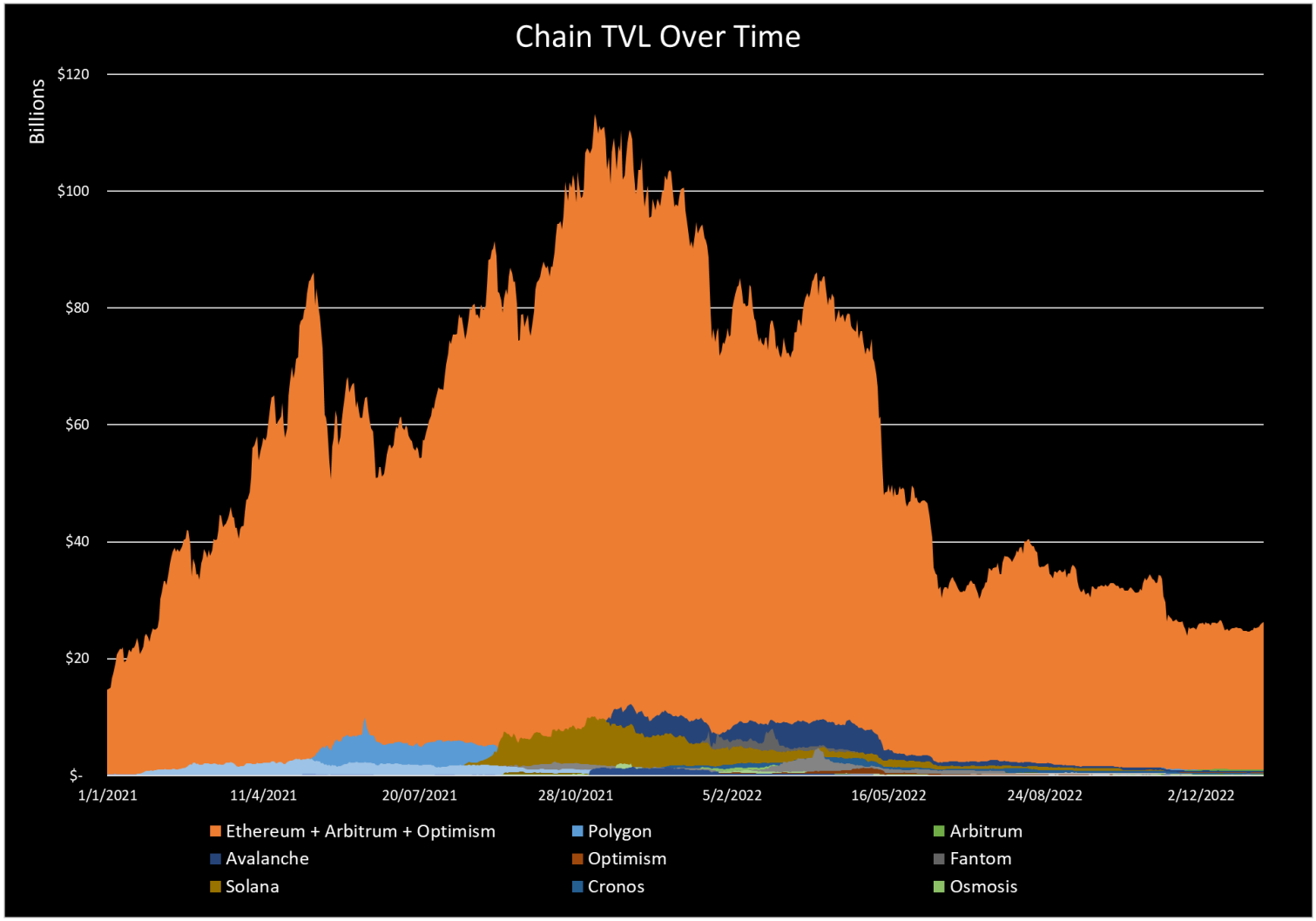
CRYPTO PRAGMATIST PRO

All views are solely my opinions. This is written exclusively for informational purposes. It is not an inducement to invest nor is it advice to follow any particular investment strategy. Data points are taken from various online sources that may or may not be accurate as of publication.

Intro

2021 was the year of the Alt-L1s, notably dubbed the ETH-killers. After network activity and TVL had been climbing up steadily into 2022, the abrupt implosion of crypto via Terra Luna, 3AC, and FTX proved the disarray of many of these shiny new networks. Now, we are back to an Ethereum dominated ecosystem:



DefiLlama

**Note: Tron and BSC are excluded to better visualize the rise and fall of the majority of other Alt-L1s. Tron and BSC adoption has been relatively persistent (although in a decline.)*

Despite this, the blockchain trilemma still exists, and different networks make different tradeoffs. Users will have different preferences based on their immediate needs which is why bridges need to exist: they allow **instant and cost-effective transfer** of assets from network to network.

Today, we will to look at:

- How bridges have evolved over time
- Why certain hacks occurred/what we can learn to avoid with bridges
- What the current bridging landscape looks like
- How the future of bridging will look with zkRollups and Layer 2s

The last point is especially important when looking at the Ethereum ecosystem today and how much attention is going towards these scaling solutions. As scaling evolves, the potential bridging protocols therein will also grow.

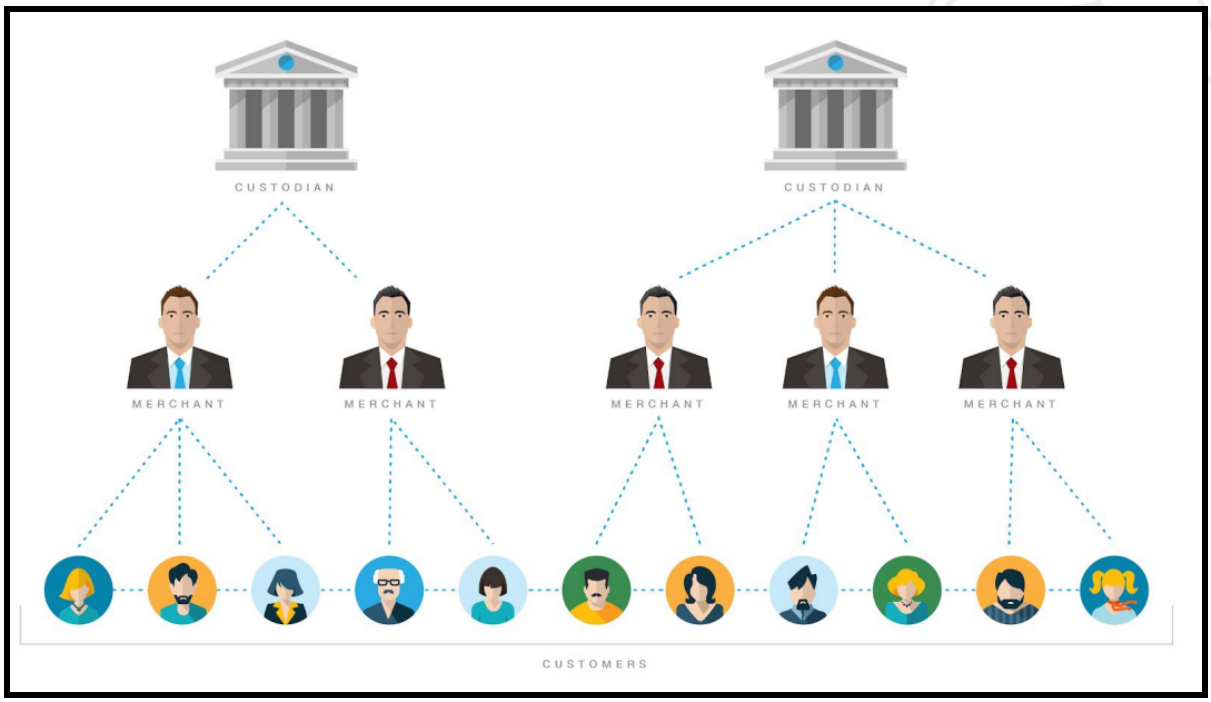
Wrapped Assets (Asset-Backed Coins) and wBTC

The first instance of bridging with Ethereum began with wrapped bitcoin. This simply allowed for users to bring their $BTC held in user owned wallets or exchanges to the Ethereum ecosystem as an ERC-20 token. The benefits here are quite apparent, some that come to mind:

1. Usability: As an ERC-20 token $wBTC can be used with smart contracts
2. Increase Transaction Speed: Ethereum blocks are created every ~15 seconds with finality in roughly 5 minutes, much faster than Bitcoin
3. Cross Asset Liquidity for $BTC: Somewhat under the umbrella of our first point, $wBTC as an ERC-20 allows for $wBTC / $token trading pairs, whereas most pairs were previously with $ETH

The beauty of wrapped bitcoin is in the simplicity. Users are able to easily verify the reserves, asset activity, and addresses associated with the creation and burning of $wBTC. In a way, this maximum transparency has allowed for the asset to become the largest “bridged” ERC-20 on Ethereum at a $3.2B market cap (although, it would be reasonable to compare it with Tether and USDC, which are much larger.)

One of the prevailing issues around this type of asset backed model is the layer of trust inherent to the creation of a wrapped asset. In $wBTC’s case, this centralization lies in the *custodian* role, solely held by BitGo. The architecture is as follows:



WBTC Whitepaper

And the roles pictured above:

- Custodian: Has the keys to mint $wBTC and holds the underlying $BTC (wallets here)
- Merchant: Dozens of entities where $wBTC will be minted to or burned from. Merchants receive $BTC from customers and initiate the minting of $wBTC (or takes $BTC from customer, initiates burn.)
- Customer: The end user and holders of $wBTC

A full list of the different entities can be viewed here. The concern regarding custody centralization can be better understood via the following threads, which look at parallels between BitGo, $wBTC, and FTX (and introduces the Ren/Alameda fiasco, which impacted competitor $renBTC):

Small Cap Scientist

For all intents and purposes, holding wrapped bitcoin is similar to holding assets on an exchange. Although BitGo is a *security focused* entity (unlike exchanges), there is still custody risk taken on by $wBTC holders. Additionally, the centralized entity of BitGo is subject to regulatory risks. The whitepaper is a great place to learn some more details on the actual minting process if you are exposed to $wBTC. And the impact of an unbacked $wBTC event, even if it is only a slight unbacking, would be catastrophic to DeFi as $wBTC is prevalent across numerous different chains and protocols. Nonetheless, the inception and growth of $wBTC marked an important moment: transactions of assets from *different networks* into the Ethereum ecosystem.

Ethereum Bridging Ecosystem Overview

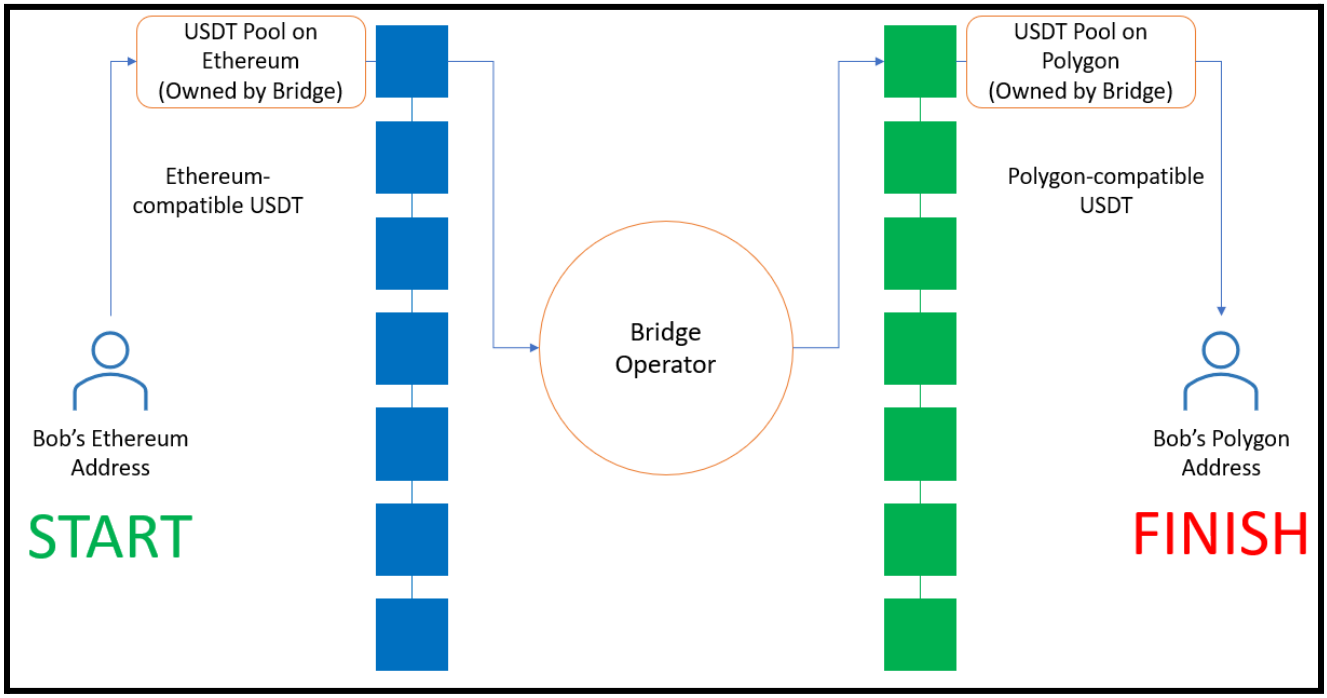
For the more “traditional” cases we think of when hearing the term bridge, competition is alive and strong: there are currently over 30 bridges and cross-chain liquidity protocols offering their services to Ethereum users. These bridges differ slightly from the architecture of wrapped $BTC, with the biggest difference being that the assets are stored in smart contracts on-chain, rather than held by a custodying entity.

There are three prevalent methods used to bridge assets from one protocol to another:

- Lock and Mint: Lock assets in smart contracts and mint equivalent assets on the destination chain. Minted tokens are thus backed by the locked asset.

- Burn and Mint: Similar to lock and mint, but burn the tokens on the source chain before the mint.
- Atomic Swap: Swap assets on the source chain with another user for their assets on the destination chain.

Sidechains, such as Polygon and Gnosis, most frequently use the **lock and mint procedure**. Users with assets on Ethereum can go to either Polygon Bridge or xDai to initiate a transfer of assets. Validators monitor the smart contracts, thus there is a reliance on both validator uptime and good-faith acting:



Amber Group

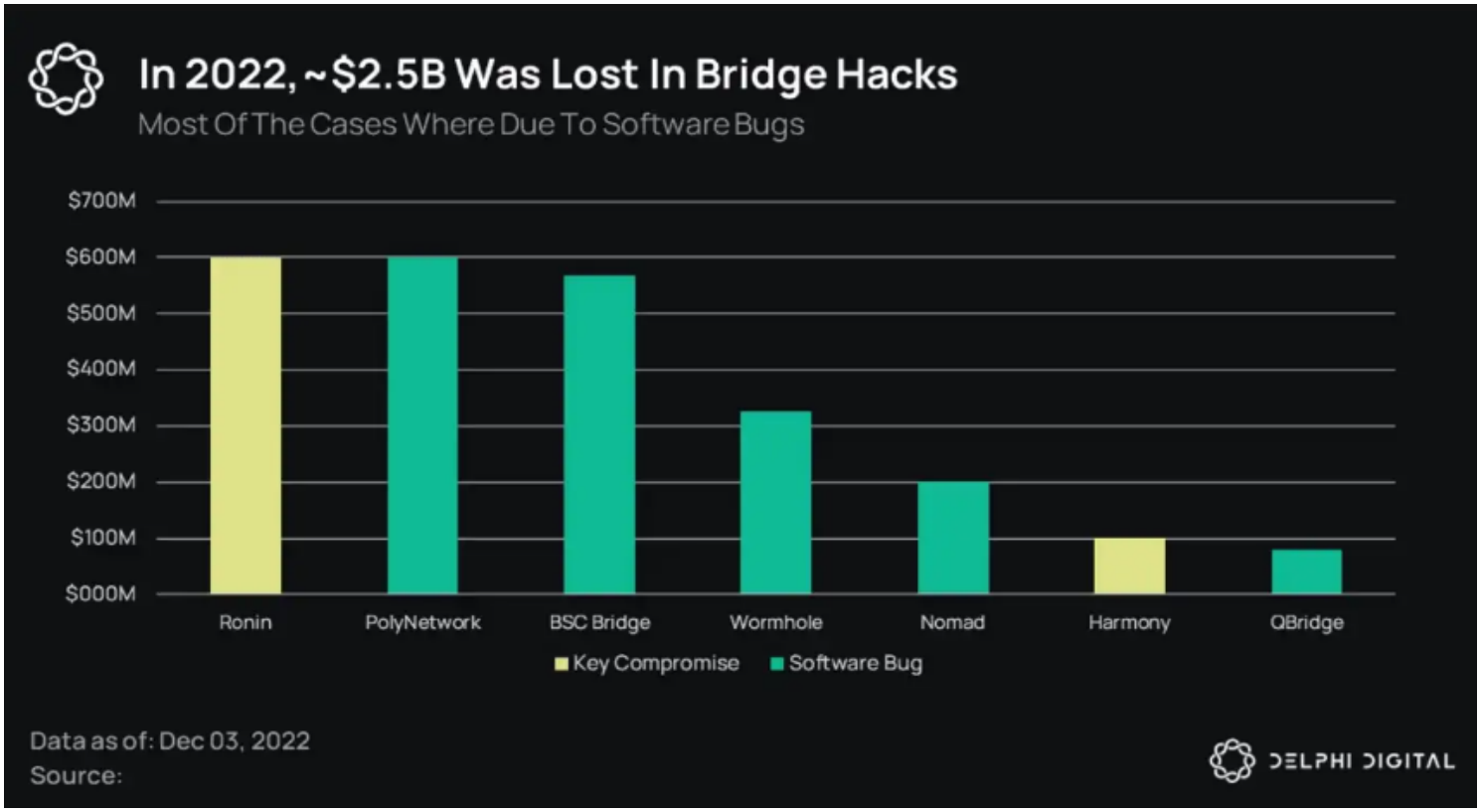
To understand the vulnerabilities that lie in trusting this type of validator setup, we can look at a simple case with the Ronin Bridge, which connects Ethereum to the Ronin sidechain that hosted all activity for Axie Infinity.

Sky Mavis, the game developer, held keys to 4 of the 9 validators responsible for monitoring and approving asset transfers on the bridge. In a phishing attack, hackers were able to steal the keys of 5 validators and approve withdrawals from the bridge without redeeming the necessary assets. The total stolen from this hack was roughly **$625 million**, the largest theft in crypto's history. This left users with worthless assets held on the Ronin network, as there is no way to redeem them back onto Ethereum.

This brings us to the deep topic of previous bridge hacks, which make up an overwhelming majority of the cybercrime in crypto markets.

Hacks and Exploits
On top of the Ronin/Axie bridge exploit, some of the other top bridge hacks were:

1. **Poly Network ($600 million)**: Hacker was able to reset themselves to be the keeper, giving them control over all of the funds on the bridge. Most funds were returned/frozen.
2. **Wormhole Bridge ($320 million)**: Hacker was able to arbitrarily mint 120k $ETH tokens. Jump Capital famously stepped in to plug the hole.
3. **Nomad Bridge ($190 million)**: Hackers were able to simply find a valid withdrawal transaction and input the destination address as their own to drain the bridge.
4. **Binance Bridge ($566 million)**: Hacker had created a transaction to register as a relayer for the BSC Token Hub, then minted 2m $BNB tokens. A swift response (shutting down the chain) by Binance reduced the actual lost amount to $100m.
5. **Horizon Bridge ($100 million)**: Private keys were compromised in a *two of four* multisig verification setup, and the hackers could simply walk away with the assets in the bridge.



Delphi Research

This is not an exhaustive list, but you get the point. These 9 figure hacks simply demonstrate that a “cross-chain universe” has extreme security concerns. This is exactly why Vitalik brought this discussion to the table, outlining why he believed in a multi-chain future, but not a *cross-chain* future. The summary is simple: keep your tokens on their native chain.

If I bridge $ETH to Solana, and the Ethereum state reverts that transaction due to an attack, the $solETH (Ether on Solana network) will be insufficiently backed. Under his original tweet announcing the blog post, we found this gem of a thought:

Vitalik Buterin

He is essentially saying that a cross-chain/interoperable ecosystem is fine with a network like Polkadot, where the “relay chain” is the zone of sovereignty, where many interdependent L1s (parachains) can run on top of. If Polkadot were to get attacked, all parachains would be affected by the revert that would occur on the relay chain. And of course there is the Cosmos IBC, which utilizes an intermediary banking system to facilitate the transfer of fungible assets between two IBC enabled chains. And it works: with >$600m worth of transfers on nearly 5.5m transactions in the past 30d, IBC activity is strong.

Things can go wrong, however, with the clawback of Evmos airdrop accidentally pulling from the IBC banking module, leaving $EVMOS holders unable to transfer their tokens before this was remediated.

The history of the above hacks does not mean that everything covered in today’s report is useless. As mentioned in the intro, there is still a world of blockchains with different advantages and disadvantages, and bridges allow users to seamlessly pick and choose where they want to play around. The current bridging technology is still nascent, there are just some questions of security that we need to be aware of.

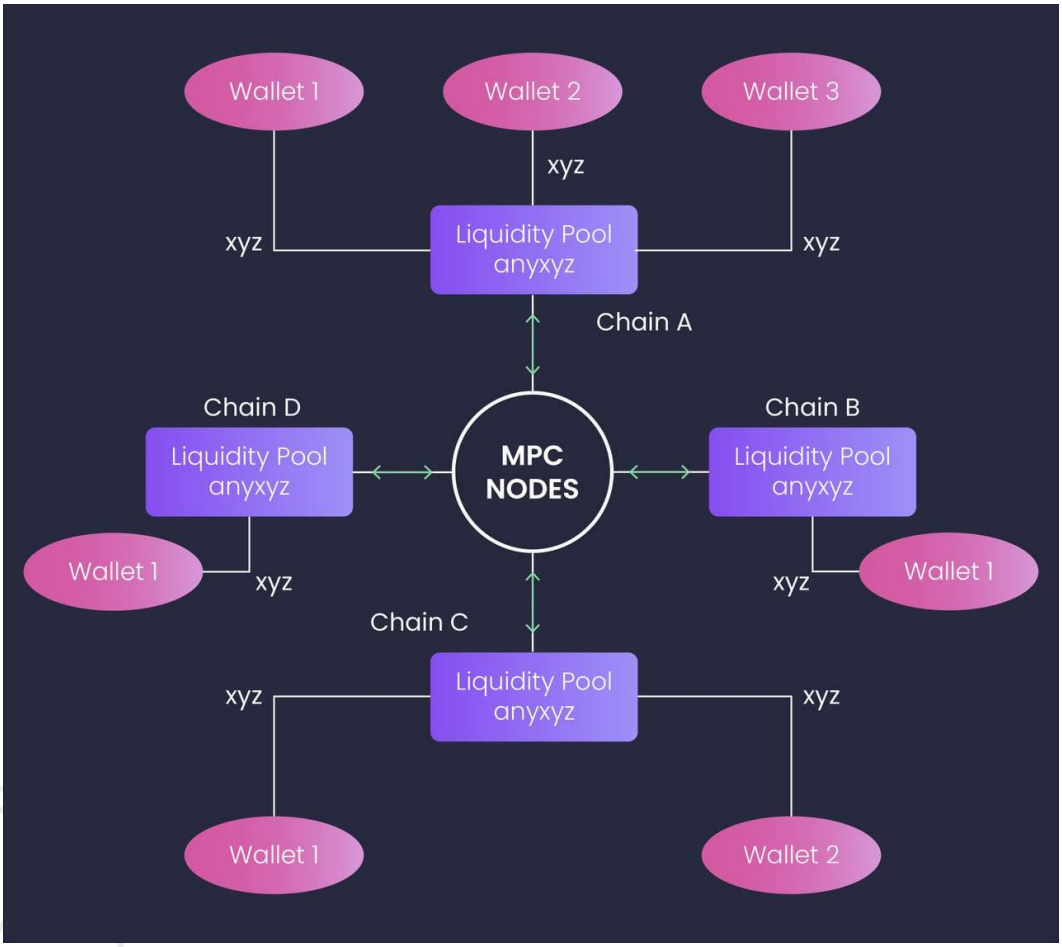
Are the hacks predictable? Not really, otherwise there wouldn’t be such large sums of crypto constantly exposed to getting rugged by the next genius hacker team. But, there are always steps we can take to ensure that we are not one of the people who suddenly goes to withdraw our tokens and *poof,* they’re gone.

- Look at the decentralization of the validator/guardian set. Ronin would've drawn some *serious* red flags in this case.
- The bridge has sufficient bug bounties in place.
- The contracts were audited by a reputable firm.

These are non-negotiables, but even then, there is some danger in using non-native assets on a chain. The conclusion is that these validator/guardian structured bridges *rely on a certain party(ies)*, and any time that is the case, our assets are exposed to significant risks. Here are some popular bridges that have managed to a) not get hacked and b) maintain a significant TVL through the previously mentioned hacks and current bear market:

1. Multichain
2. Synapse
3. Thorchain

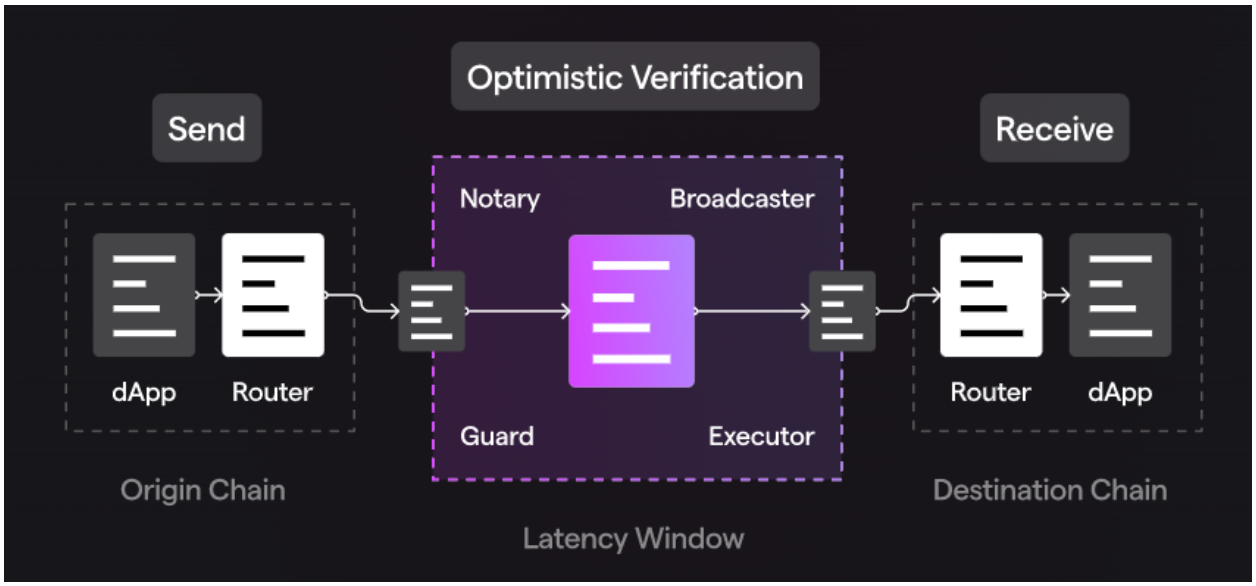
These three all use different methods to attempt to achieve cross chain messaging, aka bridging. First up is **Multichain**. As we covered in [our post] long, long ago, Multichain uses an intermediate asset in order to satisfy immediate liquidity needs if there is not enough readily available in the current pools:



Multichain Docs

This is great for cheap and quick swaps if you need it and can move assets into a native asset once on the destination chain, but providing liquidity here is almost asking for something to go wrong. Why? The security assumptions are similar to Wormhole and Ronin: there are validators watching with multi-sig verification. It is a great sign that nothing has gone wrong, and the protocol works very well, but providing liquidity should be avoided.

Synapse, which was the first bridge to launch its own chain, utilizes a mix of economic and optimistic security. Much like an optimistic rollup that we've discussed before, this just relies on one good actor to flag a fraudulent transaction in the dispute period. Similar to Multichain as well, there are synthetic assets that are backed by a liquidity pool in the bridge ($nUSD and $nETH):



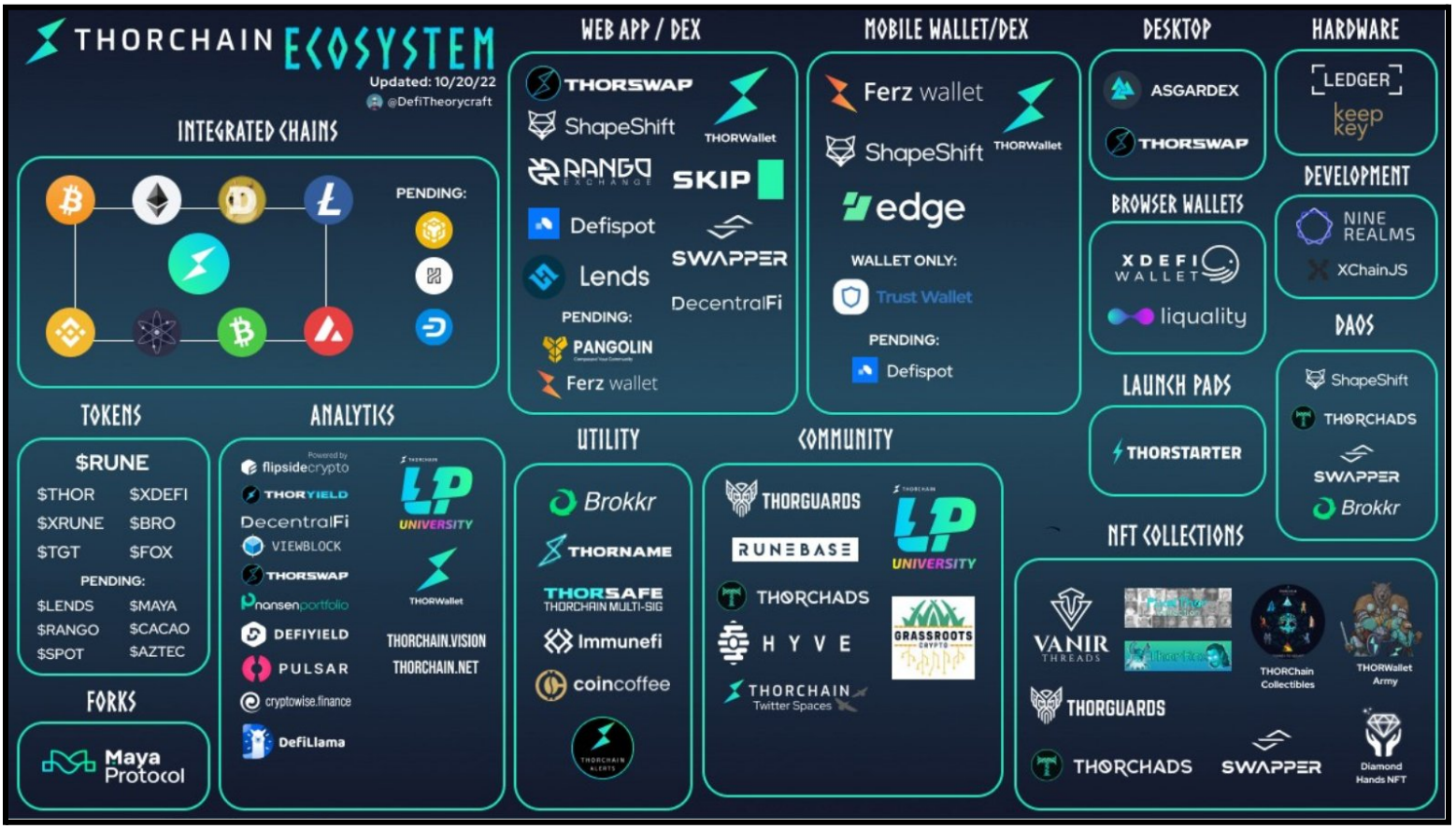
Synapse

In order for the message to get passed, the "notary" actor is responsible for running a full node on supported chains in order to verify the messages being passed. The other roles can be read about in the docs, and it is important to know that collusion between any of these parties is possible. But the optimistic setup allows for anyone to watch for fraudulent activity, which hopefully deters collusion ($SYN stake would be slashed) and sets up a reliable last line of defense.

Stargate, the bridge by LayerZero Labs, uses a similar structure, but we will leave that for its own section.

Finally, **Thorchain** taps into the economic guarantees of staking. By utilizing an intermediary chain, users swapping from $BTC to $ETH technically pass through the Thorchian on their way. Though this is beneficial in the sense that it can use an independent set of validators subject to economic slashing conditions, it is required that validators run *full nodes* on supported chains in order to be able to see and pass transactions through.

Thorchain is one of the more unique bridging solutions out there, and this can be confirmed with the fact that protocol TVL just surpassed the level that it was pre-FTX crash, which in and of itself make it a strong standout. Add on the ever growing Thor ecosystem and they have a strong (cultish) community of support:



Twitter

So, given they all have quite different models of security and UX, why have they all been relatively successful? For starters, we know that marketing initiatives, community building, and opportune timing are all relevant and can help differentiate protocols. Multichain and Synapse were able to provide cheap and efficient transfers during 2021 when everyone was moving from chain to chain, and it has been proven that a lot of this liquidity is sticky.

Initiatives to continue to develop and improve the bridge as new situations arise is also a recipe for success, Synapse shows this with their announcement of the Synapse Chain to help create a new method of token transferring.

LayerZero/Stargate

Stargate was easily one of the most hyped token ICOs of last cycle, when Sam Trabucco infamously tweeted “we did indeed buy all the tokens”. It has since fallen to just above its ICO price of $.25, which are locked for a full year starting March 18th 2022, and a 6 month linear

vest thereafter. Looks like the once 12x profit will not be much help to remediate the balance sheet of Alameda when it's all said and done:

CoinGecko

This chart proves that the token hype cycle for $STG was mainly centered around early farming of the pools that help enable the cross chain liquidity. One of the issues with this **atomic swap** method that Stargate uses is the liquidity required on both chains, which is why the farming incentives were initially so high: to help bootstrap the massive liquidity needed. Another risk is that chance timing can leave one side of the bridge's pool relatively empty, leaving some users with the short end of the stick.

Stargate has an oracle-relayer architecture that creates a pseudo light-client on the supported chains, but at a much cheaper cost because it is not required to run 24/7. Currently, LayerZero uses permissioned, off-chain parties in order to facilitate transfers, but over time they want to change this.

The downside here are assumptions that the oracle and relayer are independent, which is likely not always the case. L2Beat recently released a report on why this assumption is flawed and relies on applications to inherit their own security measures, or oracle–relayer pair. Where this gets especially interesting is with EigenLayer, which we cover briefly below.

While LayerZero/Stargate bridge are not perfect, there is at least a path forward into how it would be viable, which is promising. Hyperlane proposes a similar solution, where app developers will be able to design their security assumptions the way they want.

Layer 2 Growth: A Strong Catalyst for Bridges
Layer 2 bridges, such as Arbitrum and Optimism, require that all transaction batches are posted to Ethereum mainnet. This means that when moving to and from Ethereum to the Layer 2 network, you are essentially just initiating a transfer on Ethereum mainnet. The dispute period of 7 days to verify the transactions, however, leaves an undesirable user experience. This is obviously another reason why bridges remain such a crucial component in crypto today and crypto in the future.

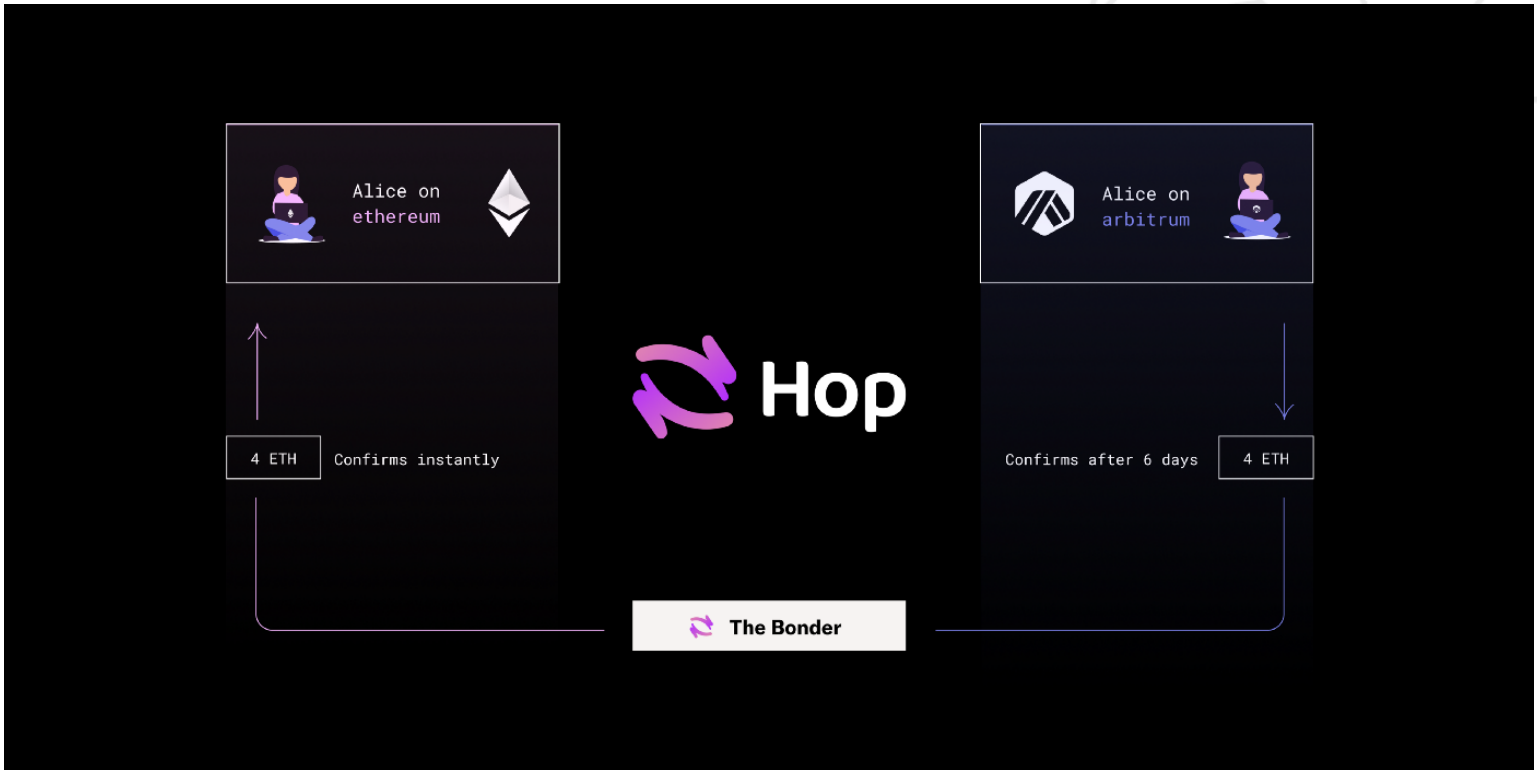
One of the protocols that has been enjoying this upside in Layer 2 activity? Hop exchange. Since its lowest TVL in early October, it has increased by more than 50%:

Defillama

Hop allows for cross chain transfers solely focused on Layer 2 networks within the Ethereum ecosystem. Based on the framework Vitalik outlined above and what we took away from all the hacks that took place, this seems to fit in nicely for the longer term (here Vitalik and Hop dev have a discussion on the viability of this bridge style.)

There are still “intermediary” tokens issued in the process of bridging, but you get a native asset on the destination chain after going through the bridging process. **Bonders** hold an important role, which are the ones who put up their capital up front and help service immediate transfer of assets while waiting for the normal withdrawal period to go through to Ethereum mainnet.

Right now, bonders are permissioned by $HOP governance, but they never have access to user funds. Even if all bonders go offline, you would simply be able to claim your bridged $ETH back on Ethereum mainnet after the dispute period:

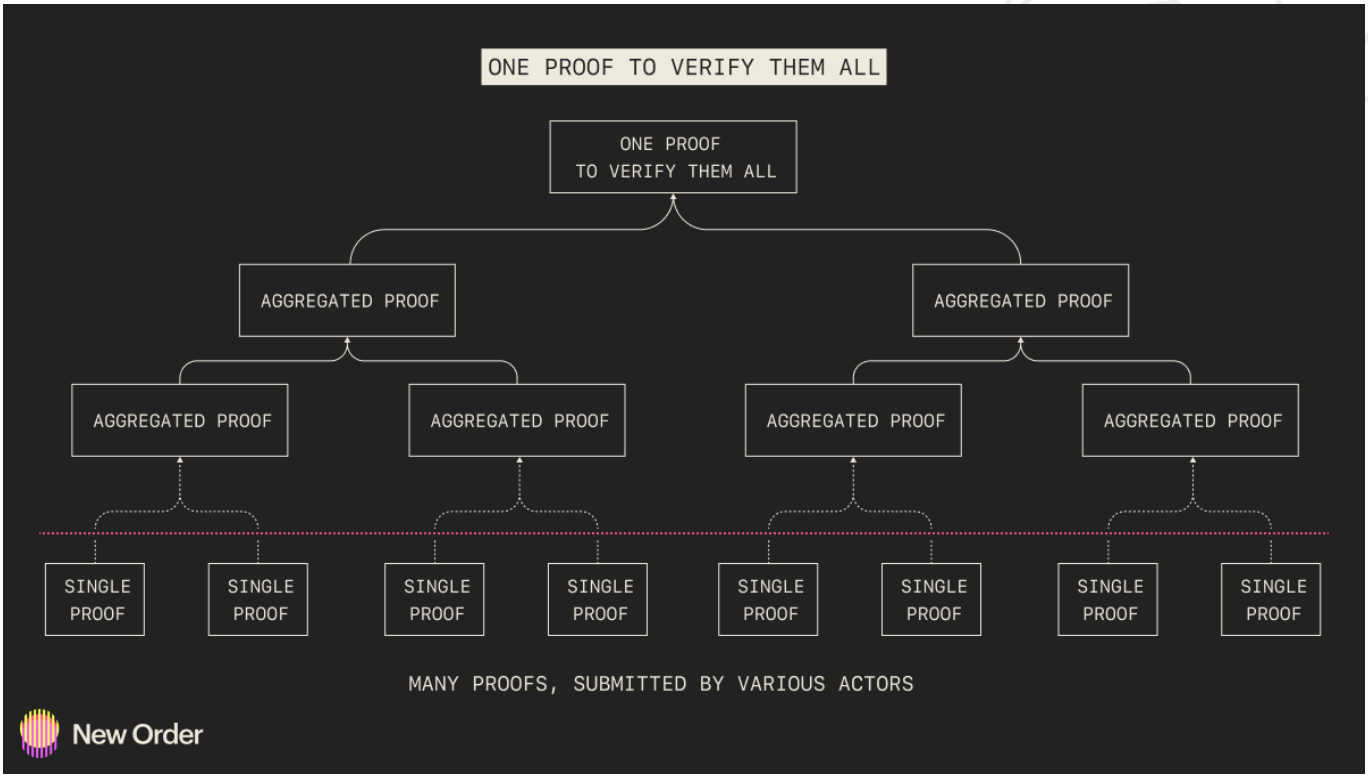


Bonders enable immediate transfer

As for the $HOP token, the 60% of it is still in the treasury, incentivizing people to deposit into the liquidity pools (token incentives account for >80% of rewards for most pools.) With team token allocation beginning to vest midway through 2023, it is probably best to steer clear of $HOP for the time being. But we see the bridge is absolutely a cost effective, economically and architecturally secure method to swap between Layer 2s.

ZK Proofs and the Future of Bridging (Math Based Bridges)

As we covered in our previous report, the development of ZK rollup chains is complex, specifically due to proof generation time being computationally intensive and compromising the level of decentralization. The good news is that ZK proofs, the mathematical verification of transactions, can be used in their current state. Development teams for Polymer, zkBridge, and SuccinctLabs are the merging of ZK technology and bridging forward with succinct proof generation. With this, transactions will be verified by a prover off-chain, with the proof then being confirmed on the source chain. Costs can be reduced and multiple light client computations batched into a single ZK proof using recursive ZK technology:



New Order DAO

In the context of zkBridge, anyone can freely join the network to relay block headers, generate proofs, and claim rewards for being involved. The issue, as we know, is that only select parties will have the computational power required to generate the proofs, so there *is* some upper limit on decentralization *as it stands today.*

The other benefits for this kind of bridging approach, outlined by zkCollective, are:

1. **Trustless and Secure:** As long as the on-chain light clients are secure and there is one honest node in the relay network.
2. **Extensible:** Applications can easily see the verified block headers, allowing for a stack of apps to be built on top of the bridge.
3. **Universal:** As long as a light client is supported, the relayer network and proof scheme of zkBridge can be applied to any PoS network.
4. **Efficient:** Recursive proofs allow for quick and cheap verification.

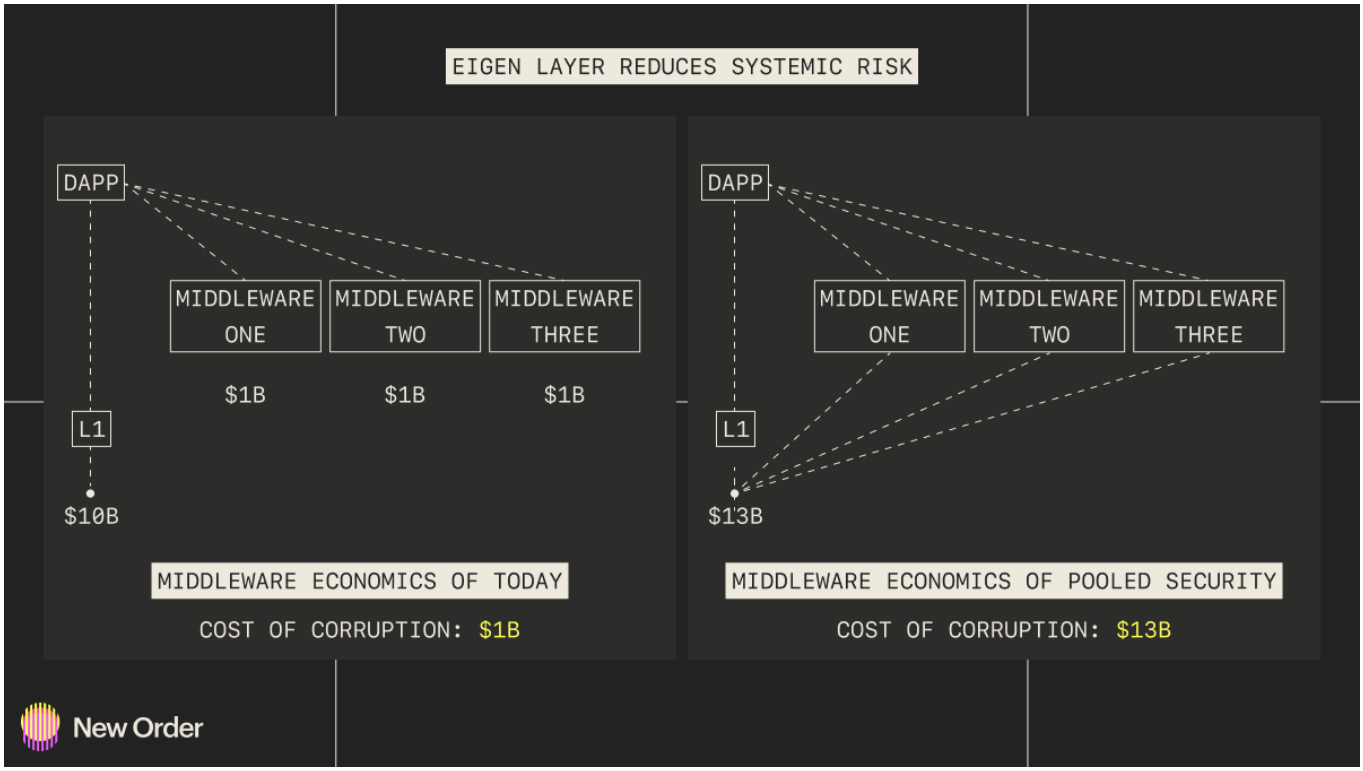
Much like the Cosmos IBC allows any IBC enabled network to easily run a light-client of another chain, this type of succinct proof creates a similar approach for EVM chains.

How EigenLayer Fits into the Picture

Eigenlayer is going to be a big development in the Ethereum network this year. In Q1 they have plans to start launching on testnets, and current schedule is planned for a late summer deployment to mainnet Ethereum. The beginning impact will likely be slow as the security

concerns for validators and protocols will be high, but it seems pretty safe to assume at some point in 2023 we will start to see in practice how big an impact this technology will have.

Eigenlayer allows for Ethereum beacon chain validators to redirect their staking withdrawal address to Eigen's smart contracts. By doing this, validators are subjecting their 32 $ETH to additional slashing conditions outlined by a given protocol (oracle, bridge, RPC node, etc.) The benefit here is additional security for protocols that would otherwise have to issue a token and bootstrap their own security, which would *never* be as robust as Ethereum's:



New Order DAO 2023 Outlook

The cost of corruption for protocols that utilize restaked $ETH is 51% of the value of staked $ETH. So as the price or the amount of staked Ether increases, these middleware services utilizing Eigen smart contracts will also improve their security. Here is a comprehensive thread with additional resources to learn more about Eigenlayer.

Bridges would be some of the most useful protocols to capitalize on the additional security of restaked $ETH. Because we have outlined the risk/importance of having a decentralized validator set in a bridging protocol, having additional economic guarantees for a cross-chain communication network will only improve its robustness.

But, the extra slashing conditions are obviously a concern, and MeirBank mentions a good point that liveness requirements will be a big consideration for nodes that might re-stake their $ETH with Eigen.

MeirBank

Eigenlayer is an exciting development to look for in the latter half of this year, but like the ZK-tech, it is not going to be realized in the immediate future.

Conclusion

The history of bridge hacks only solidifies that cross-chain communication is complicated and a long way away from being fully solved. Even though many of these hacks are old news of the past bull market, we can still look back on them as lessons and learn what to expect from the future.

Currently, the Layer 2 hype is accelerating fast as the leading narrative in early 2023. With many different chains attempting to optimize for different reasons:

- Aztec for privacy
- Arbitrum Nova for gaming and social focused applications
- Polygon's suite of rollups
- Celestia as a modular data availability layer

The list goes on and on, and the link between all of these protocols is **secure and trustless bridging**. Although we are not deep in the mathematical weeds at Crypto Pragmatist, it makes most sense to us that the ZK proof secured bridging solutions would be the optimal bridging solution from a security perspective. But that is still a ways away, and before we get there there will likely be convincing developments elsewhere.

Some of the questions that we are eager to answer and will be looking into over the next few months:

- How will real world assets be incorporated on-chain?
- What will NFT bridging look like across Ethereum L2s?
- How can we ensure that pooled assets for multichain bridges are not such a hot target for hacks?

Further Reading

[What I talk about when I talk about bridges - 0xJim]
[Ethereum is changing - Nicholas Pai]
[Bridge design tradeoffs - Amber Group]
[Optimistic Bridges - Connext]