Who's Who on the Blockchain?

Mapping the Key Players in the Cryptocurrency Ecosystem

Chainalysis

Table of Contents

Taking a trust-based approach to the cryptocurrency ecosystem 1

How we categorize the key players in cryptocurrency 2

The complete guide to cryptocurrency service and organization categories 3

Merchant services 4

Hosted wallets 5

Mining pools 7

Exchanges 8

Nested Services 12

OTC Brokers 14

DeFi 15

Cryptocurrency ATMs 18

Gambling 19

Cyber infrastructure as a service 20

Services in high-risk jurisdictions 24

Darknet Markets 24

Stolen funds 31

Illicit actor/organization 36

Ransomware 37

Terrorist financing 42

Sanctions 44

Child Sexual Abuse Material Sites 46

Taking a trust-based approach to the cryptocurrency ecosystem

Since Bitcoin's launch in 2009, cryptocurrency has driven new markets, spurred advancements in financial infrastructure, and driven innovative thinking in how to meet the world's economic needs.

Stakeholders such as governments, industry operators, and traditional financial institutions need a shared understanding of the players in the cryptocurrency ecosystem in order to drive continued growth and adaptation. Key to identifying and safely approaching new opportunities is an understanding who are the entities conducting cryptocurrency transactions and the level of risk and illicit activity associated.

Chainalysis demystifies cryptocurrency. As the industry's leading provider of blockchain analysis, investigations, and compliance software, we empower banks, businesses, and governments to understand which entities are transacting with cryptocurrency so that the industry can continue to grow safely and sustainably.

In this guide, we use our comprehensive, best-in-class, blockchain dataset along with decades of combined investigative experience, to break down the key players in cryptocurrency transactions according to the level of risk they present.

1

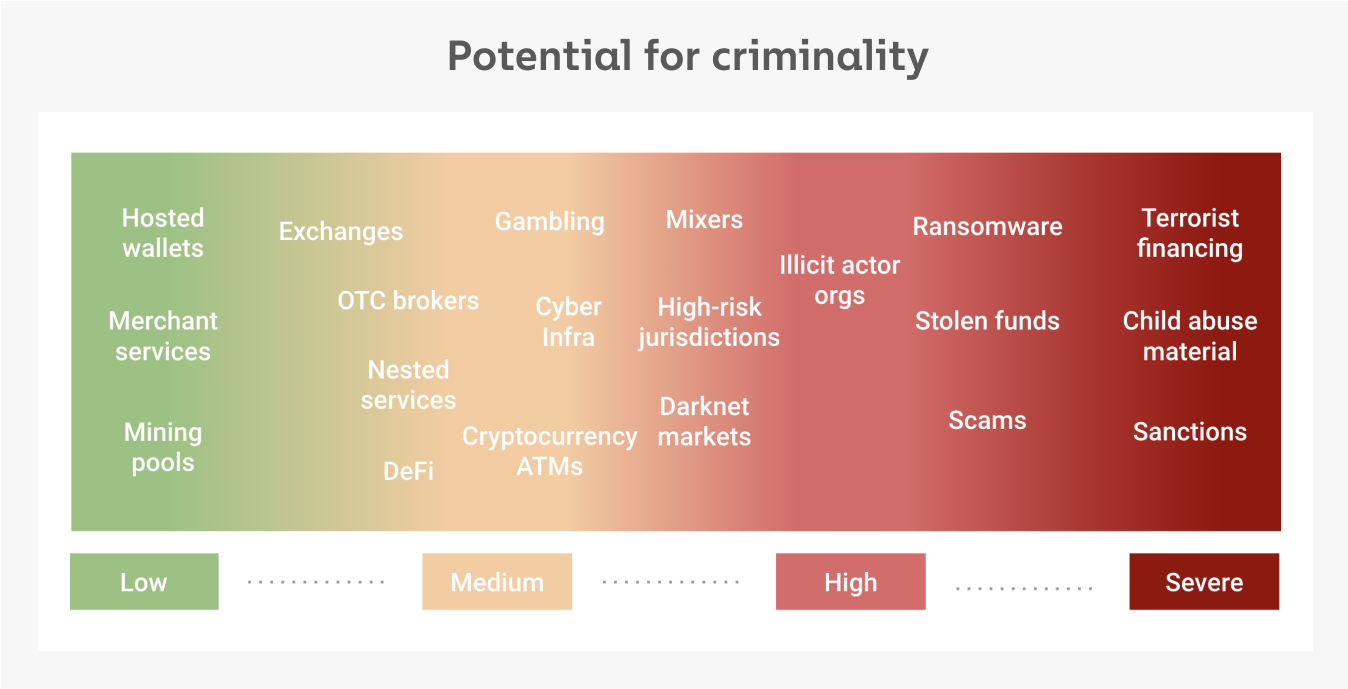
How we categorize the key players in cryptocurrency



The easiest way to group the entities transacting with cryptocurrency is to think about the ways cryptocurrency is used.

- Mining
- Storage of funds
- Investing and exchanging
- Buying and selling of legal goods and services
- Obfuscating activity for privacy reasons or to conceal illegal activity
- Buying and selling of illegal goods and services
- Stealing or scamming

The entities associated with each of these use cases make up the services and organizations, described throughout this guide, which we have organized according to risk level.



On the left are services such as hosted wallets and merchant services, which are used less often for illicit activity and are therefore lower risk.

On the right are entities such as terrorist financing schemes, which are illegal under any circumstances and therefore rated as severely risky.

Those in the middle aren't universally considered illegal, but are often linked to or used to aid in criminal activity. For example, while gambling is perfectly legal in many jurisdictions, it has also historically been used as a means of money laundering.

These risk levels only represent the services themselves, and are not enough on their own to assess the risk level of a specific entity. The only way to do that is to analyze that entity's cryptocurrency transactions and counterparties in greater detail.

If you're new to the cryptocurrency ecosystem, this guide will provide you with an understanding of how different groups use cryptocurrency and what you should be on the lookout for to limit risk of exposure to illicit activity.

The complete guide to cryptocurrency service and organization categories

Everything you need to know about the key players in the cryptocurrency ecosystem - including emerging trends, risk type, and possible exploits.

2

Merchant services

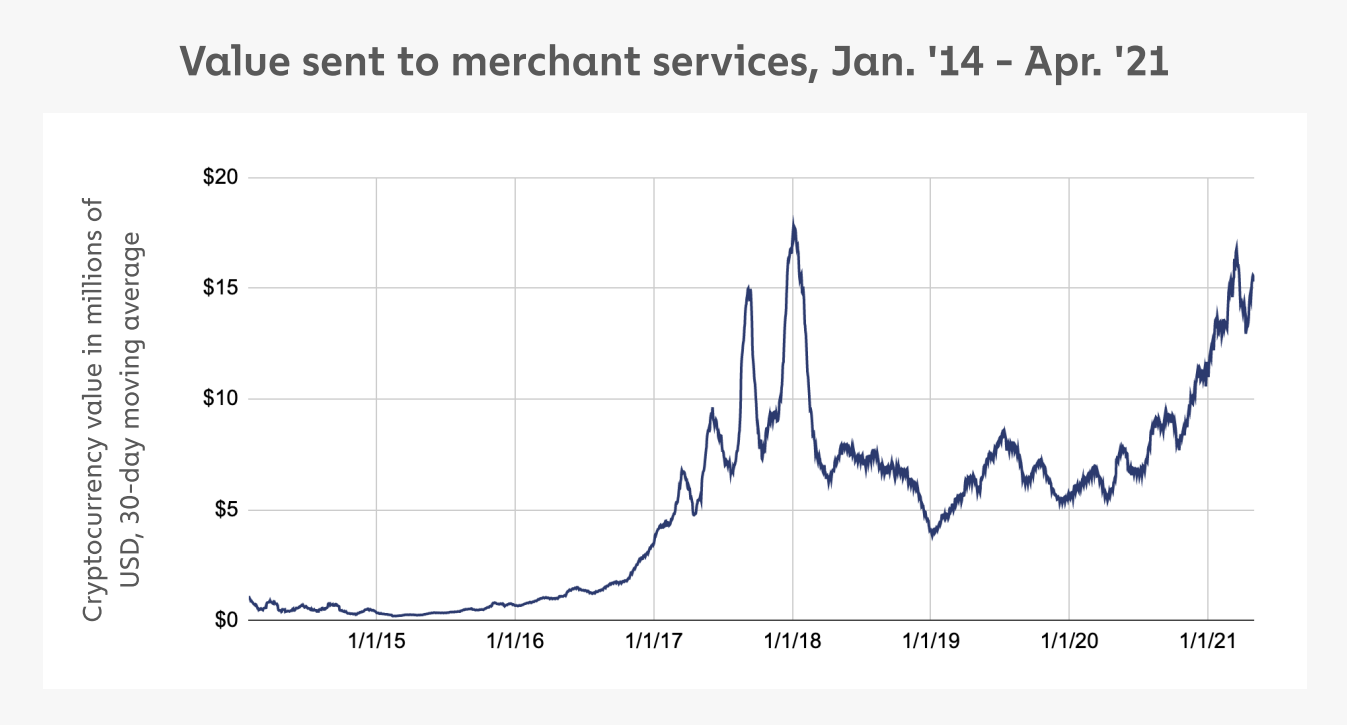
Description	Services acting as an intermediary between a merchant and customer to provide Cryptocurrency payment services.
How it works	Merchant service receives cryptocurrency payment from a customer on behalf of the merchant. A merchant will receive funds via immediate settlement to their bank account, or may choose to settle in cryptocurrency.
Examples	Worldpay, FIServ, Global payments
Risk type	Bitpay, Flexa, Coinpayments, WebMoney, Coinify etc
Possible exploit	Malicious websites can be registered to accept cryptocurrency payments that are processed by merchant services
Emerging trends	Merchant services volume is growing as cryptocurrency increases in popularity and more businesses accept it as payment.

Merchant services providers allow mainstream businesses to accept cryptocurrency as payment for everyday customer purchases, whether they're happening online or in person. Think of them as regular payment processors, like Stripe or Square, except compatible with cryptocurrencies. Merchant services allow people to use cryptocurrency the same way they use fiat currency.

Why would somebody — consumer or business — want to use cryptocurrency over fiat currency? There are lots of reasons, but the biggest is the reduction of fees. Conventional payment methods like credit cards carry a fee for each transaction, which means the business has to either absorb the cost or pass it on to the customers.

Cryptocurrency payments are more direct transactions, which means they can be processed more cheaply than credit card payments. The same goes for cross-border payments and remittances.

As cryptocurrency adoption grows, merchant services adoption is also growing, with global companies like Starbucks and Whole Foods now accepting cryptocurrency payments. In aggregate, merchant services usage has trended upwards since 2020 after a nearly two-year lull, with some dramatic spikes and declines during and after the Bitcoin price boom in 2017.



Currencies: BCH, BTC, LTC, USDT

The merchant services category is generally a low-risk category. Users are typically traditional businesses and their customers. However, it's worth noting that scammers sometimes integrate merchant services with malicious websites to accept cryptocurrency payments from their victims.

Hosted wallets

Description	Alternative to individually controlled wallets. Easier to use, and potentially more secure. Risky if you don't choose a good one.
How it works	App or web based. No storage issues, sync lag or complex operations
Examples	Xapo.com, Freewallet.org
Risk type	Usually low
Possible exploit	Scam wallet services can steal a user's private keys
Emerging trends	Increasing adoption due to ease of use and app convenience

To understand hosted wallets, you need to understand how public and private keys enable cryptocurrency transactions. Wallets manage and store users' public and private keys. In simple terms, your public key is a digital, public-facing 'identity' that represents where cryptocurrency can be received to and sent from. Your private key provides the mechanism to prove you own that public identity, but you can do so whilst keeping your private key secret. It allows you to sign off cryptocurrency transactions, sending your funds somewhere else. If someone else knows your private key, they functionally can unlock all the funds associated with it.

Unhosted wallets (also known as non-custodial wallets or self-hosted wallets) allow a user to store their public and private keys locally to their own device, giving them full control over their funds at all times.

But with that control comes responsibility. Unhosted wallet users are responsible for maintaining the security of their private keys against hackers or any other parties who would try to steal them and take control of the user's funds.

Hosted wallets (also known as custodial wallets) eliminate the inconvenience of having to secure your own keys by storing your public and private keys in a wallet infrastructure owned and maintained by the wallet service provider. This results in a user experience similar to traditional banking and finance websites, making it easier for users to transact, albeit at the risk of less financial privacy and loss of direct control over funds.

Below are some of the more popular hosted and non-hosted wallets. Keep in mind that some services offer both options.

Popular hosted and non-hosted wallets

	Hosted	Non-hosted	Key Value Proposition
EXODUS		✔	In-wallet exchange service – no KYC
xapo	✔		Offline, secure, encrypted servers
BLOCKCHAIN		✔	In-wallet exchange service
cobo	✔	✔	Can stake holdings for interest
coinomi		✔	125+ blockchains supported

Users should be on the lookout for scammers who set up malicious websites impersonating those of popular hosted wallet services in order to trick users into handing over their private keys and giving up control of their cryptocurrency.

Mining pools

Description	Miners pool their resources (GPU/ASIC mining hardware)
How it works	Mined block divided according to mining power (hash) each contributed
Examples	BTC.com (professionals). NiceHash (anyone with personal computer)
Risk type	Usually low
Possible exploit	Most are one-way but some accept deposits → could enable laundering
Emerging trends	Large corporations or mining pools dominate mining

Mining is the process of validating and adding transactions to the blockchain in exchange for newly generated cryptocurrency. It's the key process for both regulating cryptocurrency issuance and maintaining blockchain security.

The most commonly used mining process is called Proof of Work (PoW) mining. Under a PoW system, miners compete in a computational brute force guessing game. The miner who finds a valid answer first wins the right to create a new ledger entry or block, adding new transactions to the blockchain. As a reward for expending all that computational energy, the miner receives newly generated cryptocurrency.

Exactly how difficult is it to solve the math problems that power the blockchain? Their difficulty is quantified with a measurement unit called **hash rate**, which quantifies the total amount of computing power being thrown at mining for any one cryptocurrency — more computing power means more competition for each new block, making it harder for any one entity to win. The hash rate for Bitcoin has grown exponentially since 2017 [1].

[1] Blockchain.com, https://www.blockchain.com/charts/hash-rate?timespan=all

In the early days of Bitcoin, it was feasible for an individual to successfully mine new Bitcoin using their personal computer. But with increased competition, that's now nearly impossible. Miners have responded by forming mining pools, in which a group of miners combine their collective computing power to increase their chances of success. Competition is fierce — some mining pools have entire server farms dedicated just to mining. BTC.com and NiceHash are two of the biggest, most successful mining pools operating today.

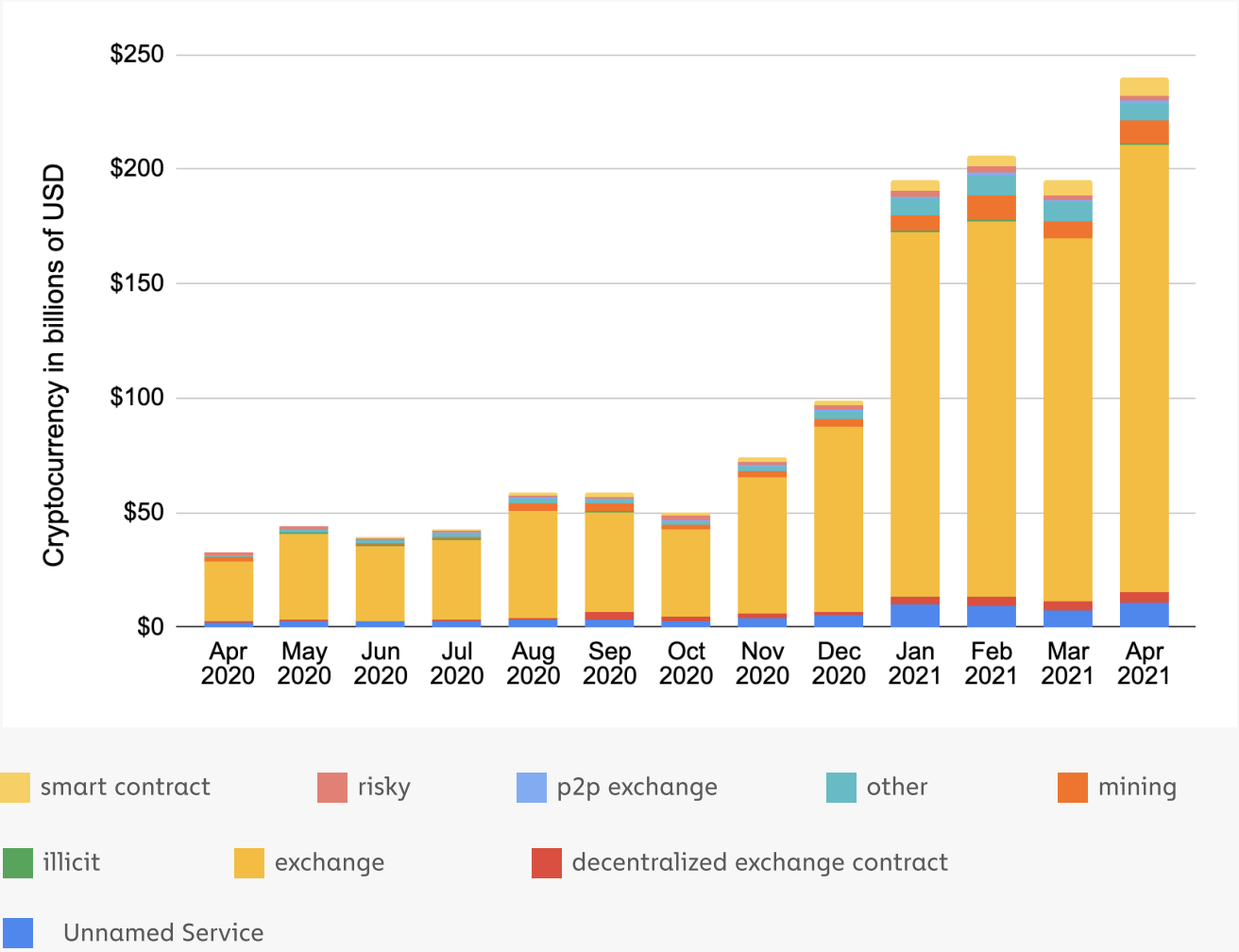
Mining pools are considered a low-risk category since they receive the vast majority of their cryptocurrency through mining, and send it to the groups and individuals participating in the pool. However, some mining pools accept donations or receive cryptocurrency through means other than mining, in which case they could be exploited for money laundering.

Exchanges

Description	Online service for buying, selling, and trading cryptocurrency
How it works	Sign up for an account, some have more KYC than others; some are p2p
Examples	Coinbase, Kraken, Binance, Huobi, LocalBitcoins (also: BTC-e, WEX)
Risk type	It varies
Possible exploit	Heavily targeted by hackers/phishing. Money laundering.
Emerging trends	DEXs, instant exchangers

Exchanges allow users to buy, sell, and trade cryptocurrency. They represent the most important and widely-used service category in the cryptocurrency industry, accounting for 90% of all funds sent by services. Since April 2020, exchanges received over $1 trillion in cryptocurrency value, more than 80% of all cryptocurrency received by services.

Monthly cryptocurrency value received by service category, 2021



Like wallets, exchanges are typically custodial, non-custodial, or give users the option for either.

Custodial	Custodial or non-custodial	Non-custodial
Hosted/retail exchanges	Instant exchangers	DEX (decentralized exchanges)
Derivatives exchanges	P2P exchanges	

Custodial exchanges technically have control of your cryptocurrency since they hold the private keys associated with the wallet. Big, centralized retail exchanges tend to be custodial, as their brand name makes them trustworthy for many users, who are often interested in trading quickly without the friction of entering their private key. In fact, trading on most of these exchanges happens off-chain—meaning, it's not recorded on the blockchain—and is managed by the exchange itself, which is faster for users but reduces transparency. The only times exchange transactions are recorded on the blockchain are when users deposit or withdraw funds to an address outside of the exchange.

Exchanges can also differ in their approach to fiat currency. Crypto-to-fiat (C2F) exchanges such as Coinbase allow users to exchange fiat currency for cryptocurrency, making them the primary on and off-ramps in and out of crypto assets. This also means that C2F exchanges are the most common place for new users to acquire their first cryptocurrency. Crypto-to-crypto (C2C) exchanges, on the other hand, only allow for swapping between different types of cryptocurrency, and are more popular among experienced users and high-frequency traders dealing in a wider variety of assets beyond the most popular coins.

Peer-to-peer (P2P) exchanges

Unlike custodial exchanges, non-custodial exchanges don't take custody of users' funds or hold the private keys associated with their wallets. P2P exchanges are the most common example. Whereas retail exchanges manage all trades centrally in an order book, P2P exchanges facilitate direct trades between individuals. Users create public listings of how much cryptocurrency they'd like to buy or sell, and other users can respond and negotiate terms with them directly. Once the terms are settled, the two parties can coordinate the transfer either in person or online via direct wallet transfers, bank transfers, wires, gift cards — whatever they decide. P2P exchanges are especially popular in regions without a strong traditional banking structure, such as parts of Latin America and Africa.

High-risk exchanges

Some are better at complying with anti-money laundering regulations (AML) than others. While the most reputable exchanges have strict Know Your Customer (KYC) protocols in place and use tools like Chainalysis to monitor transactions for risky or illicit activity,

others are much more lax on compliance, which makes them a greater money laundering risk. At Chainalysis, we designate these as high-risk exchanges, based on their transaction history, stated compliance policies, and resources like the Financial Action Task Force's (FATF) guidance on red flags for cryptocurrency businesses.

BTC-e, which was seized and shut down by the U.S. government in 2017, was a great example of a high-risk exchange.

BTC-e suspected of money laundering, shut down



$4
billion allegedly laundered

300,000
of stolen BTC from Mt. Gox laundered

$110
million civil penalty

Authorities found that BTC-e had high exposure to money laundering schemes associated with ransomware, hacker groups, identity theft, tax fraud, and drug trafficking. Overall, more than $4 billion worth of cryptocurrency was laundered on the exchange, including 300,000 BTC stolen in the Mt. Gox Hack. But as the data illustrates, the biggest exchanges today take AML compliance more seriously and are at a far lower risk of enabling money laundering.

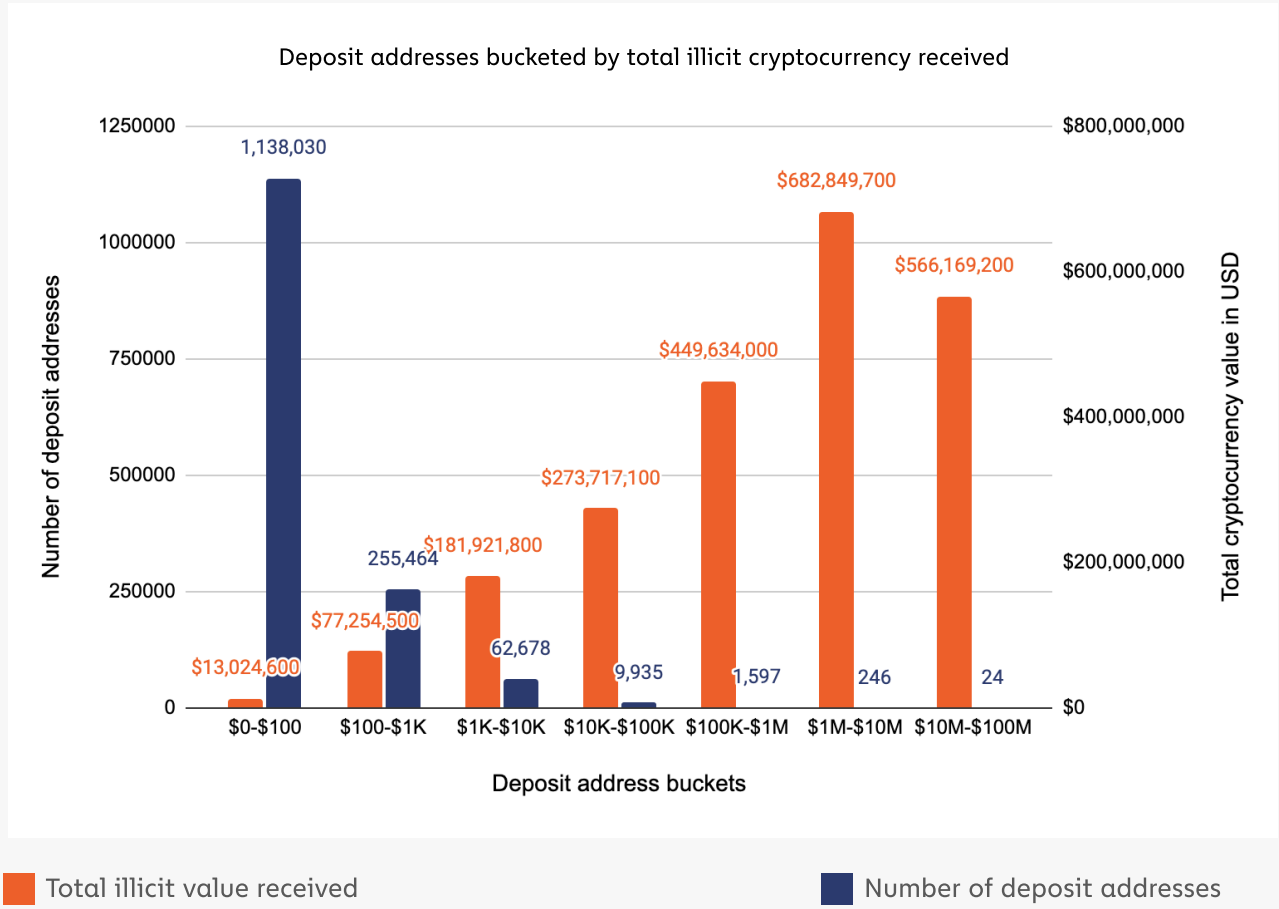
Nested services

Description	Cryptocurrency services that operate using addresses hosted by larger exchanges.
How it works	Nested services hold accounts at larger exchanges and can tap into their trading pairs and liquidity.
Examples	Many OTC brokers and instant exchangers are nested services
Risk type	It varies
Possible exploit	Exchanges sometimes don't hold nested services to high enough compliance standards.
Emerging trends	Nested services are increasingly involved in money laundering and account for a large share of funds received from illicit addresses.

Nested services are cryptocurrency businesses that operate within one or more larger exchanges, tapping into those exchanges' liquidity and trading pairs. Common examples of nested services include instant exchangers and Over the Counter (OTC) brokers, though both of these can operate independently as stand-alone services.

While most nested services operate legally and compliantly, those that don't account for a disproportionate share of money laundering activity.

All illicit cryptocurrency received by service deposit addresses, 2020



Caption: **How to read this graph:** This graph shows service deposit addresses bucketed by how much total illicit cryptocurrency value each address received individually in 2020. Each blue bar represents the number of deposit addresses in the bucket, while each orange bar represents the total illicit cryptocurrency value received by all deposit addresses in the bucket. Using the first bucket as an example, we see that 1,138,030 deposit addresses received between $0 and $100 worth of illicit cryptocurrency, and together all of those deposit addresses received a total of $13 million worth of illicit cryptocurrency.

As we cover in our 2021 Crypto Crime Report, a very small number of service-hosted deposit addresses account for the majority of cryptocurrency money laundering, with just 270 receiving 55% of all funds sent from illicit addresses in 2020. Most of the addresses receiving those illicit funds are associated with nested services.

OTC Brokers

Description	Super traders who directly facilitate deals between counterparties outside the open exchange
How it works	OTC brokers often work with customers through Skype and Telegram. Some are connected to an exchange, but not all.
Examples	Cumberland, Octagon Strategy Limited, Athena Bitcoin
Risk type	Low – Medium, depending on KYC
Possible exploit	OTC brokers are often held to lax KYC standards, enabling some to facilitate money laundering
Emerging trends	OTC brokers may account for higher trade volumes than open exchanges

Over the counter (OTC) brokers facilitate large trades between individual buyers and sellers who can't or don't want to transact on an open exchange. Many OTC brokers operate as nested services within one or more exchanges, but the largest tend to operate independently.

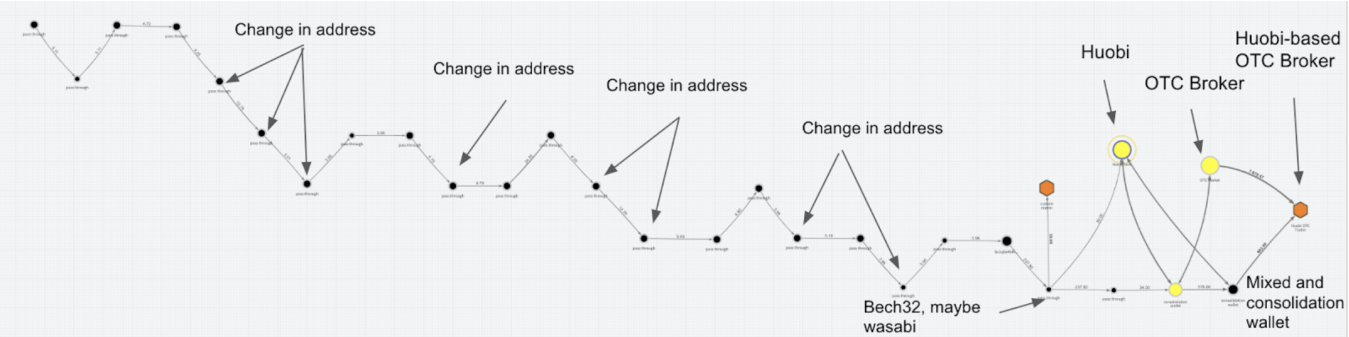
Traders can work with OTC brokers if they want to liquidate a large amount of cryptocurrency for a set, negotiated price. OTC brokers are a crucial source of liquidity in the cryptocurrency market. While it's impossible to measure the exact size of the OTC market, we know that it's quite large. Cryptocurrency data provider Kaiko even estimates that OTCs could facilitate the majority of all cryptocurrency trade volume. [2]

While most OTC brokers run a legitimate business, some work with criminal entities. OTC brokers are often held to lower KYC requirements than the exchanges on which they operate. Some take advantage of this to provide money laundering services to criminals, helping them cash out funds connected to illegal activity. An unscrupulous OTC broker would typically do this by exchanging criminals' ill-gotten cryptocurrency for cash directly or for Tether as a stable intermediary currency.

We saw examples of OTCs acting as money launderers during our investigation of PlusToken, a massive Ponzi scheme that took in billions of dollars' worth of cryptocurrency

[2] Kaiko, https://blog.kaiko.com/what-is-otc-cryptocurrency-trading-^{66}d^{725}c^{867}f

from millions of investors.[3] As of December 2019, the PlusToken scammers moved roughly $185 million worth of stolen Bitcoin to exchange accounts associated with OTC brokers to be liquidated. Most of these cashouts resemble the pattern of transactions shown below, in which hackers moved a chunk of stolen funds through a series of intermediary wallets before funnelling the majority to OTC brokers.



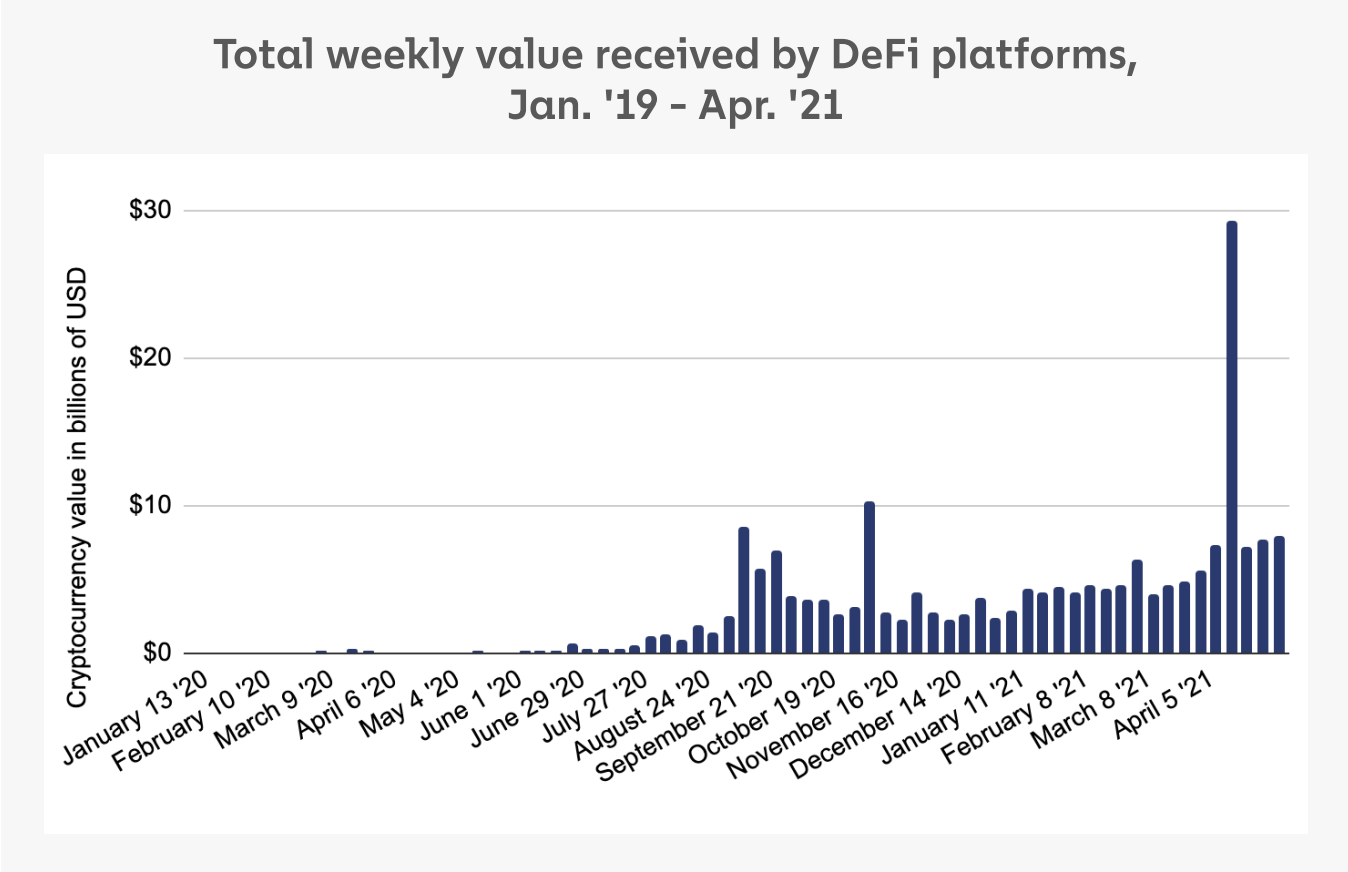
Additionally, we've found that many accounts at compliant exchanges receiving significant funds from illicit sources are controlled by OTC brokers, many of whom have played a role in multiple criminal investigations we've participated in. However, the majority of OTC brokers who operate compliantly remain an integral part of the cryptocurrency ecosystem.

DeFi

Description	DeFi stands for "decentralized finance," and refers to a class of cryptocurrency platforms that can run autonomously without the support of a central company, group, or person.
How it works	DeFi platforms are built on top of smart contract-enriched blockchains — primarily the Ethereum network — and can fulfill specific financial functions determined by the smart contracts' underlying code,
Examples	Uniswap, Sushiswap, Curve.fi
Risk type	Medium
Possible exploit	Vulnerabilities in smart contract code, potential for money laundering
Emerging trends	Flash loans, non-fungible tokens (NFTs), yield farming

[3] Chainalysis, https://blog.chainalysis.com/reports/plustoken-scam-bitcoin-price

DeFi's growth was one of cryptocurrency's biggest stories in 2020.



The weekly total value received by DeFi protocols has trended upwards since the beginning of 2020 with several spikes in between, peaking at over $29 billion during the week of April 19, 2021.

But what is DeFi? DeFi stands for "decentralized finance," and refers to a class of cryptocurrency platforms that can, at least in theory, run autonomously without the support of a central company, group or person (hence the name). How is this possible? DeFi platforms are built on top of smart contract-enriched blockchains — primarily the Ethereum network — and can fulfill specific financial functions determined by the smart contracts' underlying code, executing transactions like trades and loans automatically when certain conditions are met. Without the need for centralized infrastructure or human governance, DeFi platforms can enable users to execute financial transactions at lower fees than other fintech applications or financial institutions. Overall, DeFi platforms received $86.5 billion worth of cryptocurrency in 2020, which represents a 67x increase over the 2019 total.

Below, we'll profile three popular DeFi technology categories.

ERC-20 tokens

ERC-20 tokens are blockchain-based assets that can be sent and received using an Ethereum wallet. Many ERC-20 tokens are built to match the price of other popular crypto assets — Ethereum Bitcoin (ETH BTC), for instance, is an ERC-20 version of Bitcoin, meaning it can be swapped more easily on DeFi platforms.

How do ERC-20 tokens work exactly? One of the things that differentiates Ethereum from Bitcoin is that it can run programs like smart contracts. These smart contracts allow decentralized applications to be built on top of the Ethereum blockchain, rather than requiring their own blockchain. ERC-20 describes a standard for writing smart contracts that function as tokens. It provides a programmatic interface for basic functionality those tokens to be transferred and stored in Ethereum wallets. Because they run on the Ethereum blockchain, all transaction fees for ERC-20 tokens are paid in Ethereum. As of today, Chainalysis supports 97 ERC-20 tokens, which together account for 97% of the total value in ERC-20s and over $25 billion of ERC-20 transfers every day.

Decentralized exchanges (DEXes)

DEXes are one of the most popular types of DeFi platforms. DEXes allow users to buy, sell, and swap different tokens built on a specific blockchain (again, primarily Ethereum) directly between one another's wallets for greater privacy and security. Since these platforms never actually take custody of the funds, instead facilitating direct transfers, users can complete these currency swaps without having to provide KYC (know-your-customer) information or the trades being recorded in an order book as they would be on a standard cryptocurrency exchange.

DeFi Lending platforms

Lending platforms are another popular type of DeFi platform. DeFi lending platforms allow cryptocurrency holders to pool their assets so they can be loaned out to others. In return for supplying that liquidity, the holders receive a portion of the interest generated from the loans other users take out. Like other DeFi platforms, DeFi loan pools are governed by underlying smart contracts, which set the interest rates and collateral required from users taking out the loans.

Cryptocurrency ATMs

Description	Convert cash into cryptocurrency and vice versa, similar to fiat ATMs
How it works	ATM located in public spaces (malls, liquor stores, gas stations, etc)
Examples	CoinCloud, BitNational, CoinSource, and Coinstar
Risk type	Low – Medium, depending on KYC
Possible exploit	Bad actors with lots of cash are tempted to convert to cryptocurrency
Emerging trends	Growing. Variety of cryptocurrencies increasing (BTC, BCH, ETH, LTC+)

Cryptocurrency ATMs, also known as cryptocurrency kiosks, are physical machines that allow users to convert cash to cryptocurrency or vice versa. As cryptocurrency adoption grows, we're seeing huge increases in the number of ATMs installed.[4] It's important to note that while these machines are named after the ubiquitous cash ATMs we're all used to, they're regulated differently because of one key distinction: Whereas cash ATMs simply allow users to withdraw cash they already own from a bank account, cryptocurrency ATMs allow them to convert between fiat and cryptocurrency, and as such are generally regulated as virtual asset service providers (VASPs) under regulations such as the Travel Rule.

As a quick and easy means of converting between cash and cryptocurrency, the main concern with cryptocurrency ATMs is that they can attract criminals looking to launder funds. But many cryptocurrency ATMs have strong KYC protocols in place, which typically get stricter the more money a user is trying to deposit. Users are required to create an account with personally identifying information such as a phone number or ID photo, which makes the category relatively low-risk.

The case of United States v. Kevin C. Fusco provides a good example of what cryptocurrency ATM KYC looks like in practice. It began when Fusco, a drug dealer active on various darknet markets, went to a cryptocurrency ATM and converted $32,000 worth of Bitcoin into cash. The ATM flagged the transaction as risky, and when Fusco returned to try

[4] Coin ATM Radar, https://coinatmradar.com/charts/growth/

and convert another $200,000 worth of Bitcoin, the machine rejected the request. Since the ATM provider collected Fusco's driver's license information during signup as part of the KYC process, law enforcement agents were able to connect these transactions to Fusco and use ATM records to bolster their case when they eventually arrested him.

Gambling

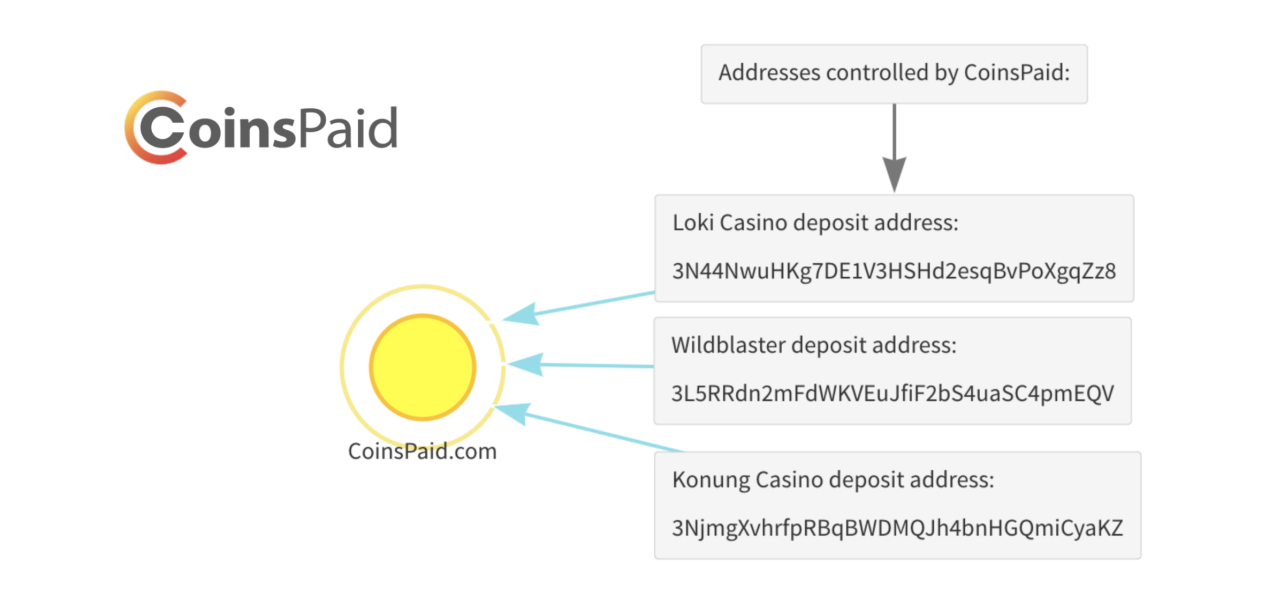
Description	Online gambling sites for slots, sports/eSports betting – increasingly accepting cryptocurrency
How it works	Individuals open account, send cryptocurrency and wager their funds. KYC is not very prevalent. Treated differently by jurisdiction.
Examples	mBitCasino, Oshi Casino, Konung Casino, BitStarz, etc
Risk type	Medium – depends on jurisdiction
Possible exploit	Can be used for money laundering
Emerging trends	Lots of gambling sites are actually owned by a few holding companies

The online gambling world was an early adopter of cryptocurrency, possibly because it allows users to gamble in jurisdictions where doing so isn't allowed.

The risk profile of gambling services depends largely on jurisdiction. Gambling sites are considered risky in the U.S., since most states don't allow gambling. But in Europe, online gambling is perfectly legal, so these services are considered low risk. However, some gambling sites have lax KYC standards, which can make them another destination for money laundering. As with the other categories, it's important to dig deep on the practices of individual services when assessing risk.

Interestingly, many gambling sites rely on the same handful of payment processors to carry out cryptocurrency transactions. While it may appear that the customer payments across distinct addresses are all being deposited to each individual casino, the addresses are all actually managed by a single, third party payment processor, which we refer to as a nested service under this arrangement. Below is one such example with popular payment processor CoinsPaid.

Funds often handled by payment gateways



This is just one example of concentration in online gambling. Many gambling websites use white label online casino software platforms that let them offer popular games without having to program the games themselves. In fact, while there may appear to be thousands of individual gambling websites operating, many of them are owned by the same holding companies.

Cyber infrastructure as a service

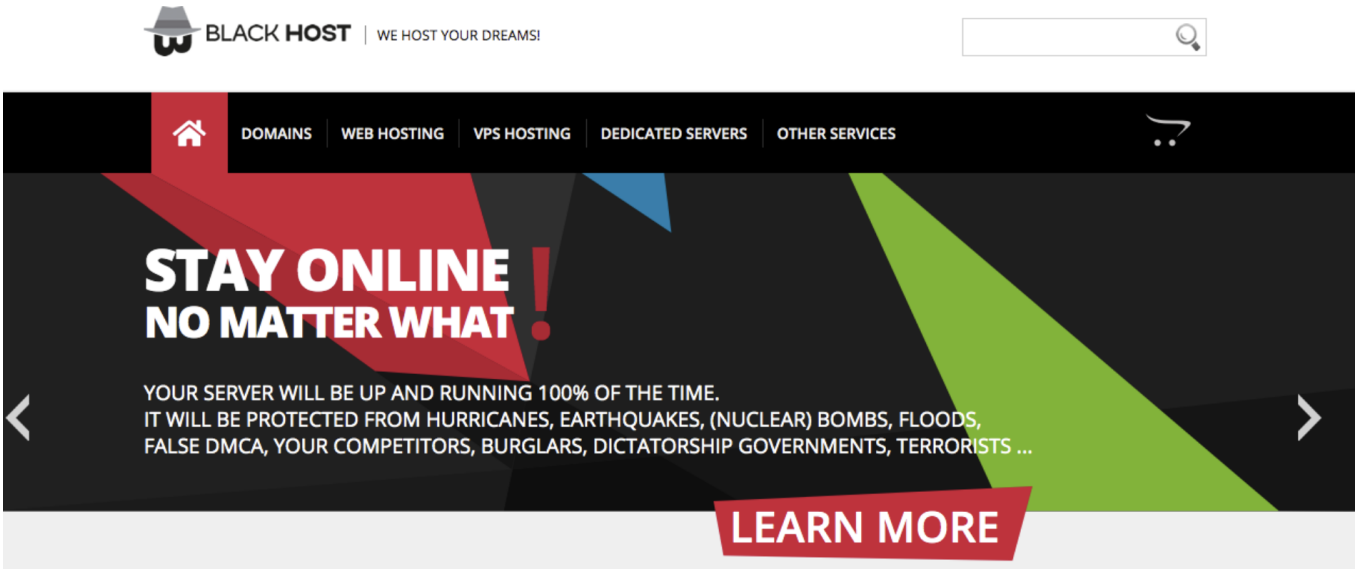
Description	Infrastructure for computing and information services, including VPN providers, VPS hosting providers, Domain Registrars, and other popular types of cyber infrastructure.
How it works	Users sign-up for the service and may pay their subscription in cryptocurrency. Many services use a 3rd party to process payments. Others accept cryptocurrency on their own or use a non-custodial payment processor.
Examples	Yalishanda, Volhav
Risk type	Medium
Possible exploit	While these services are not inherently illicit, they could be misused by criminals to carry out hacks, ransomware, and other attacks
Emerging trends	Infrastructure as a Service providers are frequently implicated in ransomware cases.

Cyber infrastructure refers to the services necessary to run a website or other internet-based business. These include:

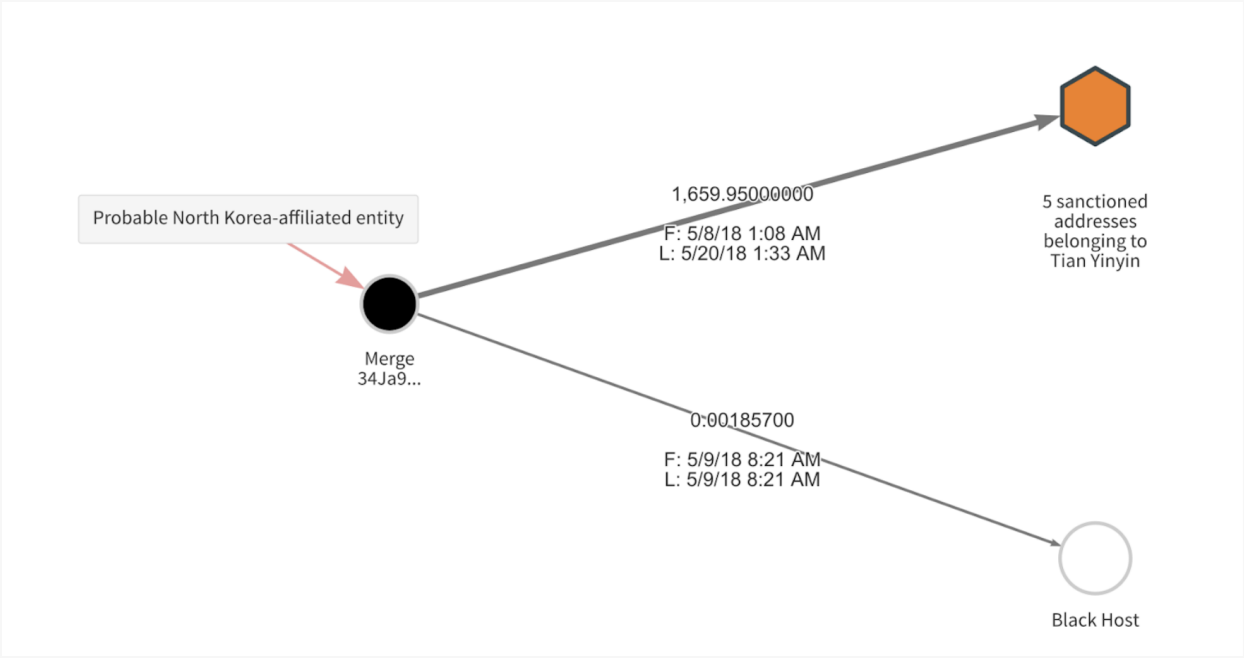
- Web hosting
- Domain registration
- Email and other communication services
- Virtual Private Networks (VPNs)
- Postage services for ecommerce

Many cyber infrastructure providers take payment in cryptocurrency. Though they typically do this through merchant services providers, we can often identify the merchant services addresses that specific cyber infrastructure providers use. In those cases, we tag those addresses with the name of the relevant cyber infrastructure provider.

We rate cyber infrastructure providers as medium risk cryptocurrency services because they often provide anonymity features that make them popular with cybercriminals. One example is web hosting service BlackHost.



BlackHost is what's known as a bulletproof hosting service, meaning that it allows customers to pay for its services anonymously and is generally lenient on the types of content they're allowed to host. Blockchain analysis shows that BlackHost's primary Bitcoin address received funds from another address that had sent substantial Bitcoin to addresses controlled by Tian Yinyin, a Chinese national sanctioned by the United States for helping North Korean cybercrime syndicate Lazarus Group convert stolen cryptocurrency into cash.



The evidence suggests that BlackHost likely received funds from Lazarus Group, and may have inadvertently provided them with web hosting services necessary to their hacking activities. This is just one example of the risks that cyber infrastructure providers can represent within the cryptocurrency ecosystem.

Mixers

Description	Websites or software for obfuscating the source of funds
How it works	No KYC required. Exist on clearnet and darknet. Typically centrally controlled.
Examples	Chipmixer.com, CryptoMixer.io, Bitcoin Fog
Risk type	High
Possible exploit	Mostly for cryptocurrency that's been stolen or from darknet markets
Emerging trends	LE shutdowns → voluntary shut downs. Also, decentralized mixing protocols (e.g. CoinJoin, CashShuffle).

Mixers are services that help users transact with greater privacy and obfuscate the source of funds. That capability, plus the fact that most mixers don't have KYC requirements, makes them a common money laundering mechanism. In fact, we've found that mixers are the most popular cashout destination for funds from illicit activity.

Mixers create a disconnect between the cryptocurrency funds that users deposit and what they withdraw, making it more difficult to trace the flow of funds. They do this by pooling together funds that all users deposit and mixing them together at random. Users can then receive funds back from the now-jumbled pool equivalent to what they put in, minus a 1-3% service fee. Some mixers make funds even more difficult to track by letting users receive different-sized chunks of funds at different addresses at staggered times. Others try to obfuscate the fact that a mixer is even being used by changing the fee on each transaction or varying the type of deposit address used.

While mixers aren't outright illegal, law enforcement agencies have been treating them with more scrutiny and shutting down ones that have received substantial amounts of ill-gotten funds. For instance, in 2018, Dutch authorities shut down Bestmixer.io, a mixing service that had processed over $200 million worth of funds in the preceding year.[5] Law enforcement determined that a substantial portion of those funds came from criminal activity.

Wasabi Wallet relies on a decentralized mixing method called the CoinJoin protocol, which differentiates it from other mixers. The first generation of mixers were vulnerable to law enforcement intervention because they functioned as centrally-managed services, fully under the mixer's control. The CoinJoin protocol addresses this by providing a wallet service that automatically mixes the funds of all users of that wallet on every transaction they conduct. CoinShuffle is another protocol that does the same thing for Bitcoin Cash.

There are legitimate use cases for more private transactions. But given their built-in conduciveness to money laundering and the previous shutdowns of large, well-established mixing services, financial institutions and cryptocurrency businesses could be expected to scrutinize their exposure to mixers more thoroughly than they would other services.

[5] The Next Web, https://thenextweb.com/hardfork/2019/05/23/cryptocurrency-laundering-bestmixer-close

Services in high-risk jurisdictions

Description	Services based in heavily sanctioned countries.
How it works	Chainalysis highlights services based in heavily sanctioned countries, as doing business with them comes with stringent guidelines and heavy risk.
Examples	Bitpay, Flexa, Coinpayments, WebMoney, Coinify etc
Risk type	Medium-High
Possible exploit	Malicious websites can be registered to accept cryptocurrency payments that are processed by merchant services
Emerging trends	As cryptocurrency grows more popular, more services are cropping up in heavily sanctioned jurisdictions.

Chainalysis products have a high-risk jurisdiction category for services based in countries that are heavily sanctioned by the United States. While these organizations are not sanctioned themselves, they warrant increased caution for cryptocurrency compliance teams, as there are stringent guidelines for interacting with businesses in heavily sanctioned countries. Currently, Iran and Venezuela are the only countries included in this category, though more could be added in the future.

Darknet Markets

Description	Black markets for drugs, stolen card data, weapons, child abuse material, etc
How it works	Commercial website or marketplaces in the dark web (via Tor or I2P)
Examples	Empire, Point, Berlusconi, Silk Road 3.1, (Silk Road, AlphaBay, Dream)
Risk type	Medium – High (depending on amount)
Possible exploit	Users at risk of “exit” scams without recourse
Emerging trends	Innovated security measures to protect against exit scams

Darknet markets are commercial websites that function similarly to eBay, where users can come together to buy and sell goods using cryptocurrency. The key difference of course is that most of the goods available are illegal, including drugs, paraphernalia, weapons, stolen credit card data, child sexual abuse material, and more. Darknet markets are typically only accessible using browsing anonymization services like Tor and I2P. Darknet markets are one of our riskiest categories, and any address or service with significant exposure to darknet markets would likely be treated with suspicion by regulators.

Given their obvious need for secrecy, it's hard to come by individual darknet markets' financials — they're not exactly releasing annual reports. But the cryptocurrency world got a glimpse of some internal data during what now appears to be an exit scam carried out by the operators of Nightmare Market in 2019. A hacker allegedly gained backdoor access to Nightmare Market and released a trove of data on its operations, including figures on sales and revenue.



Source: DarknetLive.[6]

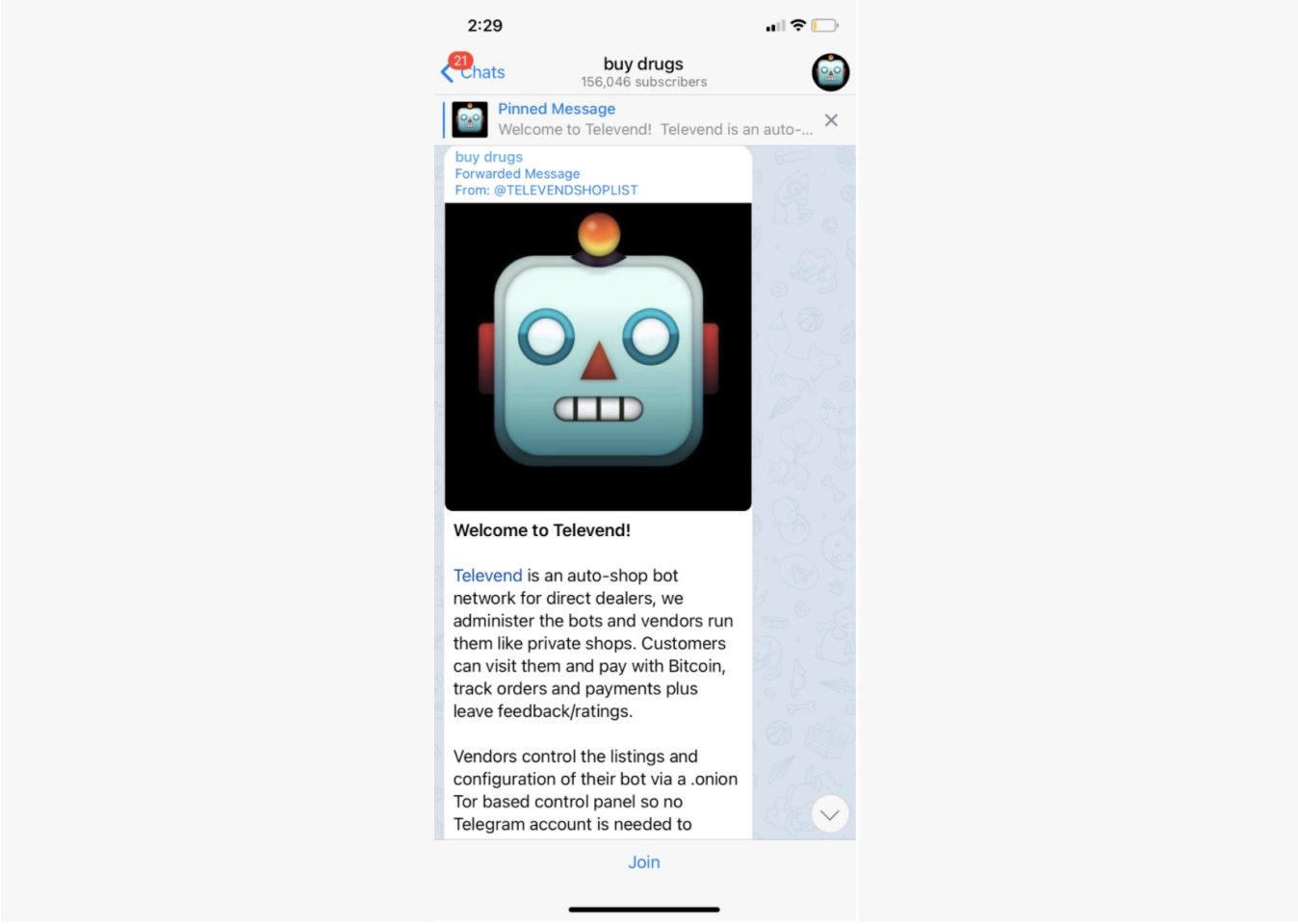
The hacker revealed key insights into Nightmare Market's operation, including:

- Approximately 80,000 users
- $22 million USD worth of revenue from late 2018 to July 2019 (when the alleged hack occurred)
- Vendor preference for Bitcoin and Monero

[6] DarknetLive, https://darknetlive.com/posts/nightmare-market-market-hacker-wreaks-havoc-on-the-darkweb/

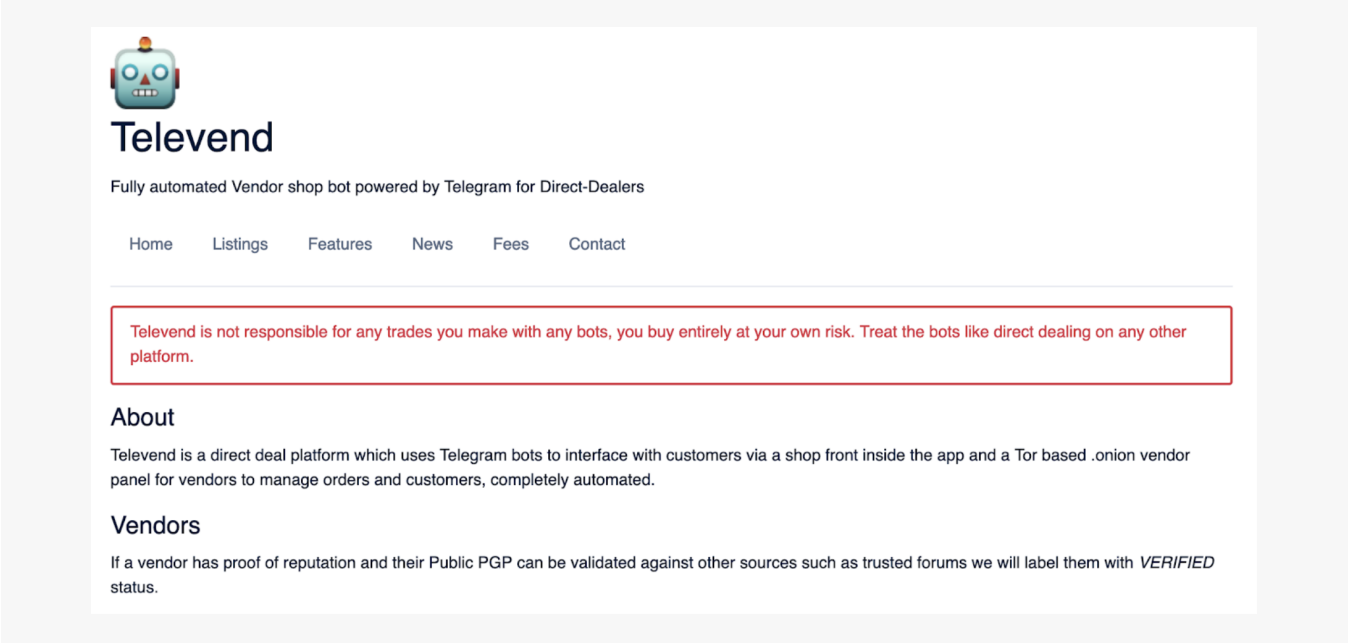
Many buyers and vendors abandoned Nightmare Market soon after this hack (which was also accompanied by difficulties cashing out), moving to alternative darknet markets like Empire Market, Berlusconi Market, Cryptonia Market, and Samsara Market.

In 2020, we saw more and more darknet markets adopt new, decentralized business models that make them more difficult to take down. One example is Televend. Televend is a Telegram-based platform with over 150,000 users where darknet market vendors can sell drugs through automated chatbots, whose communications with buyers are highly encrypted.

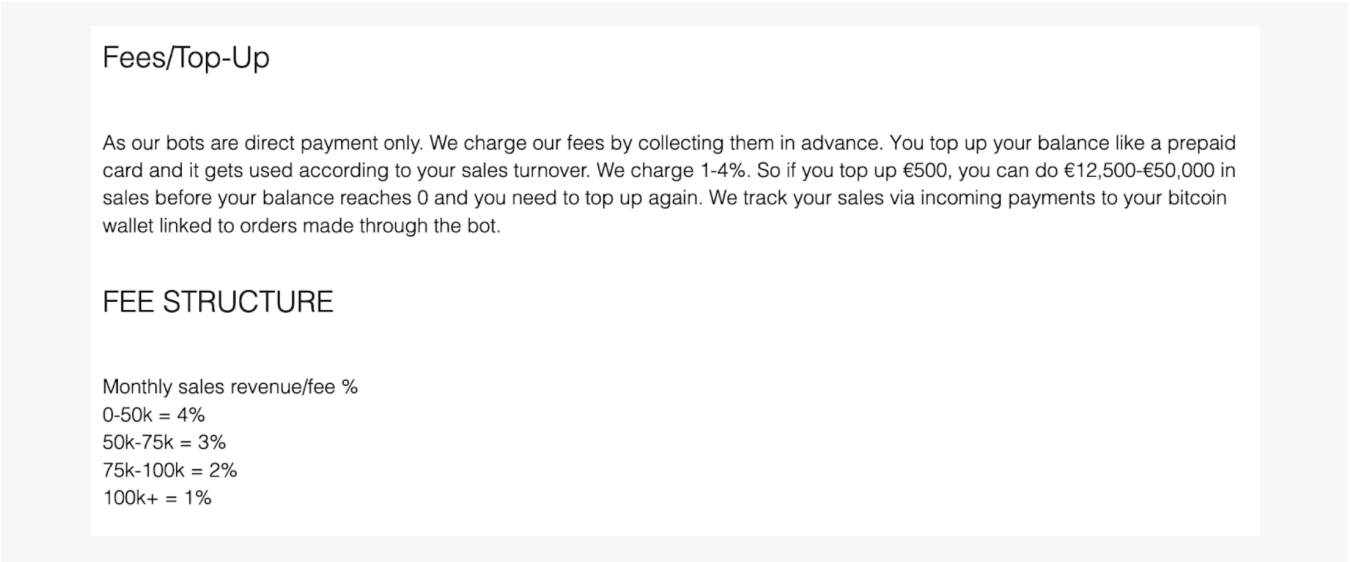


A screenshot of Televend

Buyers simply access Televend's Telegram group, where they find a directory of drug vendors broken down by region and products on offer. From there, they simply place orders with their chosen vendor's chatbot, receive an automatically-generated Bitcoin address to which they send payment, and wait for their drugs to arrive in the mail.



A screenshot from Televend's darknet site



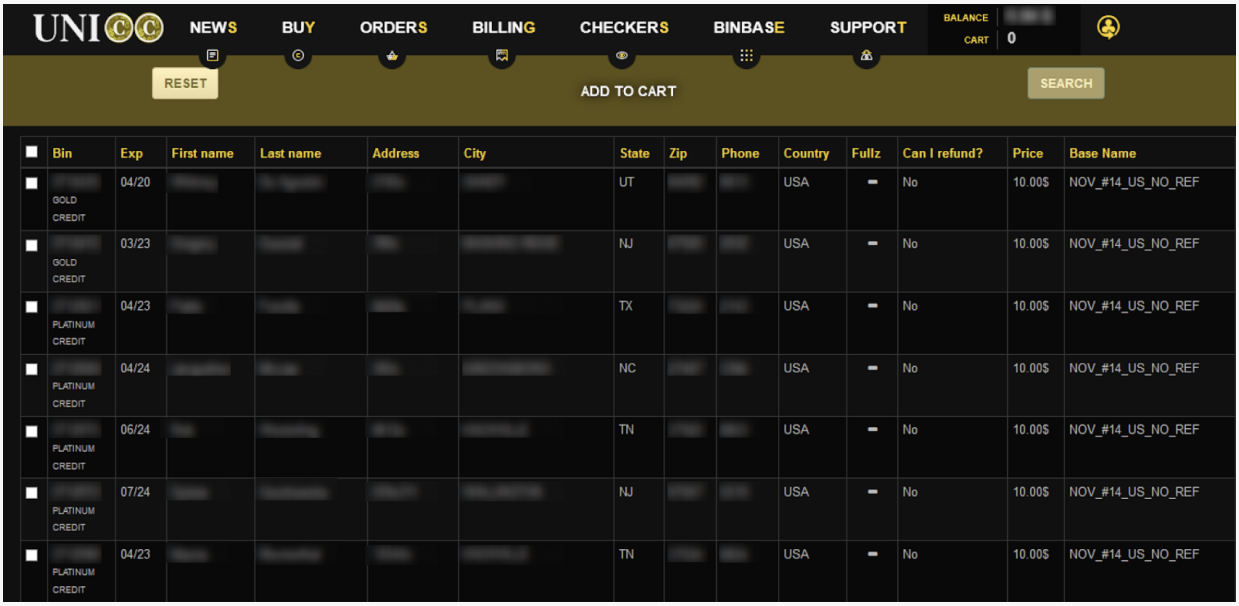
Televend's fee structure explained

Televend receives commissions on each sale, but never actually touches the funds, so there's no central entity for law enforcement to track through blockchain analysis — the transactions blend in much more easily.

We expect platforms like Televend to grow and take in a larger share of total darknet market revenue in 2021, as their decentralized nature makes them more resilient to attacks from both law enforcement and rival markets. While future decentralized markets may run on platforms other than Telegram, Televend shows that the encrypted messaging platform can offer customers an easy buying experience.

Fraud shops

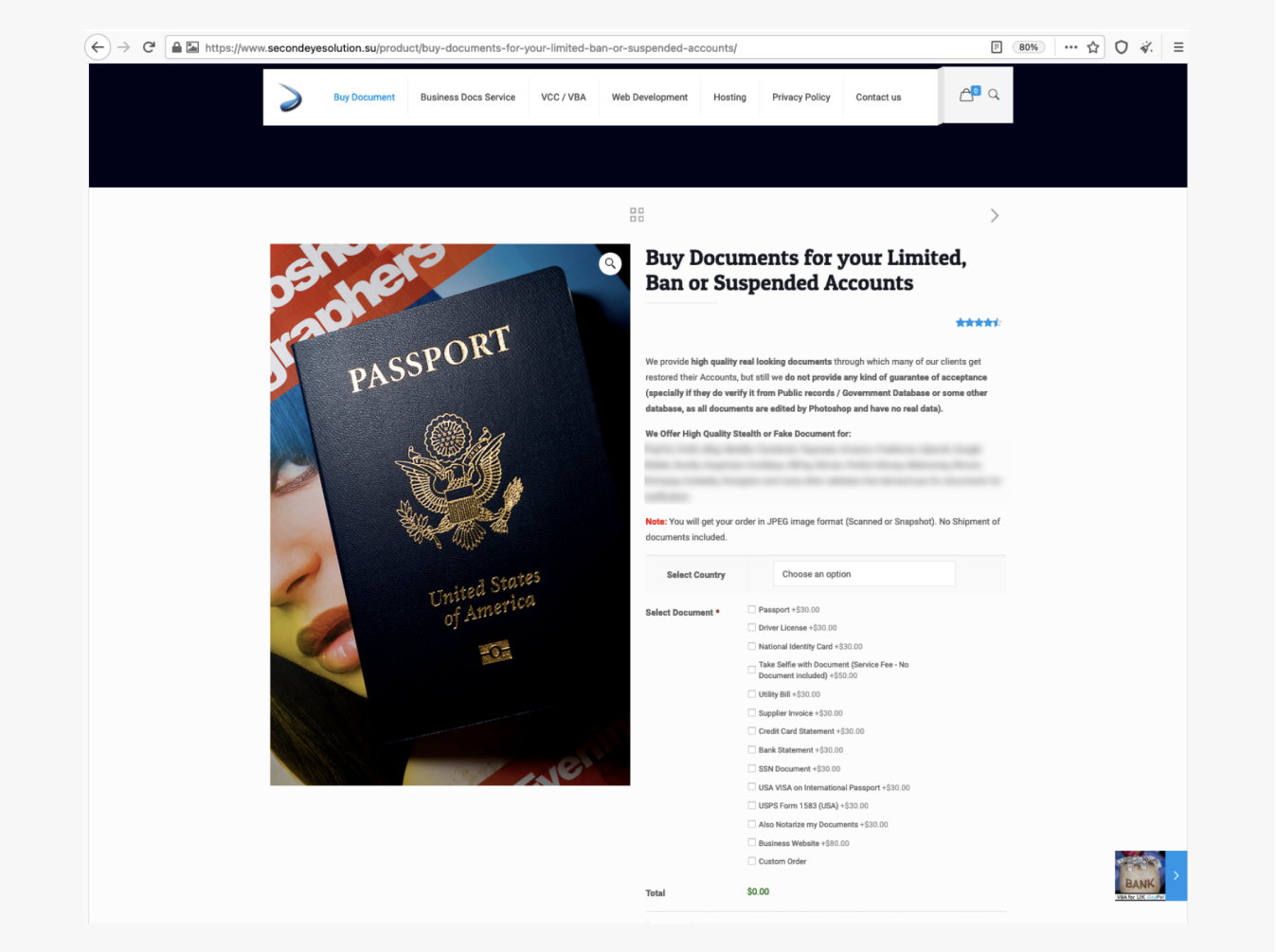
Fraud shops are a particularly common type of darknet market that specialize in stolen credit card information and other data that can be used for fraud, including personally identifying information (PII), SOCKS5, stolen accounts for different services, and hacking exploits rather than drugs. This information typically comes from large-scale data breaches, such as those suffered in recent years by companies like Capital One and Home Depot. Below, we see a screenshot of a particularly popular cardshop called UNICC.



This page shows some of UNICC's stolen credit card listings. Cards go for anywhere from $2 to $15, with the average sitting at about $10. The exact price depends on a few different factors. One is the area of origin. U.S. and western Europe-based cards typically fetch a premium. Another influence on price is the amount of the cardholder's personally identifiable information (PII) that comes with the card, such as street address and phone number. Most reputable online stores ask for this information at the point of sale, so having it increases a buyer's chances of making a successful purchase, hence the higher price.

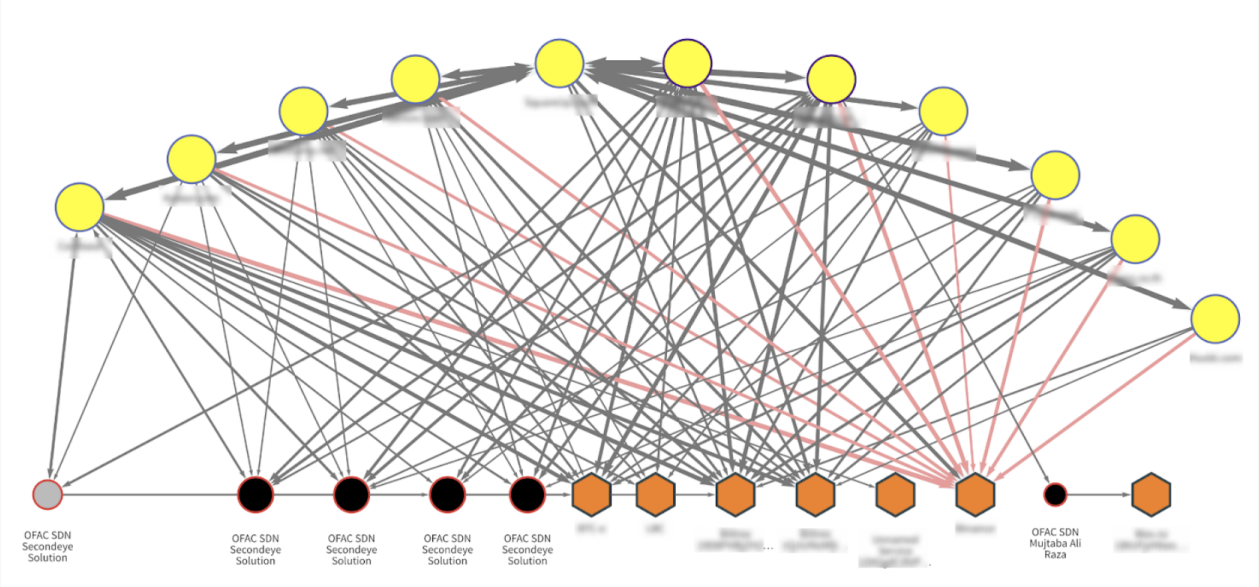
In April 2021, a Pakistan-based fraud shop called Secondeye Solution (SES) and its administrator, Mujtaba Ali Raza, were sanctioned by the U.S. government. Raza, the organization itself, and several associated cryptocurrency addresses were added to the OFAC Specially Designated Nationals (SDN) list as part of this enforcement action.

SES was a unique fraud shop in two ways. First, rather than selling stolen information, it specialized in selling fake identification documents customers could use to craft a synthetic identity, based on a mix of real and fake information, in order to sign up for accounts at cryptocurrency exchanges, payment providers, banks, and social media platforms. SES documents came in digital formats only rather than physical, and were apparently intended for the sole purpose of fooling the remote photo or video-based KYC checks conducted by many exchanges and fintech platforms as part of onboarding. Second, SES was also unique in that it operated on the clearnet rather than the darknet, meaning its website was accessible from conventional internet browsers.



This screenshot of SES' website shows the variety of fake identity documents on offer

Using Chainalysis Reactor to analyze the cryptocurrency addresses cited in OFAC's designation and those we have identified, we see that Secondeye received over $2.5 million worth of cryptocurrency across 31,000 transactions since becoming active in 2013. That works out to roughly $80 per transaction, which fits the pricing listed on its website.



This screenshot of SES' website shows the variety of fake identity documents on offer

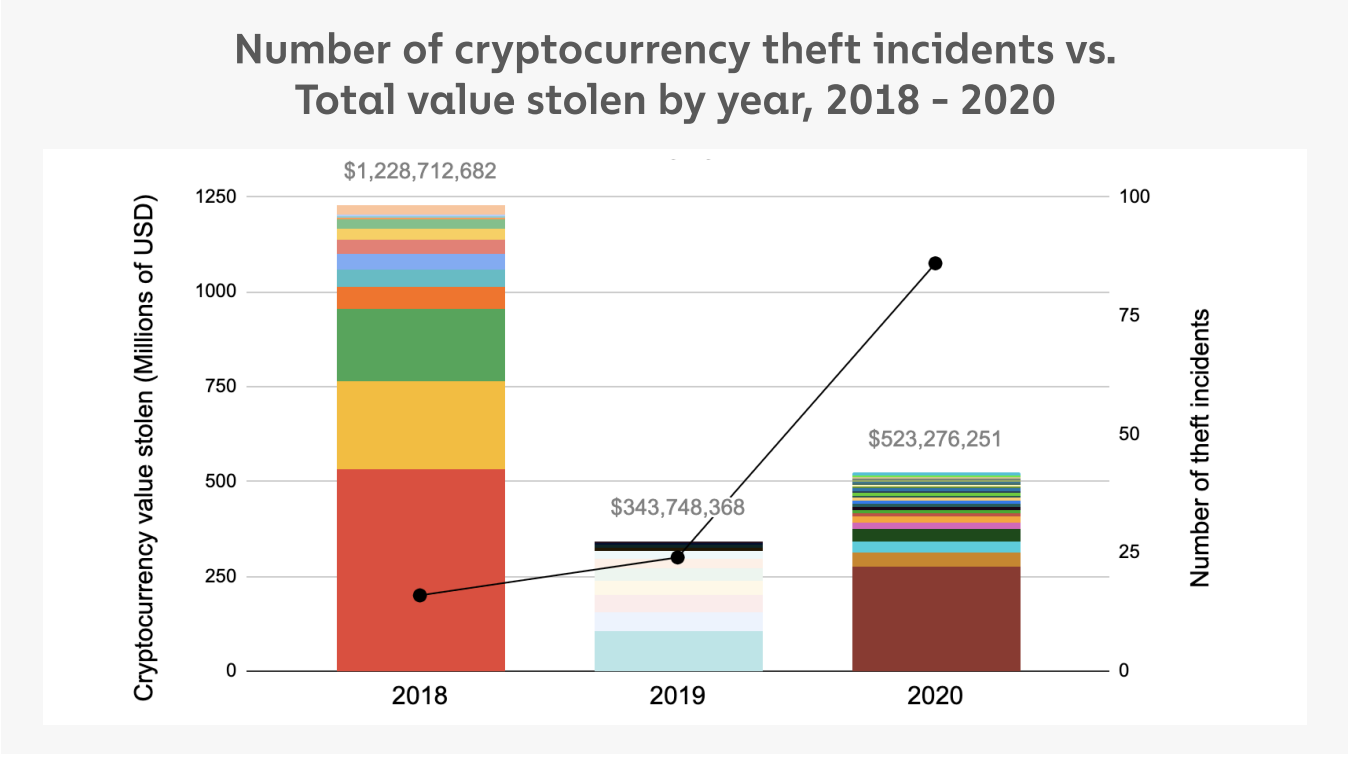
The Reactor graph above shows the incoming transactions for Bitcoin addresses associated with Secondeye and its administrator, Raza, which are positioned in a row at the bottom of the image. Some of the addresses Secondeye used to accept payment were unhosted wallets, while others were hosted at large cryptocurrency exchanges. At the top, we see that most of Secondeye's customers sent cryptocurrency from their addresses at other large exchanges. Secondeye has one active Bitcoin address as of April 14, 2021, hosted at a large exchange that has received over $1.3 million worth of Bitcoin across more than 13,000 transactions. The red lines on the graph show direct transactions from other exchanges to the active address. Secondeye addresses have also received significant funds from darknet markets, mixers, and several high-risk exchanges.

SES was ultimately sanctioned because it was discovered to have done business with a previously sanctioned organization, the Internet Research Agency (IRA). The IRA is a Russia-based "troll farm" that uses digital and social media manipulation to push public opinion on behalf of the Russian government, and is known for having interfered in the 2016 U.S. election. Investigators found that SES provided IRA operatives with fake identity documents that they used to set up online accounts under synthetic identities.

Stolen funds

Description	Billions of dollars in cryptocurrency have been stolen in exchange hacks
How it works	Vulnerabilities exploited to move exchange funds to attacker's control
Examples	Bitpoint, Binance, DragonEx, Cryptopia
Risk type	High
Possible exploit	Big payoff per hack, often resulting in tens of millions in losses
Emerging trends	Sophisticated, persistent social engineering to deliver remote access malware

Theft is one of the biggest issues in cryptocurrency, with over $500 million worth stolen in 2020 and billions stolen overall.



Different colors denote different instances of cryptocurrency theft.

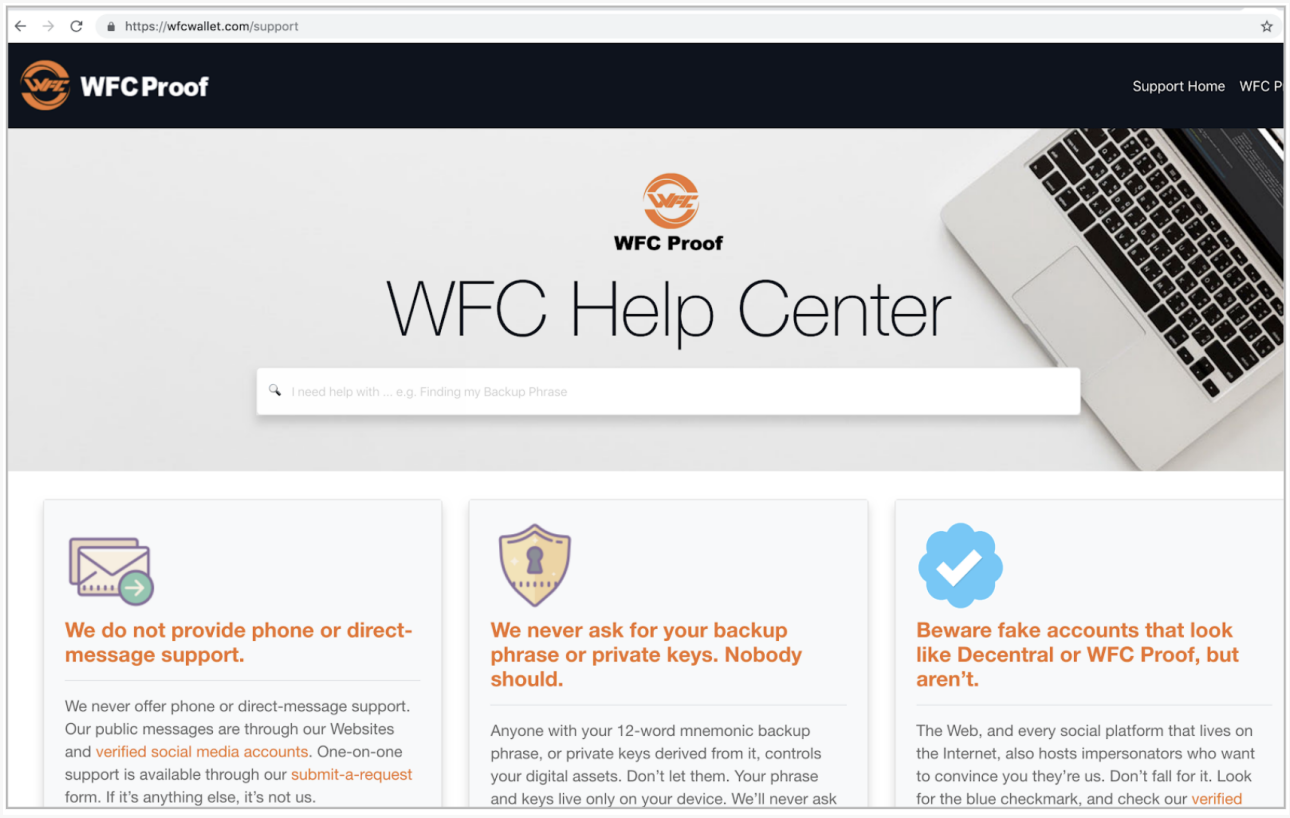
Nearly all instances of cryptocurrency theft fall into one of three categories, which we'll explore below.

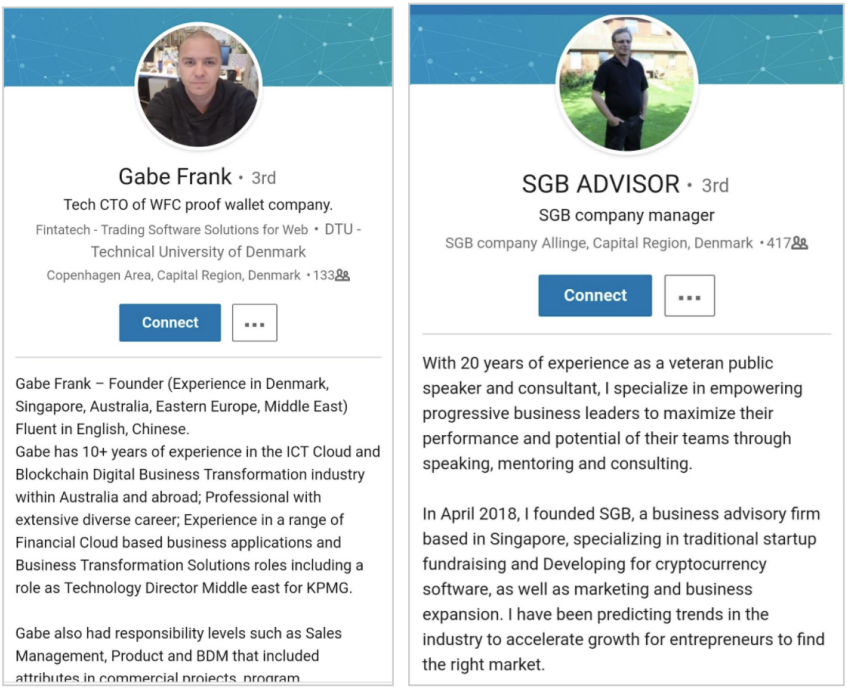
Exchange attacks

Bad actors have stolen billions of dollars' worth of cryptocurrency by attacking exchange wallets. Bitpoint, Binance, DragonEx, and several others have all been the target of prominent hacks.

You may think these cybercriminals must have exceptional computer skills to force their way into seemingly impenetrable cryptocurrency wallets. But in fact, social engineering is their most frequently used tactic. Attackers will typically try to trick exchange employees into downloading malware that gives them access to one or more accounts. Once they're in, savvy attackers will wait for months or more, observing the patterns of how money flows in and out so that they can steal the highest amount possible.

What does this look like in the real world? In one particularly audacious scheme, hackers set up an entire fake company, complete with a website, social media presence, and executive bios.





The hackers claimed to have created an automated trading bot, and messaged several employees at an exchange asking them to download the free trial. At least one of them did, and lo and behold, the trial included malware that helped the hackers obtain the private keys for several users' wallets. The hackers began draining funds from those wallets soon after gaining access.

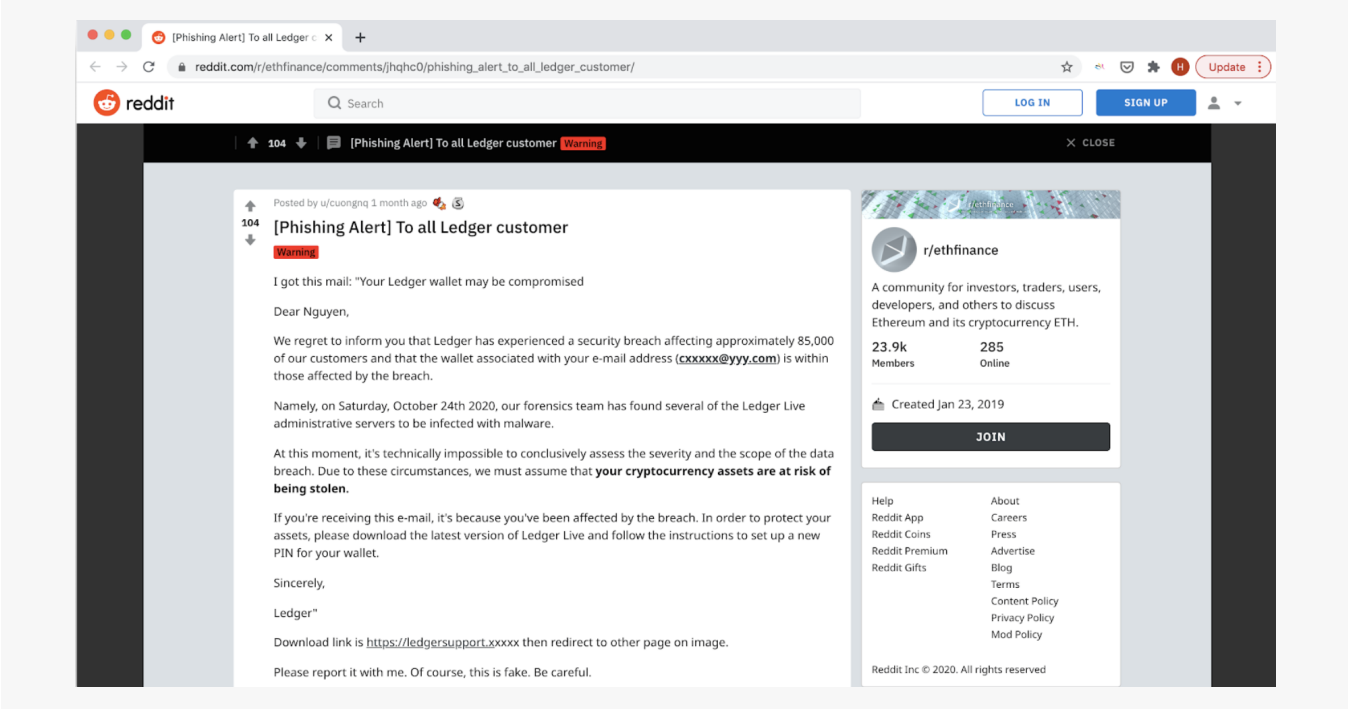
Hacks are a big concern for exchanges. It remains to be seen how the threat evolves as the industry matures and operational security measures become increasingly sophisticated.

Attacks on individuals

Even more common than exchange attacks are attacks on individual cryptocurrency holders, which are also predominantly carried out through phishing or social engineering. However, we know those numbers are almost certainly lower than the true total due to underreporting — many individuals don't report cryptocurrency theft to the authorities.

In 2020, the Ledger phishing attack resulted in cryptocurrency being stolen from several individuals. Ledger is a popular provider of hardware cryptocurrency wallets, which are physical devices on which cryptocurrency can be stored, similar to a conventional cryptocurrency wallet. In July 2020, the company published a blog post revealing that many users' email addresses had been compromised in a data breach. A few months later in October, Ledger customers reported receiving emails from closely spoofed versions of the Ledger website domain. The email claimed that Ledger's servers had been hacked with

malware and that customers' funds were in danger of being stolen unless they clicked a link in the email to download the latest version of Ledger's software. Clicking the link leads users to a web page that mimics the Ledger website.



Caption: A reddit post describing the phishing emails.

The email and website however, are part of a sophisticated phishing attack. Instead of a software update, Ledger users who click the download link on the fake web page actually download malware that drains their Ledger wallet. Overall, CoinTelegraph reported that Ledger users lost 1.1 million XRP (roughly $645,000) within the first week of the phishing campaign. Overall, we've tracked more than $3.5 million worth of cryptocurrency that was stolen from Ledger users since the phishing attack began. The Ledger attack underlines how important it is for cryptocurrency holders to be vigilant for phishing attacks, and verify that emails they receive from cryptocurrency businesses are legitimate before clicking.

DeFi exploits

As DeFi usage grew in 2020, so too did the amount stolen from DeFi platforms. In fact, the data suggests that DeFi platforms were uniquely vulnerable to attack. Despite representing just 6% of all cryptocurrency activity, DeFi platforms lost roughly 33% of all cryptocurrency stolen in 2020 and were victims in nearly half of all individual attacks. Overall, cybercriminals stole more than $170 million worth of cryptocurrency from DeFi platforms. How? Price manipulation attacks.

Price manipulation was the key to nearly every notable attack on DeFi platforms in 2020. Transactions happen almost instantly in DeFi with very few mechanisms in place to prevent shady transactions, so bad actors can reap huge gains by manipulating a cryptocurrency's price on one or more DeFi platforms. DeFi platforms rely on tools called price oracles to get asset pricing data from an external source — usually from another exchange, other service, or data provider like CoinMarketCap — to ensure its assets are priced in accordance with the rest of the market. However, most DeFi platforms use centralized price oracles, which rely on just one node to feed data to the rest of the platform and often draw on a single source of pricing data, leaving them vulnerable to attack.

Price manipulation might seem like an unlikely attack method for cybercriminals, as upping the price of any one crypto asset requires upfront capital to pump up its value, right? Not so in DeFi, thanks to **flash loans**.

Flash loans allow DeFi users to instantly receive loans without putting up collateral, use the loaned funds to make trades elsewhere, and repay the loan in one instant transaction. If they don't pay back the loan, the entire transaction is instantly rolled back, meaning the lender receives the original capital back as if the loan never happened, something only possible with smart contracts. In effect, this means little to no risk for either side: If the trade the borrower wants to make with the loaned funds doesn't work out and they can't pay back the loan, neither they nor the lender loses anything. This also means lenders can charge very low interest on flash loans. Traders often use flash loans to get the funds necessary to exploit arbitrage opportunities, using borrowed funds to take advantage of pricing disparities across platforms and come away with a small profit after paying back the loan.

However, in 2020, cybercriminals weaponized flash loans by using the borrowed funds to purchase a crypto asset, pump up its price, and sell it for a large profit, thereby enabling them to easily pay off the original loan and pocket the remaining funds. We saw an example of this in February's two hacks of bZx, a DeFi protocol that allows users to build apps for decentralized lending, margin trading, and other financial activities. In the first hack, the cybercriminals borrowed a large amount of Ether from bZx in a flash loan, used it to buy and pump up the price of wrapped Bitcoin on Uniswap — at one point, the wrapped Bitcoin price on Uniswap reached 109.8 ETH, compared to 38 for the market in general. The attacker then exchanged their wrapped Bitcoin for a healthy profit of Ether, some of which was used to pay off the original flash loan. All in all, the attacker netted $350,000 worth of Ether. The second attack, a copycat of the first, netted $633,000. The identity of the hackers is unknown, and it's unclear whether or not the same individual or group is responsible for both hacks.

Illicit actor/organization

Description	Individuals and/or organizations that operate directly or indirectly in various forms of illicit activities.
How it works	These entities are directly or indirectly involved with risky entities such as darknet markets, fraud shops, extremist financing, hacking, etc.
Examples	Shadow Broker Auction, dark.fail Donation Address, AD0
Risk type	High
Emerging trends	Several alt-right figures associated with the rally preceding the 2021 U.S. Capitol riot received cryptocurrency donations one month prior.

Illicit actor organizations are groups transacting with cryptocurrency whose activity doesn't necessarily rise to the level of criminal, but are nonetheless considered risky due to their proximity to illegal activity or reputational risk.

One example is sites implicitly associated with sex work, such as RubRatings. RubRatings allows masseuses to post ads soliciting clients, and includes Bitcoin as a payment option. While massages are obviously legal, language RubRatings' website implies the availability of sexual services, and the service has been cited as a human trafficking facilitator, so we would categorize it as an illicit actor organization.

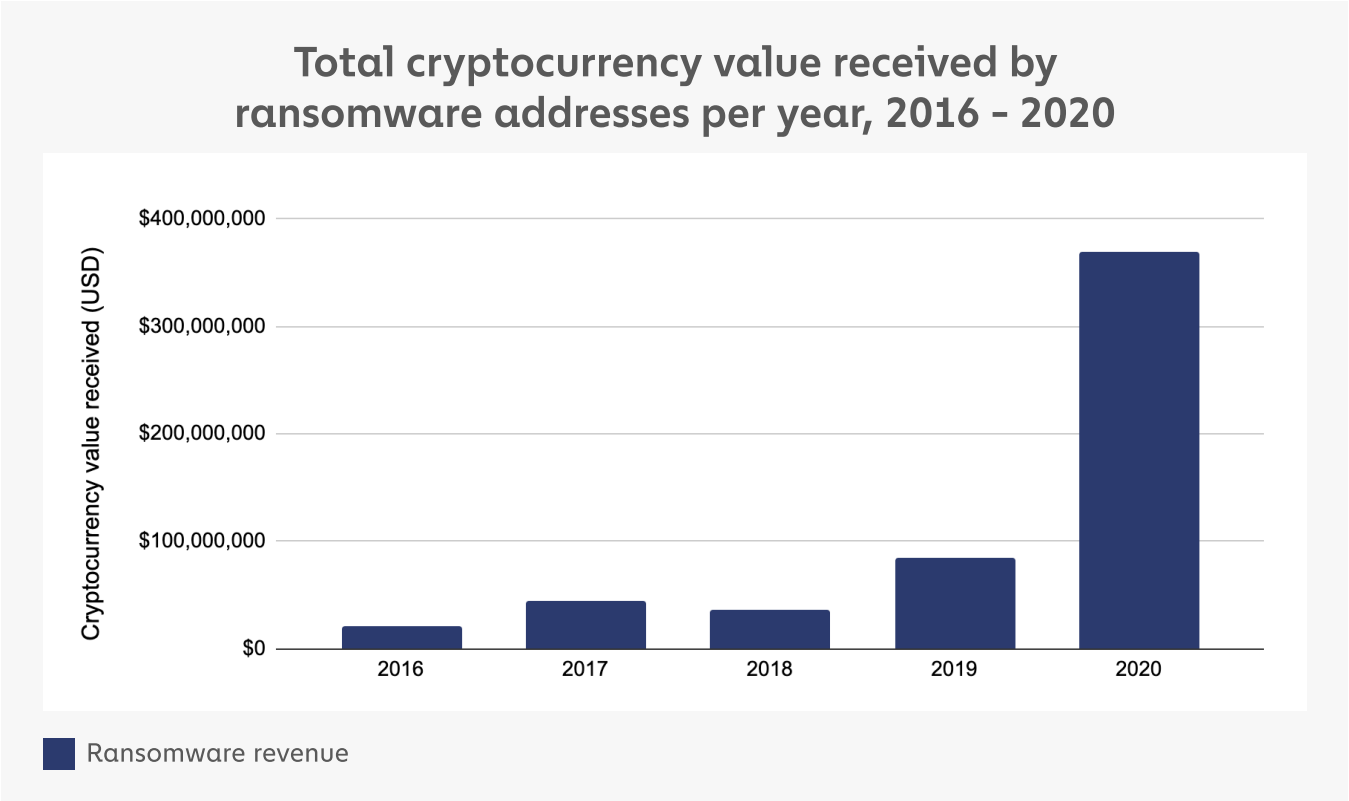
Another example is organizations and public figures associated with domestic extremism and racial hatred. Many of these organizations accept cryptocurrency donations, and we expect that more will as they continue to be deplatformed from conventional payment platforms and social media networks. Examples include publications like the Daily Stormer and public figures like Nick Fuentes. Extremist rhetoric on its own generally isn't illegal in most jurisdictions, but many of these groups have been associated with violent incidents such as the 2017 Unite the Right rally in Charlottesville, Virginia or the 2021 U.S. Capitol riot. In the latter case, Chainalysis found that several alt-right figures, including some associated with the rally directly preceding the riot, received large Bitcoin donations one month before.

Ransomware

Description	Malicious software that encrypts computer files for ransom
How it works	Social engineering or vulnerabilities that lead victims to download malicious software
Examples	WannaCry 2.0, CryptoLocker, SamSam, NotPetya, Robbinhood, CrySiS
Risk type	High
Possible exploit	Lots of organizations still haven't installed critical patches
Emerging trends	Attacks have grown more targeted, use more sophisticated social engineering techniques, and are commanding higher ransoms.

Ransomware is a method of cybercrime in which hackers inject malicious software onto a user's computer that encrypts all of the files within. The hackers then demand the user pay a ransom to regain access to the files, usually in cryptocurrency.

Ransomware attacks increased drastically in 2020 with the onset of the Covid pandemic.



Blockchain analysis shows that the total amount paid by ransomware victims increased by 336% this year to reach nearly $370 million worth of cryptocurrency. No other category of cryptocurrency-based crime had a higher growth rate. Keep in mind that this number is a lower bound of the true total, as underreporting means we likely haven't categorized every victim payment address in our datasets.

Victim organizations have ranged drastically over the years and include schools, hospitals, and even local municipalities.

The University Of California Pays $1 Million Ransom Following Cyber Attack



Davey Winder Senior Contributor ⓘ

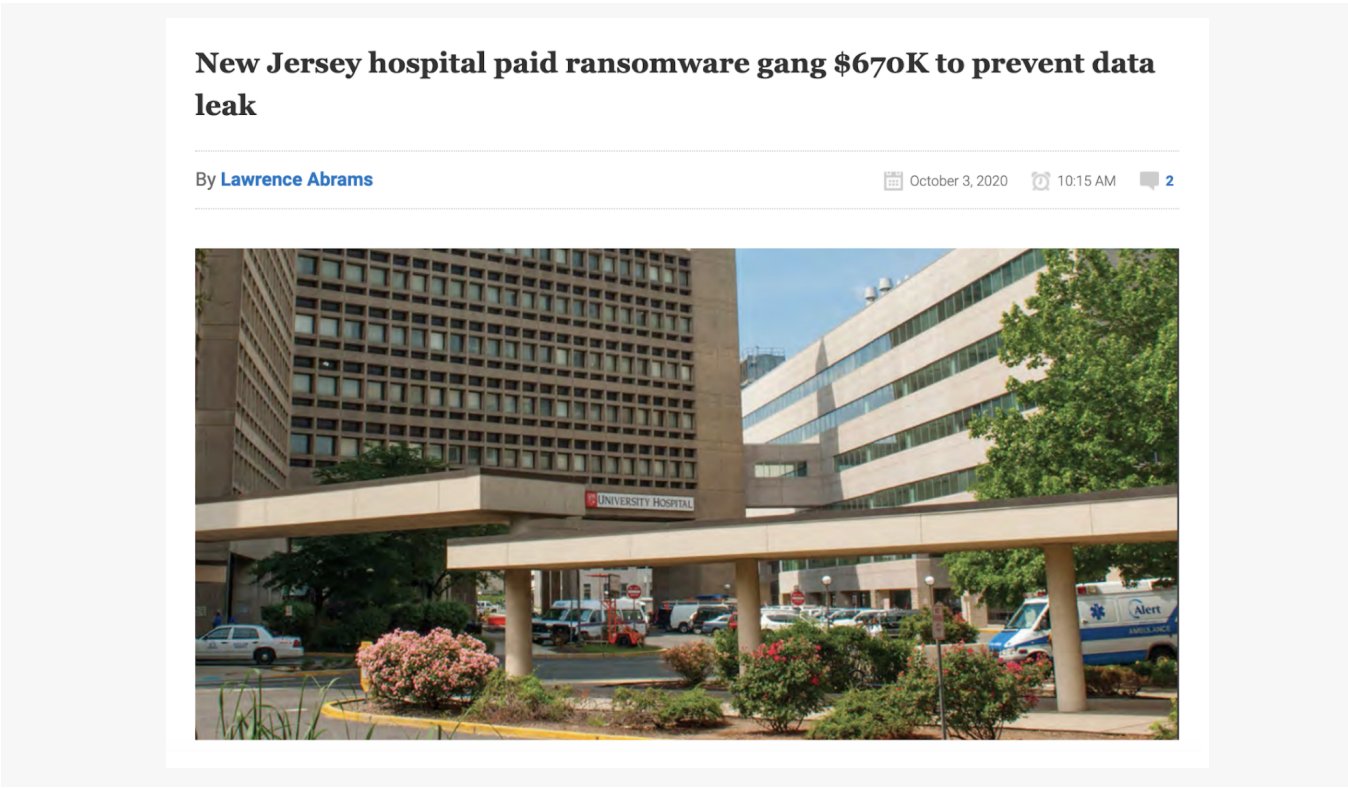
Cybersecurity

I report and analyse breaking cybersecurity and privacy stories



The University of California, San Francisco, pays $1 million to ransomware attackers

Source: Forbes



New Jersey hospital paid ransomware gang $670K to prevent data leak

By Lawrence Abrams

October 3, 2020 10:15 AM 2

Source: Bleeping Computer



Redcar cyber-attack 'cost council £10.4m'

5 August 2020

Redcar and Cleveland's online services had to be rebuilt in order to get back online

Source: BBC

Notable, widespread ransomware campaigns include:

- Doppelpaymer
- Ryuk
- Sodinokibi
- Netwalker
- WannaCry
- Petya and its updated version, NotPetya
- SamSam

The Iran-based hackers behind SamSam became the first people to have their Bitcoin addresses listed on the US Department of Treasury Office of Foreign Assets Control (OFAC) sanctions list, after allegedly extorting more than $6 million from ransomware attack victims and causing over $30 million in damage.[7]

Who's behind most ransomware attacks? According to security researchers most of these bad actors fall into one of two groups.

Many are part of **organized crime** groups. These attackers typically play a volume game, launching attacks on many organizations for low dollar amounts. Most ransomware attackers demand victims pay 1 BTC (about $7500 as of this writing), though they'll adjust that figure based on that they think the victim is able to pay.

State actors are the second group behind many of the largest attacks. For instance, security researchers such as Recorded Future and Crowstrike have reported that the North Korea-sponsored Lazarus Group hacking outfit carried out the WannaCry ransomware campaign that made headlines in 2017. WannaCry was notable for its enormous scale, infecting 200,000 computers across 150 countries and causing over $4 billion in damages. WannaCry targeted organizations known all over the world, from Fortune 100 corporations like FedEx to government services like Britain's National Health Service. In some cases of state-sponsored attacks, payment appears to have been secondary to simply causing chaos for targeted groups. In fact, the Russian-linked NotPetya attacks didn't even appear to have functioning mechanisms for collecting payment or decrypting user's files.

How do hackers determine who they target with ransomware? Victims typically fall into one or more of the following four categories.

[7] Slate, https://slate.com/technology/2018/12/iranian-indictment-samsam-ransomware-bitcoin-wallet-addresses.html

Typical targets today



High-value business targets refers to small to medium sized businesses. According to Beazley Breach Response Services, 70% of ransomware victims were small businesses in 2018, with a heavy preference for financial services companies. This isn't surprising, as these organizations tend to have less robust security than larger companies and are often willing to pay up and resume business as usual.

Organizations with sensitive data. Organizations dealing with the potential loss of sensitive data have a huge incentive to pay up fast if they get hit by ransomware. Hospitals are a good example. Every second they don't have access to patients' medical data puts those patients at risk. Other frequently-targeted companies in this category include police protection programs and news organizations.

Low-security organizations. These targets are the low-hanging fruit for hackers in that they don't have high IT security. For instance, many educational institutions have limited technology budgets, leaving them vulnerable to cyber attacks. HR departments have proven to be a weak point at many companies, as hackers have breached their systems by submitting fake job applications with malware attached.

Organizations with sensitive government information. State-sponsored actors specifically target organizations connected to their adversaries, such as government agencies, defense contractors, or political campaigns.

What happens when a ransomware attack hits an organization?



When organizations are hit by a ransomware attack, cyber security experts recommend that they contact law enforcement immediately and provide them the ransomware payment address. Investigators can then use blockchain analysis software like Chainalysis to examine the flow of funds to and from the address, identify the services the ransomware operators use to convert funds and cash out, and hopefully link the address to a real-world entity.

Terrorist financing

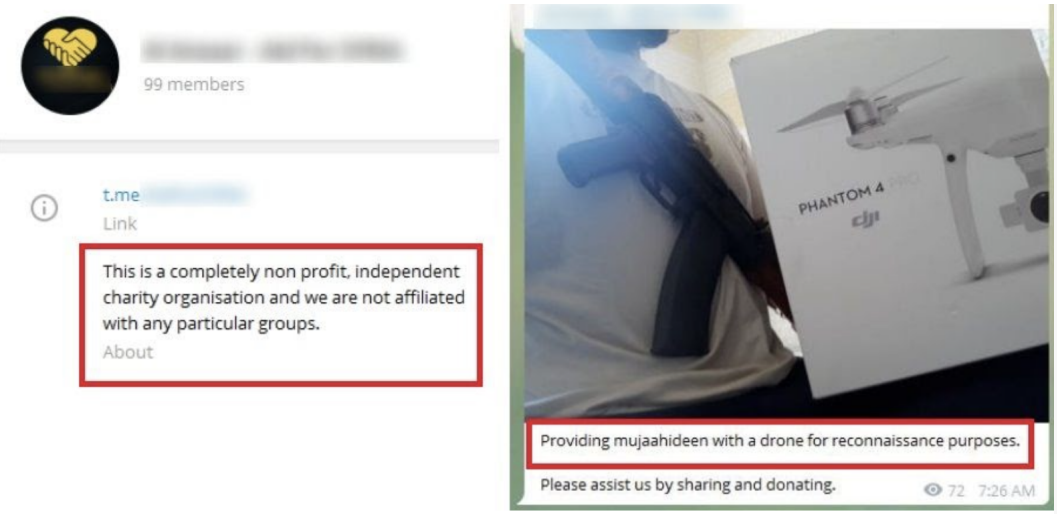
Description	Terrorist groups' fundraising campaigns soliciting cryptocurrency
How it works	Via social media or one-on-one private conversations, often via encrypted channels
Examples	Hamas, Al Sadaqah, Incite The Believers (Al-Qaeda affiliate)
Risk type	Severe
Possible exploit	Innovations (e.g. privacy coins) might increase terrorists' adoption
Emerging trends	On the rise, with varying (but increasing) levels of sophistication

Terrorist organizations are increasingly using cryptocurrency to raise money, typically soliciting donations through public fundraising efforts and one-on-one conversations on private, encrypted chat apps.

Terrorist groups are often quite explicit in stating what these donations will be used for. Check out the poster below produced by Jaysh Al-Ummah, a militant group in Gaza. They tell potential donors exactly what weapons their donations to the advertised Bitcoin address (obscured) will help their fighters buy.



Other solicitations are a bit more subtle and ambiguous in letting their audience know exactly who they're donating to. Some terrorist-linked organizations may present themselves as regional charities raising money for medical supplies or to help the inhabitants of war-torn areas. The below image shows messages from a charity group claiming not to be linked to any militant groups, but later soliciting donations for reconnaissance drones to be used by mujahideen fighters.



While the amounts of cryptocurrency being donated to terrorists are generally small today, the ability for these groups to solicit relatively frictionless donations from anyone in the world represents a troubling trend. Not to mention, the costs of executing a terrorist attack are very low. As Under Secretary to the Treasury for Terrorism and Financial Intelligence Sigal Mandelker noted in a recent presentation,[8] the average remittance payment with suspected terrorism links is only $600, which is more than enough to pay for a homemade suicide bomb or similar weapon. The activity could grow as anonymity-bolstering technology such as mixers and the like continue to improve.

Sanctions

Description	Anyone who falls under the authority jurisdiction issuing a sanction, including nationals operating elsewhere or businesses abroad that directly operate into the issuing jurisdiction, are prohibited from business dealings with the sanctioned entity.
How it works	Entity names and cryptocurrency addresses are listed (in the US, it's the Specially Designated Nationals list, or SDN)
Examples	SamSam ransomware individuals, fentanyl traffickers
Risk type	Severe
Possible exploit	Jurisdictions such as Iran and Venezuela have indicated intent to use cryptocurrencies to get around sanctions
Emerging trends	Illicit activity can involve addresses at exchanges or uniquely generated ones

Sanctions are issued by governments to designate individuals and organizations with whom citizens are forbidden from doing business. Sanctions typically cover not just the prohibited entities themselves, but also any instrumentalities owned or controlled by those entities, including operating companies, bank accounts, and most recently, cryptocurrency addresses. You can find the list of those sanctioned by the U.S., for instance, on OFAC's Specially Designated Nationals (SDN) list.[9]

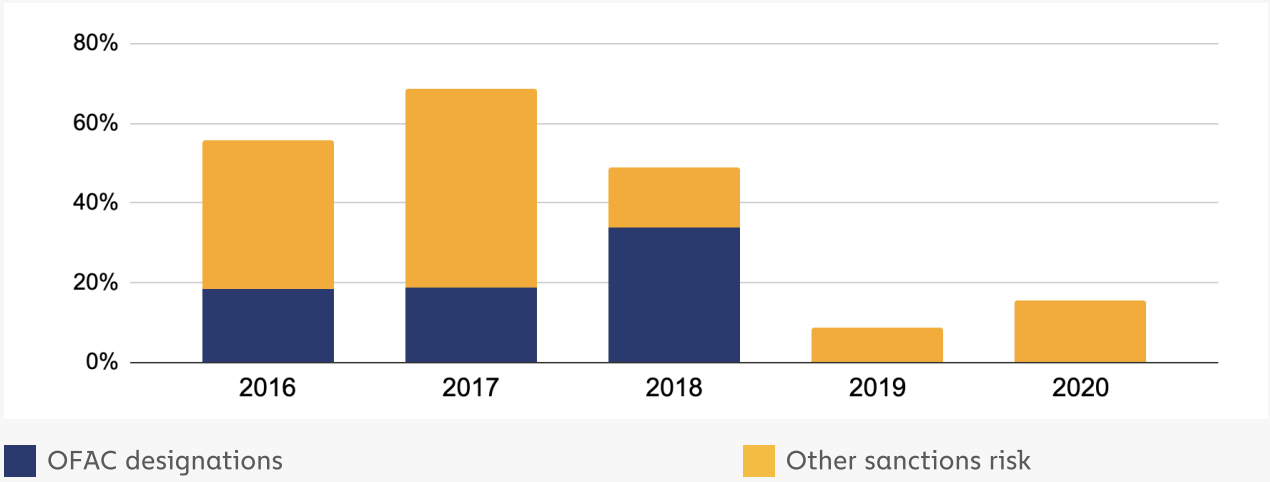
As mentioned in the ransomware section, the two Iran-based hackers who created the SamSam ransomware campaign became the first people to have their cryptocurrency addresses added to their entries on the OFAC sanctions list in [2018]. But others have joined

[8] U.S. Department of the Treasury, https://home.treasury.gov/news/press-releases/sm687
[9] OFAC Sanctions List, https://sanctionssearch.ofac.treas.gov/

them since then. In August of 2019, OFAC sanctioned two Chinese nationals accused of manufacturing fentanyl and trafficking it into the U.S. for sale, and included the cryptocurrency addresses they used to accept payments.[10]

Since then, other cybercriminal groups associated with ransomware strains such as the Russia-affiliated Evil Corp have also been sanctioned. In August 2020, OFAC released an advisory warning that ransomware victims who make ransom payments to sanctioned cybercriminal groups, as well as those who facilitate those payments, could themselves be at risk of sanctions violations. The facilitation point is important, as there's a robust industry of consultants who help ransomware victims negotiate with and pay ransomware attackers. Based on that advisor, blockchain analysis of ransomware payments to sanctioned groups shows that as much as 15% of all ransomware payments made in 2020 carried sanctions risk.

Share of all ransomware payments associated with OFAC designations and other sanctions risk, 2016 - 2020



Please note that all payments to addresses associated with OFAC-sanctioned individuals or groups noted on this chart took place before those individuals or groups were added to the OFAC sanctions list.

Generally speaking, any exposure to sanctioned cryptocurrency addresses could draw heavy scrutiny from law enforcement for cryptocurrency businesses and any financial institutions working with those cryptocurrency businesses, including potential obligations to block assets from continuing transit or returning to designated senders, or otherwise benefiting designated entities, such as relieving debts. Exposure may also trigger Suspicious Activity/Transaction Report requirements. Chainalysis updates OFAC sanctioned addresses within 15 minutes, empowering our product users to react quickly to new designations.

[10] U.S. Department of the Treasury Press Release, https://home.treasury.gov/news/press-releases/sm756

Child Sexual Abuse Material Sites

Description	Smaller scale websites on dark web that specialize in the sale of child sexual abuse material (also referred to as child pornography)
How it works	Buyers often become (re)sellers of content (it's difficult to create and the same content be consumed over and over again by new buyers)
Examples	Welcome to Video site
Risk type	Severe
Possible exploit	Scam/fake sites; mirror sites (reselling material from another site)
Emerging trends	Smaller sites don't remain open for long (may be due to law enforcement efforts). Also, Monero increasingly being accepted.

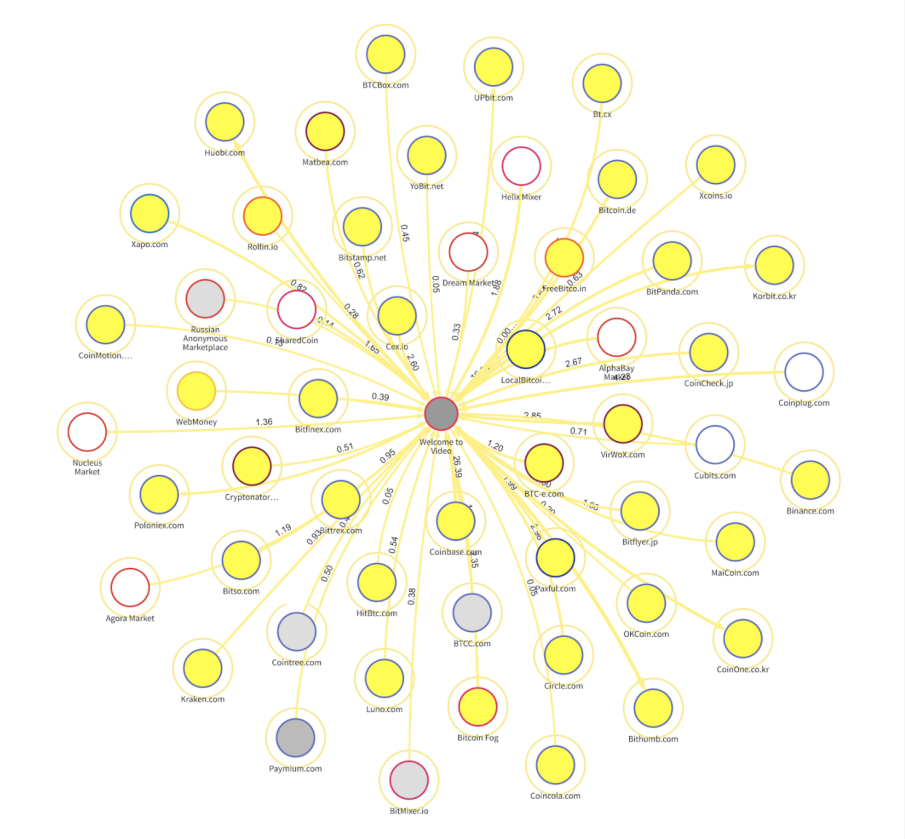
A small, opaque subset of darknet websites specialize in the sale of child sexual abuse material (CSAM), often using cryptocurrency to facilitate the transactions. Most mainstream darknet markets ban this material, hence the need for specialized shops. CSAM-focused markets typically don't stay in operation for very long, possibly due to law enforcement operations and efforts by those running the sites to avoid detection.

Some CSAM sites function similarly to darknet markets in that they bring buyers and sellers together in a central marketplace. Others act as the sole seller themselves, and some demand users upload their own CSAM content to access the site's material. Oftentimes, users will buy CSAM on one site and then turn around and sell it somewhere else.

In 2018, Chainalysis worked with the IRS Criminal Investigations unit, Department of Homeland Security, and other law enforcement agencies around the globe to take down Welcome to Video (WTV), the largest known CSAM website to date by volume of material available.



Little is known to the general public about how these sites operate, so WTV provides a useful case study. WTV operated out of South Korea and allowed users to either buy CSAM with Bitcoin or upload their own content in exchange for points they could use to download more. Users received their own unique Bitcoin address upon signing up to use the site, which they would then use to send funds in exchange for content. WTV had 1.3 million Bitcoin addresses ready to be assigned at the time it was shut down, indicating it could support a large user base. Between 2015 and 2018, the site received more than $353,000 in payments.



Investigators used Chainalysis Reactor to trace the flow of cryptocurrency funds in and out of the WTV operator's bitcoin address, as shown in the graph above. That analysis enabled investigators to identify the exchanges the site's users and operator were using, who they then subpoenaed to uncover more leads.

After shutting down the site and arresting its owner, investigators coordinated with other agencies around the world to arrest more than 330 WTV users and free at least 23 children from their abusers. You can read a more thorough breakdown of the case on our blog.[11]

[11] Chainalysis Blog, https://blog.chainalysis.com/reports/chainalysis-doj-welcome-to-video-shutdown

ABOUT CHAINALYSIS

Chainalysis is the blockchain analysis company. We provide data, software, services, and research to government agencies, exchanges, financial institutions, and insurance and cybersecurity companies in over 60 countries. Our data platform powers investigation, compliance, and risk management tools that have been used to solve some of the world's most high-profile cyber criminal cases and grow consumer access to cryptocurrency safely. Backed by Accel, Addition, Benchmark, Paradigm, Ribbit, and other leading names in venture capital, Chainalysis builds trust in blockchains to promote more financial freedom with less risk. For more information, visit **www.chainalysis.com**.

GET IN TOUCH:

info@chainalysis.com

FOR MORE CONTENT:

blog.chainalysis.com

This document is not intended as legal advice. We recommend you consult your general counsel, chief compliance officer, and/or own compliance policies & procedures for regulatory, legal or compliance-related questions.

Building trust in blockchains

Chainalysis