ciphertrace
by

Cryptocurrency crime and anti-money laundering

REPORT

MARCH 2023

Contents

Opening comment

Dave Jevans
CEO, Ciphertrace,
a Mastercard company

Thanks to those of you who downloaded and read our previous report, which focused on the state of the cryptocurrency world in the second quarter of 2022.

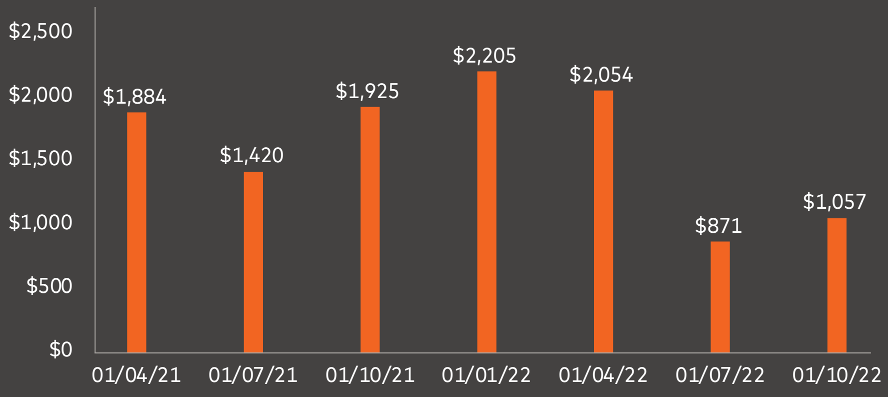
The prior report highlighted virtual asset service providers' (VASPs') and know your customer (KYC) risk across the globe, all powered by Ciphertrace analytics and intelligence. This report will focus on dark markets and cross-chain bridges. We continue looking at the trends, current events, hacks, thefts, exploits, and global regulatory developments. Our goal, as always, is to keep you informed and to highlight emerging and ongoing trends to give you the best possible information to keep your business running smoothly.

- At the end of Q3, the total market cap of all crypto assets, including stable coins and tokens, was approximately $1.1 trillion.
- On August 8, the Office of Foreign Assets Control (OFAC) sanctioned virtual currency mixer, Tornado Cash, "which ha[d] been used to launder more than $7 billion worth of virtual currency since its creation in 2019".
- At the end of Q3 2022, the Internal Revenue Service seized approximately $4 billion in virtual assets vs $3.5 at fiscal year-end 2021.
- The third quarter was plagued with bankruptcy filings throughout the industry with Nuri, Voyager Digital, Celsius, Three Arrows Capital, and others.
- After NFTs exploded in both market volume and dollar value in 2021, values rapidly eroded in 2022. The top eight blockchains for NFT trading plunged 76% in Q3 2022 ($2.3 billion) compared to Q2 ($9.2 billion) and are down 83% compared to Q1 2022 ($13.9B).
- Total value locked (TLV) of decentralized finance in the third quarter was roughly $54 billion. The Ethereum blockchain continues to have the largest volume of virtual asset tokens (57%).
- Across seven major hacks/exploits, losses reached $383 million.

Executive summary

At the end of the third quarter, the total market cap of all crypto assets, including stable coins and tokens, was approximately $1.1 trillion. Although this represents an increase of 21.3% compared to the second quarter ($871 billion), virtual assets have lost almost 50% of its value at the beginning of 2022 ($2.2 trillion) and have lost 63% compared to its all-time high ($2.83 trillion at November 14, 2021). Prices indicate that we are still in a "crypto winter" – a term used to describe the substantial declines in asset prices and market capitalization for virtual assets – as depicted in Graphic 1, which includes data for the last seven quarters.

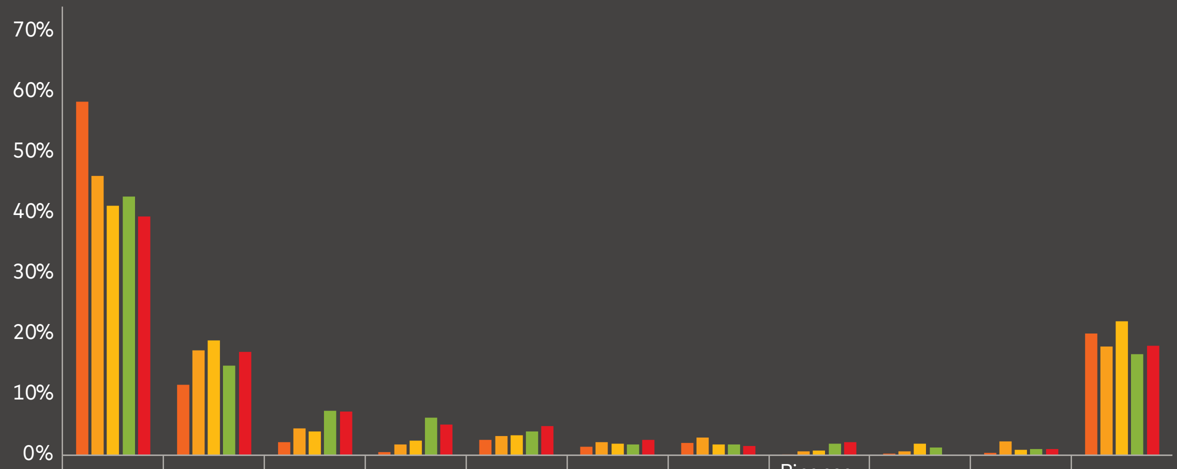
Graphic 1: Market cap ($ in billions) of virtual assets



Source: Coinmarketcap

As of September 30, 2022, Bitcoin (btc) was just above $19,500 having lost 38.6% of its value compared to Q2 (btc price dropped from $31,792). Nevertheless, bitcoin continues to be the largest crypto asset by market capitalization (40%). In an interesting development, Solana lost 26% of its value compared to Q2 2022; Solana Foundation noted ties to FTX in blog posts during Q4 2022. The price dropped from $45.77 on June 1,2022 to $33.95 on September 30, 2022, a decline of 75% of its value compared to its all-time high $136.78 on 4/4/2022. This may primarily be attributed to the bear market, as well as the Slope mobile wallet exploit in early Q3 and the network outage at the end of the same quarter. Graphic 2 shows virtual asset market caps for some of the largest individual assets; from a total population of over 20,000 virtual assets, including cryptocurrencies, stable coins and other tokens.

Graphic 2: Market cap — by top virtual assets

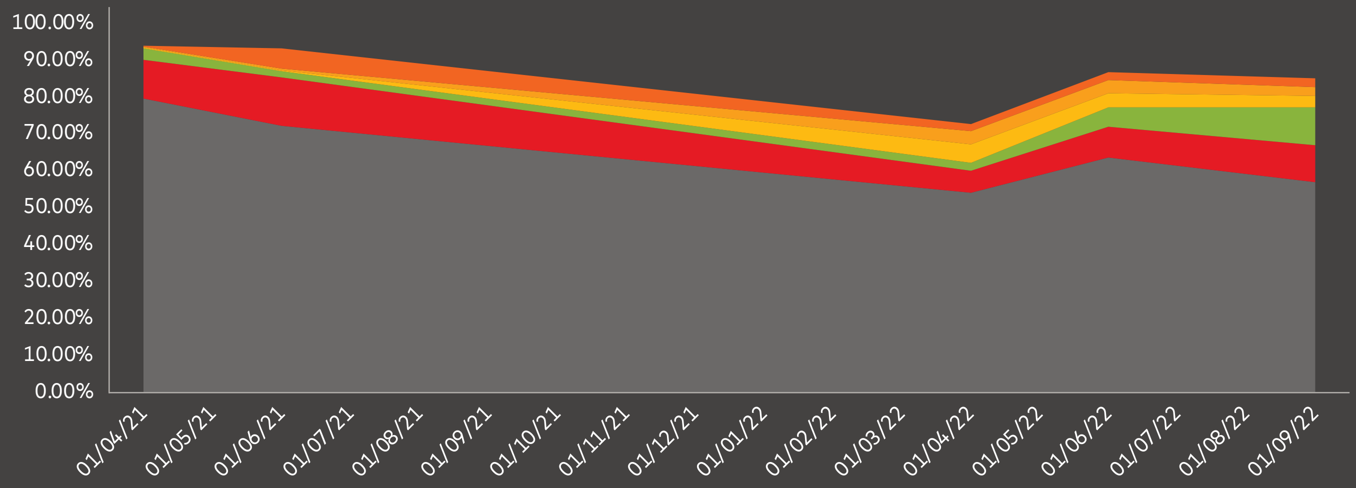


	bitcoin	ether	tether	USD coin	BNB	XRP	Cardano	Binance USD	Solana	Dogecoin	All Other
🟧 % of market cap at 4/1/2021	59%	12%	2%	1%	3%	1%	2%	0%	0%	0%	20%
🟧 % of market cap at 6/30/2021	46%	17%	4%	2%	3%	2%	3%	1%	1%	2%	18%
🟨 % of market cap at 4/1/2022	41%	19%	4%	3%	3%	2%	2%	1%	2%	1%	22%
🟩 % of market cap at 6/30/2022	43%	15%	7%	6%	4%	2%	2%	2%	1%	1%	17%
🟥 % of market cap at 10/02/2022	40%	17%	7%	5%	5%	3%	2%	2%	0%	1%	18%

Source: Coinmarketcap

Decentralized finance (DeFI) is a critical topic to understand as the report later discusses cross-chain bridge vulnerabilities. Total Value Locked (TVL) at the end of Q3 was roughly $54 billion, practically unchanged compared to the end of Q2, however, 67% down compared to Q2 start ($165B at April 4, 2022). The Ethereum blockchain continues to have the largest volume of virtual asset tokens (57%). Tron gained value from the Terra collapse. Graphic 3 illustrates the percentage of TVL by various blockchains.

Graphic 3: Total value locked by blockchain



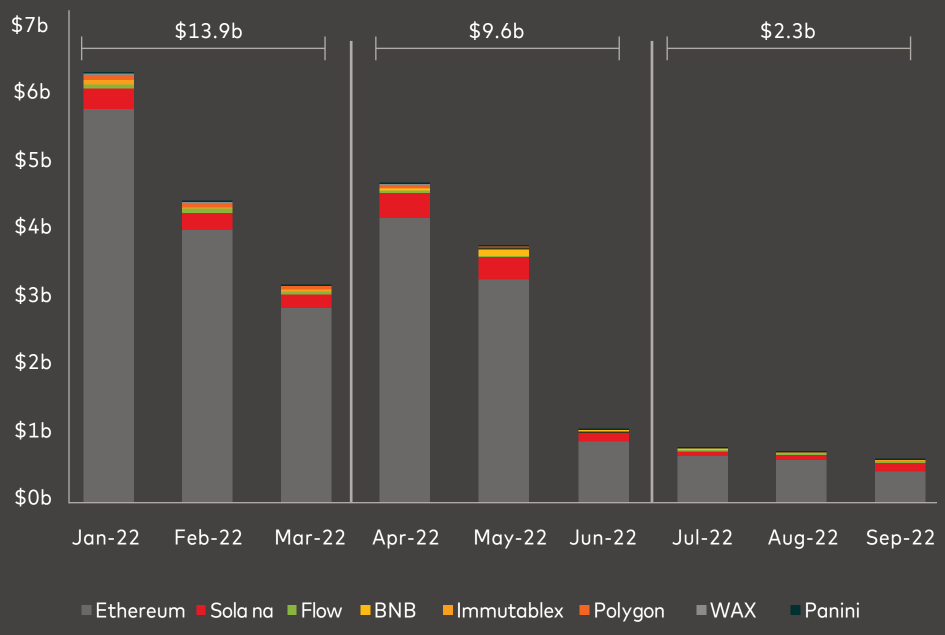
	01/04/21	30/06/21	01/04/22	30/06/22	30/09/22
🟧 Polygon	0.16%	5.37%	2.04%	2.27%	2.34%
🟧 Solana	0.30%	0.54%	3.47%	3.51%	2.39%
🟨 Avalanche	0.26%	0.17%	4.95%	3.73%	3.04%
🟩 Tron	3.11%	1.82%	2.12%	5.41%	10.34%
🟥 BSC	10.51%	13.07%	6.16%	8.16%	10.02%
◼ Eth	79.69%	72.36%	54.17%	63.88%	57.12%

Source: DeFiLlam

Additionally, non-fungible tokens (NFTs) is also a pertinent topic to understand as the report dives into cross-chain bridge vulnerabilities. The interoperability between blockchains using cross-chain bridges has applicability to both DeFi and NFT users. After NFTs exploded in both market volume and dollar value in 2021, values rapidly eroded in 2022. As illustrated in Graphic 4, the top eight blockchains for NFT trading plunged 76% in Q3 2022 ($2.3 billion) compared to Q2 ($9.2 billion) and are down 83% compared to Q1 2022 ($13.9 billion).

Graphic 4: Q3 2022 NFT trading volume across top eight chains
NFT winter has arrived

Top eight chains for NFT trading volume (Jan–Sep 2022)



Source: CoinGecko; FootPrint Analytics; Cryptoslam

The third quarter was filled with significant events, many involving or potentially involving financial crimes compliance considerations. In July, Voyager Digital (a digital asset brokerage), Three Arrows Capital (a hedge fund) and Celsius (a crypto lender) filed for bankruptcy. At this time, there is no clear and documented evidence of fraudulent or misleading activity, but many questions seem to have remained unanswered in Q3 pertaining to Three Arrows Capital. In August, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctioned virtual currency mixer Tornado Cash. This had ripple effects in the industry and caused significant compliance impacts to various entities within the virtual asset ecosystem, such as Circle. In September, the Ethereum merge took place, moving from proof-of-work to proof-of-stake, in which the network is made up of validators instead of miners. Among some benefits from the Ethereum merge is that proof-of-stake does not require mining equipment, it is estimated to require approximately 99.95% less energy compared to proof-of-work. For example, a 51% attack has an exponentially higher cost. Read more in our articles about the Ethereum merge and Tornado Cash sanctions on Ciphertrace's blog.

Cross-chain bridges

"Bridges are frequently abused by criminals to obfuscate the origin of stolen cryptocurrency and to avoid their funds being frozen or traced."

Bridge background

Cross-chain bridges, or simply bridges are services or contracts that connect two economically and technologically different blockchains, enabling users to swap value into tokens and then transfer that value over to another chain (i.e., BTC on/to ETH). Bridges are primarily utilized by crypto investors who want to take digital assets from one chain and spend, swap, or invest those assets on another blockchain. However, as with any new technology, bridges are frequently abused by criminals to obfuscate the origin of stolen cryptocurrency and to avoid their funds being frozen or traced. Although Ciphertrace investigators can trace funds through these services, there is an urgency for AML professionals to equip themselves with the knowledge to prevent fraud and identify risks associated with bridges.

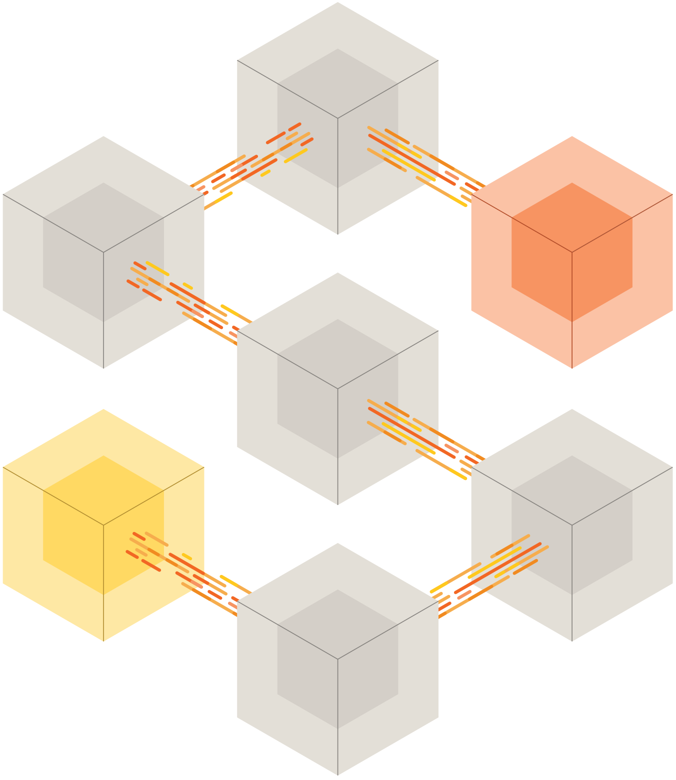
Using "wrapped" tokens is one of the most popular ways to transfer the value of digital assets from one blockchain to another. The initial coin, Bitcoin for example, is set aside into a centralized address, where it is programmatically wrapped and stored — similar to a bank safe-deposit box. On the other side of the bridge, a new token is then created, or "minted" so that it can be used on the native chain of other networks in the wrapped derivative form (such as Wrapped Bitcoin on Ethereum). This technological advantage permits the ability for the transfer of previously isolated assets created on different blockchains to be interoperable on many chains thanks to wrapped tokens.

Wrapped tokens and bridge protocols present enormous possibilities for blockchain bridge applications in the cryptocurrency industry. Opportunities for new staking rewards and liquidity markets are made possible by the elasticity of moving digital assets from one crypto ecosystem to another. That being said, with this new opportunity comes the worrying trend of significant hacks that have targeted crypto bridges in recent years that cause many to doubt the underlying safety of the various bridge platforms. Cross-chain bridges are attractive targets for criminals.

"Smart contracts leave investors susceptible to the possibility of exploits within the code itself."

The vulnerabilities of bridges are not so different from the basic cryptocurrency fundamentals of understanding the difference between custodial and non-custodial ownership. Custodial bridges require the involvement of a centralized actor, and therefore do not meet the requirements of actors committed to an end-to-end decentralized process. The trust in any centralized entity opens the possibility of hackers to direct their energy to single points of failure. Meanwhile, non-custodial bridges rely on self-executing code in a permissionless environment that carries out smart contracts. These smart contracts leave investors susceptible to the possibility of exploits within the code itself. Therefore, it is important that non-custodial bridges undergo extensive audits of their code before consumer trust and regulatory compliance can be achieved.

Cross-chain bridge exploit refers to a security vulnerability or attack that takes advantage of the transfer of assets or data between different blockchain networks through a bridge or connecting mechanism. These exploits can occur in various forms, including but not limited to the manipulation of smart contract code, the theft of digital assets, or the alteration of transaction data.



Major hacks, thefts, and fraud

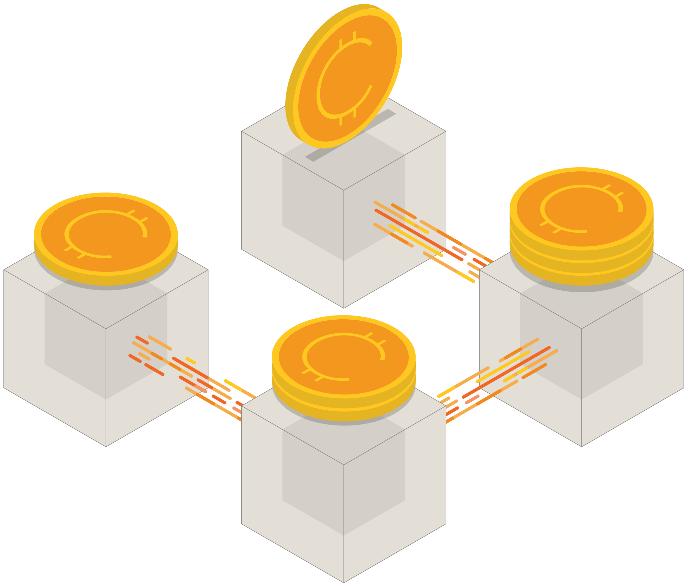
Ciphertrace continues to investigate and analyze attacks. These exercises are necessary to not only slow the attacks and their frequency, but also to prepare and adapt for what is next. Investigations and intelligence are designed to evaluate what happened, address the issues, and determine an appropriate response. From the continued post-mortem of major 2022 cases to new breaches and exploits, illicit activities continue to impact the virtual asset ecosystem during Q3 2022. Hacks and exploits totaled $383 million in this period. Below are summaries of major occurrences in Q3.

Q3 2022 hacks/exploits

Entity	Amount	Date
Nomad	$200m	8 January 2022
Wintermute	$160m	9 Febuary 2022
Crema finance	$8m	2 July 2022
Audius	$6m	23 July 2022
Solana	$5m	2 August 2022
Nirvana	$3.5m	28 July 2022
Curve	$600k	9 August 2022
Total	**$383m**	

Source: Various publicly available sources.

Ciphertrace can help you understand and mitigate your crypto risk. Reach out to learn more about Ciphertrace products and services.



Nomad

Bridge hacks and exploits were very active in the past year. However, in Q3 the most notable bridge exploit was Nomad being plundered of $190 million due to hundreds of users opportunistically taking advantage of a single typo in the code. The issue in Nomad's armor was in the way the code prevented itself from accurately authenticating a message was accepted before the transaction was executed. Once the hack was pulled off, it was easy for users to replicate the original theft by copying the transaction call data and changing it to their own personal address. In the case of Nomad, code exploits are a reminder that protocols are only has strong as the code underwriting them. While it is encouraging that there was only one major bridge exploit in Q3, bridges seem to have a way to go before they are accepted to be as safe as cryptocurrency exchanges in the court of public opinion.

Wintermute

Wintermute, a leading global algorithmic trading firm in digital assets, was hacked for approximately $160 million on September 20, 2022 potentially due to a wallet compromise via a vulnerability in Profanity, a customized vanity address generator which is speculated to have played a massive role that was disclosed by 1inch (an exchange aggregator that searches for the lowest crypto prices by scanning decentralized exchanges) days prior. The attacker exploited the bug in Profanity to recover the private key to the Wintermute hot wallet. A hot wallet is connected to the internet.

Acala

Acala is a DeFi platform. It issues the aUSD stablecoin and operates by leveraging the functionality of the Polkadot blockchain. It allows for DeFi operations on the Polkadot network, including borrowing, lending, and stablecoin activities. An on-chain setup error allowed attackers to mint aUSD (amount of loss $52 million). The vulnerability caused aUSD to lose its peg to the U.S. dollar, initially falling to $0.60 and hovering around $0.90. Acala suspended the protocol shortly after the attack (August 14, 2022) and disabled the transfer of the stolen aUSD.

Crema Finance

Crema Finance a centralized liquidity DeFi application on the Solana chain announced a $8.8 million hacker flash loan attack. Hackers bypassed contract checks by creating a fake price change data account (Tickaccount) and then used fake price data and flash loans to steal huge fees from the fund pool (July 3, 2022). Following a long negotiation, Crema Finance attackers agreed to collect 45,455 SOL (~$1.7 million) as a white hat bounty (eventually the amount of loss) and returned 6,064 Ethereum and 23,967.9 SOL (~$8.1 millino). Crema Finance has now upgraded to v2.0.

Nirvana

Nirvana, a stablecoin project on the Solana chain, was attacked by a flash loan. The attacker used a flash loan to borrow $10,250,000 USDC from Solend by deploying a malicious contract, and then called the Nirvana contract buy3 method to acquire a large amount of ANA tokens. Eventually the hacker sold the ANA tokens and passed all the dirty money through the cross-chain bridge transfer before it could be detected as a flash loan.

Audius

The community treasury of Audius, a web3music streaming service platform, was hacked, losing 18.5 million AUDIO Tokens (amount of loss: $1.1 million), due to contract vulnerabilities. The hackers exchanged the funds for about 705 ETH on Uniswap. Audius officially stated that the problem has been found and is currently being repaired.

Dark market — third quarter analysis

"Dark markets function primarily as black markets, selling or brokering transactions."

A **Dark market** is a commercial website that operates via darknets such as Tor or I2P. They function primarily as black markets, selling or brokering transactions. Dark Markets include crypto addresses associated with individuals and organizations who sell or traffic in human beings, illicit arms, counterfeit currency, forged documents, illegal narcotic drugs and psychotropic substances, unlicensed or out-of-region pharmaceuticals, steroids, sexually exploitative materials, counterfeit products, wildlife, grey market, counterfeit, or pirated products, stolen goods or other illicit items.

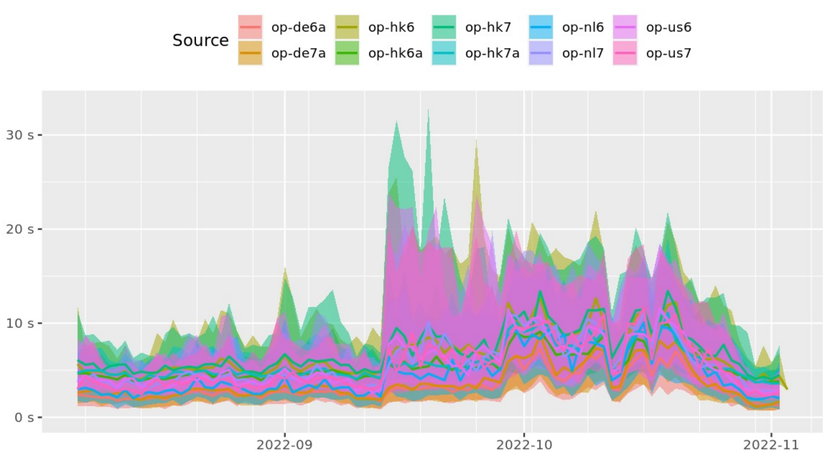
Tor network

A significant amount of criminal dealings involving cryptocurrency is conducted on the darknet. Criminal markets, forums, shops, ransomware blogs, etc. are generally hosted on the darknet. The most significant darknet network is Tor; others being I2P, freenet, and zeronet.

The end of Q3 2022 was turbulent for the Tor network. It appeared there may have been a network wide attack beginning mid-September that eased at the end of October. Ciphertrace researchers noticed darknet markets suffering from the attack with extensive downtime in mid-September.

The Tor Project provides metrics, including time to complete a static file download over the network. The graph below is the time to complete a 1MiB request to a public server. The graph shows the disruption to the network occurred around when our researchers identified criminal sites struggling to stay online. The disruption continued until the end of October. Indeed, our researchers have concluded that criminal sites seem to be struggling less to stay online.

Time to complete 1 MiB request to public server



Source: The Tor project

> "Ciphertrace researchers consider OMG!OMG! to be the most significant Russian darknet market currently running."

During this disruption, many criminal sites and their users pushed for I2P mirrors. The I2P network is more resilient, and it's likely to gain more traction over time. However, the Tor network is more well-known and easier to use for the average user. This makes it unlikely for the I2P network to gain as much traction, even if it is better. This is particularly true for darknet markets, as a large portion of the customer base are average users, and for ransomware sites, their users are normal individuals.

Major criminal entities

The following are the top three to five most significant entities in each category, based on Ciphertrace data and researcher opinion. Significance is mainly based on estimated transaction volume as well as number of users. The largest English-speaking darknet markets include: AlphaBay; ASAP Market and Bohemia.

AlphaBay was the largest darknet market in 2017 with over 400,000 users before the site was seized on July 5. In the Summer of 2021, Desnake, a former AlphaBay admin, resurfaced on a criminal forum to announce the relaunch of the market. The new AlphaBay is more security-focused, particularly as the market is Monero-only. In mid-September 2022, AlphaBay's self-reported statistic on the number of buyer accounts on the site surpassed 1 million. This would make it one of the largest markets of its kind, vastly surpassing its own peak.

AlphaBay is currently the largest Monero-only darknet market, beating Monopoly Market, which was originally a Monero-only service, but eventually caved to user pressure and accepted Bitcoin.

The largest Commonwealth of Independent States (CIS) region darknet markets included: OMG!OMG!; Shkaf; o3shop; Mega; and BlackSprut. After the seizure of Hydra market in 2021, the competition for darknet markets increased significantly in the CIS region, mostly based out of Russia. Ciphertrace researchers consider OMG!OMG! to be the most significant Russian darknet market currently running, but it doesn't dominate as much as Hydra did.

"Geographic intelligence is difficult to identify for criminal entities, as they attempt to obfuscate this information, until they're seized by law enforcement."

The following are some of the most significant fraud entities currently active: Benumb, Biden Cash, Brians Club, Genesis Market, HGN01, and Rescator. Most are carding sites, while Genesis Market is the long-running market for "bots".

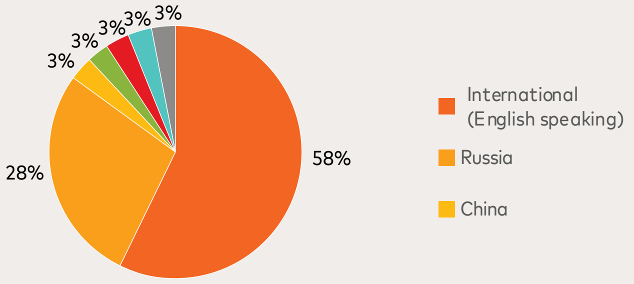
- Carding sites assist in the buying and selling of stolen credit card information. Often, the larger carding sites are "autoshops". An autoshop is a carding site that allows buyers to check if a stolen card is still active and, if it isn't, automatically get a refund.
- On Genesis Market, "bots" refers to digital identities for sale. Genesis Market mainly sells cookies, digital fingerprints, stolen login info, etc. to aid criminals in impersonating individuals and accessing their accounts. There are typically over 400 thousand different digital identities for sale at any one time.

Sample of regional statistics for darknet marketplaces

Geographic intelligence is difficult to identify for criminal entities, as they attempt to obfuscate this information, until they're seized by law enforcement. Language used, regional operational restrictions and other information give some indication as to an entity's jurisdiction. The following graph is largely based off the above details.

During Q3, Ciphertrace researchers were monitoring active, legitimate, and unique darknet markets in the following areas:.

Dark market geographic impacts



Source: Ciphertrace

In the above data, what qualifies as a darknet market is a darknet site that allows multiple/any vendor(s) to list their items for sale and that facilitates the sale of those items to buyers. A site that is hosted by an individual vendor to advertise and sell their own goods does not qualify as a market. That would instead qualify as a vendor shop. Furthermore, there are numerous fake darknet markets that aim to scam would-be buyers, which are not included in these numbers.

Ciphertrace can help you understand and mitigate your crypto risk. Reach out to learn more about Ciphertrace products and services.

Changes in global regulation

Below we've highlighted key regulatory and legislative updates and related law enforcement activity around it.

Regulatory and Legislative Analysis — September 30, 2022

Regulatory and Legislative Analysis — August 8, 2022

Regulatory and Legislative Analysis — July 11, 2022

Conclusion

The world of cryptocurrency saw tremendous challenges in Q2 2022 and those continued into Q3 2022. Market volatility lessened but major events continued, some of which were a product of financial crimes compliance failures. As noted in our sections on legislation and enforcement, the world's governments continue to grapple with how best to regulate virtual assets and virtual asset related activities. It became apparent in many countries that regulation would occur through enforcement by regulatory agencies, all of which were being done in an effort to combat fraud and financial crimes in the ecosystem.

For those reading this in VASPs, banks, payment processors and both federal and local law enforcement, Ciphertrace has considerable expertise and tools to help monitor the movement of cryptocurrency and can assist. Get in touch with us at ciphertrace.com. Sign up for email alerts to stay up to date on trends, our latest reports and significant changes to the industry.

Disclaimer
Ciphertrace is a wholly-owned Mastercard company that delivers cryptocurrency AML and counter terrorism financing (CTF) tools, blockchain forensics, and regulatory monitoring solutions. Further details about Ciphertrace can be found at www.ciphertrace.com. This publication is intended as a general overview and discussion of the subjects herein, and is not intended to be, and should not be used as, a substitute for taking legal or financial/investment advice in any specific situation. Mastercard will accept no responsibility for any actions taken or not taken on the basis of this publication.

Designed by Mastercard Creative Studio