THE BLOCK · Research

Bitcoin: Beyond the Base Layer

COMMISSIONED BY TRUST MACHINES

Commissioned by Trust Machines

TRUST MACHINES

The mission of Trust Machines is to grow the Bitcoin economy. Trust Machines builds applications, technologies, and infrastructure to make Bitcoin more productive and to extend its use as a decentralized final settlement layer for transactions. Applications are built using smart contracts for Bitcoin, payment channels, and other appropriate technologies. Trust Machines engages in innovative research and development to provide scalability and functionality for applications on Bitcoin.

Researched by The Block Research

THE BLOCK · Research

The Block is an information services company founded in 2018. Its research arm, The Block Research, analyzes an array of industries including digital assets, fintech, and financial services.

Contact

Email: research@theblockcrypto.com
Twitter: @theblockres

Authors

Saurabh Deshpande, Research Analyst
Twitter: @desh_saurabh

Andrew Cahill, Research Director
Twitter: @Andrew_Cahill_

Table of Contents

Section 1: Introduction 5

Bitcoin - A Stable Base Layer 5

Section 2: The Bitcoin-Based Protocol Landscape 10

Payments and Asset Issuance Platforms 11

Bitcoin-based General-Purpose Platforms 15

Section 3: Comparison of Bitcoin-based protocols 20

Technical Comparison 20

Network Data Comparison 21

Fundraising Landscape 25

Section 4: Outlook and Conclusion 27

Catalysts for adoption 27

Challenges for adoption 27

Conclusion 28

Appendix 29

Disclosures 32

Section 1: Introduction

What is Bitcoin? Is it peer-to-peer digital cash? Or a distributed database? Or a darknet currency? Or a global payment and settlement network? Or an uncorrelated financial asset? Or a store of value?

Bitcoin has navigated through a labyrinth of narratives since its birth. But it was meant to be sound money since inception. While Ethereum and other layer-1 networks have rapidly modified their networks to expand the reach of blockchain technology, the Bitcoin community has constantly signaled that Bitcoin's intentionally limited use cases are its defining feature and not a bug. At its base layer, Bitcoin is a secure and global settlement network with a native store of value asset, BTC – that's it.

However, many argue that the durable and decentralized base layer of the Bitcoin network can serve as the bedrock of a much broader range of economic activity. Bitcoin-based protocols that bring scale and programmability on top of this base layer, while thus far limited in adoption, continue to be developed and built on to realize this vision.

> "*Ethereum is roughly $500 billion of network value. But there are $500 billion of applications built on top [of it]. If you look at Bitcoin, it's a trillion-dollar [network] but has very few applications built on top [of it]. In the long run, I don't see a world where it stays that way. I think there is going to be a ton of value created on top of Bitcoin*" - Muneeb Ali, CEO at Trust Machines (CoinDesk Interview, February 2022)

Bitcoin - A Stable Base Layer

Bitcoin's development community has been conservative in pushing changes to its base layer. Modifications to its core protocol take months, if not years, to implement. They are discussed at length to ensure that Bitcoin's core values of decentralization, stability, and security are not traded for more functionality which could result in vulnerabilities within its core technology.

For example, one of the largest Bitcoin upgrades to date, Taproot[1], was proposed as early as January 2018 but not implemented until November 2021 - nearly four years later. Similarly, upgrades like SegWit[2] and Schnorr Signatures[3] took around three and five years, respectively, before they were included in the protocol. Accordingly, initiatives to expand the scalability and use cases of Bitcoin are taking place outside of the confines of its rigid, though stable, base layer.

[1] Taproot was an upgrade aimed at making complex Bitcoin transactions more efficient by reducing data and signature overhead.
[2] Proposed in 2015 and implemented in late 2017, SegWit (Segregated Witness) was a highly debated protocol update that changed the structure of Bitcoin transaction data.
[3] Proposed in 2016 and implemented in late 2021, Schnoor Signatures enhanced Bitcoin's multi-signature functionality to reduce their data footprint on the Bitcoin Blockchain.

Why Go Outside the Base Layer?

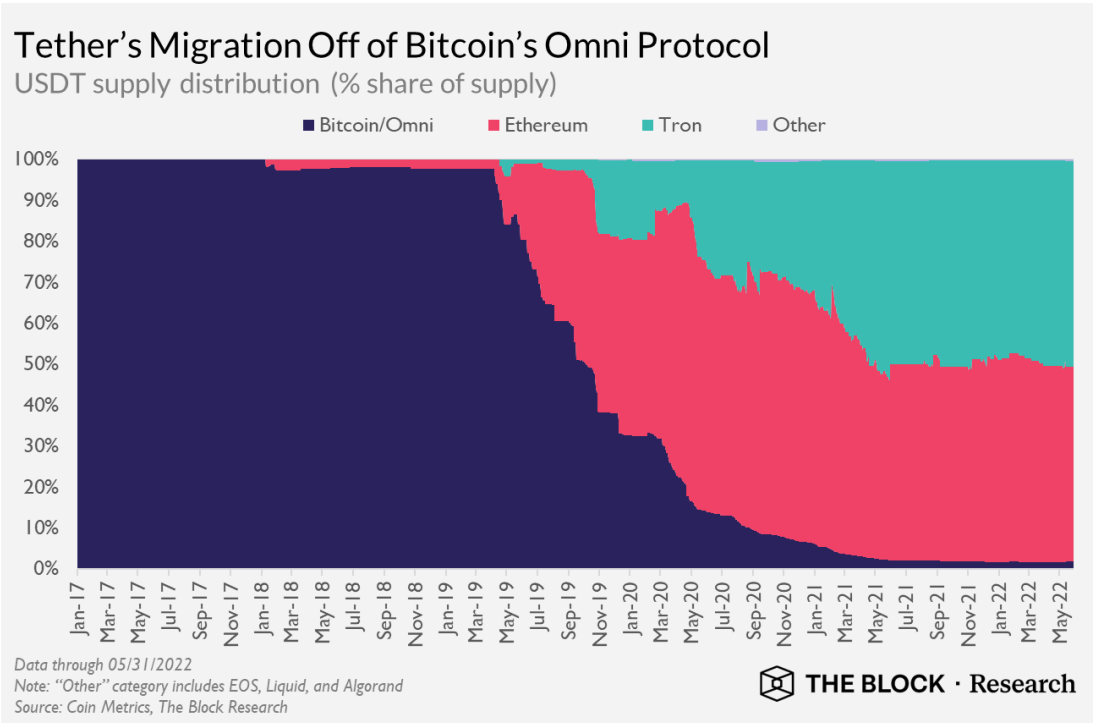
Before analyzing these Bitcoin-based protocols, one must answer the question - "why not just build directly on the base layer?".

Firstly, Bitcoin's scripting language does not support loops or complex flows, making the creation of smart contract logic and, by extension, general-purpose applications directly on its base layer difficult.

Secondly, Bitcoin's 10-minute block time is relatively long compared to Ethereum and other layer-1 blockchains. While block time is only one of the several factors needed to assess a blockchain's settlement time and quality of settlement assurances, Bitcoin's relatively long block time discourages its use in applications that require more rapid transaction confirmations, such as purchasing a cup of coffee.

Finally, fees for individual transactions on Bitcoin are relatively high - the average fee for a Bitcoin transaction was ~$10 in 2021. Many other competing networks' transaction fees are as low as fractions of one cent.

The migration of Tether's US dollar pegged stablecoin, USDT, off Bitcoin's Omni protocol (discussed in section 2 of this report) is one event that showcases these base layer limitations in action. Omni was the leading venue for USDT issuance and transactions through 2017. But following the emergence of Ethereum and alternative layer-1 platforms with larger application bases, faster confirmation times, and (in many cases) lower transaction fees, Omni's share of USDT in circulation has fallen from 100% in 2017 to merely 2% today.



What Benefits Can Bitcoin's Base Layer Provide?

While Bitcoin's rigid base layer has historically created challenges for application development, it also creates unique opportunities for developers and users.

Stability and Security

Bitcoin is the most stable and secure base layer compared to all other blockchain networks. The Bitcoin community's resistance to modifying its core protocol makes it a stable settlement platform. The core set of rules (i.e., proof-of-work consensus, finite supply, a UTXO-based data structure, etc.) that make Bitcoin what it is today are firm and have historically been resistant to change.

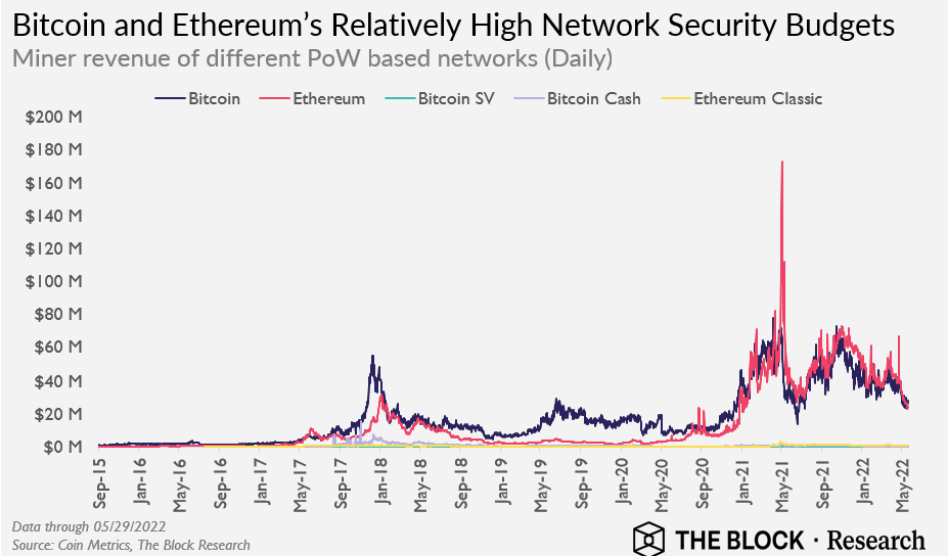
> "*You're going to want to build your buildings on a solid footing of granite, so bitcoin is made to last forever — high integrity, very durable.*" - Michael Saylor, CEO of MicroStrategy (CNBC Interview, June 2021)

This stability stands in stark contrast to Ethereum and other layer-1 networks that frequently modify their base layers to adapt to the pressing needs of their users.

For example, Ethereum recently upended its monetary policy in conjunction with its Ethereum Improvement Proposal (EIP) 1559 upgrade completed in August 2021. In conjunction with "The Merge", its network's underlying security mechanism is transitioning from proof-of-work consensus to proof-of-stake consensus, which will fundamentally alter how the network achieves security. Finally, Ethereum's network architecture is being transformed with the advent of layer-2 scaling solutions. In the future, Ethereum is slated to function primarily as a settlement and data availability layer – not a platform on which applications are directly deployed. So, somewhat ironically, while Ethereum was designed to handle the complexity that Bitcoin was incapable of accommodating, its base layer is set to become simpler over the coming months and years and, ultimately, more closely resemble Bitcoin's base layer.

Bitcoin's reliability is not limited to just how difficult its base layer is to modify. Historically, it has had nearly 100% uptime. This stand in stark contrast to many Ethereum sidechains and alternative layer-1 networks such as Solana, which have suffered attacks and routinely experienced sustained network downtime. Additionally, the cost to attack the Bitcoin blockchain (roughly approximated by total miner revenue in the chart below) through block reorganizations[4] is relatively high compared to other proof-of-work networks. Notably, while Ethereum's miner revenue has achieved parity with or even exceeded Bitcoin's on certain days, its upcoming shift to proof-of-stake introduces a new class of concerns related to the security of its base layer.

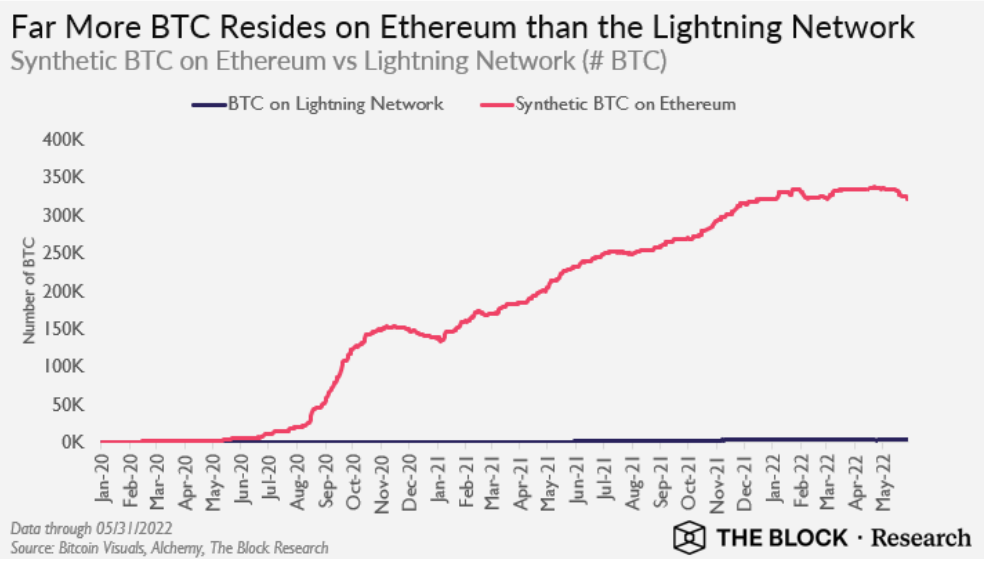
[4] Block reorganizations result in modifications to the previously finalized history of the blockchain.



BTC's Untapped Potential

At a ~$400 billion market cap[5], Bitcoin's native asset, BTC, represents the deepest pool of liquidity within the crypto asset market by a wide margin. Despite the limited functionality of Bitcoin's base layer, investors have already demonstrated a desire to put their BTC to productive use in decentralized finance (DeFi) applications to generate yield or take out crypto-denominated loans.

As displayed in the chart below, the number of BTC bridged to Ethereum (and likely deployed in DeFi applications) far exceeds the number of BTC dedicated to payments on the Lightning Network. However, as discussed later in this report, bridges introduce additional risk factors for users. Therefore, there is likely untapped demand for Bitcoin native applications (i.e., Bitcoin-based DeFi) that allow users to unlock more value with their BTC directly within Bitcoin's established security framework.

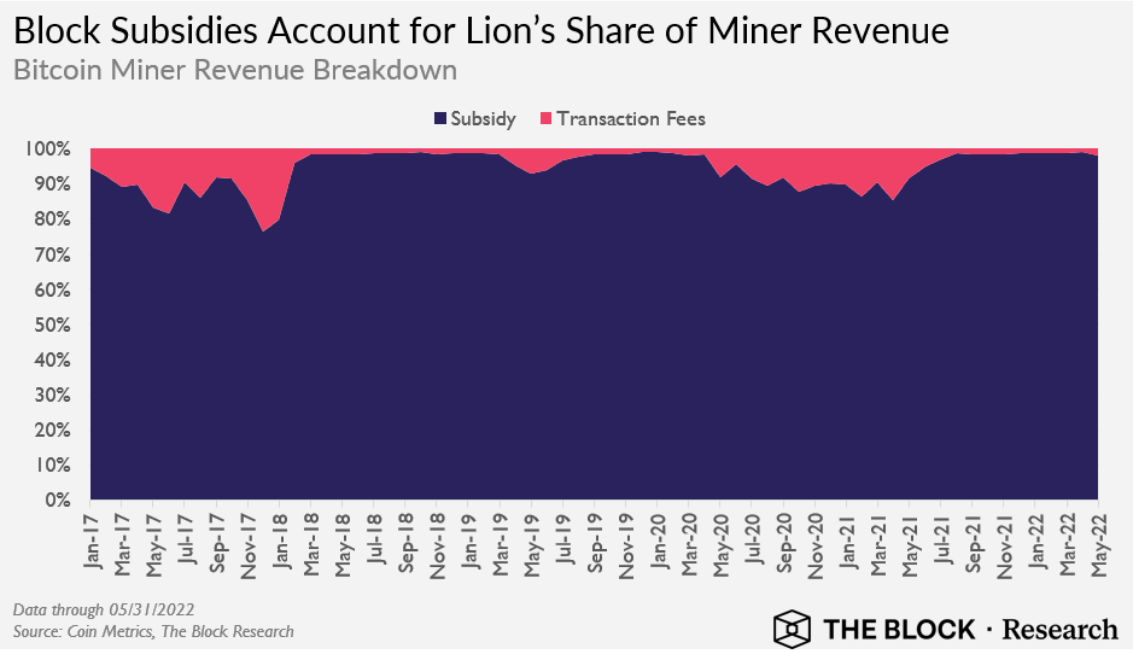


[5] Data as of 6/20/2022

Clearly, developers and users can benefit from Bitcoin-based protocols which leverage its stable base layer security and bring increased functionality. But how do these protocols affect Bitcoin's base layer itself?

A Path to Sustainable Revenues?

It is no secret that Bitcoin miners rely heavily on block subsidies[6] to earn revenue - over 90% of their revenue comes from these subsidies, which are cut by 50% with every halving cycle[7].



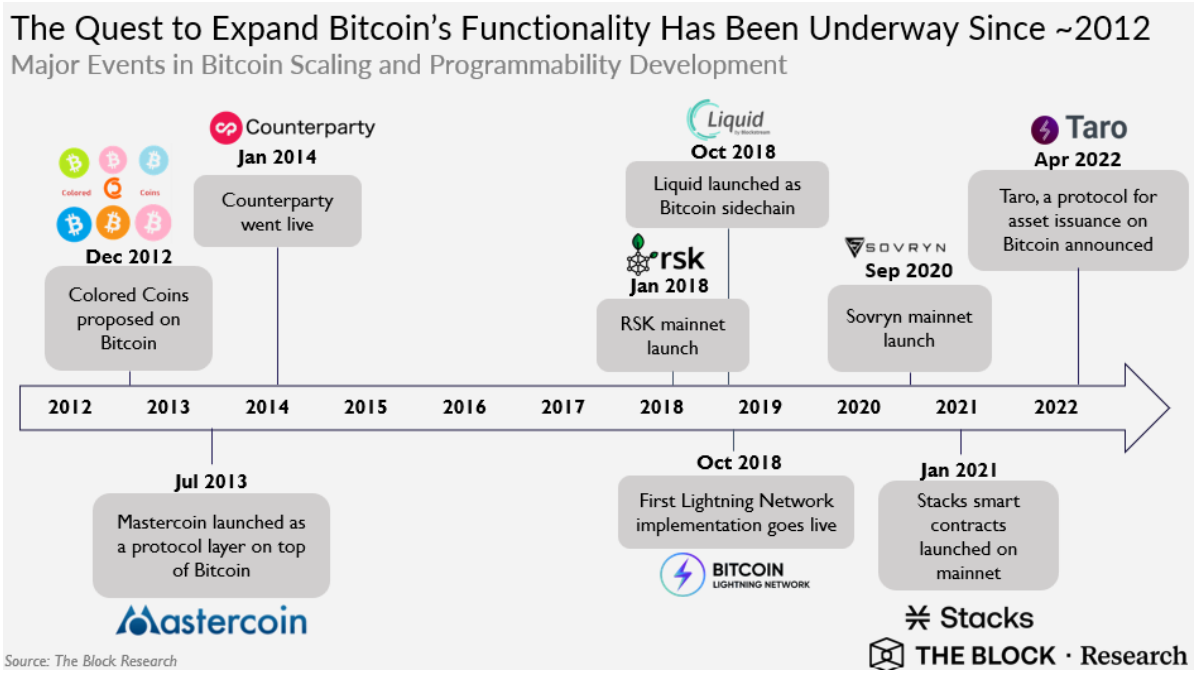
Hence, over the long-term, keeping Bitcoin's security (approximated by total miner revenue in USD) consistent with current levels is dependent on either (i) generating more aggregate transaction fees, (ii) sustained increases in BTC's price, or (iii) a combination of these two factors. For context, if Bitcoin's aggregate transaction fees remain constant, BTC's price must double every four years to keep miner revenue stable.

Bitcoin-based protocols, which increase the networks scalability and utility, are poised to expand its use cases, broaden its user base, and create a larger ecosystem that would generate more aggregate transaction fees - a positive for the network's economic sustainability.

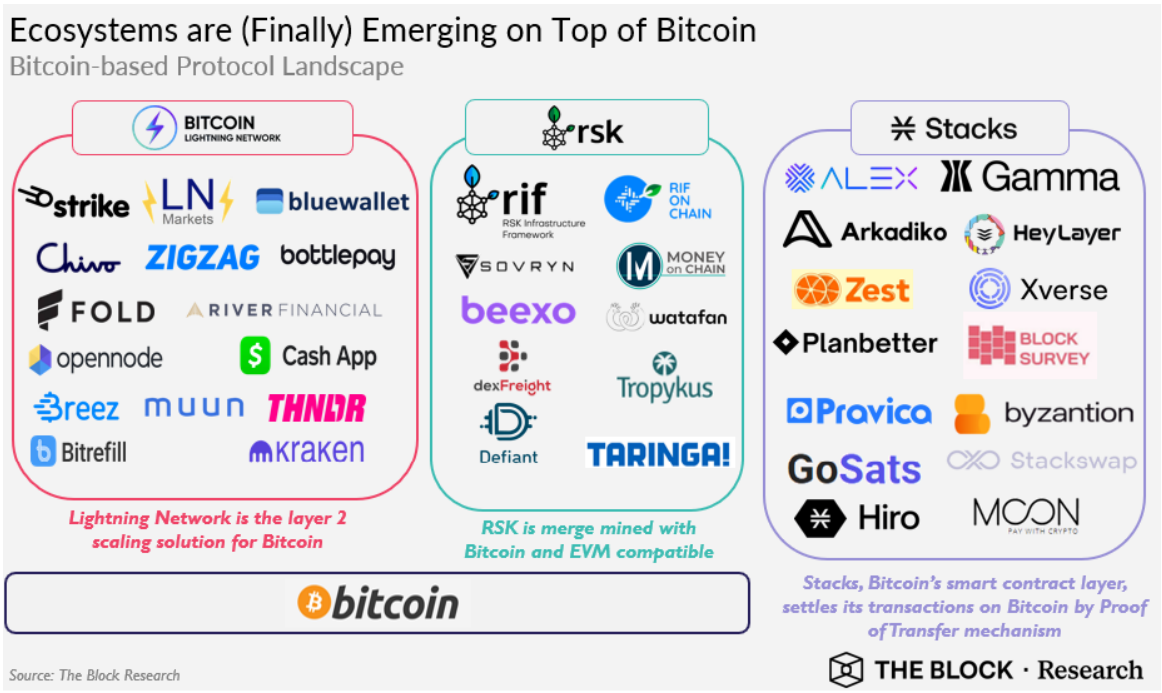
[6] New BTC are issued through block subsidies to miners for performing computational work and mining blocks. The block subsidy is currently 6.25 BTC per block.
[7] As a part of Bitcoin's monetary policy, every 4 years or ~210,000 blocks, Bitcoin's block subsidy halves.

Section 2: The Bitcoin-Based Protocol Landscape

Attempts to bring programmability and scalability to Bitcoin started as early as 2012. As displayed in the timeline below, a new class of Bitcoin-related protocols has since emerged and started to deploy new technologies into production starting in 2018.



A few short years since their mainnet deployments, Lightning Network, RSK, and Stacks have begun to incubate their own respective ecosystems. Major ecosystem participants building on or partnering with these networks are outlined in the graphic below.



Generally speaking, the landscape of projects building on top of Bitcoin span:
(i) protocols scaling payments and asset issuance and (ii) general-purpose networks.

Payments and Asset Issuance Platforms

Early initiatives to scale Bitcoin payments and enable asset issuance include:

- Colored Coins, a concept with different implementations that used the op_return[8] opcode of the Bitcoin protocol to store information about what those BTC represent (proposed in December 2012)

- Omni (formerly Mastercoin), a protocol layer on top of Bitcoin for asset issuance that also leveraged Bitcoin's op_return function (launched in July 2013)

Although prominent at one point, both Colored Coins and Omni have failed to find product-market fit. For the scope of this discussion, our report dives deeper into Lightning Network and Liquid.

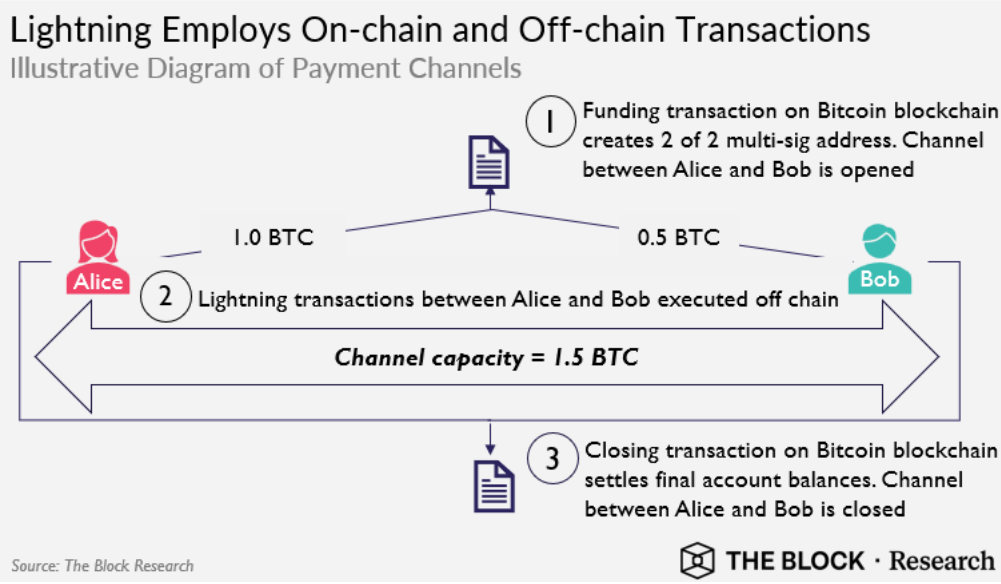
Lightning Network

Lightning Network is a payment channel network built on the Bitcoin blockchain. A payment channel is a mechanism/arrangement that allows users to spend BTC and keep track of balances. Transactions in each channel are recorded off-chain, enabling the network to achieve higher scale and drive down the cost of individual transactions.

How does Lightning Network work?

Lightning Network uses two key features of Bitcoin's limited programmability - multi-signature wallets and timelock transactions to operationalize these channels. Multi-signature wallets require two or more private keys to spend BTC, whereas timelock transactions enable developers to place controls on when coins can be spent (i.e., coins cannot be spent until a certain span of time has passed).

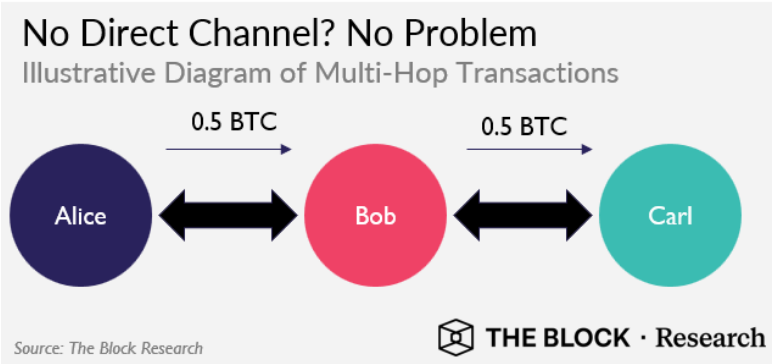
[8] OP_return is a type of Bitcoin transaction different from the standard payment transactions. Its primary use has been to write and store small amounts of data on the Bitcoin Ledger.



Say Alice and Bob want to use Lightning Network for faster BTC payments. They create a 2 of 2 multi-signature address and fund it with desired amounts via an on-chain transaction. The total funded amount is the channel's capacity (i.e., the channel cannot support individual transactions worth more than the channel capacity). Once the channel is created, users can then transfer funds indefinitely by signing off-chain commitment transactions.

If Alice wants to terminate the channel, she can submit an on-chain transaction along with the ledger. Although Bob cannot stop Alice from closing the channel, he can contest her claim by submitting proof of wrongdoing on Alice's part. In case Alice is found to be dishonest, all the funds in the channel are given to Bob.

What happens when users don't have a direct open channel?



Lightning Network allows users to transfer funds to users they are not directly connected with via a channel. For example, if Alice wants to transfer 0.5 BTC to Carl but does not have a direct channel with him, the Lightning Network protocol will chart a path for her payment. Building off the previous example, let's assume that Bob does have an open channel with Carl. In this case, the path would be Alice ➔ Bob ➔ Carl: Alice sends 0.5 BTC to Bob, Bob then sends this 0.5 BTC to Carl. Once Carl receives the payment, he confirms the receipt, and the transaction is complete.

But what if Bob gets the payment from Alice and never forwards it to Carl? This is where time-locked contracts come into the picture. If Carl doesn't confirm receipt of the funds within a pre-defined time, the payment is reverted to the originator, in this case, Alice. Hence, the Lightning Network prevents intermediaries from stealing funds in multi-hop transactions.

What are some of the benefits of the Lightning Network?

By taking execution off Bitcoin's base layer, Lightning Network allows users to use BTC for low value transactions such as purchasing a cup of coffee – which can be impractical directly on Bitcoin's base layer, where fees on individual transactions have historically been as high as ~$10 (average fee in 2021). Users do not need to wait for the expected 10 minutes block time for most merchants to consider their transactions final. Additionally, increased scalability and lower transaction fees (typically a fraction of a cent) not only make for a better user experience but also facilitate the creation of entirely new use cases (e.g., micropayments).

In conjunction with these scaling benefits, development organizations are also expanding the utility of Lightning with support for asset issuance. Lightning Labs, one of the core Lightning Network development organizations, recently announced Taro, a protocol that uses Taproot to bring multiple assets to the Lightning Network with a focus on stablecoins. Networks such as Taro could once again make Bitcoin a major platform for stablecoin issuance and transfer.

What are some of the drawbacks of the Lightning Network?

In order to make transactions on Lightning, users typically need to make at least one on-chain Bitcoin transaction. High Bitcoin blockchain fees can create undesirable upfront costs for users and require them to wait several minutes for Bitcoin's base layer to confirm the transaction before funds can be spent on Lightning.

While the Lightning Network finds the cheapest route for transactions, finding consistent paths can be an issue for larger payments because of a few key constraints. First, the maximum transaction size obviously depends on the capacity of the node initiating the transaction. Second, the timelock contracts mentioned earlier can have limitations on how much BTC they can transfer. Routing nodes set minimum and maximum levels of BTC they can send and receive through timelock contracts. Therefore, finding routing nodes to relay BTC can become challenging in some instances.

The centralization of nodes also poses a potential challenge for the network. With a more centralized node landscape, the network loses redundancy, and some users could be unable to find a connected path. However, well-connected nodes also bring scalability to the Lightning Network.

Liquid

While the idea of the Liquid network was proposed as early as 2015, it was not until October 2018 that it was launched into production by its major development organization, Blockstream. Today, Liquid is a federated network[9] managed by the Liquid Federation, which is comprised of ~60 different entities (list can be found here) spanning cryptocurrency exchanges, trading desks, and infrastructure companies. It is intended to be a scaling solution and a platform for asset issuance.

How does Liquid work?

Although Liquid Federation is comprised of ~60 members, blocks are signed by 15 members, which are referred to as functionaries. When users wish to use Liquid for BTC transactions, they send their BTC to an 11 of 15 multisig address operated by these functionaries and submit the recipient address on the Liquid sidechain (controlled by the same user). The Liquid Federation then issues an equivalent (1:1) amount of L-BTC to the user on the sidechain after 100 confirmations (approximately 16 hours). This process is called peg-in.

Once a user acquires L-BTC, they can transact on the Liquid sidechain, which has 1 minute block time and two block finality (i.e., transactions are considered final after ~2 minutes). When users want to move BTC to the base layer in exchange for L-BTC, they must burn L-BTC, and only functionaries have the authority to burn L-BTC. After a user requests a peg out, Liquid members send their L-BTC to the burn address. Like other transactions on Liquid, the peg-out transaction is confirmed after two confirmations. Peg-out transactions are processed in batches of 20-60 minute intervals.

What are some of the advantages of Liquid?

Liquid has lower block times and allows better scale than Bitcoin. It has a separate global ledger and does not burden the Bitcoin blockchain with general data.

What are some of the drawbacks of Liquid?

One of the drawbacks of Liquid is that it does not support general-purpose applications. While it allows for asset issuance, the market has not yet signaled a strong need for issuing different assets on Liquid.

Compared to Bitcoin's base layer, Liquid's consensus mechanism is highly centralized. While only 15 functionaries sign transactions on Liquid, Bitcoin has thousands of globally distributed miners competing to propose new blocks and form a consensus. We have seen several

[9] In a federated network, a pre-defined set of entities are authenticated and approved to participate in the network consensus. This stands in contrast to permissionless networks such as Bitcoin where theoretically anyone with access to the requisite computer hardware can participate in consensus

examples, such as the exploits of Ronin[10] and Wormhole[11] bridges, in which these centralization risks have manifested into major misappropriations of user funds. Additionally, bridging funds to Liquid can be cumbersome for users - they typically[12] must wait for around 17 hours for bridged assets to be released on Liquid.

Moreover, the network's key development organization, Blockstream still wields significant influence in the operation of the network. While Blockstream has stated that it is working on integrating a dynamic federation system to reduce its influence, it still has custody over emergency keys which it can use to refund users if the network is inactive for an extended period.

Finally, given the low level of activity and, by extension, the low transaction fees it currently generates, miners (Liquid Federation Functionaries) have little explicit financial incentive to participate in securing the Liquid network. This concept will be further explored in Section 3 of this report.

Bitcoin-based General-Purpose Platforms

While the aforementioned protocols aim to enhance scalability and facilitate asset issuance, others are developing general-purpose networks (capable of executing any program that Ethereum can) to also expand the use of Bitcoin to an unbound number of disciplines.

Counterparty was among the first protocols to try to bring programmability to Bitcoin. It used the op_return space to create a platform to issue and trade assets on Bitcoin. However, similar to Colored Coins and Omni, its reliance on op_return has resulted in serious limitations, and the network has failed to achieve significant adoption. Accordingly, this section focuses on RSK and Stacks and how they try to bring programmability to Bitcoin without burdening it with general data.

RSK

RSK by Rootstock is an attempt to bring functionality to Bitcoin in the form of a Turing complete and Ethereum Virtual Machine (EVM) compatible sidechain. Like Liquid, RSK does not have its own native currency. It uses smartBTC (RBTC), which is issued against BTC locked on Bitcoin and used to pay transaction fees on RSK.

[10] Ronin is an Ethereum sidechain that powers the Axie Infinity blockchain-based video game. In March 2022, it was exploited for ~$600 million when hackers were able to gain access to 5 out of 9 private keys used to sign transactions.
[11] Wormhole is a communication bridge between Solana and several other layer-one blockchains. In February 2022, it was exploited for ~$325 million worth of ETH. Wormhole has 19 guardians and demands a 2/3rd majority to mint/burn tokens. The attack was carried out by bypassing the signature verification from guardians.
[12] Exchanges may maintain L-BTC liquidity on Liquid and release it to users. But how much liquidity exchanges must keep depends on the adoption of Liquid, and it's not significant as of now.

How does RSK work?

Like Liquid, RSK has the concept of peg-in and peg-out bridging. RSK's PowPeg Federation is responsible for issuing RBTC on RSK for every BTC deposited by users in RSK's designated multisig address. For the peg-in, the SPV[13] on RSK detects the incoming transaction, and PowPeg releases equivalent RBTC on RSK after 100 Bitcoin blocks (approximately 16 hours). The PowPeg nodes sign the release transaction when they detect an incoming transaction to a special bridge address from an RSK address. To avoid centralization, the peg-out relies on PowPeg's Hardware Security Module (HSM), wherein these nodes do not have access to private keys and, therefore, cannot steal funds. The peg-out transaction is released within 4,000 RSK blocks or ~33 hours after the outgoing transaction is triggered.

Like Liquid's federation, RSK's PowPeg federation introduces a degree of centralization and additional risk for users when bridging funds.

Merge Mining

RSK is secured through merge mining with Bitcoin. With merge mining, Bitcoin miners have the option to simultaneously mine RSK blocks along with Bitcoin blocks. Because RSK does not have a separate native asset, it cannot offer block subsidies to miners - transaction fees generated on RSK compensate them for their services. Currently, ~80% of transaction fees generated on RSK platform go to miners while the rest go to other stakeholders, such as IOV Labs, one of its major development organizations.

One of the advantages of mining on RSK is that Bitcoin miners can earn fees from RSK without incurring much additional cost (i.e., incremental bandwidth and storage costs to mine RSK blocks). Currently, ~50% of Bitcoin's hash rate is merge mining RSK. Per RSK mining estimates, Bitcoin miners could collectively earn approximately ~$100k per month[14] by merge mining RSK (assuming 50% of Bitcoin's hash rate merge mines). As long as miners' earnings from RSK are greater than storage and bandwidth costs, rational miners should mine the RSK chain.

Along with RSK, IOV Labs has a complementary platform, RSK Infrastructure Framework (RIF). RIF builds infrastructure such as wallets, marketplaces, and gateways which are critical for giving users access to applications built on RSK. Although RSK doesn't have a token, the RIF Open Standard applications will be accessed through the RIF token. Whether this token will be used to incentivize development on RSK is unknown at this point.

What are some of the benefits of RSK?

Given its EVM compatibility, developers can easily port over existing applications from Ethereum to RSK. For example, Aave, leading lending and borrowing protocol originally built on Ethereum, is in the process of deploying on RSK.

[13] SPV stands for Simplified Payment Verification, and it is a method that allows users to validate their transactions without running a full node.
[14] Assuming a price of $30,685 per BTC

Additionally, RSK's more rapid block time, ~30 seconds compared to Bitcoin's 10 minutes, allows for more rapid transaction settlement.

Finally, on the security front, RSK directly benefits from Bitcoin's battle-tested security infrastructure through merge mining. With the exception of the risks introduced through its pegging process, transactions executed on RSK come with relatively high security assurances due to this merge mining.

What are some of the drawbacks of RSK?

RSK can process ~11 transactions per second (TPS)[15], which can be seen as a major bottleneck for building scalable applications. This TPS only represents a marginal improvement over Bitcoin's 3 – 7 TPS. Although the RSK community is exploring different ways to scale throughput, they are all at very early stages and may take a long time to be live in production.

Transaction fees on RSK will always be paid for with RBTC. However, RIF tokens are required to pay for applications built by RIF – thus creating friction for users by potentially requiring them to hold multiple tokens to make transactions on the network.

Although more than one entity facilitates peg-in and peg-out transactions, similar to Liquid, RSK has an emergency backup mechanism (a 3 of 4 multisig) if the hardware fails. If one has to custody BTC with well-known entities, doing so via the wrapped Ethereum versions would provide far more avenues than RSK, as the latter ecosystem is significantly smaller than the former.

Stacks

Stacks, formerly known as Blockstack, started with a vision of developing a full stack of Bitcoin-based decentralized applications. In October 2020, Blockstack underwent a rebrand to Stacks and launched its smart contract layer on mainnet in January 2021.

In all the previously listed ways, aspiring smart contract platforms or projects have connected to Bitcoin in a manner that encumbers them. Reliance on Bitcoin's op_return space has created challenges for Colored Coins, Mastercoin, and Counterparty and stifled adoption. Liquid has limited functionality and a centralized peg-in and peg-out mechanism. RSK has relatively centralized peg-in and peg-out mechanisms, low throughput, and limited ability to incentivize development as it does not have its own native token.

How does Stacks work?

Stacks is a smart contract layer for Bitcoin tethered to it via a cross-chain consensus mechanism. It connects to Bitcoin by embedding the hash of its state into every Bitcoin block. Stacks miners earn block rewards that are comprised of subsidies in STX, Stacks' native token, and transaction fees from the platform. Like Bitcoin, Stacks' monetary policy implements a declining block subsidy schedule which halves every four years until the block reward is 125

[15] RSK has a block time of 30 seconds with 6.8 million gas limit per block. A basic RBTC transfer transaction consumes 21,000 gas. Therefore, its estimated theoretical throughput limit is ~10.79 (6,800,000/21,000/30)

STX[16].

Proof of Transfer Mining

Stacks devised a novel way of being tethered to Bitcoin yet unencumbered by its limitations. Stacks is tethered to Bitcoin by a proof of transfer (PoX) mechanism. PoX is a cross-chain consensus mechanism in which both chains, Bitcoin and Stacks, are involved in forming agreement on the network. PoX is similar to Bitcoin mining, but instead of burning energy, a miner spends capital denominated in proof-of-work coins, in this case BTC, to gain the right to mine blocks and earn rewards. PoX transfers the coins of the established chain to the new chain's token holders, who opt into the chain's consensus. In the case of Stacks, miners transfer BTC to users who stake STX and receive STX block rewards in exchange.

Simply put, miners who wish to mine a Stacks block must send BTC commitment transactions on the Bitcoin network. One of the miners is selected by Stacks via a verifiable random function, and this miner must produce a Stacks block. The BTC sent by all bidding miners is distributed among those who lock capital or stack STX, and some BTC is burned (however, alternatives to burning BTC, such as using these funds for Bitcoin development, are being considered). Essentially, miners get STX (block subsidies and transaction fees) in exchange for transferring BTC to produce blocks. Stackers get BTC from miners for locking STX capital. Accordingly, miners only have an incentive to mine when the dollar value of the STX they receive exceeds the value of the BTC that they transfer.

Stacks block producers produce two types of blocks – (i) anchor blocks which are used to tether Stacks to Bitcoin for finality, and (ii) microblocks which are used to power applications that need lower latency.

Microblocks allow rapid transactions with a high degree of confidence, and are confirmed when the subsequent anchor block is mined. Moreover, In February 2022, Stacks announced Hyperchains, a scalability layer designed for increased throughput. While there can be multiple hyperchains with various trust assumptions, Hiro, an organization that supports building Bitcoin applications, has proposed an approach that starts with trusted federated hyperchains that gradually become trustless.

How are Stacks applications coded?

Stacks designed Clarity, a non-Turing smart contract language used to code applications built on Stacks. As it is not Turing complete, it has two main differentiating factors vs. Ethereum's flagship smart contract language, Solidity. Firstly, it allows developers to calculate the gas fee before transaction execution. Secondly, it allows static analysis that determines all the execution paths beforehand, ensuring that developers understand the other contracts invoked by a transaction which can help identify potential bugs.

Clarity smart contracts also have visibility into Bitcoin's state, unlocking a few innovations explained later in the report. The downside of non-Turing complete language is that it can limit developers by not supporting certain forms of recursion and looping. Despite these

[16] The current block reward is 1000 STX per block

minor limitations, Clarity is far more expressive than Bitcoin Script – among other use cases, it has already been used to build automated market makers (AMMs) on Stacks.

What are some of the benefits of Stacks?

Although it uses the Bitcoin blockchain, Stacks' consumption of Bitcoin's bandwidth is relatively low. For every Stacks anchor block, the number of Bitcoin transactions is limited to the number of miners sending a commitment transaction indicating their candidacy. Thus, activity on Stacks generates few Bitcoin transactions, which are unlikely to result in congestion of Bitcoin's base layer.

Given its novel economic design and STX token, the protocol has explicit financial incentives for miners to participate in the network and mine microblocks. Therefore, Stacks can post thousands of transactions between two Bitcoin blocks, materially improving its scalability.

What are some of the drawbacks of Stacks?

Being relatively new in production, Stacks lacks the network effects of Ethereum and other EVM-compatible blockchains. It lags Ethereum on various fronts such as developer and user traction, infrastructure availability such as wallets, liquidity, number of consumer-facing applications, and influencer networks. Stacks must overcome these barriers if it is to compete as a viable Bitcoin-native alternative to Ethereum.

Stacks has been in development for the last few years but has not been able to gain developer and user traction on par with layer-1 competitors, such as Solana and Avalanche. This could be because it had to pivot away from its earlier model of building directly on top of Bitcoin, launching a separate layer connected to Bitcoin. Stacks has to fight for intellectual capital in the industry to ensure that high-quality consumer-facing applications are built on the platform.

Section 3: Comparison of Bitcoin-based Protocols

Technical Comparison

When comparing protocols built on top of Bitcoin, several distinctions are worth highlighting. Chief among these are where data is stored, how Bitcoin is leveraged for settlement, how BTC is ported to the solution, and how miners/nodes are incentivized.

A "Look Under the Hood" of Bitcoin-Related Protocols

Comparison of Bitcoin-Based Protocols

Project	Purpose	Separate Ledger for Data Storage?	Settlement Assurance	BTC Usage	Miner/Node Incentivization
Counterparty	Asset Issuance, Trading	No	Bitcoin	Bridged	Transaction Fees
Bitcoin Lightning Network	Scaling, Payments, Asset Issuance (1)	Yes	Bitcoin	Native	Routing Fees
Liquid	Scaling, Asset Issuance, Payments	Yes	Liquid	Bridged	Transaction Fees
Omni	Asset Issuance, Payments, Escrow	No	Bitcoin	Bridged	Transaction Fees
rsk	General Purpose	Yes	RSK	Bridged	Transaction Fees
Stacks	General Purpose	Yes	Stacks, Bitcoin	Native & Bridged	Transaction Fees, STX Block Reward

Notes: (1) Lightning Network recently announced plans to add functionality for asset issuance on Lightning
Source: The Block Research

THE BLOCK · Research

Separate Ledger for Data Storage

Every protocol that extends Bitcoin's capabilities stores some data on Bitcoin's base layer. Having an additional layer, apart from Bitcoin, that can store the global state is vital for some applications. Storing all of this data on Bitcoin is not optimal given its block size constraints. In this light, it makes sense for smart contract platforms to have a separate global ledger that can store all the data that applications might need. Liquid, RSK, and Stacks can store data in separate global ledgers.

Counterparty and Omni do not have a separate data storage ledger and store transaction data in Bitcoin's op_return space. Liquid and RSK store only peg-in and peg-out transaction data on Bitcoin; the rest is stored on their respective chains. Lightning Network posts channel opening and closing data on Bitcoin while the information about transactions remains off-chain with respective channels. Stacks' mechanism for storing state on Bitcoin can be thought of as checkpointing. While the data related to Stacks transactions between two Bitcoin blocks are stored on Stacks, a compressed version of the new state is stored on Bitcoin. Regardless of the number of transactions on Stacks between two Bitcoin blocks, the size of information it stores on Bitcoin remains more or less the same. Thus, Stacks promises scale along with Bitcoin's settlement guarantees.

Settlement Assurances

Naturally, where the state of these protocols is stored has consequences for their relative settlement assurances. Storing state on Bitcoin's base layer gives a protocol Bitcoin's settlement guarantees. Because Counterparty and Omni store everything on Bitcoin, their settlement occurs on Bitcoin by default. Similarly, Lightning channels' balances are settled on

Bitcoin following the closure of payment channels. Stacks finalizes microblocks between two Bitcoin blocks and stores all the related information. When a new Bitcoin block is mined, Stacks stores the hashed version of these intermediate state changes effected by microblocks onto Bitcoin, thus settling on Bitcoin.

BTC Usage

Today, most bridge constructions involve trusted intermediaries who have custody over bridged BTC and issue wrapped versions of BTC on other blockchains. RSK and Liquid use peg-ins and peg-outs wherein BTC are technically locked in multisig addresses on the Bitcoin blockchain operated by reputed entities. Projects like Lightning Network and Stacks allow the use of native BTC so that there is no need for a trusted party to take BTC to a more efficient layer. When smart contracts on a separate blockchain can read and verify Bitcoin transactions, the fundamental need to transfer BTC to the separate blockchain does not arise. However, this design could have performance overhangs because when a smart contract on a non-Bitcoin blockchain has to wait for triggers by Bitcoin transactions, it needs to wait for the Bitcoin block to be mined, which is an expected time of 10 minutes at any given point.

While Lightning enables atomic swaps, which involve on-chain and off-chain swaps, Stacks uses a combination of native BTC and smart contracts on Stacks to execute swaps. Because the swaps involve two chains, Bitcoin and Stacks, they are called Catamaran swaps. Clarity smart contracts on Stacks can read the Bitcoin state, which helps them check whether a transaction took place on the Bitcoin blockchain. A Stacks based swap includes three transactions:

1. Sending a Stacks based asset to an escrow smart contract
2. Transferring BTC to the recipient's address
3. Once the Clarity smart contract verifies the BTC transfer, releasing the Stacks based asset

In addition to native swaps, Stacks also provides a way for users to bridge BTC through custodial services akin to wrapped BTC on Ethereum. These derived assets, such as xBTC, live on the Stacks chain and function similarly to WBTC on Ethereum.

Miner/Nodes Incentivization

Protocols that store data on-chain pay fees to Bitcoin miners to include the information in blocks. In the case of protocols where transactions take place off-chain, every protocol under consideration, barring Counterparty and Omni, needs additional miner incentives to facilitate ledger updates. Lightning Network pays node operators routing fees. RSK and Liquid reward miners by sharing transaction fees, and Stacks incentivizes miners with STX block subsidies and transaction fees.

Network Data Comparison

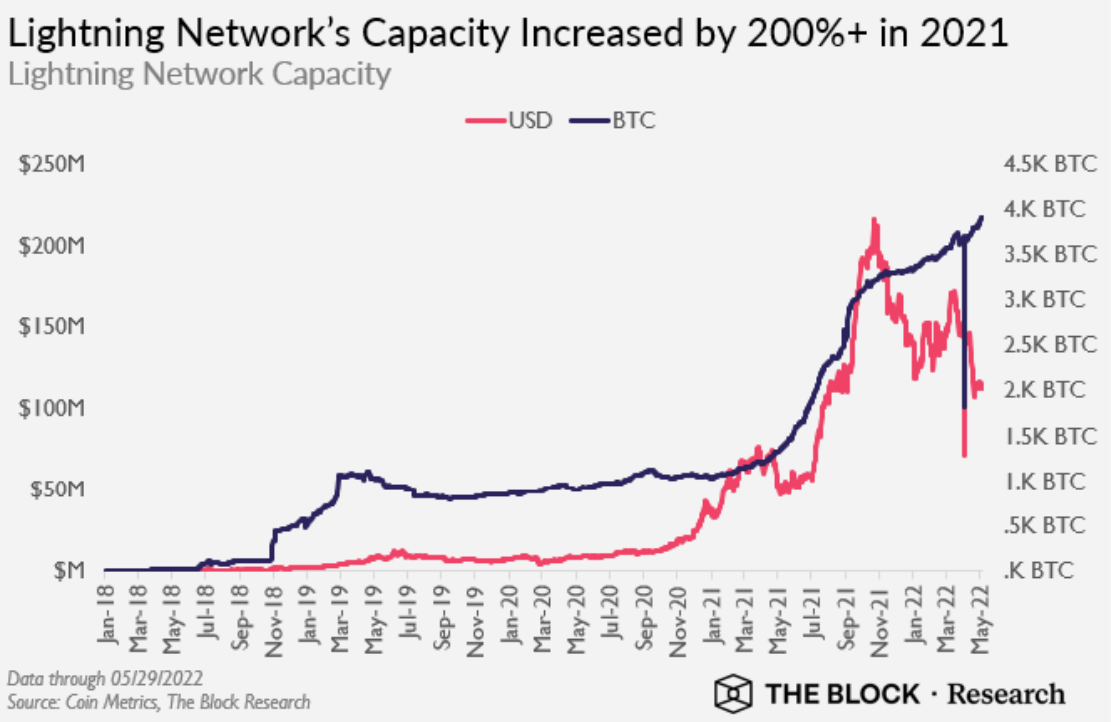
The following section of the report presents several data series that capture the current state of adoption and investment into Bitcoin-based protocols.

Data collection methodology - The Block Research requested the following metrics from Liquid, RSK Labs, and Stacks Foundation in this report: (i) daily transaction counts, (ii) daily active addresses, (iii) daily aggregate transaction fees, and (iv) number of nodes/validators over time. Any data provided by these organizations were included in the following section, along with any publicly available data.

Lightning Network

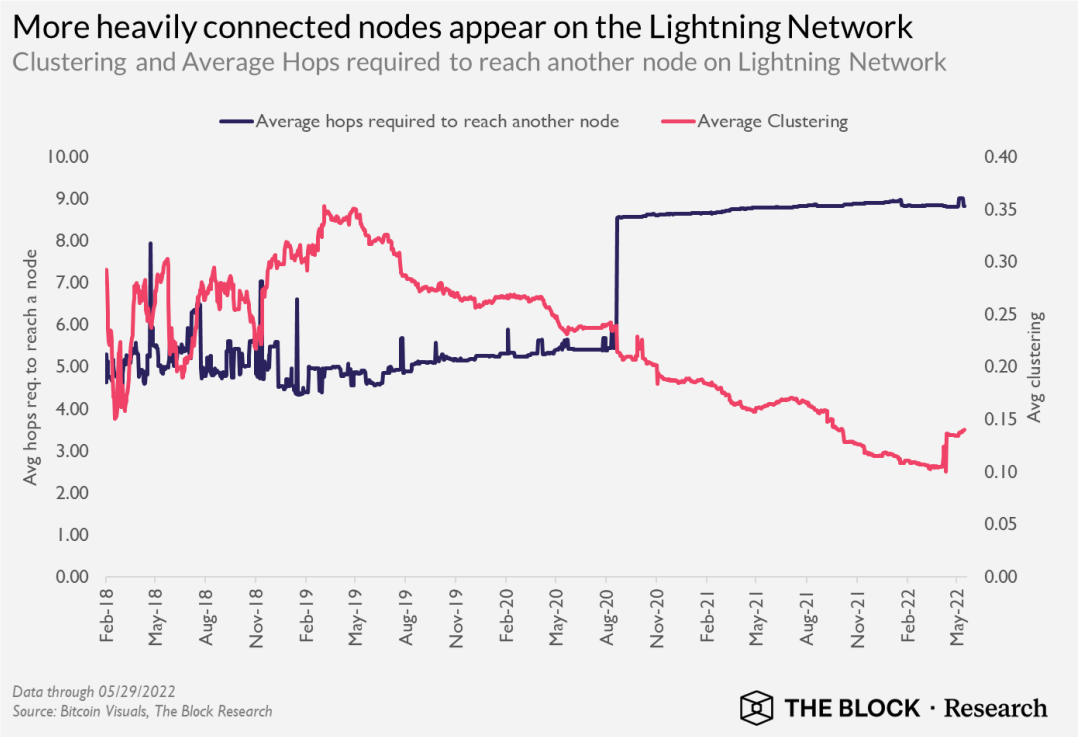
As Lightning Network doesn't have a global ledger, it is difficult to know the number of users and volume of transactions passing through all channels. While estimates of these figures can be generated by surveying active nodes that route a significant load of transactions, this report focuses on publicly available data on Lightning Network.

In 2021, Lightning Network's capacity more than doubled in BTC terms. At the time of writing, approximately $200 million worth of BTC was deposited into multi-sig wallets and spendable (at any one time) across Lightning Network.



As the Lightning Network has increased in popularity, a few nodes have become vital to connecting peers across the network, reducing the clustering coefficient[17] and increasing the number of hops required to reach the desired node. Although this implies increased centralization, in theory, it doesn't materially hamper the network as long as some crucial nodes are online.

[17] The Lightning Network's clustering coefficient measures the degree of node connectivity. A node with a clustering coefficient of 0 implies that it is a hub, and none of its neighbors are connected to each other. When a clustering coefficient is 1, it implies that all its neighbors are connected to each other.

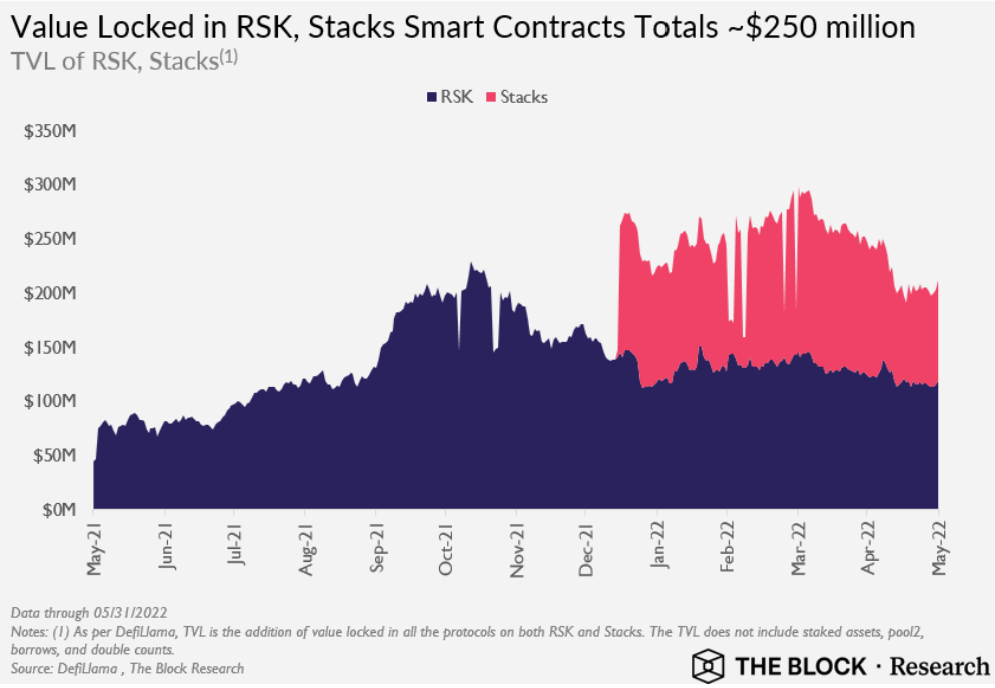


Liquid Network

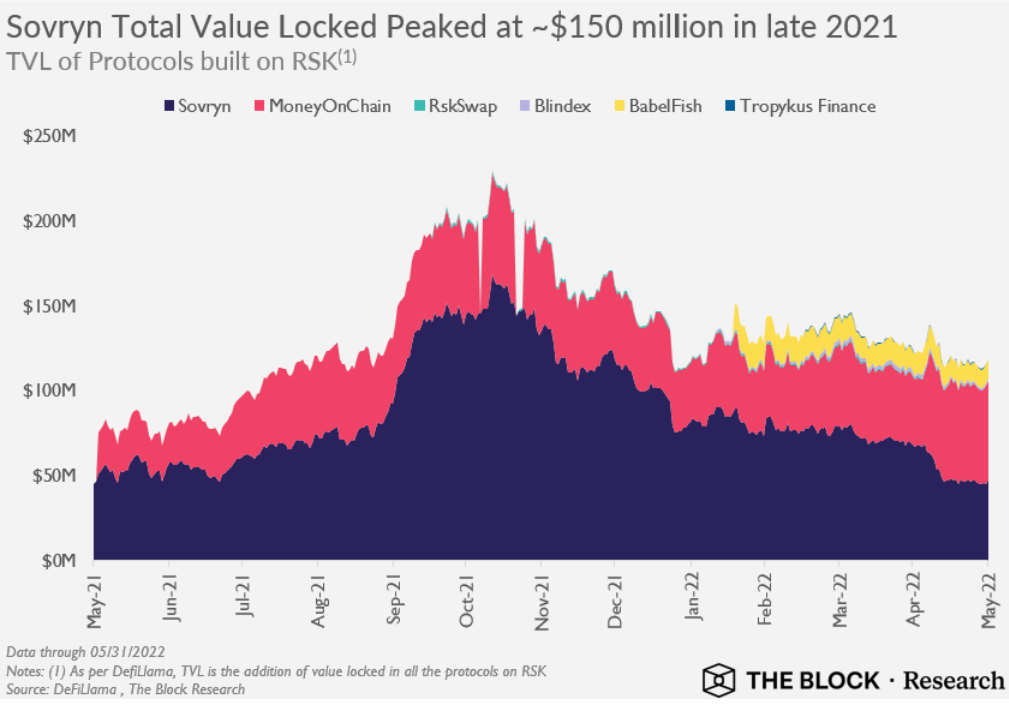
While aggregated network data from Liquid is not publicly available, the Liquid block explorer showcases relatively low levels of activity with 1 to 4 transactions per block. Like Lightning Network, the number of BTC bridged to Liquid is far lower than the number bridged to Ethereum (~4K BTC has been bridged to Liquid vs. ~270k BTC bridged to Ethereum).

RSK and Stacks

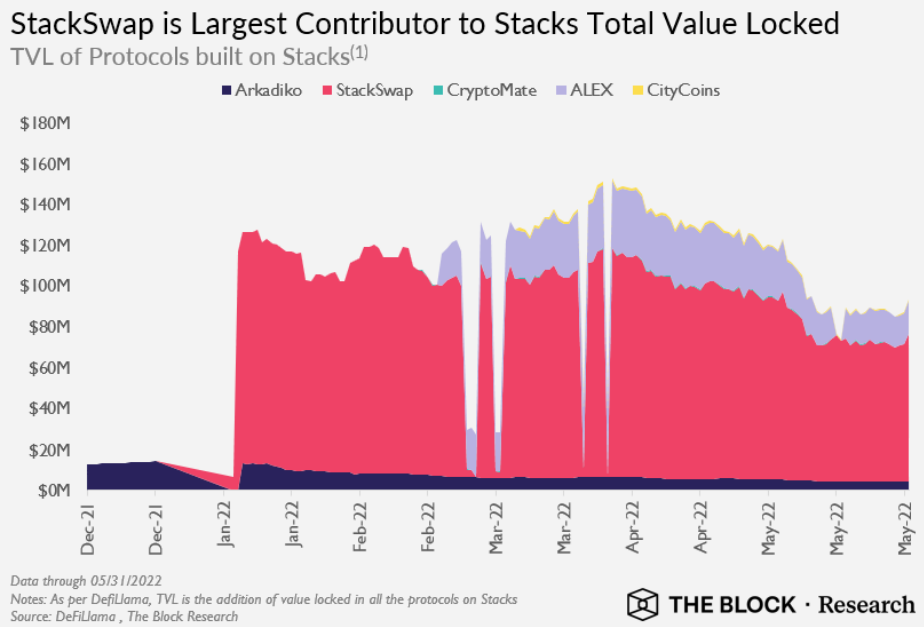
Stacks' smart contracts were launched in early 2021, and total value locked (TVL) started increasing after applications such as native-BTC swaps enabled by Catamaran swaps and NFTs went live in early 2022.



RSK has $115 million in total value locked as of May 31, 2022. Approximately $50 million is in Sovryn, a DeFi platform built on RSK. Sovryn has three layers. First is the infrastructure layer – an operating system for developers who want to use Bitcoin layer-2. This layer includes tooling solutions and bridges to other protocols such as Binance Smart Chain and Lightning Network (more to be added in the future). Second is the Sovryn core layer, which manages governance, core trading/lending primitives, etc. Finally, it has an ecosystem layer where other applications can build and integrate into Sovryn.



Stacks has around $94 million worth of total value locked[18], out of which $72 million is in StackSwap, a DEX and token launchpad that went live in January 2022.



Fundraising Landscape

Many of the aforementioned protocols are striving to build antifragile, decentralized architectures similar to Bitcoin. However, given the early stage of these networks, centralized organizations require funding to direct protocol development and ecosystem growth.

Blockstream, Lightning Labs, Hiro Systems (Stacks), and Trust Machines are among the most well-funded organizations in the Bitcoin ecosystem that have recently raised. Fundraising by these firms picked up considerably in late 2021 and into 2022 - recent funding rounds surpassed aggregate funding raised in prior years.

Apart from Liquid, Blockstream has built wallet infrastructure and is involved in Bitcoin mining. Lightning Labs is building Lightning Network based financial infrastructure. As mentioned in the previous section, Stacks is a smart contract layer for Bitcoin. Founded in February 2022, Trust Machines aims to be the Consensys of Bitcoin, and build all the necessary infrastructure for catapulting the adoption of Bitcoin-based applications.

[18] In addition to this, ~$180 million is locked in STX staking contract earning BTC yield

Recent Fundraises: Lightning Labs, Trust Machines

Bitcoin-focused Development Organizations Fundraising ($ millions)

Organization	Date	Round	($MM)	Select Investors
	Blockstream			
Blockstream	Nov-14	Seed	$ 21.0	Khosla Ventures, Real Ventures
Blockstream	Jul-15	Seed extended	*Undisclosed*	Acequia Capital
Blockstream	Feb-16	Series A	$ 57.0	Horizon Ventures
Blockstream	Nov-17	Funding Round	$ 11.0	Digital Garage
Blockstream	Aug-21	Series B	$ 210.0	Ballie Gifford, Bitfinex
Total Funding			**$ 299.0**	
	LIGHTNING LABS			
Lightning Labs	Mar-18	Seed	$ 2.5	Digital Currency Group, The Hive
Lightning Labs	Feb-20	Series A	$ 10.0	Craft Ventures, Slow Ventures, Others
Lightning Labs	Apr-22	Series B	$ 70.0	Valor Equity Partners, Others
Total Funding			**$ 82.5**	
	rsk			
RSK Labs	Jan-16	Angel	$ 0.4	Coinsilium
RSK Labs	Mar-16	Seed	$ 1.0	Digital Currency Group
RSK Labs	Mar-17	Extended Seed	$ 2.4	Digital Finance Group
RSK Labs	May-17		$ 3.5	Bitfury, Bitmain
Total Funding			**$ 7.3**	
	Mastercoin			
Mastercoin/Omni	Jul-13	Crowdfunding	$ 0.5	
Total Funding			**$ 0.5**	
	Stacks			
Hiro Systems	Dec-17	Reg D	$ 47.5	Union Square Ventures, Foundation Capital, Others
Hiro Systems	Sep-19	Reg A+	$ 23.0	Union Square Ventures, Others
Trust Machines	Feb-22		$ 150.0	Union Square Ventures, Breyer Capital, Others
Total Funding			**$ 220.5**	

Source: Crunchbase, Company blogs, The Block Research

THE BLOCK · Research

Section 4: Outlook and Conclusion

While efforts to expand Bitcoin's use cases have been ongoing for nearly a decade, they have seen relatively low levels of adoption to date. However, several catalysts are poised to accelerate Bitcoin-based application development.

Catalysts for adoption

Maturing Infrastructure

Organizations with a focus on Bitcoin have been making strides in building Bitcoin-based infrastructure. Recent examples include Lightning Labs announcing asset issuance on Lightning Network and a BTC collateralized stablecoin. Lightning Network has made significant headway in emerging markets and has been driving BTC payments adoption.

Trust Machines' $150 million fundraising is encouraging for continued improvement of Stacks' core technology. Startups in the Stacks ecosystem, such as Superfandom, Arkadiko, Gamma, and others like Sovryn in the RSK ecosystem, are actively employing these Bitcoin-based protocols today.

Furthermore, Block (formerly known as Square) has announced plans to build a Bitcoin-focused decentralized exchange. Given Block's large user base, successfully executing such an initiative could be a major catalyst for adoption.

Launching Developer Incentives

Explicit financial incentives geared towards attracting developers and users have been effective in bootstrapping ecosystem growth. In March 2022, Stacks Foundation, Okcoin, Digital Currency Group, and GSR announced a $165 million ecosystem fund, 'Bitcoin Odyssey,' focused on investing in applications that drive BTC adoption.

Evolving Mining Incentives

Miners are a vital part of the Bitcoin ecosystem. Mining schemes such as RSK's merge mining have the potential to boost miners' bottom line with minimal required investment from miners. Similarly, novel consensus mechanisms, such as Stacks' proof of transfer, do not require upfront investment in computationally intensive mining hardware – they have the potential to democratize participation in Bitcoin-based protocol operation.

Despite the emergence of these catalysts for adoption, there are several challenges that these protocols need to overcome in order to reach higher levels of adoption.

Challenges for adoption

Competition from Ethereum and other layer-1 blockchains

Ethereum and other layer-1 platforms have been optimized for general-purpose applications since their inception. Hence, their user experience remains superior to many Bitcoin-based solutions, which have far less tooling support. Wallet integrations and supporting

infrastructure for Bitcoin-based solutions need to improve to match the experience of alternative layer-1 networks.

Centralization remains a critical risk for Bitcoin-based protocols

It can be argued that bridging BTC to chains like RSK, Liquid, and Stacks exposes users to many of the same risks they assume when bridging BTC to Ethereum. Accordingly, given Ethereum's extensive ecosystems of applications and tooling, it will likely remain an attractive platform for putting BTC to productive use in DeFi. However, this is gradually changing with Lightning Network announcing asset issuance and Stacks' mechanism of using BTC natively.

Bitcoin's Stable Base Layer Can Create Development Challenges

Certain protocols building on Bitcoin could benefit from modifications (e.g., adding support for zero knowledge proof verification) to its base layer. These base layer limitations could preclude some Bitcoin-based protocols from achieving their full potential. In fact, isn't Bitcoin's resistance to change one of the reasons it is a solid foundation to build on?

Conclusion

The Lightning Network appears to be gathering steam. Its spending capacity, while still limited, increased meaningfully in 2021. Its leading development organization, Lightning Labs, is coming off a fresh round of funding and is in the process of increasing the network's functionality with upgrades such as Taro.

Early developments in Bitcoin smart contract development showed that storing transaction data directly on Bitcoin's base layer was a poor use of its limited blockspace. Protocols such as RSK have extended the use cases of Bitcoin by employing merge mining and providing EVM compatibility. Nonetheless, they have relatively centralized bridging architectures and require significant improvements to achieve scale.

After a few iterations, Stacks' approach with PoX and native BTC represents a novel approach aimed at filling the gaps associated with earlier technologies. After a year in production, Stacks has gained traction relative to RSK, but developer and user adoption remains relatively low compared to Ethereum and EVM compatible chains. This gap can narrow as comparable infrastructure and applications get built on Stacks. Whether infusion of capital and accelerator programs bring the necessary developer and user traction remains to be seen.

Appendix

Are Rollups Possible on Bitcoin?

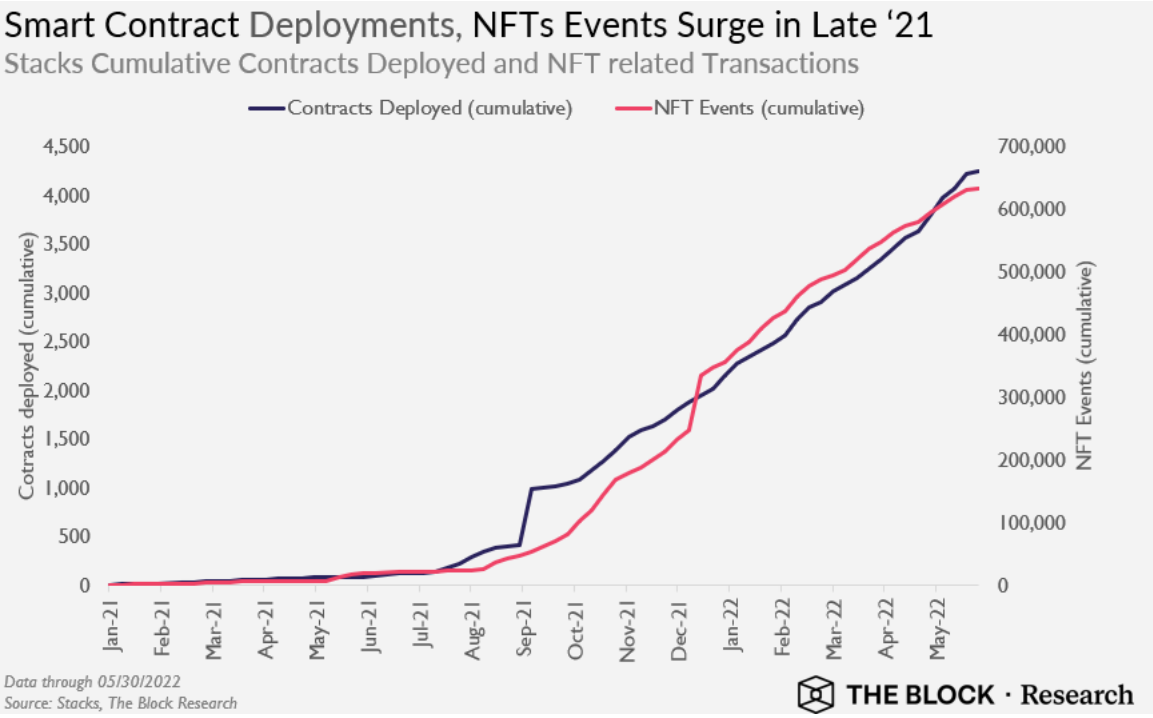
In the last two years, the Ethereum development community has embraced layer-2 scaling solutions and rollups, in particular, as the de-facto path to achieving scale. While in the very early stages, research regarding whether or not ZK-rollups can be amenable to verification on Bitcoin's base layer is being conducted. Human Research Foundation and StarkWare, a leading layer-2 development organization, have sponsored a four-month research fellowship to explore the use of ZK-Rollups on Bitcoin.

Stacks – Network Data

In conjunction with The Block's data collection process, it was able to obtain several Stacks-specific data sets which are included in the following section for reference.

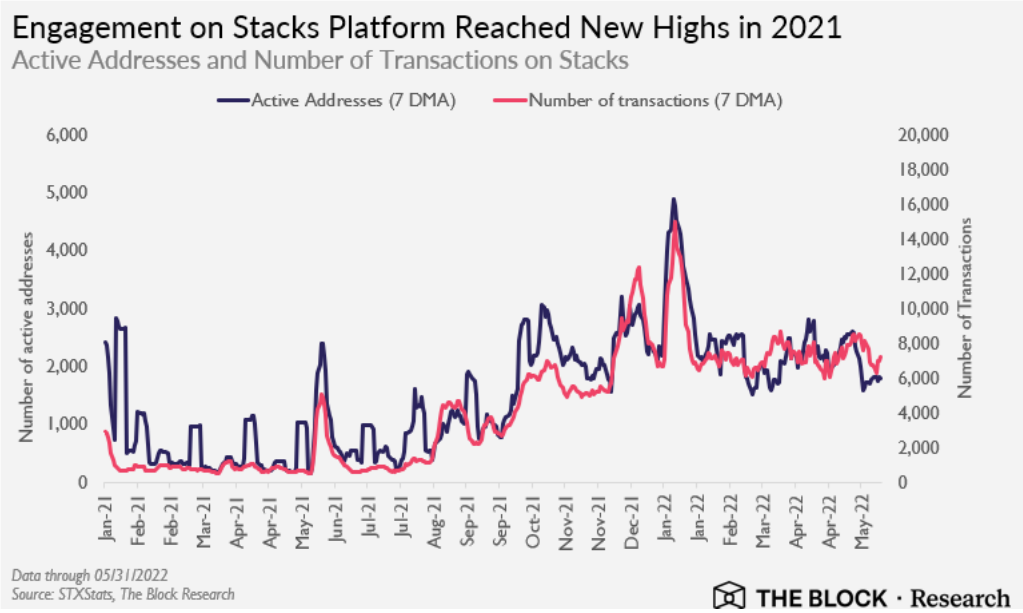
Contracts deployed and NFT-Related Transactions

Stacks saw an uptick in contracts deployed and NFT-related transactions when applications started going live in Q4-21. More statistics on NFTs which, in addition to stacking, have emerged as a top use case of Stacks can be found here.



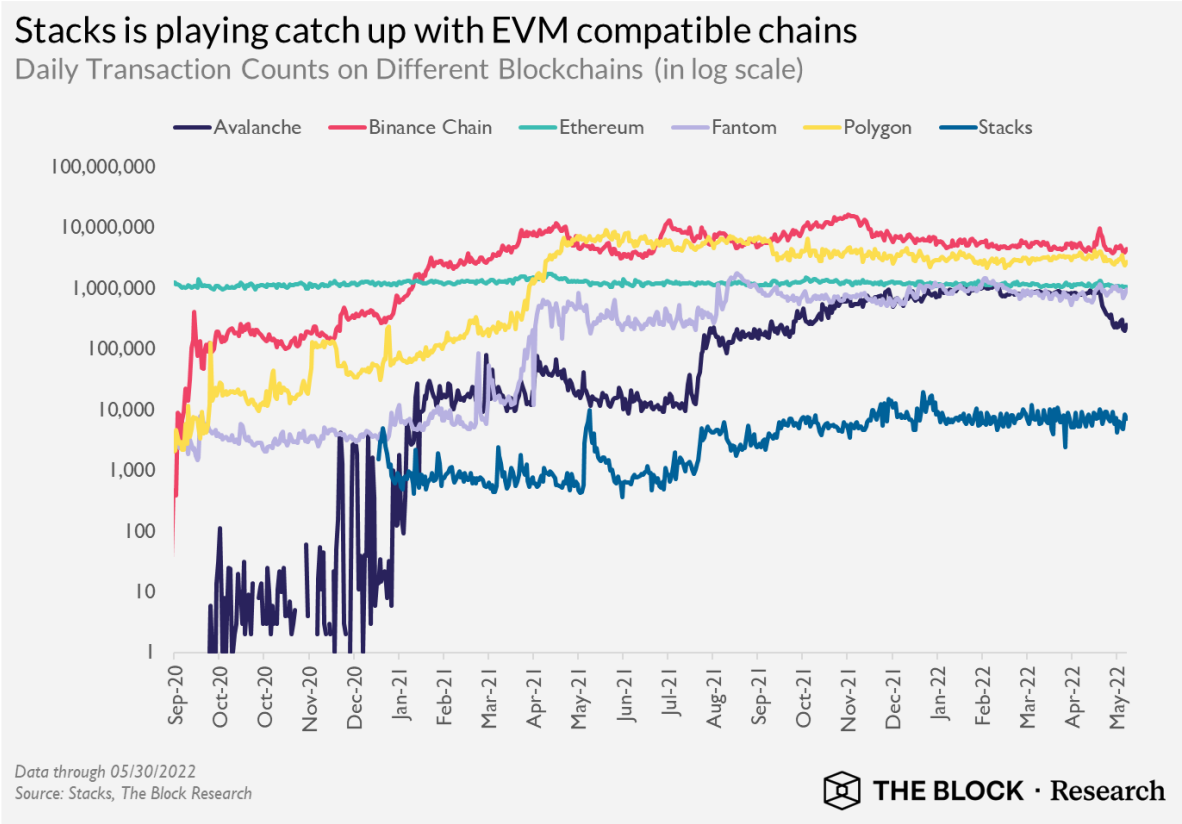
Active Addresses and Daily Transactions

Stacks started seeing marginal uptake in active addresses and transactions around the same time when applications started going live in Q4 2021.



Stacks vs. Other Layer-1 Networks

Alternative layer-1 networks, and EVM compatible blockchains have seen a quicker adoption path compared to Stacks. One of the reasons could be that EVM compatible chains piggyback on the network effects of Ethereum and its tooling ecosystem. Developers can easily copy and paste Solidity-based contracts from Ethereum to other EVM compatible chains. However, Stacks' Clarity based contracts must be written from scratch.



Block to Launch Bitcoin-based Digital Identity

In July 2021 Block Inc., formerly Square, announced TBD, a venture focused on non-custodial, permissionless, and decentralized financial services. Recently TBD announced a project called WEB5 that puts users in control of their data and identity. Three pillars of WEB5 are decentralized identifiers, verifiable credentials, and decentralized web nodes. The first two pillars will be built with the help of a Bitcoin-based layer-2, ION.

Microsoft's ION is an initiative to change the way digital identities work. Currently, all the web 2 applications, such as social media, record and store user credentials. Every time a user wants to use an application, they are asked to store their credentials with the application, and different applications control users' identities. With Decentralized Identifier (DID), Microsoft is trying to make digital identity user-centric, meaning that user controls their digital identity, not any application. These user identities exist independent of any application on a second-layer network on the Bitcoin blockchain. Why did Microsoft choose to build this network on Bitcoin? According to Microsoft, a network of decentralized identifiers for humans must have a few characteristics, such as – it should be open and permissionless, the cost to attack this network must be high, it should be deployed on machines across the globe, well-tested, and it must produce an independently verifiable record, etc. Bitcoin meets all these requirements.

Disclosures

This report is commissioned by Trust Machines. The content of this report contains views and opinions expressed by The Block's analysts which are solely their own opinions, and do not necessarily reflect the opinions of The Block or the organization that commissioned the report.

The Block's analysts may have taken positions in the assets discussed in this report and this statement is to disclose any perceived conflict of interest. Please refer to The Block's Financial Disclosures *page for author holdings. This report is for informational purposes only and should not be relied upon as a basis for investment decisions, nor is it offered or intended to be used as legal, tax, investment, financial or other advice. You should conduct your own research and consult independent counsel on the matters discussed within this report. Past performance of any asset is not indicative of future results.*