DELPHI DIGITAL

Layer 2: Rollups

December 2020

Table of Contents

DELPHI DIGITAL

Analyst

Alex Gedevani

alex@delphidigital.io

Executive Summary

Back in 2017 when Crypto Kitties congested the Ethereum network, it was an early wake-up call of the need for scaling solutions. This past summer, DeFi yield farming was another painful reminder.

This highlighted the desire for Layer 2 scaling solutions that free up the base layer by offloading execution work, leading to reduced gas costs and increased throughput via L2. Today's 15 TPS on Ethereum is not enough to support the growth of DeFi and with ETH 2 scaling a while away, the scaling torch is passed over to Layer 2s, led by rollups. The goal here is to achieve scalability gains by increasing throughput without increasing node load.

As seen in this report, there's tradeoffs across every solution and design considerations come into play depending on the type of dApp moving to L2. Quite a few of the leading solutions are in testnet with high profile projects trialing them and are nearing mainnet within 1 - 2 quarters. **To put into perspective the need for L2s, imagine what would happen if Reddit tried onboarding its millions of users on to mainnet today.** Initiatives like the Reddit Scaling Challenge calling for the right L2 solutions can help to accelerate progress drastically. The L2 ecosystem is more competitive than ever with 20+ submissions. **In this report, we look at how the L2 ecosystem is shaping up and dive into the top varying rollup solutions vying for adoption.**

Optimistic Rollups

OPTIMISM → SYNTHETIX

OFFCHAIN LABS → Chainlink, ACDEX

Zk-Rollups

LOOPRING, Aztec

zkSync → GITCOIN

STARKWARE → DeversiFi, δY/δX, IMMUTABLE

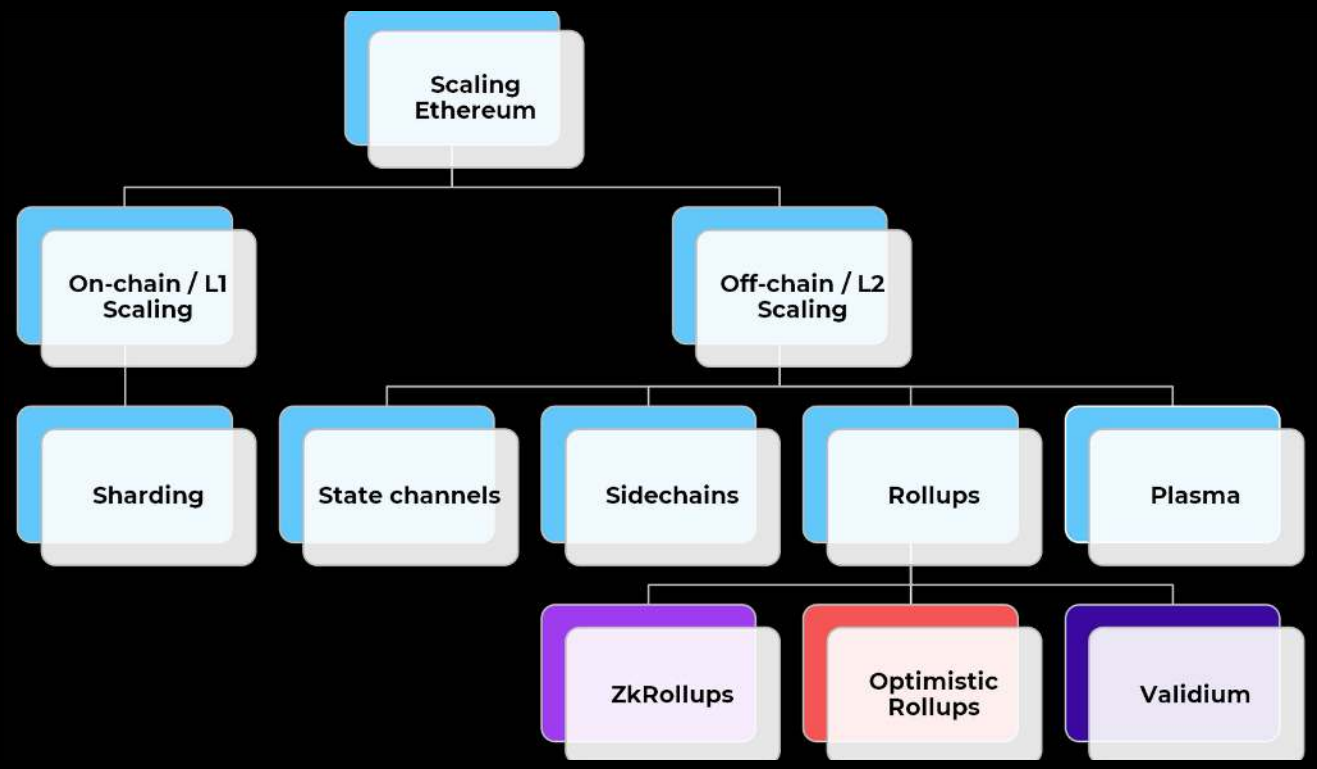
Layer 2 Overview

Rollups are a type of Layer 2 scaling solution that bundles or “rolls up” sidechain transactions into a single rollup block and posts to the Ethereum chain. This allows layer 2 transaction data to be available on Layer 1 anytime it’s needed for validating a state transition. On-chain data assures data availability however moving it off-chain only guarantees that one could verify the integrity of the data if it’s actually present. Scalability benefits in rollups come from lack of reliance on scarce Layer 1 block space, as sidechain state is maintained off-chain.

You can think of scaling solutions as going from everything being done on-chain to on-chain serving as the settlement layer for off-chain interactions. This requires mechanisms to verify the correctness of answers. Validity proofs (zk rollups) & fraud proofs (optimistic) are promising implementations that differ in how they ensure the validity of transactions off-chain.

As mentioned by Vitalik, in his state of rollups post, the near term plan heavily involves rollups. Rollups today can offer 100x+ scaling benefits without ETH 2. In phase 1, scaling with sharding and rollups will be possible, clocking in around 1k-4k TPS. With ETH 2 + Rollups years away, it's expected to scale immensely to 25k-100k TPS. As seen in the report, there is increasing competition among various flavors in the rollup space with the trend being towards EVM compatibility and incorporating optionality for dapps within the system depending on their needs.

"The Ethereum ecosystem is likely to be all-in on rollups (plus some plasma and channels) as a scaling strategy for the near and mid-term future." - Vitalik Buterin



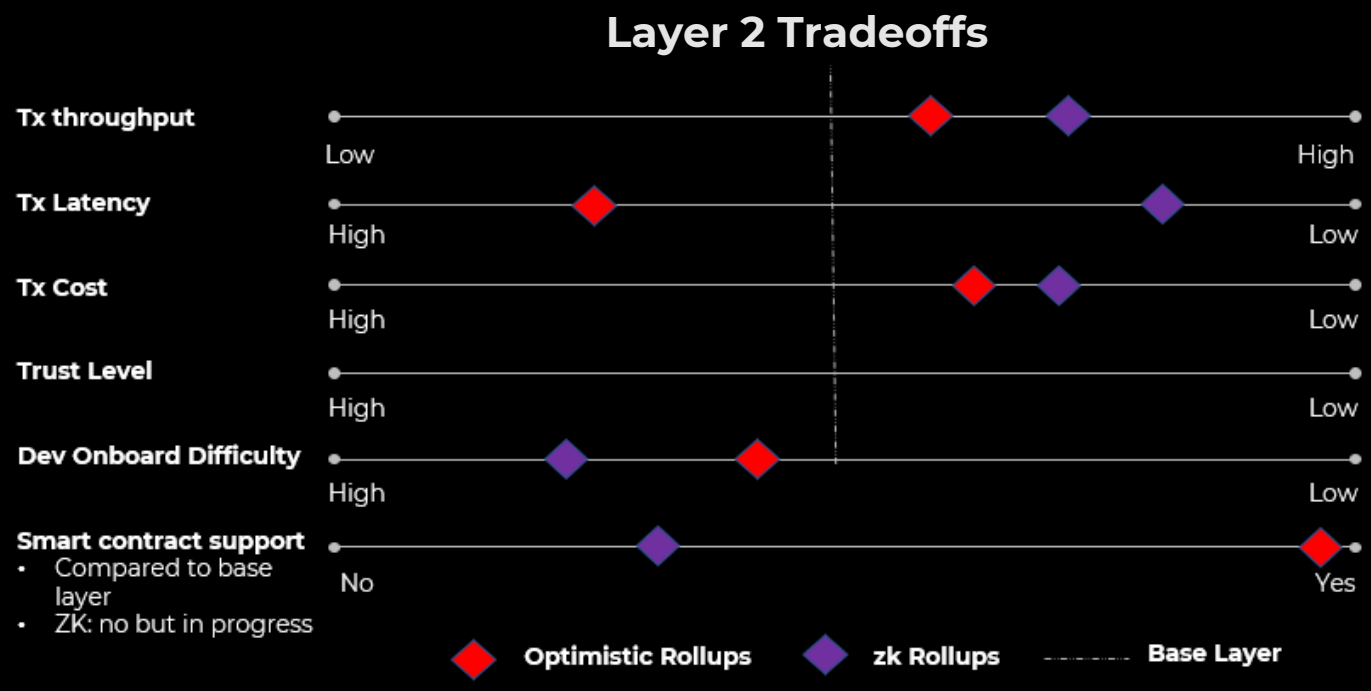
	SNARKs/STARKS	Fraud Proof
Data on-chain	ZK Rollup	Optimistic Rollup
Data off-chain	Validium	Plasma

Layer 2 Comparison

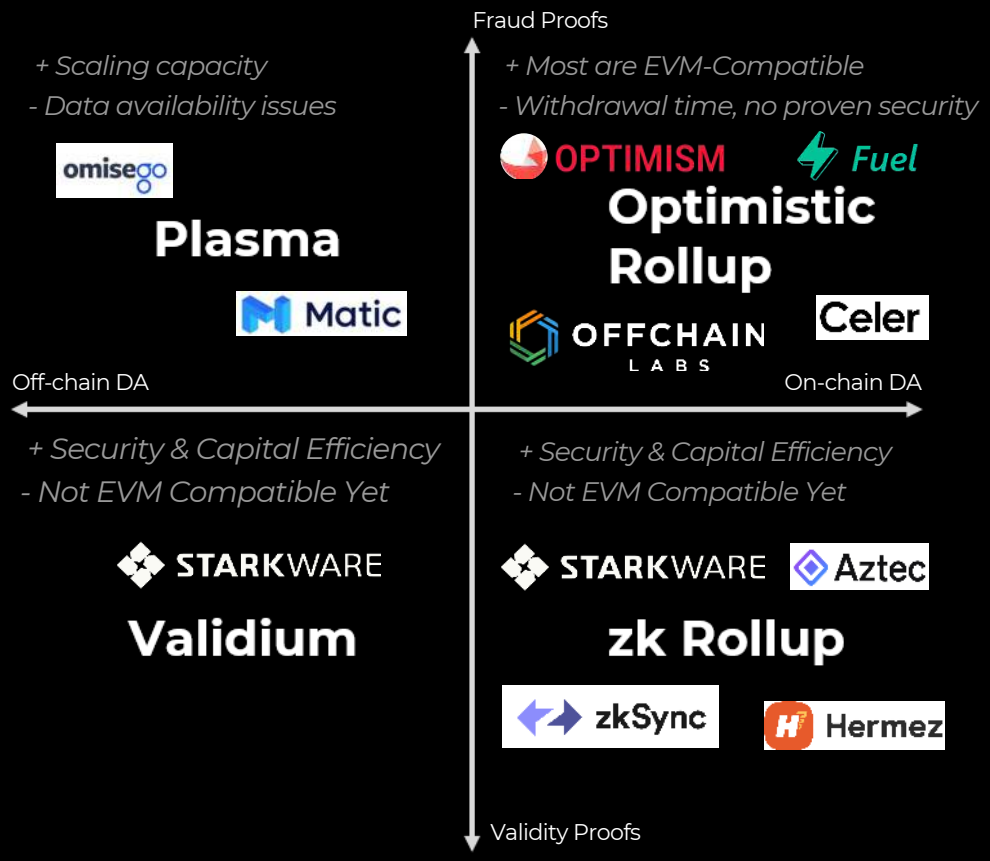
DELPHI DIGITAL

- When it comes to tradeoffs with Layer 2s there are plenty. In ZK Rollups, only valid proofs are accepted. It offers more scalability & makes the process near instant. Optimistic rollups (ORU) give up scalability gains to accommodate smart contracts on L2. There's higher latency given a delay period to give users time to challenge invalid blocks.

- Another important gap between ZK and ORU is EVM compatibility/smart contract support. zk Sync is working to address this in later versions by building functionality to be able to take any existing contract on Ethereum (solidity / viper) and port on zk Sync via a transpiler with minimal modifications.



Scaling Solutions Ecosystem



Solution Comparison

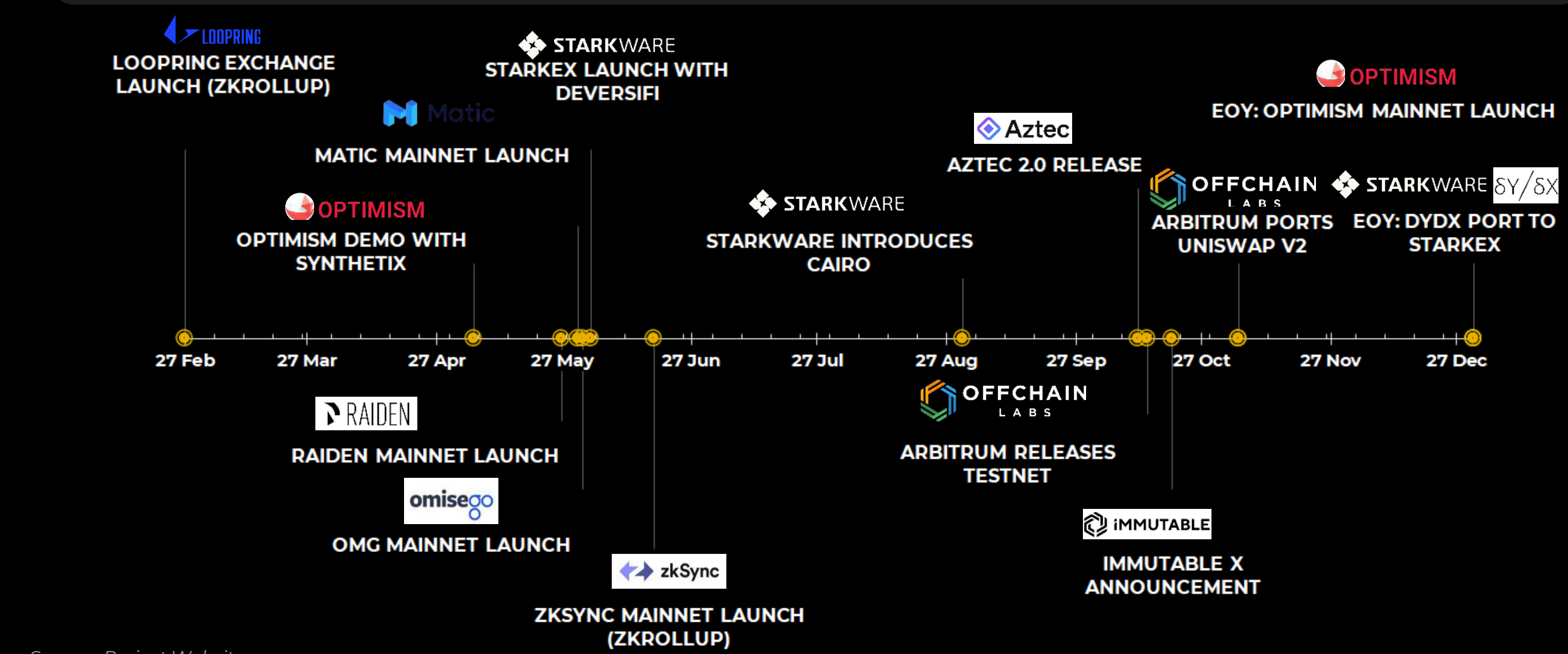
	Scaling Solutions	Sidechains	Plasma	Optimistic RU	Validium	zkRollup
Category	Examples	Skale, POA	OMG, Matic	OVM, Fuel	StarkEx	zkSync, Loopring, StarkEx
Security	Liveness assumption	Bonded	Yes	Bonded	No	No
	The mass exit assumption	No	Yes	No	No	No
	Quorum of validators can freeze funds	Yes	No	No	Yes	No
	Vulnerability to hot-wallet key exploits	High	Moderate	Moderate	High	Immune
	Vulnerability to crypto-economic attacks	High	Moderate	Moderate	Moderate	Immune
	Cryptographic primitives	Standard	Standard	Standard	New	New
Performance / economics	Max throughput - ETH 1.0	10k+ TPS	1k..9k TPS	2k TPS	20k+ TPS	2k TPS
	Capital-efficient	Yes	Yes	Yes	Yes	Yes
	Cost of tx	Low	Very low	Low	Low	Low
Usability	Withdrawal time	1 confirm.	1 week	1 week	1..10 min	1..10 min
	Time to subjective finality	N/A (trusted)	1 confirm.	1 confirm.	1..10 min	1..10 min
Other features	Smart contracts	Flexible	Limited	Flexible	Flexible	Limited
	EVM-bytecode portable	Yes	No	Yes	No	No
	Native privacy options	No	No	No	Full	Full

Source: Matter Labs - Optimistic vs. ZK Rollup Deep Dive, StarkWare's L2 Matrix

Development Timeline

Solutions like ZK rollups with plenty of advanced cryptography are being developed at a rapid pace. After the intro of ZK-rollups came the development of optimistic rollups where put simply, you're replacing a ZK-proof with a fraud proof and adding a timeout period. Optimism is in the final phase of it's testnet with Synthetix and per the roadmap targeting an EOY launch. Arbitrum testnet allows for contract re-deployment and mainnet ETA is Feb. pending final audit. Fuel launches in a few months. Aztec's mainnet ETA is a few months out and after a protocol audit in Q1, capital restrictions will be lifted. Timelines are subject to change but one thing is clear, 2021 is shaping up to be a massive year for scaling.

So what's live on mainnet? The xDAI sidechain, more of a temporary solution, has over 15+ projects in it's ecosystem. Matic using Plasma/PoS network, is live with 50+ integrations. With zk-rollups, payments have seen traction with Gitcoin integrating zk-Sync. zk-Sync SC support is coming in a few months. Loopring just added AMM support. StarkWare, meanwhile, is powering DeversiFi, with plans to support DyDx very soon. Next, let's focus in on each solution to compare the different trade-offs made.



Source: Project Websites

Optimistic Rollups Explained

DELPHI DIGITAL

Optimistic rollups (ORU) allow the ecosystem to get the benefits of sharded execution without having to wait for full blown sharding at the base layer. Transactions and state updates are all posted on the main chain while resource intensive computation and storage are moved to the rollup. **It takes an optimistic view of all rollup-blocks posted on-chain and *assumes validity*.** Aggregators publish the bare minimum with no proofs and **only provide proofs in case of fraud.**

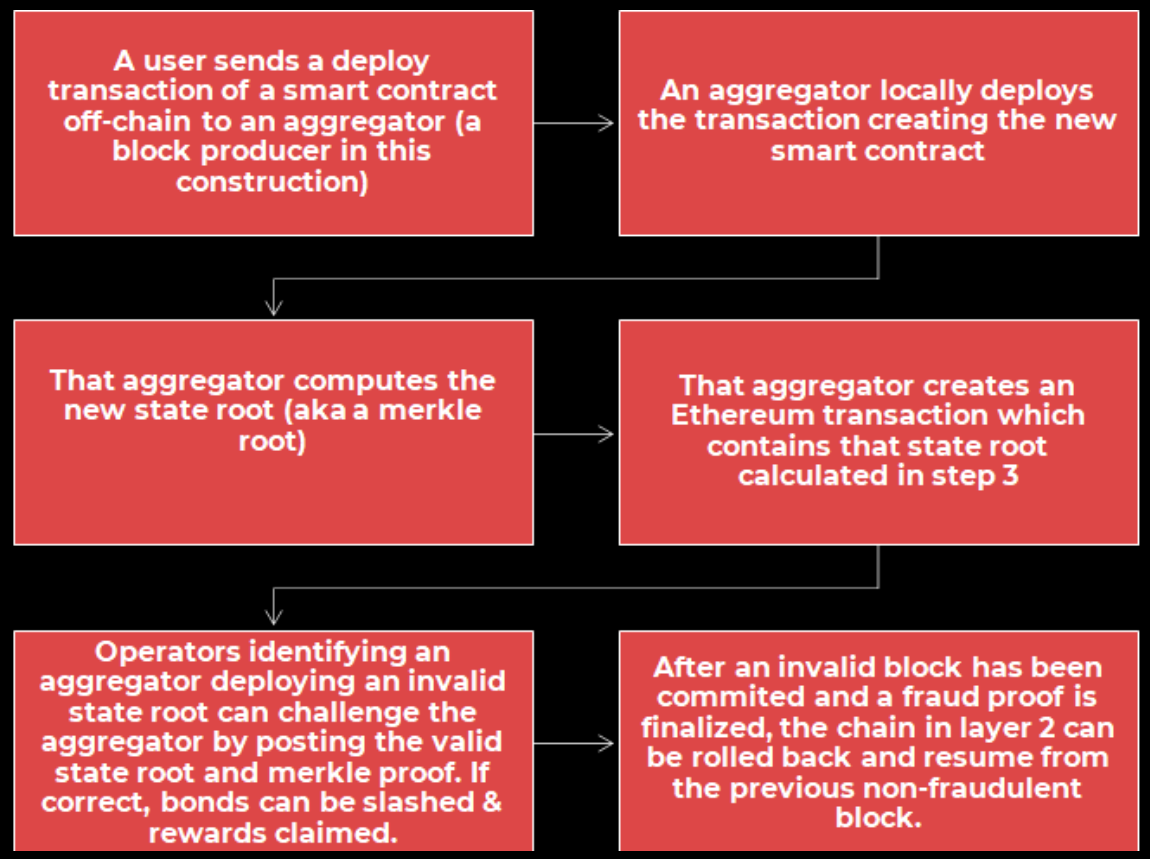
The tech relies on economic incentives for consensus as it's dependent on operators detecting and challenging reported state. Blocks can be reverted if deemed incorrect and block producers are incentivized to behave otherwise security deposits are at risk of loss.

An edge with ORU is the preservation of the L1 dev experience and smart contract support by enabling easier portability of native solidity contracts. A seamless migration of dapps and a good UX is obviously of importance for developers.

OPTIMISM

OFFCHAIN LABS

High Level: Process Overview



Optimism vs Arbitrum Summary Points

- Arbitrum computes a step rather than whole transaction in the EVM, the cost of the fraud proof is low and so congestion risk is less of an issue. This in turn enables a shorter withdrawal period but has dispute process complexity as a tradeoff.
- **Security:** Both rely on assumptions in that an honest party ensures correctness & progress
- **Data**: Arbitrum puts less data on L1 as it executes many txs. between L1 postings vs. Optimism's approach which requires posting of a state hash after every transaction (up to 4x difference in storage)
- **VM**: Optimism's OVM runs directly inside the EVM and reduces complexity and audit surface. It can support many EVM features trivially. Arbitrum's AVM is more optimized for compact fraud proofs but has implementation complexity (new VM).
- **Withdrawals:** Optimism has a 1-2 week challenge period before you can regular withdraw. Arbitrum's is 1 day but the trade-off is it takes disputes longer to resolve.
- **Gas:** Optimism plans to have a gas limit on transactions while Arbitrum does not
- **Timing:** Both in testnet. Optimism: phased approach. Arbitrum: open to anyone

Source: ethhub.io, optimism.io

Optimism

DELPHI DIGITAL

OR is the scaling solution which enables Optimism's off-chain OVM to achieve cheap, instant transactions that still inherit L1 security. It aims preserve the L1 dev experience by enabling easier portability of contracts, thanks to OVM an optimistic implementation of EVM. It will achieve higher scalability gains later when combining shards and rollups. Coinbase signaled support with Coinbase Wallet natively integrating Optimism.

Optimism is currently in the limited testnet phase with industry leaders like Synthetix, Uniswap, and Chainlink part of the earlier adopt cohort. Market views it to become a leader in adoption once live. Testnet has high demand with 90+ projects on the waitlist. In progress: V2 contracts & tooling (ganache, builder, L1-L2 testing). Initially, fees will be charged in WETH. It leverages relayer services to abstract fees away from users.

OPTIMISM

SYNTHETIX

AAVE

Synthetix - It's now expanding on its incentivized trial with SNX stakers to trial the migration from Layer 1 to 2. Post mainnet, exchange contracts would likely run in parallel in L1 and L2. **Back in May, 1.2k traders participated in L2 Synthetix Exchange OVM demo with 12k trades totaling volume of $606m OVM USD over 2 weeks. Gas costs reduced 143x and confirmation times were reduced to 0.3s.**

Uniswap - Details of V3 are not yet out. Optimism is considered the leading candidate for hosting the DEX. For adoption, this would be a huge market validation signal as scaling can also be thought of as a social coordination game.

Pros

- Flexibility in generalized computation (Turing complete/EVM compatible)
- Increase in scalability over L1
- All data available on chain
- Better UX (economic abstraction, existing tooling)

Cons

- Limited throughput compared to other L2 solutions
- Withdrawal/challenge period of 1-2 weeks
- Capital support in single rollup instance limited
- Improving capital efficiency requires shortening Dispute Time Delay, making a fraud+censor attack on L1 cheaper

Source: ethhub.io, optimism.io, https://blog.synthetix.io/why-optimism/

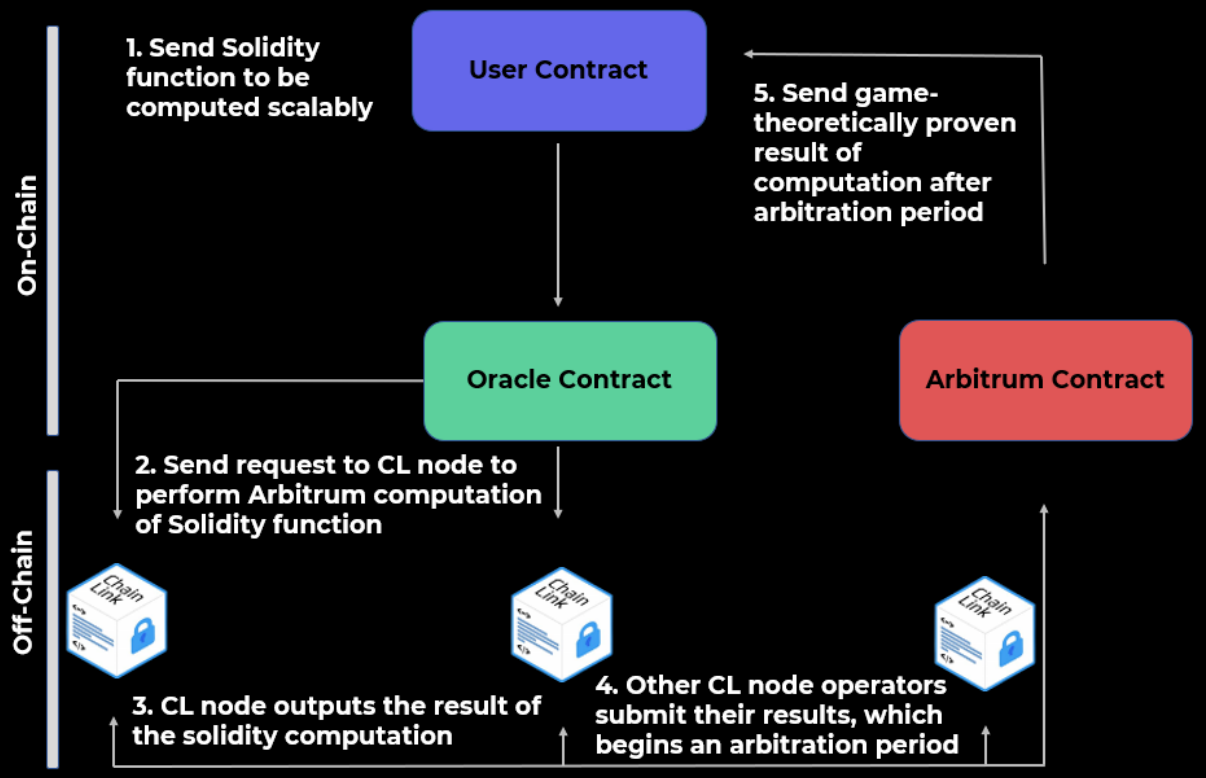
Arbitrum

DELPHI DIGITAL

Arbitrum by Offchain labs is a blockchain agnostic flavor of optimistic rollups, live on testnet. **Arbitrum can execute EVM code directly, without even requiring one to recompile contracts to test their rollup.** Testnet enables easy deployment of solidity contracts on the rollup. The dev experience is identical to that of L1 contracts and compatible with ETH tooling. Another difference is that Arbitrum is a "multi-round rollup" with an edge over single round rollups, being a smaller on-chain footprint. It aims to be a lower cost solution with wider applicability.

They've partnered with Chainlink nodes to provide Arbitrum validation services which furthers bolsters security and enables more complex app designs w/ use of scalable computation. Plan is to enable further scaling as they are working on channels and Arbitrum sidechains for early 2021 with permissioned validators, with plans to introduce a hybrid approach enabling switching.

Using Chainlink with Arbitrum



To showcase the Arbitrum testnet, the team recently rolled out Arbiswap, not a PoC but a functional Uniswap V2 port with a few wallet integrations. Note that layer 1 can handle a max of ~7 Uniswap swaps per second. **With Arbiswap rollup chain at full capacity, the L1 can handle 390 swaps per second, a 55x gain in gas efficiency.**

MCDEX chose Arbitrum for it's testnet for it's product readiness & developer friendliness. Benefit: reported 300x reduction in costs. In just a few minutes, I was able to set up a test account with minimal friction & trade ETH perps.

Long term: Arbitrum's Different Scaling Modes

	Rollum	Sidechains	Channels	L1 Ethereum
Security	Trustless	AnyTrust	Trustless	Trustless
Privacy		✓	✓	
Public Participation	✓	✓		✓
Validation	Permissionless	Permissioned	All participants validate	Permissionless
Cost	Low	Lowest	Lowest	High
Finality	Same as L1	Instant	Instant	Minutes
Censorship Resistant	✓	✓	✓	✓

Source: Offchain Labs Medium channel - Chainlink, MCDEX.medium, Arbitrum.io

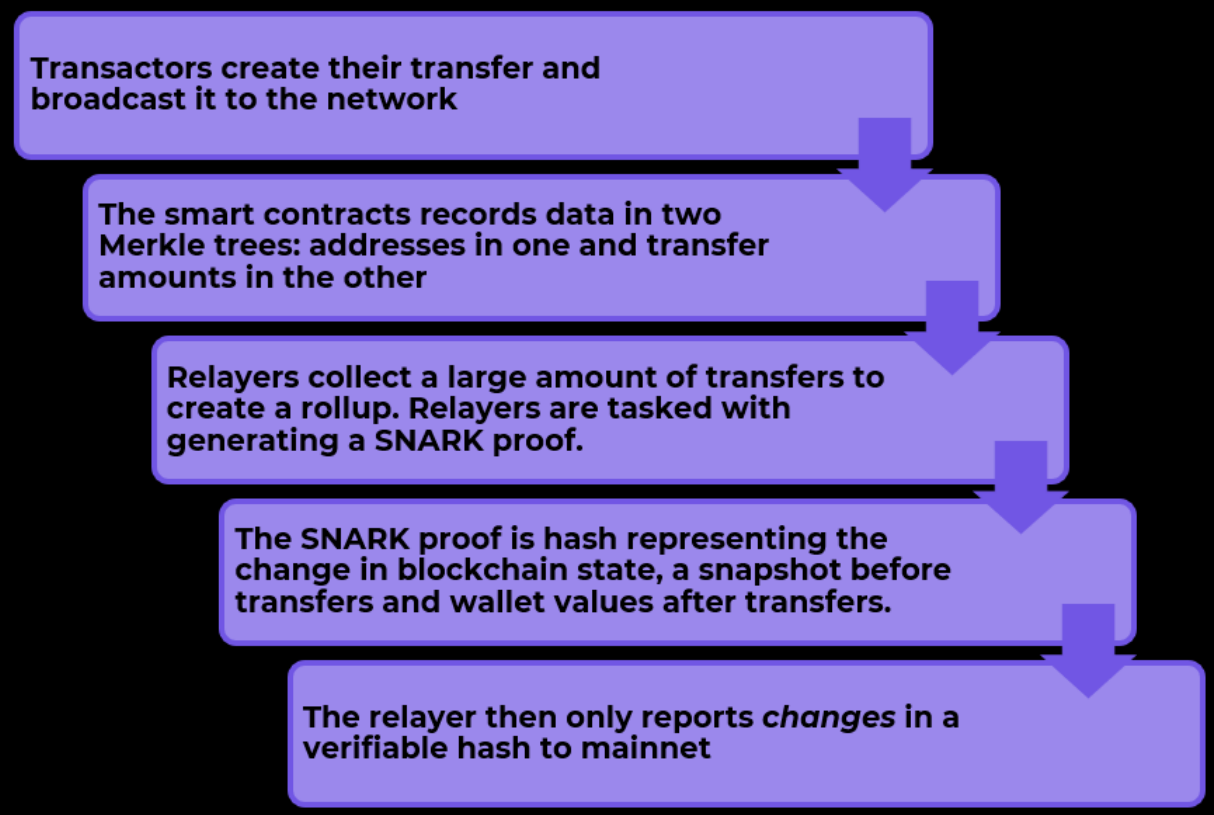
ZKRollups Explained

DELPHI DIGITAL

In ZK-Rollups, operators **generate ZK-proofs for every state transition** and submit them on-chain, to be verified by a Rollup contract on Ethereum. Assuming that the proofs only include valid transactions, it's difficult to manipulate blocks. Think of them as "**non-interactive**" rollup given reliance on succinct validity proofs. With ZK rollups you get "passive security". Cryptographic assumptions aside, get same security guarantees as layer 1. ZKR don't require active duty to keep your funds in rollup secure. With validity proofs, there's no worry about rollbacks.

Think of the ZKR approach as more math based. It bundles and compresses transactions, then creates a validity proof which verifies validity and the right state change. Note that compression of computation leads to quick verification as ZK snarks are efficient in checking proofs. Creating proofs can be expensive and ZKR are *currently* better for trivial payment transactions.

High Level: Process Overview



	Trusted Set-Up	Speed (Verifier + Prover)	Proof Size	Quantum Resistant
zK-STARK	No	Fastest	Largest	Yes
zk-SNARK	Yes	Fast	Smallest	No
Plonk*	Yes	Very Fast	Small	No
Bulletproofs	No	Slowest	Middle	No

*Developed by Aztec, Plonks are an improved zk-SNARK construction with faster prover times than SONIC. Although it has a trusted set-up similar to SNARKs, it's "universal and updateable". Instead of needing separate trusted set-ups for every program, there's a 1 to many program dynamic that allows for multiple parties to participate in the set-up. Plonk verification times are constant despite how complex proofs get.

Optimistic Fraud Proofs	vs	zkRollup Validity Proofs
1 honest validator required at all times		ZKP setup/audit required once
If a fraud proof fails, all funds are lost		If a validity proof fails, just retry
Exits take 1 week		Exits take 10-15 min
Privacy is hard and expensive		Privacy is easy and cheap
In development		Live on mainnet

Source: ethhub.io, zk-Sync Medium Channel, zksync.io, https://vitalik.ca/general/2019/09/22/plonk.html

zk Sync

DELPHI DIGITAL

It's been a year of breakthroughs for ZK-Rollups in 2020 with the introduction of the Zinc programming language, SNARK-friendly VM and implementation of recursive PLONK proof verification for Ethereum. **In short, privacy preserving smart contracts are coming to zkSync. ZKR are better than OR for scaling, security, & shorter finality.**

Curve is the first dApp to test out Zinc Alef, the new zkSync L2 smart contracts testnet. Matter Labs helped Curve re-write existing Curve contracts (Vyper) into a Zinc version. Zinc follows simple Rust syntax and borrows smart contract elements from Solidity. It can be learned in few days by experienced Solidity/Vyper developers. Note Curve views this as a PoC and is not committed to any L2, other product engagements are taking priority for now.

Curve

Pros
- Moving the AMM to a rollup would increase scalability, usability, and decrease cost gap compared to a CEX
- Contracts inside the zkSync L2 network will be able to call each other atomically similarly to how it's done on Layer 1.

Cons
- Challenge is that Zinc is currently non-turing complete although work is being done to make it turing complete in the future
- Zinc VM is not yet integrated into zkSync core

GITCOIN

The Gitcoin/zk Sync integration has cut costs and led to a smooth checkout experience. Stats from last grants round:

- **Over 52% of 13.4k contributions worth $287k came using zkSync**

Summary Points:

- **Beyond the Curve example, zk Sync is working on a transpiler to port native smart contracts in solidity, with only small modifications**
- Proof sizes can get expensive depending on complexity
- ZK Sync will have consensus at Layer 2 also serving fast confirmations for users, don't rely on validators for security
- Validators agree on the leader of block and the block producer then pushes ZKP to mainnet
- Goal is to solve censorships/reliability problems in permissionless way. ZK Sync token will play a role in governing participation. Validators will collect fees.
- 800 TPS measured on Ropstein in the non-recursive zk-Rollup. Recursive version claims up to 3k, to be proven.

zk Sync Progression

Shard	Throughput	Security	Transaction Costs
zkRollup Shard	3k TPS	L1 Security via zkRollup	~USD 0.01 (at 100 Gwei)
Guardians shard	10k-20k TPS	Bond of 2/3 of zkSync Guardians stake	~USD 0.001
Protocol x shard	Depends on protocol complexity	Secured by validators of protocol x	Low

Source: resources.curve.fi, zksync.io, Reddit Scaling Competition Bake-off

Loopring: Takeaways from a 1st mover

DELPHI DIGITAL

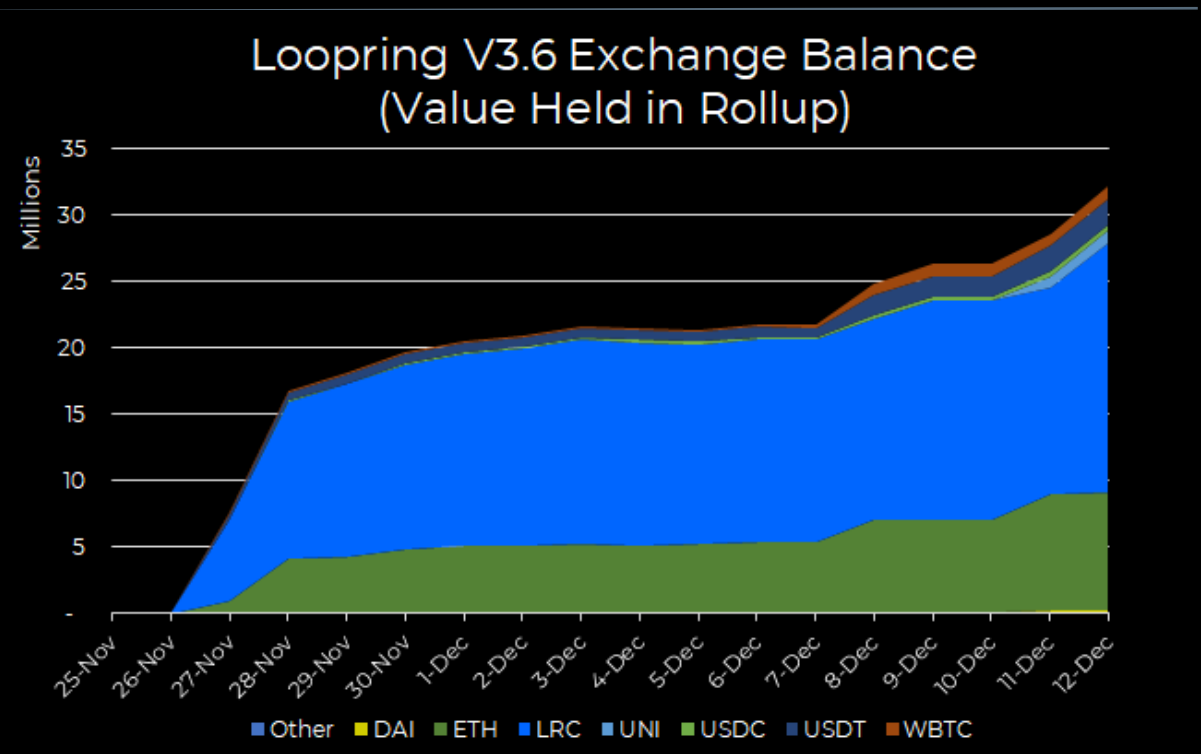
LOOPRING

Loopring has taken its real-time learnings being a 1st mover to change it's approach after better understanding its users' needs. It's designing for a future where users spend most time on L2.

- **Adoption**: Live for one year: 7k + users and 2m+ txs settled
- **Driver**: high performing orderbook DEX / payment dex (Gas-free, near instant)
- **Lesson learned:** Users hesitant on paying gas fee to create L2 account, pay more fees to deposit each asset to L2, and *then* benefit from gas free txs. Expose pros in better way
- **v.36 improvement:** Abstract away difficulties with meta txs, other design decisions -> Fewer and cheaper txs to get onboard
- **Insight**: Make L2 environment very attractive, with great utility on there, for it to become a homebase for user
- **Solution**: Loopring Wallet with zkRollup baked in. Users can spend lot of time in it: trades, swaps, transfers, provide liquidity, self-custodial
- **Changes**: Technical protocol improvements (v3.6), product improvements (wallet), working on UX improvements
- **Better pitch**: Cheap/ fast better verbiage than TPS. Focus is more on productizing and improving UX, than technicals

Loopring's new ZKR rollup with AMM support has launched:

- It supports Balancer's curve and allows for flexible design of AMM managing contracts on layer 1
- Anyone can be a passive LP, unlike L1 with inhibitive gas fees
- Mix and batch process different types of layer-2 transactions into the same block, which improves the relayer's batching efficiency and reduces the ZKP prover cost.
- UX Improvements: deposit fees & token registration fees removed, ETH addresses live by default & receive funds on L2
- It'll match regular orderbook orders with AMM pools natively without the need for extra funds to do arbitrage.
- "Withdrawal mining" rewards users for holding in assets in self-custody, incentivizing withdrawals from CEXs and assets on L1. In a 4 day span, they paid out to 903 accounts earning ~18% APY who hold $20m on Layer 2. Liquidity mining is next.



Source: Dune Analytics - Loopring, Loopring Medium, Matthew Finestone

StarkWare - StarkEx (1 of 2)

DELPHI DIGITAL

Starkware's StarkEx can be deployed either in a **ZK-Rollup mode** or **Validium mode**. To better understand Validium, think of it as a ZK-Rollup but with the primary difference being that data availability in Validium is off-chain, whereas ZK-Rollups (another Starkware option), keep it on-chain. This approach increases throughput with a tradeoff being centralization with operators of Validum but there is an escape hatch as an exit option. The Data Availability Committee holds customer balance data offline and take part in signing commitments updating blockchain state. StarkWare designed Volition, a solution where users can dynamically choose whether they want their own data on-chain or off-chain. Powered by StarkEx, DeversiFi DEX has $6.2M TVL and 772 total registrations. DyDx is moving rollup shortly. Immutable is on board given quick withdrawals & inability to attack system regardless of value transferred.

STARKWARE

δY/δX

iMMUTABLE

DeversiFi

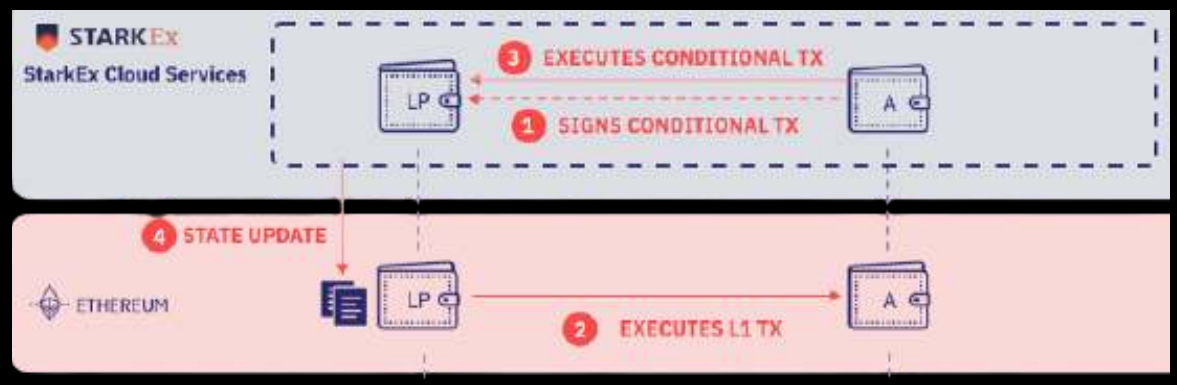
paraswap

- *StarkWare offers both ZK-Rollup (3k TPS at reddit bakeoff, dYdX, Immutable), and Validium (DeversiFi).*
- *Timing:* ***Within ~6 weeks, it will also be live with Immutable (NFT Minting Trading) and dYdX (perpetual contracts)***

Cairo: Turing complete STARK framework live on ETH mainnet

Cairo is Starkware's new higher level language for programming STARKS. **The breakthrough here is Cairo achieves turing completeness with STARKs, also coming with memory, functions, recursions, etc.** All deployments of partners will be written in Cairo, supporting programming functionalities. The intro of Cairo can be thought of as a transition from "Asic" to "CPU". It leverages just one Algebraic Intermediate Representation (AIR), which means one verifier uses a single proof to confirm the integrity of different program executions, amortizing costs across apps. There could be batches of dYdX trades and minting of God's Unchained NFTs under a single proof.

Road to Interoperability Between L2s: Phase 1



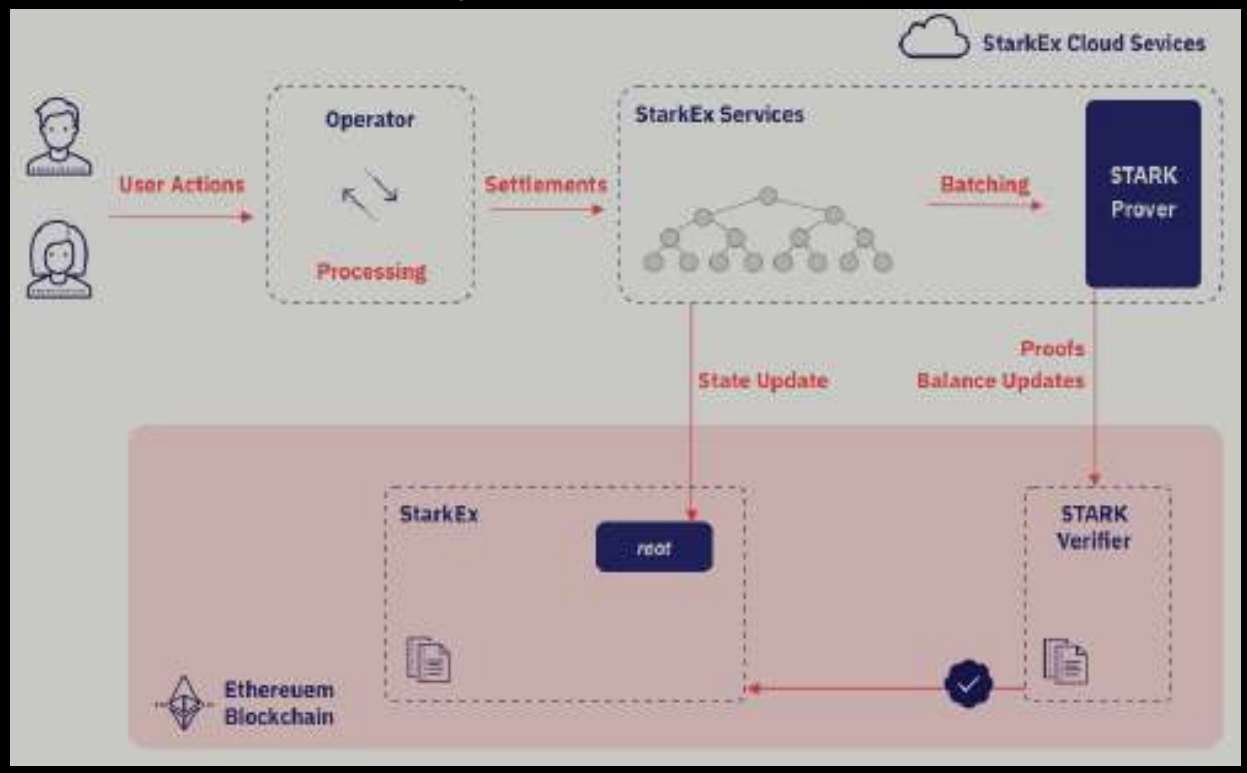
- Long term goal: Easily move between L2s with minimal L1 friction.
- Phase I: StarkEx (L2) → Ethereum (L1):
- Users pay LPs a service fee to have fast withdrawals of funds from StarkEx to any destination on L1
- "Conditional tx" executed upon an event taking place

Source: StarkWare Medium Channel, Dune Analytics - Deversify

StarkWare - StarkEx (2 of 2)

Note StarkEx has both an on-chain and off-chain components. Off-chain is leveraged for heavy-duty computation/storage whereas as on-chain is mean to be for lean verification and state commitment. The point here is Starkware is able to support basically whatever the app client wants whether it be on-chain or off-chain for which a committee will be used.

System Overview



Continuing with the principle of giving the end user choice on where they want data stored, StarkWare has designed Volition, a hybrid on-chain/off-data solution. As an example, a trading firm with valuing secure of storage of funds and low fees, could start daily by sending funds to an off-chain account for frequent trading, and sending them back to an on-chain account EOD. Although zk-Sync and Arbitrum also have non-rollup modes as well, StarkWare has applications on both modes. It currently offers more functionality on mainnet such as margin trading and proving oracle prices.

StarkEx supports the Full Data Availability Spectrum (on mainnet)

Reddit Bake-off

DeversiFi

Rollup
On-chain data

Volition
Dynamic User Control

Validium
Off-chain Data

Source: StarkWare.co

Pros / Cons

DELPHI DIGITAL

OPTIMISM

Pros

- Flexibility in generalized computation (Turing complete/EVM compatible). Clearer migration path for existing dapps on L1
- All data available on chain
- Better UX (economic abstraction, existing tooling)
- Garnering strong public support. Testnet waitlist of 90+

Cons

- Limited throughput vs. ZKR. Has centralized sequencer
- Improving capital efficiency decreases security
- Longer withdrawal period / more costly LP service fees
- Sequencer increases UX but is centralized
- Fraud proofs mechanism not published yet, building block upon which security claims rely on

MATTER LABS

Pros:

- Reduced fees per user transfer
- Less data contained in transactions increases throughput and scalability of layer 2
- Shorter/finality exit times and capital efficient
- Supports lower cost privacy
- More decentralized compared to ORU aggregation

Cons:

- Generalized smart contract support not live yet (need to see how well it'd work, costs)
- Generalized ZK Proofs inefficient, needs data optimization
- Initial set-up of ZK-Rollups promotes centralized scheme
- More advanced cryptography needs time to be proven

OFFCHAIN LABS

Pros

- Simple dev experience with direct EVM compatibility
- TPS of 453 for simple txs with plans to optimize further (via aggregating signatures)
- Non-custodial and Ethereum wallet compatible
- Support for high complexity txns (Multi-round rollup)

Cons

- Instant confirmations at cost of increased frontrunning risk with the centralized sequencer model to start
- Composability isolated to specific scaling modes
- Complexity switching between rollups and sidechains while guaranteeing high security

STARKWARE

Pros

- Powers StarkEx: Measured 9k+ TPS on Ropstein (Trades)
- Faster withdrawals and lower cost of capital for traders
- Developing VeeDo STARK-based Verifiable Delay Function. Verifable randomness can open new use cases
- Working on Volition, enables support for whatever the client wants whether on or off-chain data accounts

Cons

- Implementation speed of onboarding dApps
- Would like to see more developer awareness with Cairo
- With StarkWare's Validium option, there's technical challenge in solving data availability problem

Source: EthHub, matter-labs.io

Alternative Solutions

DELPHI DIGITAL

Aztec is a zkRollup Layer 2 focusing on privacy with plans to launch initial mainnet shortly with bug bounties. Thanks to PLONK research, each txn. is encoded as a zkSNARK, protecting user data. These transactions are then bundled by relayers using a further rollup zkSNARK, which is then sent to Ethereum in one proof. This means various in assets in private DeFi transactions can bundled all in one rollup. Aztec uses Noir, a language enabling private smart contracts. Performance wise, Aztec 2.0 has 200x gas reduction compared to Aztec 1.0 and will support 300 TPS.

Fuel is another optimistic rollup solution that is working on a UTXO based data model which allows for much higher transaction due to parallelism: transactions validated in parallel on consumer grade hardware. It's led by John Adler, original proposer of the initial optimistic rollup construction. The initial focus is on payments and basic payment applications with subsequent work being done for generalized smart contract support in V2. Simply put, compared to other ORU, **Fuel offers the cheapest and most scalable way of doing value transfer**. Generalized smart contract support is planned in V2 with ETA potentially in H2 of '21.

The L2 scaling solution allows for dApps to access app-specific chains that are secured by SKALE's validator set. It's designed for EVM-compatibility and can leverage Ethereum's existing dev tools. The mainnet went live Oct. 1st and has since amassed $80m TVL with 1k decentralized elastic chains. A cohort of 4k people and entities are securing 135 network nodes across 45 validator orgs. It's unique feature is elastic sidechains. Configurations for chains can easily be modified to accommodate an increase in transaction demand, storage and other needs. This enables flexibility for a number of apps with the highest TPS maxing out at 2K TPS.

This report is focused on rollups, but we also wanted to point out the Matic and xDAI sidechains given their traction as the ecosystem waits for more production ready rollups. Matic provides hybrid PoS and Plasma enabled sidechains. Like xDAI, Matic is EVM-compatible and suitable for deployment of Solidity smart contracts, a pro for devs. It has garnered 50+ integrations thus far. In it's Proof of Concept submission to reddit, Matic processed 3 million transactions in a period of ~12 hours. Note that sidechains lack the security properties of rollups as they don't benefit from the security of the base layer.

xDAI is a sidechain that is transitioning to POSDAO, a Proof of Stake consensus protocol. It has ~5 second block times and low gas fees. With xDAI it's easy to onboard existing Ethereum apps onto it. The compatibility, ERC-20 bridge, short dispute periods, fast block times, Metamask support and simply being production ready are a few reasons why dapps like Perpetual Protocol joined. In Sept. and Oct. alone there were 15 launches and migration announcements on xDAI. In the last 10 days, the network has processed ~23.5k tx/day. Considered an interim scaling solution, xDAI may eventually move to rollup solutions.

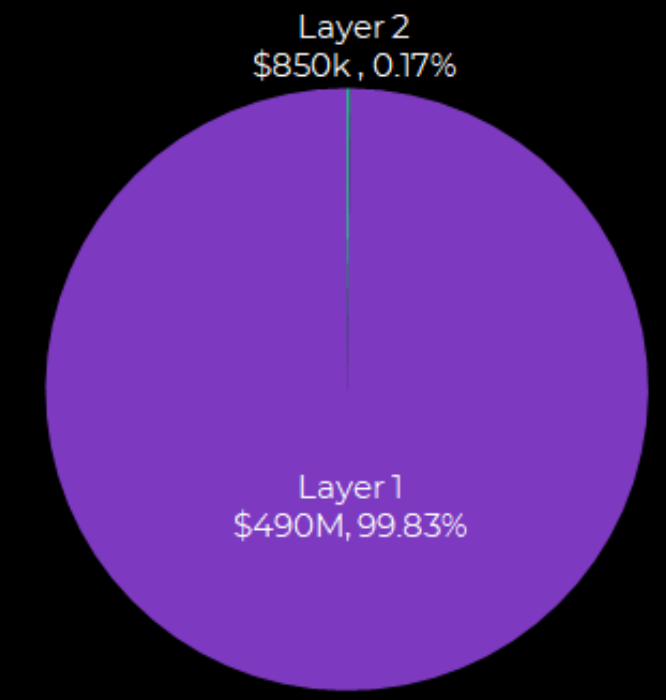
Source: https://blockscout.com/poa/xdai , Skale.network

The Adoption Problem

While all this new technology is very promising and everyone wants to see scaling solutions for Ethereum succeed, there is still the chicken and egg problem of adoption.

As a dApp or protocol developer there's little incentive to move your code, liquidity and userbase over to a layer 2 solution until there's already a critical mass of other projects, users and liquidity there.

Similarly as a user, while you may want lower transaction fees for using an AMM there's no reason to deposit funds on a layer 2 to access a pool with little liquidity, especially if transacting at size. And if the only thing on that layer 2 was the AMM you wanted to use, it would not be time or capital efficient to deposit, trade and withdraw back to layer 1.



Usage on L2 is minimal for now with trading volumes paling in comparison to L1. TVL on L2 totals $43.4M across zk-Sync at $2.2m, Deversifi at $6.2M and Loopring over $35M (incentivized). Notably, there's been a sharp increase in zk-Sync up from $112k on Dec 12. to $2.2m, driven primarily by 1 address. $43.4M on L2 is a blip in comparison to $4B TVL alone just from L1 DEXs.

Possible path to adoption for AMMs

- AMMs deploy pools with limited liquidity to L2
- Arbitrageurs keep price in check with L1 despite depth being small

- Traders who only swap very small quantities (most affected by tx fees) and use only one or two DeFi protocols move over to the L2 and swap exclusively there

- Slowly users and projects trickle over, attracted by the faster and cheaper experience, increasing userbase and liquidity.

- Once a critical mass of projects, users and liquidity exist on the L2, it makes sense for projects to incentive their remaining L1 users to move over too.
- Projects are incentivised to do this if it looks like the better and cheaper user experience is attracting new users to the project but fragmented code and liquidity is proving inconvenient

Source: Etherscan - Deversifi 2, zkSync, Loopring Dune Analytics

Exit Times/Withdrawals (1 of 2)

DELPHI DIGITAL

Fuel Labs - Use cross-chain atomic swaps to immediately withdraw (btw rollup and Ethereum using HTLCs, **few minutes** by LP negotiating atomic swap.

zk Sync- Lite clients allow for things like composable transactions between zk-rollup and contract on layer 1 to withdraw non-liquid tokens. Zero block latency between posting zk rollup block and withdrawing funds. With ORU, need at last one block of latency, making it harder to do something like a flash loan between the 2 layers.

Exit Times

Starkware - The team introduces "conditional tx" executed upon an event taking place. Users pay LPs a service fee to have fast withdrawals of funds from StarkEx to any destination on L1 (Phase 1). In Phase 2, it enables tx. across StarkEx dapps, except this time LP funds are on L2. Final phase 3 is L2 to any L2, also requires periodic re-balancing at most few hours & decreases proof generation time (minutes) as Starkex apps scale up. (Link)

Arbitrum - The OR has longer withdrawal periods at ~1 day. This can be sped up with solutions like Connext, more costly. There's a shorter dispute period vs Optimism, but in the event of spam attacks, there's throttling measures.

Optimism - There's a **1 - 2 week exit time** given the challenge period. To withdraw earlier pay LP service fee, which ends up being higher given opportunity cost (Example imagine interest charge on an in demand asset like YFI). Longer finalization delay is for censorship resistance & deterrence of spam attacks.

---

connext

Connext - Solving for cross-chain interoperability for L2s (TCP but for value transfer)

- Benefits: Ability to enter and exit L2 chains with instant finality (solve UX problem)
- Routing layer through use of state channels on top of rollups to service value transfer across layer 2s
- It's focused on building swap UIs at the moment rather than on building aggregators
- This solution accrues networks effects as more state channels join the network
- Partnering with dapps and looking for early LPs to/from L2s and earn yields
- Mainnet ETA EOY and ETA for network launch with partners is Q2

Exit Times/Withdrawals (2 of 2)

With seemingly every rollup having a different withdrawal period, a mental model to use is that they are first trying to solve L2 to L1 withdrawals, L2 app to L2 app on the same rollup, and lastly L2 rollup A to L2 rollup B. Typically faster withdrawals means a lower cost of capital for traders and the benefit of moving funds around faster to for example take advantage of arbitrage opportunities.

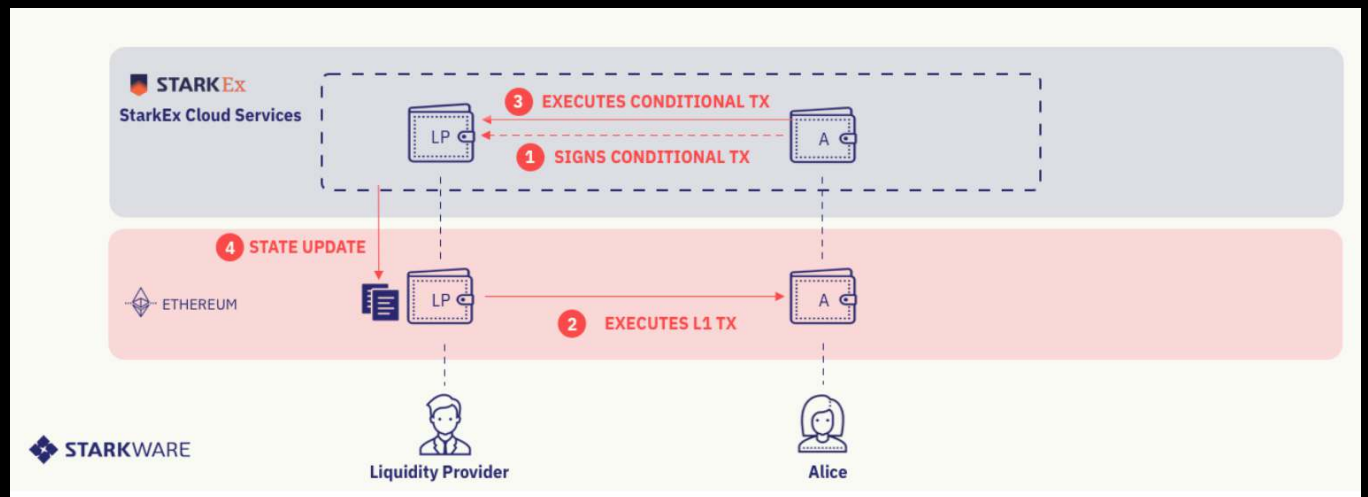
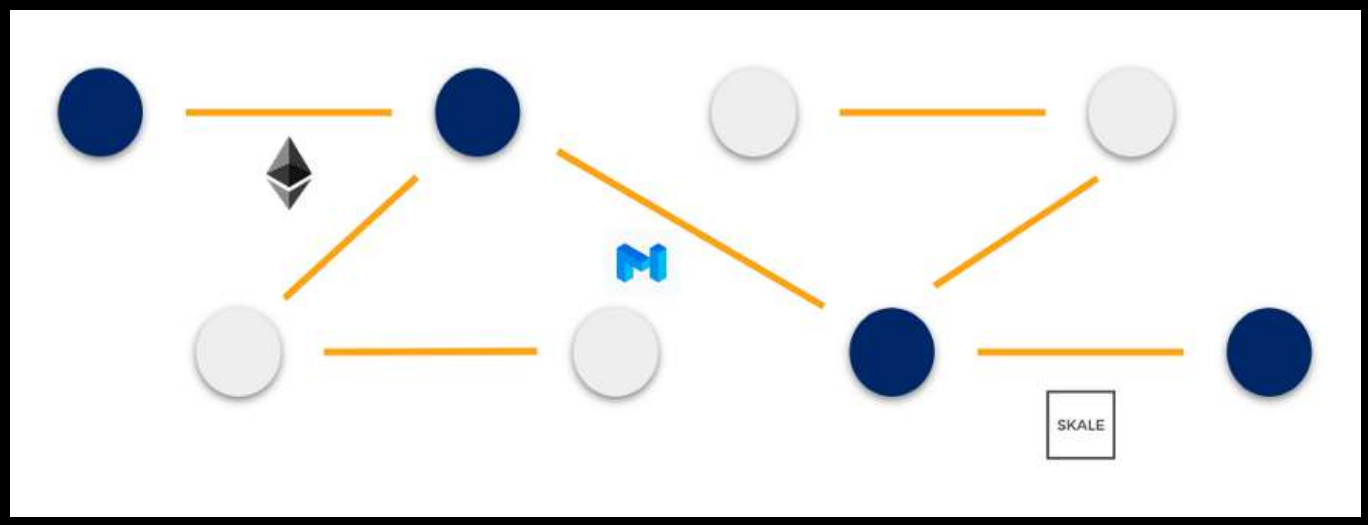
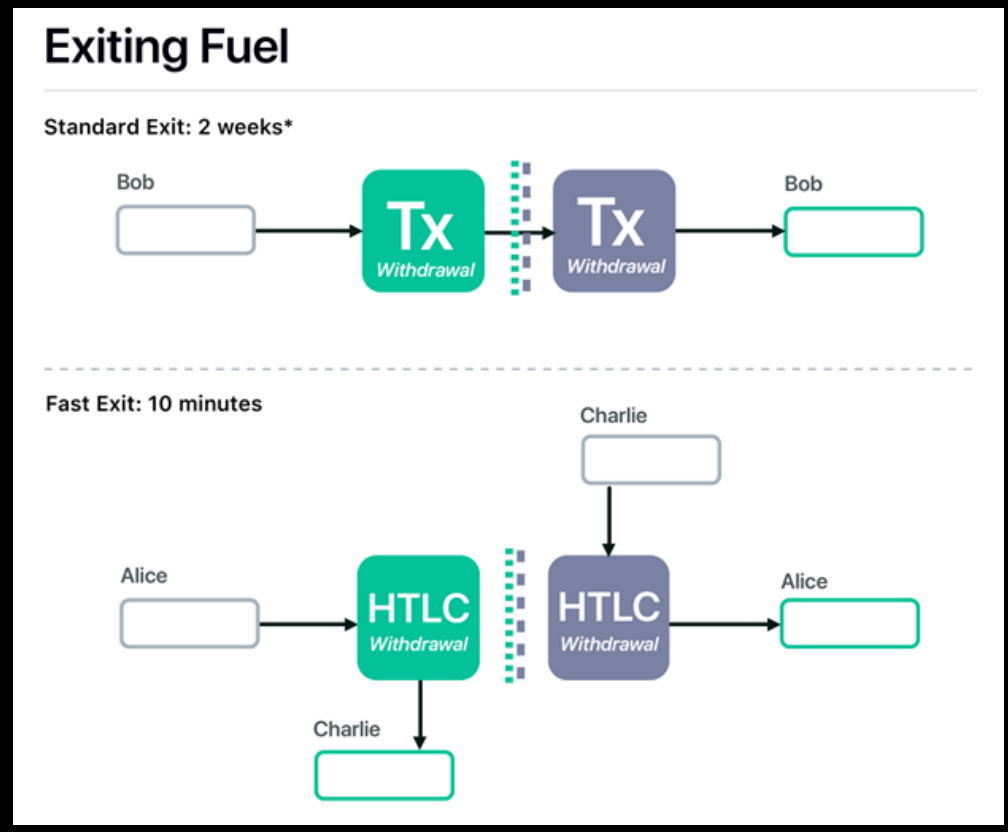


Diagram 1: Fast Withdrawal Flow

StarkWare: Conditional transactions. Cookie jars are extra smart contracts used by exchanges for fast withdrawals. Cost of capital is determined by the frequency of replenishment of funds (rebalanced).



Connext: Using Vector, routers propagate payments over liquidity in assets and across chains (+Plug-in for non-turing EVM complete chains)



Fuel: Fungible assets can be withdrawn immediately within an atomic swap powered by HTLCs, a transaction type Fuel supports. Once again LPs provide liquidity for a fee.

Source: fuel.sh , Connext

EVM Compatibility and Dev Experience

DELPHI DIGITAL

zkSync - Zinc is a subset of Rust which is currently not EVM compatible or turing complete. Ability to support turing complete contracts including recursion in couple of months. Solidity transpiler, which takes solidity code and converts into Zync with very few modifications needed, is 90% complete. ETA 4-6 months.

Starkware - Cairo is turing complete and the language used for programming starks. All partner deployments will be written in Cairo. Bit of friction in onboarding here but network effects develop as dapps onboard (split proof costs).

Aztec - It enables programmable privacy with Noir, privacy contract language. Porting an app from L1 to the zkrollup would require writing the contract in Noir. zk-sync has slightly lower barrier to entry but Noir is starting to look more similar. As all Aztec transactions are zk Snark proofs, they can be bundled into one rollup.

Fuel - It has UTXO based execution model, more scalable than EVM. Generic smart contract support coming in V2. Optimizing for performance first, then smart contracts. Plan is for more sophisticated curves/computing than other rollups. Looking at a testnet w/o fraud proofs in Q1. Fuel are very early in their development cycle so it remains to be seen when the above will become reality.

Optimism - Turing complete / EVM compatible out of the gate. Easy deployment from L1 -> L2. Preserve the L1 dev experience by enabling easier portability of contracts, thanks to OVM an optimistic implementation of EVM.

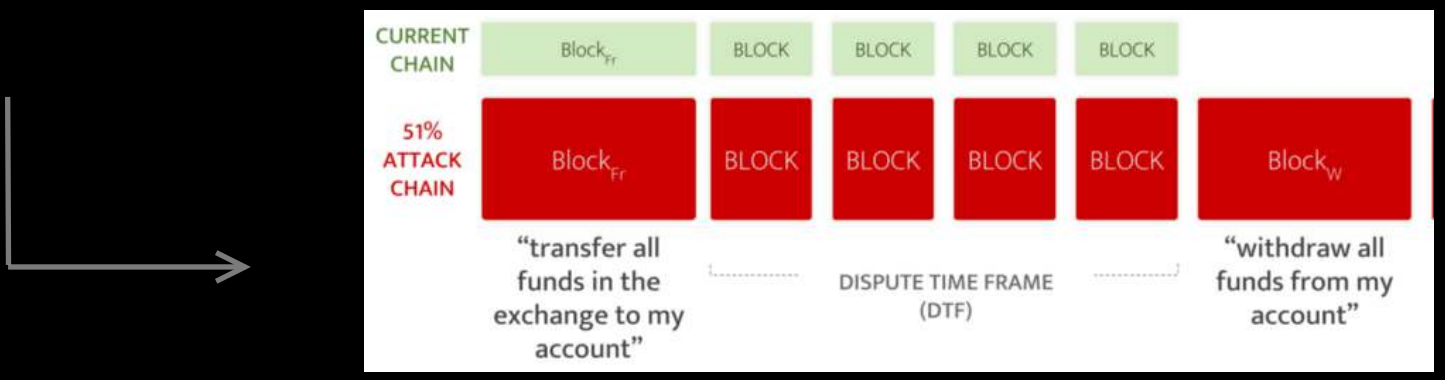
Arbitrum - Compared to Optimism, it's more compatible with tooling and accepts contracts directly. It's been developed to be compatible with the entire stack and lessen the load on developers.

Library support - Though Solidity is by all accounts problematic to work with, it has mature support in terms of tooling, SDKs and libraries. Cairo and Zinc may offer a more modern language to work with, they will be very new with limited support for the time being which may prove more frustrating than just writing in Solidity and transpiling over.

Security

Optimistic Rollups (Optimism):

- Fraud proofs rely on security assumptions in that an honest party will be able to ensure correctness and submit a fraud proof if necessary. They run into the dilemma between capital efficiency and security. **Improving capital efficiency decreases security.**
- The Dispute Time Delay of ~1 week is implemented to make a fraud+censorship attack more expensive. However, shortening this to improve capital efficiency and in turn lower LP fees, leads to weaker security.
- On top of this, they are susceptible to 51% attacks introducing the blockchain to a fraudulent state and attempting to steal funds from rollup. Example: A bad actor might try to introduce misaligned info and try to censor attempts to challenge it until the challenge period ends. In a shorter challenge period, funds are at more risk. Note that although 50m is widely viewed as an upper bound for ORU in terms of value locked with sufficient security, that number is not necessarily set in stone and can be larger.
- In an attack (below), if proofs are censored funds can be lost Remember that call data needs to be available to validate the chain.



Source: StarkWare

ZK Rollups:

- Note that with ZKR, users get the same security properties as layer 1, cryptographic functions aside. Think of it as "passive security" where nobody needs to do add on work to keep the system security. Capital can scale up on the rollup, and stored there securely. Other solutions require extra work from actors.
- Advantage with validity rollups is that they always reflect the correct state. The risk is the newer cryptography.

Validium (Another StarkWare offering)

- Given data availability is off-chain, this approach increases throughput but the trade-off is centralization where operators of Validium could freeze users' funds.
- In order to *steal* funds there'd need to be a 100% attack in Validium mode, not reliant on validator sets.

Additional Focus Points (1 of 2)

DELPHI DIGITAL

Proofs / Costs

In terms of throughput, you'll typically see ZKR outperform OR. Another factor to consider when it comes to specs is proof sizes. STARKs by StarkWare have the largest proof sizes but have fixed costs and higher throughput than SNARKs. Frequency of proofs can be determined by dapps who can choose to split fees as more join network. STARK provers are ~20x faster than SNARK provers. In zk-sync bulk of computation is from operations but done in specialized circuits, all combined recursively into a single proof. Although promising, recursion is still a nascent technique and more costly than STARKS. For optimistic rollups like Optimism fraud proofs are done only as needed, running full tx on chain leads to higher costs. Arbitrum splits costs of proofs across blocks.

Liquidity Fragmentation

As dApps and there userbases migrate over to L2s, there's the notion that liquidity will get fragmented across L1 and L2. **There's no clear, risk-free way and cheap way to pool liquidity across layers.** Market makers like Hummingbot can be integrated on L2 but note the re-balancing across layers that'd be needed. It'll also be difficult for aggregators themselves to leverage both L1 and L2 pools in a decentralized way and there's also frontrunning risk. Also in order for composability to emerge there needs to be sufficient liquidity. In the event of liquidity being fragmented across rollups and even Layer 1, solutions like Connext may gain more prominence.

Liquidity Mining

It's important to note that wherever the right incentives are put in place, liquidity will follow. Incentives can be thought of as ammo to re-direct adoption towards a desired target. Although this can be applied at the user level, it may make more sense to build up sufficient liquidity through incentivization of larger LPs/MMs first, but with care to weed out mercenary LPs & attract sticky capital.

Loopring has implemented withdrawal mining to reward users for holding in assets in self-custody, incentivizing withdrawals from centralized exchanges. The interesting thing about this program is the layered incentives you can add like scaling rewards based on participation amount or type of assets. In 4 days, they paid out to 903 accounts earning ~18% APY at the time holding $20m on L2. Same can be applied to self-custodial users, community governance can vote on parameters like size and duration.

Additional Focus Points (2 of 2)

DELPHI DIGITAL

Relationship with ETH 2.0

- Rollups take advantage of ETH 2.0 well before smart contract systems can. Rollups need high data throughput but don't need execution compared to smart contracts, hence why the earlier Phase 1 is better suited for rollups.
- **Applications adopting rollups today should be ability to easily adopt ETH 2.0 without many adjustments.** Simply put, if you are on a rollup, ecosystem will migrate on its own and everything will work BAU.
- Applications won't need to be developed natively for ETH 2.0 unless building a rollup itself. Dapps can start scaling with rollups.

L2 interactions w/ L1 Dapps

- The goal is to minimize how much interoperability (fund movement between environments) is needed between L1 /L2. Ideally, there'd be migration into a rollup able to support a subset of use cases. This way once apps are inside a rollup they operate smoothly similar to how they do on base layer and not lose composability. This is possible due to atomic transactions inside an L2 ecosystem.
- Note that to interact with L1, a message must be passed to it. **OR have a longer period given the security thresholds while ZKP on the other hand have better latency in the minutes.**
- OR can adapt for liquid tokens through paid services via external LPs but not for NFTs or calling arbitrary contracts (certain functions)

How adoption may play out

- The migration from Layer 1 to Layer 2 will likely be gradual given the nascency of the solutions and need to establish validation of the tech to gain user trust. On the other hand, Synthetix aims to be a quick mover, playing a leading role in driving adoption forward.
- A scenario is where DeFi protocols are deployed on Layer 1 and Layer 2 with the majority on L1 while experimenting begins with L2 as it's cheaper. Governance functions of protocols have a strong say in directing the gradual migration of liquidity to L2 (incentives could adjust based on liquidity ratio L1/L2).
- ZKR will be more convenient for those who may need liquidity back on L1 at times for rebalances to pursue opportunities like liquidity mining. Optimistic rollup, given it's more of a one way liquidity flow will likely have greater retention.
- **Naturally, already deployed dapps on L1 with userbases will be more difficult to fully migrate over. However, for new projects with a clean slate it'd be easier to focus on L2 from the start (Ex. Upcoming derivatives projects).** How this would work in practice is developers would build new projects still on the base layer and then port over.

Key Takeaways

dApps waiting for adoption of L2 solutions and maturity before making decision

- **Contrary to the market view, there is a greater level of indecisiveness amongst large dapps than what appears on the surface when it comes to choosing L2s**. The wait to see what others do mindset is present. However, in the event of a bull run and massive congestion, that may actually serve as a trigger towards moving sooner rather than later.

Difficulty in aggregating liquidity across Layer 1 and Layer 2 pools

- **It's infeasible to do so in a synchronous manner.** You can't have a token on 1 chain that represents an asset on chain 2. As a work-around, LPs could provide funds on both layers and communicate asynchronously, although there's front running risk. Re-balancing will play a key role here as well.

Power in the hands of LPs

- Taking Uniswap as an example, it can be easily re-deployed to a number of different rollups and doesn't require external oracles**. The leverage is in the hands of liquidity providers who decide where to put liquidity, and then users follow.** Rollup solutions can walk OTC providers through attack vectors as a part of decision making.

Interoperability problem emerges with liquidity fragmentation

- A common theme is rollups working on variations of conditional txs and fees to LPs to account for exits. There's no common standard and varying exit times throws interoperability off sync. Connext aims to solve for this.

ZK Rollups development is outpacing that of Optimistic Rollups

- **One of the biggest differences between the two, generic smart contract support and easy re-deployment from L1 to L2, is being solved.** If successfully de-risked, validity proofs may win on performance & security. Social coordination is key as well.

It will be difficult and take time to demonstrate composability on L2

- Composability on L1 AMMs is also enabled by deep liquidity, which is harder to re-produce on L2. Due to likely fragmentation, this means DEX aggregators plugging liquidity, flash loan arbridges and more, may be slow movers in relation to liquidity forming on L2 AMMs for example. Centralized market makers more likely to start off with L2.

Market Commentary (1 of 3)

To gain some further insights, we reached out to a number of teams in the L2 space

Why is your solution the best?

zkSync

zk-Sync is the best solution for scaling protocols on eth for the following reasons:

- Ultimate security on par with L1 (AMMs hold billions of value)
- Cheaper than OR (less onchain data)
- Plans for cryptographic frontrunning-resistance

STARKWARE

Core components of: StarkWare's platform,

- StarkEx, its scalability engine and Cairo, its framework and language for producing proofs for arbitrary computations

Benefits:

- Market validation: DeversiFi, and coming up are dYdX and Immutable's deployments
- over 50M tx settled on public testnets and mainnet. - The strongest, largest best capitalized zkp tech provider- Highest measured tps for Rollup on Ethereum Mainnet (3K tps, for Reddit scaling bakeoff), at 315 gas/tx. Demonstrated 9K tps on Mainnet
- No trusted setup, and tooling able to handle arbitrary computation (unlike competing ZKP solutions.- ethSTARK: fastest prover/verifier (open source under Apache 2.0), 20X faster than other systems, able to handle privacy needs too

What are the biggest misconceptions the market has about L2s?:

STARKWARE

1. OR: As long as you trust the operator, it is as secure as the base layer. ZK: It is as secure as the base layer, period
2. ZK-Rollups using the Turing-Complete Cairo are ready to handle any business logic today
3. Production-grade matters: The gap between a Tweet, Testnet, and a live system on Mainnet serving customers is substantial and hard to close

Market Commentary (2 of 3)

Loopring: Takeaways from a 1st Mover

As mentioned previously, we can learn from Loopring's takeaways that importance of UX and social coordination is just as if not more important than tech improvements.

- **Adoption**: Live for one year: 7k + users and 2m+ txs settled
- **Driver**: high performing orderbook DEX / payment dex (Gas-free, near instant)
- **Lesson learned:** Users hesitant on paying gas fee to create L2 account, pay more fees to deposit each asset to L2, and *then* benefit from gas free txs. Expose pros in better way
- **v.36 improvement:** Abstract away difficulties with meta txs, other design decisions -> Fewer and cheaper txs to get onboard
- **Insight**: **Make L2 environment very attractive, with great utility on there, for it to become a homebase for user**
- **Solution**: Loopring Wallet with zkRollup baked in. Users can spend lot of time in it: trades, swaps, transfers, provide liquidity, self-custodial
- **Changes**: Technical protocol improvements (v3.6), product improvements (wallet), working on UX improvements
- **Better pitch**: Cheap/ fast better verbiage than TPS. Focus is more on productizing and improving UX, than technicals

Oracle positioning & L2 Benefits?

" I think Chainlink will play a large role in the layer 2 space not only in providing external data to dApps on Rollups (like Synthetix when it launched on Optimism), but will also be directly powering layer 2 networks by operating the validators like in the case of Arbitrum Rollups, where the oracles aggregate transactions and submit fraud/validity proofs. This essentially provides developers a one-stop shop for all their smart contract needs. The main advantages of oracles on layer 2 is that they can update far more frequently due to the lower costs and higher throughput enabling more advanced use cases and higher leverage applications"

- ChainLinkGod

Do you plan to move to L2?

DODO

"As (a DEX), we are currently focusing on building our spot market offering, which consumes less gas than margin trade or derivatives platforms on the smart contract level. We've also implemented the gas optimistic feature, so our typical gas consumption is about 150,000, meaning that layer 2 is not a pressing need for the DODO platform."

- DODO is holding off for L2 solutions to emerge & mature

Market Commentary (3 of 3)

OFFCHAIN LABS | On the Optimistic Rollups side, we engaged with Arbitrum to hear from their vantage point as well.

For DeFi dApps looking to move to Layer 2, what are key design features to look out for when choosing amongst various L2 solutions?

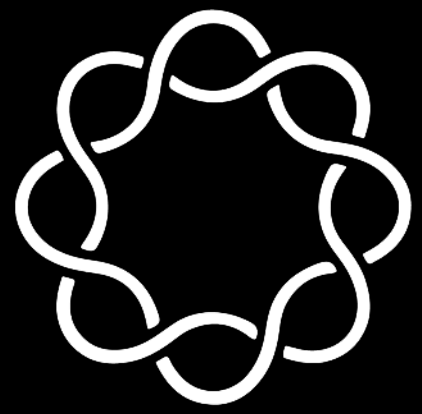
Developers will rightly focus on cost and security, but equally important is support for a thriving and diverse ecosystem that is welcoming to small and big projects alike.

Key questions to ask are: How easy is it to port apps? Is it compatible with existing tooling? Do developers have to rewrite their code? The L2 with the lowest friction for developers will get the most usage. A decision we made early on for Arbitrum is to focus on frictionless porting: no code changes are necessary and Arbitrum works with all Ethereum tooling. Arbitrum is currently the only EVM rollup with an open and public testnet that allows anyone to instantly and permissionlessly port their apps and benchmark their cost savings.

What would you define as successful 2021 for the rollup space and what are the key quantifiable metrics that can be used to measure this?

We expect 2021 to be a big year for rollup adoption. Arbitrum's mainnet launch will be the first open EVM-compatible rollup on Ethereum mainnet and will usher in this era. We anticipate an avalanche effect where once the first few dapps move over, others will quickly follow. Quantifiable metrics for success are: total liquidity in rollup chains, percentage of Ethereum's capacity that is being used for rollups, as well as the number and size of transactions processed on rollup chains.

A less quantifiable but equally important metric of success will be the growth of entirely new dApp categories that are priced out at today's L1 gas prices. We expect an explosion in blockchain gaming as well as retail DeFi (ReDeFi), or DeFi for lower-value trades that are currently priced out.



DELPHI DIGITAL

85 Broad Street
New York, NY, 10004
www.delphidigital.io