WRITTEN BY:

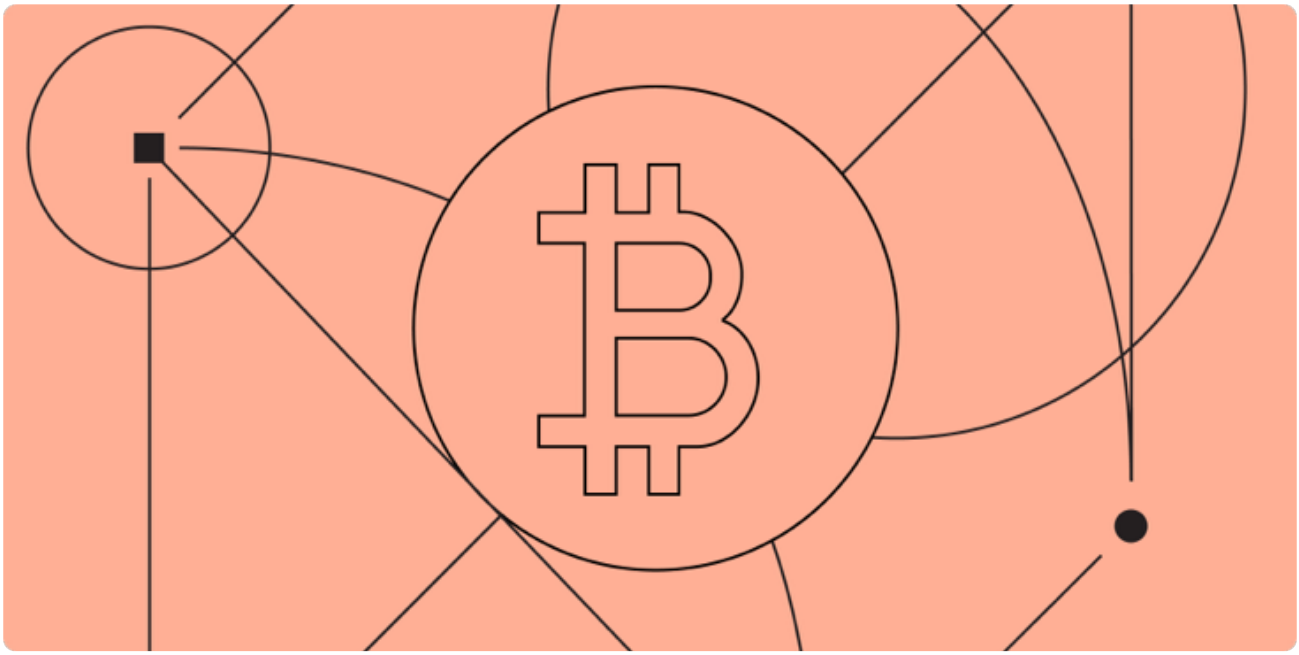
Gabe Parker
Research Analyst

TOPICS

Bitcoin

RESEARCH • AUGUST 02, 2024

Exploring Bitcoin for Data Availability



Watch Now: From the Source

Introduction

Bitcoin's blockspace is extremely scarce with the size of each block capped at 4MB.

This scarcity presents a significant challenge for Rollups seeking to leverage Bitcoin as a data availability layer. The emerging landscape of Rollups built on Bitcoin, predominantly ZK-based, aims to post ZK-Proof outputs and state differences every 6-8 blocks, thereby anchoring to Bitcoin's highly secure layer 1 blockchain. However, this approach faces a critical obstacle: each individual data posting transaction can consume up to 400KB (0.4MB) of blockspace, effectively occupying 10% of an entire block. While the maximum transaction size for a standard Bitcoin transaction is 400KB, with multiple data posting transactions in the same block, the theoretical data posting limit for a single Rollup is 4MB, which would consume an entire Bitcoin block.

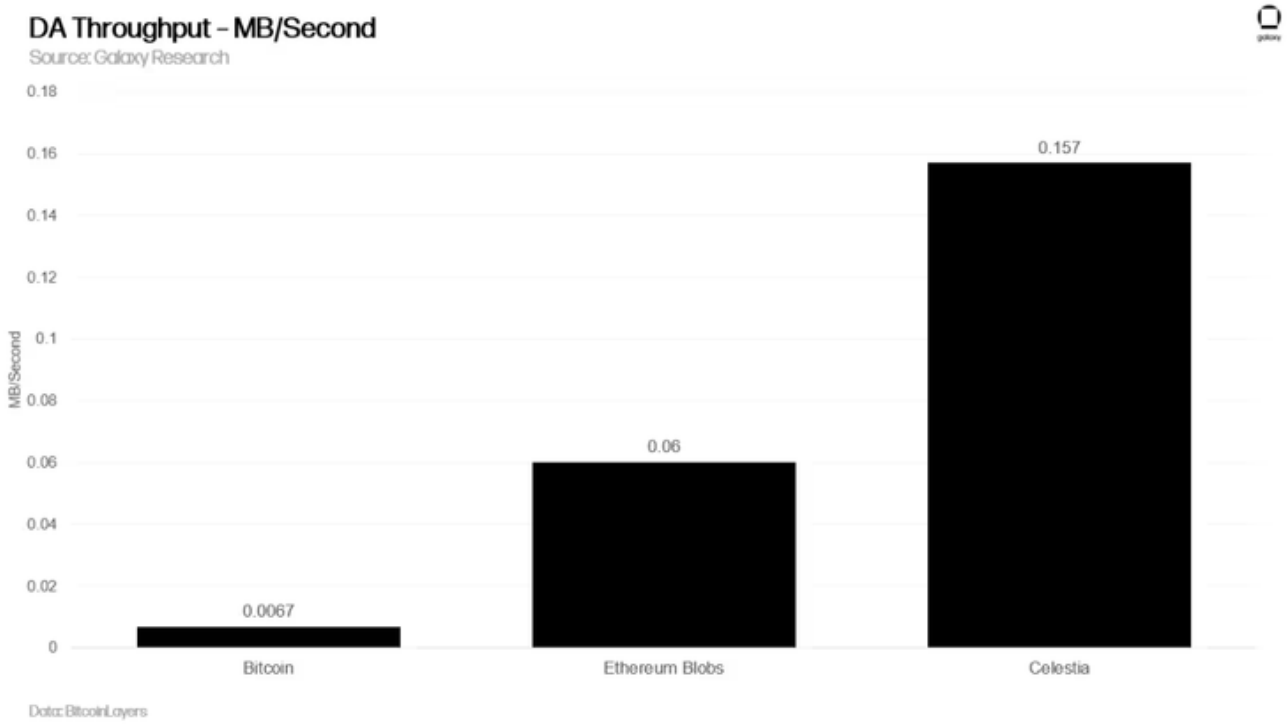
Given Bitcoin's consistently full blocks since January 2023, competition for block inclusion will intensify with the introduction of new blockspace buyers like Rollups, potentially pushing Bitcoin transaction fees to new heights that could make it economically infeasible for certain users – Rollups specifically – to afford transaction fees. Competition for space on the world's oldest blockchain may create an environment where L2s struggle to afford data posting, testing their ability to remain Bitcoin-aligned. To remain viable, Rollups on Bitcoin will need to generate substantial revenue from transaction fees on their own networks, driven by sizable numbers of users paying to transact on the Layer 2. This report analyzes the economic viability of Rollups on Bitcoin by examining data from Ethereum ZK-Rollups and projecting costs for Rollups that choose to use Bitcoin for data availability. The analysis explores the potential impacts on Bitcoin's block composition once these projects launch on mainnet, and also discusses possible alternative strategies Rollups might employ if posting data to Bitcoin becomes too costly.

Is Bitcoin L1 a Data Availability Layer?

Rollups on Bitcoin that post data to the base layer will face a significant problem: the cost to post data. Bitcoin blockspace is the most expensive per byte of any chain. Additionally, Bitcoin's block size is firmly capped at 4MB, and fees are tied to the data weight of a transaction, making any data intensive transaction expensive to execute. The emergence of Ordinals, which are inscriptions attached to individual Satoshis, highlight that transactions that occupy a significant portion of the block size cost a premium and drive-up transaction fees across the network. For example, the first 4MB Bitcoin transaction inscribed by the Taproot Wizards team (block 774,628) cost $147k in fees.

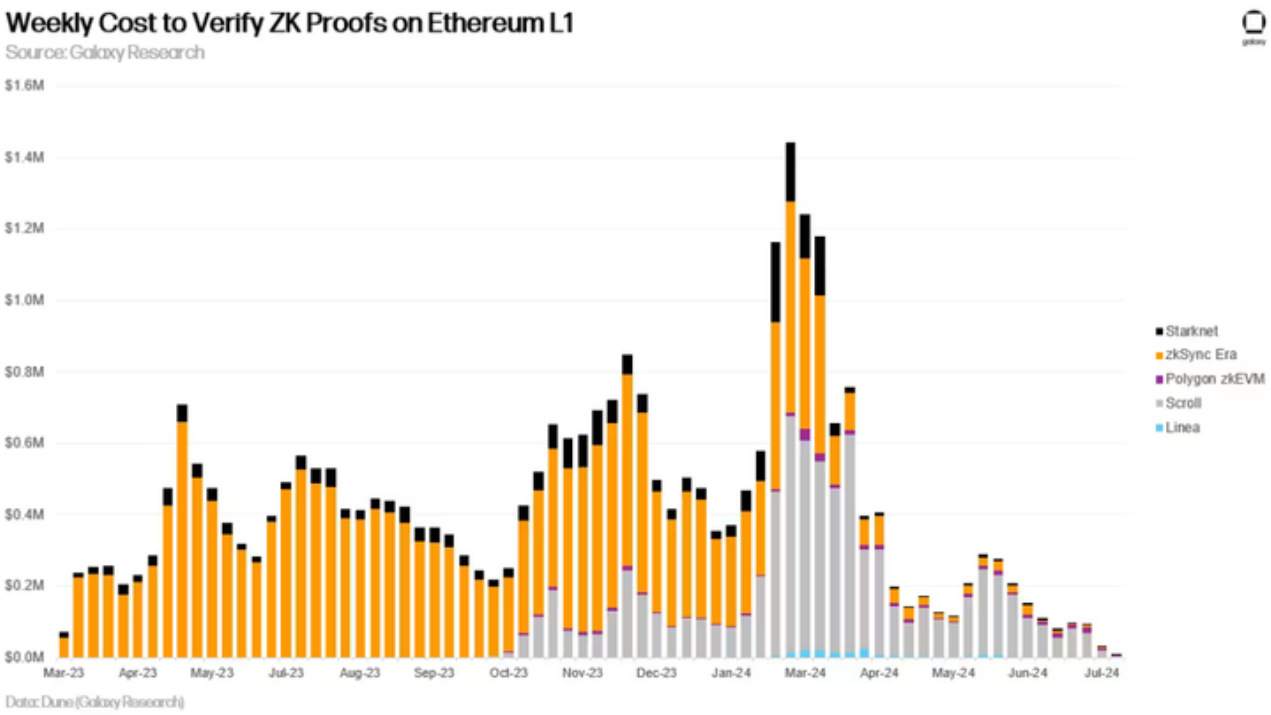
Based on conversations with several teams building ZK-Rollups on Bitcoin, we expect ZK-Rollups to post proof outputs and state differences every 6-8 blocks (1hr – 1.2hr) to Bitcoin L1 in the form of an inscription, arbitrary data stored in the witness of a transaction. This data will enable any participant running a Bitcoin node to reconstruct the most recent state of the Rollup. Based on testnets, and conversations with developers, we estimate the combination of these proof outputs and state differences will require ~400KB of blockspace per data posting transaction every 6 blocks.

When comparing the megabytes processed per second on Bitcoin to Ethereum and Celestia, it's clear that Bitcoin was never designed to be a DA layer.



Cost to Verify Proofs – Ethereum ZK-Rollups

Below is a chart showing the weekly data posting costs for ZK-Rollups on Ethereum. ZK-Rollups finance their data posting expenses through revenue generated from L2 transaction fees. Since its launch, ZK-Sync Era has demonstrated the viability of this model, generating $66.9m in total revenue from L2 transaction fees. Of this, $51.2m was allocated to ZK verification and L1 call data costs (that is, ZK-Proofs and state differences posted to Ethereum). ZK-Sync has successfully processed over 417.6m transactions for 7.8m unique addresses, maintaining an average cost of $0.16 per transaction over its lifetime. This efficient operation has resulted in a total profit of $15.7m.



Estimating Cost to Post Data to Bitcoin

Data posting costs for ZK-Rollups on Bitcoin primarily consist of two components: the ZK-Proof output and the state difference. While the size of a Stark Proof remains constant regardless of the number of transactions in a batch, the state difference size scales with transaction volume and type. Consequently, the state difference typically represents the larger portion of data posting costs for a Rollup. Given the variability in estimates and expectations for data availability requirements among ZK-Rollup teams —which depend on both transaction types and volumes—we've opted to use generalized data sizes to illustrate the costs of posting to Bitcoin L1 and associated L2 break-even points. It's worth noting that estimates for ZK-Proof and state difference sizes are continually evolving as teams research and optimize data compression mechanisms, so this exercise is meant to be demonstrative and not definitive.

For our model, we assume a Rollup's ZK-Proof and state difference is 400KB every 730 posted blocks (approximately one month). Said another way, we expected that Rollups will choose to “settle” to Bitcoin every hour or so (every 6-8 blocks), or 730 blocks per month. If Bitcoin’s L1’s transaction fees are 10 sats/vByte, each block posting would cost $630. This translates to monthly expenses of about $460k, or $5.5m annually, assuming consistent data sizes and fee rates. However, if the average fee rate rises to 50 sats/vByte, monthly expenses would soar to $2.3m, amounting to an annual cost of approximately $27.6m. Our model employs a fixed KB size for each data posting transaction within the month to emphasize that posting ZK-Proofs and state

differences on Bitcoin L1 is expensive, regardless of the fees paid by L2 users on the Rollups themselves.

The sensitivity table below estimates the transaction activity and fee rate levels required for Rollups on Bitcoin to break even after data posting costs. Our model projects monthly costs for a Rollup posting a fixed 400KB of data to Bitcoin L1 every 6 blocks at 10, 20, and 50 sats/vByte as of August 1, 2024. In a scenario where a Bitcoin Rollup processes 20m transactions monthly—comparable to ZK-Sync's volume over the past year—it would need to charge transaction fees of $0.05, $0.09, and $0.23 to break even at the respective 10, 20, and 50 sats/vByte levels.

It should be noted that due to the lack of available data on testnet, this sensitivity table assumes that the 400KB data posting size is fixed from 10k – 20m transactions per month. The Alpen team's whitepaper provides estimates on state difference sizes based on the number of transactions in a posted batch, which we took into consideration. Their whitepaper states that 10k transactions per batch, roughly 7.3m transactions a month if the Rollup is posting every 6 blocks, would be 670KB per posted batch. As these estimates are over a year old, our model attempts to account for the advancement in compression algorithms and overall room for error. We understand that the size of the state difference may be smaller than 400KB from 10k-2m monthly transactions.

Rollups that cannot facilitate enough transaction fees to cover data posting costs will need to tap their treasuries to pay L1 transaction fees and may ultimately be forced to pivot altogether from using Bitcoin as a DA layer. Should Rollups find posting to Bitcoin unviable, alternatively they could post ZK-Proofs and state differences on more cost-effective DA layers such as Celestia, Near, or Syscoin. However, using something other than Bitcoin as a DA layer reduces the layer's ability to call itself a "Bitcoin Rollup." If a layer 2 network doesn't roll up to Bitcoin, would it still be considered a Bitcoin Rollup, or would it transform into a Validium chain of the alternative DA network? Another potential solution for Rollups struggling with cost coverage involves restructuring as a Layer 3 solution. In this scenario, the Rollup would post state differences to an existing Layer 2 or Sidechain, with only merkle root hashes being posted to the Layer 1. This approach could significantly reduce data posting costs while maintaining a connection to the Bitcoin network.

Bitcoin Blockspace When Rollups Launch

Since the emergence of Ordinals and BRC-20s in early 2023, Bitcoin's daily mean block weight has consistently sat just below its 4m weight unit limit (4MB of data). Block weight is a dimensionless measurement of the "size" of a block which was introduced in the SegWit upgrade to include discounted witness data. The average daily block

weight has significantly increased following a large influx of inscription related transactions, which include arbitrary data (text, image, etc) in the witness field of a transaction. Since February 2023, the average fullness of a Bitcoin block stands at 98%.

With each proof output and state difference totaling 400k weight units, a single Rollup posting data to a block will utilize 10% of the block's weight limit if the Rollup's data size remains consistent. Given that blocks are consistently full, the introduction of Rollups will change the composition of transaction data within each data posting block. The chart below demonstrates the block composition for the most recent 30 blocks as of July 18, 2024, if two Rollups were live and posting data every 6 blocks. This chart does not account for Rollups posting state differences that undercut or exceed the 400KB data size level. Note that this chart only contemplates *two* Rollups posting data – even though there are several that hope to launch.

The consistent demand for blockspace from a Rollup posting data on Bitcoin L1 every 6-8 blocks will force time sensitive transactions to pay a premium before or during the data posting block. This will, in turn, increase fees for all Bitcoin users, including the Rollups. The chart below underscores how the increased competition of on-chain activity from Runes and Ordinals force time sensitive transactions (predominantly financial transactions, such as between trading counterparties) to pay the highest fee rate premium. "Overpayment" is the difference between the median sat/vByte of a specific transaction type in a block and the median sat/vByte level of the block it is found in. The chart below aggregates the overpayment daily, displaying the average of the block-by-block overpayment differences in a given day.

Why Bitcoin DA is Important

For a Rollup to fully align with Bitcoin, many believe the Rollup must use Bitcoin for data availability. This choice, while costly, leverages Bitcoin's unparalleled security, immutability, and decentralization. Rollups opting for alternative DA solutions introduce additional trust assumptions outside the Bitcoin network, potentially compromising their integrity and categorization as a “Bitcoin Rollup.” The strength of Bitcoin as a DA layer lies not only in its robust security but also in its extensive node distribution and low barrier to entry for setting up light or full nodes. This accessibility ensures that anyone running a Bitcoin full node can reconstruct the latest L2 state of the Rollup, enhancing transparency and decentralization.

Despite the significant expenses and potential long-term feasibility challenges, Bitcoin’s role as an elite DA layer for Rollups underscores a fundamental trade-off; the high cost of leveraging Bitcoin's infrastructure versus the unmatched security and decentralization it provides. This balance between cost and security will likely shape the future landscape of Rollup implementations on the Bitcoin network. While the high costs may not force all Rollups away from Bitcoin, they will likely create an environment where only a small number can survive.

Outlook on Rollups using Bitcoin for DA

- If the average data posting size is 400KB, a ZK-Rollup using Bitcoin for data availability will need to generate approximately between $459k and $2.3m in

monthly revenue from L2 transaction fees to operate profitably in a 10-50 Sat/vByte fee rate environment.

- Fee estimating engines will be crucial for Rollups on Bitcoin to maximize profitability.
- Bitcoin blockspace simply cannot facilitate 4-8 Rollups posting 100KB-400KB proofs every 6-8 blocks without leading to exorbitant fees for all users, including the Rollups.
- Bitcoin Rollups might explore partnerships with Bitcoin miners to offer private deal flow for guaranteed block inclusion, locking in some fixed, lower transaction fee rate.
- The teams that will achieve building a sovereign Rollup on Bitcoin will need to execute the go-to-market strategy with applications that keep users transacting on the L2.
- Absent sufficient Rollup activity to justify the cost to post to BTC, projects risk burning their funds simply to post data.
- Some Bitcoin L2s will explore L3 environments for transaction execution and use a combination of L2s and Bitcoin L1 for data availability.
- Rollups on Bitcoin will increase the competition for block inclusion, thereby driving up layer 1 fees for everyone, including the Rollups themselves.
- Bitcoin L2s using Bitcoin L1 for DA will need to hedge against unexpected volatile fee spikes through fee rate derivative markets and out of band mining deals.

particular, Galaxy Digital's views on the current and future market for certain digital assets), and there is no guarantee that these views, estimates, opinions or predictions are currently accurate or that they will be ultimately realized. To the extent these assumptions or models are not correct or circumstances change, the actual performance may vary substantially from, and be less than, the estimates included herein. None of Galaxy Digital nor any of its affiliates, shareholders, partners, members, directors, officers, management, employees or representatives makes any representation or warranty, express or implied, as to the accuracy or completeness of any of the information or any other information (whether communicated in written or oral form) transmitted or made available to you. Each of the aforementioned parties expressly disclaims any and all liability relating to or resulting from the use of this information. Certain information contained herein (including financial information) has been obtained from published and non-published sources. Such information has not been independently verified by Galaxy Digital and, Galaxy Digital, does not assume responsibility for the accuracy of such information. Affiliates of Galaxy Digital may have owned or may own investments in some of the digital assets and protocols discussed in this document. Except where otherwise indicated, the information in this document is based on matters as they exist as of the date of preparation and not as of any future date, and will not be updated or otherwise revised to reflect information that subsequently becomes available, or circumstances existing or changes occurring after the date hereof. This document provides links to other Websites that we think might be of interest to you. Please note that when you click on one of these links, you may be moving to a provider's website that is not associated with Galaxy Digital. These linked sites and their providers are not controlled by us, and we are not responsible for the contents or the proper operation of any linked site. The inclusion of any link does not imply our endorsement or our adoption of the statements therein. We encourage you to read the terms of use and privacy statements of these linked sites as their policies may differ from ours. The foregoing does not constitute a "research report" as defined by FINRA Rule 2241 or a "debt research report" as defined by FINRA Rule 2242 and was not prepared by Galaxy Digital Partners LLC. For all inquiries, please email contact@galaxydigital.io.

More Like This

RESEARCH •AUGUST 02, 2024

Bitcoin Nashville 2024: A Historic Gathering

Bitcoin

RESEARCH •JULY 31, 2024

2024 Bitcoin Mining Mid-Year Report

Bitcoin | Cryptocurrency

About Us
Who we serve
Leadership
Board of Directors
Careers
ESG
Newsroom

GALAXY INSIGHTS

Explore All Insights
Research
Perspectives
Case Studies
Podcasts
Videos
→ Subscribe

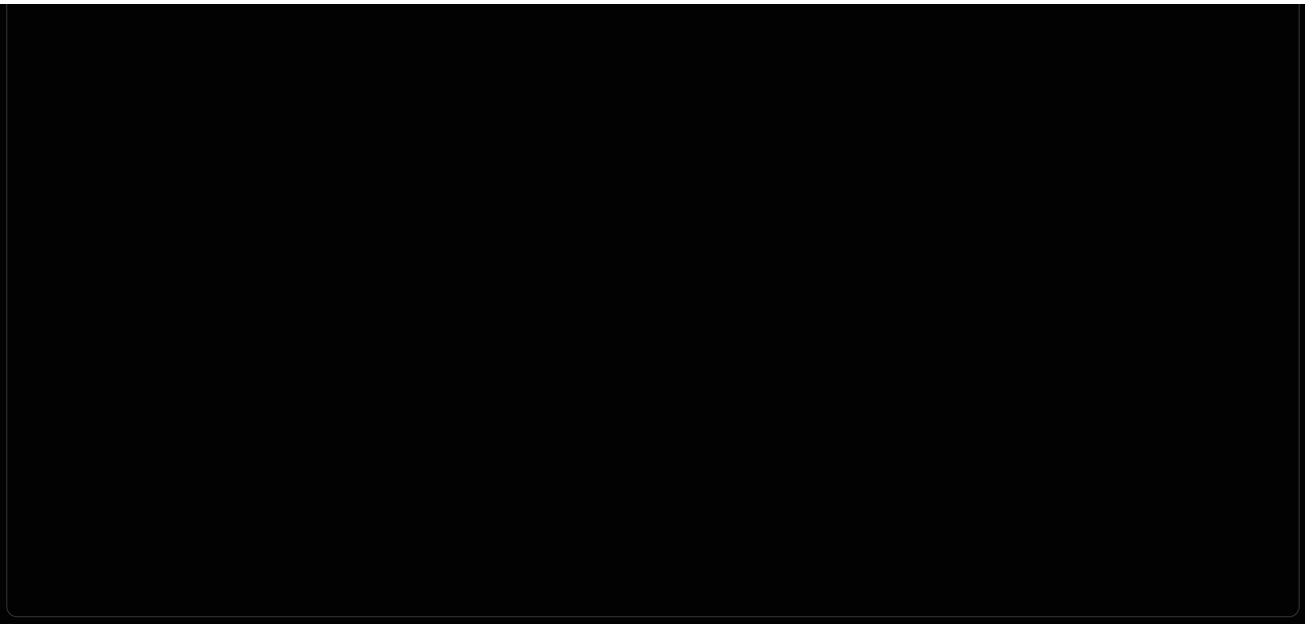
CONTACT

→ Get Started
→ Media Inquiries
→ Investor Relations

RESOURCES

Digital Assets Academy
Trust and Transparency
VisionTrack Database
Glossary

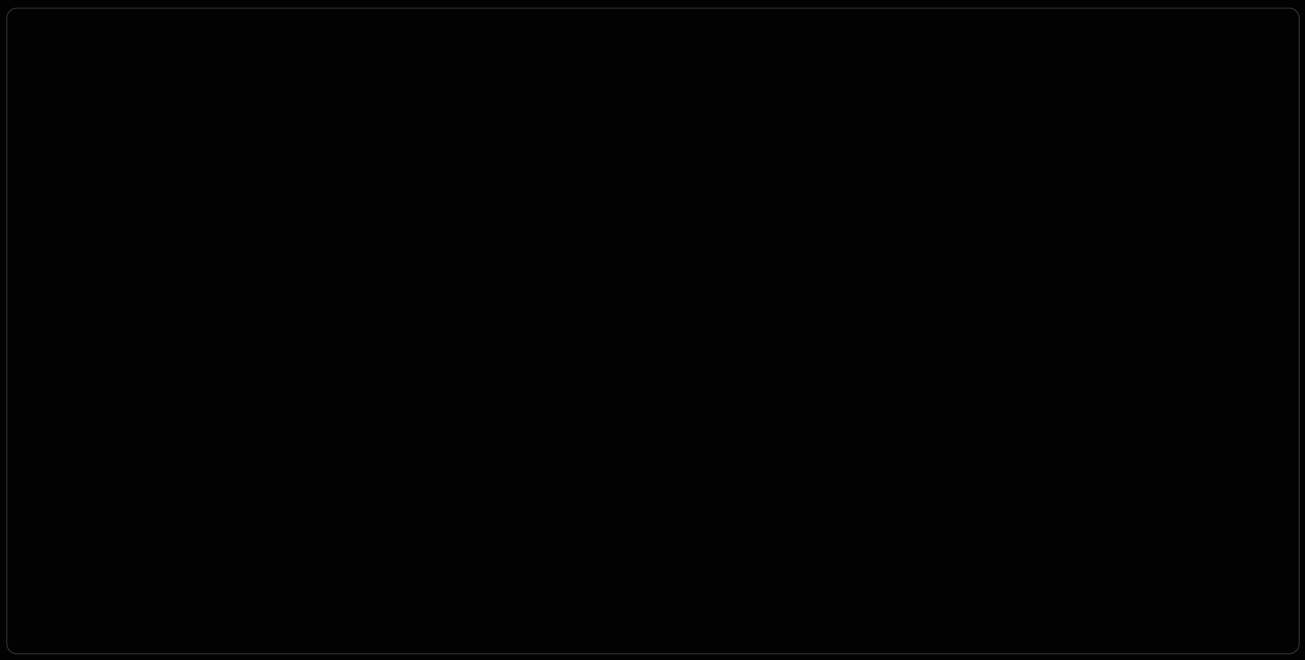
LATEST IN INSIGHTS



RESEARCH •AUGUST 30, 2024

Weekly Top Stories - 8/30

Weekly Top Stories



VIDEOS •AUGUST 30, 2024

Fed’s Shifting Focus and the Road to Rate Reductions

Markets & Macro

GALAXY RESEARCH PODCAST

PODCASTS • AUGUST 29, 2024

Telegram & Free Speech w/ Preston Byrne