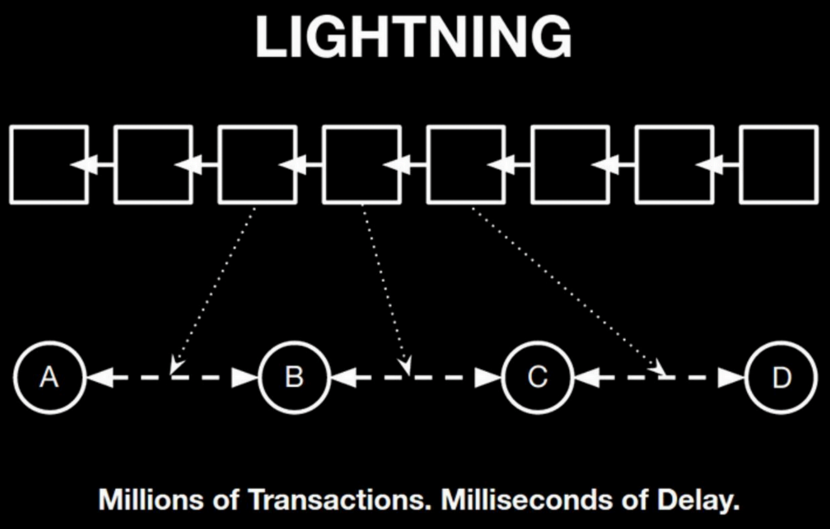
From: bitcoincore.org/en/2016/01/26/segwit-benefits/

LIGHTNING

- The Lightning Network is a decentralized system for instant, high-volume micropayments that removes the risk of delegating custody of funds to trusted third parties

- It is one of the first implementations of a multi-party Smart Contract (programmable money) using bitcoin's built-in scripting.

- lightning.network/lightning-network-summary.pdf



Millions of Transactions. Milliseconds of Delay.

Lightning Network

- The Lightning Network is a second-layer solution that operates on top of the Bitcoin network. The network uses smart contracts to create payment channels between users, allowing them to transact without the need for each transaction to be confirmed on the blockchain.

- This has dramatically increased the number of transactions the network can handle, reducing wait times and fees.

- From: btc.network/blog/how-scalable-is-bitcoin

LIGHTNING BENEFITS

- VASTLY INCREASES TRANSACTION SPEED
- FACILITATES MICROPAYMENTS
- INCREASED PRIVACY
- VASTLY INCREASES TRANSACTIONS PER SECOND

How Lightning Works

- Funds are placed into a two-party, multisignature "channel" bitcoin address.

- This channel is represented as an entry on the bitcoin public ledger.

- In order to spend funds from the channel, both parties must agree on the new balance.

- The current balance is stored as the most recent transaction signed by both parties, spending from the channel address.

- To make a payment, both parties sign a new exit transaction spending from the channel address.

- All old exit transactions are invalidated by doing so.

- https://lightning.network/lightning-network-summary.pdf

What Is Taproot?

- Taproot is an upgrade to Bitcoin which brought several new features and benefits to Bitcoin users. The Bitcoin community activated Taproot at block 709,632 on November 12th, 2021.
- The Taproot upgrade is composed of three Bitcoin Improvement Proposals (BIPs) which define three distinct upgrades to the Bitcoin protocol:
  - Schnorr Signatures (BIP 340)
  - Taproot (BIP 341)
  - Tapscript (BIP 342)
- Together, these three upgrades are known as the Taproot upgrade, often collectively referred to as BIP Taproot. These BIPs introduced new, more efficient, flexible, and private ways of transferring bitcoin.

- From: river.com/learn/what-is-taproot/

TAPROOT/SCHNORR SIGNATURES BENEFITS

- Taproot integrated the Schnorr digital signature scheme into Bitcoin, upgrading Bitcoin's core cryptography.
- Taproot built on the SegWit upgrade to improve Bitcoin's privacy and lower transaction fees.
- Taproot made future Bitcoin upgrades easier by reforming Bitcoin's scripting language.

- From: river.com/learn/what-is-taproot/

ARK (yet to be deployed)

- “Ark can be best defined as trustless e-cash or a liquidity network similar to the Lightning Network but with a UTXO set that lives entirely off-chain and it’s neither a statechain nor a rollup,” Burak said. “These UTXOs are called ‘virtual UTXOs’ or ‘vTXOs,’ which have a ‘lifespan’ of four weeks. The core of Ark's anonymous off-chain payments is driven by the vTXOs.”

- Throughout the conversation, Burak continued to emphasize his obsession with a frictionless experience for the end user, his view being that sending sats should be as easy as pushing a button.

- bitcoinmagazine.com/technical/how-ark-plans-to-scale-private-bitcoin-payments

ARK cont.

- This is one of the reasons why Ark users do not need to have channels or liquidity, as this is delegated to a network of untrusted intermediaries known as Ark service providers (ASPs).

- These are always-on servers that provide liquidity to the network, similarly to how Lightning service providers operate, but with an added benefit: ASPs are unable to link senders with receivers, which adds another layer of privacy for users.

- This is made possible by the fact that every payment on Ark takes place within a CoinJoin round which obfuscates the connection between sender and receiver.

- bitcoinmagazine.com/technical/how-ark-plans-to-scale-private-bitcoin-payments

Thanks for listening!

Feedback always welcome!

Next week, on the last episode of our
Bitcoin’s Sound Money Properties Series
we will discuss how bitcoin is

DISINFLATIONARY/DEFLATIONARY