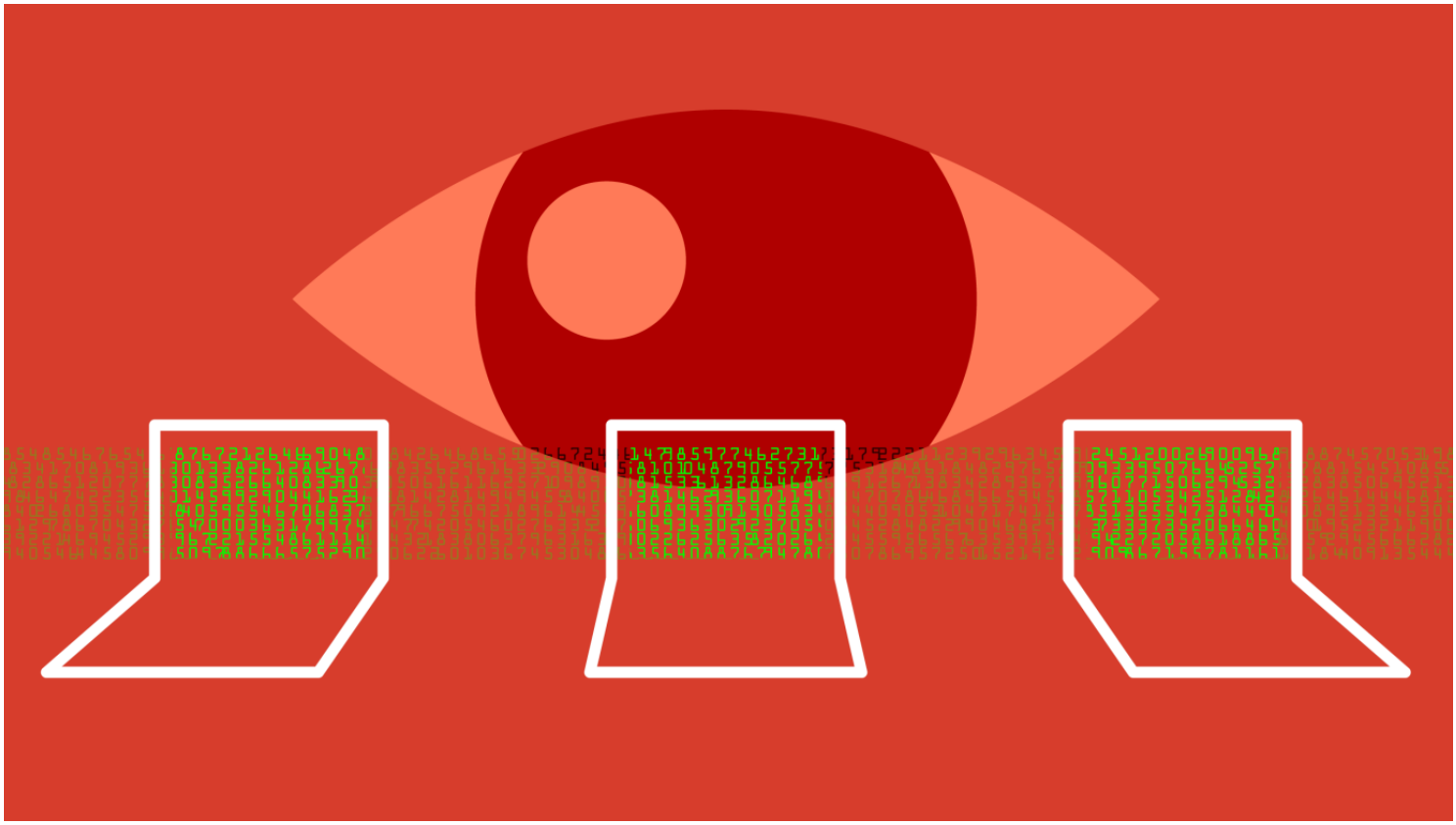
+ Market Analysis

Wormhole digs out of its hole with new security measures to move on from $320M hack

The protocol plans to add more core contributing teams by the end of the year

Jacquelyn Melinek
@jacqmelinek / 10:30 AM CDT • July 27, 2023



any projects and companies would simply give up if they'd been hacked and had hundreds of millions stolen from their ecosystem partners, but it appears Wormhole isn't one of them.

Last year, an attacker exploited a vulnerability in the Wormhole liquidity bridge between the Ethereum and Solana blockchains and stole about 120,000 wrapped ether, worth about $223 million today. A bridge, like the name suggests, facilitates transactions between different chains.

Shortly after the hack, Jump Crypto tweeted it was replacing the massive chunk of ether stolen to "make community members whole" because it saw Wormhole as "essential infrastructure" for the future's multi-chain world.

Almost a year-and-a-half later, the cross-chain crypto bridging and messaging protocol seems intent on learning from its mistakes and making a comeback.

Since the hack, the company has stepped up its security, launched two $2.5 million bug bounty programs, and had a handful of third-party firms do a number of audits to resolve critical issues. The company has paid out several bounties, and by the end of the year, plans to add three core contributing teams that will be "building in various capacities," Dan Reecer, head of operations at Wormhole Foundation, told TechCrunch+.

The company has finalized four teams so far and will potentially add one more, Reecer added. These teams will focus on building messaging protocols, zero-knowledge technology, business development, front end tools, blockchain tools and

more. “It’s skill-dependent and we’re bringing teams that have [these different] components,” he said.

Wormhole also became one of two bridging protocols chosen by the Uniswap DAO for its cross-chain messaging after a study found the bridge fulfilled the necessary security requirements, according to Uniswap’s Bridge Assessment report.

The approval stems from the number of validators, including “reputable entities,” as well as “significant improvements” in response to its exploit in February 2022, the report added. However, the report identified some areas for improvement and “recommends periodic monitoring for any material changes that may affect the protocol’s security profile.”

Summing all that up: While Wormhole has indeed stepped up and improved its security around the protocol, there are still risks and concerns for its validators in the way the protocol bridges transfer messages and tokens.

But why did it take an exploit for Wormhole to ramp up its security efforts?

Reecer said he couldn’t comment on why Wormhole didn’t implement these measures before, as he joined the team only a few months ago, but he did note that security is always going to be one of the biggest priorities for the company.

“Maybe people didn’t realize at the time [of the hack] how important this was,” he added.

Big efforts, small potatoes

Wormhole was, and still is, one of the biggest bridging protocols, so you’d expect a company of its size to have good enough security practices and regular audits to ensure major hacks don’t happen. The fact that it took such a big hack for Wormhole to take a good hard look at its security protocols is telling of how little such projects, stretched as they are for resources, focus on security.

To be fair, it’s not uncommon for bridges to suffer from exploits, given how technical and risky the process is. Some bridges are trying to change the way they transact to reduce the potential “honey pots” or pools of funds that are targeted by hackers.

Historically, bridges have used token wrapping, which involves locking up a cryptocurrency and then minting it on another chain. However, that creates a pool of tokens that can be targeted by hackers. New bridging technology tries to mitigate that risk by burning tokens and minting new ones on the subsequent chains.

“At a high level, bridging protocols, even DeFi protocols, see [security] incidents happen on a frequent basis, and it proves, especially in an open source world, that these vulnerabilities are virtually unavoidable,” Reecer said. These protocols have to plan for hacks and have the right security measures in place as well as “fallback plans for when these things happen.”

Since 2021, there have been 18 major bridge hacks, with the Ronin network’s $625 million exploit in March 2022 being the largest, according to De.Fi Rekt data. Wormhole’s bridge exploit was the third-largest bridge hack to date. In total $2.16 billion has been lost from bridging hacks, the data showed.

In general, it’s hard to tell if hacks are less frequent now, said Carlos Domingo, founder and CEO of digital assets security firm Securitize. “I assume it’s getting better, but as the industry gets bigger, you’re going to see more hacks.”

That would make sense. As more money enters the ecosystem, the greater the opportunities for bad actors to make a quick buck by finding vulnerabilities.

Hacks happen every single month in this space, according Ronghui Gu, CEO and co-founder of security-focused auditing firm CertiK. “If one bridge gets hacked, that’s something other bridges will realize and they have to pay more attention,” he said.

But Gu pointed out that the security level of crypto projects has improved dramatically in the past few years. Before the decentralized finance wave, or “DeFi Summer,” in 2020, most projects only did audits to launch tokens, Gu said. “Now, I’d say most projects are audited.”

It’s fair to assume that blockchains, smart contracts and other highly technical crypto products and platforms will continue to get more secure as they’re refined and battle tested. That said, nothing is 100% foolproof. It’s also important to remember that whenever a system gets an upgrade or a new feature, it adds potential for exploits if it’s not audited and checked properly.

“It’s so important for crypto projects to continue auditing so there are no holes in their smart contracts,” Domingo said. “Protocols like Uniswap and Aave have never been hacked, and they transact with more volume than Wormhole or other ones. Some people are good at keeping it secure and some aren’t.”

“If you want to do things the right way, there’s ways to do it properly. Don’t rush to release anything, make sure smart contracts are audited, and review the code to make sure there’s no holes,” he added.

Reecer seems to have the biggest takeaway from Wormhole’s experience: “Plan for [hacks] to happen. If you think it can happen, it will happen.”

In crypto, the stakes are high and incentives for hackers are even higher given how much capital flows in the industry and how young and shaky the technology can be.

“There’s still lots of space to improve,” Gu said. “Many projects want to do code audits but not audit the whole space because it’s very expensive, so they only want to do it with the core part. But different parts work closely, so any single point missing in a loop can cause a problem. Only auditing the core part is not enough.”

It’s important to have multiple levels and layers of security, so if something goes wrong, it’s limited to a small amount stolen instead of cascading to massive amounts, Reecer added.

But Reecer is optimistic that the technology will improve with time. “We’re still at a point where bridging protocols are at an early stage, and this infrastructure has to be laid down.”

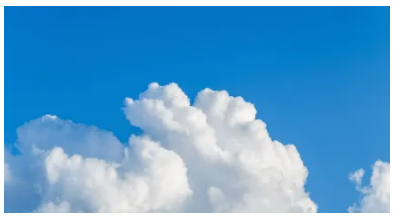
More TechCrunch

Tags

crypto EC Blockchain EC Cryptocurrency EC Cybersecurity exploits hacks security Wormhole

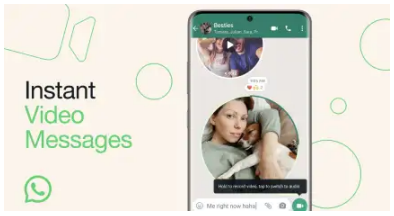
Bluesky sends some users personalized apologies after racism controversy

Morgan Sung
10:30 AM CDT • July 27, 2023



WhatsApp now lets you record and share short video messages directly in chats

Aisha Malik
9:57 AM CDT • July 27, 2023



Mastodon is launching merch to help fund its development efforts

Sarah Perez
9:53 AM CDT • July 27, 2023

Peacock lags behind competitors, gains just 2M subs for Q2

Lauren Forristal
9:52 AM CDT • July 27, 2023

Cash-strapped instant delivery giant Getir, trying to close funding, pulls out of Spain, Italy and Portugal

Ingrid Lunden
9:10 AM CDT • July 27, 2023

Helpful secures $7.5M to launch family caregiver app

Christine Hall
9:01 AM CDT • July 27, 2023

Hackers are infecting Call of Duty players with a self-spreading malware

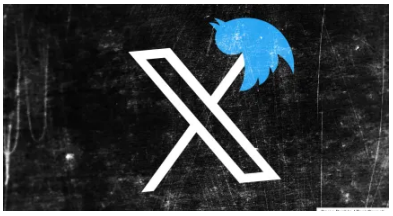
Lorenzo Franceschi-Bicchierai
8:41 AM CDT • July 27, 2023

Coalition Operators, Cowboy Ventures and Finix set an equitable cap table at TC Disrupt 2023

Lauren Simonds
8:30 AM CDT • July 27, 2023

Ex-Twitter Blue chief on Musk's 'lack of process' and impulsive management style

Ivan Mehta
8:02 AM CDT • July 27, 2023

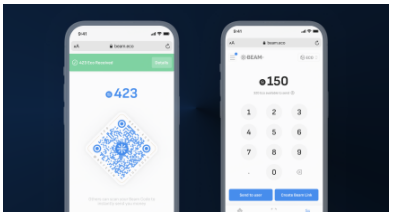


Photoshop's new generative AI feature lets you 'uncrop' images

Kyle Wiggers
8:00 AM CDT • July 27, 2023

a16z-backed Eco unveils Beam, a P2P crypto transfer service aiming to be a 'global Venmo'

Rita Liao
8:00 AM CDT • July 27, 2023



TC+ Fundraising

Flipturn hauls in $4.5M seed funding to help trucking fleets electrify for less

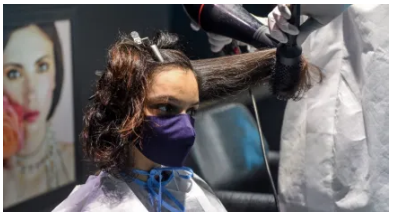
Tim De Chant
8:00 AM CDT • July 27, 2023

US government contractor says MOVEit hackers accessed health data of 'at least' 8 million individuals

Carly Page
7:10 AM CDT • July 27, 2023

GlossGenius raises $28M to expand its bookings and payments platform for beauty businesses

Kyle Wiggers
7:00 AM CDT • July 27, 2023



Previous governments' incompetence crippled India's semiconductor growth, deputy IT minister says

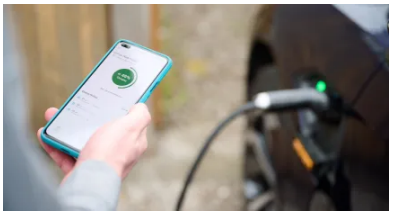
Manish Singh
6:50 AM CDT • July 27, 2023

EU opens competition probe of Microsoft bundling Teams with Office 365

Natasha Lomas
6:29 AM CDT • July 27, 2023

TC+ Fundraising

EV.energy snags $33M Series B to help utilities save billions on grid upgrades



Tim De Chant
5:35 AM CDT • July 27, 2023

Upgrade acquires travel-focused BNPL startup Uplift for a song

Kyle Wiggers
5:00 AM CDT • July 27, 2023

Patently messy: How a $6B deal may spur more IP lawsuits

Paul Sawers
5:00 AM CDT • July 27, 2023