Intro

ZK-rollups (ZKRs) are going to play a **massive** role in the future of blockchain scalability. They can also help simplify the user experience, lower fees (over 20x cheaper than Ethereum!), and potentially provide great investment opportunities if you know where to look. However, to understand why ZKRs can grow into such widely used and beneficial products, some background is needed.

Background

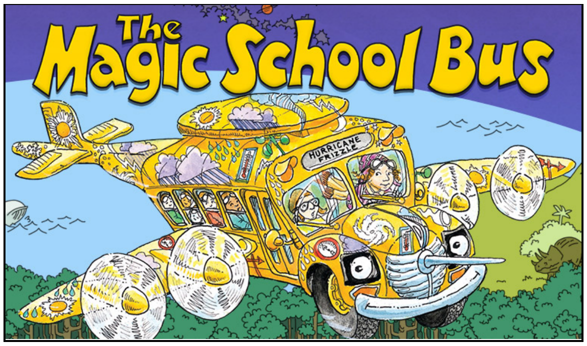
Ethereum is a monolithic blockchain, meaning that it has to handle three things all by itself:
1. Consensus - Coming to agreement on, and including, valid transactions and blocks.
2. Execution - Executing all transactions, including smart contract code, in order to compute the new state (for instance, executing a transfer of an NFT from me to you and updating our balances).
3. Data Availability - Keeping track of all data in order to allow network participants to do things like view and/or verify past transactions, and to prevent attacks like the double spend of a token.

The fact that Ethereum is required to do all of this means that it runs into scalability bottlenecks as network demand increases. You must look no further than the high gas fees, such as having to pay over $200 (at times) for a simple token swap, to see this issue. In order to scale, Ethereum, and potentially many other chains, will need to make some changes. How will they do this? By taking a rollup-centric approach.

ZK-Rollups, Explained

ZK-rollups can help blockchains scale by moving (1) execution and (2) data availability off-chain. Off-chain means off of the main blockchain – let's refer to the main blockchain, like Ethereum, as the "layer 1" since ZKRs act as a "second layer" that can communicate with the layer 1. Before going into any of that, a high-level metaphor for how ZK-rollups work, courtesy of @HaymanLiron on Twitter.[1]

Imagine Ethereum as a bus. Each bus can only fit so many people (transactions) due to the limitations of having to take care of decentralized consensus, execution, and data availability. So, if only 50 people can board the bus, but 5,000 people want to get on it, the price of tickets will go up due to increased demand (this represents gas fees going up).



A ZK-Rollup Bus

A ZKR allows the entire bus to only cost a certain amount, and the bus can fit as many people as possible. This way, the cost of the bus ride can be distributed among all riders, making it far cheaper and more scalable than the "Ethereum bus".

As stated earlier, ZKRs move execution and data availability off-chain. How do they do this?

1. Execution is moved off-chain by using zero-knowledge cryptography, sometimes referred to as "moon math" due to its complexity, to generate **proofs** for batches of transactions. This math has an extremely useful property: it is **impossible** to generate a false proof - any false proof will fail verification. This proof is then stored on the layer 1 blockchain, which comes to consensus on it and includes it in a block. The layer 1 no longer needs to execute transactions; the ZKR's provers, which are explained later, execute transactions.
2. Data availability **can** be moved off-chain. One option is for the ZKR to, after executing all transactions in a batch, store all the data on the layer 1. This is more expensive, so there is a second option. ZKRs can move data off-chain by using a separate network of computers to store this data. This is cheaper, albeit a bit less secure. We'll see examples of each of these approaches later.

To understand this better, let's walk through an example. Say you had 10 ETH on the Ethereum (layer 1) blockchain, and you had moved that ETH onto a ZKR via a deposit. Now, you want to swap that 10 ETH for 40,000 USDC, a stablecoin. So, you use a decentralized exchange to make this swap, gaining 40,000 USDC and losing 10 ETH. The fees paid for this transaction should be miniscule (under 20 cents, but this can get **much** cheaper). You can pay this small gas fee in a variety of tokens – it's up to you. You're done!

Under the hood, the ZKR takes your transaction and sends it to a **prover**. This is software that can take your transaction and, along with others, execute them and generate, using zero knowledge cryptography, a succinct proof that these transactions were executed correctly.

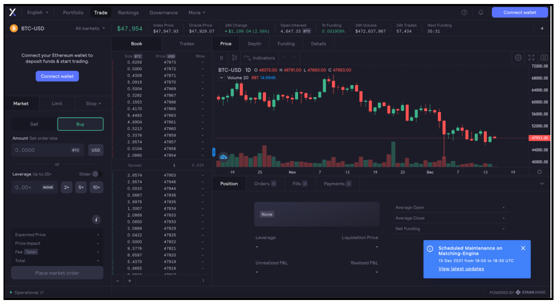
Next, validators (a decentralized network of computers) are able to verify the validity of the prover's proof. Again, due to the use of zero knowledge cryptography, there is, statistically speaking, **no way** for a false proof to ever make it past the validators. In fact, the validators don't even need to know what is being proved! Once this is done, the proof can be sent to the layer 1, where it is safely stored using the layer 1 blockchain's consensus and security. The data from all transactions involved in the proof can either be sent to the layer 1, just like the proof, or it can be stored by a separate decentralized network (again, this is cheaper).

Compared to Optimistic Rollups (described in our "*Blockchain Basics: Part 2*" Education section), ZKRs are more scalable, have lower fees, have faster withdrawal times for when you want to move your funds off the ZKR, and are more secure.

There are many other cool properties of ZKRs being worked on such as interoperability (multiple ZKRs being able to work together), privacy (transactions where no one else can see the details), conditional transactions ("only execute this transaction if another one happens"), shared liquidity across multiple rollups,[2] and more.

ZK-Rollups of Today

There are ZKRs live today, already processing transactions. dYdX, a decentralized exchange running on a ZKR developed by Starkware,[3] has already processed over $11 billion in trades.[4] Gas fees have been so low that the dYdX team has actually been paying for all of them themselves, taking the burden off of the user.



$47,954	Index Price	Oracle Price	24h Change	Open Interest	1h Funding	24h Volume	24h Trades	Next Funding
	$47,947.93	$47,929.07	▲$1,199.04 (2.56%)	4,647.33 BTC	0.001908%	$472,637,967	57,434	35:31

Connect your Ethereum wallet to deposit funds & start trading.

Amount Set order size: 0.0000 BTC USD

Leverage Up to 25×: 0.00×

Expected Price -
Price Impact -
Fee Taker -
Total -

Size BTC	Price USD	Mine
0.6258	47973	-
0.5000	47972	-
0.4308	47971	-
5.0918	47970	-
0.5004	47969	-
0.3292	47967	-
0.1553	47966	-
0.4170	47965	-
9.4483	47963	-
4.6904	47961	-
0.5213	47960	-
0.3376	47959	-
2.8574	47957	-
0.0104	47956	-
2.0860	47954	-
Spread	1	0.01%
2.8574	47953	-
2.8574	47946	-
0.0010	47944	-
0.5667	47936	-
3.9979	47935	-
1.3007	47934	-
2.0869	47933	-
0.0850	47930	-
2.0869	47929	-
0.0422	47925	-
0.5000	47922	-
9.3776	47921	-
6.6597	47920	-
5.4370	47919	-
0.8655	47918	-

BTC-USD 1D O 48373.00 H 48791.00 L 47860.00 C 47953.00
Volume 20 887 14.594K

None
Leverage -
Liquidation Price -
Unrealized P&L -
Realized P&L -
Average Open -
Average Close -
Net Funding -

Scheduled Maintenance on Matching-Engine
15 Dec 2021 from 18:00 to 18:30 UTC
View latest updates

dYdX Home Page

Immutable X is another Starkware rollup, designed specifically for NFTs and gaming, that provides zero gas fees. Other current ZKRs include Loopring, Polygon Hermez, Aztec, and ZkSync 1.0. There are even entire blockchains running on zero knowledge proofs, such as Zcash, though these are out of the scope of this writeup since they are not rollups.

Current ZKRs are usually limited to one application and are not extremely decentralized. However, that is changing; let's look into the two biggest names in the space (and their token plans!).

Starkware

Starkware is a ZKR-building company founded by a team of world-class cryptographers, including founders of Zcash and the co-inventors of STARKs, which we'll get into soon. The company is already valued at $2 billion and has raised funds from an all-star cast of investors including Paradigm, Three Arrows Capital, Alameda Research, Sequoia, Coinbase Ventures, the Ethereum Foundation, Naval, and Pantera Capital.

Starkware, as mentioned before, already runs ZKRs that are doing massive volumes, including dYdX and Immutable X. Many ZKRs use SNARK proofs, a type of zero knowledge proof, but Starkware uses STARK proofs, a type of zero knowledge proof that is quantum computing resistant, invented by two Starkware co-founders, and faster to compute than SNARKs.

To accommodate this different proof type, Starkware created the Cairo programming language, which allows developers to write smart contracts that can be deployed on Starkware's ZKRs. Starkware is also working with another company, Nethermind, to allow Solidity smart contracts to be converted into Cairo. Solidity is the language Ethereum smart contracts are coded in. However, developers should keep in mind that, for max efficiency and to take advantage of the higher/cheaper compute power offered by Starkware's ZKRs, Cairo should be used directly.

Starkware also takes an interesting approach to data availability. As we know from earlier, data availability can either be done via the layer 1 (more expensive) or by employing an off-chain network. Starkware's solution to this is called Volition; Volition allows users to **choose** whether their transaction data should be posted to the layer 1 or posted to the data availability committee (DAC), an off-chain network. This committee is run by extremely reliable participants, but, just to be safe, you could always post transaction data to the layer 1 every now and then.

Starkware has continued evolving since the release of their rollups for specific projects like dYdX. Starknet, a ZKR that will allow *anyone* to deploy smart contracts onto it, went live in late November. Starknet currently employs a whitelist, only allowing specific applications to use it, but the goal is to eventually open it up to all developers. Starkware also currently controls the prover.

Starkware's future vision is much more decentralized. Eventually, there will be multiple rollups, each able to support any number of smart contracts and applications, and there can be many provers and validators. Starkware is also open to using other layer 1s in addition to Ethereum - Ethereum is just extremely secure and decentralized, which likely played a role in Starkware choosing it as their initial layer 1.

But…where's the token?

What about the token? There is currently no Starkware token, but rumors have it that, once Starkware shifts to a more decentralized model, there will be one. Despite the already-high valuation ($2 billion), Starkware has such a great team and such high ambitions that this is certainly something to keep an eye on. Applications that find early success on Starkware should also be good to watch, since writing efficient Cairo code is hard and can provide them with a competitive, first-mover advantage.

ZkSync

ZkSync is another big player in the up-and-coming ZKR ecosystem. ZkSync is a ZKR created by Matter Labs, and it uses SNARK proofs rather than STARKs. ZkSync also has a very solid team of investors, including Binance, Coinbase Ventures, Andreessen Horowitz, Consensys, the Ethereum Foundation, and founders of many large DeFi applications such as Aave, Paraswap, Gnosis, Lido, and Perpetual.

ZkSync may seem to be a bit behind (they have no applications with mass-usage yet) compared to Starkware, but one advantage they will have is already-prepared Solidity compatibility. Developers from Ethereum, Avalanche, Binance Smart Chain, or any other chain that uses Solidity smart contracts will be able to deploy on ZkSync with hardly any changes to existing code. This, combined with the funding support of many large DeFi protocol founders, could allow ZkSync to onboard many existing DeFi projects quickly.

ZkSync 1.0, as mentioned before, is already live. This allows very basic transactions like sending and receiving tokens. However, ZkSync 2.0, which is currently in the testnet phase, will allow full Solidity compatibility, and a clone of the Uniswap exchange has already been deployed to the testnet to showcase this capability. However, to reiterate, ZKRs offer cheaper and higher compute abilities, so even existing Solidity code can be rewritten to take advantage of this.

In terms of data availability, ZkSync has taken a similar approach to Starkware in that users will be able to choose to post their data to the layer 1 or an off-chain network. However, unlike Starkware which uses an off-chain network composed of trusted entities, ZkSync will use zkPorter, a network run by "Guardians" who are incentivized with tokens to provide data availability. This is more decentralized than Starkware's current DAC solution.

What about the token? ZkSync has already announced a token, but not many details are known. The token will for sure be used to incentivize Guardians, but not much else is known about the timing of the release or the mechanism for it. Be that as it may, I would not be surprised to see an announcement related to this in the coming months. Tokens incentivize users, so ZKRs can use this fact to help attract early adopters.

The Future of ZK-Rollups

The future of blockchains looks bright given the amount of scaling (and other cool properties) that can be provided by ZKRs. Vitalik Buterin, the co-founder of Ethereum, has confirmed the "rollup-centric roadmap" for Ethereum, and other chains can follow as the need arises. In addition to future tokens from Starkware and ZkSync, Polygon's MATIC token (Polygon is building the Hermez ZKR), LRC (Loopring, a ZKR), and IMX (Immutable X) are other ZK-related tokens to watch. For Immutable X specifically, make sure to research the token distribution schedule before considering an investment, as there are a **lot** of tokens being released in 2022.

In order to gain mass adoption, rollups will likely need direct bridges from centralized exchanges. For instance, being able to withdraw tokens directly from Coinbase onto a rollup for fractions of a dollar will be a major help in getting more users onto rollups. Just as some exchanges already support withdrawals directly to Optimistic Rollups, we hope to see the same for ZKRs.

ZKRs, as mentioned earlier, can also provide many other benefits. For instance, in the future, we may see a time where users do not need to know or care (unless they want to) which layer 1 their transactions settle on! They will be able to pay their small gas fees in a variety of tokens, including stablecoins, and the rollup will take care of everything behind the scenes. This would provide a much easier user experience, and it *could* drive more value to the tokens of applications that can successfully provide this experience. Blockchain gaming can also benefit tremendously from ZKRs, both from the low fees and also the ability to create private transactions, allowing randomness to be more easily implemented in games.

We could (and will in the future) go more in-depth on the technical details of ZKRs and the investment theses for specific ZKR tokens, but hopefully this serves as a good overview of how they work and why they are important. There are certainly people out there who believe there are **other ways**, including expensive hardware requirements, to achieve mass scalability on monolithic blockchains using models like Solana's, and this argument will certainly continue on for the foreseeable future. Regardless of whether or not this is true, for Ethereum specifically, rollups are the way forward. Perhaps many other chains will follow, and perhaps, in 5-10 years, everyone is using rollups. I'll close with a quote from Vitalik describing ZKRs, and their role in the future, written in an article he wrote describing a potential "endgame" for blockchain scaling:[5]

It will likely take years for all of this to play out. [Interoperability and data availability] are complex technologies to implement. It will take years of refinement and audits for people to be fully comfortable storing their assets in a ZK-rollup running a full EVM…but it does look increasingly clear how a realistic but bright future for scalable blockchains is likely to emerge. -Vitalik Buterin

P.S. If you'd like to learn more about rollups and some common misconceptions, Polynya has a great blog with a variety of rollup-focused articles here.

Citations

[1] https://twitter.com/HaymanLiron/status/1470287878911664128

[2] https://medium.com/starkware/damm-decentralized-amm-59b329fb4cc3

[3] https://starkware.co/

[4] https://indodax.academy/en/dydx-this-weeks-new-crypto-asset-that-you-should-know/

[5] https://vitalik.ca/general/2021/12/06/endgame.html

Links

Starkware: https://starkware.co/
ZkSync: https://zksync.io/

Disclaimer

The opinion and commentary herein is provided for general information purposes only and should not be construed as investment, tax

or legal advice, and does not constitute an attorney/client relationship. Such information is believed to have been obtained from sources deemed reliable but is not guaranteed. Past performance of any market results including crypto currencies and such related assets is no assurance of future performance. Investing is risky, and you can lose what you put in.