



copper.co

Risk Bytes

Newsletter
Volume 11

58°

l=188

l=169

74°

Date
22/03/2023

Risk Bytes Newsletter
Volume 11

copper.co

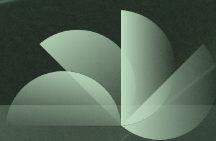


Ethereum steps up its game while DeFi hacks strike again

In this edition of Risk Bytes, we're taking a look at a couple of key developments for the Ethereum ecosystem, as well as an examination of the Euler hack and Oasis' counter hack and their possible implications for the space. The EIP-4337 contract standard made a big impression at ETH Denver, so we're looking under the hood to see how it works. We'll also be talking about Coinbase's Base chain, a layer 2 network for ETH that could help aid the development of EVM protocols and applications.

To finish up, two hacking stories. Euler Labs' hack is yet another case of a flash loan exploit that we've dug into with a controversial bounty program. Finally, Oasis.app, under the order of a High Court in the UK, managed to reverse a recent hack on their own platform. This has raised questions on "immutability" and how multi-sig wallets are managed.

Abstraction at its finest!
New Contract Standard:
EIP-4337



ETH Denver brought to light a variety of noteworthy themes, announcements, and innovations, ranging from ZK proofs, layer 2s, cross-chain bridges and as always, a multi-chain future. However, what particularly piqued our interest and what we'll delve into further is the newcomer among contract standards: EIP-4337 (aka Account Abstraction).

EIP-4337 has been deployed on the Ethereum mainnet as of 1st March 2023, marking a shift in how end users will interact with EVM-based chains going forward and the hope of onboarding the next wave of adopters with this development. This implementation of the token standard was first suggested in a paper co-authored by Vitalik Buterin, co-founder of Ethereum, in September 2021. The paper outlined a proposal for account abstraction that avoids changes to the consensus-layer protocol.

Instead, it will rely on a higher-layer infrastructure change in the form of the ERC standard. To put it simply, account abstraction enables Ethereum wallets to operate as programmable smart contracts ("wallets"). This means users can recover lost private keys, secure their wallets without seed phrases, and enable 2FA and biometrics data. They can also carry out automated payments and set time-based spending limits, such as monthly or weekly spending limits. Moreover, users will now be able to send gasless transactions, so dApps can cover the gas fees to make it cheaper and simpler for end-users to interact with their applications.

This marks a shift away from both externally owned accounts (EOA), that hold one set of private keys, and contract accounts programmed by smart contracts. An EOA is controlled by a private key, has no associated code, and can send transactions. On the other hand, a contract account has an associated code that executes when it receives a transaction from an EOA. EIP-4337 will put both functions under roof. With the new contract comes a novel flow with an introduction of a new mempool for user operations that will be serviced by "bundlers" — similar to validators and miners — but at an account's function level. Rather than submitting a transaction, users will submit user operations to the mempool. Bundlers will then take it from the mempool and include it in blocks on Ethereum or any other EVM chain.



The implementation of EIP-4337 marks a big step forward in reimagining the functionality of wallets. By combining the security and transactional capabilities of EOAs with the programmability of contract accounts, users will benefit from increased flexibility and control over their funds. This new token standard has the potential to greatly enhance the user experience for Ethereum and other EVM-based chains. Even if it takes some time for adoption to arrive from developers and applications, this is a step in the right direction for the continued development of Ethereum.

Additionally, institutions that use Ethereum can benefit greatly from this new standard, as it allows for a more flexible and sophisticated management of assets. As this market continues to mature, we can anticipate seeing innovative solutions that help this technology become more user-friendly and robust.

Source:

[Ethereum.org](https://ethereum.org) →



Coinbase has revealed plans to introduce Base — its own Layer 2 (L2) on Ethereum. It is worth noting that an L2 blockchain simplifies and reduces the cost of creating and implementing dApps. With Ethereum at the forefront of L1s, L2s such as Arbitrum and Optimism have emerged as frontrunners.

Base is constructed using Optimism's OP Stack, which features the open-source code used to power Optimism. Coinbase's adoption of the OP Stack is a significant endorsement of Optimism, which led to a price increase for the OP token after the announcement. There was also a 200% price increase in an unrelated token called BASE due to speculation in the market.

Coinbase has not announced any plans for a token on their new network and given the SEC's increased scrutiny/enforcement in the space, launching one on this network would be reckless. Many networks, such as Optimism and Arbitrum, have been launched without a token at first, and although Optimism now has a live token called OP, there are rumours that Arbitrum is working on a token, but nothing has been confirmed.

Coinbase will act as the sole sequencer for transactions on the new blockchain to incubate its development. Sequencers are responsible for validating and executing transactions on a blockchain. This means that initially, Base will be centralised, however Coinbase plans to gradually decentralise it by adding other sequencers over time. A test network was launched a few weeks ago, and 48 partners, including Chainlink, Magic Eden, and Uniswap, were given access. Coinbase has also introduced a new fund named Base Ecosystem, which will invest in early-stage projects that utilise the new blockchain. Additionally, Coinbase Venture's portfolio has a healthy number of projects that could also launch on Base as the network grows. As a result of the announcement, Coinbase's stock price increased, while Optimism's token saw a surge of over 20%.



Over the past nine months, Optimism and Coinbase have been working on EIP-4844, also known as Proto Danksharding. This proposal is a clever way to reduce the call-data costs on Ethereum Rollups by 10-100 times, making the network more efficient and scalable. The importance of this feature has led to a shift in its timeline, moving from a projected 2024 release to a potential Q2 or Q3 2023 release. This development could lead to other market participants deploying L2 solutions on Ethereum, taking advantage of the network's simplicity and potential for use as a settlement layer.

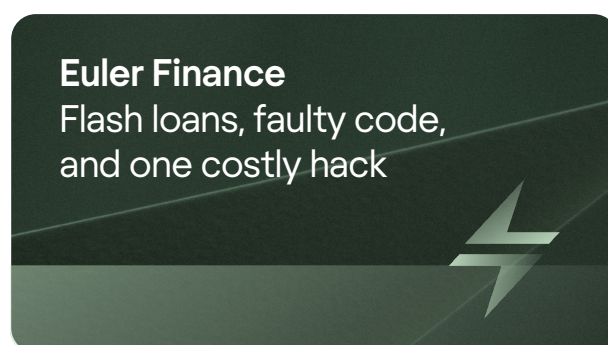
Why is Coinbase's entry into the L2 race important for institutions? As one of the largest exchanges in the world and the largest in the US, Coinbase's entry into the L2 space offers the potential for cheaper and faster transactions compared to other L1s, such as BNB Chain and Solana. Leveraging the scalability and security of Ethereum, Coinbase's L2 also presents opportunities for exploring DeFi, NFTs, and tokenisation within a sandbox environment. One intriguing possibility is the concept of offering gated DeFi, which would allow decentralised protocols to create environments within the Base network that specific institutions could access. While this is merely speculation, it is certainly an idea worth exploring and understanding.

This development has given the market a glimmer of hope and could potentially identify a clear winner in the L1 space. As a result, many players may explore how to deploy a public or private L2 that utilises Ethereum as a settlement network. Coinbase has their own reasons for launching this network, as they believe the future lies on-chain, and their long-term goal is the onboarding of one billion users into the crypto economy.

Only time will tell how developers, users, and the broader market will respond to the launch of this network.

Source:

[EIP-4844: Proto-Danksharding \(eip4844.com\) →](https://eip4844.com/)
[Introducing Base - Blog \(coinbase.com\) →](https://blog.coinbase.com/introducing-base/)



DeFi and lending protocol Euler Finance suffered a flash loan attack in mid-March. Not once, not twice, but repeatedly, resulting in losses of over \$197 million. A flash loan is an exploit used by hackers targeting flawed smart contracts. The hacker managed to steal millions of dollars in digital assets in DAI, USDC, stETH (Staked ETH) and WBTC (wrapped Bitcoin) – becoming the largest hack so far in 2023.

Flash loans are a critical attack vector to consider when battle testing DeFi protocols. Flash loans allow users to quickly borrow funds without needing collateral. These loans must be repaid in full during the same transaction. They are popular among DeFi traders for maximising arbitrage opportunities and swapping collateral. However, flash loans can also be exploited by hackers to manipulate token prices by borrowing large amounts of funds without collateral and buying or short selling tokens with low supply levels.



The Euler Finance platform facilitates borrowing and lending using two tokens: eTokens and dTokens. eTokens represent deposited collateral while dTokens represent debt. Euler issues eTokens based on the types of funds deposited, and when the platform has more dTokens than eTokens, on-chain liquidation is triggered. The hack occurred because the DonateToReserve function of the eToken had a liquidity issue that caused it to burn just eTokens and not dTokens during the conversion of borrowed assets to collateralised assets. The hacker exploited this inconsistency to create a false impression of low deposited eTokens and fake debt.


To execute the exploit, first the hacker obtained funding from Tornado Cash to cover gas fees and create the contracts used in the hack. They then borrowed around \$30 million in DAI from Aave using a flash loan. DAI tokens worth \$20 million were deposited into Euler's platform, where it was converted to eDAI tokens. By taking advantage of Euler's borrowing capabilities, the hacker was able to borrow 10 times the original deposited amount. The remaining \$10 million of the original loan was used to repay part of the acquired debt (dDAI), and the mint function was reused to borrow again until the flash loan was closed. After the hack was complete, the hacker moved some of the funds back to Tornado Cash.

The Euler Labs team issued a \$1 million bounty for any information leading to the hacker's arrest and also extended an offer to the hacker of \$20 million in exchange for not pursuing criminal charges. This move has caused some users to lose faith in Euler, saying they would prefer the bounties to be used to help affected users. Interestingly, the hacker showed some remorse by sending around 100 ETH, valued at approximately \$165K, to a wallet address likely owned by one of the victims.

The victim had previously pleaded on-chain for the return of their "life savings." According to Euler Labs' CEO, the platform had been audited 10 times in the last two years, showing that hacks of this nature require more robust protections and DeFi projects require continuous improvements and further testing.

Source:

[ChainLink – What are flash loans? →](#)



High Court, Jump, and Oasis Multi-Sig A Suspect Collaboration for Funds Recovery in a Semi-Decentralized World

Jump Crypto and Oasis.app collaborated to carry out a "counter exploit" on the Wormhole protocol hacker, recovering \$225 million worth of digital assets and moving them to a secure wallet. The hack occurred in February 2022, with the hacker exploiting a vulnerability in the protocol's token bridge to steal roughly \$321 million worth of wrapped ETH (wETH). The hacker then moved the stolen funds through various Ethereum-based decentralised applications (DApps), including Oasis, which had recently opened wrapped stETH (wstETH) and Rocket Pool ETH (rETH) vaults.



In a blog post on 24th February, Oasis.app confirmed that they received an order from the High Court of England and Wales to retrieve assets related to the Wormhole exploit's associated address. The retrieval was carried out via the Oasis multi-sig and Jump Crypto which was court-authorised. Although the collaboration between Jump Crypto and Oasis.app showcases how semi-decentralised systems can unite to combat malicious activities in the DeFi space, it raises questions about trusting projects that can control users' funds.

One might wonder how contracts that can be controlled by multi-sig wallets work. In contrast to regular contracts, upgradable proxy contracts are used in the automated vaults offered by Oasis. These contracts enable auto-management of a vault's collateralisation ratio based on user-defined parameters. To summarise, Jump Crypto upgraded the automation contract to a new proxy, allowing them to move the collateral and debt from vault 30100 into a new vault under their control, out of the hacker's reach, and recover the stolen funds. It's important to note that this is not an issue with how the contracts work, but rather the Oasis multi-sig or team allowing it to happen due to the court order.

This incident highlights the varying levels of decentralisation, even in DeFi. Often, teams like Oasis.app have more control than users realise. The question is, how should we treat contracts that can be upgraded in the future? This issue remains a subject of discussion in the wider market.

Source:

[Oasis.app →](#)

[Blockworks →](#)



Meet Copper Prime

Michael Roberts

Head of Prime

michael.roberts@copper.co 

+44 (0) 203 836 9170

Franky Gonidis

Head of Financial Risk

fragkiskos.gonidis@copper.co 

+44 (0) 203 836 9161

Dr Eirini Mavroudi

Quantitative Risk Analyst

eirini.mavroudi@copper.co 

+44 (0) 20 7101 9455

Kadar Abdi

Product Associate - DeFi

kadar.abdi@copper.co 

+44 (0) 203 836 9258

Ben Thomas

Asset Optimisation Director

ben.thomas@copper.co 

+44 (0) 203 974 6316

Tobie Dunnnett

Account Manager

tobie.dunnnett@copper.co 

+44 (0) 203 911 7425

Get in touch with Copper Sales

Mike Milner

Head of Sales EMEA

mike.milner@copper.co 

+44 (0) 203 927 8494

Takatoshi Shibayama

Head of Sales APAC

takatoshi.shibayama@copper.co 

+65-9060-0177



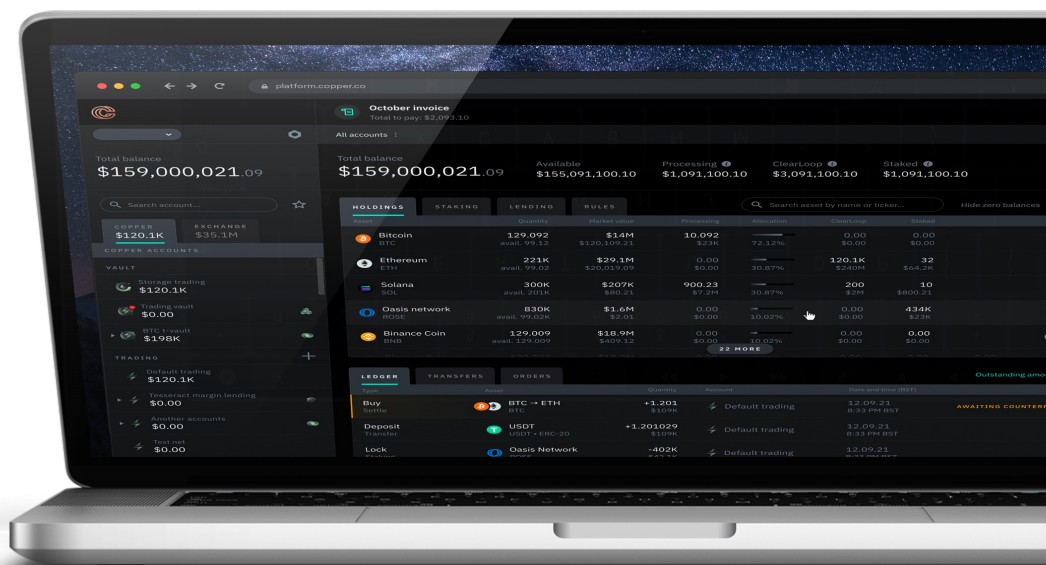
Certified by QMS - Cert No: 351052020



SWISS
BLOCKCHAIN
FEDERATION



OMFIF ISDA



Disclaimer

THE INFORMATION CONTAINED WITHIN THIS COMMUNICATION IS FOR INSTITUTIONAL CLIENTS, PROFESSIONAL AND SOPHISTICATED MARKET PARTICIPANT ONLY THE VALUE OF DIGITAL ASSETS MAY GO DOWN AND YOUR CAPITAL AND ASSETS MAY BE AT RISK

Copper Technologies (Switzerland) AG ("Copper") provides various digital assets services ("Crypto Asset Service") to professional and institutional clients in accordance with the Swiss Federal Act on Financial Services (FinSa) of 15 June 2018 as amended and restated from time to time.

This material has been prepared for informational purposes only without regard to any individual investment objectives, financial situation, or means, and Copper is not soliciting any action based upon it. This material is not to be construed as a recommendation; or an offer to buy or sell; or the solicitation of an offer to buy or sell any security, financial product, or instrument; or to participate in any particular trading strategy in any jurisdiction in which such an offer or solicitation, or trading strategy would be illegal. Certain transactions, including those in digital assets, give rise to substantial risk and are not suitable for all investors. Although this material is based upon information that Copper considers reliable, Copper does not represent that this material is accurate, current, or complete and it should not be relied upon as such. Copper expressly disclaims any implied warranty for the use or the results of the use of the services with respect to their correctness, quality, accuracy, completeness, reliability, performance, timeliness, or continued availability. The fact that Copper has made the data and services available to you constitutes neither a recommendation that you enter into a particular transaction nor a representation that any product described herein is suitable or appropriate for you. Many of the products described involve significant risks, and you should not enter into any transactions unless you have fully understood all such risks and have independently determined that such transactions are appropriate for you. Any discussion of the risks contained herein with respect to any product should not be considered to be a disclosure of all risks or complete discussion of the risks which are mentioned. You should neither construe any of the material contained herein as business, financial, investment, hedging, trading, legal, regulatory, tax, or accounting advice nor make this service the primary basis for any investment decisions made by or on behalf of you, your accountants, or your managed or fiduciary accounts, and you may want to consult your business advisor, attorney, and tax and accounting advisors concerning any contemplated transactions.

Digital assets are considered very high risk, speculative investments and the value of digital assets can be extremely volatile. A sophisticated, technical knowledge may be needed to fully understand the characteristics of, and the risk associated with, particular digital assets.

While Copper is a member of the Financial Services Standard Association (VQF), a self-regulatory organization for anti-money laundering purposes (SRO) pursuant to the Swiss Federal Act on Combating Money Laundering and Terrorist Financing (AMLA) of 10 October 1997 as amended and restated from time to time. Business conducted by us in connection with the Crypto Asset Service is not covered by the Swiss depositor protection scheme (Einlagensicherung) or the Financial Services Compensation Scheme and you will not be eligible to refer any complaint relating to the Crypto Asset Service to the Swiss Banking Ombudsman.

It is your responsibility to comply with any rules and regulations applicable to you in your country of residence, incorporation, or registered office and/or country from which you access the Crypto Asset Service, as applicable.