Enigma Research Note. April 5, 2022

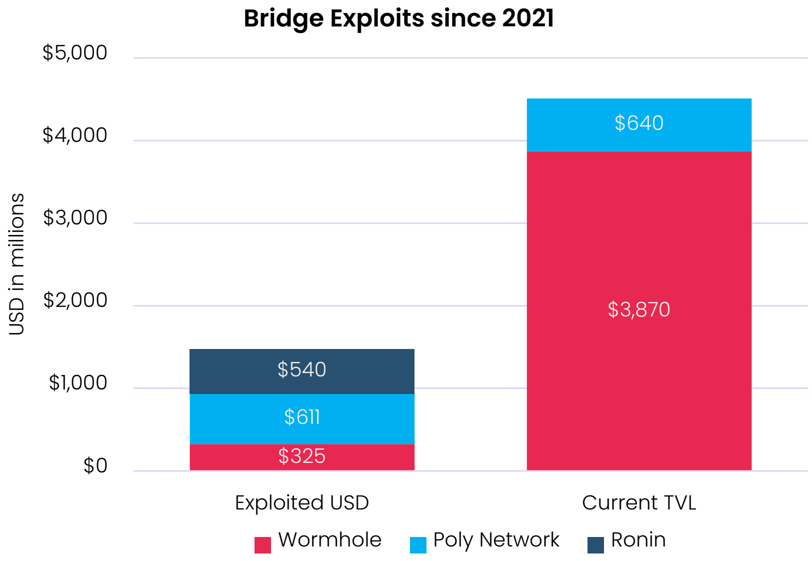
Bridges, You Are the Weakest Link

- TYPE: Cross-Chain Bridges, Interoperability
- MARKET CAP: $549 BILLION
- TVL: $34.7 BILLION

Centralized Vulnerabilities

Cross-chain bridge attacks validate the blockchain trilemma. The network theory states that resources limit a sufficiently distributed system's optimization to two of three goals: scalability, decentralization, and security. As a type of distributed system, the theory may very well constrain even the most well-designed blockchains to two of the three. While several Layer-1 networks attempt to disprove the trilemma, cross-chain bridge vulnerabilities support the theory to the tune of $1.5B value exploited over the last year.

The attacked bridges all resemble third-party applications that use independent consensus to move the assets through the bridge between each blockchain. While their validators may cryptographically validate the bridge's state, the validators are only as strong as the most vulnerable member. If private keys control a validator its security depends on the physical security of those keys. Private key security that relies on humans is no more secure than legacy infrastructure, like a password.



Currently at Stake

The interoperability landscape holds roughly $35B, or nearly 2% of value on-chain. Across all bridge applications, excluding the Ronin bridge, TVL grew 52% on average over the last month alone. Digital asset users are clamoring to use their favorite apps and tokens unconstrained by digital geography. Unfortunately, cross-chain transactions proliferate risk across networks.

Cross-Chain Bridges by TVL & Market Cap

USD in millions

Name	Symbol	TVL, USD	Ch 7D	Ch 30D	Mkt Cap, USD	MC/TVL
WBTC	WBTC	$12,650	-2.1%	24.1%	$12,830	1.0x
Multichain	MULTI	$6,580	2.3%	-5.8%	$257	0.0x
Stargate	STG	$4,020	11.2%	0.0%	-	-
Wormhole	-	$3,870	7.6%	0.0%	-	-
hBTC	hBTC	$1,830	-2.4%	20.3%	$1,883	1.0x
Terra Bridge	-	$1,430	14.5%	0.0%	-	-
JustCryptos	JST	$1,390	-1.8%	22.2%	$533	0.4x
RenVM	REN	$1,310	-7.8%	13.6%	$456	0.3x
Synapse	SYN	$821	7.7%	10.1%	$562	0.7x
ChainPort	-	$241	9.7%	50.2%	-	-
Allbridge	ABR	$226	-1.1%	-22.4%	$5	0.0x
ioTube	-	$146	8.1%	606.0%	-	-
Wrapped BNb	-	$134	1.7%	24.8%	-	-
RelayChain	RELAY	$46	-15.2%	86.9%	$4	0.1x
Octus Bridge	-	$32	-3.7%	17.4%	-	-
Hyphen	-	$18	5.4%	0.0%	-	-
deBridge	-	$4	31.7%	72.0%	-	-
Strudel Finance	TRDL	$1	-2.5%	20.3%	-	-
Total		$34,750			$16,531	

Source: DeFi Llama, CoinGecko

Take last week's Ronin Network Bridge announcement. Human control over a validator set contradicts distributed ledger security benefits. By 29 March, a Ronin Newsletter post announced that an attacker stole 173.6k ETH and 25.5M USDC from five of the nine total Ronin Network validators. Early stages of the ongoing investigation revealed that attackers used social engineering techniques to withdraw the assets with private keys. According to the updated post, Sky Mavis keys retained delegated signature authority from November 2021 when The Axie DAO provided temporary signature permission to the Sky Mavis keys to conduct an airdrop to a booming network. Because the permissions were not revoked, the four Sky Mavis validators could sign transactions on behalf of the five Axie DAO validators to control the bridge.

As of 4/2/22, the Ronin Network and assets on the Ronin blockchain were secure. All Sky Mavis validators were replaced, with plans to add new validators to the network. The Ronin newsletter noted that the "root cause of [their] attack was the small validator set which made it much easier to compromise the network." However, no more details from the ongoing investigation were available. The Ronin Network Bridge and conversion between Ronin WETH and ETH remained closed.

The Ronin Bridge attack demonstrates the risk of centralized network control. While economic activity grew exponentially, network security failed to keep pace. From a security perspective, the centralized and cross-permissioned vulnerability reduced the network's validator count from nine to four, because the four Sky Mavis keys could access the five Axie DAO keys. Control over all value locked in the bridge at any time only required four of the nine validators.

Potential Solutions

Algorand State Proofs, or ASP, offer a bridge solution that relies on each network's existing consensus and security system. A user locks (deposits) their assets in a smart contract on their home network. The ASP app sends a message to the destination smart contract on the destination network. The message contains a cryptographically verified zero-knowledge proof of the Algorand network at transfer. With the proof, the destination mints corresponding tokens directly to the recipient's wallet. The ASP assures the assets remain locked because it provides a snapshot of Algorand's network consensus and state.

A zero-knowledge proof generally creates a message that proves to the recipient that the sender knows secret information without revealing the information itself. StarkWare offers a suite of zk-powered Layer 1 and 2 scalability and interoperability solutions that also seek to eliminate reliance on trusted third-party applications. As a bridge solution, StarkEx zk-proofs allow asset transfers among separate blockchains without an intermediary. Senders lock their assets in the departing StarkEx app, which sends the user's signature and a state proof to the StarkEx app on the destination network. Like ASP, StarkEx bridges the assets verified by each network's existing security and consensus.

The bar for potential solutions is low: a safer interoperability project need only add no additional risk to its constituent networks. The latest bridge attacks exploited weaknesses that each bridge introduced to the system. The most recent bridge attacks demonstrate that attackers will target the weakest point in the system. Any transaction requires a degree of trust among the parties. Each additional trusted party represents new risks. Reliable and secure interoperability solutions will eliminate third-party risk and improve communication among networks. These trustless bridges will improve at the pace of blockchain development because they rely on each blockchain's security protocol.

DISCLAIMER

This document has been prepared by Enigma Securities Ltd. in cooperation with members of the Makor Group ("or the "Makor Group") including Makor Securities London Limited, Oscar Gruss Son, Inc. and Enigma Securities Limited. This document is intended for institutional investors and is not subject to all the independence and disclosure standards applicable to research reports prepared for retail investors. This information represents neither an offer to buy or sell any security or cryptocurrency nor, because it does not take into account the differing nee ds of individual clients, investment advice. Trading cryptocurrency and related instruments carries a high level of risk and may not be suitable for all investors. Those seeking investment advice specific to their financial profiles and goals should contact their Makor Group representative. Makor believes this information to be reliable, but no representation is made as to accuracy or completeness. This information does not analyze every material fact concerning a company, industry, security, or cryptocurrency. Makor assumes that this information will be read in conjunction with other publicly available data. Matters discussed here are subject to change without notice. There can be no assurance that reliance on the information contained here will produce profitable results.

A security or other instrument denominated in a foreign currency is subject to fluctuations in currency exchange rates, which may have an adverse effect on the value of the security or instrument upon the conversion into local currency of dividends, interest, or sales proceeds. Makor trades, and will continue to trade, the securities covered in this document on a discretionary basis on behalf of certain clients. Such trading interests may be contrary to or entered into in advance of this document.