Regulatory Updates

Uniswap's Encounter with the SEC

The SEC has issued an enforcement notice to Uniswap, highlighting the regulator's increasing focus on decentralized finance (DeFi) platforms. Uniswap is a decentralized finance protocol used for exchanging cryptocurrencies. It enables users to trade various tokens directly without the need for an intermediary, utilizing an automated market-making system, relying on liquidity pools rather than traditional order books, which allows anyone to supply liquidity and earn transaction fees in return. This proactive measure underscores the complexities and challenges of applying traditional compliance frameworks to decentralized systems, which inherently lack central oversight.

Wells notices are preliminary warnings that inform respondents of the charges the regulator is considering bringing against them. They usually lead to enforcement actions. As authorities grapple with the decentralized nature of these platforms, the SEC's scrutiny of Uniswap could herald a new era of more robust regulatory oversight in the DeFi sector. The outcome of this enforcement could significantly influence future regulatory approaches towards DeFi platforms, potentially leading to a reshaping of the sector's regulatory landscape. This case may signal the need for DeFi platforms to develop more transparent operations and compliance mechanisms. In response to this notice, Uniswap CEO Hayden Adams noted that he was "annoyed, disappointed, and ready to fight.". (Source 1)

The Craig Wright - Satoshi Saga

A recent court ruling has definitively stated that Craig Wright, an Australian computer scientist, is not Satoshi Nakamoto, the elusive creator of Bitcoin. This pivotal decision closes a significant chapter in one of the cryptocurrency world's most debated controversies, impacting the broader crypto community's views on leadership and credibility.

Judge Mellor was quoted saying: "I will make certain declarations, which I am satisfied are useful and are necessary to do justice between the parties. First, that Dr. Wright is not the author of the Bitcoin white paper. Second, Dr. Wright is not the person who adopted or operated under the pseudonym Satoshi Nakamoto in the period 2008 to 2011. Third, Dr. Wright is not the person who created the Bitcoin System. And fourth, he is not the author of the initial versions of the Bitcoin software."

This is the result of a 2021, lawsuit filed by COPA, against Wright to obtain a judgment that would stop him from initiating lawsuits against developers and other crypto community members, or from asserting ownership rights over the open-source technology of Bitcoin. The result was widely received as a triumph for COPA, which is supported by prominent industry figures such as Twitter's founder Jack Dorsey, Coinbase, and others.

Settling this claim helps solidify the narrative surrounding Bitcoin and also facilitates more rapid development as Dr. Wright has in the past sued Bitcoin Core developers for their involvement in the project. (Source 2)

Evolving Global Frameworks in Cryptocurrency Regulation

The UK's Digital Pound

The UK government is advancing its digital pound proposal, a central bank digital currency (CBDC) designed with strong privacy features. This initiative is part of the UK's broader strategy to align with global digital currency trends and establish benchmarks for enhancing user privacy in financial technologies. As other countries explore similar initiatives, the UK's approach to the digital pound could influence global financial systems' integration of CBDCs, affecting the overall approach to digital currencies. (Source 3)

International perspectives in Stablecoins

Simultaneously, the UK, but also Hong Kong is tightening their regulatory frameworks for stablecoins, responding to the perceived risks these digital assets pose to financial stability. The UK is crafting comprehensive legislation to address regulatory loopholes and ensure a stable financial infrastructure, while Hong Kong is updating its trading rules to safeguard its status as a financial hub and ensure market security. These actions demonstrate a shift towards, stricter governance of stablecoins, suggesting a move towards stabilizing this digital asset class, especially in light of emergent CBDCs.(Source 4; Source 5)

A Balancing Act Between Environmental Regulation and Cryptocurrency Mining

The U.S., Norway, and Sweden are implementing regulatory measures to address the environmental impacts of crypto mining, reflecting their commitment to reducing the significant energy demands of these operations.

The U.S. Energy Information Administration (EIA) has launched a comprehensive survey to assess the energy consumption patterns of cryptocurrency miners across the nation. This move has sparked uproar within the cryptocurrency community, as it involves collecting detailed and sensitive information about their operations, such as mining fleet specifications and hash rates. The concern among stakeholders is that this could lead to more stringent regulations that may impact the operational freedom and profitability of crypto mining activities.

Norway/Sweden is contemplating imposing regulations on data centers that engage in cryptocurrency mining, motivated by the "substantial" energy demands of such operations and their potential environmental impact. The proposed regulations aim to mitigate the environmental concerns associated with the high energy consumption of crypto mining. Norwegian lawmakers believe that through regulation, they can encourage more sustainable practices in the burgeoning sector.

(Source 6; Source 7)

Technological Trends & Developments

EIP-4844: Proto-Danksharding: Scaling in a decentralized way

Ethereum's Dencun Upgrade

The Ethereum Dencun Upgrade has been one of the most significant upgrades since the Merge. The hard fork has been activated on the Ethereum mainnet at the epoch 269568. While the upgrade has introduced 9 Ethereum Improvement Proposals (EIPs), one of the most important has been the EIP-4844 known as Proto-Danksharding which creates a dedicated data channel on Ethereum for Layer2 data. Following the upgrade, Ethereum rollups have experienced notable benefits that eliminated both transaction time and fees.

The upgrade is introducing a new transaction type which is called "blob-carrying". This new type will be utilized by rollup sequencers to post data to the Ethereum mainnet. The EIP will help the network to scale in a decentralized manner while ensuring that the size and number of blobs are limited, and hence the computational and storage requirements of the network don't drastically increase. Blob data are less expensive than regular Ethereum calldata because the data is not made available to EVM- Ethereum's execution layer. Only a reference to the blob's data is accessible, and the data will be downloaded and stored solely by Ethereum's consensus layer for a limited period- which is usually 18 days long.

What is a blob?

In the Ethereum network, the blocks are filled with standard transactions. After the upgrade, the blocks can be filled with a combination of the standard transactions, and with blob-carrying transactions. Those transactions are envisioned to be used initially by Ethereum Layer 2 rollups that will send blobs that include batched transactions. The research community describes those blobs such as compressed files.

The structure of blob-carrying transactions:

This new transaction structure contains two additional fields that a typical transaction does not include:

- A bid that defines how much the submitted is ready to pay to have their blob-carrying transaction included in a given block *max_fee_per_blob_gas* *https://github.com/ethereum/EIPs/blob/master/EIPS/eip-4844.md*
- A list of references to the blobs included in the transaction *blob_versioned_hashes* *https://github.com/ethereum/EIPs/blob/master/EIPS/eip-4844.md*

The blob-carrying transaction doesn't include the blob data, but rather a reference to it. A full explanation of the mathematics and structure of blobs is available in the following article: https://domothy.com/blobspace/

What are rollups?

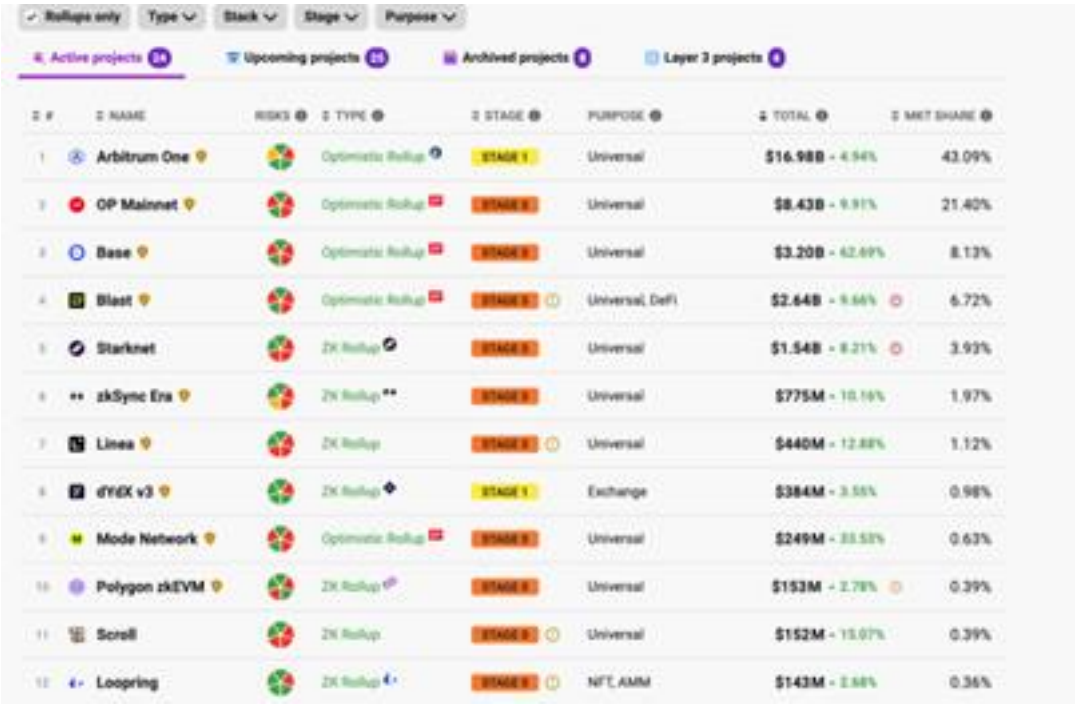
Ethereum Rollups perform transaction execution outside of the core layer, and then the data is posted to the Ethereum mainnet to reach a consensus. This allows scaling networks to benefit from Ethereum's security. There are two types of rollups:

There are two types of rollups with different security models:

A.) Optimistic rollups: These assume that transactions are valid by default and only execute computation in the event of a challenge, which can be proven through fraud proofs. Optimistic rollups aim to achieve

scalability by minimizing on-chain computation. In this report, we will only focus on Zero-Knowledge rollups since there weren't significant technology updates

B.) Zero-knowledge rollups: These run the computation off-chain and submit a proof of validity to the Mainnet. Zero-knowledge rollups leverage advanced cryptographic techniques to ensure the correctness of transactions while maintaining privacy.



Source: Ethereum scaling solutions ranked according to Total Value Locked
https://l2beat.com/scaling/summary

How do Rollup sequences use the blobs?

Currently, rollups account for 12% of all gas paid on the Ethereum network. The rollup sequencers need to post data to the Ethereum mainnet. Until the upgrade, the rollups were batching transaction data as Ethereum calldata, which was a costly exercise. After the EIP-4844 implementation, rollups are submitting their data as the blob-carrying transaction type.

To outline how each rollup utilize the blobs, we'll quote EIP-4844 itself:

"Optimistic rollups only need to provide the underlying data when fraud proofs are being submitted. The fraud-proof submission function would require the full contents of the fraudulent blob to be submitted as part of calldata. It would use the blob verification function to verify the data against the versioned hash that was submitted before, and then perform the fraud-proof verification on that data as is done today."

"ZK rollups would provide two commitments to their transaction or state delta data: the KZG in the blob and some commitment using whatever proof system the ZK rollup uses internally. They would use a commitment proof of equivalence protocol, using the point evaluation precompile, to prove that the KZG (which the protocol ensures points to available data) and the ZK rollup's own commitment refer to the same data."

Numerous popular rollups have already extended their support for blobs. Among these leading rollups are zkSync Era, StarkNet, Optimism & Base, Zora, Mode, Arbitrum, and Paradex.

Dynamic Market

The number of blobs attached to a block is dynamic, and it could be from 0 with a maximum of 6 blobs. The Ethereum community is currently aiming for three blobs per block. There is a pricing incentive, which constitutes more expensive the submission of a blob if there are already three blobs in each block. On the other hand, it's cheaper if there are not three blobs in each block. The pricing is based on a dynamic model.

Exploring more about Blobs

Leading blockchain explorers, including the well-known Etherscan, are now offering insights into the blobs market. You can view these insights directly on Etherscan. Furthermore, a new explorer, Blobscan, has been launched, specifically designed to provide visibility on blob transactions.

In addition to the explorer, there are also other valuable tools and analytics dashboards available for those interested in diving deeper into the blob data. One such resource is a Dune dashboard, which offers useful insights into the utilization and impact of blob transactions within the Ethereum ecosystem.

This Dune board reveals, among other things, that the current average blob count per block stands at 2.2, which is below the targeted goal of 3 blobs per block. Moreover, the dashboard provides insights into the top users of the blobs market, identifying major rollups as top consumers -such as Inscriptions, Base, Optimism, Arbitrum, and zkSync. For those diving deeper into the dynamics of Ethereum's blobs market, another resource is the Dune dashboard maintained by 0xRob.

L2beat, a platform for tracking and analyzing the Layer 2 scaling solutions ecosystem, has introduced a Data Availability (DA) dashboard. This new feature serves as an extensive repository, showcasing the Data Availability Layer for the most important rollups, and offering insights into how these rollups manage and store their data.

Market Updates

Concluding a lengthy court process, Dr Craig Wright, who had claimed to be Satoshi Nakamoto, was defeated in court by the Crypto Open Patents Alliance. The judge found that Dr Wright was not the author of the Bitcoin White Paper, Satoshi Nakamoto, the creator of Bitcoin, or any initial Bitcoin Software. This concludes a saga that began in 2021 as COPA sought to protect Bitcoin developers from Dr Wright's legal threats, as well as protect the open-source technology of Bitcoin.

Enforcement agencies in the United States have been incredibly active, with cases raised and won against cryptocurrency-related projects, setting a combative tone and with no federal regulation or supervision framework in sight. In a landmark case, a Cryptocurrency trader was found guilty of theft following the manipulation of a Decentralised Finance protocol. The US has been particularly focused on decentralized services, with actions, a backbone decentralized exchange service; Samourai Wallet, a privacy-enhancing non-custodial mixing service; Consenys, provider of the MetaMask platform; as well as actions against former Binance CEO, C Zhao, and the sentencing of former FTX CEO, Sam Bankman-Fried to 25 years in prison for his role in an $8 billion USD fraud. Overall, this shows a maturing enforcement framework in the United States who are seeking to curb industry excesses; however, with more stable and 'friendly' regulators

based in the United Arab Emirates, EU, and elsewhere, the effect of this action may force more US based crypto businesses to seek shelter in other locations.

The European Union's flagship Crypto Asset Regulation, MiCA (Markets in Crypto Assets), was approved by legislators on 24 Apr. Generally, these have been well received by industry who see them as a positive result for the sector. Patrick Hansen, of Circle, a US-based stablecoin issuer was positive about the rules, however, noted that it took much industry persuasion to arrive at the current position and was "not a fan of the AMLR" due to its low thresholds for cash payments. Further, the European Securities and Markets Authority (ESMA) indicates that there has been little if any increase in Crypto-Euro transactions following the announcement though remains optimistic about its role in attracting growth through greater investor protection mechanisms.

In parallel, ESMA has also suggested that Maximum Extractable Value (MEV), a practice where blockchain transactions are optimized by the operator to maximise their profits, may be problematic and tantamount to market abuse. In particular, ESMA raises concerns that operators may have an unfair trading advantage and are effectively frontrunning user activity through abuse of their position.

Sweden and Norway have enacted separate legislation to curb energy-intensive activities, including cryptocurrency mining operations and data centers, repealing the large tax incentives that had been in place since 2017. With growing energy costs, northern areas of Sweden and Norway with an abundance of hydroelectricity and natural cooling were sought after by proof of work mining firms seeking to maximise profitability. The technical impact on proof of work networks is fairly limited, as Norway and Sweden represent a total of 1.58% of global hashrate, however as energy costs increase mining operations have to find alternative locations as well as compete more directly with traditional data centers.

ByBit, a Singaporean headquartered cryptocurrency exchange with a daily trading volume of over $2.8bn USD, launched in the Netherlands despite a public warning by the Hong Kong Securities and Futures Commission (SFC) for its offer of services in jurisdictions it was not licensed to.

The Bank for International Settlements has proposed a 'Finternet' of unified ledgers in its latest proposal to use blockchain and unite multiple financial asset markets using smart contracts and tokenized assets. Whilst it remains in proposal stages under the moniker 'Project Agora', the concept of a unified ledger has attracted interest from the SWIFT network. The project involves support from seven central banks, including the UK, Japan, Korea, Mexico, New York, and the EU.

In the UK, greater rules as well as enhanced powers for law enforcement to seize assets without an arrest highlight major steps forward for consumer protection. Amidst a backdrop of a record seizure of $2.5 bn USD worth of Bitcoin In connection with financial fraud, additional powers for British law enforcement to take proactive measures against anonymous accounts involved in criminal activity seem well timed. In addition, the UK's Financial Conduct Authority also issued guidance regarding the promotion of Crypto asset services.

The International Organisation of Securities Commissions (IOSCO) has announced greater attention to tokenization and the utilization of distributed ledger technology in its 2024/5 strategy. Under the topics of 'Addressing New Risks in Sustainability and Fintech' and 'Protecting Investors', IOSCO seeks to explore the role and risks of 'finfluencers', as well as the literacy of investors in crypto assets. More significantly, there is a focus on the tokenization of securities markets in both native tokens (i.e. Bitcoin, Ethereum) and non-native tokens and developing a shared understanding among IOSCO members.