DLResearch x Zircuit

ZIRCUIT

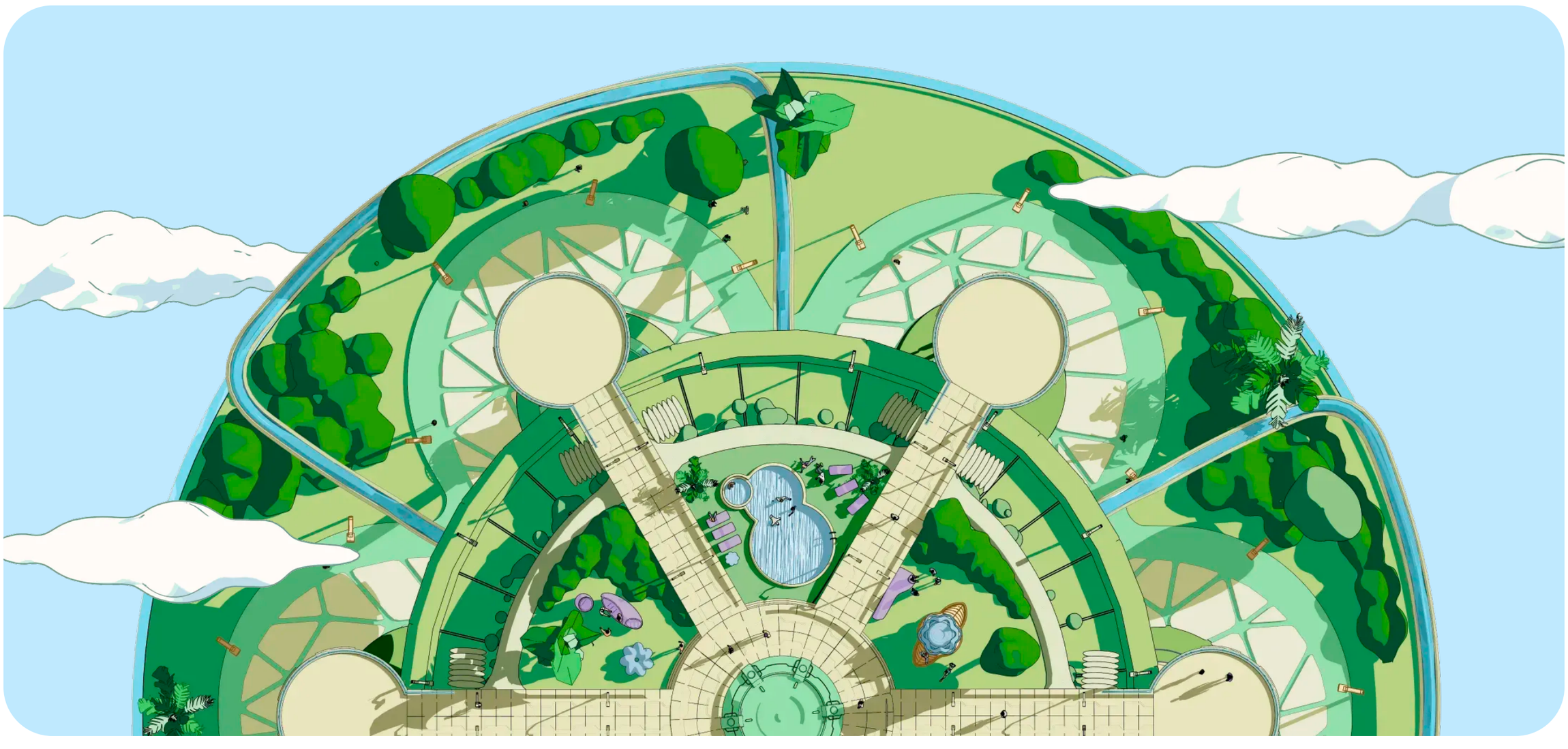
The L2 with AI-enabled Security

www.dlnews.com/**research**

Zircuit: The L2 with AI-enabled Security

The layer 2 (L2) ecosystem has truly taken off, transforming how we interact with blockchains and opening up a host of new use cases. L2s originated in the need to tackle scalability issues on Ethereum. They reduce gas fees and facilitate higher throughput, offloading a sizable chunk of execution from the main chain to reduce network congestion and boost overall performance. L2s relieve the work and stress of Ethereum developers and have paved the way for more functional and accessible decentralised applications (dApps).

The L2 landscape is crowded, and it's hard to stand out. But one protocol is making its way through the noise, attracting column inches, big-name investors, and a community that has already staked billions... and it's done it all in the testnet phase. With Phase 1 of its mainnet launch now under its belt and Phase 2 imminent, we take a closer look at Zircuit.



What is Zircuit?

Founded in 2022, Zircuit is led by a team with solid web3 chops and research emphasis. Zircuit is an Ethereum rollup using zero-knowledge tech, a privacy technique that validates transactions without revealing their full details. It has long-term ambitions to become a fully functional ecosystem that supports lending protocols, oracles, DEXs, and stablecoins. Currently, the focus is on launching its mainnet. Phase 1 went live in early August, with the second public phase expected in a few weeks later.

Zircuit was born from research conducted by veterans in web3 security and scaling. The team behind Zircuit identified rollups as critical to Ethereum scaling and went all in on investigating the space. The resulting research identified an opportunity to proactively enhance blockchain security, eventually founding Zircuit and its sequencer level security.

The team sees Zircuit's security offering as its defining feature — and for good reason. It is helping it stand out in a crowded L2 marketplace by offering users and developers a secure environment for their projects. Co-founder Martin Derka is on the record stating that the protocol is also exploring ways to optimise its zero-knowledge-proof technology to increase efficiency and reduce operating costs. To that end, Zircuit's research focuses on performance as well as security. Through the help of multiple L2 grants from the Ethereum Foundation, Zircuit's current research areas include security tooling, rollup compression, and cryptography.

The challenges of decentralisation

Blockchain's decentralised nature complicates the coordination of swift, effective responses to potential security attacks. Unlike centralised systems, which can more easily preempt attacks, the decentralised framework restricts the available options for addressing such challenges. In the case of hacks or bad actors, most blockchains have to temporarily centralise decision-making to pause the network, roll back transactions, or implement forks in response to breaches.

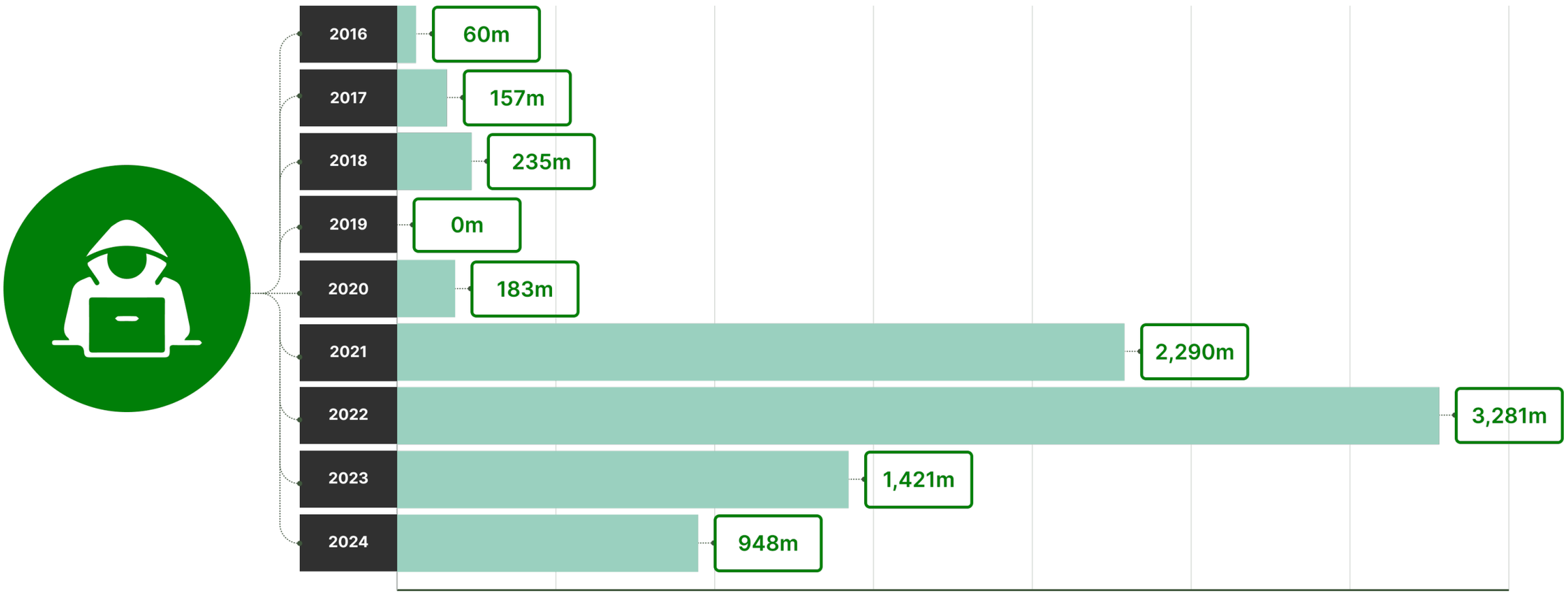
The history of blockchain is littered with examples of centralised responses. In 2010, an integer overflow allowed attackers to introduce a block to Bitcoin that created over 184 billion Bitcoins (the protocol has an upper limit of 21 million). The community responded by releasing a soft fork to invalidate the impact. A backward-compatible update, the soft fork restored Bitcoin to the point before the hack, invalidating several blocks and removing them from the chain to restore it to an earlier state. It was helpful that this occurred during the chain's nascency and could be rectified early. If it happened today, the impact would be catastrophic, disrupting trading, cancelling any transactions made after the hack, and decimating confidence in the cryptocurrency.

Six years after the Bitcoin hack, an attack on The DAO protocol on Ethereum resulted in the theft of around 5% of all $ETH in circulation at the time. A controversial coordinated hard fork was used to address the attack. Unlike a soft fork, a hard fork is not backward-compatible and often represents a fundamental change to the network's rules. This means every node needs to upgrade to continue participating. Otherwise, a permanent split occurs, resulting in two incompatible chains. The DAO's fork rewrote the ledger, and Ethereum forked into Ethereum (upgraded) and Ethereum Classic (original). This set the clock back to before the hack and reversed its effects, returning the hacked funds to their original owners and leading many to question if blockchain could really claim immutability.

In 2022, Binance Smart Chain (BSC) suffered a bridge hack that saw $560 million of its native token, BNB, stolen from its official bridge. Binance reacted by temporarily suspending deposits and withdrawals on BSC. Then, Binance introduced a blacklist mechanism and hard fork to combat the hack. This incident is one of many, as the decentralised finance space has seen a significant number of security breaches. According to data from DefiLlama, the total value of hacks in DeFi has now reached an alarming $6 billion.

These incidents highlight the challenges decentralised networks face when addressing attacks. Further, there is a lack of tools in their arsenal to detect, isolate, and block them without reverting to a centralised approach.

GRAPH 1. **TOTAL VALUE HACKED SINCE 2016**



Source: **DefiLlama**

The invention of SLS

Ethereum rollups are designed to scale transaction throughput by batching transactions off-chain and submitting them as a single transaction to the main chain. This approach maintains a separate blockchain state and provides a checkpoint for security before transactions are finalised on the main chain. However, like Ethereum itself, rollups lack mechanisms to evaluate transactions before they are included in the blockchain.

Sequencers play a vital role in the efficiency of L2 rollups by processing and ordering batches of transactions before submitting them to the Ethereum base layer for inclusion in a block. Typically, these rollups operate under a centralised sequencer that determines the order of transactions within a batch and assigns them to blocks.

Zircuit's research identified a crucial opportunity to enhance rollup security by adding a layer of protection at the sequencer level. This led to the development of Zircuit's Sequencer Level Security (SLS) for rollups. As described by Martin Derka to CryptoPotato, SLS is a sequencer that actively checks for malicious intent before including a transaction in the block. Derka stated, "We use artificial intelligence to simulate transactions and assess their impact, determining if they're hacks."

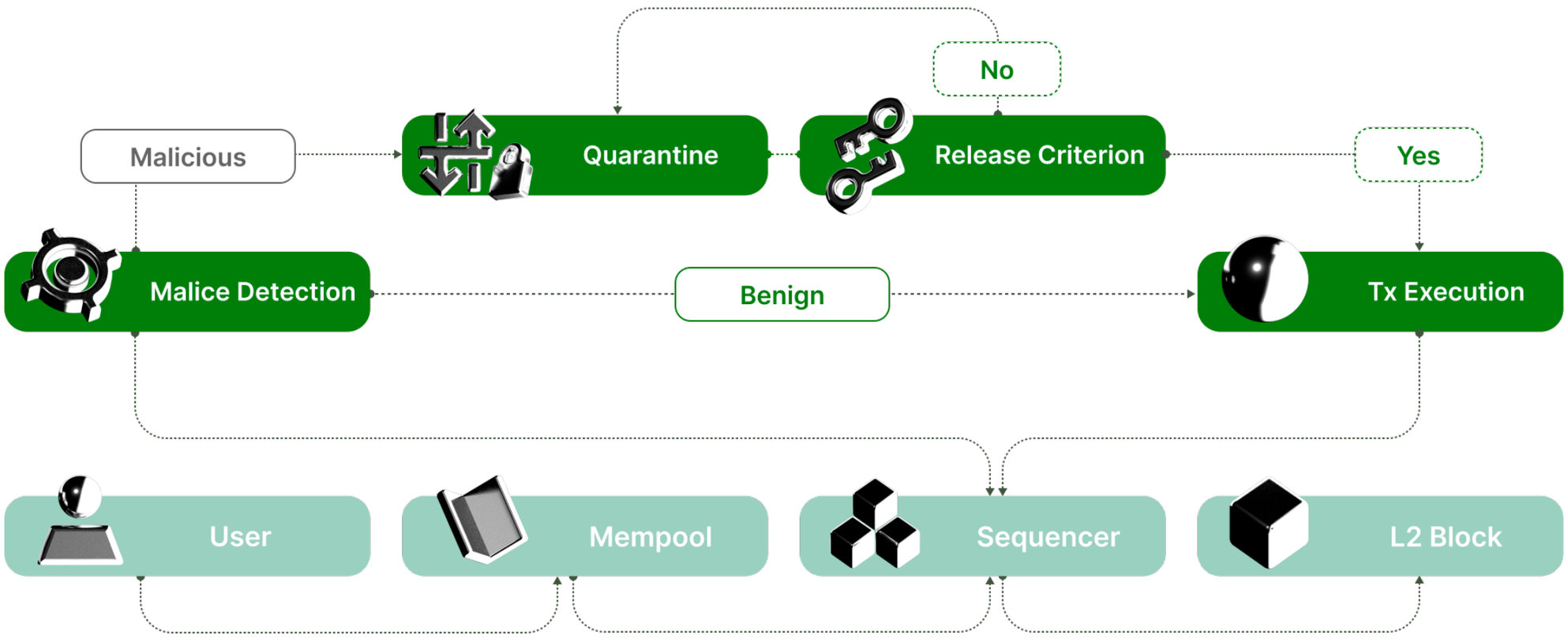
In essence, SLS is a specialised transaction sequencer that integrates Zircuit's AI security software, automatically assessing the potential impact of each transaction before it is included on-chain. If any suspicious activity is detected, Zircuit's system can quarantine potentially harmful transactions before they reach the main chain.

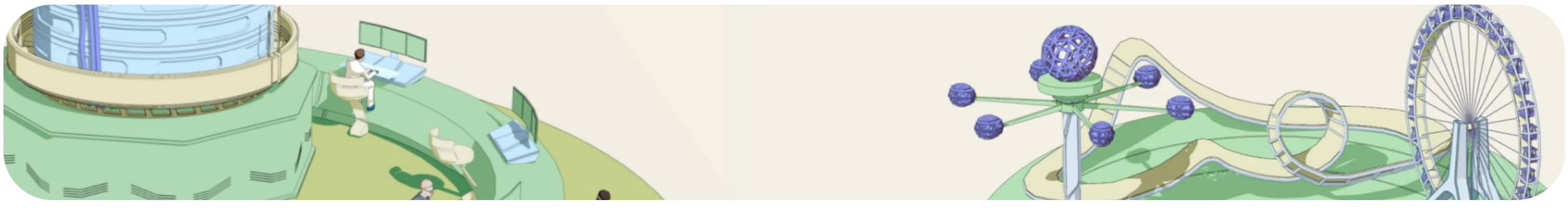
The SLS protocol consists of three core components: a malice detection engine, quarantine release criteria, and transaction execution.

Malice detection engine

Once a transaction arrives at the SLS sequencer, it routes it to the Malice Detection Engine. Referred to as the 'Oracle' by the Zircuit team, the Malice Detection Engine simulates every transaction in the batch using the current state of the network (i.e., the last block added). The data generated by these simulations is used to classify transactions, grouping them into either benign or potentially malicious. This initial simulation also identifies any dependencies between the transactions. If executing one transaction in the batch may change the outcome of another, they're grouped together as dependent. These are then listed for sequential simulation.

GRAPH 2. **ZIRCUIT'S SEQUENCER LEVEL SECURITY**





All transactions deemed safe are queued for block inclusion. Dependent transactions that were too complicated or took too much time to fully analyse defer to the next cycle and repeat the process to be considered for inclusion.

If deemed malicious, those transactions divert to a holding area, called the Quarantine-Release Criterion module. Any transactions held here cannot be executed or included in a block. Each transaction is verified against specific release criteria and will either be released if it meets these criteria or dropped from the mempool once it meets retirement criteria. The exact criteria for each is determined by the sequencer.

Quarantine release criteria

With every new block added, the sequencer checks any quarantined transactions against retirement and release criteria.

RETIREMENT
Transactions will be retired if the nonce (a unique number assigned to each transaction) is no longer valid or too many transactions clutter the mempool.

RELEASE
A number of criteria can determine if transactions are released from quarantine. These include:

FAILURE: Transactions that fail due to changes in the chain's state can be safely included in the block and are released.

TIME: A reaction time allowing users to react to malicious transactions is baked into a time criterion. If the transaction has been quarantined beyond this time — set to years by default — it can be released and considered for inclusion again.

ADMINISTRATION: An administrative criterion is in place for any false positives flagged by the sequencer, allowing administrators to override transactions that are incorrectly labelled as malicious.

ECONOMIC: This criterion gives accounts that submitted a flagged transaction the option to stake collateral that will be slashed (i.e., imposed as a penalty) if the transaction does turn out to be damaging. A transaction meets this criterion if the damage the sequencer expects it to cause is less than the amount staked.

Transaction execution

The third component of the SLS protocol is transaction execution. Transactions released from quarantine are eligible to be considered for inclusion in the next block, providing they meet the sequencer's rules.

The SLS protocol can recognise resubmitted transactions by account address, transaction data, and value, therefore it won't resubmit them to quarantine. For example, in the case of a transaction quarantined for being underpriced (i.e., the transaction fee was too low to meet network conditions at the time) but was then resubmitted with the right fee, the protocol will recognise it as a resubmitted transaction and prevent a repeated quarantine.

LST and LRT liquidity

Zircuit's SLS is designed primarily to enhance security within the network. However, by operating as an L2 solution, there are additional benefits. It reduces congestion by processing transactions off-chain, which not only increases transaction efficiency but also results in lower network fees and higher throughput compared to the Ethereum mainnet. Zircuit aims to leverage this combination of security and efficiency to establish itself as a major hub for staked assets.

Liquid Staking Tokens (LSTs) represent assets staked on a proof-of-stake network. They allow users to stake assets without locking them up, providing the flexibility to participate in staking while still transacting with the staked asset.

Liquid Restaking Tokens (LRTs) take this concept further. With LRTs, users can stake assets multiple times, enabling them to secure multiple protocols simultaneously, thereby enhancing capital efficiency.

While LSTs for staked assets like ETH have been available for several years, LRTs are relatively new, with new protocols emerging frequently. This has led to liquidity being spread across various networks, making it challenging for users to track different protocols and assess their safety.

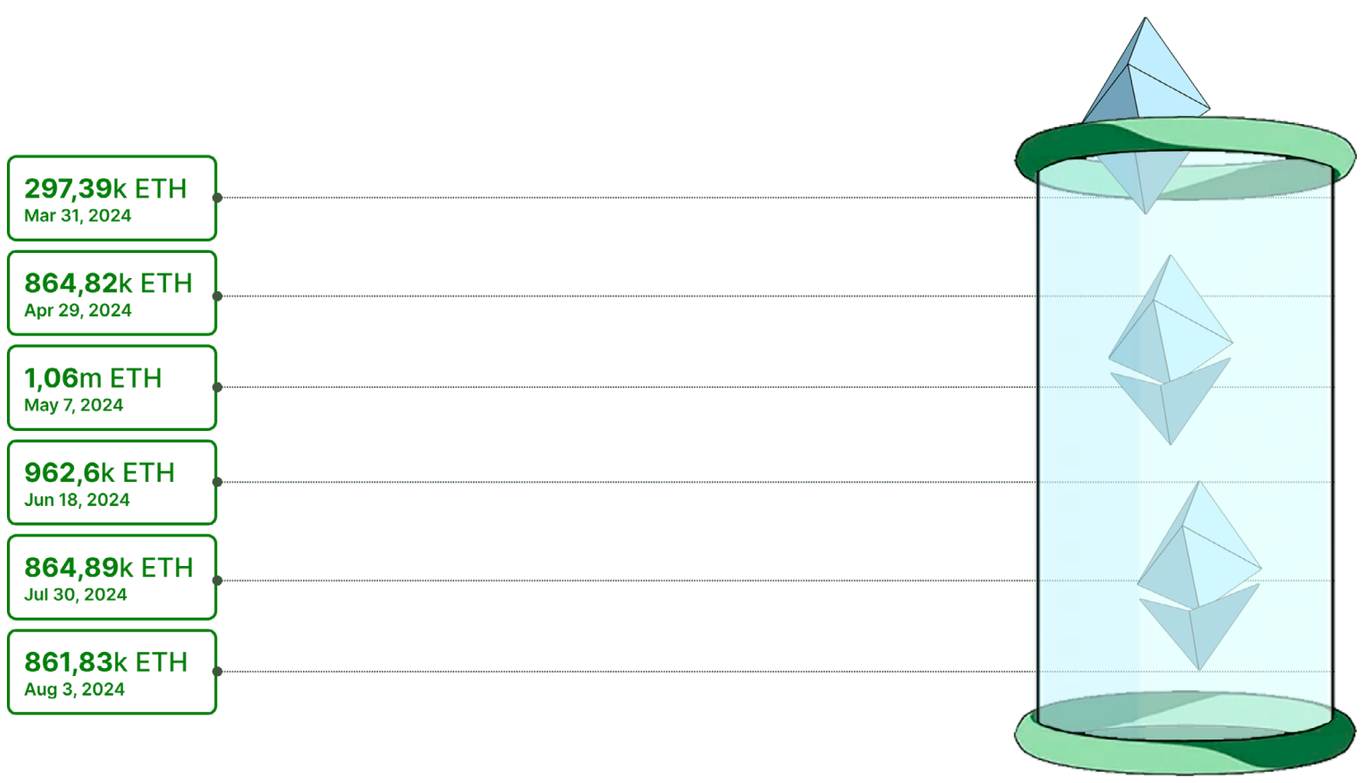
Zircuit aims to address these challenges by becoming the definitive liquidity hub for ETH, BTC, LSTs, and LRTs. The ultimate goal is to simplify capital allocation for users while ensuring that Zircuit's robust security measures provide confidence that funds are deployed in high-quality, safe protocols.

The rise of Zircuit staking

Even before its mainnet Phase 1 launch, many in the community signalled that they agreed with Zircuit's approach. Earlier this year, the network bootstrapped liquidity by partnering with select LST and LRT protocols and launching a points programme.

The programme allows users to earn points for engaging with the network; these generally convert to tokens at a later date. The earlier users deposit, the less diluted — and more valuable — their rewards should be, which in turn attracts airdrop farmers (users who engage solely for a future airdrop) to nascent projects. The first conversion of points to ZRC tokens happened alongside the Phase 1 launch on August 5, which saw 7% of the total ZRC supply distributed to 262,200 point holders. These tokens are currently non-transferable until a later date.

GRAPH 3. **MONTHLY HIGHEST POINTS OF TVL IN ZIRCUIT STAKING (MARCH 4TH-AUGUST 13TH)**



Source: **DefiLlama**

In addition to the points programme, Zircuit has introduced a unique feature called Gas Mining. This approach rewards users based on the gas they spend on transactions: for every ETH spent, users earn 125% back in ZRC tokens. This mechanism not only incentivizes transactions within the network but also enhances user engagement by directly rewarding their activity.

Assets staked in the Zircuit staking contract earn varying yields. These include:

- Staking rewards for securing the Ethereum network.
- Rewards from actively validated services (AVS) secured by restaking — such as EigenLayer.
- Rewards from LST and LRT partners.
- Zircuit points which convert to ZRC tokens.

The points programme and yield incentives worked as an incentive. In April, an influx of airdrop farmers saw deposits on Zircuit top $80 million in just 24 hours. By May, the Total Value Locked (TVL) in Zircuit had reached a staggering $3.5 billion. While it has since pulled back under the $3 billion mark, if the majority of these assets do transfer to the mainnet this would give Zircuit a TVL to rival established Ethereum rollups like Base and Blast from day one.

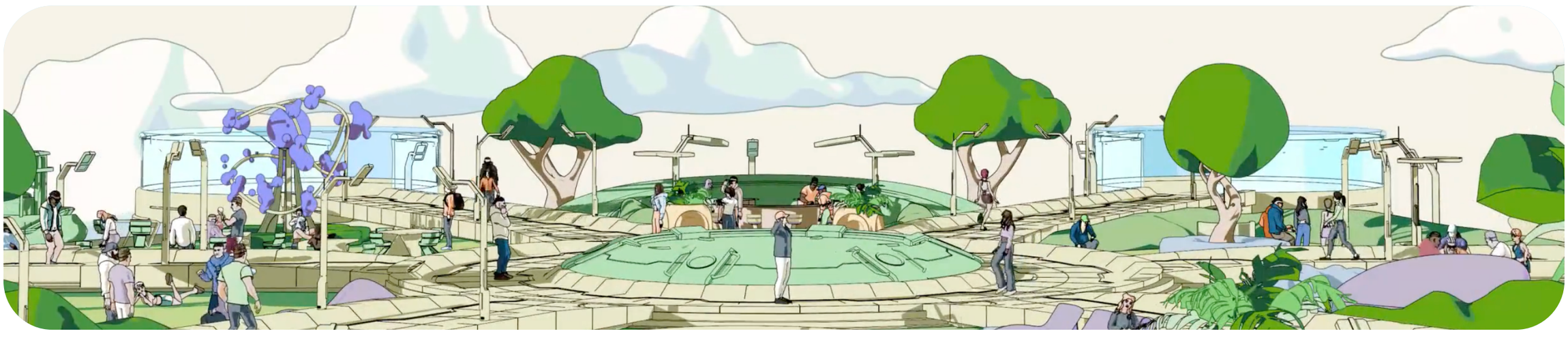
The future of LRTs

The Zircuit team anticipates that LRTs will follow a similar adoption curve to LSTs, which are known for their ease of use, safety, and attractive yields. Due to these qualities, LSTs have seen widespread adoption within the crypto ecosystem. Zircuit sees LRTs as having similar potential for appeal.

However, the current fragmentation of the ecosystem is unsustainable, and as the LRT category matures, Zircuit expects key differentiators to emerge. These include yield rates, the assets secured by the tokens, management structures, slashing risks (potential losses from protocol penalties), and the degree of decentralisation.

Aiming to become a major liquidity hub, Zircuit is actively supporting the development of LRTs. It currently partners with Renzo, Mellow LRT and Kelp DAO, and others, with plans to expand its network of reputable protocols. Zircuit is also working on integrations to enable native staking on its network, which will secure other protocols beyond its rollup, thereby enhancing the utility of its staking capabilities and potentially increasing rewards and use cases for its users.

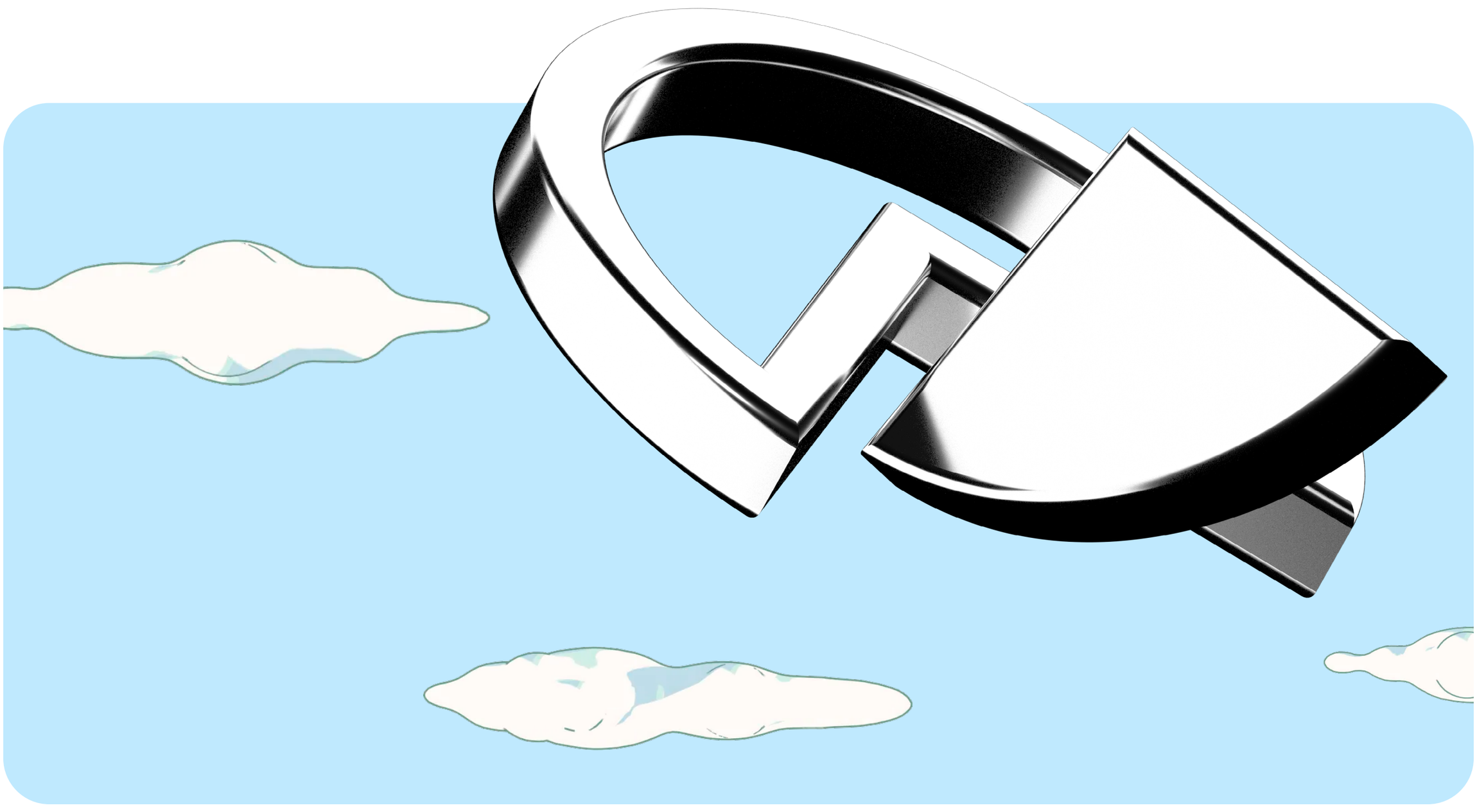
Zircuit is positioning itself as the go-to platform for users seeking trustworthy LST and LRT protocols and convenient yield opportunities. The success of its liquidity bootstrapping campaign suggests that Zircuit has a strong chance of achieving this goal. If it can maintain a total value locked in the billions, it will become an attractive ecosystem for LST and LRT developers and partners.



Beyond the hype

Zircuit has hit several impressive milestones and built an engaged community during its testnet phase. Its $3.5 billion TVL aside, Zircuit is underpinned by impressive research and genuine innovation. Its SLS technology provides a framework for identifying and quarantining malicious transactions before they reach the main chain and could set a new standard for security within L2s that inspires other protocols to enhance their security by adopting or developing similar technologies.

If Zircuit can translate the excitement around its points programme into loyalty and retain users once its mainnet goes live, then the rollup could quickly become a mainstay of the Ethereum ecosystem.



DLResearch x Zircuit

ZIRCUIT

L2 with AI-enabled security

www.dlnews.com/**research**