

Blockchain Security Outlook 2021

Featuring 2021s major DeFi & NFT exploits,
security measures & Key Web3.0 Trends for
2022

Contents

Here We're!	1
Yearn Finance - 2021s first major DeFi Hack	3
Alpha Finance Exploit	4
The Paid Network Hack	5
Uranium Finance Exploit	6
The Spartan Protocol Hack	7
The Rari Capital Hack	7
The PancakeBunny Protocol Hack	9
PolyBunny Finance Hack	10
The Belt Finance Hack	10
The Bondly Finance Hack	12
The Thorchain Hack	12
The Popsicle Finance Hack	13
The Poly Network Hack - "the elephant in the room."	15
DAO Maker Exploit	15
Indexed Finance Hack	16
PancakeHunny Hack	17
The Cream Finance Hack	18
Vulcan Forged Hack	18
Squid Game Token Crash	19
BitMart Hack	20
Key takeaways from the 2021 Crypto & DeFi Hacks & Scams	21
2021 was a record-breaker for zero-day hacking attacks	21
2022 and the future of DeFi	23
3 Web3.0 Predictions For 2022	26
How Web2.0 Companies Can Join the Web3.0 Revolution	27
Role of Smart Contracts in Creating a Secure Decentralized Ecosystem	28
In the End!	29
References	29
About QuillAudits	29



Here We're!

When we decided to spread awareness about DeFi and NFT hacks last year, we have then come up with twitter threads featuring post mortem analysis of those hacks and exploits.

But the frequency of scams kept on rising, with millions and millions of dollars taken away by the fraudsters. Then, to cover up those hacks and spread awareness among stakeholders, we have started publishing a weekly newsletter ('HashingBits'). Still, as if that wasn't enough to slow down the rising bar of hacks and scams, the exploits in this segment kept on continuing (this time, targets were voluminous!).

This report summarizes (of course compilation of all the hacks and their analysis would have made it bulkier!) all the major DeFi and NFT hacks, along with some interesting insights to venture into the Web3 ecosystem.

Before we begin exploring the Blockchain on the security front, here are some words on Decentralized Finance (DeFi) -

DeFi is being considered as the new face of finance. Showcasing an unrealistic growth over the past few years, DeFi has attracted millions of people, offering better investment opportunities, higher returns, transparency, and unmatched trust. In the long run, DeFi is bound to become a mainstream system for accessing financial services.

However, as every coin has two sides, DeFi is moving towards a disastrous future because of the potential risks that remain unnoticed across the industry. A proper understanding of these risks is essential to define the path for a better, secured future for the world of finance.

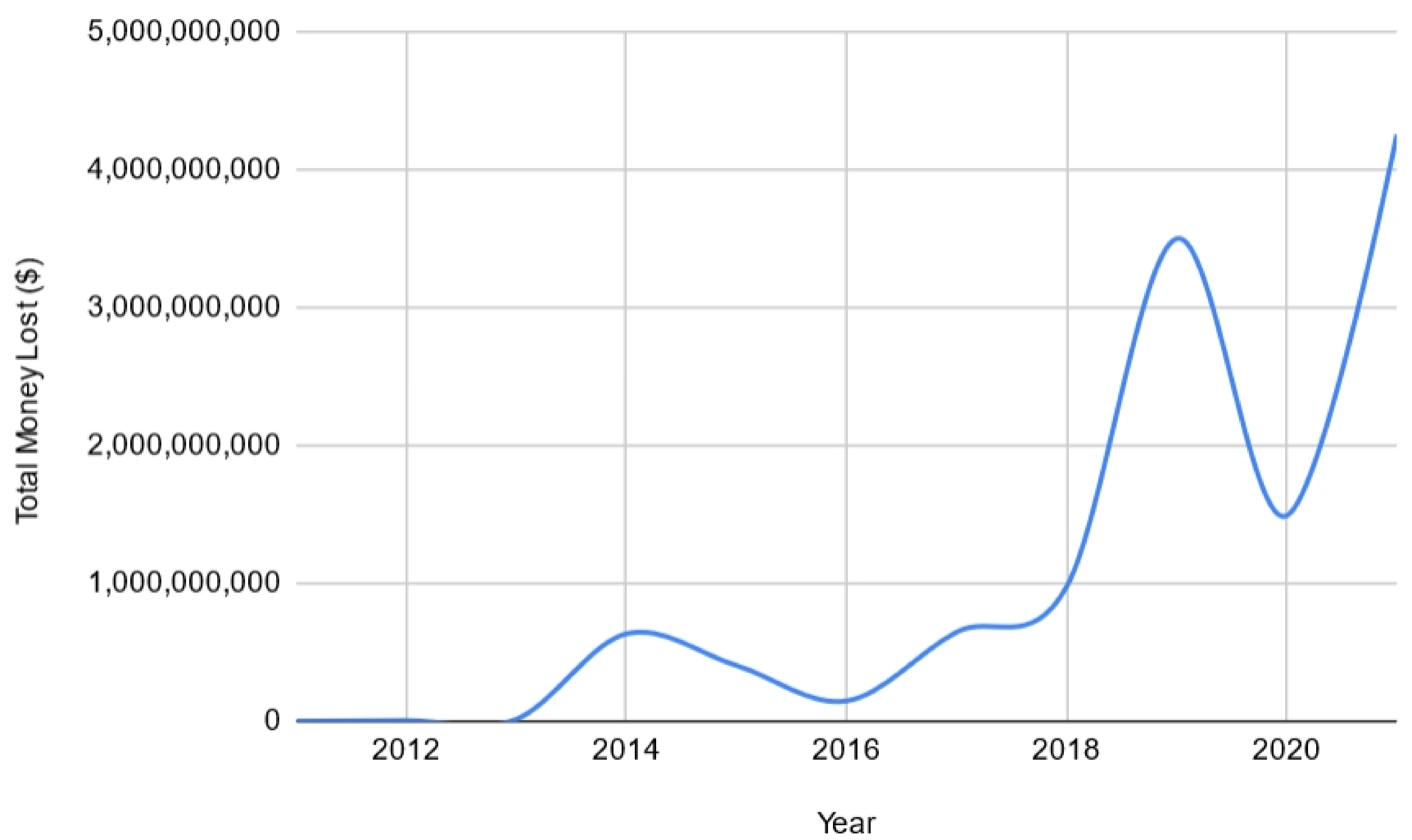
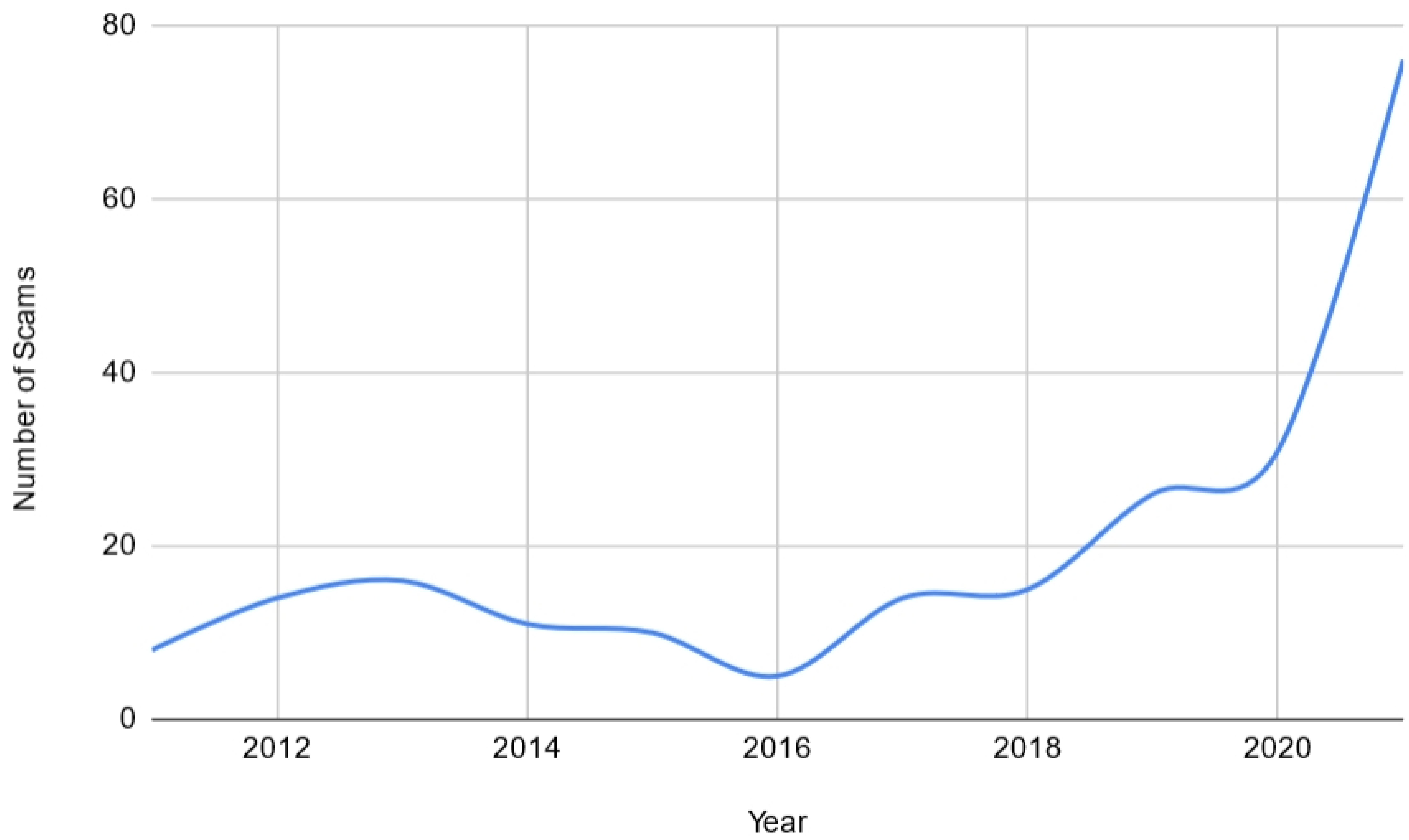
In this report, we take a glance at the existing DeFi market and how it has been affected over the years due to the negligence of risks associated with it, and then we discuss the different possible attacks on DeFi protocols as well as a few of the methods that can ensure greater security in the DeFi ecosystem.

It should be noted that there are several other risks associated with the DeFi ecosystem that is not included in this report. Threats such as economic incentive risk, financial illiteracy risk, and regulatory risk require an expert's opinion.

Moreover, as DeFi is still in a nascent stage, there is a high probability that more risks will arise over time as DeFi evolves further. Therefore, a business in the DeFi space needs to constantly touch with the ever-changing trends of the DeFi ecosystem and continuously evaluate the new possible risks.



Crypto Breaches Over the Years



To Begin With...

In the past, we have posted multiple twitter threads comprised of the DeFi/NFT hacks and their analysis. But in the forthcoming sections (of course that's our primary objective), we have tried to explain the various major exploits and it's cause and technical pitfalls (or the key actors) behind them!

As we already have put down the gross amounts for the losses incurred (for the whole year as well as individual hacks), you can keep away the calculators & comfortably have a go-through!

YEARN FINANCE - 2021s first major DeFi Hack

Yearn.finance is a group of protocols running on the Ethereum blockchain that allows users to optimize their earnings on crypto assets through lending and trading services.

Total Loss - \$11M

Cause - As for the reason of the attack, yearn.finance reports that a confluence of three factors led to the vulnerability.

1. The hacked vault's slippage protection was set too loose at 1%.
2. The normal 0.5% withdrawal fee was charged to 0% to encourage migrations to v2 vaults without incurring costs.
3. This being a v1 vault, the exploiter was able to call `earn()` and push deposits into the vault's strategy at will.

Technical Analysis

The attacker used flash loans to borrow 116K Ether from the margin trading platform dYdX and 99K from Aave's lending platform.

They were then able to use 215K ETH, worth ~\$342M, as collateral to borrow 134M USDC and 129M DAI from the lending platform, Compound Finance.

› From dYdX: Solo Margin To 0x62494b3ed96633... For 116,918.301246079787520826 (\$187,591,906.80)  Wrapped Ethe... (WETH)
› From Aave: aWETH Token... To 0x62494b3ed96633... For 100,701.209262451858593301 (\$161,572,069.23)  Wrapped Ethe... (WETH)
› From Compound Ether To 0x62494b3ed96633... For 10,862,976.92127864 (\$346,311,704.25)  Compound Eth... (cETH)
› From Compound Dai To 0x62494b3ed96633... For 130,081,210.716250884645322752 (\$129,385,016.08)  Dai Stableco... (DAI)
› From Compound USD Coin To 0x62494b3ed96633... For 134,000,000 (\$133,231,644.00)  USD Coin (USDC)

The attacker then added all of the borrowed USDC and 36M of the borrowed DAI to Curve Finance's 3-token USDC/DAI/USDT pool. They then withdrew 165M USDT from the Curve pool.

› From 0x0000000000000000... To 0x62494b3ed96633... For 169,207,181.762470641006750353  Curve.fi DAI... (3Crv)
› From 0x62494b3ed96633... To 0x0000000000000000... For 167,544,699.904197864576917996  Curve.fi DAI... (3Crv)
› From Curve.fi: DAI/USDC/... To 0x62494b3ed96633... For 166,203,625.544857 (\$165,320,918.09)  Tether USD (USDT)

Then the attacker repeated the strategy of depositing the remaining 93M DAI, borrowed from Compound into Yearn's yDAI vault, adding the 165M USDT back into the Curve 3-token stablecoin pool (3pool), withdrawing 92M DAI from the yDAI vault, then removing the 165M USDT again from the Curve pool



Each time the hacker executed the repeating part of the strategy, they gained more Curve's DAO Token, which they later converted to stablecoins, eventually netting them \$2.8M, and losing Yearn's vault, for whose deposits are now disabled, \$11M.

ALPHA FINANCE EXPLOIT

Alpha Finance Lab is focused on innovating the decentralized finance (DeFi) space. It is building an ecosystem of DeFi products that will interoperate to maximize returns while minimizing risks for users.

Total Loss - \$37.5M

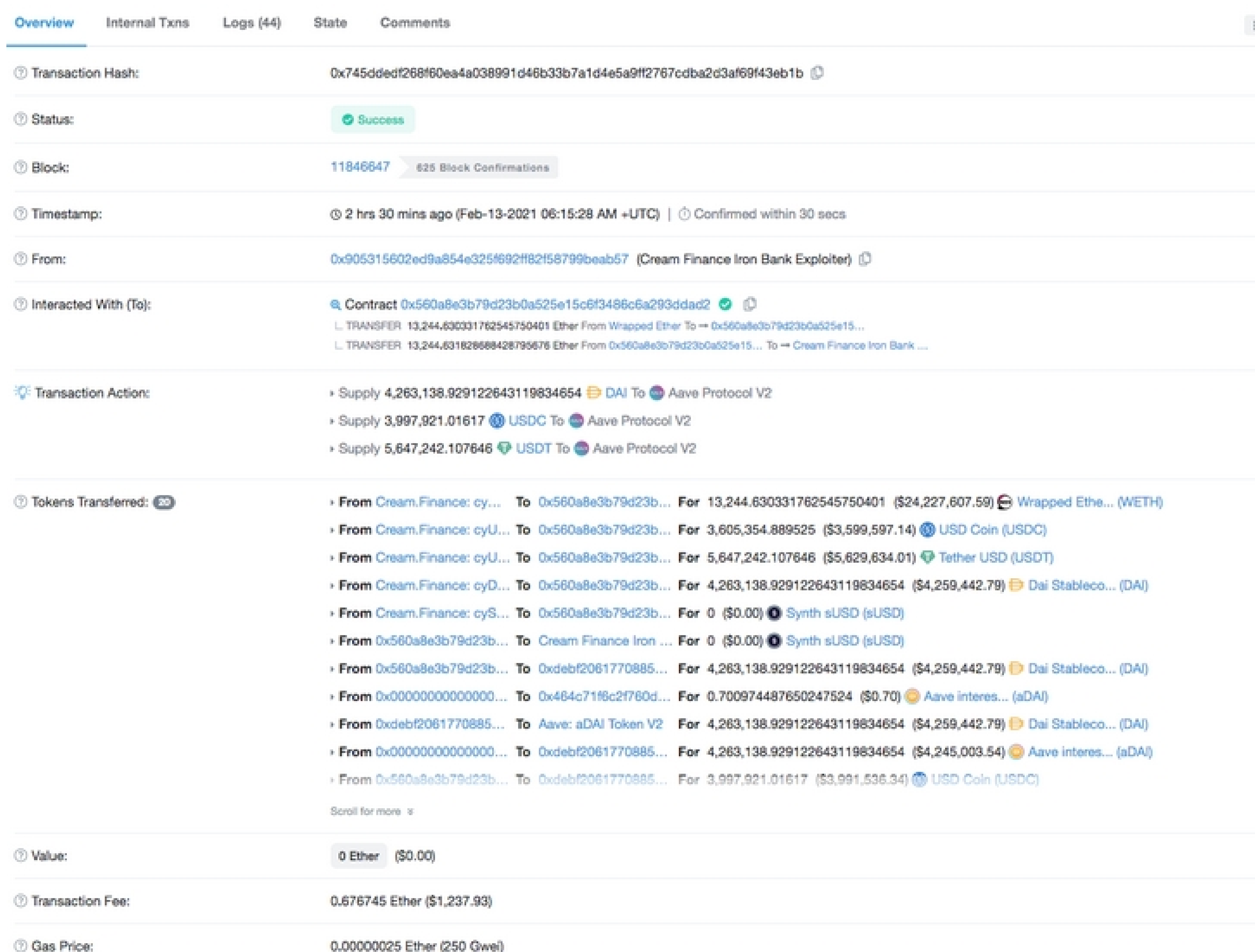
Cause - HomoraBankv2 allows the use of any custom "spell," which is similar to a Yearn strategy (a special type of smart contract).

The only check is that the collateral used in a loan is greater than the borrowed amount. In this case, the attacker used a custom malicious spell (address 0x560a8e3b79d23b0a525e15c6f3486c6a293ddad2) to perform the attack.

With this custom spell, the attacker could perform a multi-stage attack.

Technical Analysis

An Etherscan transaction shows that the attack was worth over \$37.5 million. A large chunk of that sum was a loan of 13,244 ETH.



Overview Internal Txns Logs (44) State Comments

Transaction Hash: 0x745ddedf268f60ea4a038991d46b33b7a1d4e5a9ff2767cdba2d3af69f43eb1b

Status: Success

Block: 11846647 625 Block Confirmations

Timestamp: 2 hrs 30 mins ago (Feb-13-2021 06:15:28 AM +UTC) | Confirmed within 30 secs

From: 0x905315602ed9a854e325f692ff82f58799beab57 (Cream Finance Iron Bank Exploiter)

Interacted With (To): Contract 0x560a8e3b79d23b0a525e15c6f3486c6a293ddad2 Success

- L TRANSFER 13,244.630331762545750401 Ether From Wrapped Ether To → 0x560a8e3b79d23b0a525e15...
- L TRANSFER 13,244.631828688428795676 Ether From 0x560a8e3b79d23b0a525e15... To → Cream Finance Iron Bank ...

Transaction Actions:

- + Supply 4,263,138.929122643119834654 DAI To Aave Protocol V2
- + Supply 3,997,921.01617 USDC To Aave Protocol V2
- + Supply 5,647,242.107646 USDT To Aave Protocol V2

Tokens Transferred: 30

- + From Cream.Finance: cy... To 0x560a8e3b79d23b... For 13,244.630331762545750401 (\$24,227,607.59) Wrapped Eth... (WETH)
- + From Cream.Finance: cyU... To 0x560a8e3b79d23b... For 3,605,354.889525 (\$3,599,597.14) USD Coin (USDC)
- + From Cream.Finance: cyU... To 0x560a8e3b79d23b... For 5,647,242.107646 (\$5,629,834.01) Tether USD (USDT)
- + From Cream.Finance: cyD... To 0x560a8e3b79d23b... For 4,263,138.929122643119834654 (\$4,259,442.79) Dai Stableco... (DAI)
- + From Cream.Finance: cyS... To 0x560a8e3b79d23b... For 0 (\$0.00) Synth sUSD (sUSD)
- + From 0x560a8e3b79d23b... To Cream Finance Iron ... For 0 (\$0.00) Synth sUSD (sUSD)
- + From 0x560a8e3b79d23b... To 0xdeb2061770885... For 4,263,138.929122643119834654 (\$4,259,442.79) Dai Stableco... (DAI)
- + From 0x0000000000000000... To 0x464c71f8c2f760d... For 0.700974487650247524 (\$0.70) Aave interes... (aDAI)
- + From 0xdeb2061770885... To Aave: aDAI Token V2 For 4,263,138.929122643119834654 (\$4,259,442.79) Dai Stableco... (DAI)
- + From 0x0000000000000000... To 0xdeb2061770885... For 4,263,138.929122643119834654 (\$4,245,003.54) Aave interes... (aDAI)
- + From 0x560a8e3b79d23b... To 0xdeb2061770885... For 3,997,921.01617 (\$3,991,536.34) USD Coin (USDC)

Scroll for more

Value: 0 Ether (\$0.00)

Transaction Fee: 0.676745 Ether (\$1,237.93)

Gas Price: 0.00000025 Ether (250 Gwei)



The exploit involved two specific products from the platforms. CREAM Finance's Iron Bank and the recently launched Alpha Homora V2.

In nine transactions, the hacker created several loans from HomoraBankV2, depositing the borrowed funds to CREAM's Iron Bank.

These loans made use of an "evil spell" (similar to a "strategy" in a Yearn Vault) to call an sUSD pool that exists at the contract level on HomoraBankV2.

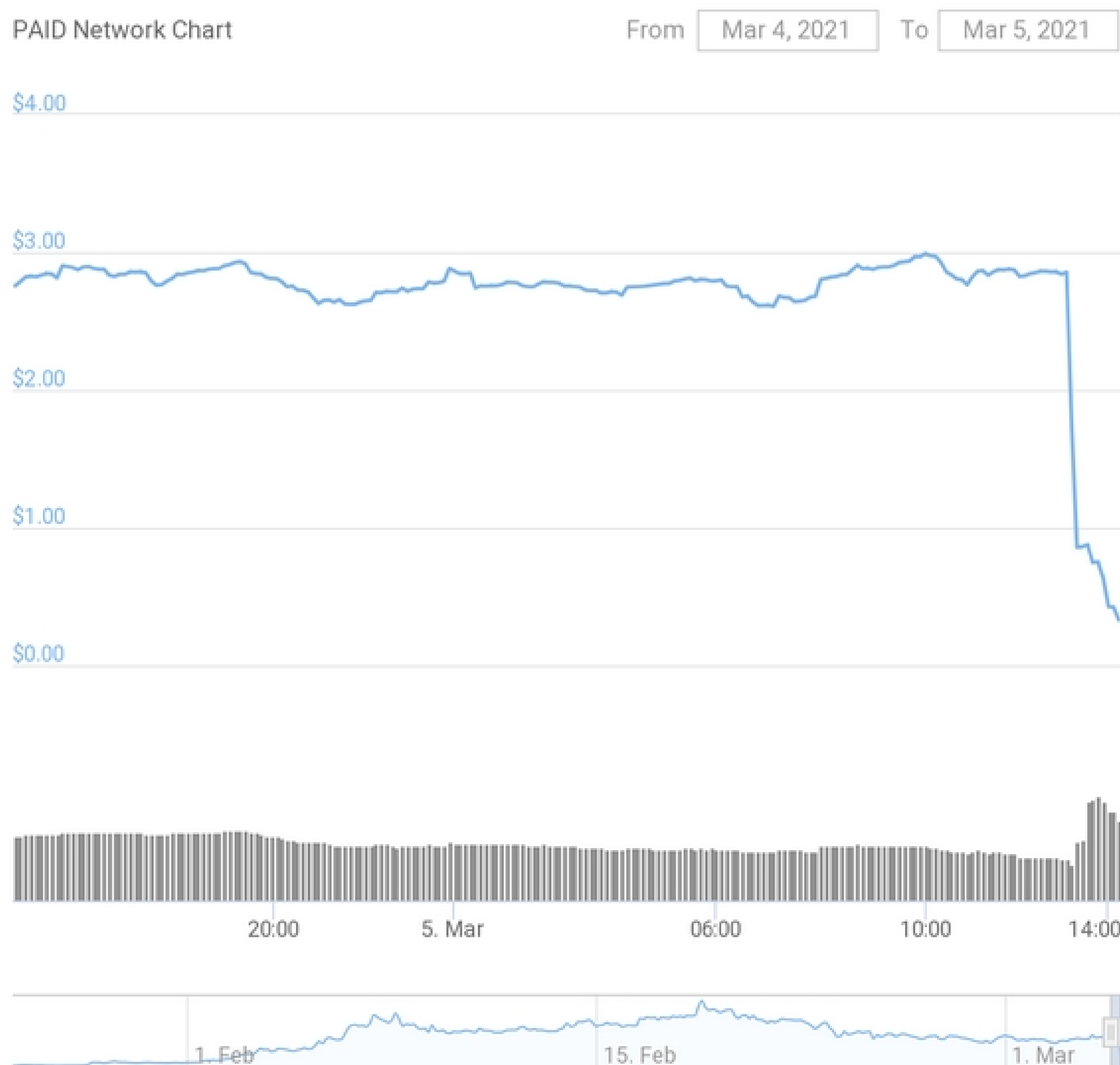
The post-mortem points out the ALPHA team placed the sUSD pool on the HomoraBankV2 contract in preparation for an upcoming release. Information on this contract was not publicly available or accessible through the user interface.

This suggests the hacker possessed a degree of inside knowledge to carry out the attack.

THE PAID NETWORK HACK

PAID Network is an ecosystem DAPP that leverages blockchain technology to deliver DeFi powered SMART Agreements to make business exponentially more efficient.

Total Loss - The attacker extracted approximately \$100 million worth of \$PAID tokens and converted about \$3 million of it to Ether before being blocked by the PAID Network team. \$PAID token price plummeted to more than 80% after the hack.



Source: CoinGecko



Cause - The attacker used a compromised private key to the original contract deployer to leverage the upgrade function of the smart contract. The attacker then proceeded to 'upgrade' to a new smart contract that could burn and re-mint tokens.

Technical Analysis

The root cause of the attack was a combination of two vulnerabilities: a leaked private key and a failure in key management processes.

URANIUM FINANCE EXPLOIT

Uranium is an automated market maker (AMM) protocol, forked from Uniswap V2, and its users claim to give daily dividends.

Total Loss - \$50M

Cause - This problem occurred on the pair contract of the Uranium project. The swap function part of the contract logic refers to the reason of PancakeSwap, allowing users to lend out funds through flash loans.

Technical Analysis

The Uranium Finance hack was made possible by a calculation error in the swap function of version 2 of the project's contracts.

```
function swap(uint amount0Out, uint amount1Out, address to, bytes calldata data) external lock {
    require(amount0Out > 0 || amount1Out > 0, 'UraniumSwap: INSUFFICIENT_OUTPUT_AMOUNT');
    (uint112 _reserve0, uint112 _reserve1,) = getReserves(); // gas savings
    require(amount0Out < _reserve0 && amount1Out < _reserve1, 'UraniumSwap: INSUFFICIENT_LIQUIDITY');

    uint balance0;
    uint balance1;
    { // scope for _token{0,1}, avoids stack too deep errors
        address _token0 = token0;
        address _token1 = token1;
        require(to != _token0 && to != _token1, 'UraniumSwap: INVALID_TO');
        if (amount0Out > 0) _safeTransfer(_token0, to, amount0Out); // optimistically transfer tokens
        if (amount1Out > 0) _safeTransfer(_token1, to, amount1Out); // optimistically transfer tokens
        if (data.length > 0) IUraniumCallee(to).pancakeCall(msg.sender, amount0Out, amount1Out, data);
        balance0 = IERC20(_token0).balanceOf(address(this));
        balance1 = IERC20(_token1).balanceOf(address(this));
    }
    uint amount0In = balance0 > _reserve0 - amount0Out ? balance0 - (_reserve0 - amount0Out) : 0;
    uint amount1In = balance1 > _reserve1 - amount1Out ? balance1 - (_reserve1 - amount1Out) : 0;
    require(amount0In > 0 || amount1In > 0, 'UraniumSwap: INSUFFICIENT_INPUT_AMOUNT');
    { // scope for reserve{0,1}Adjusted, avoids stack too deep errors
        uint balance0Adjusted = balance0.mul(10000).sub(amount0In.mul(16));
        uint balance1Adjusted = balance1.mul(10000).sub(amount1In.mul(16));
        require(balance0Adjusted.mul(balance1Adjusted) >= uint(_reserve0).mul(_reserve1).mul(1000**2), 'UraniumSwap: K');
    }
}
```

In the image above, [shared](#) on Igor Igamberdiev's Twitter feed, the issue is marked in red and green. The "sanity check" code for the balance adjustment uses a value of $1000^{**}2 = 1,000,000$; however, the actual balance adjustments were for 10,000, a deal 100 times lower.

This discrepancy allowed the attacker to send a small amount of value to the contract and extract a much larger one with the swap function, draining the contract's value reserves.



THE SPARTAN PROTOCOL HACK

Spartan Protocol provides community-governed and programmable token emissions functions to incentivize the formation of deep liquidity pools.

Total Loss - \$30M

Cause

The attack against the SPARTA smart contract takes advantage of a failure in the contract's liquidity calculations.

If the attacker inflates the asset balance within the liquidity pool, burning pool tokens will allow them to withdraw an unfair share of the underlying assets.

Technical Analysis

The attack can then be broken up into three main stages:

Stage 1: Pool Token Acquisition: The attacker performs five transactions swapping approximately 1,913 WBNB each round for a total of about 2,536 SPARTA tokens. These SPARTA tokens and an additional 11,853 WBNB are added to receive about 933,350 pool tokens.

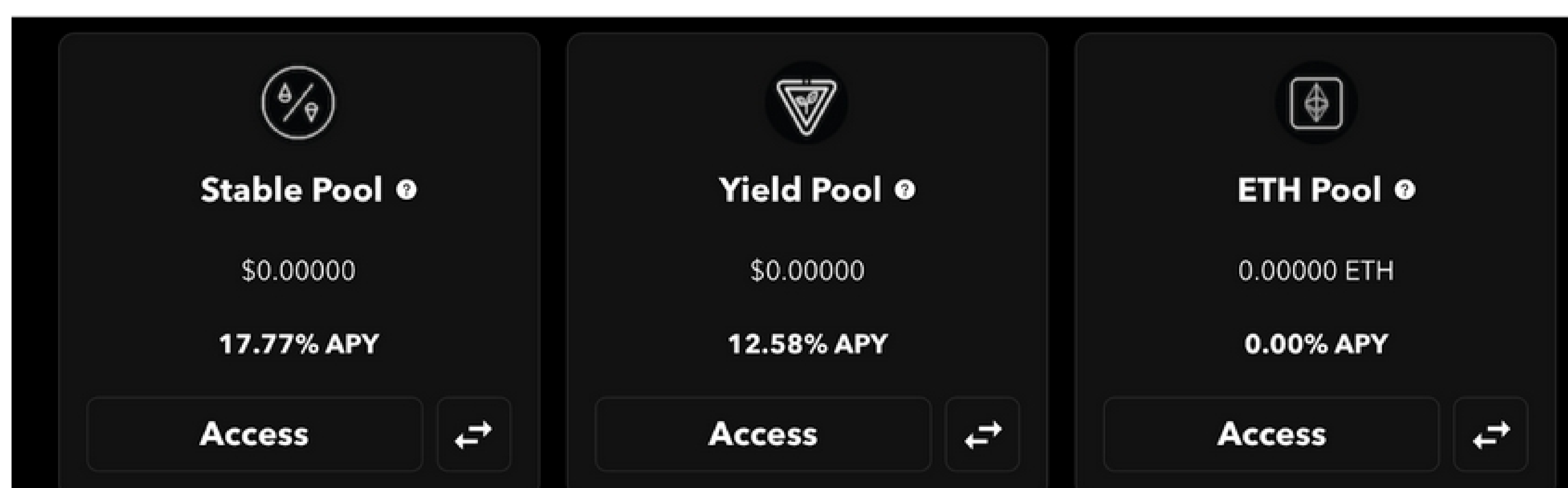
Stage 2: Asset Balance Inflation: The attacker performs an additional ten swaps of about 1,674 WBNB to SPARTA. This resulting approximately 2,639,121 SPARTA and about 21,632 WBNB are added to the pool, inflating its asset balance.

Stage 3: Liquidity Extraction: The attacker burns the approximately 933,350 pool tokens from the first step for about 2,538 SPARTA and 20,694 WBNB (a 9k WBNB profit). They then used the assets from the second step to extract pool tokens, which are burned for about 2,643,882 SPARTA and 21,555 WBNB.

The attacker repeated this process multiple times and extracted about \$30 million in tokens from the pool.

THE RARI CAPITAL HACK

“Rari Capital, The smartest roboadvisor that ensures you receive the highest yield, far beyond just lending.” — from Cypherhunter. Rari Capital provides three pools to users, Stable Pool, Yield Pool, and ETH Pool. ETH Pool is the hacked pool we are talking about today. Rari Capital is like yValut.



Total Loss - \$11M

The Rari Capital governance token \$RGT fell sharply in price following the attack.



Cause

Like the recent Spartan Protocol hack, the attack against Rari Capital took advantage of how a smart contract within the project calculated liquidity shares.

Technical Analysis

The attacker's actions on BSC were as follows:

- 1: Create a fake token and pool it with BNB on PancakeSwap to use Alpaca Finance.
 - 2: Interact with Alpaca Finance, where when calling approve() for a fake token, a payload is called, which allows an attacker to use VSafe through Codex farm to get vSafeWBNB
 - 3: Convert vSafeWBNB to WBNB
 - 4: Transfer WBNB to Ethereum through Anyswap.
- Repeat 2x.

The attack on Rari was as follows:

- 1: Create a fake token and pool with it on SushiSwap
- 2: Interact with Alpha Homora, where a payload is also called so that the attacker can get ibETH in the Rari ETH pool contract.
- 3: Convert ibETH to ETH in the Rari ETH pool.

As a result, 2.9k ETH (\$11.1M) was stolen, and another 1.7k ETH was at risk before the actions of the Rari team.

The total profit from the two attacks was \$15M in ETH.



THE PANCAKEBUNNY PROTOCOL HACK

PancakeBunny is a decentralized finance (DeFi) yield aggregator and optimizer for the Binance Smart Chain.

Total Loss - More than \$200M

The attack saw the price of BUNNY quickly pump from \$150 to \$240 before plummeting to \$0 in just 30 minutes.



Cause

This attack on PancakeBunny's protocol was made possible by a flash loan and the ability for attackers to manipulate the exchange rates of certain tokens on an exchange.

Technical Analysis

1. The exploiter staged (and exited) the attack using PanCakeSwap (PCS).
2. By exploiting a difference in PCS pricing, the hacker intentionally manipulated the price of USDT/BNB and Bunny/BNB, acquiring a huge amount of Bunny through the use of Flash Loans.
3. The exploiter dumped all the Bunny in the market (Ethereum), causing the price of Bunny to plummet.
4. The exploiter then exited the attack by paying back the remaining BNB (by exploiting the price difference from before) on PCS.

POLYBUNNY FINANCE HACK

PolyBUNNY is the Polygon (MATIC) blockchain equivalent of PancakeBunny.

Total Loss - \$2.4M

The token price crashed 82% at the time of mining.



Source: CoinGecko

Cause

The attack began after the malicious actor took out a flash loan on Aave. The protocol's Bunny Vaults and a SushiSwap smart contract that it uses were exploited to inflate the performance fee and profits.

Technical Analysis

1. The hacker used PancakeSwap to borrow a huge amount of BNB.
2. The hacker then went on to manipulate the price of USDT/BNB as well as BUNNY/BNB.
3. The hacker ended up getting a huge amount of BUNNY through this flash loan.

THE BELT FINANCE HACK

Belt.fi is an AMM protocol with multi-strategy yield optimizing on Binance Smart Chain that also provides aggregation for maximum returns.



Total Loss - \$6.3M

Cause

The core developer of SushiSwap Mudit Gupta stated -

“Basically, the issue happened because the belt incorrectly integrated with Ellipsis. A similar issue happened last month in belt finance, but at that time, the problem was a buggy integration with Venus. I wonder if the belt has any bug-free integration.”

Technical Analysis

1: Use 8 flash loans on \$385M BUSD from PancakeSwap

2: Deposit 10M BUSD in bEllipsisBUSD strategy (only for the first transaction, where it was the 'Most Undersubscribed Strategy')

- From 0x58f876857a02d... To 0x4eb362934d56f... For 107,736,995.181428080466763522 (\$107,729,992.65) Binance-Peg ... (BUSD)
- From 0x2354ef4df11afa... To 0x4eb362934d56f... For 38,227,899.20026643768020011 (\$38,225,414.52) Binance-Peg ... (BUSD)
- From 0x7efaef62iddcca... To 0x4eb362934d56f... For 153,621,552.664648194085106148 (\$153,611,567.80) Binance-Peg ... (BUSD)
- From 0x66fdb2eccfb58cf... To 0x4eb362934d56f... For 31,372,406.80087301838491625 (\$31,370,367.70) Binance-Peg ... (BUSD)
- From 0x05faf555522fa3f... To 0x4eb362934d56f... For 17,505,135.133349282372649578 (\$17,503,997.36) Binance-Peg ... (BUSD)
- From 0x133ee93fe9332... To 0x4eb362934d56f... For 17,294,888.215168936840783967 (\$17,293,764.11) Binance-Peg ... (BUSD)
- From 0x7752e1fa9f3a2e... To 0x4eb362934d56f... For 10,828,766.507628240277418295 (\$10,828,062.68) Binance-Peg ... (BUSD)
- From 0x804678fa97d91... To 0x4eb362934d56f... For 10,728,353.170906869924155636 (\$10,727,655.87) Binance-Peg ... (BUSD)
- From 0x4eb362934d56f... To 0x9171bf7c050ac... For 10,000,000 (\$9,999,350.04) Binance-Peg ... (BUSD)
- From 0x9171bf7c050ac... To 0x2ec2ddd12566b... For 10,000,000 (\$9,999,350.04) Binance-Peg ... (BUSD)

3: Deposit 187M BUSD to bVenusBUSD strategy ('Most Undersubscribed Strategy')

4: Swap 190M BUSD to 169M USDT through Ellipsis

- From 0x4eb362934d56f... To 0x9171bf7c050ac... For 187,315,996.874269060031993506 (\$187,303,821.99) Binance-Peg ... (BUSD)
- From 0x0000000000000000... To 0x9171bf7c050ac... For 183,330,311.027564342527408894 bVenusBUSD (bVenus...)
- From 0x9171bf7c050ac... To 0x53a53a9e10abe... For 187,315,996.874269060031993506 (\$187,303,821.99) Binance-Peg ... (BUSD)
- From 0x0000000000000000... To 0x4eb362934d56f... For 183,917,614.828794108117986198 beltBUSD (beltBU...)
- From 0x4eb362934d56f... To 0x160caed037953... For 190,000,000 (\$189,987,650.67) Binance-Peg ... (BUSD)
- From 0x160caed037953... To 0x4eb362934d56f... For 169,949,807.019748917627458054 (\$169,949,807.02) Binance-Peg ... (BUSD-T)

5: Withdraw more BUSD from bVenusBUSD strategy ('Most Oversubscribed Strategy')

6: Swap 169M USDT to 189M BUSD through Ellipsis

7: Deposit BUSD to bVenusBUSD strategy ('Most Undersubscribed Strategy')

- From 0x4eb362934d56f... To 0x0000000000000000... For 193,732,905.553416775192717049 beltBUSD (beltBU...)
- From 0x9171bf7c050ac... To 0x0000000000000000... For 193,971,107.046568770389048447 bVenusBUSD (bVenus...)
- From Venus: vBUSD To... To 0xf322942f644a99... For 1,084.628429373004476632 (\$1,084.56) Binance-Peg ... (BUSD)
- From Venus: vBUSD To... To 0xa6c8a1cf8ebc3c... For 10,845,199.665300671761853031 (\$10,844,494.77) Binance-Peg ... (BUSD)
- From 0xa6c8a1cf8ebc3c... To Venus: vBUSD To... For 526,119,102.40745643 (\$10,845,379.82) Venus BUSD (vBUSD)
- From 0xa6c8a1cf8ebc3c... To 0x53a53a9e10abe... For 10,840,861.151583179743946498 (\$10,840,156.53) Binance-Peg ... (BUSD)
- From 0xa6c8a1cf8ebc3c... To Venus: vBUSD To... For 4,338.513717492017906533 (\$4,338.23) Binance-Peg ... (BUSD)
- From Venus: vBUSD To... To 0xa6c8a1cf8ebc3c... For 210,447.64096298 (\$4,338.15) Venus BUSD (vBUSD)
- From 0x53a53a9e10abe... To 0x9171bf7c050ac... For 198,156,858.025852239775940004 (\$198,143,978.52) Binance-Peg ... (BUSD)
- From 0x9171bf7c050ac... To 0x4eb362934d56f... For 198,156,858.025852239775940004 (\$198,143,978.52) Binance-Peg ... (BUSD)

(Steps 4 - 7 were repeated seven times)

8: Repay flash loans and withdraw profit



THE BONDLY FINANCE HACK

Bondly is the premiere NFT solutions provider empowering the next generation of NFT creators.

Total Loss - 373 million BONDLYs were sent to the Ethereum network, causing the token price to drop rapidly. The token was estimated to be worth \$22 million before the price fell.



Source: TradingView

Cause

The Attacker, through a well-orchestrated strategy gained access to a password account belonging to Brandon Smith, CEO of Bondly.

The password account contained a mnemonic recovery phrase for his hardware wallet, which, when replicated allowed the assailant access to the \$BONDLY smart contract, as well as corporate wallets that were also compromised.

Technical Analysis

1. Ownership of Bondly's token contract was compromised and transferred to the Attacker's wallet.
2. The attack occurred on the following three chains: Ethereum, Binance Smart Chain, and Polygon.

THE THORCHAIN HACK

THORChain is an independent blockchain built using the Cosmos SDK to serve as a cross-chain decentralized exchange (DEX).



Total Loss - \$8M

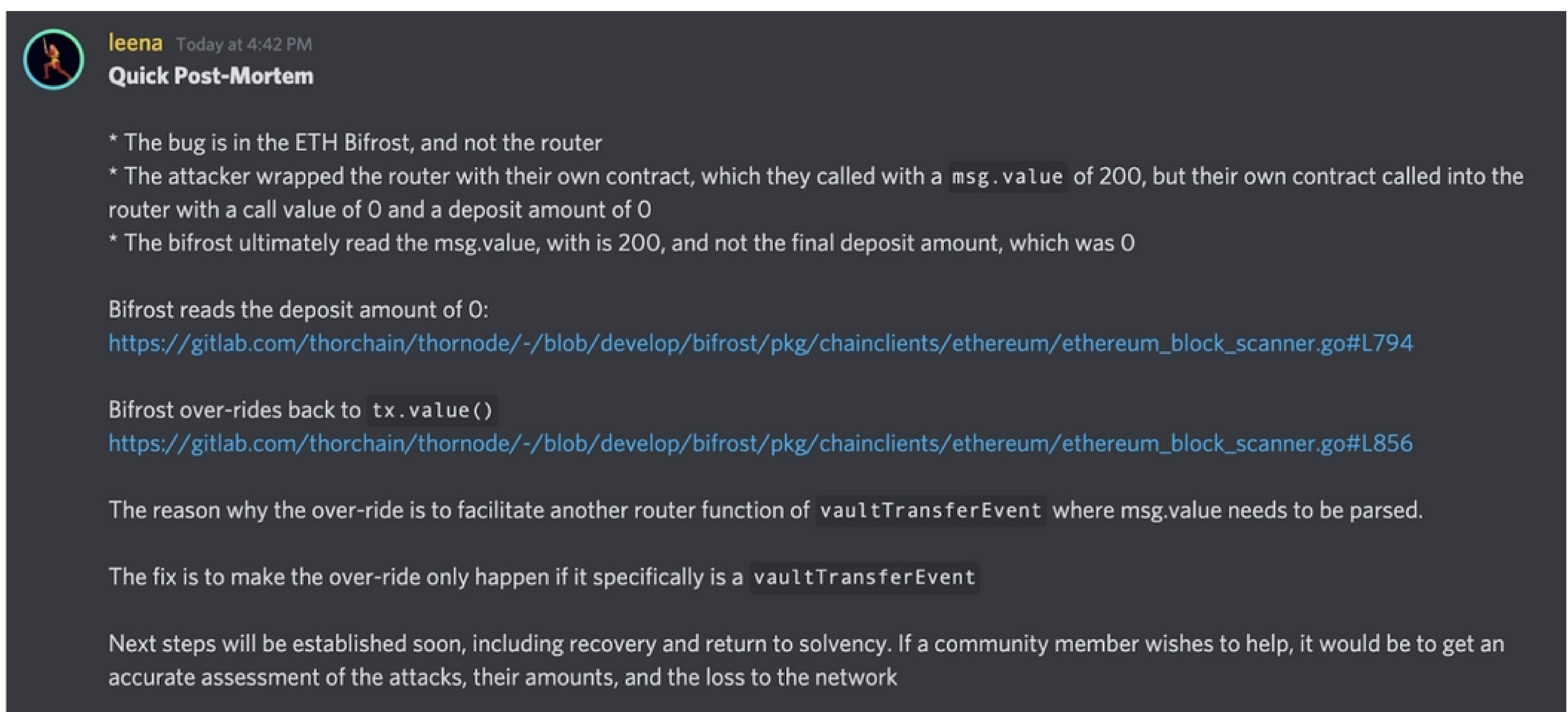
Cause

A hacker deployed a custom contract that could trick its [Bifrost](#) Protocol into receiving a deposit of fake assets.

When using Solidity, the Ethereum smart contract coding language was used in the protocol, programmers advise developers against using certain coding methods to transfer funds.

However, this was allegedly overlooked by the team in charge, leading to an issue within the protocol's native RUNE token's contract code.

Technical Analysis



leena Today at 4:42 PM
Quick Post-Mortem

- * The bug is in the ETH Bifrost, and not the router
- * The attacker wrapped the router with their own contract, which they called with a `msg.value` of 200, but their own contract called into the router with a call value of 0 and a deposit amount of 0
- * The bifrost ultimately read the `msg.value`, with is 200, and not the final deposit amount, which was 0

Bifrost reads the deposit amount of 0:
https://gitlab.com/thorchain/thornode/-/blob/develop/bifrost/pkg/chainclients/ethereum/ethereum_block_scanner.go#L794

Bifrost over-rides back to `tx.value()`
https://gitlab.com/thorchain/thornode/-/blob/develop/bifrost/pkg/chainclients/ethereum/ethereum_block_scanner.go#L856

The reason why the over-ride is to facilitate another router function of `vaultTransferEvent` where `msg.value` needs to be parsed.

The fix is to make the over-ride only happen if it specifically is a `vaultTransferEvent`

Next steps will be established soon, including recovery and return to solvency. If a community member wishes to help, it would be to get an accurate assessment of the attacks, their amounts, and the loss to the network

Post-Mortem from Leena via THORChain Discord

THE POPSICLE FINANCE HACK

Popsicle Finance is a multichain yield optimization platform for Liquidity Providers.

Total Loss - \$25M

When news of the hack became public, Popsicle Finance's ICE token dropped in value, initially dropping more than 55%.





Cause

The perpetrator reportedly used flash loans — where tokens are borrowed, used for some function, and repaid all in the same transaction — to borrow some \$30 million in tether (USDT) and \$32 million in ether (ETH).

Technical Analysis

The hack was due to the lack of proper fee accounting when LP tokens are transferred.

Specifically, the attacker creates three contracts: A, B, and C and repeats in the sequences of:

A.deposit(),

A.transfer(B),

B.collectFees(),

B.transfer(C),

C.collectFees() for eight pools.

Step 1: Flashloan 30M USDT, 13K WETH, 1.4KBTC, 30M USDC, 3M DAI, and 200K UNI from Aave to attack eight PLP pools.

Below we take the USDT-WETH pool as an example.

Step 2: Alice calls deposit() to add 30M USDT and 5.467K WETH liquidity into the USDT-WETH PLP pool and gets 10.51 PLP tokens.

Step 3: A transfers the 10.52 PLP tokens to B

Step 4: B calls the collectFees() function to get its tokenRewards updated.



Step 5: B transfers the 10.52 PLP tokens to C

Step 6: C calls the collectFees() function to get its tokenRewards updated.

Step 7: C transfers the 10.52 PLP tokens back to A, so A can remove the liquidity later on.

Step 8: A calls withdraw() to remove the liquidity and gets back 30M USDT and 5.46 WETH.

Step 9: B calls collectFees() to get 2.15M USDT and 392 WETH as rewards.

Step 10: C calls collectFees() to get 2.15M USDT and 402 WETH as rewards.

Step 11: The attacker repeats step 2 to 10 for several other PLP pools and repays the flash loan in step 1.

A portion of the attack's profits (4,100 ETH, about \$10M) is immediately deposited to Tornado Cash.

THE POLY NETWORK HACK - The Elephant in the Room

Poly Network is a global cross-chain interoperability protocol for implementing blockchain interoperability and building the Web3.0 infrastructure.

Total Loss - \$600M

Cause

Poly Network tweeted that a preliminary investigation found that the hackers exploited a vulnerability in the smart contract.

Technical Analysis

1. Poly Network operates on the Binance Smart Chain, Ethereum, and Polygon blockchains.
2. Tokens are swapped between the blockchains using a smart contract containing instructions on releasing the assets to the counterparties.
3. According to an analysis of the transactions tweeted by Kelvin Fichter, an Ethereum programmer, the hackers appeared to override the contract instructions for each blockchains. They diverted the funds to three wallet addresses digital locations for storing tokens.

DAO MAKER EXPLOIT

DAO maker is the crypto project launchpad that provides growth solutions to your crypto project, keeping them apart from the skirmishes of the cut-throat competition and creating a cryptocurrency revolution in the real-time market prices.



Total Loss - \$7M

Cause

A security vulnerability allowed an unknown third party to transfer funds.

Technical Analysis

1. DAO Maker is fundraising for new crypto projects on Ethereum.
2. The platform requires users to pre-fill their wallets with USDC tokens to avoid gas wars before crowd sales.
3. Once allocated, the USDC is automatically deducted from the pre-funded account.
4. According to analysts, the attacker could access the withdrawal features because the contract did not include sufficient security checks.
5. They also pointed out that Etherscan did not verify the exploited contract.
6. The lack of verification is usually considered a red flag and indicates that the team did a sloppy job creating the contract.
7. The attack came shortly after the project's founders reported an increase in volume for their launchpad, DAO pad.
8. The team also announced plans to issue fully regulated tokenized stocks. In the postmortem report, DAO Maker also stated that a total of 5,251 users were affected, with an average loss of \$1,250 per user.

INDEXED FINANCE HACK

Indexed Finance is a decentralized protocol for passive portfolio management on Ethereum.

Total Loss - \$16M

Cause

The attack was typical of DeFi exploits: the hacker used the flash loan mechanism by overloading the protocol with new assets.

This lowered the price of the Indexed tokens, which then allowed the attacker to mint new ones and cashed them out.

Technical Analysis

According to the developers, the target of the attack was two indexes – DEFI5 and CC10. Additionally, the attacker took advantage of the vulnerability of rebalancing pools.

The Indexed Finance protocol offers users the management of a DeFi portfolio similar to exchange-traded funds and indices with assets under management.



Assets were withdrawn, probably due to a vulnerability in the rebalancing of index pools. When a token is added to the index pool, the approximate values of Uniswap oracles are used to evaluate the token in the load balancer pool. This is necessary to speed up transactions and limit interaction with external markets.

PancakeHunny HACK

PancakeHunny is the newest DeFi yield aggregator built on BSC.

Total Loss - \$1.9M

The price of the HUNNY token crashed from \$0.3 to \$0.1.



Cause

This hack was possible due to a profit inflation bug, which converts the relatively small amount of harvested ALPACA to a large TUSD for staking.

Technical Analysis

In the preliminary report by PancakeHunny, the attack was carried out in the following sequence: -

1. Obtained a 53.25 BTC flash loan from Cream Finance
2. Used the loan to get a 2,717,107 TUSD loan from Venus
3. Manipulated the price of BNB/TUSD Pool on PancakeSwap
4. Use 50 different wallet addresses to deposit 38,250 TUSD into HUNNY TUSD Vault
5. Redeemed 2842.16 TUSD and minted 12,020.40 HUNNY
6. Sold the minted HUNNY for 7.78 WBNB
7. Steps repeated for 50 wallets 26 times



THE CREAM FINANCE HACK

C.R.E.A.M. Finance is a decentralized lending protocol for individuals, institutions, and access to financial services.

Total Loss - \$130 million

Cause

According to the blockchain security firm BlockSec, the hackers exploited a vulnerability in the platform's lending system, called flash loaning, to steal all of Cream's assets and tokens running on the Ethereum blockchain.

Technical Analysis

The AMP token contract implements ERC777, which has the `_callPostTransferHooks` hook that triggers `tokensReceived()` function that the recipient implemented.

The reentrancy opportunity related to ERC-777-style transfer hooks allowed the exploiter to nest a second `borrow()` function inside the `token transfer()` before the initial `borrow()` was updated. This was used over 17 transactions.

VULCAN FORGED HACK

Vulcan Forged is a non-fungible token (NFT) game studio, marketplace, and dApp incubator with multiple games and an active community of users.

Total Loss - \$140M

Cause

According to the company's CEO, Jamie Thomson, the attack targeted wallets in semi-custody managed by Vulcan Forged. However, it was not the wallet vendor, Venly, that was at fault.

"What happened is that someone exploited our servers, obtained Venly's credentials, and used them to extract the private keys of MyForge users," the executive testified on social networks.

Technical Analysis

The private keys of 96 addresses were compromised, allowing the attacker to drain their contents. As well as \$PYR, users also lost substantial amounts of other tokens, including ETH and MATIC.

Subsequent sales of the stolen PYR had a large impact on the token price, which dropped ~30% initially, from around \$31 to a low of \$21.47.



SQUID GAME TOKEN CRASH

The squid was billed as a token that could be used for a new online game inspired by the Netflix series - which tells the story of a group of people forced to play deadly children's games for money.

Total Loss - Developers Vanished with \$3.3M, and the value plummeted from a peak of \$2,850 to \$0.003028 overnight, losing investors millions of dollars.



Cause

Binance claims that this was a classic pump-and-dump, or “rug pull” scheme, and feels somewhat involved because it developed the blockchain used by the DEX PancakeSwap, namely Binance Smart Chain, on which the token was issued and traded.

Technical Analysis

The token’s developers appear to have used a mixer called Tornado Cash to hide their operations, but according to a Binance spokesperson, their team is tracking the movements of those funds.

The exchange expects to hand over the results of its analysis shortly to law enforcement in the jurisdiction where the fraudsters reside, but it appears that the real chances of recovering the funds are very slim indeed.

The developers of the SQUID token have always managed to remain anonymous, and even from their Twitter account and website, it seems they cannot be traced. Tracking them down could be quite complicated, even if the movements of the tokens can be traced.



BitMart HACK

BitMart is a leading digital asset exchange that enables users to trade digital currencies or cryptocurrencies for other popular assets, such as fiat or digital currencies, such as Bitcoin and Ethereum.

Total Loss - \$200M

Cause

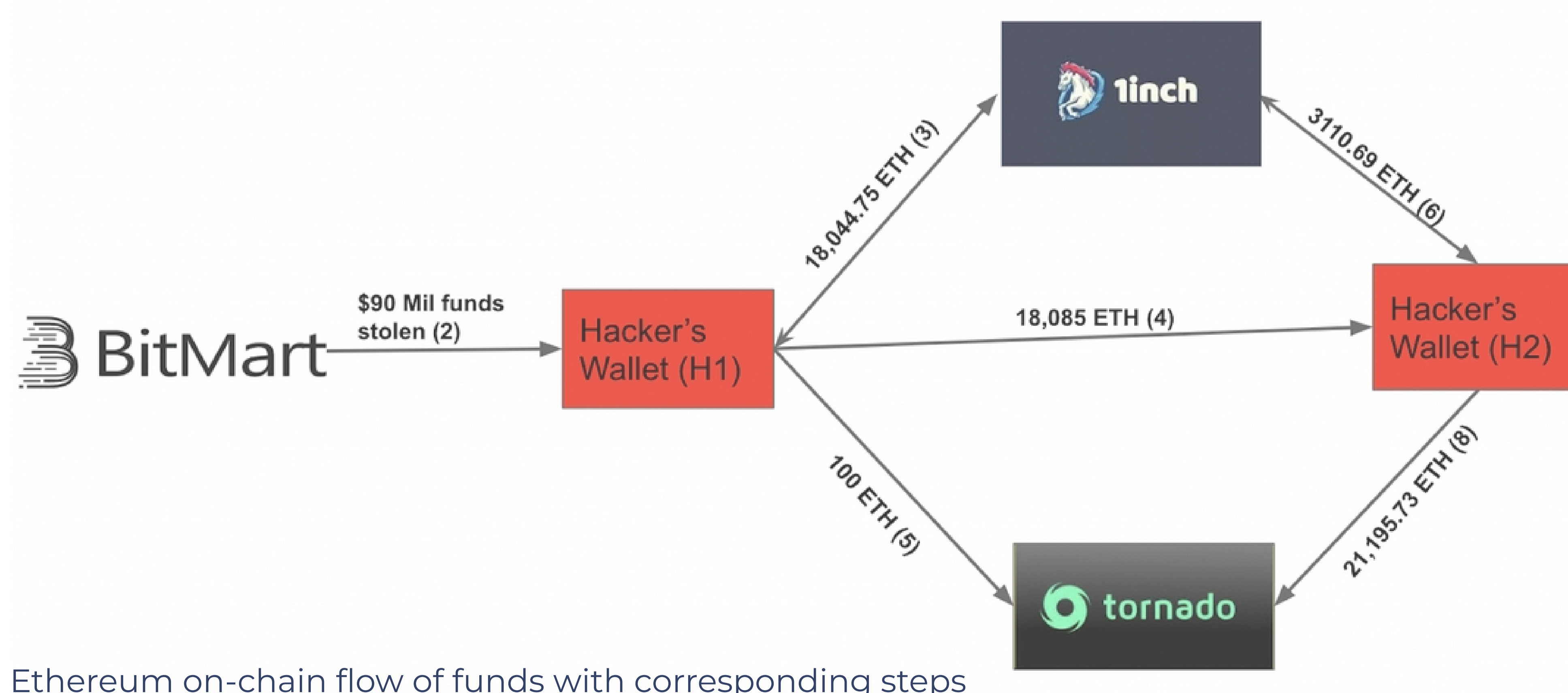
BitMart revealed in a [tweet](#) that the attack was mainly caused by a “stolen private key that had two of our hot wallets compromised.”

Technical Analysis

Merkle Science’s On-Chain Analysis

Ethereum Blockchain Analysis

1. On the Ethereum blockchain, the hacker stole 29 types of tokens, including ETH. In total, \$90,487,593.65 worth of crypto was stolen from the Ethereum blockchain.
2. 148.87 ETH (\$599,576.39) was stolen from BitMart’s hot wallet 0x68b22215ff74e3606bd5e6c1de8c2d68180c85f7 and transferred to the hacker’s wallet 0x39fb0dcd13945b835d47410ae0de7181d3edf270 (H1) on December 4, 2021.
3. Around 18,044.75 ETH (\$74.07 million) worth of stolen ERC-20 tokens from H1 was converted into ETH using a well-known decentralized exchange aggregator 1inch.
4. 18,085 ETH (\$74.61 million) from H1 was then transferred to the hacker’s 2nd wallet 0x4bb7d80282f5e0616705d7f832acfc59f89f7091 (H2) on December 5, 2021.
5. 100 ETH (\$417,118.62) was then transferred from H1 to Tornado Cash to mix the stolen funds.
6. H2 received 3,110.69 ETH (\$12.97 million) from the swapped ERC-20 tokens via 1inch. These were not funds that were stolen from BitMart hot wallets.)
7. In total, H2 received a total of 21,195.73 ETH (\$85.36 million) from steps 3 and 6.
8. The hacker then moved more than 99.9% (21,170 ETH) of the total ETH from H2 to Tornado Cash in order to mix the funds.

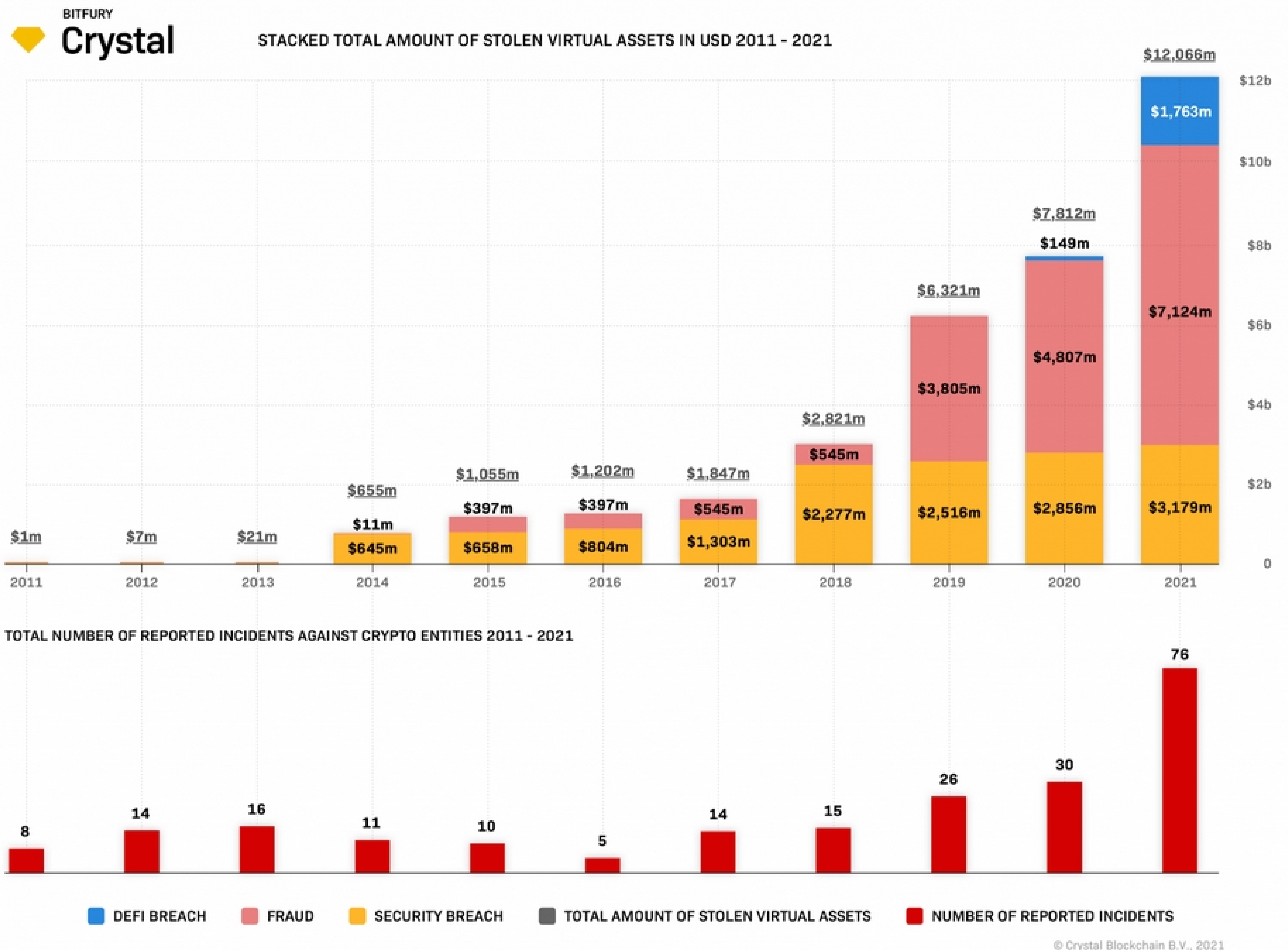


Ethereum on-chain flow of funds with corresponding steps



An Overview of the DeFi Hacks and Scams

According to [Crystal Blockchain](#), there were 120 security attacks, 73 attacks on DeFi protocols, and 33 fraudulent schemes that have so far resulted in the theft of approximately \$12.1 billion worth of crypto assets in total between 2011-2021.

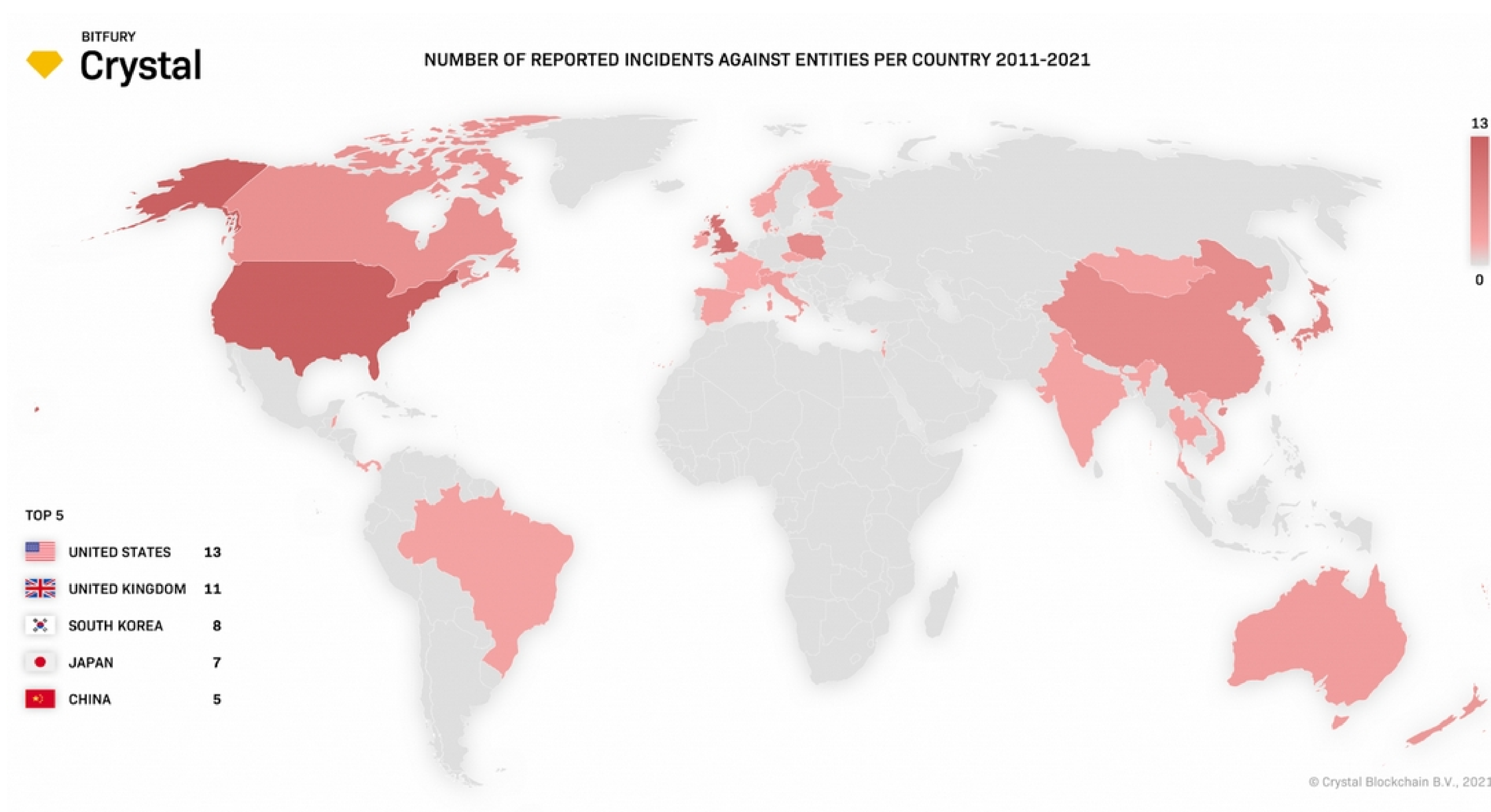


Key takeaways from the 2021 Crypto & DeFi Hacks & Scams Report by Crystal

- The most popular method of crypto theft has been the infiltration of crypto-exchange security systems.
- So far, \$3.18 billion has been stolen through security breaches, \$7.12 billion has been stolen through scams, and \$1.76 billion through DeFi hacks.
- The most common locations for exchange security breaches are the US, the UK, South Korea, Japan, and China.
- In 2020–2021, DeFi hacks started trending and continue to grow.



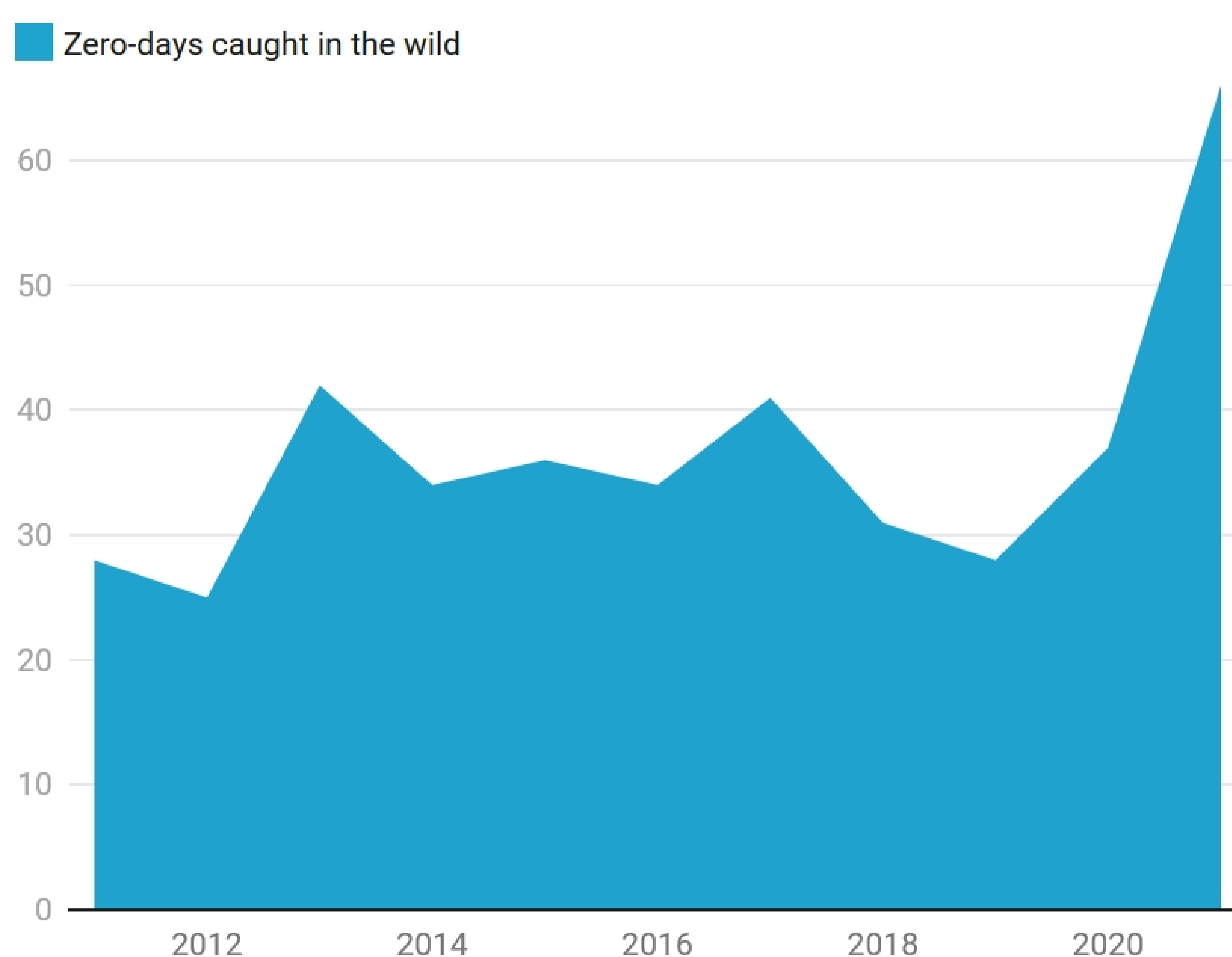
- Ransomware is on the rise, with the most noticeable attacks in 2021 being on JBS (paid \$11m to REvil ransomware) and Colonial Pipeline (paid \$7m to DarkSide).
- Scams using NFTs are also trending, with the market cap for NFTs having jumped by 1785% so far in 2021. Growing adoption inevitably leads to more bad actors in the space.



2021 was a record-breaker for zero-day hacking attacks

A zero-day exploit—a way to launch a cyberattack via a previously unknown vulnerability—is just about the most valuable thing a hacker can possess. These exploits can carry price tags north of \$1 million on the open market.

And this year, cybersecurity defenders have caught the highest number ever, according to multiple databases, researchers, and cybersecurity companies who spoke to MIT Technology Review. At least 66 zero-days have been found in use this year, according to databases such as the 0-day tracking project—almost double the total for 2020, and more than in any other year on record.



2022 and the future of DeFi

Soon, we can expect huge growth and substantial investment to flow into this space soon. This segment will see massive progress due to increased DeFi Exchange offerings, regulatory evolution, and NFTs and GameFi momentum overlapping with DeFi.

Flashback: Status of DeFi in 2020

2020 has proved to be a remarkable year for the growth of DeFi, it has scaled \$700 mn in Total Value Locked in the system in December of 2019 to \$20bn by year end 2020 and \$230 bn today, as per Defi Llama data.

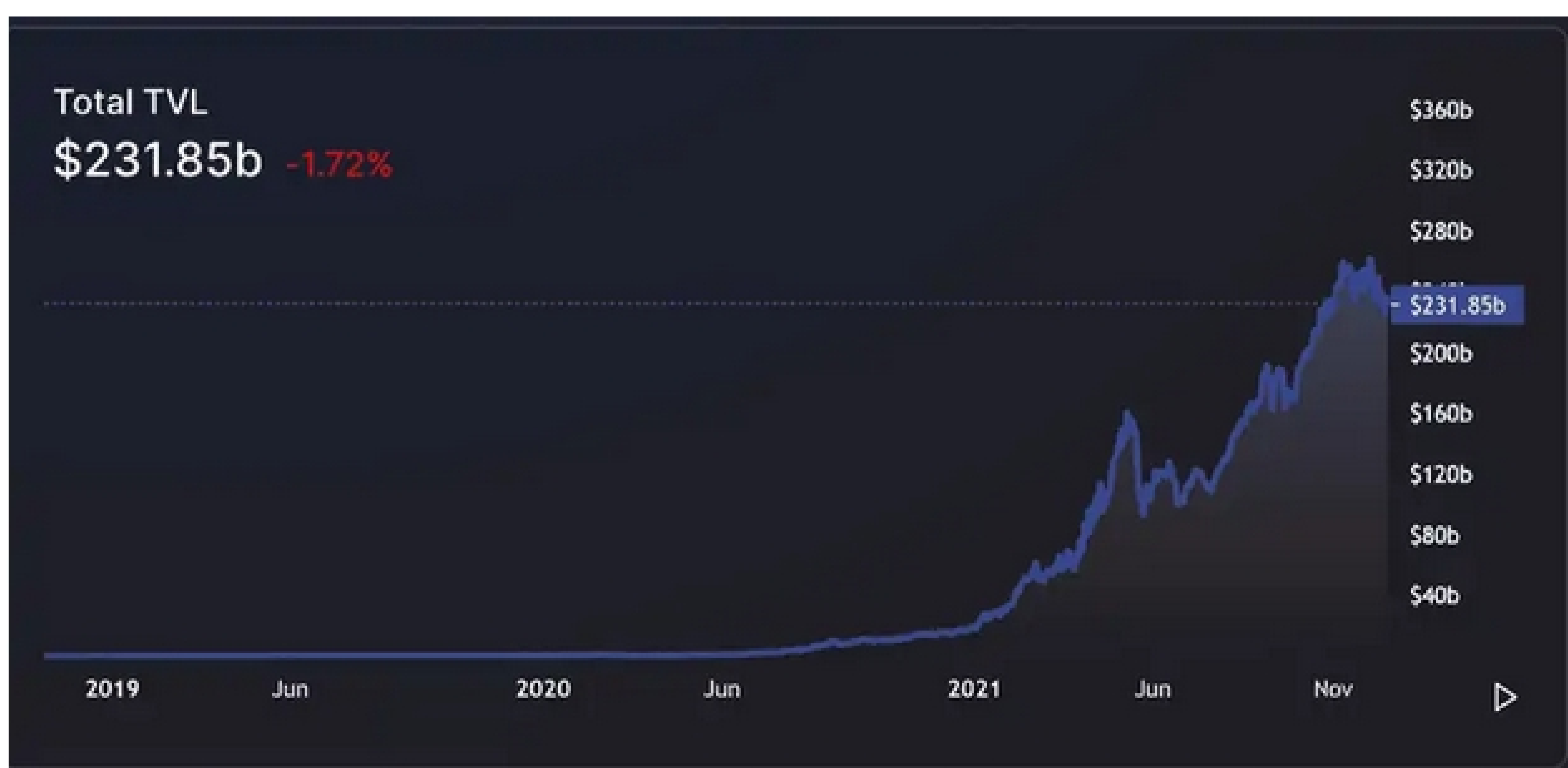
The trend that kicked off in 2020 accelerated in 2021, with a steady rise in TVL and users despite the market prices of many projects well off their highs. Expect growth to continue given the size of the total addressable market is in the trillions, and access is still cumbersome for individuals who are not crypto natives.

2022 should be a pivotal year as progress is made on several fronts. Exchanges are already looking to offer DeFi products to their customers, such as the recent Coinbase announcement to offer yield on stablecoins to users.

Finally, the widely popular NFT and Gamefi applications that have emerged as well as investment into the Metaverse by players such as Facebook will blur the lines between DeFi, Gaming, and NFT's.

New applications that combine elements of finance in gaming, such as the case of Axie Infinity, will crop up. Already, traditional gaming companies are vying to mimic Axie Infinity's success, with \$200 million in transactional volume per week.

Total Value Locked in the DeFi Ecosystem



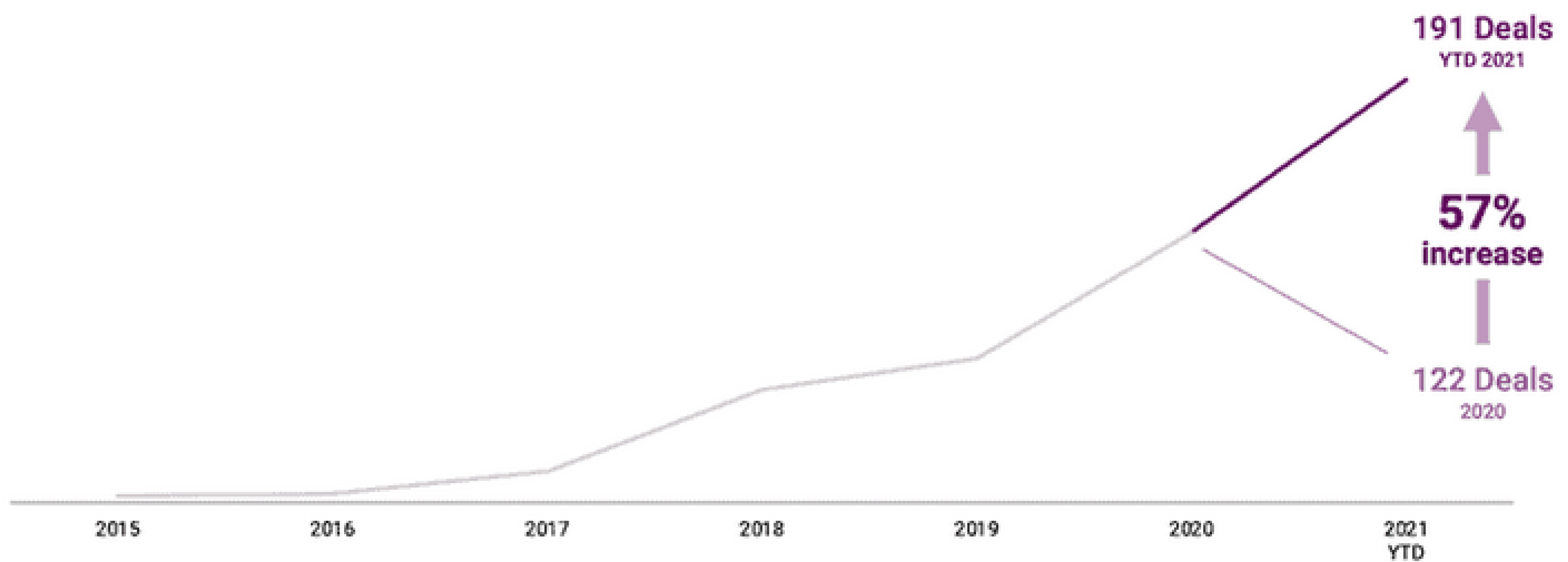
Source: DeFi Llama



TVL is the sum of all assets deposited in decentralized finance protocols earning rewards, interest, new coins and tokens, fixed income, etc. Because blockchain services are developed on peer-to-peer networks, there is no central authority to govern, build, or improve the ecosystem. Therefore, cryptocurrency investors themselves receive consideration for building these networks from the bottom up with their coins and tokens (Nasdaq).

DeFi Investments reach \$2bn as of Q3-21

DeFi startups see nearly 200 funding rounds in 2021 YTD



Ethereum has emerged as a clear winner; will it continue to dominate?

Ethereum emerged as the go-to protocol for open source defi applications because it was the only viable option a few years ago, given Bitcoin's limitations.

This first-mover advantage created a network effect, as it became a building block for these apps. Ethereum's edge was that it was the first to allow for the creation of smart contracts — a piece of code that executes according to a pre-set rule so that the terms of the contract can be set in the code and allow for its execution without the need for a trusted third-party.

While Ethereum continues to be the protocol of choice, it also faces risks. From a dominance of 95% at the beginning of 2021, it has fallen to 64%. This trend is likely to continue, though as the whole system is growing, in absolute terms, so will Ethereum.

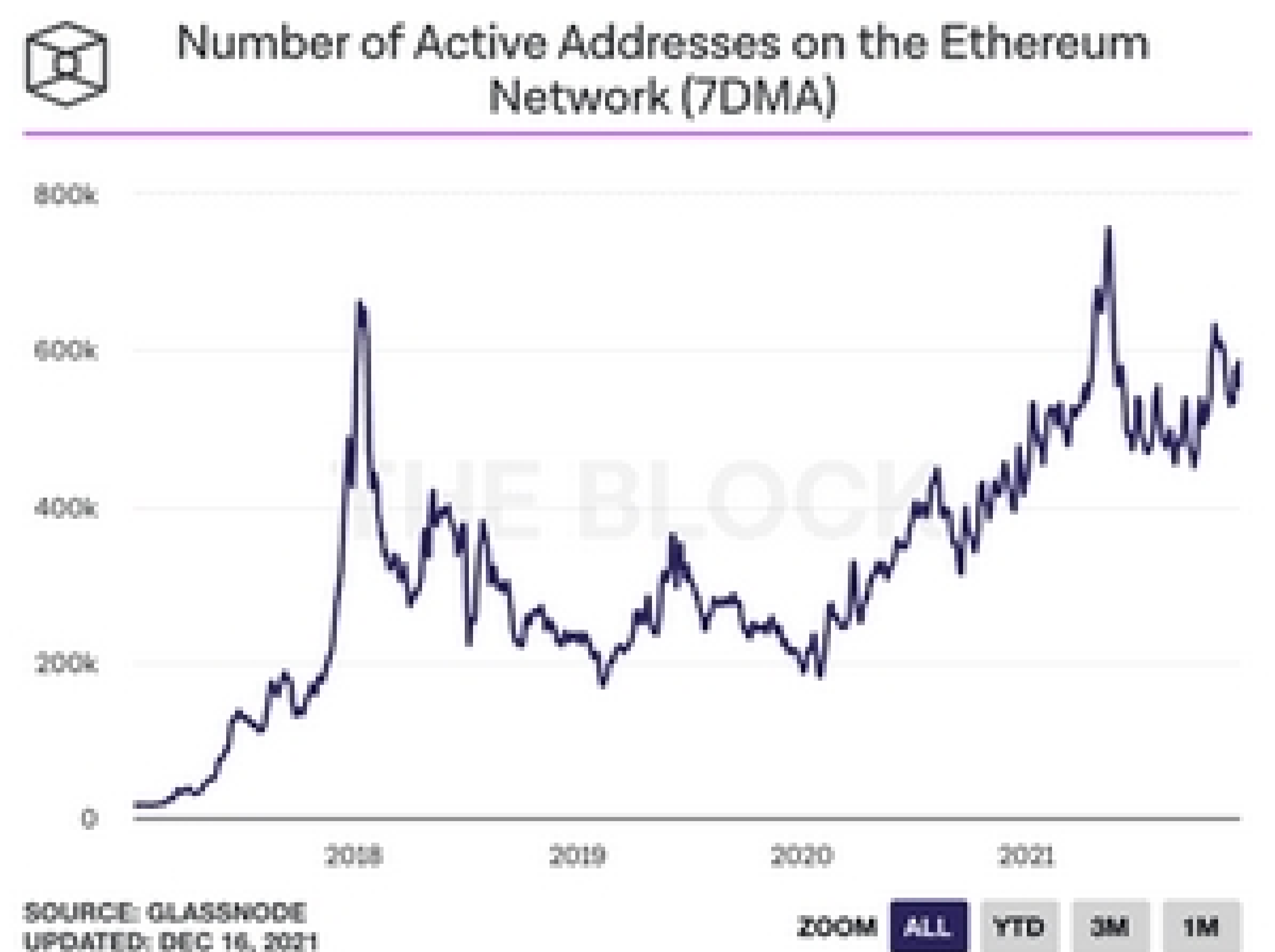
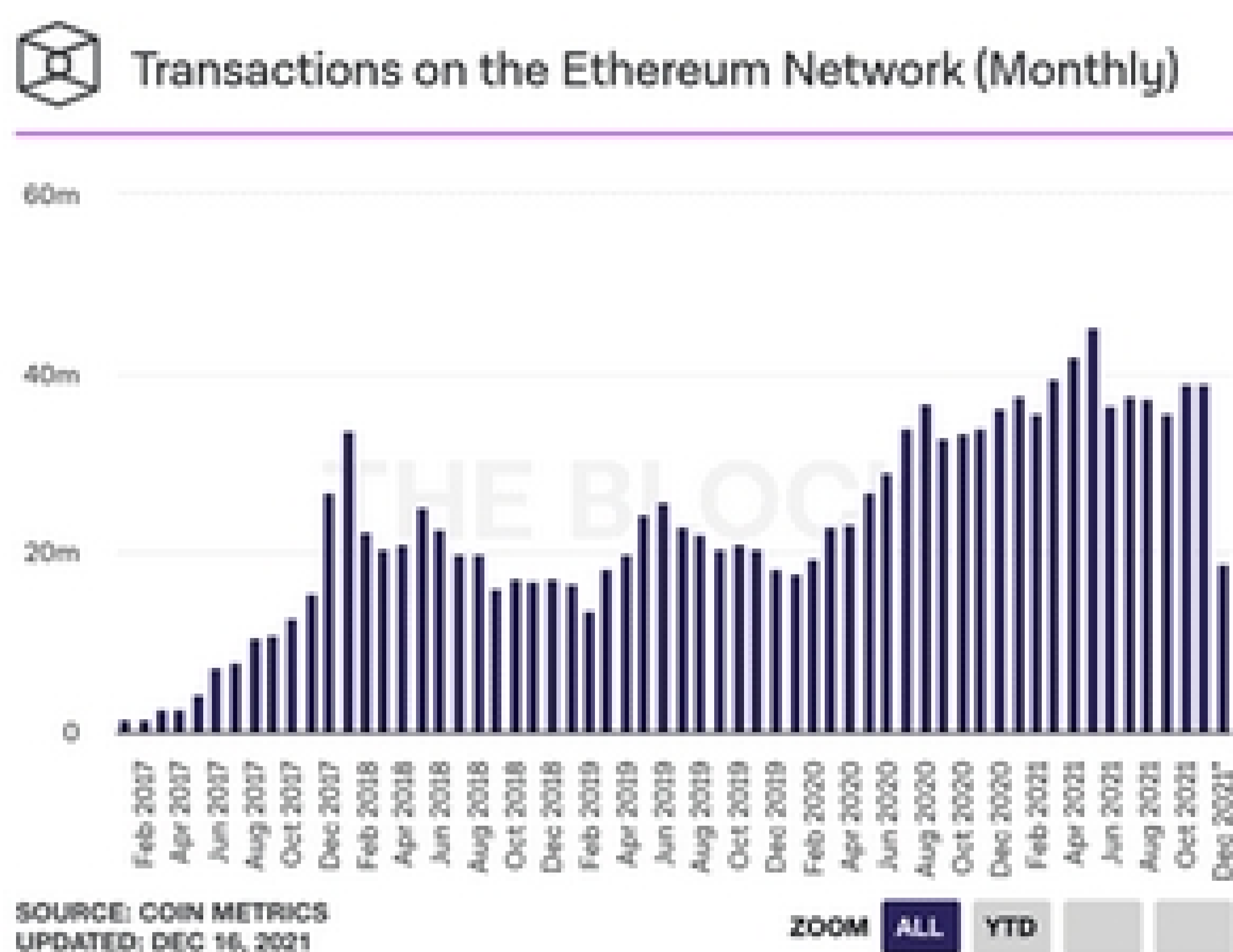
Ethereum has been a victim of its success with slowing transaction times and high fees, despite the London hard fork in 2021. The NFT craze over the summer added to its woes.

An upgrade, Ethereum 2.0., has been in the works for years, but developers may choose to shift to other platforms if it is delayed.

Ethereum 2.0, slated for 2022, will make the network more secure and scalable meaning it will be better equipped to handle larger amounts of work.

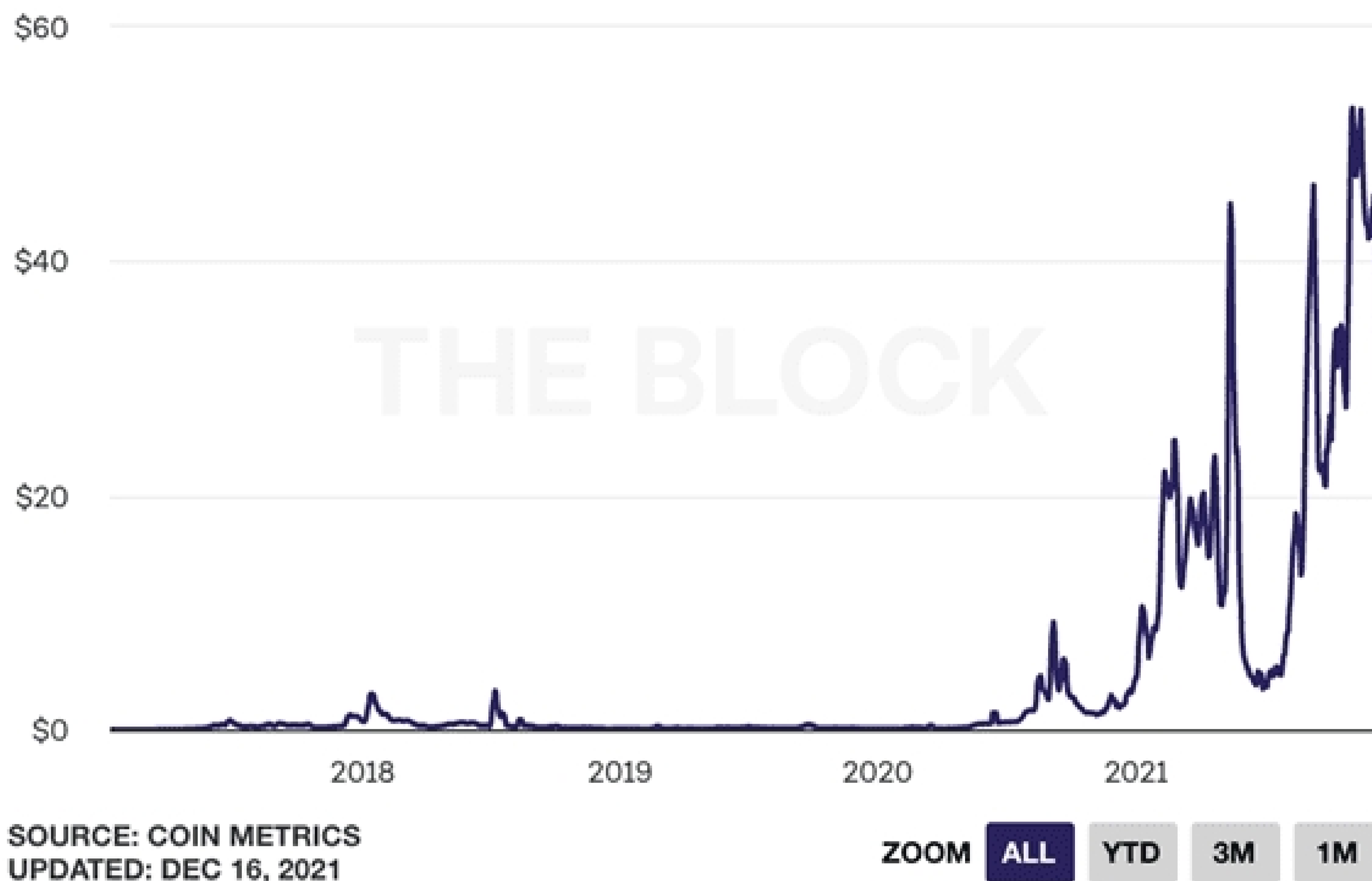
Competition from other smart contract blockchains like Solana (6% of TVL), Binance Smart chain (10%), and Terra (5%) means it is not certain that Ethereum will ultimately prevail or there may be room for several competitors, as in any industry.

Ethereum dominance has fallen but is still high; that should improve when it moves to Proof of Stake in mid-2022.





Average Transaction Fee on Ethereum (7DMA)



3 Web3 Predictions For 2022

Venture capital investment in blockchain related industries and technologies surpassed \$25 Billion in 2021, which was 445% more than 2020.

With Web3 being all the buzz ringing out 2021, the increased investment trend and interest in Web3 looks to only continue in 2022. Here are three (too early) predictions for Web3 in 2022.

- The debate on how decentralized Web3 is will decentralize investment into Web3: Jack Dorsey says VCs own Web3 (and Web3 boosters are pretty mad about it).
- With intellectual property and patent protection being filed in 2018 and 2019 and patents are being issued, the interaction of "Thought Acre" and "Meta Acre" will need to be an important part of everyone's Web3 strategy.
- NFT will trend towards more AR than VR to leverage mainstream adoption.



How Web2 Companies Can Join the Web3 Revolution

The Web3 revolution is a marathon, not a sprint. Companies that governed the Web 2.0 space are starting to acknowledge recent developments and their importance. The key to digital space hegemony is early adoption. Web 2.0 companies have the advantage of an established user base, which is a make or break for many upcoming platforms.

Companies are already testing out and implementing Web 3.0 features. Granted, Web 2.0 companies can better integrate new features and offer a seamless transition to the new way of the internet because users are already versed in their UI design.

Twitter

Twitter is the most proactive incumbent as it's incredibly bullish on the new decentralized web. For example, Twitter implemented tips to everyone, allowing users to reward their favorite creators using any form of currency, including crypto. What's more, Twitter plans to bring in a new verification feature for users to claim their NFT profile picture.

Meta (Facebook)

Facebook is drastically changing its strategy and betting big on the metaverse after it rebranded itself to Meta. However, the metaverse is not similar to Web 3.0 because it builds on distinct features without having to consider Web 3.0 applicability.

Facebook's metaverse immersion has pushed the company to redefine its values. Even before the new shift, Facebook has dabbled with the idea of stablecoins by introducing Diem, a Facebook native stablecoin that generated a lot of unwanted negative discussion.

Now Facebook has released Novi wallet to allow users to send Paxos stablecoins. Interestingly, the company has omitted Diem but chose to implement Paxos in a partnership with Coinbase.

Crypto-reward platforms

Steemit has been presented as an alternative to established social media platforms as early as 2017 using a crypto-reward model. Steemit was the first decentralized open-source blog form, which rewarded users for their contributions. In short, it was similar to a Reddit bulletin board, where each post would earn STEEM tokens through common user consensus.

Protocols like DEIP take it to the next level by implementing a standalone protocol and blockchain for creators. DEIP provides tools and economic models to automate rewards for creators and earn much more than on centralized platforms.

Reddit

Reddit is tackling a new segment of the Web 3.0 network, specifically gaming. Job vacancies on Reddit emphasize that the platform is looking for specialists to help create and drive the new NFT marketplace.

What's more interesting is that Alexis Ohanian stressed that the company is striving to integrate and become a middleman for Blockchain game creators. For example, one of their job openings highlights B2B Marketing lead for blockchain gaming.

Web 3.0 is the desired ideal and the progression towards which every digital platform should strive to achieve. Web 2.0 has failed because it concentrated most of the power in the hands of the few.



Role of Smart Contracts in Creating a Secure Decentralized Ecosystem

DeFi or Decentralized Finance, also known as Open Finance, is considered as the long-pending evolution of the financial sector. The the unprecedented growth of DeFi since the past few years has resulted in a boost to the global economy, enabling more inclusivity and trust in the System.

However, the growth of DeFi is still believed to be just the beginning as experts believe that it is an underdeveloped sector whose potential is unfathomable. It has evolved as a unique and dynamic industry that bears great significance for a considerable percentage of the world population.

The main reason for the inclusion of smart contracts in the DeFi the ecosystem is to enhance the transparency and credibility of the entire lifecycle of the agreement process.

Smart contracts have played a significant role in the growth of DeFi as the incorporation of smart contracts is the reason behind the appropriateness of DeFi in various use cases. For instance, using decentralized finance to create an ecosystem that synchronizes the needs of buyers and sellers without any third party.

Here, smart contracts will act as the terms of agreements and enforce the predefined, mutually agreed upon rules. Other products of the the synergy between DeFi and smart contracts are true digitization, enhanced security, safeguard from external factors such as bribes, unmatched speed, improved accuracy, lower costs such as transaction fee, and utmost transparency.

When it comes to comparing smart contracts with traditional contracts, the main difference is that the governance and execution of smart contracts are not only fast, but it is self-dependent. Therefore, the process of smart contracts is entirely digital, which is beneficial for both entities participating in the agreement.

This digitalization of the whole process saves a tremendous amount of time, energy, and resources.

Moreover, smart contracts with DeFi have also become a highly secured the system which stores the various records providing more auditability and accessibility.



In the End!

Well, if you've been with us till here, a note of thanks to you for being so patient. We hope this roller coaster ride didn't wear you out!

The report's perspective focuses on creating a secured Web3.0 ecosystem for the coming year with community collaboration and awareness.

See you around!

References

We didn't want to put random facts and figures; therefore, we took the help of various online resources, Twitter threads, community posts, and news articles to make this report.

The majority of exploits data and analysis were taken from the [rekt](#), [cointelegraph](#), [coindesk](#), [Fortune](#), [The Armchair Trader](#), etc.

About QuillAudits

QuillAudits is a secure smart-contracts audit platform with the main purpose of providing security to DeFi & NFT protocols.

We are on a mission to make Web3.0 a safer place using our smart contracts audit, NFT due Diligence, DeFi due Diligence and dapps VAPT expertise.





Blockchain Security Outlook 2021

 audits.quillhash.com

 audits@quillhash.com

 Canada, India, Singapore, United Kingdom