Layer 2: Scaling Ethereum for Mass Adoption

I. Executive Summary

1. **"So, what is Layer- 2?"** Layer 2 (L2) is a collective term for solutions designed to increase the throughput and lower the per transaction cost of Layer 1 (L1), in this case, Ethereum, by handling transactions off-chain while taking advantage of the underlying L1's security model.
    - We are bullish on rollups, which group and compress transactions in a batch into a "rollup" that is stored on Ethereum. There are two types of rollups, depending on the verification method.
    - In Optimistic Rollups (OR), transaction verification is only performed if a node suspects that a transaction is fraudulent, thus further increasing transaction speed and throughput. Arbitrum and Optimism are the two most popular general-purpose OR solutions.
    - In ZK-Rollups (ZKR), proof of the execution is generated for every bundle such that transactions can be verified later in 10-30 min. StarkEx and Loopring are application-specific ZKR, while StarkNet, zkSync 2.0, Scroll, and Polygon are developing general-purpose ZKR.
    - Validium is similar to ZKR, except it stores transaction data on L2 instead of L1, thereby increasing the throughput by roughly 5x at the expense of lower security. Immutable X is a Validium solution designed for games, featuring zero gas fees for NFT minting.
2. **"Cool tech, but how big is the opportunity?"** The market size of L2 cannot be easily quantified as new use cases are still being developed. That said, we know that the potential is huge. Global payments alone present ample room for growth for L2; it presents US$105B/month revenue opportunities for Ethereum, whose revenue is just US$86M/month. Ethereum's transaction fees are too high for it to compete with Visa/Mastercard, but L2 has been able to reduce transaction fees by 75%-97%. Initiatives such as proto-danksharding will lower all rollup fees further by ~100x. Global payments is just one segment poised to get disrupted. Ethereum is a universal computer, and now L2 makes it possible to build dApps that had not been possible directly on Ethereum, e.g. games.
3. **"That's huge. Which L2 should I keep an eye on?"** By comparing project adoption, we see that simplicity, generality, and EVM compatibility are important in attracting adoption. Arbitrum and Optimism are ORs that are general purpose and EVM compatible, and they own 80% of the market. StarkNet and zkSync 2.0 are generalized ZKRs that have superior tech but are harder to use and not fully compatible with EVM, jeopardizing their adoption. Polygon and Scroll are developing generalized ZKRs that are fully EVM-compatible so existing projects can migrate to L2 as-is. Arbitrum, StarkNet and zkSync are slated to offer tokens soon—you can get free tokens using their network and dApps.
4. **"Is it too late to get in?"** TVL on L2 has grown 10x in the last 12 months, but plenty of growth is left, as this TVL is just ~13% of that on Ethereum. The growth will be fuelled by further adoption of rollups. With proven tech and EVM compatibility, OR owns 84% of TVL in L2. ZKR has superior tech and we think it can take over the market dominance when it has true EVM compatibility. Validium would be relevant for specific use cases that require higher throughput and extremely low fees but lower security.
5. **"Also, does this mean competing chains are dead?"** With L2, the justification of monolithic L1s like Solana is diminished. We think Ethereum would become the platform of choice to build dApps for most people. That said, we believe that the market is big enough for a second player, but it remains to be seen which L1s will rise to be the contender.
6. **"What would happen to the price of ETH?"** L2s have a near-term adverse effect on the demand for gas as existing projects migrate to L2 to save gas fees, exerting downward pressure on the price of ETH. In the mid- to long-term, we are bullish on ETH as new use-cases for Blockchain are developed and Ethereum as the platform of choice will experience significant growth in transaction volume.

Kuriakin Zeng, Blockchain Research Analyst kz@gsgasset.com
Ray Shu, Head of Research ray@gsgasset.com https://twitter.com/GSGResearch

II. Table of Contents

Kuriakin Zeng, Blockchain Research Analyst kz@gsgasset.com
Ray Shu, Head of Research ray@gsgasset.com https://twitter.com/GSGResearch

III. L2 Scaling Solution Basics

Background

To understand how L2 scaling solutions work, we start with why they exist.

Suppose Dan and Kev live in a universe where everyone transacts on Ethereum. They are roommates who share expenses, so they have to pay one another throughout the month.

As it stands, each transaction between Dan and Kev is recorded separately on Ethereum. Ethereum is decentralized and secure, but it currently can only handle 15 transactions per second (tps) and each transaction costs ETH 0.0012 (~$2).

But why can't Ethereum handle more transactions and at lower fees? Essentially gas fee is determined by supply and demand, where "supply" is the space available for transactions. The supply is limited by the amount of work that the nodes need to perform at one given time. Secure and decentralized blockchain networks require every node to verify every transaction processed by the chain.

This leaves us with the option to increase the size and power of Ethereum's nodes so that they could process more nodes. However, in doing so, the hardware requirement would restrict who could run a node – this threatens decentralization.

This is the scalability trilemma: a blockchain can only pick two out of decentralization, security, and scalability.

What if the Ethereum mainnet can "outsource" most of its transaction processing? By having a separate chain that processes the transactions for Ethereum, it can focus on being decentralized and secure, and rely on the other chain on improving scalability.

That's where scaling solutions come about. We could break Ethereum into smaller chains (Sharding), or create an entirely new processor (a chain or a channel) that either inherits Ethereum's security (L2) or relies on its own security (Sidechain).

	On-chain	Off-chain
Rely on Ethereum's security	**Sharding**	**Layer 2**
Rely on its own security		**Sidechains**

There are many ways that an L2 can offload transactions from Ethereum but still inherit the security of the Ethereum network: State Channels, Plasma, Optimistic Rollups (OR), ZK-Rollups (ZKR), and Validium.

Different Solutions

If we allow Dan and Kev to open a tab where they record their payments and at the end of the month, they close the tab and record the net payment on Ethereum. The tab between Dan and Kev is a **State Channel**.

Kuriakin Zeng, Blockchain Research Analyst kz@gsgasset.com
Ray Shu, Head of Research ray@gsgasset.com https://twitter.com/GSGResearch

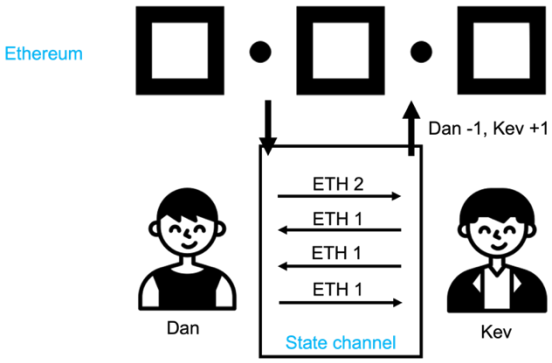


Exhibit 1 State Channel

Great! We managed to capture all transactions between Dan and Kev in one, and this method can handle 25 million tps[i]. However, this method requires Dan and Kev to open a tab between them every time they want to pay one another. Similarly, even when Dan wants to make a one-time payment to a third person, say Nick, he needs to open a tab between him and Nick.

Ethereum needed a better way to scale; one that does not require a setup every time one performs transactions.

A smaller blockchain, **Sidechain**, comes along and offers to process transactions for Ethereum. At a fixed interval, Sidechain will process all transactions from the account holders, and Ethereum just needs to record the resulting account balances. An example of Sidechains is xDai. As you can see, this solution requires the users to trust that Sidechain is secure—what if it's compromised?

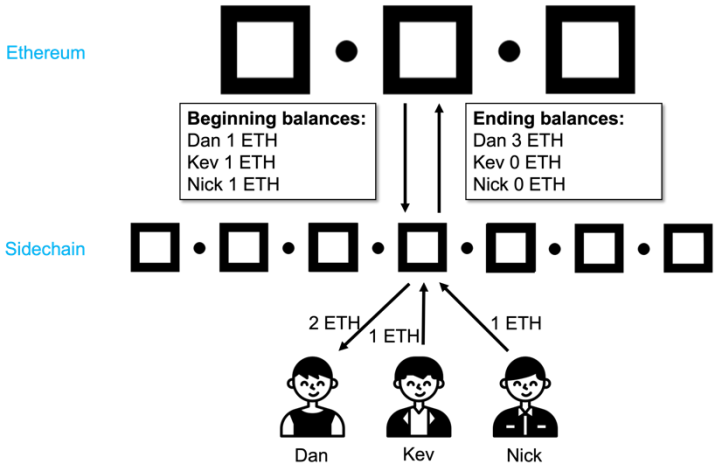


Exhibit 2 Sidechain

Wouldn't it be great if the Sidechain can inherit Ethereum's security? Enter Plasma.

Plasma is an L2 that allows a 7-day period for its users to challenge the resulting account balances and provides a piece of code (i.e. fraud proof) that anyone can use to replay the transactions to see if it arrives at the same resulting account balances. Plasma can process as many as 65,000 tps[ii].

Kuriakin Zeng, Blockchain Research Analyst kz@gsgasset.com
Ray Shu, Head of Research ray@gsgasset.com https://twitter.com/GSGResearch

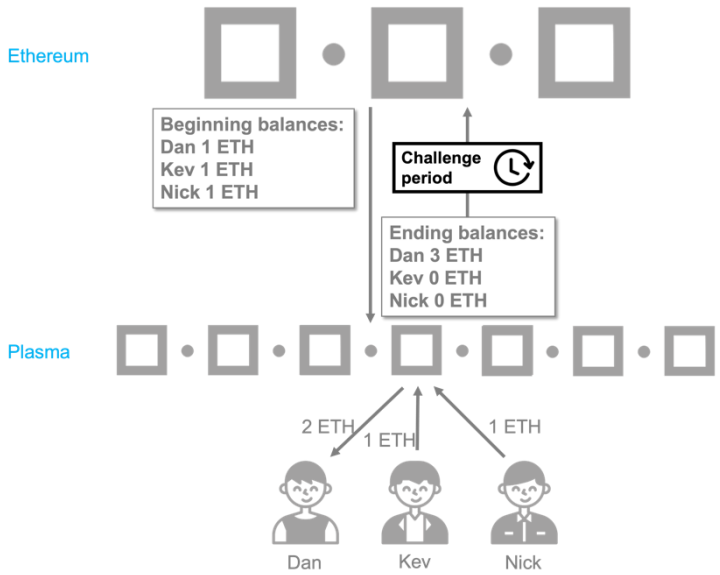


Exhibit 3 Plasma

Plasma is not the panacea though, because it makes account holders wait for at least 7 days before they can withdraw their money. In addition, Plasma had encountered issues, such as dropping transaction records. As a result, users prefer that their transactions are directly recorded in Ethereum because it has been reliable and secure.

In response, **Optimistic Rollups (OR)** were developed. OR processes multiple transactions and submits only the essential data to Ethereum. This allows OR to inherit the security of Ethereum while still handling 5,000 tps. To make things simple, OR continues to use the same proof system as Plasma; it assumes that all transactions are valid until someone proves it otherwise during the 7-day challenge period. While a step-up from Plasma, it still suffers from the same withdrawal issues; users need to wait for the challenge period to end before they can withdraw their money.

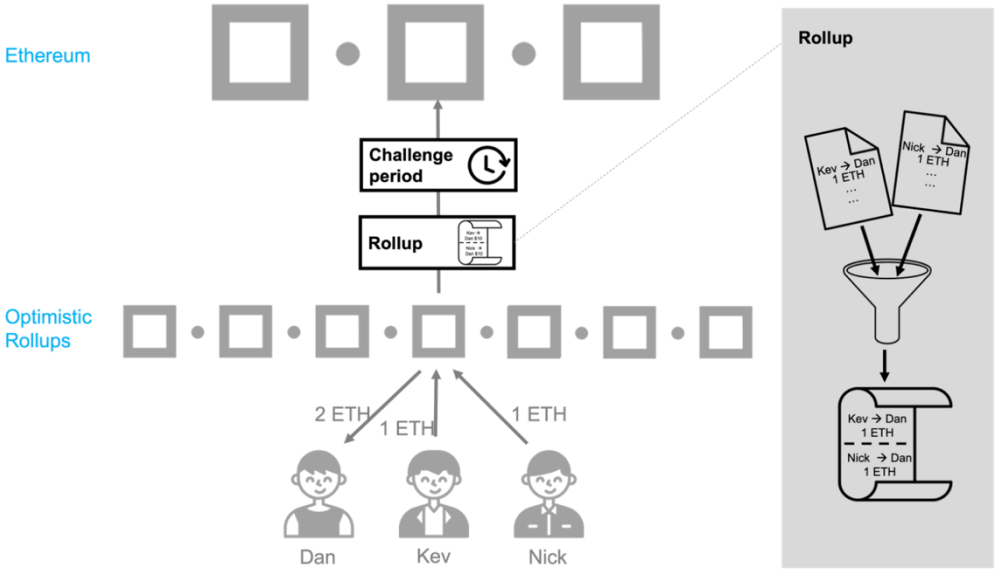


Exhibit 4 Optimistic Rollups

Kuriakin Zeng, Blockchain Research Analyst kz@gsgasset.com
Ray Shu, Head of Research ray@gsgasset.com

To circumvent the 7-day waiting period, users can use a Liquidity Provider (LP). Suppose Dan wants to withdraw his 2 ETH but doesn't want to wait for 7 days. He could pay LP a fee to take over the ownership of his 2 ETH on L2 and send him 2 ETH on L1 upfront. This Fast Withdrawal has worked well as OR is the most popular L2 in terms of TVL at the moment.

Fast Withdrawal does not work, nevertheless, on non-fungible assets like NFTs. Suppose Dan has bought an IreneDAO Pass #84 on OR-based L2, it would not be possible for him to perform a Fast Withdrawal because the LP does not own IreneDAO Pass #84 to send to Dan on L1. OR is the king of the hill for dApps that don't involve non-fungible assets.

But what if Dan and Kev now want to trade NFTs on top of paying one another without waiting for 7 days to withdraw? We could replace the fraud-proof system with a new, advanced proof system called **validity proof** that leverages zero-knowledge proof (ZKP). Validity proof proves beforehand that each batch of transactions is correct. There are three solutions that implement ZKP: ZKR, Validium, or a combination of both called Volition.

As its name suggests, **ZK-Rollups (ZKR)** bundle transactions into one like OR, except they use validity proof. With ZKP, the validity of each transaction can be quickly verified, users can withdraw their funds within 10-30 minutes. In addition, while OR post all transactions to Ethereum, ZKR submits only the changes required to represent all the transactions, resulting in smaller footprints on L1.

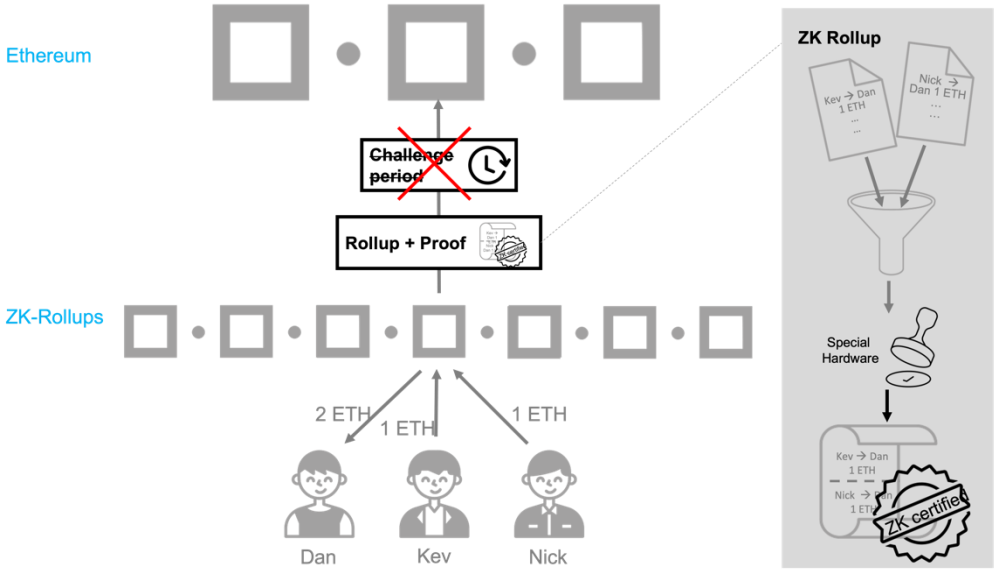


Exhibit 5 ZK-Rollup

ZKR is superior to OR but it is still in development and testing. Unlike OR which is EVM-compatible and can support all types of dApps, ZKR is a primitive piece of technology whose EVM compatibility is still in development and testing. ZKR-based L2s in production right now are developed for specific purposes such as exchanges, trading, payments, and NFTs. This will change soon with zkSync 2.0 planning to launch EVM-compatible ZKR to mainnet in Q4 2022.

ZKR uses validity proof and still stores data on Ethereum, making them the most secure and trustless solution of all L2. It still can achieve a throughput of 2,000 tps and a gas fee that's low enough for it to be the best choice for most dApps, especially DeFi applications.

But suppose now Dan and Kev want to port their favorite game "Animal Crossing" to Ethereum. The game will need to mint billions of NFTs a year. Even if minting an NFT on ZKR costs $0.10, the cost quickly becomes

unsustainable for them. If we can sacrifice some security, Dan and Kev could use **Validium**. It's another rollup solution that uses validity proof so it doesn't require the user to wait for 7 days for withdrawal. Validiums achieve higher throughput than ZKR (9,000 tps) by keeping all transaction data off-chain and only post state commitments (and validity proofs) to the main Ethereum chain. This comes at the cost of the susceptibility to crypto-economic attacks that should Validium's operators want or be forced to freeze users' assets, they could do so by refusing to provide the data to users. However, this shortcoming is being actively mitigated by projects that offer the Data Availability layer such as Polygon Avail.

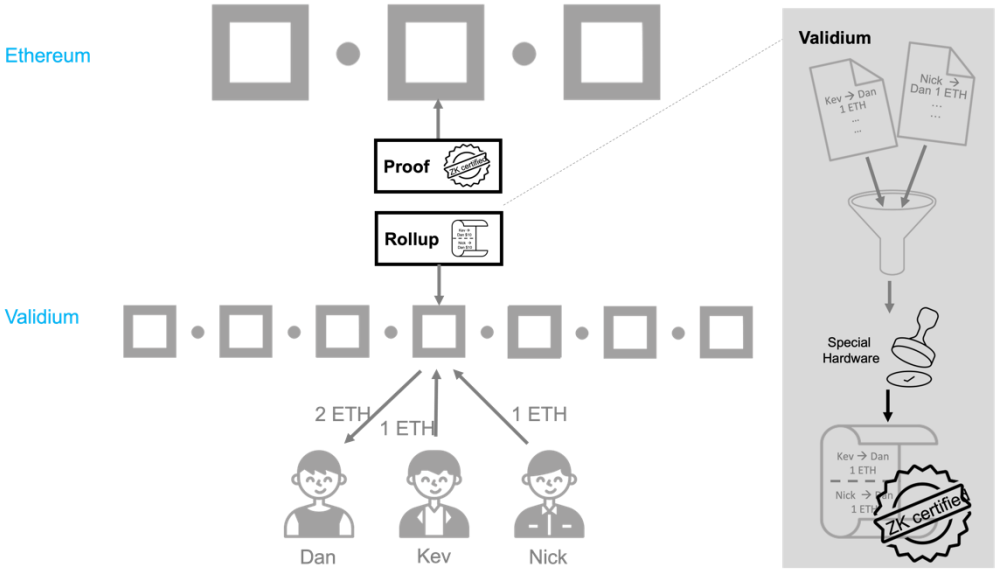


Exhibit 6 Validium

Finally, **Volitions** combine ZKR and Validium chains and allow users to choose whether to store their transaction data on L1 or L2, respectively.

Summary

The table below offers a summary of the main technological differences in the main four L2 solutions:

	Fraud proof	Validity proof
On-chain data	**Optimistic Rollups**	**ZK-Rollups**
Off-chain data	**Plasma**	**Validium**

It's clear from the presentation above that Rollups and Validium are better than State Channels and Plasma. The best L2 solutions to choose between OR, ZKR and Validium depend on what we are optimizing for. We compare the five solutions in detail in **Exhibit 7** in terms of performance, security, and/or usability.

The exhibit shows that State Channels and Plasma have more drawbacks than the others. We believe what mainly prevented them from ever gaining significant traction was the work imposed on the end users.

On the other hand, ZKR seems to be the best Layer-2 solution that has no major downside. However, the ZKP technology is primitive and not battle-tested yet. Further, producing validity proofs requires specialized hardware, which may encourage centralized control of the chain by a few parties.

Even if we assume that the cryptographic technology works seamlessly, there are use cases where other solutions could be more suitable. While DeFi with billions of dollars at stake may benefit from ZKR's security,

Kuriakin Zeng, Blockchain Research Analyst kz@gsgasset.com
Ray Shu, Head of Research ray@gsgasset.com https://twitter.com/GSGResearch

Blockchain-based games may be willing to trade off transaction speed and costs against slightly lower security and choose Validium.
Except for dApps involving non-fungible assets, it remains to be seen if users will choose ZKR over OR for the immunity to crypto-economic attacks when such risk at OR is not that high.

	State channels	Plasma	Optimistic Rollups	ZK-Rollups	Validium
Scaling approach	Move computation off-chain	Move computation & data storage off-chain	Rollup txn as an argument to the smart contract	Rollup txn as an argument to the smart contract	Move computation & data off-chain
Tech complexity	Low	Medium	Medium	High	High
Main Technology	Smart contract	Smart contract, Merkle Tree	Smart contract, Merkle Tree	Smart contract, Merkle Tree, ZKP	Smart contract, Merkle Tree, ZKP
Performance					
Throughput	25,000,000 tps	65,000 tps	5,000 tps	2,000 tps	9,000 tps
Transaction cost[iii]	Very low	Low	Low; $0.02 (Arbitrum One)	Low; $0.25 (ZKSync)	Very Low
Security					
Centralization risk	Standard	Standard	Standard	Higher as special hardware required	Higher as special hardware required
Mass exit problem	No	Yes	No	No	No
Liveness requirement	At least 1 user must stay online to keep the channel alive	At least 1 plasma operator must stay online	No	No	No
Vulnerability to crypto-economic attacks (e.g. compromise L2 validators)	Moderate	Moderate	Moderate	Immune	High. A quorum of validators can freeze and confiscate funds
Maturity of cryptographic technique	Standard	Standard	Standard	New	New
Usability					
Work imposed on the end user	Users need to keep records between themselves and counterparties	Users need to monitor txn to detect malicious behavior by the operator	No	No	No
Transaction between arbitrary users	No. Users need to initiate a channel with counterparties	Yes	Yes	Yes	Yes
Finality (Withdrawal time)	1 confirmation	1 week	1 week	10-30 min	10-30 min
Support for general-purpose computation	No. Only basic token transfer and swaps	No. Only basic token transfer and swaps	Yes	Yes	Limited support
EVM-compatibility	No	No	Yes	Yes	No. Require specialized language
Other					
Privacy	No	No	No	No	Yes

Exhibit 7: Comparison of L2 in Performance, Security & Usability

Legend:
Good

Kuriakin Zeng, Blockchain Research Analyst kz@gsgasset.com
Ray Shu, Head of Research ray@gsgasset.com https://twitter.com/GSGResearch

Acceptable
Bad

IV. Market Opportunity of L2

The world has increasingly been digitalized. There are 5.2B smartphone users, 2.1B online shoppers, and 2.0B online banking users, and yet there are only 11-15m monthly active Blockchain users. We know the long-term market opportunity for blockchains is huge, and believe that Ethereum with L2 will command a significant share: L2 makes it possible for dApps that had previously not been feasible to be built on Ethereum. The hard part is quantifying the potential size, particularly since new use cases are still being developed—so we focus on the market opportunity for just one industry that L2 is poised to disrupt: global payments.

According to the latest McKinsey report (October 2021), global payment **revenues** totalled US$1.875 trillion in 2020, representing 37% of banking revenues. Excluding account-related transactions such as interest income ($619bn), the transactional payment market stands at US$1.26 trillion a year and is projected to grow 7%+ annually. This is **US$105B per month** of **revenues** from processing transactions like credit cards, wire transfers, and international remittances, compared to Ethereum's 30D revenue of **US$86M paid in gas fees**. We see ample room for growth in terms of the adoption of blockchain technology by both financial institutions and consumers, with the possibility of completely disintermediating banks and their fees.

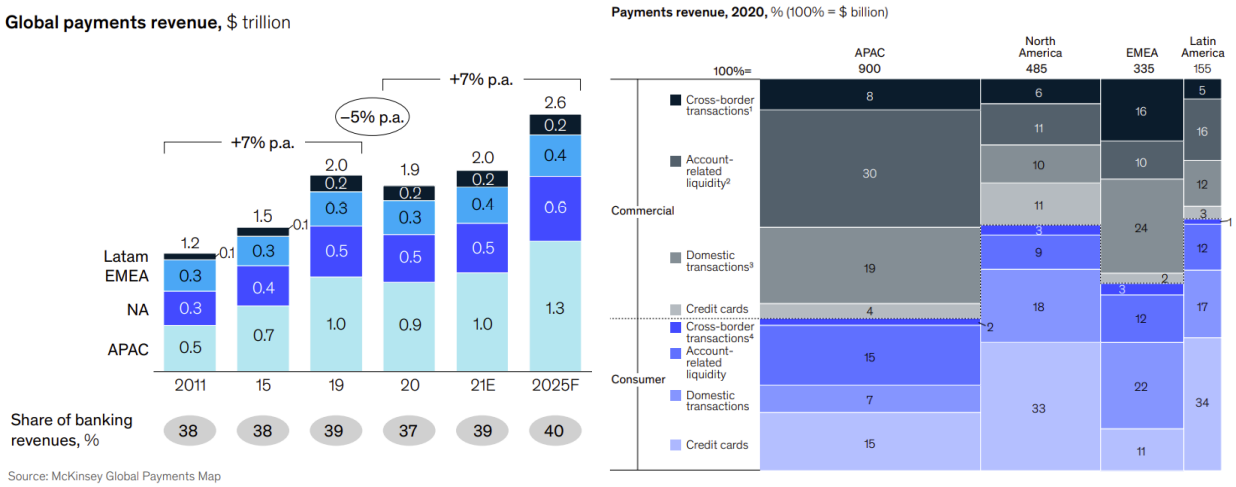


Exhibit 8: Breakdown of Global Payments Revenue

Exhibit 9: Total Revenue of Blockchains in the past 30 days[iv]

Kuriakin Zeng, Blockchain Research Analyst kz@gsgasset.com
Ray Shu, Head of Research ray@gsgasset.com
https://twitter.com/GSGResearch

Blockchains like Ethereum can also be used in conjunction with services provided by traditional financial institutions. Using the example of credit cards, Ethereum can be used by itself as a payment network operator like Visa/Mastercard, i.e. Dan can send ETH from his wallet to Kev's wallet on Ethereum. Or, Ethereum can also be used in conjunction with DeFi dApps that bring additional value to the user, similar to how banks can offer credit facilities to their credit card customers.

But for Ethereum to win market share from the likes of Visa/Mastercard, its fees need to be consistent and much lower than the incumbents to justify the switching costs. As a point of reference, the average network fee on Visa/Mastercard is $0.16, estimated from total revenue divided by the number of transactions in 2021[v] (We acknowledge this figure does not include the cost of payment processing on both ends of the transaction.) In comparison, the current fee on Ethereum is US$0.33 to US$1.67, depending on the transaction type. While this is roughly 2x-10x the average network fee on Visa/Mastercard, it is also <10% of the average wire transfer fee banks charge.

But we would argue that because gas fees on Ethereum would increase significantly if ETH price and network transaction volume increase (similar to what we witnessed in 2021), gas fees need to start so low that these factors are no longer significant—if it only costs $0.01 to make a transaction on Ethereum, it would not matter if ETH increased by 10x because the transaction fee would become $0.10. This would also make Ethereum competitive against alternative L1 chains which currently lack the robustness and breadth of the Ethereum ecosystem.

Name	Transaction Costs (in USD)		Estimated Max Throughput (in tps)
Visa	0.15		24,000
Mastercard	0.17		5,000
	Send ETH	Swap tokens	
Ethereum	0.33	1.67	15-35
Loopring	<0.01	0.40	2,025 (Data on-chain) -16,400 (Data off-chain)
Metis Network	0.01	0.06	5,000
ZKSync	0.02	0.05	2,000
Arbitrum One	0.02	0.07	5,000
Optimism	0.05	0.07	5,000
Boba Network	0.08	0.23	5,000
Aztec Network	0.14	-	2,000
Polygon Hermez	0.25	-	2,000

Exhibit 10: Comparison of Transaction Costs and Throughput among Visa, Mastercard, Ethereum & L2

L2 will bring Ethereum closer to the goal of lower gas fees. As **Exhibit 10** suggests, L2 has thus far been able to reduce gas fees to swap tokens on Ethereum by between 75% and 97%, from $1.67 to anywhere between $0.05 and $0.40.

However, even these fees are too expensive; Vitalik Buterin, the founder of Ethereum, thinks that the fees "need to get under $0.05 to be truly acceptable." We're optimistic (pun not intended) though because Ethereum Foundation has clear roadmaps to reduce gas fees, including the highly anticipated danksharding. Rollup-centric projects, in particular, would be set to benefit the most from the implementation of EIP-4844: Shard Blob Transactions, aka proto-danksharding. The proposal creates a new transaction format for "blob-carrying transactions" that would decrease the storage and memory performance requirements of the Ethereum network, and reduce all rollup fees by up to ~100x compared to the current level. We can expect proto-danksharding to be implemented as early as 2023 ahead of full sharding later on.

The potential of L2 doesn't stop there; unlike Visa/Mastercard, which is limited to payments, Ethereum with L2 and lower fees open up possibilities for creating all types of applications on top of it or to support the

ecosystem. On Arbitrum alone, there are over 300 dApps, from lending and payments to NFTs and marketplaces.

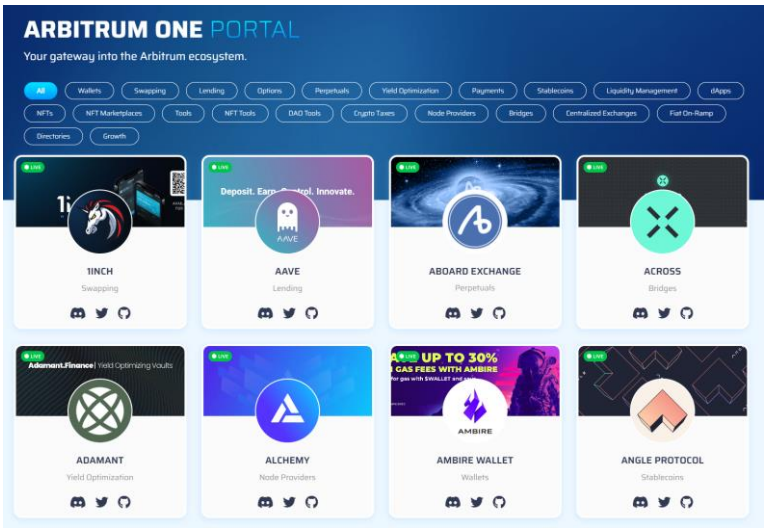


Exhibit 11: Dapps on Arbitrum

For Blockchain gaming specifically, lower gas fees can revolutionize the industry. As the gaming industry pivots its focus to in-game assets, Ethereum could potentially solve several related problems: eliminating fraudulent items, creating scarcity, aligning developer's and player's interests by implementing royalty schemes, and incentivizing more purchases by making items transferable across games. These in-game purchases translate to a US$54B market opportunity for L2[vi].

Moving forward, as L2 fees continue to slide, L2 will attract more users, and in turn, more developers creating dApps on L2. This is how the L2 will take over one industry at a time.

V. Select L2 Project Summaries & Comparison

Here are some L2 projects grouped based on scaling technology and generality.

General-purpose L2s behave just like Ethereum yet are cheaper. Anything that you can do on Ethereum L1, you can also do on L2. Many dApps have already begun to migrate to these networks or have skipped Mainnet altogether to deploy straight on an L2.

In contrast, application-specific L2s are projects that specialize in optimizing for a specific application space, bringing improved performance. As you can imagine, application-specific L2s are easier to develop so they have been around for a while. Alas, we think there is a cap to their adoption because they cannot be reused for other purposes apart from what they are built for. This is not to say they will be obsolete, because being laser-focused on one use-case can make them a better choice than the general-purpose L2s in the category that they play in.

Kuriakin Zeng, Blockchain Research Analyst kz@gsgasset.com
Ray Shu, Head of Research ray@gsgasset.com https://twitter.com/GSGResearch

	General Purpose	Application-Specific
State Channels	-	Raiden
Plasma	-	OMG Network
Optimistic Rollups	**Arbitrum One** **Optimism**	Layer2.Finance
ZK-Rollups	**Polygon (Hermez)** **zkSync 2.0** Scroll **StarkNet**	**StarkEx (dYdX)** **Loopring**
Validium / Volition	-	**StarkEx (Immutable X)** DeversiFi Arbitrum Nova

Exhibit 12: L2 Projects by Technology & Universality

We will give an overview of the ones in bold and compare the adoption of the live projects.

General Purpose L2s

Compared to application-specific L2s, general-purpose L2s are harder to build. As a result, the projects are relatively young—in fact, some of them are not even on testnet.

Arbitrum One is an Optimistic Rollup that aims to feel exactly like interacting with Ethereum, but with transactions costing a fraction of what they do on L1. Like Optimism, its transactions are recorded on Arbitrum One but are secured on Ethereum. Although the mainnet launch is relatively late compared to other L2 (May 2021), its EVM-compatibility helped it to become the most popular L2 with a TVL pool of ~$4 billion and over 300 dApps already on its platform. It includes major dApps such as 1inch, Uniswap, Sushi, Aave, and The Graph (read about our coverage on The Graph here). Arbitrum One does not have a token yet and ETH is the currency used on the platform.

Optimism (OP) is a popular Layer-2 that benefits from the security of the Ethereum mainnet and helps scale the Ethereum ecosystem by using OR. That means transactions are trustlessly recorded on Optimism but ultimately secured on Ethereum. Being EVM-compatible, Optimism grew to be the second largest scaling solution for Ethereum with over $1.57 billion in TVL. It hit the mainnet on January 2021 and is now home to 200 dApps, the biggest being Synthetix (SNX), a derivatives exchange, Uniswap (UNI), a DEX, and Velodrome (VELO), an AMM. Users can begin their journey on Optimism by adding the chain on their Metamask and bridging tokens like ETH to the L2. While Optimism has a token, it only gives holders participation rights in their governance system that makes technical decisions and public-goods funding decisions. Fees on Optimism are paid in ETH.

StarkWare's **StarkNet** is the only general-purpose ZKR that is already on the mainnet. Unlike most ZKR solutions that use zk-SNARKs, StarkNet uses zk-STARKs, a ZKP technology that is more secure in theory but requires more gas, takes longer to verify, and occupies more block space. StarkNet launched its Alpha version to the mainnet on November 2021. It had the advantage of being the first and only general-purpose ZKR in the market but StarkNet failed to gain meaningful traction; its TVL is $1.38M. We believe this has to do with the requirement to use Cairo, a new, low-level language that has a high learning curve. The barrier to entry is especially high in contrast to their EVM-compatible alternatives. The situation may change as Nethermind's Warp, a transpiler that translates Solidity to Cairo, has become available, making StarkNet Type-4 zkEVM.[vii] zkEVM Type-4s are equivalent to high-level languages only, not the EVM itself. They come with the advantage of faster and cheaper proof generation, but a small subset of applications may be incompatible with StarkNet. Fees on StarkNet are paid in ETH right now, but StarkNet plans to launch their native tokens for staking, governance and payment of transaction fees on StarkNet in September 2022.

Kuriakin Zeng, Blockchain Research Analyst kz@gsgasset.com
Ray Shu, Head of Research ray@gsgasset.com https://twitter.com/GSGResearch

zkSync 2.0 is an EVM-compatibility upgrade to zkSync 1.0 which is an application-specific ZKR platform that's already live, having a $58.1M TVL and ~130 dApps including 1inch. zkSync 1.0 supports only payments, token swaps, and NFT minting. That will change with zkSync 2.0 which supports general-purpose functions with its zkEVM scheduled to launch in Q4 2022. Despite its marketing, zkSync is not technically compatible with the EVM, but rather with Solidity and Vyper. This makes zkSync 2.0 a Type-4 zkEVM, just like StarkNet. As a Type-4 zkEVM, zkSync 2.0 experienced quicker proving times but suffers from less application compatibility than its competitors. zkSync 2.0 comes with a ground-breaking feature: 'paymaster.' If enabled by dApps, it allows users to pay fees in any ERC-20 tokens. With paymaster, dApps can subsidize users' transactions to make them even cheaper (or completely free).

Polygon is a set of Ethereum scaling solutions with a flexible framework that allows developers to build and connect various L2 solutions to the Ethereum network. Its flagship is the Polygon PoS chain (a Sidechain—not an L2) which is a stranger to no one. With a TVL pool of $1.44b, it is more popular than all L2s except Arbitrum. Polygon Hermez team is working on a Type-2 zkEVM which would head to mainnet in early 2023. Type-2 zkEVM aims to be fully compatible with existing applications but suffers from a slower proving time compared to Type-4.

Application-specific L2s

Compared to general-purpose L2s, application-specific L2s are simpler to develop. Some projects like dYdX and Loopring have attracted significant adoption, but the adoption is capped at the market size of the use case they are developed for. This is why while they have been around longer, general-purpose L2s have taken over them in terms of TVL.

StarkEx is an application-specific Layer-2 that supports transfers, minting, and trading created by StarkWare. Just like StarkNet, StarkEx uses zk-STARKs, a ZKP technology that is more scalable and secure at the cost of a larger proof size. StarkEx supports three Data Availability modes: Rollups, Validium, and Volition. Since its mainnet launch in June 2020, it has garnered a TVL of US$558M across all deployments. It powers various L2 projects such as dYdX and Immutable X:

- **dYdX** leverages StarkEx to scale its cryptocurrency exchange. Launched in April 2021, dYdX has emerged as an early success story of the scaling advantages afforded by ZKR and owns the third largest TVL of $466M among L2 projects. Its native token DYDX is a governance token that grants holders the right to propose changes on the dYdX's layer 2, and the opportunity to profit through token staking and trading fee discounts. It's free to trade on dYdX but the gas cost incurred during deposits and withdrawals are paid in ETH.
- **Immutable X** (IMX) positions itself as the first L2 for Games and NFTs on Ethereum, with instant trading, massive scalability, and zero gas fees for minting and trading, all without compromising users or asset security. Launched in April 2021, Immutable X owns a TVL of 43.49M. The IMX token is the native token, which users can earn by conducting pro-network activities such as trading, and which can be used to pay fees, perform governance, or stake on the protocol.

Loopring is an L2 designed for the DEX protocol built with ZKR for Ethereum. Using the Loopring protocol (loopring.org), one can build high-performance, orderbook-based, decentralized exchanges that do not take custody of users' crypto assets. Loopring Exchange (loopring.io) is an example. Loopring protocol was first deployed on the mainnet in December 2019 and has become the fourth most popular L2 project with $146M TVL. The native token on Ethereum LRC is used for incentivizing positive behavior from liquidity providers, insurers, and DAO governors as well as giving them a say in how the protocol is run. Users pay fees in the token they are buying. The fees are distributed to liquidity providers, insurers, and Loopring DAO in LRC or ETH after conversion.

Kuriakin Zeng, Blockchain Research Analyst kz@gsgasset.com
Ray Shu, Head of Research ray@gsgasset.com https://twitter.com/GSGResearch

Comparison of Adoption

By comparing the adoption of live projects, we can deduce that neither the first mover advantage nor superior cryptographic technology (i.e. ZKR) matters to adoption as much as ease of use and EVM compatibility. For this reason, EVM-compatible solutions are likely to dominate the market.

Ordered by Mainnet Launch Date →

	Loopring	StarkEx (dYdX, IMX)	Optimism	Arbitrum One	StarkNet
Mainnet launch date	Dec 2019	Jun 2020	Jan 2021	May 2021	Nov 2021
Purpose	Payment, Trading	Exchange, NFT	General	General	General
EVM compatibility	No	No	Yes	Yes	Yes, via transpiler
Technology	ZKR	ZKR, Validium	OR	OR	ZKR
TVL	$148M	$558M	$1.57B	$2.82B	$1.38M
Unique addresses	152K	50.1K	1.43M	1.23M	26.9K
Number of daily txns	50K	409.79K	115K	209K	70
Fee to send ETH	<$0.01	N/A	$0.09	$0.02	N/A
Number of dApps	N/A	4	~200	~300	~100
GitHub commits	1	N/A	48	98	N/A

Exhibit 13: Comparison of Live L2 Projects (Data as of 9 Sep 2022)

We will further discuss Arbitrum, Optimism, and StarkEx in the Appendix along with zkSync 2.0 and Polygon Hermez although they are not live yet.

VI. Outlook

Where are we in L2 adoption?

The TVL on L2 (in ETH) increased by ~10x, from 200k in Sep 2021 to 3m as of today. The growth in TVL is not showing any signs of slowing down despite crypto winter. There is plenty of growth left; for context, the current TVL on L2 is just ~13% of that on Ethereum.

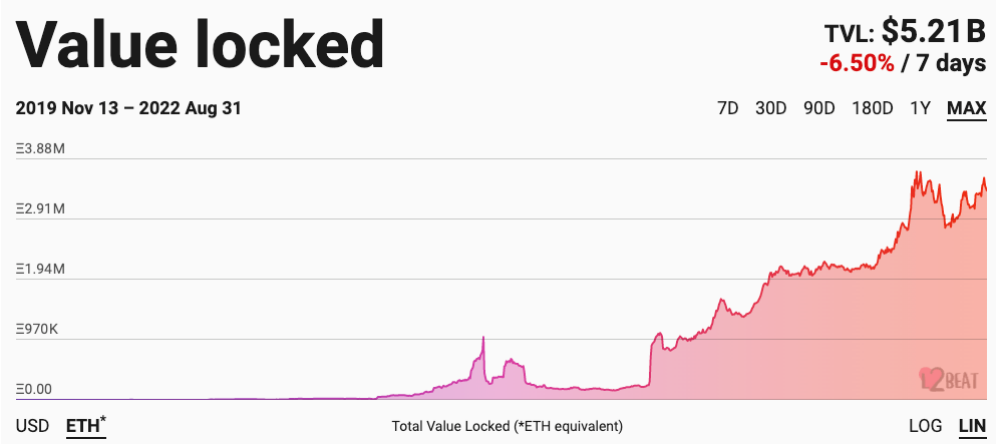


Exhibit 14: Total Value Locked on L2 in ETH

The number of transactions paints the same picture. The number of transactions on L2 hovers around 150K for the past 4 months, representing only ~4% of the number of transactions on the base layer. Given that L2 will be where most transactions will take place, we have probably just seen the onset of the explosion of L2.

Kuriakin Zeng, Blockchain Research Analyst kz@gsgasset.com
Ray Shu, Head of Research ray@gsgasset.com https://twitter.com/GSGResearch

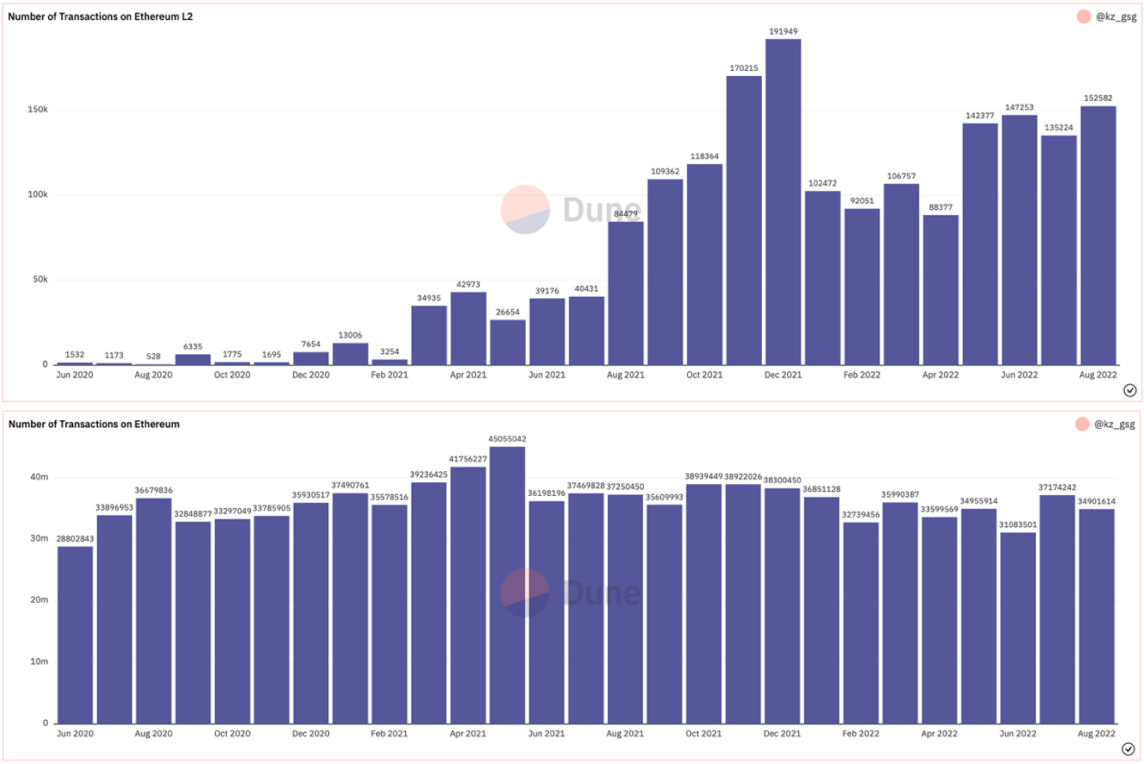


Exhibit 15: Monthly Number of Transactions on Ethereum vs. on L2 between Jun 2020 and Aug 2022

Which L2 scaling solution will win?

Rollup-centric projects are dominating the L2 market. They will continue their domination as they stand to benefit the most from the upcoming proto-danksharding in 2023, which would decrease the storage and memory performance requirements of the Ethereum network, and reduce all rollup fees by up to ~100x from the current level.

Between the two flavors of rollups, OR has been the L2 with the largest TVL, dominating the market with a share of 84%. It's easy to see why. It is EVM-compatible, and the technology is simple and has been around for a while.

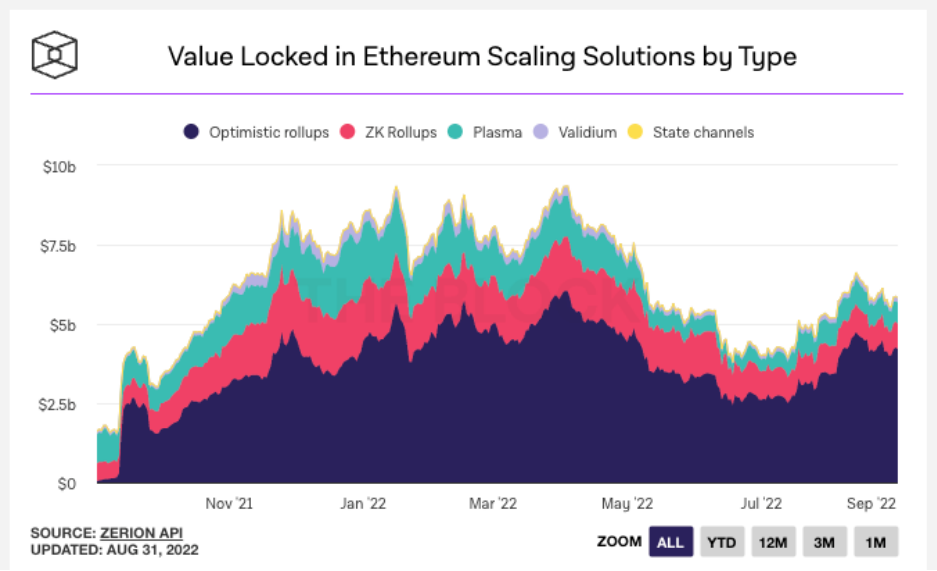


Exhibit 16: Total Value Locked in L2 Solutions by Type

Kuriakin Zeng, Blockchain Research Analyst kz@gsgasset.com
Ray Shu, Head of Research ray@gsgasset.com https://twitter.com/GSGResearch

However, we believe that we are at the pivotal moment where ZKR starts to steal the limelight from OR. Previously, one of the main issues facing ZKR was their lack of EVM compatibility. The zkSync 2.0 protocol is currently available on the Rinkeby testnet and supports the majority of Ethereum opcodes. Polygon Hermez has also announced their zkEVM at EthCC, and is scheduled to hit the mainnet in early 2023.

Our thesis is that the next cycle will be led by three narratives: (1) financial institutions adopt Blockchain technology to solve their business problems, (2) consumer brands launch NFTs for loyalty and brand extension, and (3) Blockchain-based games with excellent gameplay disrupt traditional games.

In the first narrative, we believe that ZKR will be the primary choice for most TradFi use cases as ZKR scores high on security and usability with 2000 tps, which is more than 1700 tps that Visa is handling[viii]. For specific use-cases, such as high-frequency trading, TradFi might look into Validium, which boasts a throughput of 9000 tps and increased privacy, so that users' trading strategies are protected.

In the second narrative, we believe that ZKR is the winner because consumer brands such as Tiffany[ix] will limit the supply of NFTs and care about user experience more than minting costs. This makes OR unsuitable because it would take at least one week before the user can officially receive the NFT. Validium, on the other hand, offers lower minting fees, but it is not worth lowering security and risking your brand image over lower fees, especially when the minting fees are borne by the consumer.

It's a different story for the third narrative, though. The fact that Validium-based zkPorter, Immutable X, or Arbitrum Nova are designed for games and charge little to zero gas fees may make Validium more attractive for game developers than ZKR. If "League of Legends" is deployed on Ethereum, it is possible to cast billions of NFTs a year. Even if minting an NFT on ZKR costs $0.10, the cost quickly becomes unsustainable for the game developers. We believe the high throughput and low cost make Validium the choice for large-scale games.

Impact on Alternative L1s: You Only Need One Internet

With L2, Ethereum will become the ecosystem of choice to build dApps for most people.

Most alternative L1s exist because Ethereum is deemed not scalable and too costly. With L2 built on Ethereum, the value proposition of these L1s has thus diminished. Chains like Solana try to make a chain that is as fast as possible, but ultimately they are still a single, monolithic blockchain bounded by scalability trilemma. Solana, for example, cranks up the spec of its nodes, but it is at the expense of decentralization because the price of the hardware required to run a node increases the barrier to participation. Ethereum on the other hand "escapes" from the scalability trilemma by transitioning into a modular blockchain.

Modular blockchains split chains up into execution, security, and data availability layers. Each chain has a specific role and is built on top of another in order to inherit the qualities of the underlying blockchain. Without L2, Ethereum needs to handle all three layers. Some L2s (Rollups) take over the responsibility of the execution layer and others (Validium) both the execution and data availability layers.

The promise of modular architecture is to be several orders of magnitude better than monolithic blockchains on every level. The aim is for L2s to be able to do anything that a monolithic L1 can do but better and be seamlessly interoperable with other L2s.

Kuriakin Zeng, Blockchain Research Analyst kz@gsgasset.com
Ray Shu, Head of Research ray@gsgasset.com https://twitter.com/GSGResearch

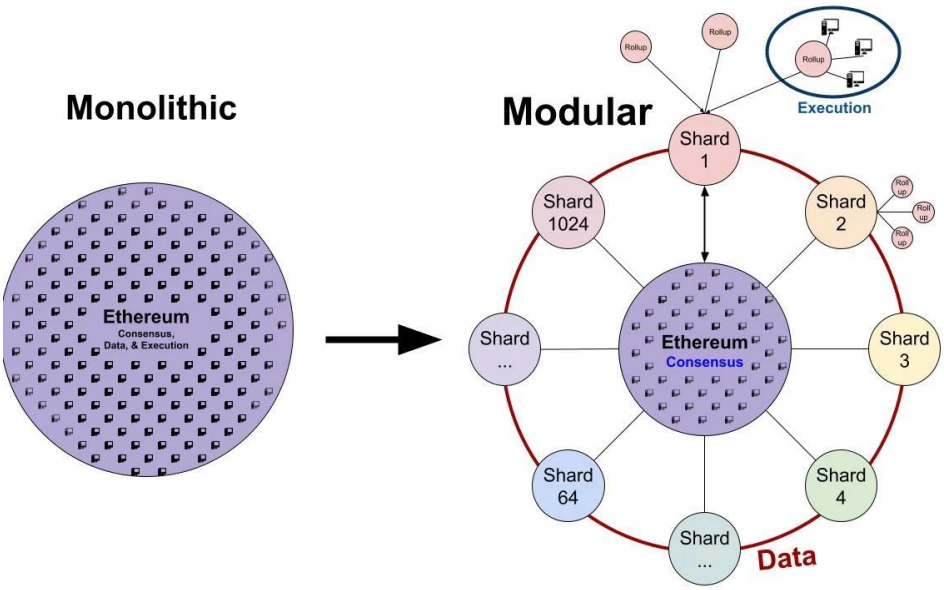


Exhibit 17 Monolithic vs. Modular Blockchains

There are other versions of modular blockchains such as Cosmos. Cosmos believes that all dApps would eventually need their own chains. The challenge is that each blockchain needs to maintain its own state and validator community. Why not build on Ethereum which is already secured by 420,000 validators and a large user base?

One compelling reason is the need for self-sovereignty while safely interoperating with other chains. In a rare move, dYdX recently announced the plan to move to Cosmos so that they can achieve the throughput, finality, and fairness required to decentralize the orderbook and matching engine by the end of 2022.

Given our thesis that the next cycle will be driven by the three narratives, we see that Ethereum and other chains that focus on modularity and interoperability like Cosmos winning in the short to medium term:

- TradFi and brands who want to build a dApp / mint NFTs would choose Ethereum; they have too much to lose by using Solana, which experienced a 4-hour outage as recently as 1 June 2022
- Some TradFi institutions may want to preserve self-sovereignty and launch their own chains, and this is where chains like Cosmos shine
- Games can use Validium-/Volition-based chains such as zkPorter (especially with zkEVM), Immutable X, or Arbitrum Nova

Long term, however, we think that chains like Solana will build their own L2 to compete with Ethereum. The second L1 that develops a good L2 ecosystem still has a chance to get significant market share from the growing market. It remains to be seen which alternative L1s will rise to be the contender to the king.

For a detailed analysis of alternative L1s and L2s, you can request access from kz@gsgasset.com. We have recently published a report on Solana here.

Kuriakin Zeng, Blockchain Research Analyst kz@gsgasset.com
Ray Shu, Head of Research ray@gsgasset.com https://twitter.com/GSGResearch

Impact on ETH

A factor that drives the price of ETH is the demand for gas, measured by the total gas fees paid in ETH. There are two forces at play: (1) lower gas fees per transaction, and (2) higher volume of transactions.

When the user performs a transaction on L2 instead of L1, the user needs a lot less ETH to pay for the transaction, reducing the demand for gas. Currently, it costs 3%-25% ETH of what it used to. When EIP-4844, i.e. proto-danksharding, is implemented, it might cost 1/100 of the current rates.

This means to get to the current level of total gas fees paid in ETH, we will need an exponential increase in volume to offset lower fees per transactions. We present a mock analysis below to demonstrate the possible near-, medium- and long-term impact of L2 on the total gas fee on the mainnet. Assuming two-thirds of gas fees are paid on L2, we would need the volume of transactions in the Ethereum ecosystem to grow by ~13x to get to the current total gas fees paid in ETH when unit gas fees fall by 75%.

Mock Analysis of L2's Impact on Total Gas Fee on Ethereum Mainnet
Assume 2/3 migration to L2s

	Total Gas Fee on Ethereum Mainnet	Gas Fee (unit) on Ethereum Mainnet		Ethereum Mainnet Volume	L2 Volume	Total Ecosystem Volume
Original	1,670,000	$ 1.67	Base	1,000,000	-	1,000,000
			Bundle from L2	53,333		
Without	132,000	$ 0.40	Base	330,000	670,000	1,000,000
Growth	-92%	-76%	Total	383,333		1x
			Bundle from L2	223,333		
5x Growth	660,000	$ 0.40	Base	1,650,000	3,350,000	5,000,000
"Near Term"	-60%	-76%	Total	1,873,333		5x
			Bundle from L2	580,667		
13x Growth	1,716,000	$ 0.40	Base	4,290,000	8,710,000	13,000,000
"Medium Term"	3%	-76%	Total	4,870,667		13x
			Bundle from L2	4,466,667		
100x Growth	13,200,000	$ 0.40	Base	33,000,000	67,000,000	100,000,000
"Long Term"	690%	-76%	Total	37,466,667		100x

Exhibit 18: Mock Analysis of L2's Impact on Total Gas Fees on Ethereum Mainnet

In the near term, we will likely see existing projects continue to migrate from L1 to L2 to save gas fees. As a result, the demand for gas on Ethereum will drop significantly and adversely affect the price of ETH.

In the medium term, we expect to see dApps migrating from EVM-compatible chains to Ethereum L2 as well as new dApps being developed on Ethereum L2. Use-cases that had not been viable on Ethereum would become viable. Use cases that had been hard to build on Ethereum would become easy. SkyMavis had to build their own Sidechain for Axie Infinity and secure it with their own set of validators. But now someone could build it on an L2 like zkPorter (especially with zkEVM), Immutable X, or Arbitrum Nova. In the medium term, a 13x growth in volume for the Ethereum ecosystem is entirely achievable.

In the long term, we believe that Ethereum with L2 can grow by 100x in volume as new use-cases of blockchain are discovered and for most people, Ethereum becomes the logical choice to build them on: we do not need a second Internet.

Kuriakin Zeng, Blockchain Research Analyst kz@gsgasset.com
Ray Shu, Head of Research ray@gsgasset.com https://twitter.com/GSGResearch

VII. Appendix

Arbitrum One

Overview

Arbitrum One is an Optimistic Rollup that aims to feel exactly like interacting with Ethereum, but with transactions costing a fraction of what they do on L1. Like Optimism, its transactions are recorded on Arbitrum One but are secured on Ethereum. Although the mainnet launch is relatively late compared to other L2 (May 2021), its EVM-compatibility helps it to become the most popular L2 with a TVL pool of ~$4 billion and over 300 dApps already on its platform. It includes major dApps such as 1inch, Uniswap, Sushi, Aave, and The Graph (Read about our coverage on The Graph here).

Unique Selling Points

Arbitrum One's secret sauce that differentiates it from Optimism is its interactive fraud proofs. In Optimism, fraud proofs are executed in a single round of state re-execution. In contrast, Arbitrum One uses interactive multi-round proving, which takes place through a multi-step exchange between the node operator proposing a new state transition and a validator challenging its validity.

Counterintuitively, interactive proving is more efficient in L1 gas usage. Unlike single-round fraud proving, it does not require the L1 smart contract to re-run the transaction. Further, multi-round proving can support highly complex transactions because transactions are not bound by gas limitations or contract size limits.

How Network Is Secured

To publish a block on Arbitrum, validators must provide a bond in ETH before producing blocks, much like a proof-of-stake system. It specifies a time window during which anyone can dispute a state transition. If a node disputes a batch, then Arbitrum will initiate the fraud-proof computation. Part of the malicious validator's bond is awarded to the challenger, while the other part is burned. The burning prevents collusion among validators; if two validators collude to initiate bogus challenges, they will still forfeit a considerable amount of the stake.

Team

- Ed Felten is Co-Founder and Chief Scientist at Offchain Labs. He was formerly the Robert E. Kahn Professor of Computer Science and Public Affairs at Princeton University. He also served at the White House as Deputy United States Chief Technology Officer and senior advisor to the President. He is an ACM Fellow and member of the National Academy of Engineering.
- Steven Goldfeder is Co-Founder and CEO. He holds a Ph.D. from Princeton University, and he worked on cryptography and cryptocurrencies. He co-authored Bitcoin and Cryptocurrency Technologies, the leading textbook on cryptocurrencies.
- Finally, Harry Kalodner is Co-Founder and CTO. He attended Princeton as a Ph.D. candidate where his research was on economics, anonymity, and incentive compatibility of cryptocurrencies.

Project Backers

Arbitrum is backed by big names such as Lightspeed, Pantera, Polychain Capital, Redpoint, Ribbit Capital, Alameda Research, Coinbase Ventures, and Compound.

Key Historical Events

- Aug 2018: Detailed vision of Arbitrum One published for the first time
- Oct 2020: Arbitrum One rollup deployed on Ethereum's testnet
- May 2021: Arbitrum One deployed on mainnet
- Sep 2021: Arbitrum One TVL crosses $1 billion for the first time
- Jan 2022: Arbitrum One sequencer goes offline for ~7 hours due to hardware failure
- Apr 2022: Arbitrum Nitro launched in testnet

Kuriakin Zeng, Blockchain Research Analyst kz@gsgasset.com
Ray Shu, Head of Research ray@gsgasset.com https://twitter.com/GSGResearch

- Aug 2022: Arbitrum Nova launched
- Sep 2022: Arbitrum Nitro mainnet launch

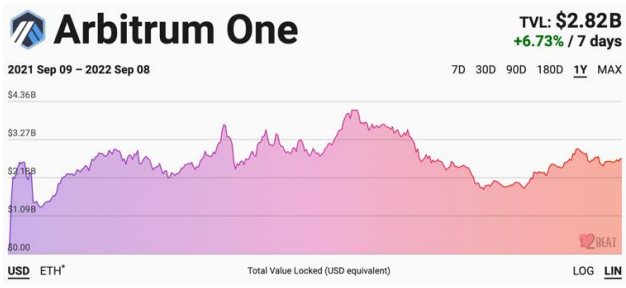
Upcoming Events

- Decentralized sequencing

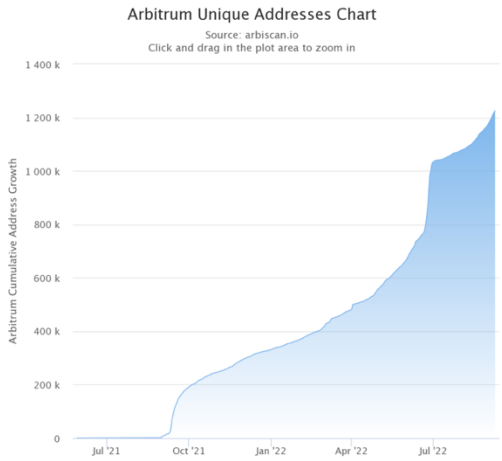
Statistics

Although the entire market has been in a downtrend since the start of the year, statistics show that Arbitrum One's TVL, unique addresses, transaction volume, and developer activities are growing.

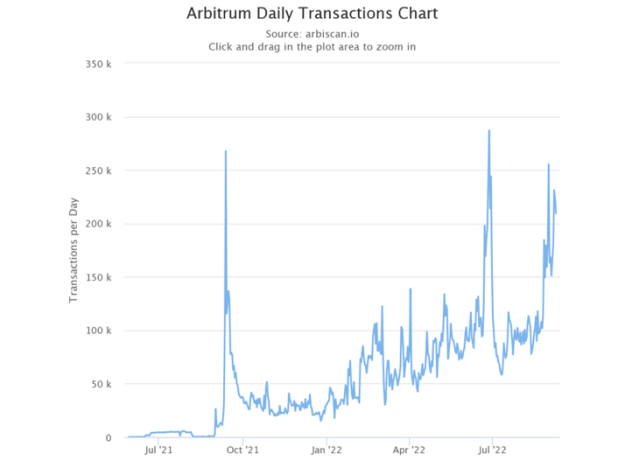
TVL: $2.82b (L2 Beat, 9 Sep 2022)



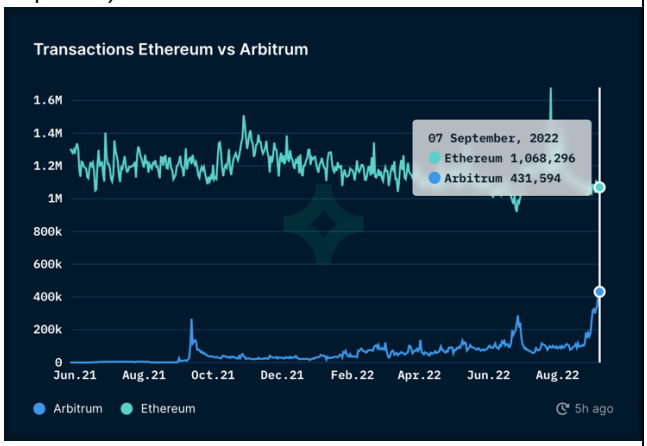
Unique Addresses: 1,225,478 (Arbiscan, 08 Sep 2022)



Daily Txn: 209,354 (Arbiscan, 08 Sep 2022)



% Txn on Arbitrum One / Ethereum: 40.4% (Nansen, 07 Sep 2022)



GitHub Commits: 98 commits (28 Aug 2022)

Daily Arbitrum One Gas: $0.02 (L2 Fees, 09 Sep 2022)

Name	Send ETH	Swap tokens
Metis Network	$0.01	$0.06
Loopring	$0.02	$0.42
Arbitrum One	$0.02	$0.07

Tokens

Arbitrum One does not have native tokens. ETH is used for gas fees and for. We can expect Arbitrum to eventually release a token. You can position yourselves to receive some free tokens via airdrops.

Kuriakin Zeng, Blockchain Research Analyst kz@gsgasset.com
Ray Shu, Head of Research ray@gsgasset.com https://twitter.com/GSGResearch

Optimism

Overview

Optimism (OP) is a popular Layer-2 that benefits from the security of the Ethereum mainnet and helps scale the Ethereum ecosystem by using OR. That means transactions are trustlessly recorded on Optimism but ultimately secured on Ethereum. Being EVM-compatible, Optimism grew to be the second largest scaling solution for Ethereum with over $1.57 billion in TVL. It hit the mainnet on January 2021 and is now home to 200 dApps, the biggest being Synthetix (SNX), a derivatives exchange, Uniswap (UNI), a DEX, and Velodrome (VELO), an AMM.

Unique Selling Points

The key differentiator of Optimism from Arbitrum One is that it uses single-round fraud proofs, which begin with the last correct state, re-run the allegedly invalid transition on L1, and then compare the resulting state with the one that was published by the sequencer (the privileged node operator who proposes new states to L1). Any invalid transition in the proposed batch will trigger a mismatch between the two states.

The benefits of single-round fraud proofs are that it is much simpler to design and removes the need for the parties involved to coordinate among themselves; this makes fraud proofs instant. Interactive fraud proofs in contrast require two or more parties to work together to dissect the challenge, taking a longer time to resolve.

The simplicity comes with the higher cost of computing the entire transaction on the L1. There are also limitations on the size of blocks and transactions (based on the L1) that can be effectively verified in a non-interactive method while an interactive method does not face this constraint as only the single step is verified.

How Network Is Secured

To publish a block on OP, validators must provide a bond in ETH before producing blocks, much like a PoS system. It specifies a time window during which anyone can dispute a state transition. If a node disputes a batch, then Optimism will initiate the fraud-proof computation. Part of the malicious validator's bond is awarded to the challenger, while the other part is burned. The burning prevents collusion among validators; if two validators collude to initiate bogus challenges, they will still forfeit a considerable chunk of the entire stake.

Team

- Jinglan Wang, Co-founder & CEO, is the former Executive Director both at Plasma Group and at Blockchain Education Network. She has worked at Handshake, a decentralized naming protocol.
- Karl Floersch, Co-founder & CTO, is previously a researcher at Ethereum Foundation, and a blockchain engineer at Consensys.
- Ben Jones, Chief Scientist, was a Scalability Researcher at Plasma Group, and a former Cryptoeconomic Researcher at Ethereum Foundation.

Project Backers

Paradigm, a16z and IDEO CoLab Ventures

Key Historical Events

- Jun 2019 - Introduced Optimistic Rollup
- Oct 2019 - Unipig Optimistic Rollup Testnet
- Sep 2020 - EVM Compatible Testnet
- Jan 2021 - Alpha Mainnet
- Oct 2021 - EVM Equivalent Mainnet
- Dec 2021 - Open Mainnet

Kuriakin Zeng, Blockchain Research Analyst kz@gsgasset.com
Ray Shu, Head of Research ray@gsgasset.com https://twitter.com/GSGResearch

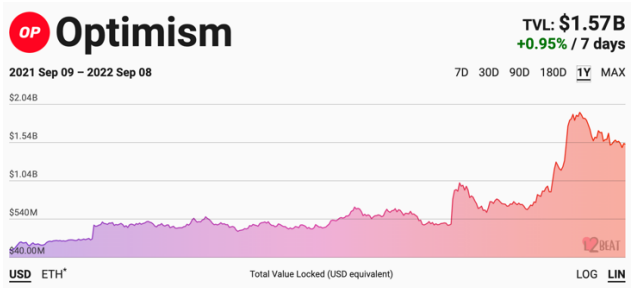
Upcoming Events

- 2022 - Next Gen Fault Proof
- 2023 - Sharded Rollup
- 2023 - Incentivized Verification
- 2023 - Decentralized Sequencer
- 2024 - L1 Governed Fault Proofs

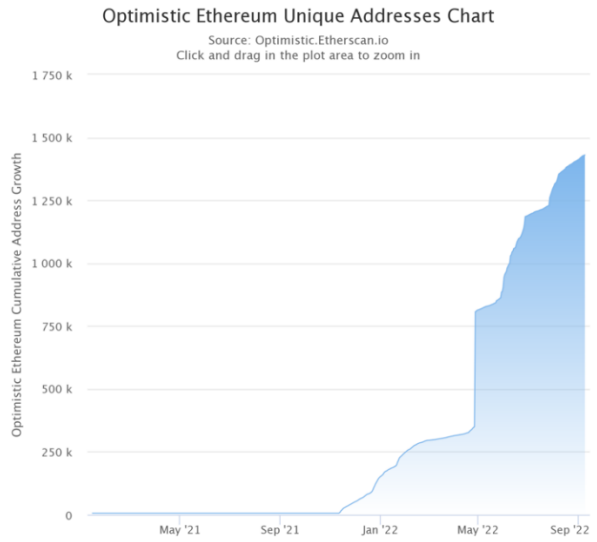
Statistics

Although the entire market has been in a downtrend since the start of the year, statistics show that Optimism's TVL, unique addresses, transaction volume, and developer activities are growing.

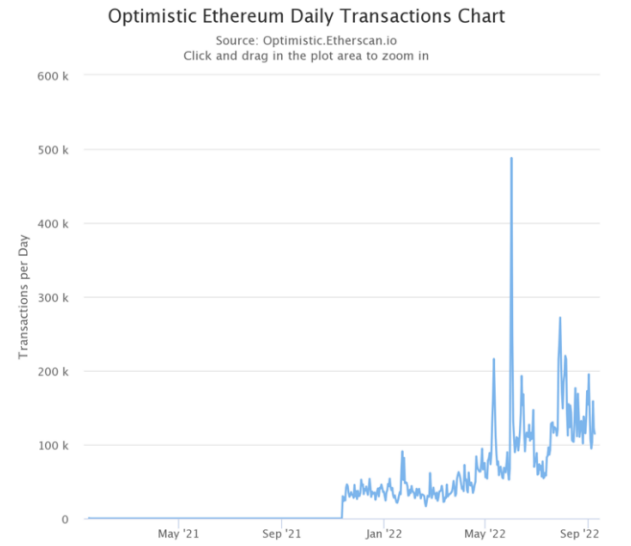
TVL: $1.57b (L2 Beat, 9 Sep 2022)



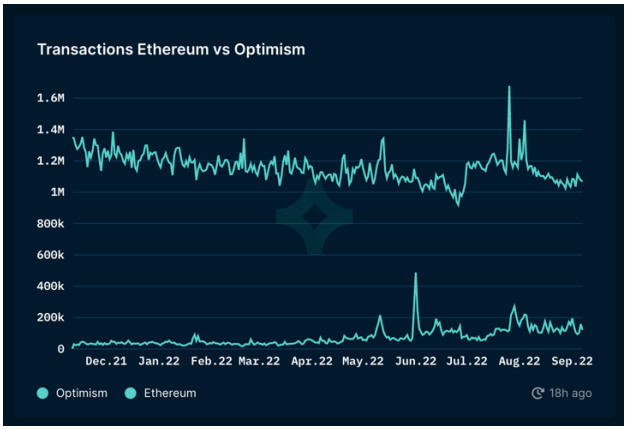
Unique Addresses: 1,430,349 (Etherscan, 8 Sep 2022)



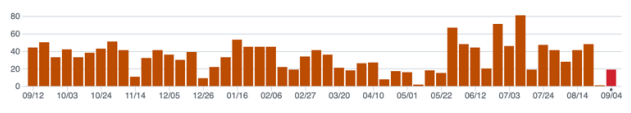
Daily Txn: 114,636 (Etherscan, 08 Sep 2022)



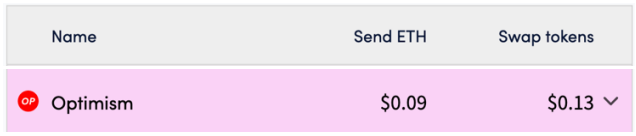
% Txn on Optimistic / Ethereum: 14.7% (Nansen, 06 Sep 2022)



GitHub Commits: 48 commits (21 Aug 2022)



Daily Optimism Gas: $0.09 (L2 Fees, 09 Sep 2022)



Kuriakin Zeng, Blockchain Research Analyst kz@gsgasset.com
Ray Shu, Head of Research ray@gsgasset.com

Tokens

Token Utility

While Optimism has a token, it only gives holders participation rights in their governance system that makes technical decisions and public-goods funding decisions. Fees on Optimism are paid in ETH.

Token Supply & Inflation

The initial token supply is 4,294,967,296 OP tokens, at an inflation rate of 2% a year. In Year 1, 30% of the initial token supply will be made available to the Foundation for distribution. After the first year, token holders will vote to determine the Foundation's annual OP distribution budget. The Foundation expects to seek the following annual allocations:

- Year 2: 15% of the initial token supply
- Year 3: 10% of the initial token supply
- Year 4: 4% of the initial token supply

Token Distribution

- Ecosystem fund (25%): split between the governance fund (5.4%), the partner fund (5.4%), the seed fund (5.4%), and unallocated (8.8%).
- Retroactive Public Goods Funding (20%)
- User airdrops (19%): split into a first airdrop of 5% and subsequent airdrops yet to be announced.
- Core contributors (19%): people who help bring the Optimism Collective from concept to reality
- Investors (17%)

Price Performance

OP was listed in June this year into a bear market. It hit a peak of $2.00 before declining to $1.10.

Kuriakin Zeng, Blockchain Research Analyst kz@gsgasset.com
Ray Shu, Head of Research ray@gsgasset.com

StarkEx (dYdX, Immutable X)

Overview

StarkEx is a permissioned, application-specific Layer-2 engine that supports transfers, minting, and trading created by StarkWare. Just like StarkNet, StarkEx uses zk-STARKs, a ZKP technology that is more scalable and secure at the cost of a larger proof size. StarkEx supports three Data Availability modes: Rollups, Validium, and Volition. Since its mainnet launch in June 2020, it has garnered a TVL of US$558M across all deployments. It powers various L2 projects such as dYdX and Immutable X:

- dYdX leverages StarkEx to scale its cryptocurrency exchange. Launched in April 2021, dYdX has emerged as an early success story of the scaling advantages afforded by ZKR and owns the third largest TVL of $466M among L2 projects. Its native token DYDX is a governance token that grants holders the right to propose changes on the dYdX's layer 2, and the opportunity to profit through token staking and trading fee discounts. It's free to trade on dYdX but the gas cost incurred during deposits and withdrawals are paid in ETH.
- Immutable X (IMX) positions itself as the first L2 for Games and NFTs on Ethereum, with instant trading, massive scalability, and zero gas fees for minting and trading, all without compromising users or asset security. Launched in April 2021, Immutable X owns a TVL of 43.49M. The IMX token is the native token, which users can earn by conducting pro-network activities such as trading, and which can be used to pay fees, perform governance, or stake on the protocol.

Unique Selling Proposition

- StarkEx uses zk-STARKs, a ZKP technology that is more scalable and secure at the cost of a larger proof size.
- StarkEx supports three Data Availability modes. In ZKR mode, data is published on L1. In Validium mode, data is stored off-chain. Volition is a hybrid mode where the user can choose whether to place data on L1 or L2.

Team

- Eli Ben-Sasson, Co-founder & President, is the co-inventor of STARK, FRI, and Zerocash protocols and a Founding Scientist of Zcash. Previously cryptographic and ZKP researcher for 20+ years across Princeton, Harvard, and MIT.
- Uri Kolodny, Co-founder & CEO, is a Serial Entrepreneur behind tech startups like OmniGuide and Mondria. He is the advisor to Certora, a provider of formal verification of smart contracts.
- Allesandro Chiesa, Co-founder & Chief Scientist, is a current faculty member at Berkeley's Computer Science department who researches complexity theory, cryptography, and security and focuses on ZKP. He is also the co-inventor of Zcash and an author of libsnark, the leading library for zkSNARK.

Project Backers

Paradigm, Sequoia, Pantera, 3AC, Intel Capital, and Data Collective

Key Historical Events

- Jun 2020: StarkEx 1.0 Mainnet Launch
- Aug 2020: Cairo Software Release
- Dec 2020: StarkEx 2.0 Mainnet Launch
- Apr 2021: dYdX, DeversiFi (rhino.fi), and Immutable launched using StarkEx
- Jul 2021: Sorare launches NFTs with StarkEx
- Jul 2021: StarkEx 3.0 Mainnet Launch
- Jul 2021: DeversiFi Renames as rhino.fi and Changes to L2 gateway to multi-chain DeFi
- Aug 2021: Cairo whitepaper is released
- Aug 2021: Warp EVM to Cairo transpiler PoC released for ERC-20 tokens

Kuriakin Zeng, Blockchain Research Analyst kz@gsgasset.com
Ray Shu, Head of Research ray@gsgasset.com https://twitter.com/GSGResearch

Upcoming Events

- TBC: dYdX v4 moves to Cosmos
- TBC: Immutable X to support staking

Statistics

TVL: $559M (Starkware, 19 Sep 2022)	Total Number of Txns (Starkware, 15 Sep 2022)
	

Tokens

StarkEx has no native tokens.

Kuriakin Zeng, Blockchain Research Analyst kz@gsgasset.com
Ray Shu, Head of Research ray@gsgasset.com

zkSync 2.0

Overview

zkSync 2.0 is an EVM-compatibility upgrade to zkSync 1.0 which is an application-specific ZKR platform that's already live, having a $58.1M TVL and ~130 dApps including 1inch. zkSync 1.0 supports only payments, token swaps, and NFT minting. That will change with zkSync 2.0 which supports general-purpose functions with its zkEVM scheduled to launch in Q4 2022.

Despite its marketing, zkSync is not technically compatible with the EVM, but rather with Solidity and Vyper. This makes zkSync 2.0 a Type-4 zkEVM, just like StarkNet. As a Type-4 zkEVM, zkSync 2.0 enjoys cheaper and faster proof generation but suffers from less application compatibility than its competitors like Polygon zkEVM who are building Type-2 zkEVM.

Unique Selling Points

- Cheaper and faster proof generation, at the cost of less application compatibility
- zkSync 2.0 comes with a ground-breaking feature: 'paymaster.' If enabled by dApps, it allows users to pay fees in any ERC-20 tokens. With paymaster, dApps can subsidize users' transactions to make them even cheaper (or completely free).
- In comparison to Polygon zkEVM, zkSync claims that "users do not rely on the sequencer for security." Their ZKR has a priority queue/emergency exit mechanism to protect users from censorship by the sequencer: users will always be able to exit zkSync regardless of malicious/faulty sequencers.

How the Network is Secured

Initially, zkSync 2.0 will use an authorized sequencer, which executes transactions and aggregates them into batches before submitting them to L1. This means a dishonest sequencer could theoretically pause a rollup or strategically reorder transactions in order to squeeze some extra profit for himself. If he goes offline, a sequencer can also bring the whole chain down. But even with these risks, a centralized sequencer is unable to falsify transactions, meaning rollups still hold security advantages relative to other, more centralized scaling products.

But eventually, zkSync 2.0 will switch to a collective sequencer secured by a multi-validator consensus with PoS where prospective operators deposit funds in the rollup contract, with the size of each stake influencing the staker's chances of getting selected to produce the next rollup batch. The operator's stake can be slashed if they act maliciously, which incentivizes them to post valid blocks.

Team

- Alex Gluchowski, Co-founder & CEO, is previously the Director of R&D at Entropy Labs and a serial entrepreneur with 10+ years of experience in software development and engineering
- Alex Vlasov, Co-founder & Head of R&D, is previously the Chief Research Scientist at BANKEX Foundation, a company focused on scaling Ethereum via plasma technology. He has a Ph.D. in Electrical Engineering from McGill University.
- Zoé Gadsden, COO, is a former product manager at Google, advisor at Tech Open Air, and the founding member of Female Narratives.

Project Backers

Ethereum Foundation, a16z, Dragonfly Capital, 1kx, Placeholder, and Union Square Ventures

Key Historical Events

- Jun 2020: zkSync 1.0 for scalable payments went live on mainnet
- Apr 2021: zkPorter data availability solution announced
- May 2021: zkSync 2.0 alpha went live on testnet

Kuriakin Zeng, Blockchain Research Analyst kz@gsgasset.com
Ray Shu, Head of Research ray@gsgasset.com https://twitter.com/GSGResearch

- Oct 2021: UniSync, a port of Uniswap launched on zkSync 2.0 testnet
- Feb 2022: zkSync's general-purpose zkEVM goes live on testnet

Upcoming Events

- zkEVM mainnet launch and support for validity proofs
- zkSync native token and zkPorter launch
- Decentralized sequencing launch

Statistics

zkSync 2.0 is not yet a live project

Tokens

zkSync has no native tokens yet, but the team has publicly stated that they will be launching a native token.

Kuriakin Zeng, Blockchain Research Analyst kz@gsgasset.com
Ray Shu, Head of Research ray@gsgasset.com https://twitter.com/GSGResearch

Polygon (Hermez)

Overview

Polygon is a set of Ethereum scaling solutions with a flexible framework that allows developers to build and connect various L2 solutions to the Ethereum network. Its flagship is the Polygon PoS chain (a Sidechain—not an L2) which is a stranger to no one in crypto. With a TVL pool of $1.44b, it is more popular than all L2s except Arbitrum. Polygon Hermez team is working on a Type-2 zkEVM which would head to mainnet in early 2023. Type-2 zkEVM aims to be fully compatible with existing applications but suffers from a slower proving time compared to Type-4.

Unique Selling Points

Polygon is working on Type-2 zkEVM which is fully compatible with existing applications

How the Network is Secured

Similar to zkSync 2.0, Polygon Hermez will initially use an authorized sequencer, which executes transactions and aggregates them into batches before submitting them to L1. This means a dishonest sequencer could theoretically pause a rollup or strategically reorder transactions in order to squeeze some extra profit for himself. If he goes offline, a sequencer can also bring the whole chain down. But even with these risks, a centralized sequencer is unable to falsify transactions, meaning rollups still hold security advantages relative to other, more centralized scaling products.

But eventually, they will switch to a collective sequencer secured by a multi-validator consensus with PoS where prospective operators deposit funds in the rollup contract, with the size of each stake influencing the staker's chances of getting selected to produce the next rollup batch. The operator's stake can be slashed if they act maliciously, which incentivizes them to post valid blocks.

Team

- Sandeep Nailwal, Co-founder, was previously the cofounder & CEO at ScopeWeaver.com, a marketplace for professional services, and the Head of Technology and Supply Chain at Welspun Group, a conglomerate operating in steel, energy, and textile industries, and software engineer at Computer Sciences Corporation.
- Jaynti Kalani, Co-founder, was the Data Scientist at Housing.com, a real estate search platform, and senior software engineer at Persistent Systems, an IT services company
- Mihailo Bjelic, Co-founder, was a prominent Ethereum community member and researcher

Project Backers

Sequoia, Tiger Global, SoftBank, Galaxy Digital, Union Square Ventures, Sino Global Capital

Key Historical Events

- Jun 2019: Matic launches alpha mainnet that allowed developers to build and test their applications
- Jun 2020: Matic network mainnet goes live with staking and delegation
- Feb 2021: Matic rebrands to Polygon
- Aug 2021: Polygon announces strategic focus on ZK scaling technology
- Aug 2021: Polygon acquires ZK-Rollup protocol Hermez Network
- Dec-21: Critical vulnerability in Polygon PoS contracts discovered, with $1.6M MATIC stolen

Upcoming Events

- Testnet launch of Polygon Hermez zkEVM

Statistics

Polygon zkEVM is not yet live

Kuriakin Zeng, Blockchain Research Analyst kz@gsgasset.com
Ray Shu, Head of Research ray@gsgasset.com

Tokens

Token Utility

The native token MATIC was launched in 2019 in conjunction Polygon PoS sidechain. It has been used for staking, governance, and paying transaction fees on the PoS chain. Recently Polygon announces that it will be the native token of Polygon Hermez and other projects as well. However, MATIC on Polygon Hermez is only for staking; transaction fees are paid in ETH. That said, in an interview with Bankless, Co-founder Mihailo mentioned that the token MATIC is undergoing a redesign. No details are out yet, but we think it will have a significant impact on MATIC's price.

Token Supply & Inflation

MATIC has a circulating supply of 4,877,830,774 and a max supply of 10,000,000,000 tokens.

Token Distribution

At its initial private sale in 2017, 3.8 percent of MATIC's max supply was issued. In the April 2019 launchpad sale, another 19 percent of the total supply was sold. The MATIC price was $0.00263 per token, and $5 million was generated. The remaining MATIC tokens are distributed as follows:

- Team tokens: 16 percent of the total supply.
- Advisors tokens: 4 percent of the total supply.
- Network Operations tokens: 12 percent of the total supply.
- Foundation tokens: 21.86 percent of the total supply.
- Ecosystem tokens: 23.33 percent of the total supply.

Price Performance

MATIC is listed in 2019 at the price of 0.0035. It hit a peak of $2.88 late last year before declining to $0.90 as of 09 Sep 2022. Despite the decline, it's still a 250x growth from its inception.

Kuriakin Zeng, Blockchain Research Analyst kz@gsgasset.com
Ray Shu, Head of Research ray@gsgasset.com

VIII. End Notes

[i] Lightning Network
[ii] Polygon PoS Chain
[iii] Sending ETH as the benchmark https://l2fees.info/
[iv] Total revenue is equal to the total fees paid by the users for the given time period
[v] Total revenue on Visa & Mastercard divided by number of transactions in 2021 = (24.1 + 18.9) / (164.7 + 112.1) billion = $0.16
[vi] https://www.statista.com/statistics/558952/in-game-consumer-spending-worldwide/#:~:text=In%202020%2C%20global%20gaming%20audiences,surpass%2074.4%20billion%20U.S.%20dollars.
[vii] https://vitalik.ca/general/2022/08/04/zkevm.html
[viii] https://news.bitcoin.com/no-visa-doesnt-handle-24000-tps-and-neither-does-your-pet-blockchain/
[ix] https://sea.mashable.com/tech/21038/tiffany-is-turning-nfts-into-jewellery-for-us50000-yeah-its-weird

Kuriakin Zeng, Blockchain Research Analyst kz@gsgasset.com
Ray Shu, Head of Research ray@gsgasset.com https://twitter.com/GSGResearch

Legal Disclaimers

This research report (the "**Research Report**") is provided and intended for select clients of Anduril Pte. Ltd and its affiliated or related companies (collectively, "**GSG**") who are authorised by GSG to receive it. If you are not so authorised, you must immediately delete or destroy this Research Report. If you receive this Research Report from GSG or any other source, you agree that you shall not copy, revise, amend, create a derivative work, provide to any third party, or in any way commercially exploit any of the information provided and that you shall not extract data from this Research Report, without the prior written consent of GSG.

The information provided by GSG, either in this document or otherwise, is for informational purposes only. This Research Report should not be relied upon as investment, financial, legal, tax, regulatory, or any other type of advice. This Research Report has not been prepared or tailored to address and may not be suitable or appropriate for the particular financial needs, circumstances, or requirements of any person, and it should not be the basis for making any investment or transaction decision. This Research Report is not, and is not intended to be, an offer to sell, a solicitation of an offer to buy, or a recommendation to purchase or sell any digital asset by GSG or any third party; or (3) official confirmation or official valuation of any transaction or asset mentioned herein.

GSG is not providing any personalized investment recommendations nor is it advising you on the merits of any investments when providing this Report. Nothing in this document constitutes a representation that any investment or strategy or recommendation is suitable or appropriate to an investors individual circumstances or otherwise constitutes a personal recommendation. The provider of this Research Report may be inexperienced or unprofessional and the ultimate purpose or intention, or financial status of such provider may differ from you.

If any person elects to enter into transactions with GSG, whether as a result of the Research Report or otherwise, GSG will enter into such transactions as principal only and will act solely in its capacity under the separately managed account agreement as between GSG and the person (the "**SMAA**") or any other relevant contractual capacity.

Before entering into any such transaction, you should conduct your own research and obtain your own advice as to whether the transaction is appropriate for your specific circumstances. In addition, any person wishing to enter into transactions with GSG must satisfy GSG's eligibility requirements. GSG may be subject to certain conflicts of interest in connection with the provision of the Research Report. For example, GSG may, but does not necessarily, hold or control positions in the digital assets discussed in the Research Report, and transactions entered into by GSG could affect the relevant markets in ways that are adverse to a counterparty of GSG. GSG may engage in transactions in a manner inconsistent with the views expressed in this Research Report.

All information is presented only as of the date published or indicated, and may be superseded by subsequent market events or for other reasons. GSG SHALL NOT HAVE ANY LIABILITY TO YOU FOR ANY LOSS OR DAMAGE OF ANY KIND INCURRED AS A RESULT OF THE USE OF OR RELIANCE ON THIS RESEARCH REPORT OR ANY INFORMATION CONTAINED HEREIN. YOUR USE OF THE RESEARCH REPORT AND YOUR RELIANCE ON ANY INFORMATION IS SOLELY AT YOUR OWN RISK.

GSG makes no representations or warranties (express or implied) regarding, nor shall it have any responsibility or liability for the accuracy, adequacy, timeliness, or completeness of, the information in the Research Report, and no representation is made or is to be implied that the information in the Research Report will remain unchanged. GSG undertakes no duty to amend, correct, update, or otherwise supplement the Research Report.

The digital asset industry is subject to a range of risks, including but not limited to: price volatility, limited liquidity, limited and incomplete information regarding certain instruments, products, or digital assets and a still emerging and evolving regulatory environment. The past performance of any instruments, products, or digital assets addressed in the Research Report is not a guide to future performance, nor is it a reliable indicator of future results or performance. Investing in digital assets involves significant risks and is not appropriate for many investors, including those without significant investment experience and capacity to assume significant risks. Please refer to the risk factors set out in and/or appended to the SMAA or other relevant contractual agreement.

Anduril Pte. Ltd. is exempted by the Monetary Authority of Singapore ("**MAS**") from holding a license to provide digital payment token ("**DPT**") services. Please note that you may not be able to recover all the money or DPTs you paid to a DPT service provider if the DPT service provider's business fails. You should not transact in a DPT if you are not familiar with the DPT. This includes how the DPT is created, and how the DPT you intend to transact is transferred or held by your DPT service provider.

You should be aware that the value of DPTs may fluctuate greatly. You should buy DPTs only if you are prepared to accept the risk of losing all of the money you put into such tokens. You should be aware that your DPT service provider, as part of its licence to provide DPT services, may offer services related to DPTs which are promoted as having a stable value, commonly known as "stablecoin."

You are responsible for determining whether the use of any of GSG's services is legal in your jurisdiction and you shall not use the services should such use be illegal in your jurisdiction. If you are uncertain, please seek independent legal advice.

Kuriakin Zeng, Blockchain Research Analyst kz@gsgasset.com
Ray Shu, Head of Research ray@gsgasset.com https://twitter.com/GSGResearch