Digital Intelligence
Securing the Future

Cryptocurrency Threat Landscape Report- A Year in Review 2022

Introduction

Cryptocurrency and Blockchain technologies have been one of the most prevalent and growing technology industries over the past few years. Threat actors have begun to see cryptocurrency as a highly profitable target for a wide range of reasons, including the ease of laundering, lack of effective testing, and the large number of holders which can be manipulated. In 2022 the total funds stolen by threat actors reached a new high, with the average cost per hack being around $24 million.

Throughout 2022 Cyjax tracked the main threats to cryptocurrencies, identifying some of the year's trends and attack methodologies, and publishing findings in a series of blogs. This helped paint a picture of the main areas that cryptocurrency organisations and projects should focus on, to understand the tactics, techniques and procedures that are being used by these cybercriminals.

This report will detail the main trends and threats identified throughout 2022 and provide some insight into the threat landscape of the cryptocurrency and Web3 space.

Cyjax is moving to a quarterly reporting format for the cryptocurrency threat landscape series. This allows for a wider breadth of trends to be observed, such that more meaningful analysis and conclusions can be drawn.

Identified Trends in Attacks

2022 saw all manner of different kinds of cyber incidents, with a mixture of new Web3 based attacks such as Flash Loan and Oracle Manipulation, and classic attacks such as DNS hijacking and Denial of Service being adapted to the new infrastructure. It was also seen how threat actors can simply gain and move money through fraud and laundering. Some of the most effective and utilised attacks by malicious actors during the year are highlighted below.

Flash Loan Attacks and Oracle Manipulation

Flash Loan attacks have become one of the most talked about attack methods used by hackers to take home large profits. This attack works by utilising a large uncollateralised crypto loan to manipulate a market. These kinds of uncollateralised lending providers have used cryptocurrency to allow for loans that would previously have been impossible to offer, with the only caveat being that the money needs to be paid back within one block transaction. This is supported and operated using smart contracts, with a popular example being the AAVE Flash Loan[1]. With this massive amount of potential operatable cash, threat actors have found ways to utilise this to manipulate markets quickly such that they are able to return the funds and pocket the extra earned through the exploitation.

This technique has been used to conduct some of the largest attacks against exchanges and projects alike, with the biggest example occurring in April 2022 against the Beanstalk Defi platform, where around $182 million was stolen. The platform[2] operates a "A Permissionless Fiat Stablecoin Protocol" that works on the Ethereum blockchain, known as $BEAN. Unfortunately for Beanstalk an attacker was able to identify a vulnerability that could be exploited through the use of a Flash Loan attack. In a post-mortem analysis[3] of the situation, it was found that the protocol operated a majority vote governance system. This allowed for Beanstalk Improvement Proposals (BIPs) to be voted on by the community; however, this meant that with enough collateral an attacker would be able to pass a BIP by force.

This was how the threat actor conducted an attack on Beanstalk, taking and conducting a Flash Loan attack which enabled them to pass a BIP (BIP18) that transferred around $182 million worth of BEAN and other currencies which were promptly transferred into WETH. After paying the loan back the attacker was able to net around $76 million in stolen funds, which was predictably transferred into TornadoCash to be mixed. This attack caused the peg of $BEAN to drop by 75%, effectively crippling the platform; it now stands as the 10th largest crypto hack of the year[4].

This example shows how deadly a Flash Loan attack can be, allowing attackers to use potentially hundreds of millions of dollars as a tool to conduct an exploit. While in standard FIAT terms this sounds ludicrous, within cryptocurrency this is a genuine threat that needs to be managed appropriately. In the example above, the Beanstalk team published a "Path Forward" post[5] detailing how they would be looking to secure their economic model but also stating that this "was an attack on Beanstalk's governance model, not its economic design".

While talking about Flash Loan attacks is important, another kind of attack that went hand in hand this year with it: the Oracle Manipulation attack. As with the previous attack, the main goal of the manipulation is to steal invested funds by abusing a crypto instrument known as an Oracle. An Oracle is the protocol used to transmit information from external sources to update values within smart contracts. This often comprises financial information, such as exchange rates and values; however, if this data feed received is incorrect the smart contract is often built to trust it blindly, leading to a malfunction. Due to the increased popularity of Flash Loans, this tactic was also used much more frequently during 2022 as Oracle providers, both on and off chain, were unable to deal with such large sums of cash being used to manipulate their transmitted values.

One such incident was the attack on Mango Markets in October, where a price oracle manipulation attack was used to steal around $116 million from the platform. The attack was reported by OtterSec[6] who explained that the attacker conducted the Price Oracle attack using a Flash Loan, massively boosting the value of their collateral. After this, the attacker was able to take out a loan of over $116 million worth of Solana tokens. This caused the platform to be completely crippled, with Mango themselves tweeting[7] that the platform should not be used and reaching out to the threat actor to discuss a bounty. While the majority of the funds were frozen within their respective wallets, the attacker did agree to return a portion of the stolen currency, apparently keeping around $47 million worth of the tokens in return.

Overall, Flash Loans and Oracle Manipulation attacks paint a very clear picture of the 2022 threat landscape, and of one where the trusting nature of Web3 is abused by those with large amounts of money. Due to the speed and effectiveness of these kinds of attacks, it is vital that all cryptocurrency projects assess the risk that a malicious actor may pose and implement measures to help protect projects and chains from potential exploitation.

Traditional Attacks in Web3

Another of the most potent trends seen in 2022 was the manipulation and modernisation of classic attacks to target the Web3 industry. As Web3 platforms begin to focus on increasing their level of security, the thoughts of many people are on security analysis, such as smart contract auditing. However, because of this jump, a blind spot has begun to appear within the Web3 security landscape. Traditional security is still highly relevant but appears to have become a side note to the more blockchain oriented procedures. Threat actors have been pivoting their attacks as they begin to exploit this supposed blind-spot by conducting a combination of standard and modified traditional attacks against the Web3 space.

Denial of Service (DoS) has been an ever-present problem since the early days of computers, with the first DoS attack taking place in 1996[8]. It seems, however, that this technique has entered the crypto space, with attacks such as transaction flooding becoming a way to cause disruption and deny access to the chain. One of the most common methods conducted in 2022 was the "Transaction Spamming Attack" with the most notable among these being multiple month-long spamming attacks against Zcash.

Zcash[9] is a privacy focused currency, with the main goal being to offer fast confidential transactions through their token $ZEC. In October the protocol came into the spotlight after a Twitter user noted[10] that its total blockchain size had ballooned to around 100GB in only a few months. After some analysis it was concluded that attackers were making thousands of tiny transactions, each only amounting to around one cent. This, however, was enough to cause the chain size to almost triple, while only costing the attackers around $10 a day.

It is often thought that a large number of transactions on a network would be a positive point; however, an issue arises when they are being made maliciously with the sole purpose to cause inflation on the chain. While the company behind Zcash responded[11] explaining that despite the attack "vast majority of Zcash users are unaffected", it was noted that the use of their more confidential wallets was taking longer to sync. The damage caused in this case was small, yet it shows a first step towards the modernisation of traditional attack methodologies. While decentralised systems often are heralded for their abilities to protect from DDoS attacks[12], it is important that security professionals do not treat this as absolute protection. As threat actors begin to mould attacks to Web3 based targets, the traditional defences for these attacks must develop at the same rate.

While the adaptation of traditional attacks has been one of the ways threat actors have developed new exploit patterns, a blind spot within cryptocurrency was also found in 2022. Blockchain companies have begun to comprehend and build in new Web3 security protocols, such as regular smart contract auditing and correct use of hot and cold wallets. However, despite this focus on protecting the new infrastructure, there has been a failure in safeguarding the traditional infrastructure. This has led crypto-oriented threat actors to revert back to standard attacks, exploiting the hole left in the security landscape.

One example of this seen repeatedly throughout 2022 was the targeting of both exchanges and protocols websites. While a protocols website is often not built with blockchain technology, it is a vital part of its operation, often allowing users to interact with the protocol. Common examples include the facilitation of payments; viewing wallet balances; and trading between instruments.

A simple yet effective technique utilised is a Domain Name System (DNS) cache poisoning attack, which exploits the design of how DNS utilises a caching system. When requests are made a local cache of the request is stored on the device. This is done for efficiency as this stops the requirement for another request to be made if a site has been visited recently. This protocol can be targeted if a client requests a site and then the DNS server receives a false translation: this will be stored on its cache. This means that if a client then requests the site, the DNS sever will respond with the incorrect translation. If the false translation has been responded to maliciously by a threat actor, this could lead to a victim visiting a spoofed version of the site that may be stealing credentials, or carrying out other malicious activities.

One notable DNS poisoning attack in 2022 was conducted against Curve Finance, one of the top 10[13] decentralised exchanges; which offers users the ability to exchange currency utilising their stablecoin liquidity pools. In August the service was subjected to a DNS cache poisoning attack leading to over $620,000 worth of currency being stolen by the threat actor. This was originally reported in a tweet by the Curve Finance team[14] where they stated that the *curve.fi* site should not be visited and that the nameserver had been compromised. From further research it was identified that the attacker had compromised the nameserver and had made a spoofed copy of the site which, when visited, would inform the user that they needed to approve a smart contract. Once approved, it would allow the threat actor to maliciously transfer the funds from the victim's wallet.

The attack surface with this utilises very little blockchain exploitation, only using asking the user to approve the malicious contract. The effectiveness of this kind of exploitation led to big players such as Binance releasing a blog[15] after the incident, detailing the importance of protecting against DNS cache poisoning. While this specific attack is difficult to defend against, it is vital that cryptocurrency companies educate users on all kinds of general security. This should also be combined with a complete security approach ensuring both traditional and Web3 security procedures are being considered.

Crypto Fraud and "Ice Phishing"

Fraud has always been one of the most popular kinds of crime, with 875,622 reports received by ActionFraud in 2020/21[16]. It has slowly been trending towards becoming most commonly a cyber- based crime, with the ONS stating that an "estimated 61% of fraud incidents in the year ending March 2022 TCSEW were cyber-related"[17]. As happens when new technologies are discovered, the cryptocurrency space has become the new focus for fraudsters looking to make some cash. New social engineering tactics have emerged with these new scams, as threat actors look for new ways to trick users out of their own money. The most popular among these has been the "Ice Phishing"[18] attacks, where cryptocurrency users have been targeted in phishing attacks aiming to steal funds.

Cryptocurrency fraud reportedly hit a new all-time high in 2022, with the *Financial Times* reporting[19] that from October 2021 to September 2022 around £226 million worth of crypto had been stolen: an increase of a third on the year prior. While any search of "crypto fraud in 2022" will bring up the well-known story of FTX, there has not been a trend of this kind of activity throughout 2022. Obviously, this event is one of the most egregious examples of potential fraud, with the trusted owner of the company "running away with the cash"; however, there have been some bigger players within the fraud space, with one of the most prolific among them being the surge in crypto-oriented romance scams, and investment scams.

Romance scams have surged alongside the adoption of online dating platforms, and when supported with crypto's fast ability to launder the funds, it is no surprise that they have become so popular. They come in many forms. However, in 2022 a big uptick was seen within "Pig Butchering"[20] scams. This seemingly strange name originates from the practice of fattening pigs before slaughter: a metaphor for the large amounts of social engineering to make the target want to hand their money over. The process of the attack is a simple one: firstly, the victim is approached on social media, often by accounts with attractive profile photos which begin to express interest in them. Over often a long period of time the attacker builds a relationship with the target, leading to them believing that they have found a new lover. After this the conversation turns sour, with the attacker telling the victim to invest in some financial opportunity.

This last stage is the hook, and here the attacker relies on the fact that they have built up enough of a relationship with the victim that they will hand over the money. Often these investment schemes will be a scam, or the attacker will even ask for funds directly, which once transferred will be mixed away into obscurity. This activity has led to many people losing serious amounts of money: the Global Anti-Scam Organisation[21] estimates an average of around $121,926 per victim, with the majority of these being young women. Thanks to its simplicity, this trend is one that is not slowing, with the IC3 reporting[22] that in 2021, more than 4,300 complaints were made surrounding "Pig Butchering" scams, with an estimated total loss of over $429 million.

While love may be one motivator to get a target to part with their money, investment scams rely on the fact that with enough attractive returns, the victim may just do it of their own accord. Since cryptocurrencies were first popularised, threat actors have been known to promise insane gains from investing in different projects, with large numbers of these being branded as "rug-pulls". This term comes from the phrase "pull the rug from under them" showing how the owner of a project will often leave their investors holding the bag. Solidus Labs[23] detailed that there was a total of 117,629 scam tokens created in 2022, an increase of over 34,000 than in 2021.

One of these investment scams was the Frosties NFT project, which rug-pulled its users for over $1.1 million. The project claimed to offer images of a series of different characters wearing different outfits and designs. However, only hours after the mint went live, users noticed that the Discord server for the project had disappeared, followed swiftly by their Twitter account. It did not take long for the US Department of Justice to announce[24] that they had arrested two men accused of running the Frosties scam, charging them with wire fraud. It is vital that users thoroughly investigate all projects they are looking to invest in, and do not fall for any pre-generated hype through influencers or other personalities.

“Ice Phishing” was a term originally coined by Microsoft in a report[25] detailing how phishing attacks were being adapted to the blockchain. Phishing is still one of the most simple and effective ways to attack a target, and within the crypto space this is no different. Crypto-related phishing has been used to conduct some very effective attacks, requiring little to no technical know-how.

One of the best examples in 2022 was the attack targeting OpenSea customers in February[26]. The famous NFT marketplace underwent a contract upgrade where users were required to sign their NFTs over to the new contract. To do this the company sent out a series of emails asking all users to sign their NFTs over to the new chain. A threat actor saw this as a potential opportunity to make some money, and immediately sent out a series of identical phishing emails to OpenSea customers. The scam relied on the users not checking the transaction they were signing, as the transfer in the phishing email would instead sign over the victim’s wallet to the attacker. In total the attacker was able to profit by around $2 million from the sale of the NFTs, many of which were sold below their market value.

Fraud and phishing-based threats have become one of the most impactful trends within the crypto threat landscape. This is partially due to the advanced nature these attacks have reached, combined with the fundamental lack of understanding in large sections of the userbase. This kind of attack is likely to continue to grow in popularity, as more and more people begin to adopt cryptocurrency.

Cryptocurrency Laundering and Blockchain Anonymity

Throughout 2022 there was one trend that must be mentioned, and that is the critical role that blockchain anonymity protocols played in crypto attacks. Since cryptocurrency has become a target in cybercrime, there has been a massive development in the methods threat actors use to launder their ill-gotten gains. As opposed to traditional money, cryptocurrency offers a large amount of different options to turn the funds into legitimate cash. Interestingly, however, throughout 2022 threat actors began to utilise a variety of different methods to mix stolen funds effectively.

Crypto mixers[27] offer a way to anonymise illegitimate funds through the use of tumbling. This process works by taking money inputted into the service and mixing it together into one large pool; after this the funds are withdrawn into the users’ output addresses where they can retrieve them. While this process does not fully anonymise the currency, by utilising other protection methods such as random transaction times and amounts over large numbers of wallets, it can be very difficult to track. The TornadoCash Ethereum mixer was among those noted in 2022.

TornadoCash is a decentralised anonymity protocol, enabling private transactions of Ethereum. The protocol is a highly effective cryptocurrency tumbler that utilises a series of smart contracts to enable the depositing and withdrawing of funds. What makes TornadoCash special, however, is that it uses smart contracts to break the on-chain link by enabling depositing into one address and withdrawing from another, making it almost impossible to track. Another key aspect of TornadoCash is that even as a protocol it is completely decentralised. When the developers created the contracts on chain, they made sure they were immutable and in May 2020 handed the protocol over to the community. This means the original developers have no control over it.

Throughout 2022 TornadoCash came under significant scrutiny with millions of dollars being laundered across the platform, including almost half a billion dollars by the notorious North Korean hacking group Lazarus after they conducted a monumental heist against the Axie Infinity’s Ronin network bridge[28]. This drew large amounts of attention to the protocol, with the US Treasury issuing sanctions[29] against it. This shone light into the impact that TornadoCash was having on the cybercrime community, and really highlighted what a staple this protocol had become within the crypto threat actor’s toolkit.

Because of this there has been a shift away from TornadoCash, with large amounts of the services wallets becoming blacklisted[30] and their accounts and websites being shut down[31]. Newer alternatives such as

“Bridge Laundering” started to take over in the latter half of 2022. The RenBridge is one example of this, with reports[32] stating that since its creation around $540 million has been laundered across the platform, with specific notes including an estimated $153 million linked to Russian ransomware crews such as Conti. Despite the changes in the landscape, stolen funds will always need to be laundered one way or another. The steps which government agencies and larger cryptocurrency companies take in their effort to tackle this problem are important in helping to dampen the ease and effectiveness of laundering offered by privacy platforms to criminals.

While laundering money has been a cornerstone of crime, enabling the transfer of illegitimate to legitimate cryptocurrency has brought light to what may be one of the single most effective and powerful trends seen in the cybercrime space in 2022. This is the popularisation of the “Backwards Bounty”, a new term coined by Cyjax to describe a worrying pattern. The standard roadmap for a crypto heist was to conduct some form of attack, transfer the funds to the attacker’s infrastructure or wallets, launder those funds through a mixer, and then begin the process of realisation. One small problem with this, however, is that this process is a difficult one, as often suddenly making millions of dollars can bring some unwanted attention. Some threat actors have seen this roadmap and flipped it on its head and have decided to see if they can not only get the funds legitimised, but also to make it a legitimate payment.

This process initially works the same way by first conducting the attack against a certain platform and then heisting the funds to attacker infrastructure, often mixing them for safety. The next stage is where the “Backwards Bounty” element is used. The attackers will then contact the victim, offering to return the money stolen as long as they can keep a portion of it as a “bounty” and all wrongdoing is waived. This is playing on the new trend of bug bounty programs, where companies will give security testers a scope and then offer money or rewards in return for any bugs identified. With the threat actors here, because they have already stolen the funds, the victim is in a lose-lose scenario. Either accept the offer and regain the funds, whilst having no ability to have any justice served; or refuse and lose all the money stolen, and hope to be able to investigate and prosecute the offender. Often, this tactic has a much higher success rate when more money has been stolen, as without some of the funds returned, the victim may become insolvent, adding to the pressure. With these kinds of situations, it is not unheard of to see bounties greater than 50%, allowing the criminal to walk away with potentially millions in now “legitimate bounty” money.

Some examples of this include the previously mentioned attack against MangoMarkets, where the attackers stole around $116 million and then offered to return $46 million, keeping a $70 million bounty. This was rejected by the team: an agreement to return $69 million was eventually settled on, leaving the attackers with an astoundingly large bounty of $47 million. With this case, however, justice was served, after the threat actor admitted to conducting the attack and he was charged in the US.[33]. Unfortunately, not all these incidents are as positive as was in the case with the attack against Crema Finance back in July 2022[34]. In this attack, the threat actor utilised an exploit within the protocol that netted them around $8.8 million in stolen cryptocurrency. Interestingly, however, the protocol reached out first, asking[35] the attacker “to consider becoming a white hat” by returning $8 million in exchange for keeping the left over $800,000 as a bounty. This deal was swiftly accepted and in exchange the attacker had all charges against them dropped. It is important to note that while these bounties provide organisations a last lifeline to save themselves from potential ruin, the continued offering of larger-than-normal bounties to malicious actors is likely to continue this trend growing.

Throughout 2022, just as the attacks have adapted, so have the laundering and anonymity methods. As seen with the sanctions brought against TornadoCash, it is vital that large cryptocurrency firms and government departments step up their efforts to help combat the moving of illicit funds. An increased number of government actions and wallet freezes are taking place, and they can be made more effective through combining them with a stronger level of monitoring and tracking at the organisational level. As with bounties, the battle must be fought purely on the white-hat front. One way to help this would be for more blockchain companies to offer bug bounty programs, as opposed to waiting for an exploit to happen and then paying through the nose for it. The main issue still arises at the point of realisation, and it is important that sufficient monitoring is conducted to follow and identify any points where laundered funds are being realised and spent.

Identified Trends in Targeted Infrastructure

It is also important to evaluate the kinds of Web3 infrastructure that have become the target of these kinds of attacks, as through this it will become apparent where threat actors have set their sights. From cryptocurrency communities to bridges, all kinds of services have become targets. Some examples are given below.

Blockchain Bridges

When it comes to blockchain infrastructure, one target has stood out both for its profitability and difficulty to appropriately secure. A Blockchain Bridge is a type of technology that enables two different kinds of blockchains to be connected together. An example of this may be a bridge that connects Bitcoin and Ethereum, enabling a user to bridge currency from one chain to another. There are many different kinds of bridges, utilising all kinds of different blockchain tech such as smart contracts and liquidity pools, with the main aim to enable fast and efficient transfer. Unfortunately, however, bridges are required to hold large amounts of funds to enable these kinds of transfers to happen, and because of this threat actors have begun to see them as a juicy target.

Blockchain bridge hacks are often the result of a lack of effective auditing and testing around the code implementing the bridge. While the effective functioning of blockchains is heavily tested and validated by thousands of users, the code behind these bridges can often be released with little to no testing. Another problem that arises with bridges is that they are highly complex pieces of infrastructure, often relying on large amounts of off-chain data or third-party support. The code is effectively “bodging” two chains together, and this may require multiple complex steps in the process. An attacker need only find a problem in one step within the process to begin to siphon funds away from the intended target. This has led to some popular kinds of attacks, with a report[36] suggesting that three attacks of note are: Fake Deposit Attacks, Validator Majority Attacks, and Signature Verification Bypasses.

First among these is the Fake Deposit Attack which, as the name suggests, is where an attacker aims to trick the bridge into believing a deposit has been made. As the bridge requires a deposit to be made for the new tokens to be minted on the other side of the chain, an attacker can attempt to fake a deposit being made. This would lead to the bridge producing tokens on the other side without any money being inputted. Last year saw an attack of this nature conducted against the Qubit cross-chain bridge, where a threat actor was able to successfully steal around $80 million. Qubit Finance[37] is a “decentralized money market platform” where users could participate as both lenders and borrowers. Relevant to this attack however was that Qubit also operated a Ethereum-BSC bridge[38] called the X-Collateral Bridge.

As can be seen within a post-mortem report[39] of the incident, Qubit’s chain had a logical bug within its code where it did not validate that when the deposit function was called, tokens had been deposited. While this may seem simple at first, the attacker utilised some malicious input data which caused the deposit function to believe that ETH had been deposited, causing it to generate BSC on the other side of the chain. This led the attacker to mint $80 million worth of ETH which was then quickly transferred into TornadoCash[40]. While simple, this attack highlights the importance of ensuring that all deployed code within infrastructure has been thoroughly tested and audited.

Another kind of bridge attack utilised within early 2022 was the Signature Verification bypass. When transactions are made, a process of verification can be used to ensure the bridge transaction is legitimate and digital signatures can help achieve this. A digital signature constitutes a public and private key pair, which together hold a special mathematical relationship enabling the sender of some data to sign it with their private key, and the receiver to verify the signature with the corresponding public key to prove authenticity. This can also be used with transactions. However, threat actors have found that Signature Verification bypasses can occur if an attacker can create an account that can spoof another valid signature, enabling the generation of free tokens on the bridge utilising a complex authentication bypass vulnerability.

One notable example of this happened in February 2022, where the Wormhole protocol was hacked for a monumental $325 million, making it the second largest cryptocurrency theft to date[41]. The protocol[42] offered users a way of bridging a variety of different tokens from one chain to another. It does this through the Wormhole Core Layer contract, which unfortunately was where the vulnerability was discovered. A post-mortem report[43] by the Wormhole team details how the attacker found a vulnerability within the "signature verification code of the core Wormhole contract". The function, used to conduct this verification, took a user account as one of its inputs; however, no one had tested what happened if the user called the function with the *instruction sysvar* account, used to operate the contact on Solana. Because of this if the attacker called the function to make it look as if the *instruction sysvar* account called it, it would believe the signatures were verified. This enabled the threat actor to sign any message with the Solana chain as the destination and allowed them to mint 120,000 Wormhole-wrapped Ethereum on the Solana chain, which was quickly bridged to standard Ethereum netting the attacker around $325 million. Since then, Wormhole has committed to conducting a series of audits to help ensure that this kind of incident does not occur again.

Finally, when discussing the trend of blockchain bridge attacks throughout 2022, the most serious attack of the year must be highlighted. The Ronin Bridge attack is the largest ever cryptocurrency attack, where the protocol was exploited for over $600 million utilising one of the most fundamental attacks in cryptocurrency history. In cryptocurrency there is a famous kind of attack known as a "51% Attack"[44]. It abuses the core functionality of how cryptocurrencies work by stating: if an attacker was able to gain control of more than 50% of a chains' hash-rate, they would be able to validate any transactions they wish. This, for example, can be used to conduct a double spend, reverse transactions, or even halt payments altogether by refusing to validate. The defence against this is that a 51% attack against a sizable chain would be highly expensive to conduct and would require a large amount of compute power. Some bridges, however, use a system where the validator's job is to vote on whether a transfer should be approved or not. A Validator Majority attack works in the same way to the 51% attack, as by owning the majority of the validators, an attacker would be able to approve any transaction: in essence, they can print their own money.

This was the problem that the Ronin bridge faced, as in March 2022 the organisation announced on Twitter[45] that they had been subject to a security breach. As explained within a community alert[46] published by the team, an attacker had been able to compromise five of the nine validator nodes through compromised private keys. Using these five validators the threat actor had a majority and was able to authorise two withdrawals from the network, stealing a total of 173,600 Ethereum[47] and 25.5 million USDC[48] from the bridge's contract. This was possible because four of the nine validators were all operated by a single owner "Sky Mavis", meaning once they were compromised only one further validator was required.

This trend is one that is not slowing, with bridges often being required to hold millions of dollars' worth of different currencies to operate at scale. Being such a big target makes it all the more vital that regular testing and auditing is conducted to ensure that simple code flaws are found and fixed before they can be exploited. In most of the examples discussed above, a simple code flaw gave the threat actor the ability to access the bridge's funds. It is because of this that 2022 saw the trend of bridges becoming the new number one target for threat actors looking to make significant profits, even attracting the likes of state-sponsored actors such as Nother Korea's Lazarus Group in the case of the Ronin Bridge hack[49]. Simply, bridge security needs to be treated with the same level of severity as the chains they are bridging between.

Cryptocurrency Communities

While some may argue that the communities themselves are not a kind of infrastructure, there has been a rise in community infrastructure being compromised. The cryptocurrency space is a very community-based environment with many commodities cultivating large online communities on platforms such as Discord, YouTube and Twitter. Some threat actors see this as a launchpad to spread malicious campaigns utilising traditional social engineering techniques, as discussed above.

Twitter accounts were a major focus for threat actors in 2022, with some large cryptocurrency figures being targeted to spread investment scams or other such things. Often this tactic relies on the attackers being able to find high-profile individuals whose accounts have below average security practices. Once the threat actor can access the account, they will often distribute fake investment opportunities, hoping that victims will trust the person tweeting over the content of the tweet. Some example accounts hijacked include that of famous NFT artist Beeple, whose account was used to shill a fake NFT minting scam and phishing domain[50]. While simple, in the short amount of time that the scam was live, the threat actors were able to net around $438,000 from victims in only five hours.

Another interesting example of this kind of attack happened back in July 2022, where the YouTube and Twitter accounts for the British Army were hijacked simultaneously and used to promote a series of NFT and cryptocurrency scams. The threat actors behind this campaign were able to compromise the accounts, changing the profile pictures, banners and display names. The Twitter account[51] became a scam attempting to impersonate the famous NFT collection “Possessed”. Interestingly, this happened earlier in the year to professional e-sports player MkLeo[52], with the same customisations made to the account: the posts on it contained phishing links aiming to get users to visit a fake minting website, pretending to be a drop of the Possessed collection. The YouTube account[53] on the other hand, underwent a very different change, rebranding to “Ark Invest”, the name of an asset management firm closely linked with Elon Musk. This account began to run a series of livestreams playing old videos of the tech billionaire talking about cryptocurrency, whilst shilling a “double your bitcoin” scam alongside it.

This technique is another trend that took off in 2022, with the number of financial, technology and general influencers used in these fake “double your money” scams rapidly increasing. The simplest examples just utilise old footage of the celebrity talking about cryptocurrencies while promoting investment scams, the most popular among them being free giveaways and money doublers. One such livestream ran in May last year[54], and was able to net $1.3 million in only 24 hours using old footage of Elon Musk, Jack Dorsey, and Cathie Wood from an interview titled “Bitcoin as a Tool for Economic Empowerment”. Since this, newer techniques have begun to be utilised by threat actors in an increased effort to part victims with their cash. One of these is the use of deepfake technology to generate fake interviews or conversations to lure people to click scam links.

Deepfakes are an AI-assisted video editing technique where large datasets of someone’s face can be used to replace another one in an existing video clip. This was originally used light-heartedly to place actors into films which they were not in[55]. However, since then, threat actors have found ways to manipulate the tool for their own purposes. In 2022 some of the first campaigns utilising this technology emerged, where cryptocurrency icons such as Elon Musk were having deepfaked videos running of them promoting scam platforms. In an example from May[56] the attacker had also utilised an AI voice program to have the fake Musk repeat a script promising up to 30% returns on a platform known as BitVex. Another high-profile individual, the Chief Strategy Officer at Binance, Patrick Hillman, has written a blog[57] about his experience with this kind of attack, where he alleges that a “sophisticated hacking team used previous news interviews and TV appearances over the years to create a “deep fake” of me”. In this instance, however, this was not for a YouTube livestream but was allegedly used on a one-on-one Zoom call with the victim. As this kind of technology becomes more widely available and believable, it is guaranteed that scammers will use it more frequently to target cryptocurrency communities.

The final and most prevalent attack against cryptocurrency communities is through those aiming to compromise crypto project Discord servers. Discord is a platform that enables users to create "servers" which act like a personalised forum, allowing for multiple messaging channels, voice channels and livestreaming of content. It is very common for different communities surrounding crypto projects to have a Discord server, where members can come together and meet. The most predominant among these is the communities that form around NFTs, with famous collections such as Board Ape Yacht Club (BAYC) having invite-only servers for holders of the art. Threat actors have found that being able to compromise these servers is a lucrative attack method, due to the shared trust among the members of these groups.

One notable example was when the aforementioned BAYC had their Discord server hacked[58]. The group, which is invite-only, had one of their community manager's accounts compromised. With this access the threat actor chose to post a series of announcements detailing an "exclusive giveaway" to the holders of specific NFTs. The phishing link led to a site where users were asked to link their wallets to claim the free mint; the attacker would then steal all NFTs from the wallet. In total the threat actor was able to steal around 200 Ethereum for a profit of around $360,000 which was quickly transferred to TornadoCash. To put context around this kind of attack, crypto researcher *@NFTherder* released a tweet[59] detailing how in the same month, a further 106 Discord servers were hacked. It is vital that administrators of Discord communities ensure that their accounts have appropriate security controls in place to help prevent against this kind of attack and abuse of trust.

As cryptocurrency communities grow larger and become a cornerstone of the crypto landscape their infrastructure must be treated with the same level of importance as that of the cryptocurrency itself. Major figures within these communities, either on private groups such as Discord Servers or on public services such as Twitter, should maintain a good level of security on their accounts through usage of multi-factor authentication and strong passwords. Public platforms must conduct regular scans to help take down the malicious actors' attempts to abuse the community infrastructure.

Cryptocurrency Exchanges

Exchanges are the heart of what keeps the cryptocurrency landscape ticking by facilitating the purchase and sale of new currency. However, as with the rest of the cryptocurrency landscape, the number of exchanges is expanding at a rapid rate, with the total number tracked by *coinmarketcap.com* increasing by 83 over the course of 2022. Exchanges have become a large target for threat actors looking to conduct a "virtual bank heist" against the platforms. Throughout 2022 a variety of different cryptocurrency exchanges were targeted in attacks, with one notable exception of the FTX collapse, which highlighted how an exchange can be crumbled from what some would call an insider threat attack.

Starting off the year, well-known exchange Crypto.com was subject to an attack where over $34 million in user funds was stolen. The exchange,[60] which is used by over 80 million customers worldwide, offers markets on over 400 different tokens and currencies has a total of nearly $4 billion in reported assets. In January, however, a group of Crypto.com users woke up to find that their wallets had experienced unauthorised transactions. In a report released by the team[61] it was found that the exchange had suffered an attack where victims' funds were transferred from their wallets without the two-factor authentication (2FA) being required. While they do not explain how the attacker was able bypass the 2FA, the company explain that as soon as the attack was identified, all 2FA tokens were revoked and additional security hardening measures were put in place. These include the adoption of "true multi-factor authentication" as part of their new Account Protection Program (APP).

That example shows the consequences of failing to enforce high security standards. In early August the self-proclaimed "world's most secure exchange" ZB Exchange was subject to a hack where nearly $5 million was drained from the platform. It was announced[62] that the organisation was suspending withdrawals and deposits due to "the sudden failure of some core applications". However only one day later cryptocurrency researcher PeckShield reported[63] that around $5 million-worth of different currencies had been transferred out of the main wallet. The full story of what happened here is still not known. As with the previous example above, ZB Exchange is reluctant to share the exact details of how an exploit was conducted; more egregiously in this case, however, is that very little has been said since the attack took place. Two main theories dominate the community with the main one being that a threat actor compromised the service by gaining access to a private key enabling the mass transfer of the funds. Another theory is that the service was subject to an insider threat attack. This is where the threat actor is inside the organisation, often using their elevated access from being an employee to carry out the attack. In this case, many speculated that some internal staff may have conducted what is known as an "exit scam"[64] within the crypto community: this is where the owners of a project or organisation disappear with customer or investor funds.

When it comes to insider threat, however, only one story dominates the conversation and really hammers home why the trend of exchange attacks is still as prevalent as it is. FTX was a cryptocurrency exchange and hedge fund that at its peak was the third largest in the world. In November it suffered a mass liquidity crisis leading to a "run on the bank" leaving the exchange around $10 billion out of pocket and forcing bankruptcy proceedings. This sent shockwaves through the entire cryptocurrency landscape, with users losing billions of dollars, and other cryptocurrency organisations failing due to their stake in FTX. It also highlighted the potentially fraudulent nature of the exchange's operations.

The main problem arose when a report was leaked[65] in early November detailing how the CEO Sam Bankman-Fried's secondary trading company Alameda Research held a very large stake in FTT token, created by FTX and used mainly as a utility token on the exchange: holding such large amounts on Alameda's books made the solidity of those books look shaky. What then followed was Binance CEO Changpeng Zhao[66] announcing that because of this revelation Binance would be liquidating all remaining FTT on their books. For FTX, this led to a massive liquidity pull, where over $6 billion was taken from the platform in only three days as the community lost trust in the large exchange. The issue arose because a large amount of FTX's liquidity was also stored within their FTT token: as soon as the mass sell occurred, the price of FTT dropped from around $25 pre-announcement to around $1 where it stays today. This led to FTX experiencing further liquidity issues, eventually having the exchange file for bankruptcy[67] on 11 November.

Remarkably however, this was not the end of the story: the WSJ published a report[68] explaining how FTX had transferred around $10 billion-worth of customer assets to Alameda Research to be used for investment opportunities. Not only was this firmly against FTX's own terms and conditions but also these funds could have been transferred using a potential "backdoor" which Bankman-Fried had reportedly[69] asked Chief Technology Officer Gary Wang to build in the book-keeping software. While this has not been confirmed, it paints an interesting picture as to the internal state of FTX before the collapse.

Only one day after the bankruptcy had been filed, threat actors saw a chance to strike, taking advantage of the weakened platform to carry out an attack leading to over $400 million-worth of funds being stolen. Cryptocurrency researcher *@ZachXBT* tweeted[70] that former FTX employees "do not recognise these transfers", and in a report released by Elliptic[71] they stated that a series of unauthorised transfers were conducted against the platform. It did not take long for the attacker to start to move the money from their wallet[72] with a total of 180,000 Ethereum being transferred to 12 newly created wallets. Funds were also moved in other ways, with Chainalysis reporting[73] that currency was bridged across RenBridge from Ethereum to Bitcoin. Because of the now tarnished reputation of FTX, however, many speculate that this attack could also be an insider threat with staff attempting to siphon what was left of the company's funds. While this situation is still ever evolving, it paints a grim picture of the cryptocurrency landscape. The silver lining is that it has highlighted the level to which cryptocurrency is reliant on the big players within the industry, and what can happen when "too big to fail" fails.

The trend of exchange attacks across 2022 is one that gives us some serious takeaways. Most simple among these is that both cryptocurrency users and companies need to assess the level to which they are reliant on some of the bigger players within the space. It is important that, with technology built on the principles of decentralisation, it does not become centralised by proxy through these bigger players. It is also vital that all cryptocurrency platforms enforce the highest possible levels of security, both internally and externally. Simple changes such as operating on the principles of least privilege, combined with enforcing good security practices, are key in tackling the ever-growing trend of exchange hacks.

Conclusions

Throughout this report two core aspects have been outlined and used in the analysis of the cryptocurrency threat landscape of 2022. Through assessment of the attack trends utilised and the infrastructure targeted, a picture can be built of how threat actors have both used and abused cryptocurrencies for their own gain. Most importantly, however, is crypto's full acceptance as a core part of the cybercrime landscape, as threat actors begin to innovate using the technology as a key tool in their arsenal. It is also worth mentioning that while 2022 saw threat actors utilising cryptocurrencies, the legitimate world also increased its adoption of them, as government departments and security companies started to appropriately tackle the problems that crypto poses.

Inside this report some major themes have emerged, as threat actors begin to find the most efficient and effective ways to build upon the move to blockchain technologies. The most obvious among these is that cryptocurrency has become the new currency of crime. While it is abundantly clear that only a small percentage of all cryptocurrency usage is for illicit transfers, the adverse is not necessarily true. Cybercriminals are increasingly adopting the use of cryptocurrencies, whether for the purchase of services or the payment of ransoms: the new king is crypto. When this is combined with the wide access and mass adoption of cryptocurrency tumblers, threat actors are beginning not only to use the technology but wield it with a greater understanding. Tools such as TornadoCash posed a simple and effective way for attackers to anonymise their crime proceeds. The impact of this is potentially huge, acting as a possible enabler for crime by helping those new to "dip their toe" in the crime world. Popular tumblers alone do not lead to this conclusion however, but the development of new and innovative methods for laundering criminal funds. From the usage of bridges to the potential power of "backwards bounties" a whole new world of financial crime capabilities has opened up. While this problem is one with no easy solution, it is clear that something must be done. And, as seen in 2022[74], when large players within the industry come together to tackle cybercrime, it can be done. The positive news that companies such as Binance are reportedly[75] looking to train law enforcement on how to stop cryptocurrency crime also means that the fraudulent activity should be significantly better understood and more effectively policed.

The attacks that took place in 2022 also showed that the holders of cryptocurrencies themselves are seen as a weak point and a great place to make money. It has often been the case within cybercrime that social engineering is "low hanging fruit" with CISCO reporting[76] that 86% of organisations had a user try to connect to a phishing site in 2021. However, thanks to technology and security education, things are improving. Unfortunately, cryptocurrency re-opens this old wound once again. While it is often believed that investors and users in the crypto landscape fully understand the technology they are using, a report by Cardify[77] explains that "the majority of investors (83.1%) report moderate or low levels of cryptocurrency knowledge". Without fully understanding the technology that they are using; it becomes significantly harder for victims to see the signs of an attack. The difference between a legitimate wallet signature and a malicious one is not an easy spot and explains the reason why "Ice Phishing" became such a large part of 2022's threat landscape. Standard phishing techniques often rely on either a "spray and pray" style attack- hoping for someone to fall victim within a large attack group- or a "spear phishing" attack, where specific individuals are targeted utilising inside knowledge to gain a much higher success rate. "Ice Phishing" on the other hand has the best of both worlds, by utilising large cryptocurrency communities to allow for a spear phishing level of customisation to a much larger audience. This is why such effectiveness has been noted, and why the communities have become such a goldmine for a well-crafted phishing campaign. End-users will always be a critical asset within the general security landscape, but within the crypto threat landscape they play a significant role. Education around cryptocurrencies and blockchain technology is the key to supporting this as by increasing general awareness surrounding the threats to cryptocurrency, the effectiveness of these kinds of attacks can be reduced. This becomes even more of a necessity as cryptocurrencies continue their trend from niche online currency to popular commodity. Last year a survey showed[78] that cryptocurrencies were the second most well-known kind of investment, behind traditional stocks; however, despite this level of attention, around 60% of respondents admitted that they "did not understand cryptocurrencies". By bolstering the level of general as well as specific cryptocurrency security awareness, it is possible to reduce the risks significantly by building a more secure crypto community.

A final trend seen throughout 2022's attacks is the vital need for cryptocurrency companies to understand the level of risk they hold and build their security policies around this. A multitude of attacks were the result of insufficient software tests being conducted or a lack of care and attention taken when building the security procedures surrounding the business. Simple changes such as the inclusion of regular contract audits and infrastructure tests could have prevented some of the major attacks of the year, saving potentially hundreds of millions of dollars. While originally the access to good contract auditing was limited, the large number of companies now offering this is a positive step in the right direction. This enables blockchain organisations big and small to gain access to high quality security testing. The importance of standard security policy must also not be forgotten. Multi-factor authentication, traditional penetration tests and security by design are fundamental principles that enable further safety both for users and for the organisation as a whole. Combining this with well-funded and maintained bug bounty programs helps to encourage this complete secure environment by utilising the wealth of knowledge within the "white hat" space to discover and fix any issues discovered. To do this, however, organisations must first understand the risks, and this is something that is critically needed within the cryptocurrency space. Understanding the risk that a breach may pose to the value of customer funds, a chain's ability to operate, or to other systems internally or externally can make the process of creating security policy easier and more effective. Conducting regular audits of each piece of infrastructure to understand the risk level they pose to all aspects of the organisation builds not only a better understanding of a threat landscape, but also of how to protect it, entrenching security as a foundation within the cryptocurrency landscape.

While looking at 2022 has given insights into how the cryptocurrency space has evolved, it also allows some predictions into the threat landscape in 2023. The FTX saga threw cryptocurrency fraud and crime into the spotlight and shone a light into an area that most agencies were yet to tackle at this scale. As this and other crimes become more commonplace, it is not difficult to see the regulations on both blockchain companies and holders tightening as governments begin to strengthen their grip on the field that is quickly catching up on them. Another area which is likely to see some development is that of the cryptocurrency malware space: while 2022 has seen the utilisation of traditional cryptojacking malware, there appears to have been very little new development of the features within them. As defences improve, it is possible that the malware used will become more sophisticated as it begins to form part of larger threat groups' weaponry.

As the blockchain space grows, it is vital that throughout 2023 threat actors are not leading the way. Already in 2022, these attackers began to pull ahead in their general understanding of the landscape, able to quickly adapt and utilise new tools, tokens, and techniques to avoid investigation and prosecution. As 2023 progresses this is a knowledge gap that needs to be closely monitored and addressed. If the cryptocurrency threat landscape is to improve, the positive forces within the industry need to be leading the charge, developing new methods and protocols for blockchain security, and providing education to help all members of the community, both technical and non-technical. While some positive steps were made in 2022, these must continue as the constant tug of war rages between those who protect and those who abuse the ever-growing technology. By taking the lead in this race, threat actors can be placed on the backfoot to limit their operational capabilities, allowing the future crypto threat landscape to be shaped not through the actions of cybercrime, but by actions taken to prevent it.

Joe Wrieden

Endnotes

1 https://docs.aave.com/faq/flash-loans

2 https://bean.money/

3 https://medium.com/coinmonks/beanstalk-exploit-a-simplified-post-mortem-analysis-92e6cdb17ace

4 https://www.investopedia.com/news/largest-cryptocurrency-hacks-so-far-year/

5 https://bean.money/blog/path-forward

6 https://twitter.com/osec_io/status/1579969927020412929

7 https://twitter.com/mangomarkets/status/1579976051878658048

8 https://archive.nytimes.com/www.nytimes.com/library/cyber/week/0914panix.html

9 https://z.cash/

10 https://twitter.com/lopp/status/1577718171468972033

11 https://twitter.com/ElectricCoinCo/status/1578161923178516480

12 https://www.allerin.com/blog/employing-blockchain-to-mitigate-ddos-attacks

13 https://coinmarketcap.com/rankings/exchanges/dex/

14 https://twitter.com/CurveFinance/status/1557107088962224132

15 https://www.binance.com/en/blog/community/a-note-on-curve-finance-and-preventing-dns-attacks-584383509573613582

16 https://data.actionfraud.police.uk/cms/wp-content/uploads/2021/07/2020-21-Annual-Assessment-Fraud-Crime-Trends.pdf

17 https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/natureoffraudandcomputermisuseinenglandandwales/yearendingmarch2022

18 https://www.microsoft.com/en-us/security/blog/2022/02/16/ice-phishing-on-the-blockchain/

19 https://www.ft.com/content/c7d2eeae-9a66-4dc4-a10e-11dcd2807600

20 https://www.michigan.gov/ag/consumer-protection/consumer-alerts/consumer-alerts/scams/cryptocurrency-scam-pig-butchering

21 https://www.globalantiscam.org/about

22 https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

23 https://www.soliduslabs.com/reports/rug-pull-report

24 https://www.justice.gov/usao-sdny/pr/two-defendants-charged-non-fungible-token-nft-fraud-and-money-laundering-scheme-0

25 https://www.microsoft.com/en-us/security/blog/2022/02/16/ice-phishing-on-the-blockchain/

26 https://blog.checkpoint.com/2022/02/20/new-opensea-attack-led-to-theft-of-millions-of-dollars-in-nfts/

27 https://blog.chainalysis.com/reports/crypto-mixers/

28 https://roninblockchain.substack.com/p/community-alert-ronin-validators

29 https://home.treasury.gov/news/press-releases/jy0916

30 https://twitter.com/bantg/status/1556712790894706688

31 https://twitter.com/TornadoCash/status/1557048526986780677

32 https://hub.elliptic.co/analysis/cross-chain-crime-more-than-half-a-billion-dollars-has-been-laundered-through-a-cross-chain-bridge/

33 https://www.reuters.com/legal/us-charges-accused-mango-crypto-manipulator-with-fraud-2022-12-27/?taid=63ab83809b50560001124bc4

34 https://twitter.com/Crema_Finance/status/1543638844410499073

35 https://etherscan.io/tx/0xa38b894b2bb1c8a3eaf816d879a542e080443f7bf5a84214a00e6e509f9f6130

36 https://boxmining.com/cross-chain-bridge-hack-explained/

37 https://docs.qbt.fi/

38 https://xbridge.qbt.fi/bridge

39 https://certik.medium.com/qubit-bridge-collapse-exploited-to-the-tune-of-80-million-a7ab9068e1a0

40 https://etherscan.io/txs?a=0xd01ae1a708614948b2b5e0b7ab5be6afa01325c7

41 https://www.forbes.com/sites/ninabambysheva/2022/12/28/over-3-billion-stolen-in-crypto-heists-here-are-the-eight-biggest/?sh=74ff4f9a699f

42 https://wormholenetwork.com

43 https://wormholecrypto.medium.com/wormhole-incident-report-02-02-22-ad9b8f21eec6

44 https://www.investopedia.com/terms/1/51-attack.asp

45 https://www.investopedia.com/terms/1/51-attack.asp

46 https://roninblockchain.substack.com/p/community-alert-ronin-validators?s=w

47 https://etherscan.io/tx/0xc28fad5e8d5e0ce6a2eaf67b6687be5d58113e16be590824d6cfa1a94467d0b7

48 https://etherscan.io/tx/0xed2c72ef1a552ddaec6dd1f5cddf0b59a8f37f82bdda5257d9c7c37db7bb9b08

49 https://www.fbi.gov/news/press-releases/press-releases/fbi-statement-on-attribution-of-malicious-cyber-activity-posed-by-the-democratic-peoples-republic-of-korea

50 https://twitter.com/sniko_/status/1528320829741842432

51 https://web.archive.org/web/20220703165818/https://twitter.com/britisharmy

52 https://kotaku.com/smash-bros-mkleo-nft-crypto-twitter-hacked-hack-ultimat-1848717423

53 https://web.archive.org/web/20220703165856/https://www.youtube.com/c/britisharmy

54 https://www.mcafee.com/blogs/other-blogs/mcafee-labs/crypto-scammers-exploit-elon-musk-speaks-on-cryptocurrency/

55 https://www.creativebloq.com/news/star-wars-deepfake

56 https://www.bleepingcomputer.com/news/security/elon-musk-deep-fakes-promote-new-bitvex-cryptocurrency-scam/

57 https://www.binance.com/en/blog/community/scammers-created-an-ai-hologram-of-me-to-scam-unsuspecting-projects-6406050849026267209

58 https://twitter.com/NFTherder/status/1533037408144572417

59 https://twitter.com/NFTherder/status/1543607137431085057

60 https://crypto.com/

61 https://crypto.com/product-news/crypto-com-security-report-next-steps

62 https://www.zb.com/en/message/1406

63 https://twitter.com/peckshield/status/1554849892153131011

64 https://www.investopedia.com/tech/whats-cryptocurrency-exit-scam-how-spot-one/

65 https://www.coindesk.com/business/2022/11/02/divisions-in-sam-bankman-frieds-crypto-empire-blur-on-his-trading-titan-alamedas-balance-sheet/

66 https://twitter.com/cz_binance/status/1589283421704290306

67 https://restructuring.ra.kroll.com/FTX/

68 https://www.wsj.com/articles/ftx-tapped-into-customer-accounts-to-fund-risky-bets-setting-up-its-downfall-11668093732

69 https://www.reuters.com/technology/ftxs-bankman-fried-begged-rescue-even-he-revealed-huge-holes-firms-books-2022-11-16/

70 https://twitter.com/zachxbt/status/1591276687228035074

71 https://hub.elliptic.co/analysis/477-million-in-unauthorized-transfers-from-ftx/

72 https://etherscan.io/txs?a=0x59abf3837fa962d6853b4cc0a19513aa031fd32b&f=2

73 https://twitter.com/chainalysis/status/1594349583416840199

74 https://www.bnbchain.org/en/blog/bnb-chain-ecosystem-update/

75 https://www.coindesk.com/business/2022/10/03/binance-to-train-law-enforcement-on-how-to-stop-crypto-crime/

76 https://cloudmanaged.ca/wp-content/uploads/2021/09/2021-cyber-security-threat-trends-phishing-crypto-top-the-list.pdf

77 https://www.cardify.ai/reports/crypto

78 https://finbold.com/over-60-of-people-dont-understand-crypto-global-study-reveals/

About Cyjax

Cyjax was formed in 2012. Working closely with the financial sector, we developed technologies and methodologies to help stem the advance of digital threats impacting banks and consumers around the world. We quickly established ourselves as a leading provider of cyber threat intelligence capabilities across all industry verticals, a journey we continue today. Cyjax is built on its own growth and remains wholly owned by its founding members in the UK.

CYJAX

Cyjax Limited
The Old Chapel, Union Way
Witney
Oxon OX 6HD

info@cyjax.com
+44 (0)20 7096 0668
www.cyjax.com

bsi
ISO/IEC
27001
Information Security
Management
CERTIFIED
IS 676012