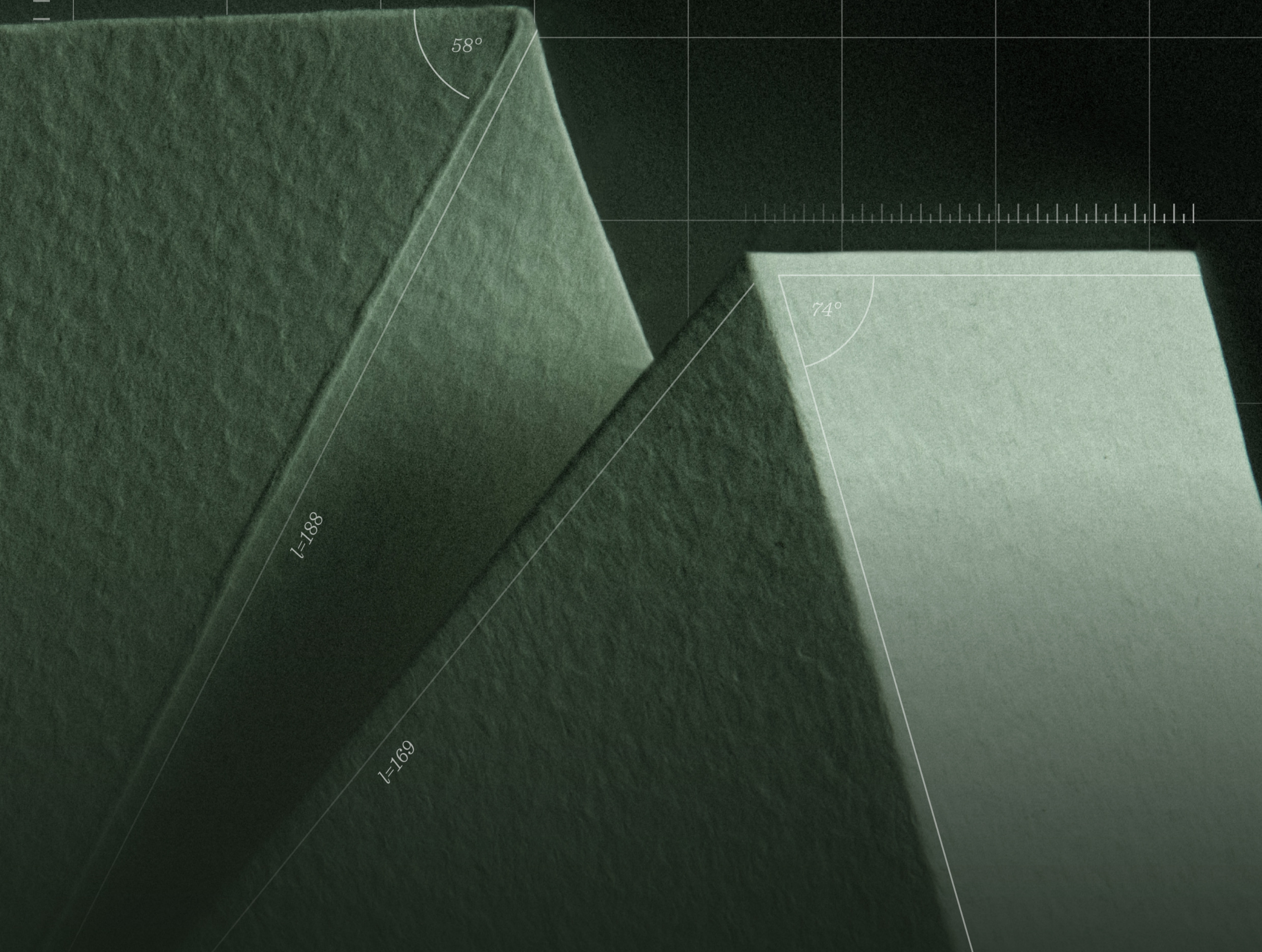
copper.co

Risk Bytes

Newsletter
Volume 12

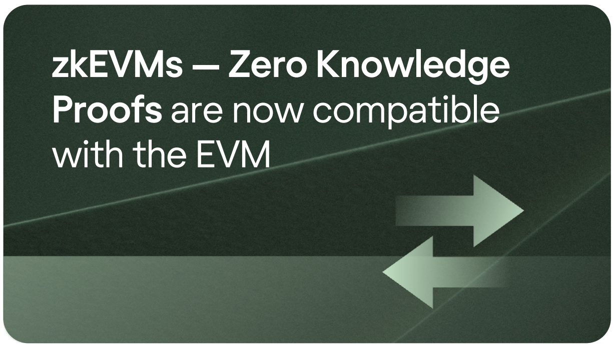


Date
04/05/2023

Risk Bytes Newsletter
Volume 12

copper.co

zkEVMs — Zero Knowledge Proofs are now compatible with the EVM



Over the past year, Layer 2 (L2) scaling solutions have been gaining more attention within the Ethereum community — Coinbase recently built its BASE L2 network on the Optimism stack and Arbitrum launched its token and DAO. One type of L2 scaling solution that has been getting a lot of attention lately are Zero-Knowledge (ZK) Rollups. Unlike optimistic rollups, which rely on fraud proofs to ensure the validity of transactions, ZK Rollups use Zero-Knowledge proofs, more specifically a type of cryptographic proof called zk-SNARKs.

In simple terms, ZK Rollups allow all transactional data to be compressed and stored off-chain while only the cryptographic proof is submitted to the Ethereum network. This means the network only needs to process the proof, which can be verified much more quickly than the full transaction data. This reduces the amount of data that needs to be processed, allowing for more transactions to be processed in a single block.

In the past, ZK Rollups did not have EVM compatibility, which presented challenges for developers to scale them effectively, requiring them to work in newer, less familiar smart contract development environments. However, this is now changing with the launch of zkEVMs.

zkEVMs, or Zero-Knowledge Ethereum Virtual Machines, enable EVM-compatible smart contracts to be executed on ZK Rollups. This means developers can use smart contract development tools and environments they are already familiar with, making it easier for them to build applications on ZK Rollups. With the launch of zkEVMs, it is expected that ZK Rollups will become a more attractive scaling solution for Ethereum. This is because they will provide a familiar and efficient way for developers to build applications on a Layer 2 scaling solution while still maintaining full compatibility within the Ethereum ecosystem.

Recently, there have been several announcements regarding the development of zkEVMs. Polygon's zkEVM is now in Mainnet Beta, Scroll's zkEVM raised $50 million from investors such as Sequoia China & Bain Capital Crypto, while ConsenSys has announced its zkEVM solution, Linea, is live on testnet. It's clear that the adoption of zkEVMs is on the rise, and for good reason.

Let's delve deeper into why ZK Rollups have arguably a more robust approach to ensuring the validity of activity compared to Optimistic Rollups. Both scaling solutions operate an off-main chain layer that enables activity to occur independently of Ethereum's Mainnet by aggregating transaction activity before settling back to the Mainnet. However, they achieve this objective using different approaches.

Optimistic Rollups rely on a game theoretic security model, which assumes that most network participants will act honestly. Dishonest behaviour is punished through the use of fraud proofs. This means that if a transaction is incorrectly processed, anyone can submit a fraud proof to the Ethereum network to prove that the transaction was invalid, and the Rollup will be rolled back to a previous state.

However, this security model requires a high degree of cooperation and honesty from network participants, and it can be vulnerable to attacks by well-funded attackers who are willing to take on the costs of creating fraudulent transactions.

On the other hand, ZK Rollups use a cryptographic security model based on the use of Zero-Knowledge proofs to ensure the validity of transactions. This means that all transactions are checked using cryptographic proofs, removing the need for fraud proofs or other mechanisms to correct invalid transactions. The cryptographic security model of ZK Rollups is arguably more secure than Optimistic Rollups because it does not rely on assumptions about the behaviour of network participants. Instead, it relies on the mathematical security of the underlying cryptographic primitives.

In essence, while both ZK Rollups and Optimistic Rollups are promising Layer 2 scaling solutions for Ethereum, they have different security models that are based on different assumptions about the behaviour of network participants. With the launch of zkEVMs, ZK Rollups are expected to become an even more attractive scaling solution for Ethereum, providing a familiar and efficient way for developers to build applications on an L2 scaling solution while still maintaining full compatibility with the Ethereum ecosystem. This makes ZK Rollups an ideal solution for financial primitives, especially those involving high-value transactions, such as DeFi and tokenisation.

On a final note, as the infrastructure for zkEVMs becomes more robust, it's becoming clear that the EVM standard is emerging as the model for blockchains and smart contract frameworks.

The adoption of zkEVMs is expected to make Ethereum an even more attractive base layer for other developers and market participants.

An interesting thesis is that Ethereum could become something akin to Cosmos with zkEVMs and application specific L2s all using Ethereum as their settlement layer. Overall, the rise of zkEVMs is an exciting development in the evolution of the Ethereum ecosystem.

Source:
Coinmarketcap →
ChainLink →
Blockworks →

Firedancer
— Solana's third party validator

At a time when L2 scaling solutions are in the spotlight, building key infrastructure to improve the speed, scalability and security of their Layer 1 (L1) counterparts, existing L1 blockchains are working on key enhancements of their own. Highly regarded as one of the most promising L1 blockchains in recent years, Solana is on a mission to return to its place at the top through its collaboration with Jump Crypto to develop a next-generation Validator client, named Firedancer.

While Solana is able to process transactions at faster speeds and lower costs compared to Etherem, the network has struggled with outages since its launch. The most recent outage in February 2023 resulted in the network halting for 18 hours, adding to concerns regarding its stability.

As part of a project ongoing since 2022, Jump Crypto are building an additional full validator client for Solana. When the project began, there was only one full validator client in existence, originally launched by Solana Labs, but we have since seen the introduction of the first third party validator client on Solana by Jito Labs. Currently, approximately 16% of the network's stake runs through the Jito client, with high incentive for validators as it maximises MEV (Maximal Extractable Value) rewards. MEV rewards are additional revenue earned by validators in exchange for favourable ordering of transactions within a block.

With an extensive background in high-frequency trading, one of Jump's key goals with the development of Firedancer is to increase the network's performance and attractiveness towards quantitative traders and their strategies. Unlike the original validator client, written in Rust, Firedancer is written in C/C++, allowing for comhighly efficient use of computer hardware. Speed and efficiency are paramount to success in the HFT space, as the strategies rely on finding an edge amongst peting software. In a space where liquidity is often fragmented due to consistent innovation, increased HFT activity could lead to more efficient markets through the reduction of spreads and higher liquidity.

Overall, the introduction of new validator clients is a welcome move for the space, as the improved user experience combined with an enhanced competitive edge will help to propel innovation amongst the community, whilst contributing to a safer and more secure network.

Sources:
Jump Crypto →
The Block →

Ethereum's Shanghai impact —Institutional Investors have upped the stakes

Ethereum's Shanghai (AKA Shappella) upgrade, the follow up to the Merge, has allowed Ethereum stakers to withdraw their staked assets for the first time. In the run up to the upgrade, there was a widely supported narrative in the markets that this would cause a drop in Ethereum's price as stakers withdrew their holdings en masse and looked to take profits.

The good news for Ethereum holders is that this hasn't come to pass thus far, with just 4% of total staked ETH due to be withdrawn, demonstrating the Ethereum ecosystem's stability. Currently around 18.1 million Ether is staked to the network with a value around $33 billion according to data from CryptoQuant.

The aftermath of the upgrade was also met by an uptake in staking by institutional investors. April saw a three-fold increase of in-flows of staked Ethereum by institutions , with an 80% increase taking place after the upgrade went live on 12th April. Between the 13th and 16th April, around 1.1 million ETH was staked, while around 921,579 were removed, resulting in a net positive flow of staked ETH. After this immediate post-upgrade spike, staked ETH levels returned to their pre-upgrade levels, revealing the selloff narrative was incorrect, at least in the short term.

According to a survey by Kiln in February, 68% of institutional investors said they were looking to increase their staked holdings after the upgrade. Now we're a few weeks out, we can see a total of around 24,640 ETH has been subsequently added to staking pools. This news will be a vote of confidence for Ethereum's development and its supporters, especially among other institutional investors that are unsure of Ethereum.

In related post-Shanghai news, Liquid Staking Derivatives (LSDs), such as Lido, have seen their share of total value locked (TVL) surpass DEXes (decentralised exchanges) for the first time. This was due to a sharp decline in the value held on DEXes of around $1.66 billion, while LSDs saw their value increase by $280 million.

LSDs were used as an alternative staking mechanism to direct staking on the Ethereum network as they provide stakers with LSD tokens that can be used for trading to free up locked up liquidity. Now that withdrawals are possible thanks to the Shanghai upgrade, it will be interesting to see how this effects the long term value held on LSDs.

In the short term, current LSDs have arguably lost one of their key selling points in offering withdrawals, which could lead to more experimental and novel forms of LSDs emerging as viable competitors looking to capture some of Lido's 30% market share of total staked ETH.

Sources

CoinDesk →
CryptoQuant →

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 Dunnett

Account Manager

tobie.dunnett@copper.co

+44 (0) 203 911 7425

Get in touch with **Copper Sales**

Mike Milner

Head of Sales EMEA

mike.milner@copper.co

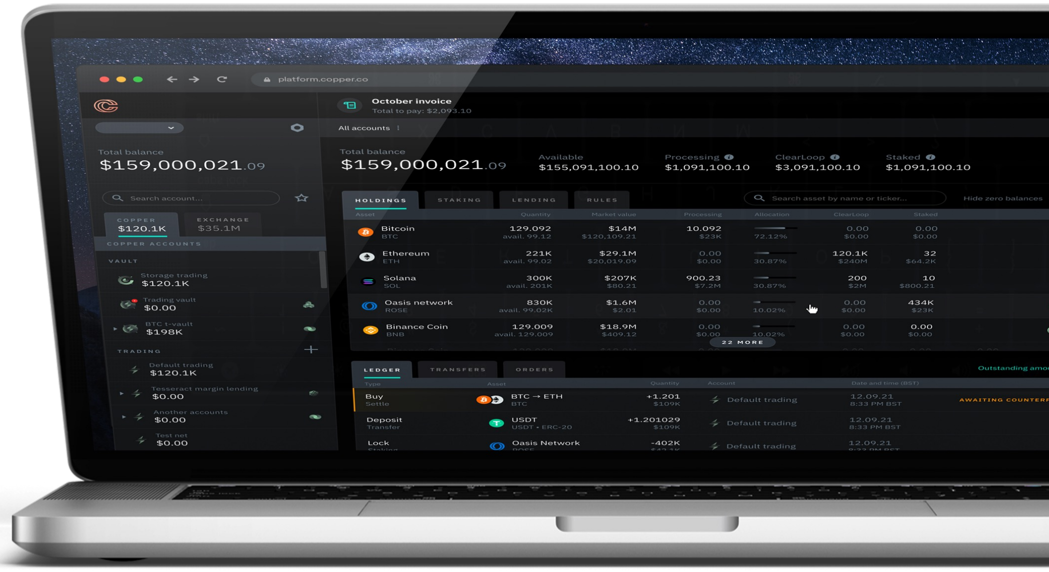
+44 (0) 203 927 8494

Takatoshi Shibayama

Head of Sales APAC

takatoshi.shibayama@copper.co

+65-9060-0177



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.