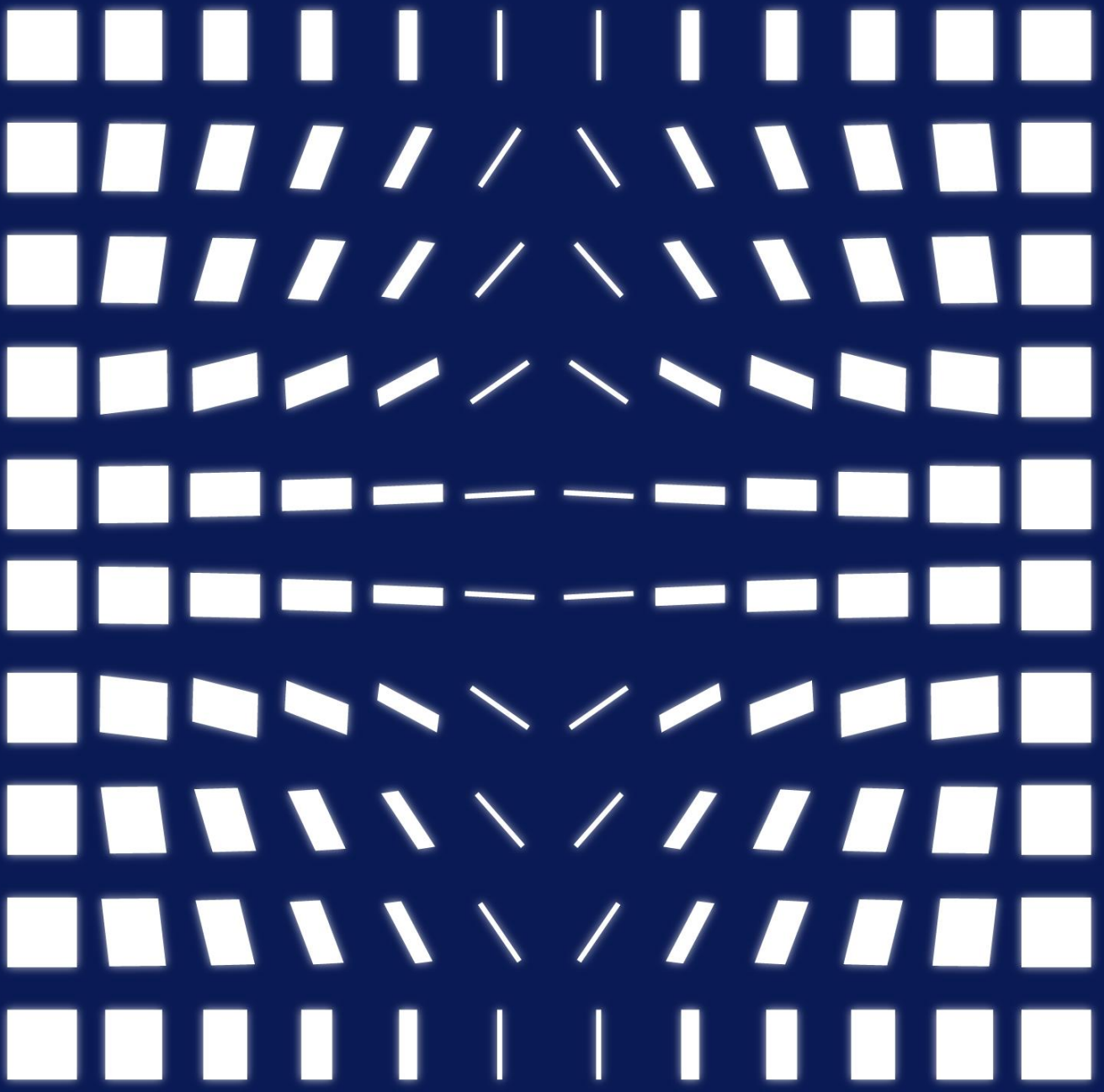
Huobi Research

How Far is Rollup from Maturity: A Dive into Rollup's Development Path



Author: Huobi Research Institute / Barry Jiang

How Far is Rollup from Maturity:

A Dive into Rollup's Development Path

Abstract

The current Ethereum Layer 1 chain is too busy to fulfill most of the demand in the market, Rollup has become the most feasible solution for scaling. However, Rollup's performance has not been as stellar as expected – its TVL only occupies around 5% of the market, less than 20 % of projects have been migrated using Rollup, and active addresses account for less than 1%. This data seems to indicate that Rollup has not been broadly accepted by the market. There are four possible reasons for this:

1. Poor user experience - Optimistic Rollup can only complete a cash-out activity when the challenge period closes. OP's transaction fee is not low enough to entice users. Plus, interoperability among various Rollup types is low, which causes a barrier to inflow of funds.
2. Low capital efficiency Predominantly the issue of fragmented liquidity and lower capital efficiency.
3. Security - Users are concerned with potential security flaws in Rollup
4. Compatibility with EVM As ZK Rollup is incompatible with EVM, it is unfeasible for applications to migrate.

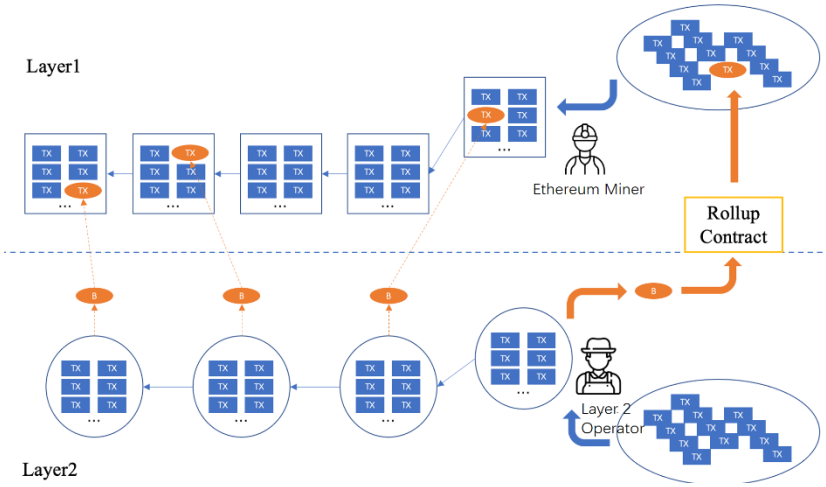
<u>Possible solutions:</u>

1. To improve user experience, more effort needs to be focused on bridging and enabling more convenient deposits via exchanges., Fees could be reduced due to less data upload, increasing off-chain processing efficiency.
2. Capital efficiency could be enhanced by concentrating liquidity.
3. To elevate the level of security, further focus decentralized operations and insertion of forced cash-out rules are desirable.
4. Difficulty of application migration could be mitigated by more R&D on zkEVM.

1 Status Quo of Rollup

Rollup carries vast expectations as being the solution to scaling. The main idea of Rollup is around allowing users to trade off-chain, and data produced from the off-chain transactions and the proof of status off-chain will be condensed and submitted by Layer 2 operators and verified by verifiers on Ethereum (or other Layer 1 chains). As more efficient coding and less data upload takes place, the number of bytes consumed for Ethereum to store the data has been lowered. At the same time, gas fees could be reduced as Ethereum does not need to recalculate the transaction off-chain. According to statistics, fees spent for Optimism and Arbitrum are merely 10%-30% of those on the Ethereum Mainnet, with fees for zkRollup are being less than 5% of those of the Ethereum Mainnet. Rollup thus could be the evolution to Ethereum in terms of decentralization and security, being the unparalleled Layer 2 solution, with its reduced on-chain consumption and retained availability of data that Ethereum Mainnet has access to, which no one could forge off-chain. Vitalik himself too said, “For Ethereum, Rollup may be the only solution to scaling without necessary trust in the short term, even in the long run.”Rollup carries vast expectations as being the solution to scaling. The main idea of Rollup is around allowing users to trade off-chain, and data produced from off-chain transaction and the proof of status off-chain will be condensed and submitted by Layer 2 operators and verified by verifiers on Ethereum (or other Layer 1 chains). As more efficient coding and less data upload takes place, the number of bytes consumed for Ethereum to store the data has been lowered. At the same time, gas fees could be reduced as Ethereum does not need to recalculate the transaction off-chain. According to statistics, fees spending for Optimism and Arbitrum are merely 10%-30% of those on the Ethereum Mainnet, with fees for zkRollup are being less than 5% those of the Ethereum Mainnet. Rollup thus could be the evolution to Ethereum in terms of decentralization and security, being the unparalleled Layer 2 solution, with its reduced on-chain consumption and retained availability of data that Ethereum Mainnet has access to, which no one could forge off-chain. Vitalik himself too said, “For Ethereum, Rollup may be the only solution to scaling without necessary trust in the short term, even in the long run.”

■ **Figure 1.** Workflow of Rollup in Scaling



Source: Huobi Research

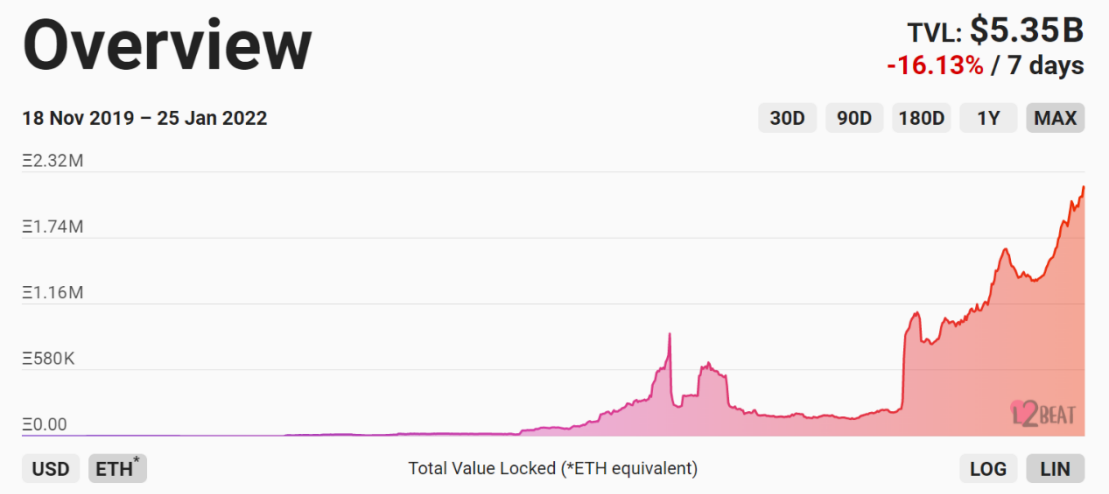
Rollup can be classified into two categories by whether the verifier on Ethereum Mainnet needs interaction with assertions uploaded from Layer 2 – Optimistic Rollup (OP) and ZK Rollup (ZK). OP operates under optimistic assumption — it assumes Layer 2 operators will condense and upload off-chain transactions "as is"— It is unnecessary for Layer 2 operators to prove innocence if no proof of guilt from Layer 1 verifiers is received in a certain time period; data for on-chain submission from Layer 2 operators are deemed valid. For convenience on Layer 1 verification, OP needs to upload an assertion, including intermediate state of off-chain operations, elaborating actions of Layer 2 operators. If Layer 1 verifiers suspect OP, fraud statement will be submitted, revealing a false OP statement.

As opposed to OP, ZK establishes the scheme that Layer 2 operators must prove themselves innocent. That is to say, data submission for an on-chain request is only deemed valid when Layer 2 operations match the transaction data to upload. For more convenient verification, ZK needs to submit a proof of validity, which is a zero-knowledge proof that reflects the off-chain transaction. Thus, Layer 1 verifiers can complete the verification with less effort thanks to the quick verification process in zero-knowledge proof.

In less than 2 years, Rollup has achieved considerable development. However, in terms of capital volume, number of projects and number of addresses, the proliferation of Rollup may not be as smooth as we think.

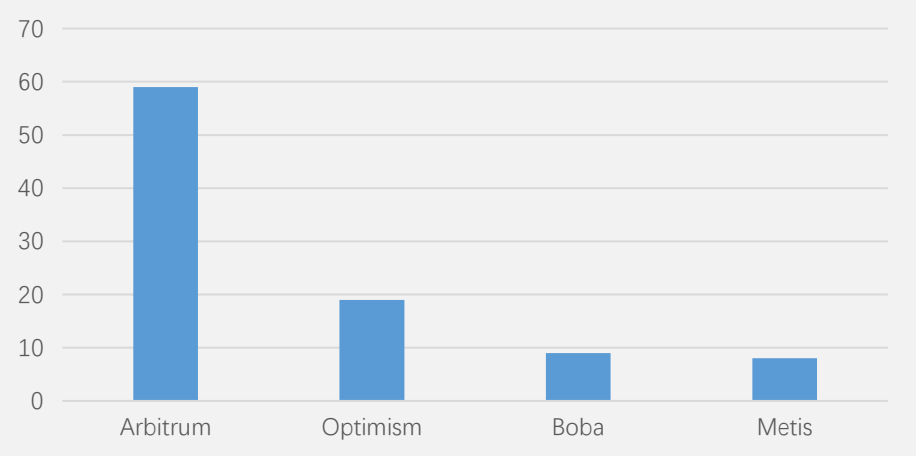
Firstly, capital volume has increased tremendously. According to 12beat, Layer 2 Rollup TVL increased from 20,000 ETH at the end of 2020 to 2.172 million ETH as of Jan 25, 2022, roughly 108[1] times more. Comparatively, Rollup TVL merely accounts for 4.5% of the Ethereum Mainnet.

■ **Figure 2.** Total Rollup TVL



Secondly, deployment numbers wise, Rollup projects are heavily OP focused, especially on the four largest OP platforms: Arbitrum, Optimism, Metis and Boba. According to DeFiLlama, the number of projects being deployed on Rollup is roughly 80, or around 19.3% of the 415 projects on the Ethereum Mainnet, indicating Rollup still has some way to go.

■ **Figure 3.** Number of Projects on Top 4 OP Platforms



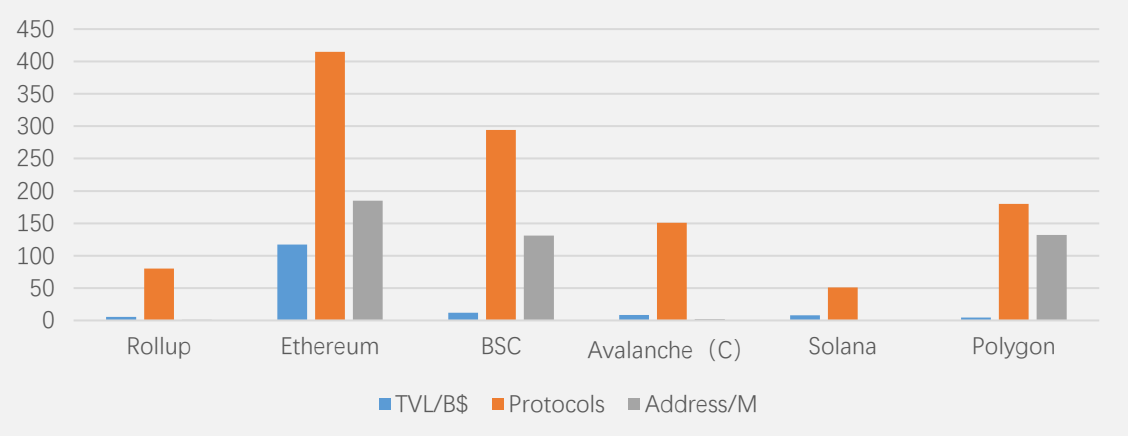
Source: DeFiLlama, Huobi Research

[1] Price of ETH is volatile, so ETH is used as unit price instead of USD.

Furthermore, based on the number of addresses at first glance, Rollup is still in a primitive phase of development. By rough estimation of publicly released addresses from multiple Rollup blockchain browsers, there are 1 million Rollup addresses, compared to 185 million addresses on Ethereum (less than 1%). According to the Diffusion of Innovations Theory, which seeks to explain how, why and at what rate new ideas and technology spreads, Rollup is mostly adopted by innovators, which account for less than 2.5% of the market, so Rollup has a long journey yet to gain mainstream recognition.

Lastly, while Rollup has considerable capital volume, with some projects willing to migrate from Layer 1, it appears to be less appealing for most projects.

■ **Figure 4.** Comparison of Rollup to Ethereum and Other Layer 1 Chains



Source: DeFiLlama, Blockchain Browsers, Huobi Research

2 Reasons Rollup is not yet Mature

Reasons why Rollup is still developing could be endogenous and exogenous. A new technology per se proliferates with time, and the overall market status impedes the pricing of gas and various campaigns. Besides these exogenous variables, other obstacles need to be tackled within Rollup itself.

In my humble opinion, there are four possible causes that have bottlenecked the development of Rollup:

2.1 Poor User Experience

2.1.1 Challenging Period for Withdrawal on OP

As the nature of OP relies on an optimistic assumption, uploaded data will be deemed valid as long as Layer 1 verifiers cannot prove Layer 2 operators wrong; a certain time period will be reserved for security, which is the so-called challenging period. A withdraw operation is invalid during this period as it has not yet been confirmed by Ethereum Mainnet; users can only retrieve their assets after the challenging period ends, when the transaction data is confirmed and returned by Ethereum Mainnet.

Waiting periods for bridges on the current top four OP platforms are at least 7 days, which adds more anxiety to users in the extremely volatile world of cryptocurrency.

2.1.2 Low Interoperability between Rollups

Interoperability stands for the capability to integrate and share info between various computing systems, networks and applications, specifically aimed at the completion level of user operations across multiple Rollup Dapps. As ecosystems of various Rollups somewhat differ from one another, interoperability is a must. For instance, users on Rollup A desire to deploy on a Dapp on Rollup B. As it is a dynamic process for Rollup ecologic development, interoperability must also be a continuous development process.

Since it differs from how Ethereum stores user info and smart contracts via an integrated MPT

tree, Rollups organize accounts and activities by independent Merkle Trees. If another platform does not store user-related data on Dapp, then the service is not desirable. In order to achieve a high level of interoperability, the current best feasible solution would be a cross-chain solution that loads assets awaiting further action to a particular place, which is the desired Dapp deployed on a certain Rollup. This step often needs to be achieved by fast cross-link bridges, and official bridges are time-consuming and incompetent for this purpose.

Most Rollups are in need of bridging for native assets. Bridging for native assets cannot solely depend on simplistic lock and mint; there is a need to redeem intermediate assets to native assets. This creates a cage for the capital volume on targeted Rollup, leaving an inadequate scenario for handling bridging for a large amount of assets in a short time. Some employ the HTLC solution that users and routers exchange assets on different chains, bypassing the intermediate assets; nonetheless, the maximum bridging volume in a short time is also constrained by the capital volume on a targeted chain.

Besides, some bridging tools support very asset types, users must redeem assets that await bridging to bridging-friendly assets and restore them afterward. Not only is no value added, but more steps and transaction fees are incurred.

■ **Table 1.** Available Bridges for Direct Bridging between Rollups[2]

Bridges	Supported Chains	Supported Tokens	Smaller Pools TVL
Hop Exchange	5	5	1.6 M
xPollinate（Connext）	11	9	1 M
cBridge	11	8	1 M
Synapse	12	2	5 M

Source: Various bridging protocols, Huobi Research

[2] The amount of Supported Tokens is calculated from Arbitrum bridged to Optimism. As the capital volume is small, Smaller Pools TVL captures only the capital volume of ETH, USDP,USDC and DAI in the fund pool.

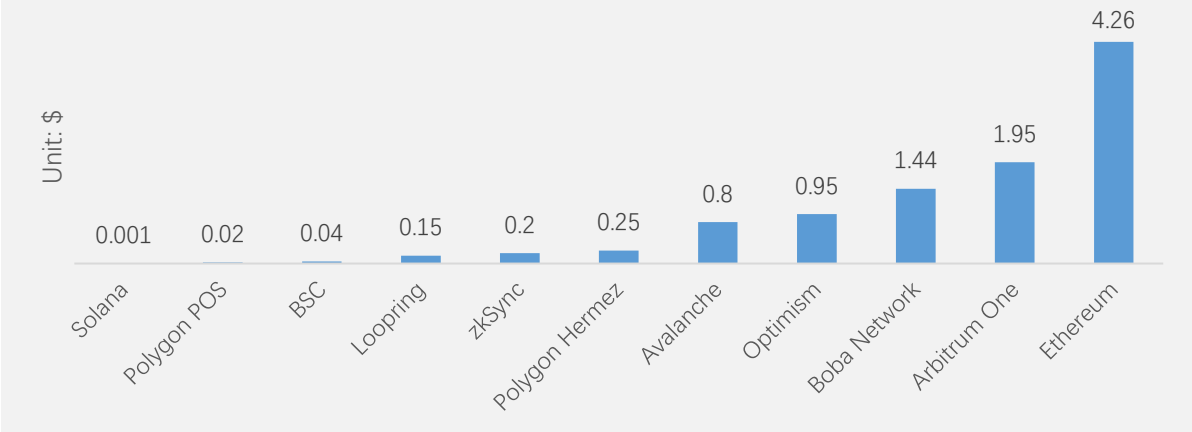
2.1.3 Lack of Fee Advantage

One of the primary purposes or Rollup concerns lowering Ethereum's gas fee. All scaling solutions must consider a lower fee structure for more traffic, otherwise the solution would be off the table. According to 12fees, ETH transfer, other crypto transfer, and crypto exchange for OP are higher than $1. Although this is still much lower than that of the Ethereum Mainnet, it is still not a negligible amount for users. What's more, if one includes the fees for the Layer 2 roundtrip, i.e., Arbitrum One Bridge, total fees add up to 0.01 ETH, approximately $25. At this time, users will choose to take the actions necessary to offset the cost incurred for Layer 2. Furthermore, additional actions in the process of recharge and cash-out activities may be a nightmare for those users who prefer a simpler process.

For the purpose of verification on Layer 1, OP must submit an assertion, containing intermediate states of transactions on Layer 2, and the intermediate states include the Merkle roots for Layer 2 status once after one or more transactions is completed. Data for these intermediate states occupies large storage on the block, producing a large pack of data for OP to upload, adding more costs for OP. Whereas ZK submits only ZKP (Zero Knowledge Proof), which is unlike large data pack as OP, providing proof based on cryptology for transactions executed on Layer 2. Less storage needed for ZKP is commensurate with a smaller data pack to be uploaded, and with this comes a lower fee structure.

Moreover, transaction fees for Rollup are disadvantageous to other Layer 1 chains. From a lower fee perspective, Rollup must possess more technological breakthroughs in order to be equal to or more competitive with other Layer 1 chains.

■ **Figure 5.** Transaction Fees to Transfer Native Tokens on Various Mainstream Rollups and Layer 1 Chains



Source: 12 fees, Various Blockchain Browsers, Compiled by Huobi Research

2.1.4 Complicated Deposit Process

Users must possess the same type of assets in order to utilize applications on Rollup. A configuration of RPC in the Rollup network is necessary to send assets from wallets on the Ethereum Mainnet to Rollup via bridging to top up a wallet on Layer 2. The smoothness of wallet operations, bridging, and additional ETH as gas fees may be a barrier to entry. Exchanges are the easiest option so far for most crypto users as they can easily recharge their wallets or cash out to various Layer 1 chains. However, a similar procedure for Rollups is still rare, and that is one of the possible causes why the Rollup market appears barren.

2.2 Low Capital Efficiency

2.2.1 Fragmented Liquidity Lowers Capital Efficiency

For most applications, scale of service depends on capital volume. For example, the fundamental application for DeFi, DEX, has less impact from the volatility of transactions if the fund pool is considerably large. Buyers and sellers can redeem more assets no matter in a larger scaled AMM or DEX order book, as the fund pool per se is capable of supporting large transaction volumes. Rollups and affiliated applications will further divide total liquidity by dispersing liquidity among

various Rollups, various applications on the same Rollup, or various divisions for the same application deployed on various Rollups. In other words, ceteris paribus, if the number of fund pools increases, the average fund pool volume decreases. Users will bear more burden from price volatility, and capital efficiency, on the whole, will suffer.

2.2.2 OP's Challenging Period Lowers Capital Efficiency

As forementioned, cash-out from OP requires a one-week long challenging period. No returns from the capital invested will be born from this period, so capital efficiency suffers. This waiting time could be mitigated by some fast bridging, but it is not pro bono: Transaction fees are proportional to the volume of assets for bridging, which appears to be more expensive for large-scale holders.

■ **Table 2.** Waiting Time and Fees for Mainstream Fast Bridges

Bridges	Time spent	Rates Fees	Additional
Boba Fast Bridge	20mins-3hours	0.1% - 3%	
Multichain	10-30 mins	0.1% rate with minimum fee limits ranging from 20-80$.	Minimum cross-chain amount of 80-200$.
Hop Protocol	10 mins	Approx. 0.1% rate,	
cBridge	5-20 mins	Approx. 0.4%	
Synapse	5-30 mins	0.04%	Bridge fees are charged according to different chains.

Source: Official bridges' documents, compiled by Huobi Research

2.3 Security Defects

As Layer 2 and Rollup are cutting-edge and newly emerged technologies, many are suspicious of its security capabilities, predominantly:

1. The smart contract for Rollup itself is flawed and assets may be vulnerable;

2. Any intentional misconduct or glitches of Rollup operators may initiate a freeze on assets;

3. An attack on the bridge or intentional misconduct may result in loss of assets in transit.

Point 1 appears to be the most critical security defect, however, there is little to worry about in reality. All Rollup teams have conducted thorough auditing procedures and trials on Testnet, which mitigates the risk of severe security incidents. Moreover, since data availability is granted by the Ethereum Mainnet, the state could be rebuilt from Ethereum in the case of severe incidents, thus achieving minimal loss due to a rollback from Ethereum. The latter two hidden risks may be more worrying for users.

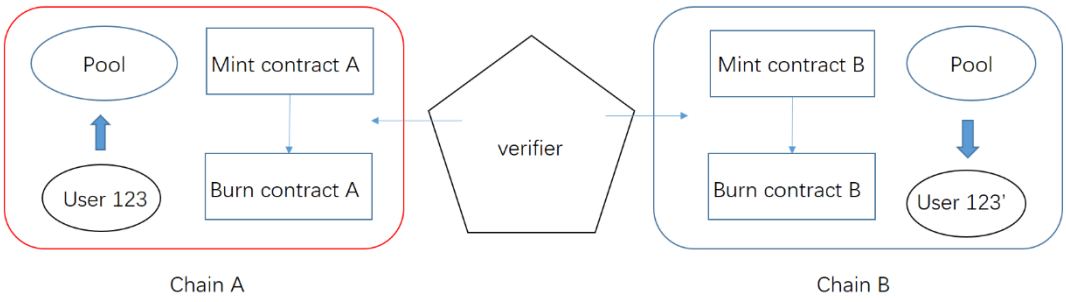
Both OP and ZK need the cooperation of Layer 2 operators in terms of compiling transactions, arranging transaction orders and piling afterward, and generating proofs. This process is usually done by the project team or authorized teams, which is usually centralized. The sequencer of the top four OP platforms is maintained by their official project teams. Arbitrum and Metis have proposed to decentralize the Sequencer, but have remained silent about the initial actual working efficiency or technological difficulties. A single Sequencer exacerbates the risk of a single point of failure, and although spare equipment can be set aside to handle unexpected situations, the unanticipated can always happen.

On Jan 9, 2022, a glitch occurred in Arbitrum's Sequencer. The main Sequencer encountered a glitch in hardware, and the backup node could not take full responsibility for the main Sequencer due to a software update. The whole Arbitrum Layer 2 network was paralyzed as no Sequencer could reinforce the network, causing a temporary freeze in several hours so no new transactions could be received, and cash-out activities were suspended. Despite the fact that no assets were damaged, incidents like this will harm user perception of such newly-emerged technologies.

Bridges can be categorized by different types of verifiers: centralized exchanges, singular/multiple external verifiers, native verifiers, local/liquidity network verifiers. Official Rollup bridges are native cross-chain, relying on the smart contracts on light nodes deployed on Ethereum and Rollups to ensure the verification can be completed for users' actions, such as lock, mint and burn. Even though native cross-chain possesses a higher level of security, the challenging period

cannot be bypassed, and this fails to cater to the need for fund flow. Main steps for external cross-chain verifications include: lock assets and redeem/mint intermediate assets from source chain, verify by external source and destroy intermediate assets from source chain, initiate smart contract and forge intermediate assets for targeted chain, and redeem intermediate assets to native assets. This set of procedures involves 2 fund pools, 4 mints/burns of smart contracts, and 1 external verifier; security breaches resulting in token theft or unlimited token supply could emerge anytime in every single step. Anyswap (Currently known as Multichain) once fell victim to a severe security exploit that saw hackers take advantage of two transactions with the same account signature to deduce the private key of the external verifier, resulting in severe token loss. In this case, due to the glitch, the same random variable is repeated twice, generating partially same output from the signature. Whereas liquidity network verifiers appear to be safer, utilizing the forementioned HTLC method without any centralized fund pool or forged/burnt smart contract, or any external verifiers present. Regarding CEX cross-chain, namely recharging and cash-out on Layer 2, the transfer could be completed on a targeted chain or Rollup safely so long as the internal calculation is appropriate for exchanges; it depends solely on the overall security settings of the exchanges.

■ **Figure 6.** Workflow of the Externally Verified Bridge



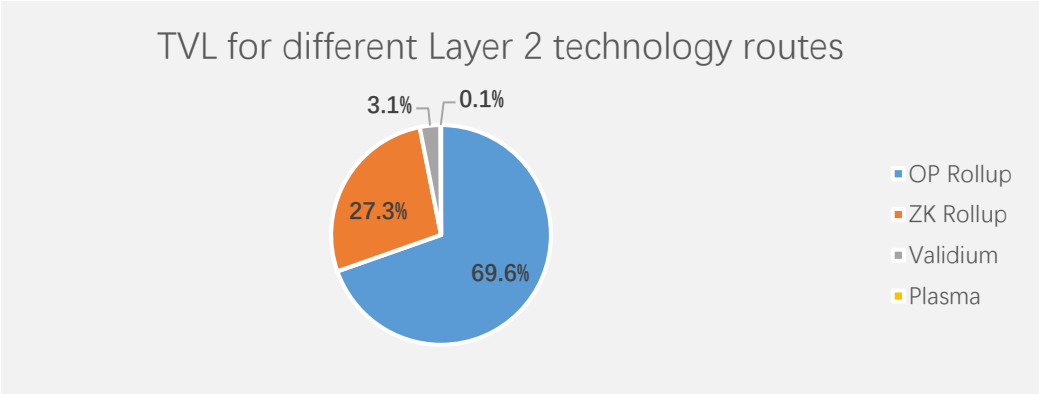
Source: Huobi Research

2.4 ZK Rollup is not EVM-compatible, and Monotonous

Current mainstream ZK Rollups are not completely compatible with EVM so very limited operations can be performed, which appears to be monotonous and less appealing for average users. Only users in certain fields, namely payment processing and transaction processing, may be

attracted. According to 12beat, TVL of ZK accounts for less than 30% of the overall Layer 2 TVL.

■ **Figure 7.** TVL for Different Layer 2 Technology Routes



Source: 12beat, Huobi Research

More specifically, the proof of efficiency ZK Rollup submits to Ethereum Mainnet is a zero-knowledge proof, and the zero-knowledge proof is comparatively difficult to produce —The process may contain a conversion of program logic to mathematical calculation circuit, plus, the program logic may consist of not only simple calculations but also logical judgements like “and”，“or”,“not”,etc., and far more complicated operations such as bit operation, HASH computation and other actions on smart contracts. However, this circuit only contains addition gate and multiplication gate, and Ethereum did not take the compatibility issue of zero-knowledge proof into consideration upon initial design – the opcode of Ethereum is zero-knowledge-proof-unfriendly. Besides, the frequently used HASH computation, such as AES-128 and SHA-256, are full of bit operations. These actions would be enormous and sophisticated when converting to “gate constraints” in the circuit.

Last but not least, the lack of EVM leads to the rarity of projects in ZK. For a project to kick off, besides its own business principle, foundations have to be built from the very bottom, including assembling account mechanism and state tree, designing ZKP circuit, completing status switch and generating ZKP, etc., all of which create an invisible threshold for new projects. The only two desirable platforms are StarkEX and zkSync. For the convenience of proof generation, StarkWare and Matter Labs has developed new programming languages, Cairo and Zinc; existing solidity program cannot be migrated directly to ZK, which elevates the level of difficulty for migration and prolongs the learning curve of developers. As a result, there are merely four projects deployed on

StarkEX, and Dapps on zkSync have never stepped out of the Testnet.

3 Forward-looking on Rollup

Even though the shortcoming of Rollup somehow impedes mass adoption, the solutions to this are not impossible to implement.

3.1 Improve the User Experience

3.1.1 Minimize the Impact of OP Cash-out Period

The waiting period of OP has been deeply established in its design, and foundations are hard to shake. Nonetheless, this issue could be resolved from head to toe when third-party cross-chain bridges are adopted on a mass scale. Fast cash-out can improve capital efficiency and kill two birds with one stone. Current mainstream third-party cross-chain bridges can complete the process in less than 30 minutes; the core limitation resides in the unfeasibility for large-scaled funds to cross, which is not a thorny issue where OP cash-out is concerned. Fast cash-out requires funds on Ethereum Mainnet to be sufficient for exchange, which is not a problem since Ethereum has larger capital volume than OP Rollup by far.

On the other hand, demand for OP cash-out may become weak. From a user standpoint, the original intention for cashing out reflects a low level of satisfaction, that the current platform cannot fulfill their needs, i.e., they may wish to use some functions that are not available here but deployed on the Ethereum Mainnet or other chains, participate in incentive plans provided by new projects on other platforms, invest in other assets not on this platform, or exchange some of their crypto to fiat.

As cross-chain bridges are compatible with more diversified assets, these demands above could be satisfied by a simple interaction of L2-L1 or L2-L2, which makes the seven day waiting time redundant. Next, the usage cost must be upfront. To fulfill the demand for exchanging fiat is an

absolute advantage of centralized exchanges. OP needs to interact with CEX more, enabling recharging and cash-out via exchanges, therefore users who need fiat could recharge to an exchange address and do whatever they desire upon receipt of their assets. For instance, the cash-out time from Arbitrum to Huobi is 5 minutes without any other additional fees except for the Layer 2 gas fee. By doing this, users could bypass the complicated route of needing to make the first stop at Ethereum in order to exchange fiat. It is such a smooth experience that users will be unable to distinguish fund flows behind the scenes. Exchanges could utilize the advantages of the large user base and the large capital volume to bootstrap transactions and reduce the marginal cost for each user acquisition.

Moreover, cross-chain bridges could cement the interoperability between Rollups. The greater the capital volume flows on Rollup, the broader the bridges between Rollups are, and the smoother the transaction is for assets to cross-chain. Cross-chain aggregators have huge potential: they could accelerate the fund flow of large-scale capital by rational route design according to the capital volume, status quos of various fund pools, and gas fee on targeted chain, etc..

3.1.2 Further Reduce OP Cost

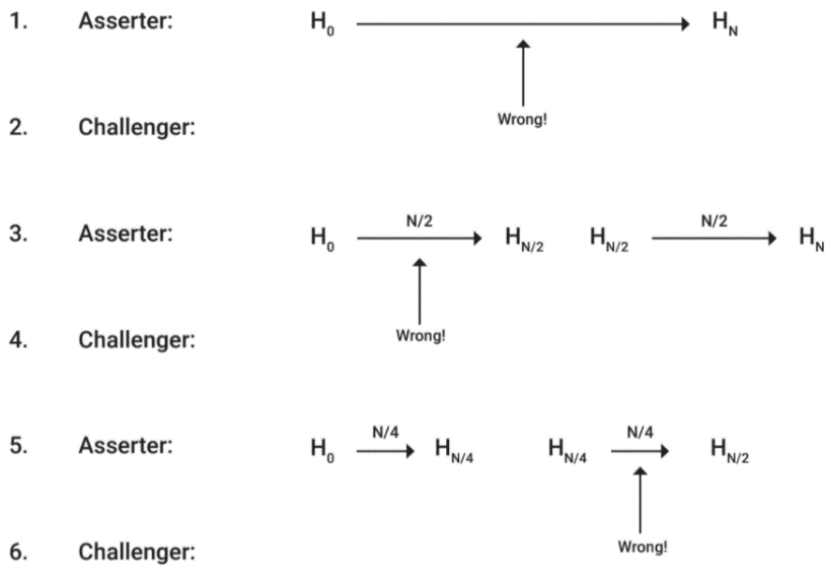
The high fee structure of Rollup, especially OP, can be resolved. Cost structure of Rollup constitutes two parts: on-chain and off-chain. The on-chain part deals with the uploads and proofs, which consumes Ethereum gas, whereas the off-chain part handles the process of compiling, computing, status switching and generating proofs, which also consumes resources such as computation and storage, namely gas.

Three solutions are desirable for OP to further reduce the gas fee:

Firstly, reduce the total on-chain gas consumption. By altered compiling and bulk processing, storage usage for transaction data can be minimized. The Ethereum community has also committed to reducing the costs for Rollup, for instance, the EIP-4488 Proposal suggests that the gas consumption for CALLDATA (the location where the compiled data of Rollup is stored in EVM) could be reduced from 16 to 3 per byte. Gas fee could be reduced as much as 80% in a short time if the EIP-4488 Proposal is approved and effective.

Secondly, another desirable path to reduce cost is to decrease the size of the proof. By altering the pattern of how intermediate data is organized or aggregation proof in fraud proof is arrived at, or applying more advanced cryptographic methods, gas fees for uploading proofs could be substantially lowered, or gas fee per each user is shaved. Normal assertions submitted to Ethereum Layer 1 by OP must contain every statement for off-chain transaction, namely the updating state roots with transaction executions, which are responsible for the consumption of gas. However, the interacted proof of Arbitrum deems the transactions as two halves, so assertions submitted only contain statements regarding the two halves; therefore, Layer 1 resources are saved by reducing the volume of data to be uploaded. Verifiers can only challenge one half at a time, and operators divide the challenged half into another two halves repeatedly until it reaches the finale - verification on the Ethereum Mainnet. The process of halving, which relieves divergence, takes place off-chain, so it is immune to Ethereum gas fees. Besides, the SHARP technology of StartEX aggregates zero-knowledge proofs generated in a certain time period into a whole: the size of the proofs adds up to a commensurate size, which would not be predominantly larger, yet the amount is now 1 instead of many, which reduces gas consumption.

■ **Figure 8.** Solution to Arbitrum Divergence



Source: Aribitrum

Lastly, reduction in off-chain cost cannot be neglected. OP has realized full compatibility with EVM, and it aims at reducing the cost by increasing the efficiency of VM. For example, VM of Arbitrum will be upgraded to WASM, which stands for a new standard command set, being the

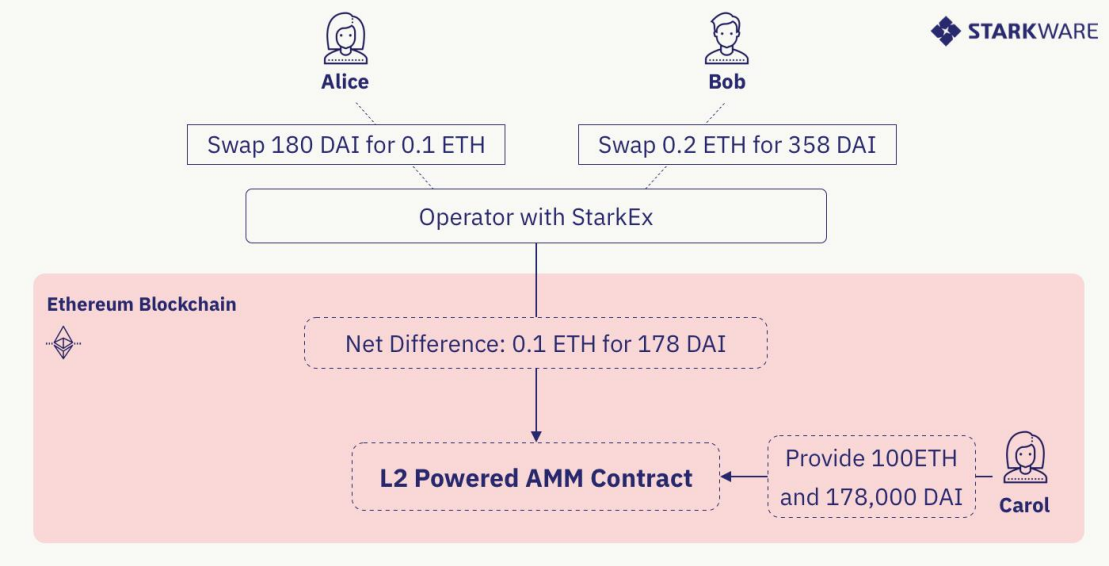
target for coding and supporting various coding languages to a unified standard format. As the WASM coding is more approximate to actual hardware commands, commands could be reflected and transmitted to the machine precisely, ensuring a more efficient process in translating actual logic of commands. Therefore, WASM has a comparatively higher efficiency and a theoretically lower execution expenditure compared to AVM, and fee reduction could thus be achieved. Major consumption of ZK off-chain resides in generating proofs; costs for generating proofs can only by lowered by continuous updating on cryptographic algorism and hardware. Meanwhile, the withdrawal period of ZK is further shortened as a complementary benefit.

3.2 Elevate Capital Efficiency

To elevate capital efficiency is to resolve the issue of fragmentation in liquidity, which is feasible.

One possible solution is to concentrate the dispersed liquidity. StarkWare and Loopring proposed the idea of dAMM: to establish a mock exchange on Layer 2, where users could trade. It simulates and matches trade requests and brings the net transaction to be closed in real exchange on Layer 1 only afterwards. Real exchanges on Layer 1 only interact with the mock exchange, which can be seen as the bank and the vault. Basic trade requests could be fulfilled partially, which could be deemed as a transfer between users. Thanks to the larger fund pool, the net trade is less volatile in price, thus elevating overall efficiency.

■ **Figure 9.** Working Principles of dAMM



Source: StarkWare

To further promote this idea, the amount of assets being calculated could be separated from the real ones so long as security and ownership can be guaranteed. Similar to what happens in bill sharing, aggregated liquidity (whether on Layer 1 or Layer 2) can achieve higher efficiency.

3.3 Improve Security

Even if, as discussed earlier in the article, Rollup operators misconduct themselves, nothing can be stolen from users, although an intentional freeze of assets could occur as a result. In order to improve the security, focus should be placed around reducing the possibility that users' assets could be viciously frozen, and preparations made for more precautionary solutions to be put in place.

3.3.1 Reduce the Level of Centralization

Reducing the level of centralization in Rollup is a mandatory and feasible solution to avoid singular glitch. Various projects, including Arbitrum, Optimism, Metis, and StarkEX, etc., have proposed a working target on decentralization in their roadmaps or white papers. Sieged by all kinds of Layer 1 chains, Rollup has no excuse to not approach decentralization.

Two major questions should be answered prior to planning the decentralization of Rollup: how to incentivize Layer 2 operators and how to decide which entity should be responsible for organizing, compiling and submitting data on-chain for the bulked transactions. Tokenomics can be modified such that operators can receive part of the gas fee as gratitude, assuming that it adds no additional burden to users. Meanwhile, operators could choose to operate fewer nodes so a more flexible consensus could be achieved in terms of efficiency instead of an exorbitant level of decentralization. With the help of economical methods, such as mortgage, singular glitches can be avoided.

3.3.2 Set Forced Cash-out Mechanism

Once there a glitch appears, Rollup must ensure that precautionary solutions are in place so users can extract assets safe and sound. This forced mechanism must be deployed on the Ethereum Mainnet as Rollup will malfunction when the time comes. The uploaded data compilation is of utmost significance to provide references for Ethereum to fully collaborate with the cash-out activities (refer to their activities illustrated in the references).

Forced Operations designed by StartEX shed some light. First, forced cash-out request is received on Layer 1 from users, StarkEX initiates a judging process according to the business logic of Dapp: if the request overlaps with the business logic, for instance, when the user does not meet the forced liquidation margin, which deems it a valid account, the account status will be updated on Layer 2 by StartEX and the cash-out request for users is thus fulfilled, or declined otherwise. This action prevents irregular freeing for users triggered by intentional misconduct of Dapp and glitches. StarkEX will post a ZKP and record the activity in the mainnet no matter whether the cash-out is successful or not. If nothing happens after a certain time period, users could take further forced actions: Merkel roots and paths on StarkEX must be submitted to the Ethereum Mainnet so that the account status on Layer 2 can be found. After verification, StarkEX will establish a Vault on Layer 1 and duplicate the account status on Layer 2, forced cash-out is then completed when assets are retrieved.

Decentralized nodes and forced cash-out mechanism could become the default settings of Rollup in the future, making it commensurate with Ethereum security level-wise.

3.4 R&D in zkEVM

As mentioned earlier, the main conflict for projects in ZK series is the R&D behind ZKEVM. With ZKEVM, coverage of applications will be much broader as ZK is capable of more complex calculations and logics. Moreover, a low fee structure could attract more traffic and expedite the on-chain process for transactions (current Rollups accumulate to a certain amount of transactions and only then submits them in bulk), diluting the costs for uploading ZKP and lowering the cost further. As a result, developed ZKEVM will enhance the overall construction of Ethereum, with the focus on ZK Rollup, at large.

To sum up, there are two tech stacks for ZKEVM: EVM-friendly and ZKP-friendly. EVM-friendly path originates from current EVM, adding ZKP and supporting native EVM opcode. Codes are executed in EVM, which is completely compatible with solidity command set. ZKP-friendly path constructs EVM based on ZKP-friendly opcodes. A new VM will be designed so commands in there stand a higher chance in generating ZKP, at the same time, some ZKP-unfriendly codes will be altered.

Since last year, Matter Labs, Hermez and other teams have been active in developing ZKEVM. Matter Labs chose the latter path. The Ethereum Foundation too, assembled a team working on the integration of EVM opcodes to ZK circuit according to the former path, so that original smart contracts can be deployed on Layer 2 with the least effort. In October 2021, Matter Labs first introduced the beta version for zkSync 2.0, UniSync, which runs Uniswap V2 in zkEVM test environment. On Feb 22 this year, public testnet for zkSync 2.0 was launched. The protocol supports Solidity 0.8.x and Ethereum cryptographic primitives, announcing that deployment and execution of current codes could be completed without mass modifications. Web 3 API is also supported so that developers could integrate current index and browsers with no additional steps needed. Hardhat plugins are supported for the convenience of test and development of smart contracts. Testnet now only supports cash-out and transfers; more functions will be available in the future.

Furthermore, StarkNet by StartWare team has launched mainnet, supporting any business logics (by Cairo), but is incompatible with EVM. ZK Rollup that executes universal solidity smart

contract will eventually emerge as the translation tool from Solidity to Cairo, Warp, is being developed by the Nethermind team day and night. With reference to the earlier roadmap, it is very likely we could experience the product in either Q1 or Q2.

Unexpected issues are more than likely to occur during the development and testing process of zkEVM. Fully functional zkEVM still needs compatibility with other EVM-friendly tools; expectations should be lowered as rush jobs can never produce something ironclad. The only thing we should do now is to sit tight and look forward to the emergence of a a brighter future for Rollup and the blockchain.

References

[1] https://hackernoon.com/fraud-proofs-secure-on-chain-scalability-f96779574df

[2] https://blog.matter-labs.io/worlds-first-practical-hardware-for-zero-knowledge-proofs-acceleration-72bf974f8d6e

[3] https://eips.ethereum.org/EIPS/eip-4488

[4] https://medium.com/huobi-research/layer-2-bridges-the-present-and-the-future-2da5aeb1e942

[5] https://medium.com/starkware/caspian-an-l2-powered-amm-f20e93b5421

[6] https://matterlabs.medium.com/zksync-2-0-public-testnet-is-live-de870ba9632a

[7] https://matterlabs.medium.com/unisync-a-port-of-uniswap-v2-on-the-zkevm-b12954748504