BINANCE RESEARCH

Layer 2 Scaling
Market Update

Stefan Piech

Table of Contents

Key Takeaways

- Once L1s are strong enough, the majority of transactions can take place on L2s, allowing for further scalability and faster transactions with lower gas cost
- Comparing the different solutions, we can observe differences in speed and security. Optimistic and ZK-Rollups are seen as more secure than Side Chains and Plasma, though they are more limited in terms of speed and execution
- Looking at the different characteristics of Layer 2 scaling solutions (including Side Chains), we believe that ZK-Rollups offer the best overall approach in terms of security, performance, usability, and other noteworthy aspects
- The Ethereum blockchain will remain the settlement layer, while scaling solutions will continue to manifest their place as execution layers for the growing dApp ecosystem
- The introduction of zkEVM is a major milestone in terms of coding language usability and accessibility for developers. Currently, most ZK-Rollups are written in a low-level hexadecimal-based assembly language rather than Solidity, which introduces new levels of abstraction and complexity
- While Arbitrum's centralization tradeoff in pursuit of lower gas fees is understandable in the short term, we urge the project to continue its focus on creating a decentralized system
- Leveraging the power of ZK-Rollups, BNB Smart Chain has introduced zkBNB, bringing further scalability to the blockchain
- Optimistic rollups will likely see a further rise in popularity until zkEVMs are strong enough to compete. ZK-Rollups, using validity proof, offer long-term benefits due to fewer limitations compared to Optimistic rollups
- As of now, the majority of applications on Ethereum today will likely move to L2, further underlying the need for secure bridges. We consequently expect more bridges between L2s and centralized exchanges to emerge, as well as bridges between various L2s

Demystifying Layer 2 Scaling

Over the last years, we have seen the blockchain ecosystem growing at an exponential rate. This brought to attention the old and fundamental concerns that existing Layer 1 ("L1") platforms are limited in their scalability due to low transaction speeds.

The solution to this that found the most traction over the following months was Layer 2 ("L2") scaling which brought along the layer separation vision. **The goal of this layer separation is to build out L1s as foundational layers for security and dependability while moving rapid iterations and actions onto L2s.** Once L1s are strong enough, the majority of transactions can take place on L2s, allowing for further scalability and faster transactions with lower gas costs.

Once L1s are strong enough, the majority of transactions can take place on L2s, allowing for further scalability and faster transactions with lower gas cost

When building Layer 2 scaling solutions, it is important that they inherit the underlying security of the main chain. This is one of the elements differentiating them to sidechains, where validators secure the chain. The two main L2 solutions that have seen traction in the last few months are **zero-knowledge** ("zk") and **optimistic** rollups. While we assume some basic understanding, we'll still go over some of the basics first.

❖ Zero-Knowledge Rollups

Zero-knowledge rollups - simply put - are bundles of data that are processed and computed off-chain. This off-chain computation reduces the amount of data that has to be posted to the blockchain. They produce validity proofs to prove the correctness of their changes. The validity proof is a cryptographic assurance that the state change proposed by the rollup is really the result of executing the given batch of transactions. This means that ZK-rollups only need to provide validity proofs to finalize transactions on Ethereum, instead of posting all transaction data on-chain. Important data relevant to the smart contracts are requested less frequently than in L1 blockchains. This saves a large amount of processing power, and less of the blockchain capacity is used for transaction validation. Gas fees decrease, as a result, making transactions faster and cheaper.

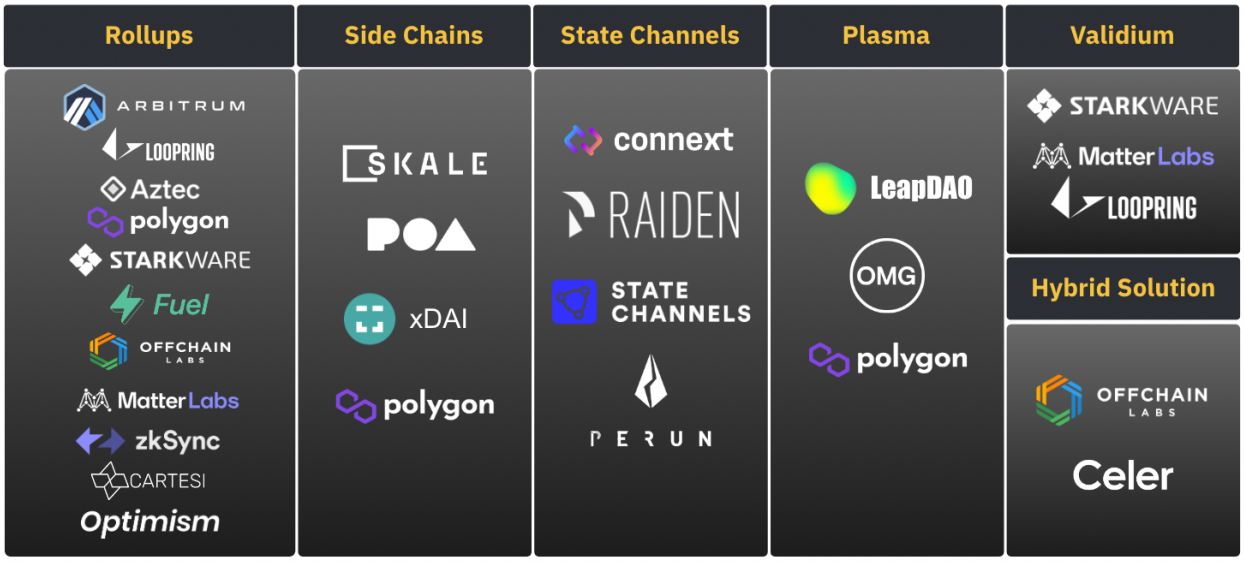
❖ Optimistic Rollups

Optimistic rollup operators bundle multiple off-chain transactions together in large batches before submitting them to Ethereum. This approach enables spreading fixed costs across multiple transactions in each batch, reducing fees for end-user. Data aggregators will compute Merkle roots to achieve increased transaction speeds. However, they offer less throughput than Plasma and ZK-Rollups. Optimistic rollups are considered "optimistic" because they assume off-chain transactions are valid and don't publish proofs of validity for transaction batches posted on-chain. This separates optimistic rollups from zero-knowledge rollups. Optimistic rollups have to rely on external validators to check the Merkle roots before the state can be updated.

Vitalik Buterin called Rollups his favorite Layer 2 solution[1]

While there are other scaling solutions worth mentioning, like Plasma, which uses child-chains to assist the main chain in verification, Polkadot's parachains, Bitcoin's Lightning Network, Sidechains, Validium, and State Channels, we will focus exclusively on Rollups in this report due to their increased adoption and relative importance compared to alternative solutions.

Figure 1: Selection of Layer 2 Scaling Solutions on Ethereum indicate a focus on Rollups

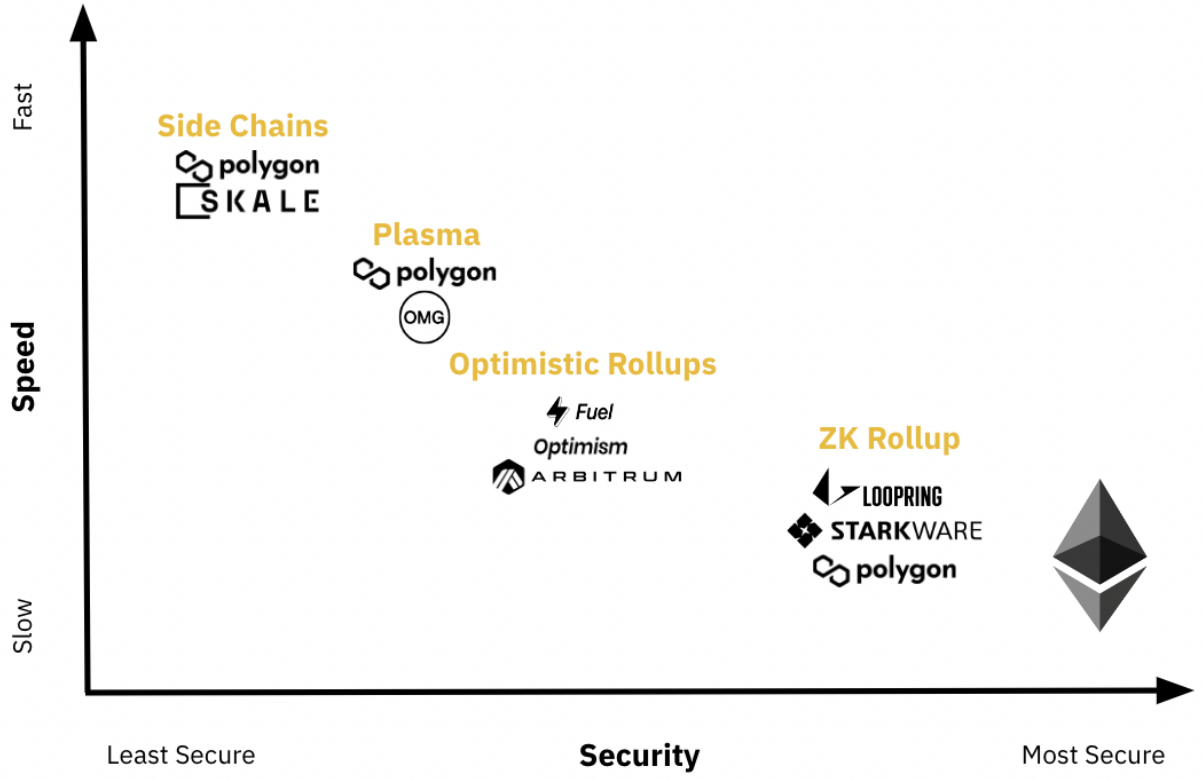


Source: Coin98, Binance Research

[1] Comments from Vitalik Buterin during ETHSeoul 2022

Comparing the different solutions, we can observe differences in speed and security. Optimistic and ZK-Rollups are seen as more secure than Side Chains and Plasma, though they are more limited in terms of speed and execution.

Figure 2: Layer 2 solutions differ in Security and Speed



Source: Binance Research

It is important to remember that even if sharding achieves its full scaling potential of offering a 64-fold improvement, it will still likely fall short of expected demand, indicating that we will see the continuous need of scaling solutions, be it Side Chains, Plasma, or a Rollup-centric approach. The Ethereum main chain will remain the settlement layer while scaling solutions will continue to manifest their place as an execution layer for the ecosystem.

The Ethereum main chain will remain the settlement layer while scaling solutions will continue to manifest their place as an execution layer for the ecosystem

Looking at the different characteristics of Layer 2 scaling solutions (including Side Chains), we can see that ZK-Rollups offer the overall best approach in terms of security, performance, usability, and other noteworthy aspects.

Figure 3: Characteristics of different scalability approaches

	State Channel	Side Chains	Plasma	Optimistic Rollup	Validium	ZK-Rollup
Security						
Liveness assumption	Yes	Bonded	Yes	Bonded	No	No
Mass exit assumption	No	No	Yes	No	No	No
Quorum of validators can freeze funds	No	Yes	No	No	Yes	No
Quorum of validators can confiscate funds No	No	Yes	No	No	Yes	No
Vulnerability to hot -wallet key exploits	Yes	Yes	Moderate	Moderate	Yes	Immune
Vulnerability to crypto-economic attacks	Moderate	Yes	Moderate	Moderate	Moderate	Immune
Cryptographic primitives	Standard	Standard	Standard	Standard	New	New
Performance						
Max throughput on ETH 2.0	1 - ∞ TPS*	10k + TPS*	1k - 9k TPS*	20k+ TPS*	20k+ TPS*	20k+ TPS*
Capital-efficient	No	Yes	Yes	Yes	Yes	Yes
Separate on-chain tx to open new account	Yes	No	No	No	No	No
Cost of tx	Very Low	Low	Very Low	Low	Low	Low
Usability						
Withdrawal time	1 confirmation	1 confirmation	1 week	1 week	1-10 min	1-10 min
Time to subjective finality	Instant	N/A	1 confirmation	1 confirmation	1-10 min	1-10 min
Client-side verification of subjective finality	Yes	N/A	No	No	Yes	Yes
Instant tx confirmations	Full	Bonded	Bonded	Bonded	Bonded	Bonded
Other aspects						
Smart contracts	Limited	Flexible	Limited	Flexible	Flexible	Flexible
EVM-bytecode portable	No	Yes	No	Yes	Yes	Yes
Native privacy options	Limited	No	No	No	Full	Full

Source: Binance Research, Matter Labs
**TPS are theoretical and can be subjective*

Market Update - The Future is zkEVM

The L2 landscape has been changing drastically this year with the introduction of Ethereum Virtual Machine ("EVM") zero-knowledge rollups (also referred to as zkEVM). Following the idea of functionality escape velocity, we can see how L2 will play an increasingly important role once L1s become strong enough. Thus, assuming that more economic activity will occur on L2s, it also becomes essential to increase dApp functionality through zkEVMs and other initiatives.

As such, assuming that Ethereum will continue its journey towards a settlement layer for security and dependability, we expect that L2s will increasingly accumulate revenues away from the Ethereum mainnet, thus introducing the potential for lower staking yields for validators, which in turn could introduce new risks to the security of the Ethereum network.

Comparing different L2s with the Ethereum mainnet shows us that this thesis is likely to play out due to their competitive nature in terms of transactions per second ("TPS") and fees.

Figure 4: Popular L2s vs. Ethereum and their current estimated Fees & TPS

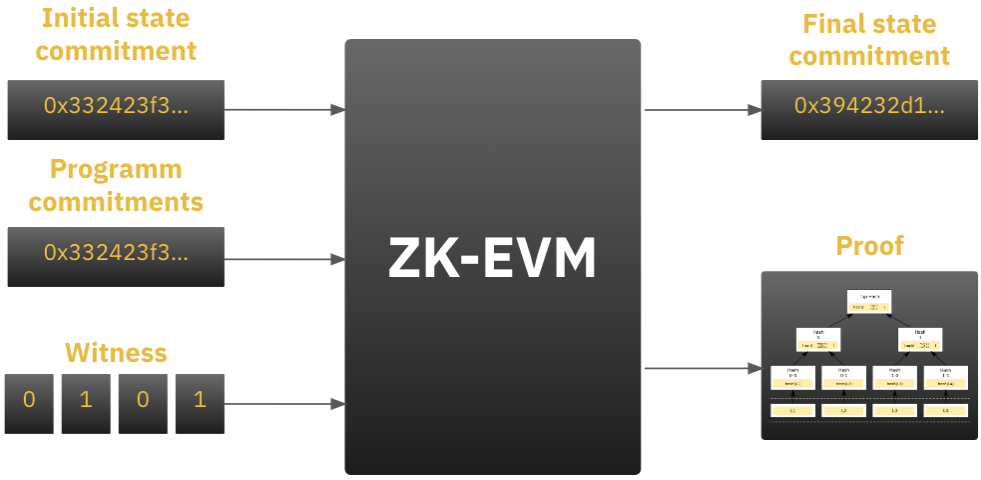
L1/L2	TVL (US$)	Fees (US$)	TPS*	Type
Ethereum	$31.94 B	1.30	15	Mainnet
Polygon PoS	$1.36 B	0.25	65,000	Side Chain
Arbitrum One	$2.42 B	0.25	4,500	Optimistic
Optimism	$1.45 B**	0.21	-	Optimistic
Metis	124 M	0.02	2000	Optimistic
zkSync	$53.77 M	0.05	2000	ZK-Rollup
Boba Network	$28.43 M***	0.10	-	Optimistic
Aztec	$2.68 M	0.39	300	ZK-Rollup
StarkNet	$1.43 M	-	700	ZK-Rollup
Polygon Hermez	$307 K	0.25	-	ZK-Rollup

Source: Binance Research, Company Websites, DeFiLama, L2Beat
** as of 7/10/2022*
***OP Token associated with Optimism accounts 12.5% of TVL*
****The BOBA and OMG token associated with Boba Network account for 65% of TVL*

With zkEVM, we are one step closer to bringing the full capabilities of the Ethereum mainnet to L2s, and multiple projects are working on their mainnets already. Polygon is estimated to launch its zkEVM mainnet in 2023, while zkSync 2.0 is a little less than 3 weeks away from the date of this publication. As a matter of fact, the zkSync 2.0 testnet just underwent a regenesis (Monday, October 10th), which will reset transaction history, token balances, and require developers to redeploy contracts. Scroll (which works with the Ethereum Foundation) recently announced a pre-alpha version of its testnet.

The introduction of zkEVM is also a major milestone in terms of coding language used and accessibility for developers. Currently, most ZK-Rollups are written in a low-level hexadecimal-based assembly language rather than Solidity, which introduces new levels of abstraction and complexity.

Figure 5: ZK-EVM functionality



Source: Binance Research

With EVM functionality, dApps can work natively on L2 rollups without having to worry about risks introduced to differences in the programming language of the L2 and Ethereum. Amongst zkEVMs, both Polygon and Scroll stand out due to their bytecode equivalence (rather than compatibility) which is why we expect to see both these products to see further adoption in the future. The bytecode equivalence allows both products to more seamlessly integrate and transition smart contracts. While the long-term aspiration is for zkEVMs to be on an Ethereum equivalent level, developments in this area are still underway. EVM equivalence is different from EVM compatibility because it creates less user friction, removing the need for any kind of modification or re-implementation of code.

Over the last few months, we have seen competition amongst zkEVMs increasing and we expect this trend to continue in the near future.

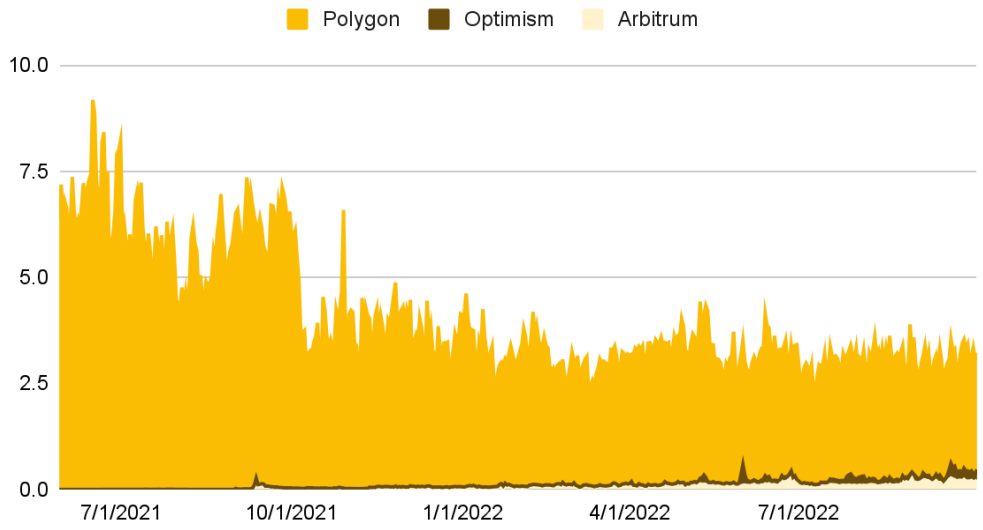
Competition amongst zkEVMs has been increasing and we expect this trend to continue in the near future

One thing seems clear, however - the likelihood that L2s will divert revenues away from the mainnet onto their own chains is only increasing, suggesting to us that the future is indeed on

Layer 2 solutions with Rollups taking a clear market leader position. If more users migrate to L2s, we could see staking yield on Ethereum being negatively affected, discouraging staking on the platform and thus introducing new risks due to a decrease in overall security.

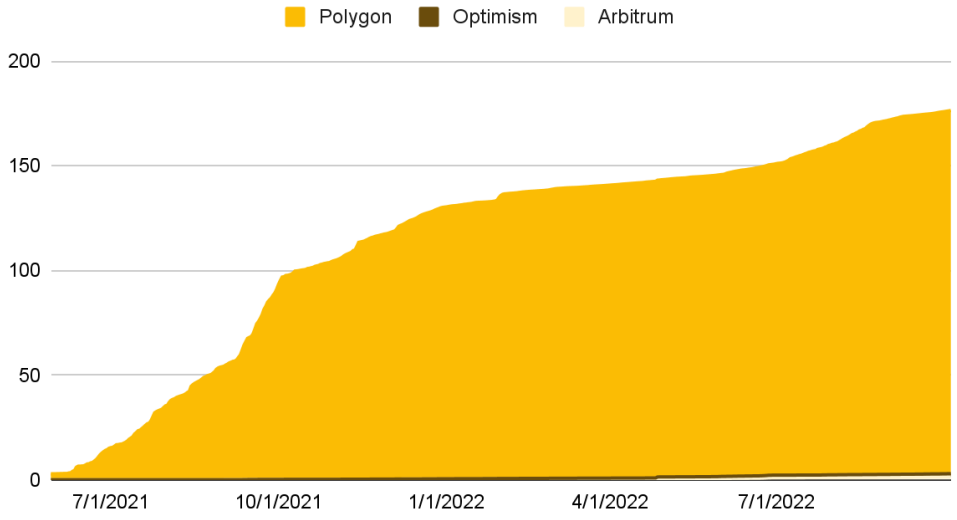
Looking at recent market trends a bit closer, we can see that despite the higher TVL (Figure 5) in Arbitrum, Polygon is leading in terms of total transactions per day (Figure 6) and in terms of cumulative addresses (Figure 7). This indicates that while fewer transactions and participants are on Optimism and Arbitrum, these participants have bigger wallets compared to the average Polygon user.

Figure 6: Transactions per Day (in millions) on Polygon, Optimism, Arbitrum



Source: Binance Research, arbiscan.io, optimistic.etherscan.io, polygonscan.com

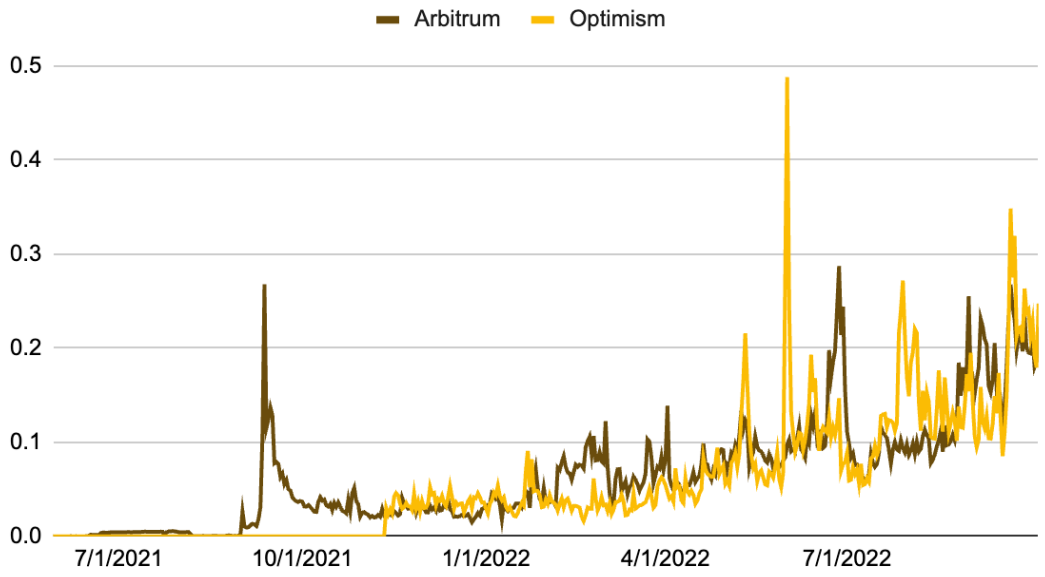
Figure 7: Cumulative addresses (in millions) on Polygon, Optimism, Arbitrum



Source: Binance Research, arbiscan.io, optimistic.etherscan.io, polygonscan.com

Just looking at the transaction on Arbitrum and Optimism (Figure 8) we can see both projects having a similar amount of transactions.

Figure 8: Transactions per Day (in millions) on (just) Optimism, Arbitrum, shows clear dominance



Source: Binance Research, arbiscan.io, optimistic.etherscan.io

This is manifesting our current observation that outside of zkEVM, we have also increased adoption and attention in the space of Optimistic Rollups. Within the space, Arbitrum stands out to us due to its recent release of Arbitrum Nitro.

In addition to that, Binance recently announced zkBNB, which brings zero-knowledge rollups to BNB Chain. Since both projects have gained recent attention, we will have a closer look at them in the upcoming segments of this report.

Arbitrum Update

Arbitrum is an L2 solution designed to boost the speed and scalability of Ethereum smart contracts while adding additional privacy features. Arbitrum further allows developers to run unmodified EVM contracts and transactions without compromising on layer 1 security.

Around a month ago, Arbitrum updated its platform to "Nitro," - introducing changes to the platform that bring along long-term improvements.

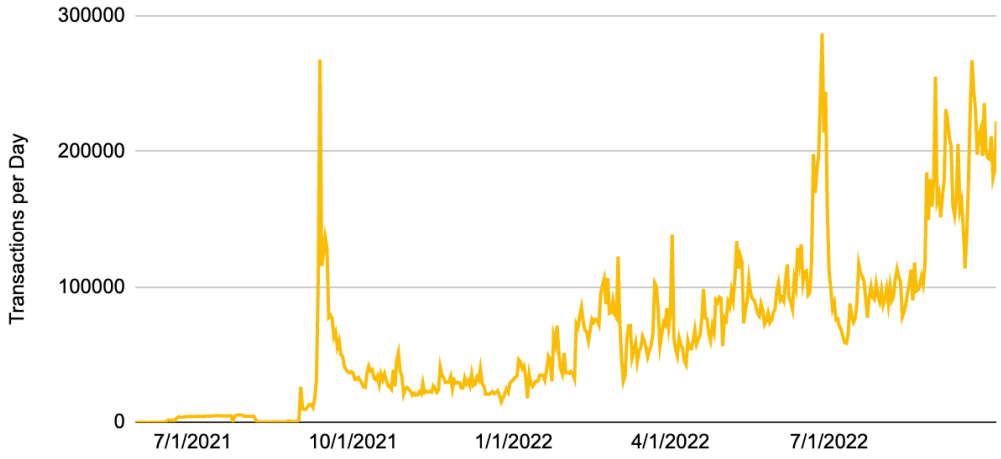
Key changes include:

- **Increased throughput -** 7x-10x higher compared to pre-Nitro
- **Advanced call data compression -** Driving down transaction costs on Arbitrum by reducing the amount of data posted to Ethereum
- **Ethereum L1 gas compatibility -** Pricing and accounting for EVM operations in line with Ethereum
- **Additional L1 interoperability -** Including tighter synchronization with L1 Block numbers
- **Safer retryable -** Eliminating the failure mode
- **Geth tracing -** Broader debugging support

With the introduction of Nitro, transactions are now handled in two stages. In the first stage, Nitro puts transactions into a sequence in which they will be processed. It then publishes the sequence and applies a deterministic state transition function to each transaction in sequence. For now, the Sequencer is a centralized component operated by Offchain Labs, but it will gradually transition into a distributed system as Arbitrum enters later stages. While the centralization tradeoff in pursuit of lower gas fees is understandable in the short term, we do urge the project to continue its focus on creating a decentralized system.

While the centralization tradeoff in pursuit of lower gas fees is understandable in the short term, we do urge the project to continue its focus on creating a decentralized system.

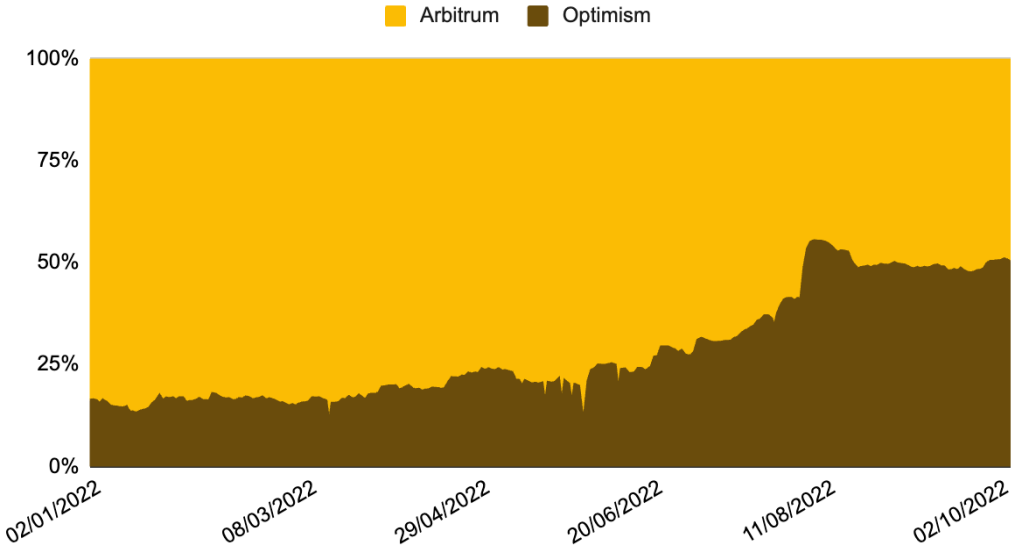
Figure 9: Daily Transactions on Arbitrum



Source: arbiscan.io, Binance Research

Just looking at transactions on Arbitrum, we can observe a positive trend since the beginning of the year. However, in order to see further adoption, we hope to see increased exchange listings. While Binance is currently supporting Arbitrum, most other exchanges do not. As such, the only way to enter Arbitrum for most is through an L1 native address. As such, we saw the Arbitrum Odyssey as a key event, driving further adoption (and we're looking forward to the continuation of it now that Nitro is introduced) - but expect that long-term growth will need to come from further integration of centralized exchanges ("CEX").

Figure 10: DeFi TVL on both Arbitrum and Optimism

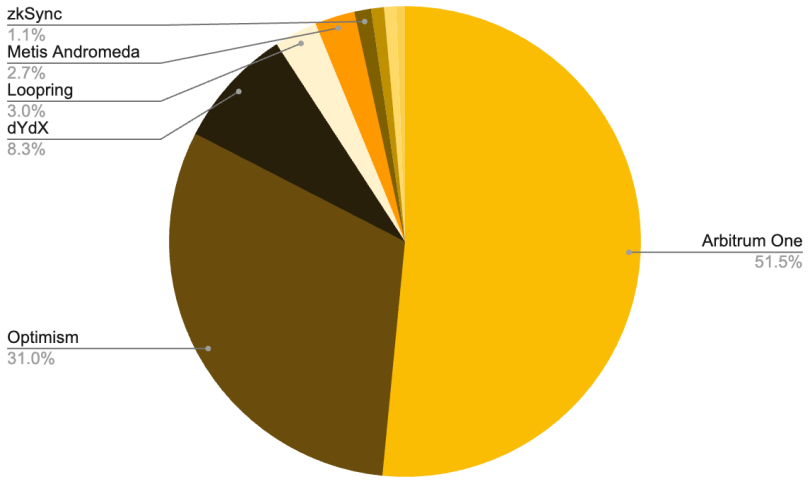


Source: Binance Research, DefiLama

While decentralized finance ("DeFi") TVL has been initially bigger on Arbitrum, the TVL is now almost equally split between Arbitrum and Optimism (a competing project focusing on

Optimistic Rollups). As such, despite recent developments and improvements to Arbitrum, we have not seen substantial market share gains. However, Arbitrum has more TVL on it overall when considering the token balances of Arbitrum.

Figure 11: TVL on both Arbitrum and alternative scaling solutions



Source: Binance Research, L2Beat

We can also observe a lot of change when looking closer at the Arbitrum ecosystem. GMX (recently listed on Binance) has gained substantial market share and reached a project dominance of 39.53%, according to DeFiLama. While GMX has seen a continuation in growth, projects like Curve and SushiSwap have been losing market share during the same period.

Not only did OpenSea announce its support for Arbitrum and its NFT ecosystem, but the combination of new infrastructure, incoming users with new NFTs from Odyssey, and a token launch create a perfect storm for the continued growth of Arbitrum.

We can conclude that while being in constant competition with Optimism and other scaling solutions, Arbitrum's ecosystem has still been on a consistent rise throughout the year. As a project, the newly introduced updates will introduce new competitiveness and contribute to what we're all looking for - increased adoption of Layer 2 scaling solutions, lower gas fees, and faster transactions. While centralization is still a key risk factor that we want to point out - Arbitrum is not alone with this as most L2s are, in one way or another, still mainly exposed to some form of centralization risk. While the beginning of the year had a strong emphasis on Bridges, we see that L2s found a revival in the last few months and will likely continue to play an important role for the rest of the year. That being said, Optimistic Rollups aren't the only solution out there, and we should have a closer look at the most recent zkBNB before concluding this report.

zkBNB Update

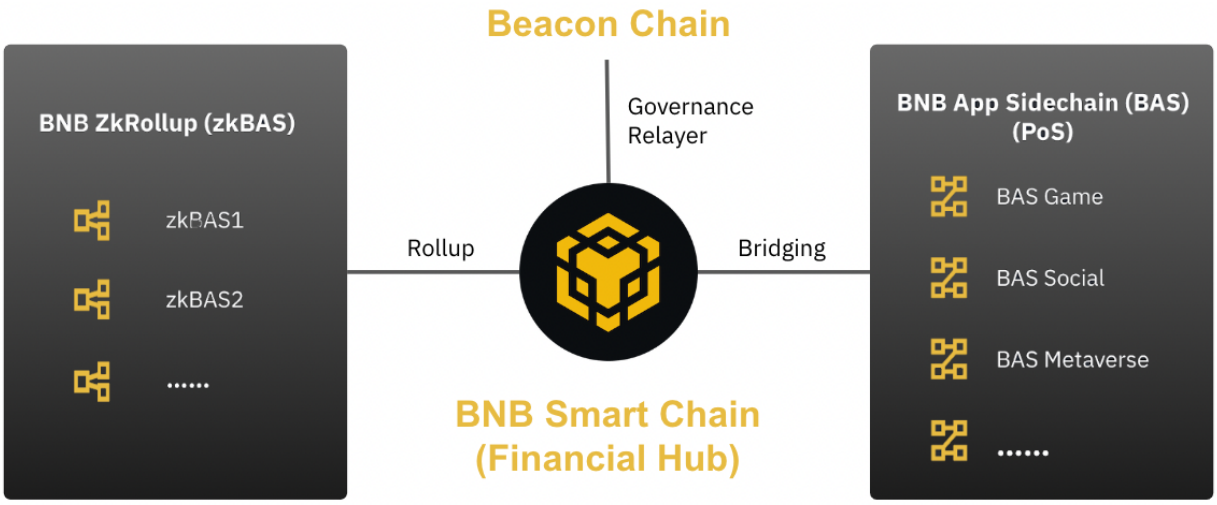
Leveraging the power of ZK-Rollups, BNB Smart Chain has introduced ZkBNB, bringing further scalability to the blockchain. In line with other ZK-Rollups, ZkBNB has the same capability to bundle hundreds of transactions into a single batch off-chain and generate cryptographic proof. These proofs can come in the form of a succinct non-interactive argument of knowledge ("SNARK"), which can prove the validity of every single transaction in the rollup block. SNARK ensures that all funds are held on the BNB Chain while computation and storage are performed on BNB Sidechains. Furthermore, thanks to the use of zk-SNARK proofs, ZkBNB shares the same security as that of BNB Smart Chain.

Thanks to the use of zk-SNARK proofs, ZkBNB shares the same security as that of BNB Smart Chain

Currently, ZkBNB implements the following features:

- **Same Security as that of L1 -** The ZkBNB shares the same security as BSC does. Due to the use of zkSNARK proofs, the security is guaranteed cryptographically
- **Seamless L1-L2 Communication -** BNB and BEP20/BEP721/BEP1155 tokens created on BSC or ZkBNB can flow freely between BSC and ZkBNB
- **Built-in instant AMM (Automated Market Maker) swap -** ZkBNB allows digital assets to be traded without permission and automatically by using built-in liquidity pools
- **Built-in NFT marketplace -** Developers can build marketplaces for crypto collectibles and NFTs (non-fungible tokens) out of the box on ZkBNB
- **Fast transaction speed and faster finality -** With performance a key priority for BNB Smart Chain, zkBNB puts up astonishing figures with an ability to support 100 million addresses and handle up to 10 thousand TPS
- **Gas Tokens -** The gas token on the ZkBNB can be either BEP20 or BNB, with fees up to 10x lower
- **"Full exit" on BSC -** If a user feels that his transactions are censored by ZkBNB, at any time, they can request a "full exit" operation to withdraw funds. This means users can withdraw funds at any time

Figure 10: ZkBNB Design



Source: Binance Research, BNB Chain

As ZkBNB offers straightforward token operations out-of-the-box, developers can now efficiently transfer BNB and other digital tokens (BEP20/BEP721/BEP1155) seamlessly between BSC and ZkBNB. Resulting in faster execution of lengthy transaction lists while ensuring a seamless undisturbed experience.

With the release of ZkBNB Testnet in November, the Mainnet is targeted to launch in Q1 of 2023. More about BNB Smart Chain's innovative projects can be looked at on BNB Chain's 2022 roadmap.

Conclusion

We see increased real-world adoption of cryptocurrencies, and with it comes a key challenge that needs to be addressed. Scaling current Layer 1 solutions to drive further adoption through scalability and low fees. With Ethereum 2.0, we have reached a key milestone in terms of blockchain consensus mechanism and opened the door for further improvements. Sharding, once it achieves its full scaling potential, can offer a 64-fold improvement. However, in order to drive further growth, this is likely not enough, and L2s will likely be at the center of attention for Ethereum due to the numerous improvements that they bring to the mainnet.

Sooner or later, L2s will be able to offer faster transactions and lower fees to the masses and most likely drive transactions from Ethereum onto their own chains bringing new challenges to the system. We expect that the idea of functionality escape velocity will lead to L2 playing an increasingly important role once L1s become strong enough. Thus, assuming that more economic activity will occur on L2s. As such, it is also possible that the rise of L2s will drive further growth in the DeFi space.

With a similar focus on bridges, users will be able to benefit from higher blockchain interoperability in the future. While L2s still see limitations in terms of interoperability, this could change in the coming years. Consequently, L2 scaling solutions will play a key role in building a multichain world. In the short term, bridges could be at the forefront of development, however. We expect that the majority of applications on Ethereum will likely move to L2, further underlying the need for secure bridges. We consequently expect bridges between L2s and centralized exchanges to emerge, as well as bridges between various L2s.

Despite the growing importance of Optimistic Rollups, we are ultimately convinced that ZK-Rollups, and especially zkEVM, will play a key role for the future of Ethereum. That being said - Optimistic Rollups have their justification and place in the Ecosystem. As such, developers will likely still be fractured between optimistic and ZK-Rollups throughout 2022 and 2023.

Optimistic rollups will likely see a further rise in popularity until zkEVMs are strong enough to compete. We're convinced that ZK-Rollups, using validity proof, offer long-term benefits due to fewer limitations compared to Optimistic rollups. Another key trend will be the development of dApps that reside and operate natively on L2 platforms - a trend we yet have to play out.

We're overall excited about the space and welcome the developments we have seen over the last few months and expect more to come in the remaining parts of this year and 2023.

Closing Thoughts

In order to drive further growth, L2s will likely be at the center of attention for Ethereum due to the numerous improvements that they bring to the mainnet. We're overall excited about the space and welcome the developments we have seen over the last few months and expect more to come in the remaining parts of this year and 2023.

About Binance Research

Binance Research is the research arm of Binance, the world's leading cryptocurrency exchange. The team is committed to delivering objective, independent, and comprehensive analysis and aims to be the thought leader in the crypto space. Our analysts publish insightful thought pieces regularly on topics related but not limited to, the crypto ecosystem, blockchain technologies, and the latest market themes.

Stefan Piech, Macro Researcher

Stefan is currently working for Binance as Macro Researcher. Prior to joining Binance, he worked as an Equity Portfolio Manager at Cape Capital, a Swiss Family Office, and as an Equity Research Analyst for BlackRock's European and UK Hedge Fund. He has prior experience in both Private Equity and Venture Capital. Stefan started his career as Government Official for the District Government Muenster. Stefan has been involved in Crypto since 2019.

Read more

https://research.binance.com/en/analysis

Share your feedback

https://tinyurl.com/bnresearchfeedback

Table of Contents

Key Takeaways

- Once L1s are strong enough, the majority of transactions can take place on L2s, allowing for further scalability and faster transactions with lower gas cost
- Comparing the different solutions, we can observe differences in speed and security. Optimistic and ZK-Rollups are seen as more secure than Side Chains and Plasma, though they are more limited in terms of speed and execution
- Looking at the different characteristics of Layer 2 scaling solutions (including Side Chains), we believe that ZK-Rollups offer the best overall approach in terms of security, performance, usability, and other noteworthy aspects
- The Ethereum blockchain will remain the settlement layer, while scaling solutions will continue to manifest their place as execution layers for the growing dApp ecosystem
- The introduction of zkEVM is a major milestone in terms of coding language usability and accessibility for developers. Currently, most ZK-Rollups are written in a low-level hexadecimal-based assembly language rather than Solidity, which introduces new levels of abstraction and complexity
- While Arbitrum's centralization tradeoff in pursuit of lower gas fees is understandable in the short term, we urge the project to continue its focus on creating a decentralized system
- Leveraging the power of ZK-Rollups, BNB Smart Chain has introduced zkBNB, bringing further scalability to the blockchain
- Optimistic rollups will likely see a further rise in popularity until zkEVMs are strong enough to compete. ZK-Rollups, using validity proof, offer long-term benefits due to fewer limitations compared to Optimistic rollups
- As of now, the majority of applications on Ethereum today will likely move to L2, further underlying the need for secure bridges. We consequently expect more bridges between L2s and centralized exchanges to emerge, as well as bridges between various L2s

Demystifying Layer 2 Scaling

Over the last years, we have seen the blockchain ecosystem growing at an exponential rate. This brought to attention the old and fundamental concerns that existing Layer 1 ("L1") platforms are limited in their scalability due to low transaction speeds.

The solution to this that found the most traction over the following months was Layer 2 ("L2") scaling which brought along the layer separation vision. **The goal of this layer separation is to build out L1s as foundational layers for security and dependability while moving rapid iterations and actions onto L2s.** Once L1s are strong enough, the majority of transactions can take place on L2s, allowing for further scalability and faster transactions with lower gas costs.

Once L1s are strong enough, the majority of transactions can take place on L2s, allowing for further scalability and faster transactions with lower gas cost

When building Layer 2 scaling solutions, it is important that they inherit the underlying security of the main chain. This is one of the elements differentiating them to sidechains, where validators secure the chain. The two main L2 solutions that have seen traction in the last few months are **zero-knowledge** ("zk") and **optimistic** rollups. While we assume some basic understanding, we'll still go over some of the basics first.

❖ Zero-Knowledge Rollups

Zero-knowledge rollups - simply put - are bundles of data that are processed and computed off-chain. This off-chain computation reduces the amount of data that has to be posted to the blockchain. They produce validity proofs to prove the correctness of their changes. The validity proof is a cryptographic assurance that the state change proposed by the rollup is really the result of executing the given batch of transactions. This means that ZK-rollups only need to provide validity proofs to finalize transactions on Ethereum, instead of posting all transaction data on-chain. Important data relevant to the smart contracts are requested less frequently than in L1 blockchains. This saves a large amount of processing power, and less of the blockchain capacity is used for transaction validation. Gas fees decrease, as a result, making transactions faster and cheaper.

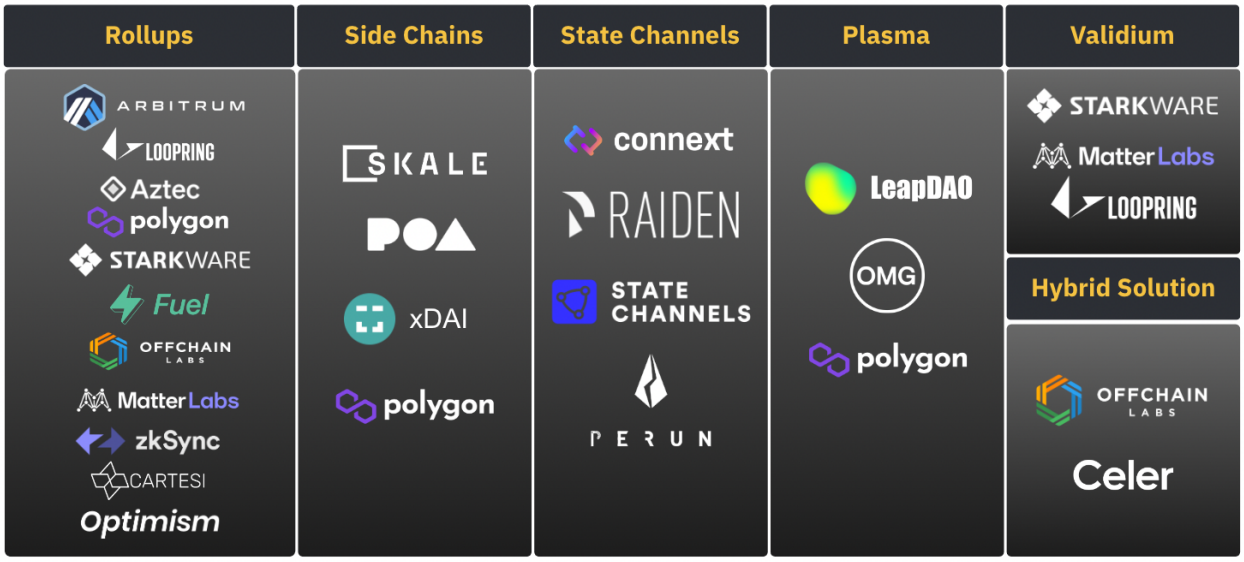
❖ Optimistic Rollups

Optimistic rollup operators bundle multiple off-chain transactions together in large batches before submitting them to Ethereum. This approach enables spreading fixed costs across multiple transactions in each batch, reducing fees for end-user. Data aggregators will compute Merkle roots to achieve increased transaction speeds. However, they offer less throughput than Plasma and ZK-Rollups. Optimistic rollups are considered "optimistic" because they assume off-chain transactions are valid and don't publish proofs of validity for transaction batches posted on-chain. This separates optimistic rollups from zero-knowledge rollups. Optimistic rollups have to rely on external validators to check the Merkle roots before the state can be updated.

Vitalik Buterin called Rollups his favorite Layer 2 solution[1]

While there are other scaling solutions worth mentioning, like Plasma, which uses child-chains to assist the main chain in verification, Polkadot's parachains, Bitcoin's Lightning Network, Sidechains, Validium, and State Channels, we will focus exclusively on Rollups in this report due to their increased adoption and relative importance compared to alternative solutions.

Figure 1: Selection of Layer 2 Scaling Solutions on Ethereum indicate a focus on Rollups

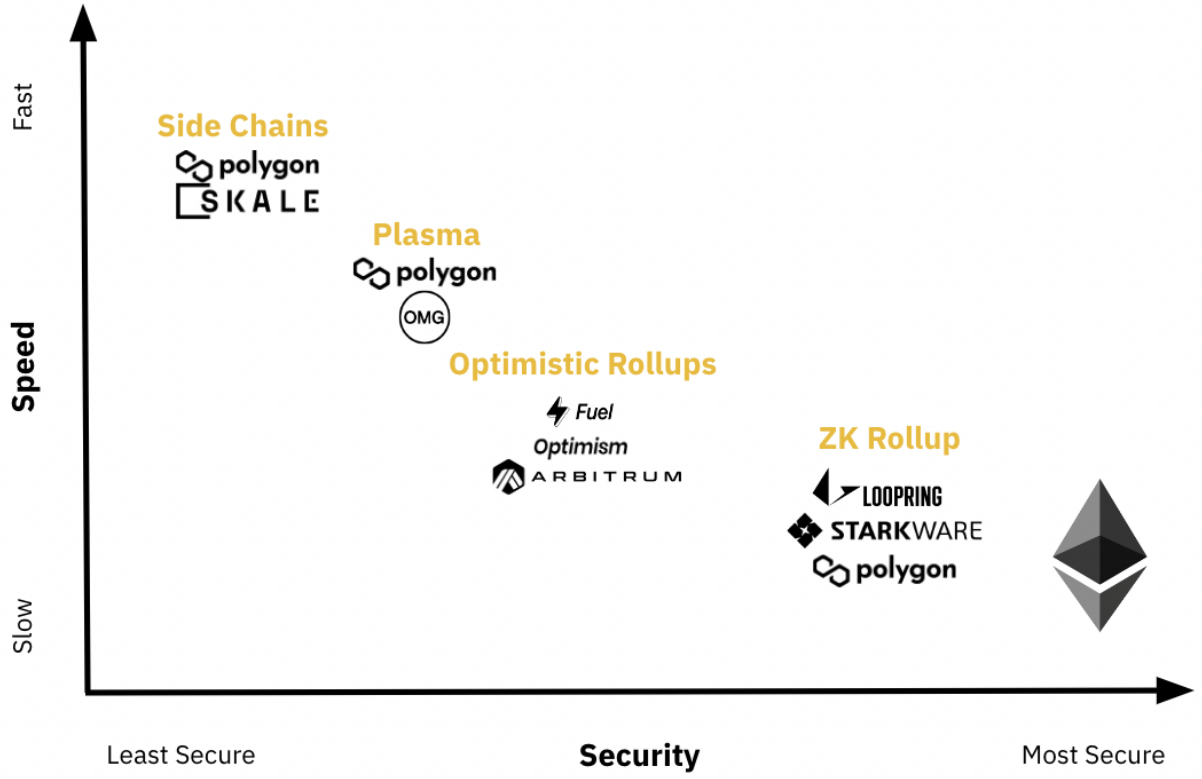


Source: Coin98, Binance Research

[1] Comments from Vitalik Buterin during ETHSeoul 2022

Comparing the different solutions, we can observe differences in speed and security. Optimistic and ZK-Rollups are seen as more secure than Side Chains and Plasma, though they are more limited in terms of speed and execution.

Figure 2: Layer 2 solutions differ in Security and Speed



Source: Binance Research

It is important to remember that even if sharding achieves its full scaling potential of offering a 64-fold improvement, it will still likely fall short of expected demand, indicating that we will see the continuous need of scaling solutions, be it Side Chains, Plasma, or a Rollup-centric approach. The Ethereum main chain will remain the settlement layer while scaling solutions will continue to manifest their place as an execution layer for the ecosystem.

The Ethereum main chain will remain the settlement layer while scaling solutions will continue to manifest their place as an execution layer for the ecosystem

Looking at the different characteristics of Layer 2 scaling solutions (including Side Chains), we can see that ZK-Rollups offer the overall best approach in terms of security, performance, usability, and other noteworthy aspects.

Figure 3: Characteristics of different scalability approaches

	State Channel	Side Chains	Plasma	Optimistic Rollup	Validium	ZK-Rollup
Security						
Liveness assumption	Yes	Bonded	Yes	Bonded	No	No
Mass exit assumption	No	No	Yes	No	No	No
Quorum of validators can freeze funds	No	Yes	No	No	Yes	No
Quorum of validators can confiscate funds No	No	Yes	No	No	Yes	No
Vulnerability to hot -wallet key exploits	Yes	Yes	Moderate	Moderate	Yes	Immune
Vulnerability to crypto-economic attacks	Moderate	Yes	Moderate	Moderate	Moderate	Immune
Cryptographic primitives	Standard	Standard	Standard	Standard	New	New
Performance						
Max throughput on ETH 2.0	1 - ∞ TPS*	10k + TPS*	1k - 9k TPS*	20k+ TPS*	20k+ TPS*	20k+ TPS*
Capital-efficient	No	Yes	Yes	Yes	Yes	Yes
Separate on-chain tx to open new account	Yes	No	No	No	No	No
Cost of tx	Very Low	Low	Very Low	Low	Low	Low
Usability						
Withdrawal time	1 confirmation	1 confirmation	1 week	1 week	1-10 min	1-10 min
Time to subjective finality	Instant	N/A	1 confirmation	1 confirmation	1-10 min	1-10 min
Client-side verification of subjective finality	Yes	N/A	No	No	Yes	Yes
Instant tx confirmations	Full	Bonded	Bonded	Bonded	Bonded	Bonded
Other aspects						
Smart contracts	Limited	Flexible	Limited	Flexible	Flexible	Flexible
EVM-bytecode portable	No	Yes	No	Yes	Yes	Yes
Native privacy options	Limited	No	No	No	Full	Full

Source: Binance Research, Matter Labs
**TPS are theoretical and can be subjective*

Market Update - The Future is zkEVM

The L2 landscape has been changing drastically this year with the introduction of Ethereum Virtual Machine ("EVM") zero-knowledge rollups (also referred to as zkEVM). Following the idea of functionality escape velocity, we can see how L2 will play an increasingly important role once L1s become strong enough. Thus, assuming that more economic activity will occur on L2s, it also becomes essential to increase dApp functionality through zkEVMs and other initiatives.

As such, assuming that Ethereum will continue its journey towards a settlement layer for security and dependability, we expect that L2s will increasingly accumulate revenues away from the Ethereum mainnet, thus introducing the potential for lower staking yields for validators, which in turn could introduce new risks to the security of the Ethereum network.

Comparing different L2s with the Ethereum mainnet shows us that this thesis is likely to play out due to their competitive nature in terms of transactions per second ("TPS") and fees.

Figure 4: Popular L2s vs. Ethereum and their current estimated Fees & TPS

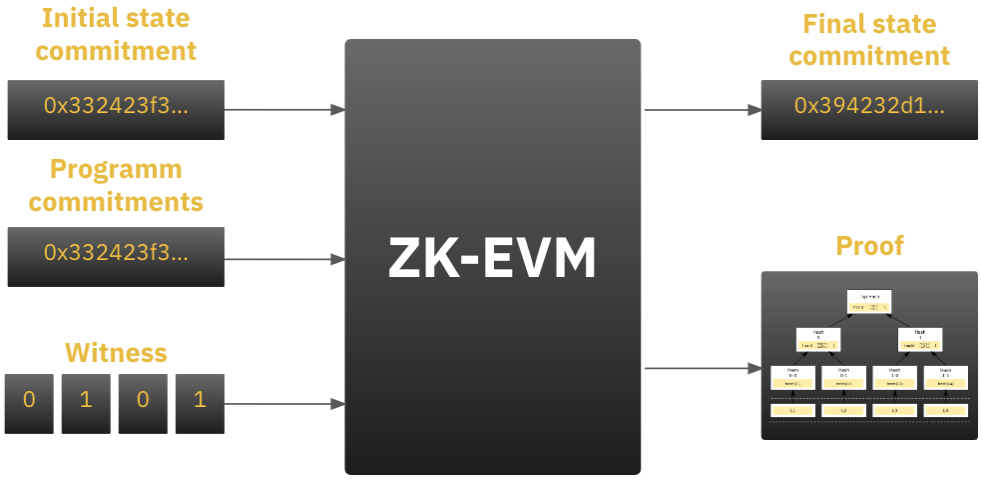
L1/L2	TVL (US$)	Fees (US$)	TPS*	Type
Ethereum	$31.94 B	1.30	15	Mainnet
Polygon PoS	$1.36 B	0.25	65,000	Side Chain
Arbitrum One	$2.42 B	0.25	4,500	Optimistic
Optimism	$1.45 B**	0.21	-	Optimistic
Metis	124 M	0.02	2000	Optimistic
zkSync	$53.77 M	0.05	2000	ZK-Rollup
Boba Network	$28.43 M***	0.10	-	Optimistic
Aztec	$2.68 M	0.39	300	ZK-Rollup
StarkNet	$1.43 M	-	700	ZK-Rollup
Polygon Hermez	$307 K	0.25	-	ZK-Rollup

Source: Binance Research, Company Websites, DeFiLama, L2Beat
** as of 7/10/2022*
***OP Token associated with Optimism accounts 12.5% of TVL*
****The BOBA and OMG token associated with Boba Network account for 65% of TVL*

With zkEVM, we are one step closer to bringing the full capabilities of the Ethereum mainnet to L2s, and multiple projects are working on their mainnets already. Polygon is estimated to launch its zkEVM mainnet in 2023, while zkSync 2.0 is a little less than 3 weeks away from the date of this publication. As a matter of fact, the zkSync 2.0 testnet just underwent a regenesis (Monday, October 10th), which will reset transaction history, token balances, and require developers to redeploy contracts. Scroll (which works with the Ethereum Foundation) recently announced a pre-alpha version of its testnet.

The introduction of zkEVM is also a major milestone in terms of coding language used and accessibility for developers. Currently, most ZK-Rollups are written in a low-level hexadecimal-based assembly language rather than Solidity, which introduces new levels of abstraction and complexity.

Figure 5: ZK-EVM functionality



Source: Binance Research

With EVM functionality, dApps can work natively on L2 rollups without having to worry about risks introduced to differences in the programming language of the L2 and Ethereum. Amongst zkEVMs, both Polygon and Scroll stand out due to their bytecode equivalence (rather than compatibility) which is why we expect to see both these products to see further adoption in the future. The bytecode equivalence allows both products to more seamlessly integrate and transition smart contracts. While the long-term aspiration is for zkEVMs to be on an Ethereum equivalent level, developments in this area are still underway. EVM equivalence is different from EVM compatibility because it creates less user friction, removing the need for any kind of modification or re-implementation of code.

Over the last few months, we have seen competition amongst zkEVMs increasing and we expect this trend to continue in the near future.

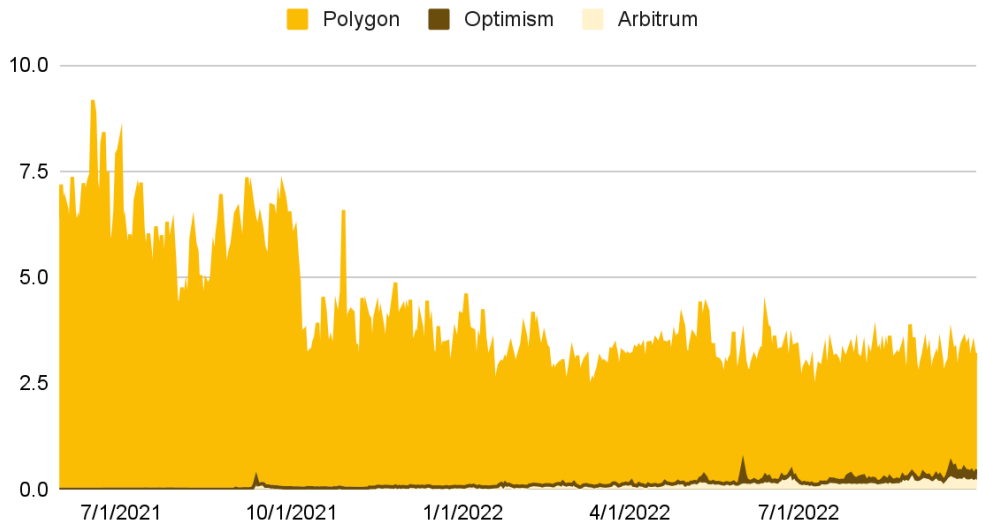
Competition amongst zkEVMs has been increasing and we expect this trend to continue in the near future

One thing seems clear, however - the likelihood that L2s will divert revenues away from the mainnet onto their own chains is only increasing, suggesting to us that the future is indeed on

Layer 2 solutions with Rollups taking a clear market leader position. If more users migrate to L2s, we could see staking yield on Ethereum being negatively affected, discouraging staking on the platform and thus introducing new risks due to a decrease in overall security.

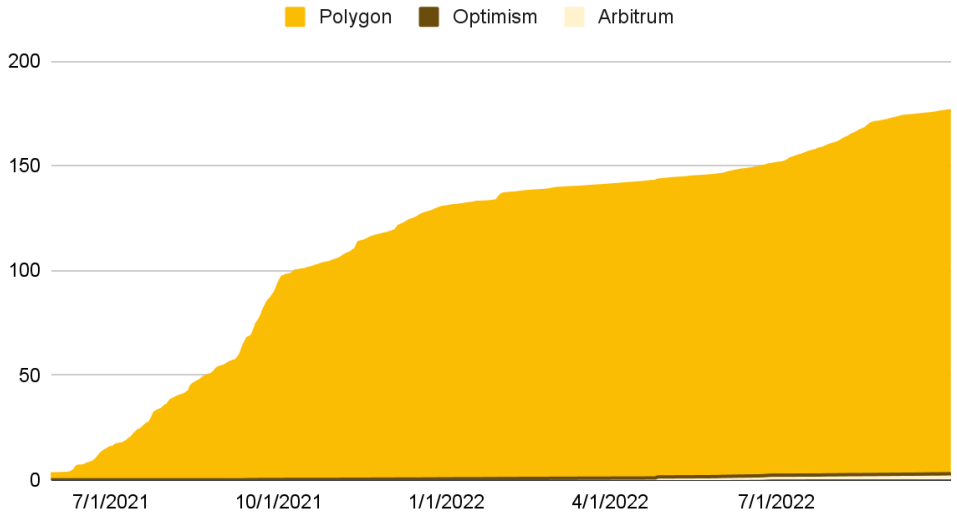
Looking at recent market trends a bit closer, we can see that despite the higher TVL (Figure 5) in Arbitrum, Polygon is leading in terms of total transactions per day (Figure 6) and in terms of cumulative addresses (Figure 7). This indicates that while fewer transactions and participants are on Optimism and Arbitrum, these participants have bigger wallets compared to the average Polygon user.

Figure 6: Transactions per Day (in millions) on Polygon, Optimism, Arbitrum



Source: Binance Research, arbiscan.io, optimistic.etherscan.io, polygonscan.com

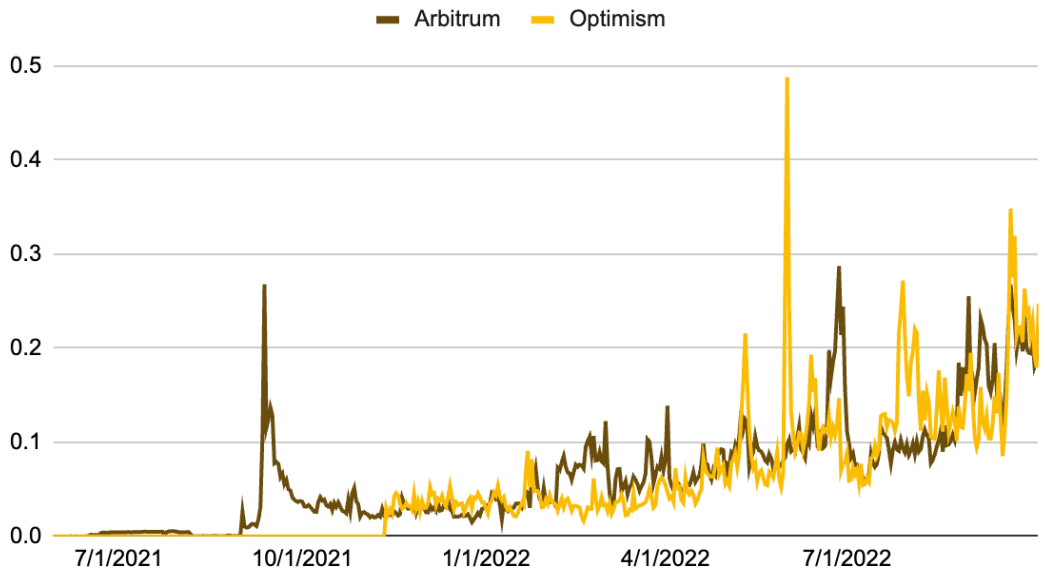
Figure 7: Cumulative addresses (in millions) on Polygon, Optimism, Arbitrum



Source: Binance Research, arbiscan.io, optimistic.etherscan.io, polygonscan.com

Just looking at the transaction on Arbitrum and Optimism (Figure 8) we can see both projects having a similar amount of transactions.

Figure 8: Transactions per Day (in millions) on (just) Optimism, Arbitrum, shows clear dominance



Source: Binance Research, arbiscan.io, optimistic.etherscan.io

This is manifesting our current observation that outside of zkEVM, we have also increased adoption and attention in the space of Optimistic Rollups. Within the space, Arbitrum stands out to us due to its recent release of Arbitrum Nitro.

In addition to that, Binance recently announced zkBNB, which brings zero-knowledge rollups to BNB Chain. Since both projects have gained recent attention, we will have a closer look at them in the upcoming segments of this report.

Arbitrum Update

Arbitrum is an L2 solution designed to boost the speed and scalability of Ethereum smart contracts while adding additional privacy features. Arbitrum further allows developers to run unmodified EVM contracts and transactions without compromising on layer 1 security.

Around a month ago, Arbitrum updated its platform to "Nitro," - introducing changes to the platform that bring along long-term improvements.

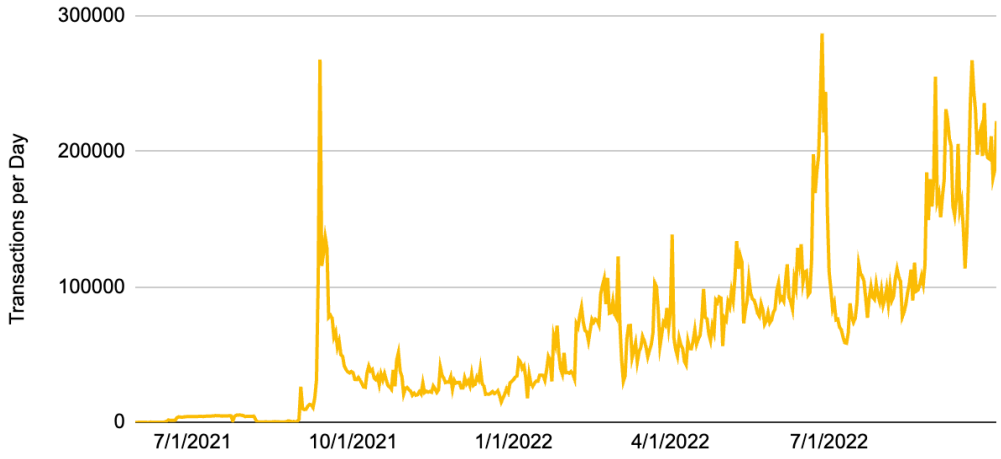
Key changes include:

- **Increased throughput -** 7x-10x higher compared to pre-Nitro
- **Advanced call data compression -** Driving down transaction costs on Arbitrum by reducing the amount of data posted to Ethereum
- **Ethereum L1 gas compatibility -** Pricing and accounting for EVM operations in line with Ethereum
- **Additional L1 interoperability -** Including tighter synchronization with L1 Block numbers
- **Safer retryable -** Eliminating the failure mode
- **Geth tracing -** Broader debugging support

With the introduction of Nitro, transactions are now handled in two stages. In the first stage, Nitro puts transactions into a sequence in which they will be processed. It then publishes the sequence and applies a deterministic state transition function to each transaction in sequence. For now, the Sequencer is a centralized component operated by Offchain Labs, but it will gradually transition into a distributed system as Arbitrum enters later stages. While the centralization tradeoff in pursuit of lower gas fees is understandable in the short term, we do urge the project to continue its focus on creating a decentralized system.

While the centralization tradeoff in pursuit of lower gas fees is understandable in the short term, we do urge the project to continue its focus on creating a decentralized system.

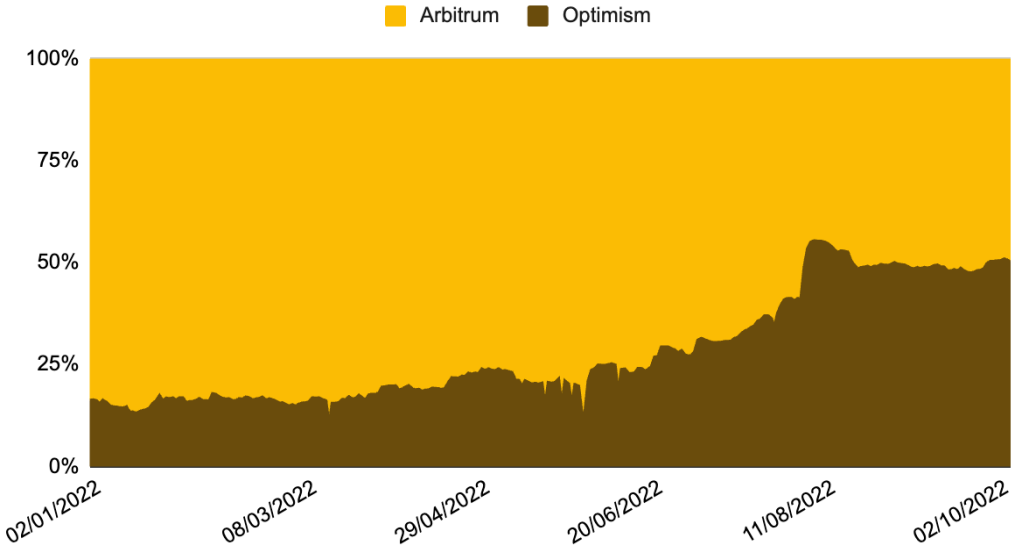
Figure 9: Daily Transactions on Arbitrum



Source: arbiscan.io, Binance Research

Just looking at transactions on Arbitrum, we can observe a positive trend since the beginning of the year. However, in order to see further adoption, we hope to see increased exchange listings. While Binance is currently supporting Arbitrum, most other exchanges do not. As such, the only way to enter Arbitrum for most is through an L1 native address. As such, we saw the Arbitrum Odyssey as a key event, driving further adoption (and we're looking forward to the continuation of it now that Nitro is introduced) - but expect that long-term growth will need to come from further integration of centralized exchanges ("CEX").

Figure 10: DeFi TVL on both Arbitrum and Optimism

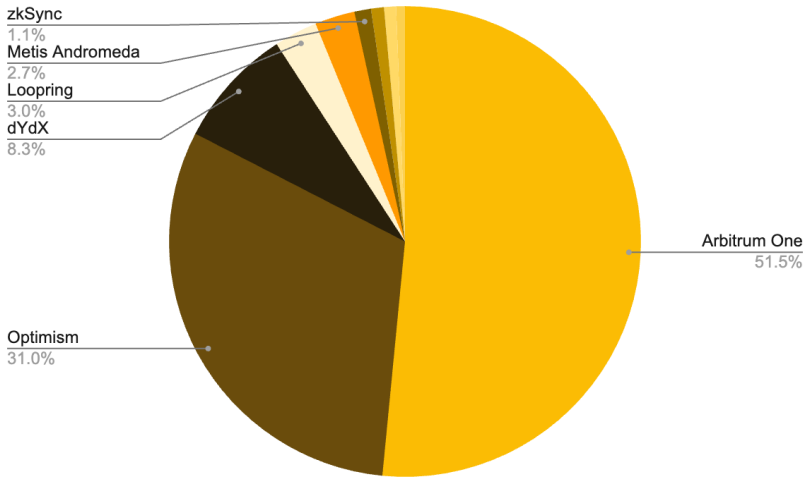


Source: Binance Research, DefiLama

While decentralized finance ("DeFi") TVL has been initially bigger on Arbitrum, the TVL is now almost equally split between Arbitrum and Optimism (a competing project focusing on

Optimistic Rollups). As such, despite recent developments and improvements to Arbitrum, we have not seen substantial market share gains. However, Arbitrum has more TVL on it overall when considering the token balances of Arbitrum.

Figure 11: TVL on both Arbitrum and alternative scaling solutions



Source: Binance Research, L2Beat

We can also observe a lot of change when looking closer at the Arbitrum ecosystem. GMX (recently listed on Binance) has gained substantial market share and reached a project dominance of 39.53%, according to DeFiLama. While GMX has seen a continuation in growth, projects like Curve and SushiSwap have been losing market share during the same period.

Not only did OpenSea announce its support for Arbitrum and its NFT ecosystem, but the combination of new infrastructure, incoming users with new NFTs from Odyssey, and a rumored token launch create a perfect storm for the continued growth of Arbitrum.

We can conclude that while being in constant competition with Optimism and other scaling solutions, Arbitrum's ecosystem has still been on a consistent rise throughout the year. As a project, the newly introduced updates will introduce new competitiveness and contribute to what we're all looking for - increased adoption of Layer 2 scaling solutions, lower gas fees, and faster transactions. While centralization is still a key risk factor that we want to point out - Arbitrum is not alone with this as most L2s are, in one way or another, still mainly exposed to some form of centralization risk. While the beginning of the year had a strong emphasis on Bridges, we see that L2s found a revival in the last few months and will likely continue to play an important role for the rest of the year. That being said, Optimistic Rollups aren't the only solution out there, and we should have a closer look at the most recent zkBNB before concluding this report.

zkBNB Update

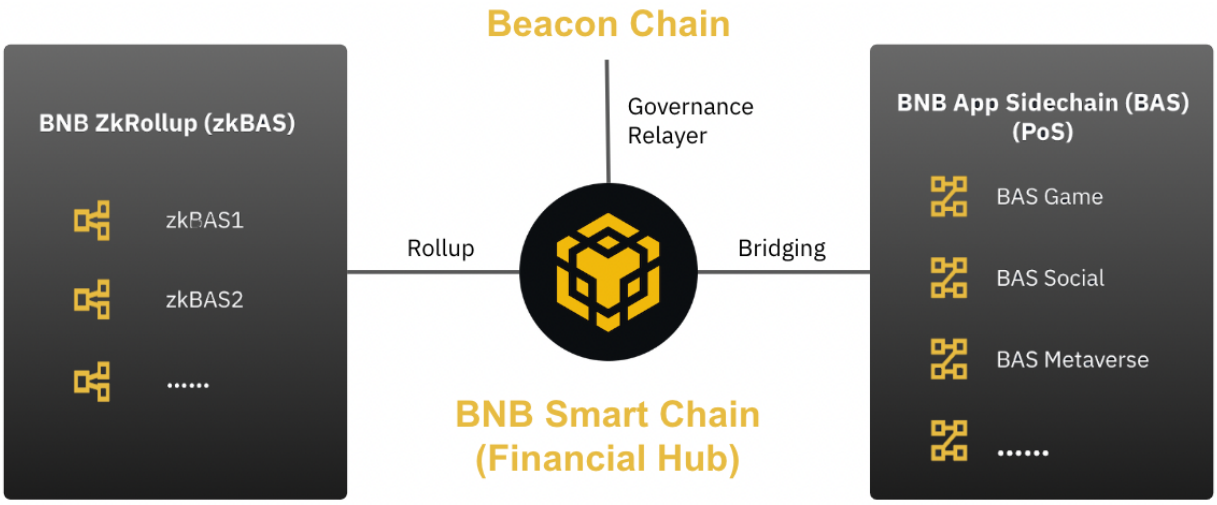
Leveraging the power of ZK-Rollups, BNB Smart Chain has introduced ZkBNB, bringing further scalability to the blockchain. In line with other ZK-Rollups, ZkBNB has the same capability to bundle hundreds of transactions into a single batch off-chain and generate cryptographic proof. These proofs can come in the form of a succinct non-interactive argument of knowledge ("SNARK"), which can prove the validity of every single transaction in the rollup block. SNARK ensures that all funds are held on the BNB Chain while computation and storage are performed on BNB Sidechains. Furthermore, thanks to the use of zk-SNARK proofs, ZkBNB shares the same security as that of BNB Smart Chain.

Thanks to the use of zk-SNARK proofs, ZkBNB shares the same security as that of BNB Smart Chain

Currently, ZkBNB implements the following features:

- **Same Security as that of L1 -** The ZkBNB shares the same security as BSC does. Due to the use of zkSNARK proofs, the security is guaranteed cryptographically
- **Seamless L1-L2 Communication -** BNB and BEP20/BEP721/BEP1155 tokens created on BSC or ZkBNB can flow freely between BSC and ZkBNB
- **Built-in instant AMM (Automated Market Maker) swap -** ZkBNB allows digital assets to be traded without permission and automatically by using built-in liquidity pools
- **Built-in NFT marketplace -** Developers can build marketplaces for crypto collectibles and NFTs (non-fungible tokens) out of the box on ZkBNB
- **Fast transaction speed and faster finality -** With performance a key priority for BNB Smart Chain, zkBNB puts up astonishing figures with an ability to support 100 million addresses and handle up to 10 thousand TPS
- **Gas Tokens -** The gas token on the ZkBNB can be either BEP20 or BNB, with fees up to 10x lower
- **"Full exit" on BSC -** If a user feels that his transactions are censored by ZkBNB, at any time, they can request a "full exit" operation to withdraw funds. This means users can withdraw funds at any time

Figure 10: ZkBNB Design



Source: Binance Research, BNB Chain

As ZkBNB offers straightforward token operations out-of-the-box, developers can now efficiently transfer BNB and other digital tokens (BEP20/BEP721/BEP1155) seamlessly between BSC and ZkBNB. Resulting in faster execution of lengthy transaction lists while ensuring a seamless undisturbed experience.

With the release of ZkBNB Testnet in November, the Mainnet is targeted to launch in Q1 of 2023. More about BNB Smart Chain's innovative projects can be looked at on BNB Chain's 2022 roadmap.

Conclusion

We see increased real-world adoption of cryptocurrencies, and with it comes a key challenge that needs to be addressed. Scaling current Layer 1 solutions to drive further adoption through scalability and low fees. With Ethereum 2.0, we have reached a key milestone in terms of blockchain consensus mechanism and opened the door for further improvements. Sharding, once it achieves its full scaling potential, can offer a 64-fold improvement. However, in order to drive further growth, this is likely not enough, and L2s will likely be at the center of attention for Ethereum due to the numerous improvements that they bring to the mainnet.

Sooner or later, L2s will be able to offer faster transactions and lower fees to the masses and most likely drive transactions from Ethereum onto their own chains bringing new challenges to the system. We expect that the idea of functionality escape velocity will lead to L2 playing an increasingly important role once L1s become strong enough. Thus, assuming that more economic activity will occur on L2s. As such, it is also possible that the rise of L2s will drive further growth in the DeFi space.

With a similar focus on bridges, users will be able to benefit from higher blockchain interoperability in the future. While L2s still see limitations in terms of interoperability, this could change in the coming years. Consequently, L2 scaling solutions will play a key role in building a multichain world. In the short term, bridges could be at the forefront of development, however. We expect that the majority of applications on Ethereum will likely move to L2, further underlying the need for secure bridges. We consequently expect bridges between L2s and centralized exchanges to emerge, as well as bridges between various L2s.

Despite the growing importance of Optimistic Rollups, we are ultimately convinced that ZK-Rollups, and especially zkEVM, will play a key role for the future of Ethereum. That being said - Optimistic Rollups have their justification and place in the Ecosystem. As such, developers will likely still be fractured between optimistic and ZK-Rollups throughout 2022 and 2023.

Optimistic rollups will likely see a further rise in popularity until zkEVMs are strong enough to compete. We're convinced that ZK-Rollups, using validity proof, offer long-term benefits due to fewer limitations compared to Optimistic rollups. Another key trend will be the development of dApps that reside and operate natively on L2 platforms - a trend we yet have to play out.

We're overall excited about the space and welcome the developments we have seen over the last few months and expect more to come in the remaining parts of this year and 2023.

Closing Thoughts

In order to drive further growth, L2s will likely be at the center of attention for Ethereum due to the numerous improvements that they bring to the mainnet. We're overall excited about the space and welcome the developments we have seen over the last few months and expect more to come in the remaining parts of this year and 2023.

About Binance Research

Binance Research is the research arm of Binance, the world's leading cryptocurrency exchange. The team is committed to delivering objective, independent, and comprehensive analysis and aims to be the thought leader in the crypto space. Our analysts publish insightful thought pieces regularly on topics related but not limited to, the crypto ecosystem, blockchain technologies, and the latest market themes.

Stefan Piech, Macro Researcher

Stefan is currently working for Binance as Macro Researcher. Prior to joining Binance, he worked as an Equity Portfolio Manager at Cape Capital, a Swiss Family Office, and as an Equity Research Analyst for BlackRock's European and UK Hedge Fund. He has prior experience in both Private Equity and Venture Capital. Stefan started his career as Government Official for the District Government Muenster. Stefan has been involved in Crypto since 2019.

Read more

https://research.binance.com/en/analysis

Share your feedback

https://tinyurl.com/bnresearchfeedback