

Coin Swap Services

Cashing out dirty crypto in the
cybercriminal underworld

Executive Summary

One of the weak points of a typical cybercriminal operation is the need for the offender to cash out their illicitly-acquired cryptoassets in order to enjoy their criminal profits. For most criminals, centralized exchanges and other typical virtual asset services are off-limits, as they require compliance with anti-money laundering (AML) regulations and therefore leave a trace for law enforcement.

Instead, a rising group of services have begun to offer cashing-out and crypto conversion services in a more anonymous way – often advertising themselves exclusively to a cybercriminal audience. These are services that do not require an account or any form of identity checks to operate. The user simply sends crypto to a wallet address belonging to the service, which then sends the converted equivalent (minus commission) in either cryptoassets or fiat currency (often the Russian Ruble) to a predetermined account.

These services are “coin swap services” – otherwise known as “instant swap exchanges”. While some are legitimate-facing, many others make no secret of their intention to cater to a cybercriminal clientele. Many of these illicit services are often advertised on the same forums as stolen data, malware and other illicit products or services. They usually operate anonymously, sometimes on Telegram, and boast about their crypto “cleaning” features as much as their conversion rates.

The function of coin swap services are becoming increasingly integral to the cybercriminal ecosystem. Elliptic’s [“The State of Cross-Chain Crime”](#) report identified at least \$1.2 billion of illicit funds being processed by coin swap services, including from sanctioned entities. Virtual asset service providers and criminal investigators need to be aware of and effectively manage the growing risks from engaging with illicit coin swap services.

This briefing note delves deeper into the nature, function and ecosystem of these services, providing case studies on some of the most prolific criminal exchangers.

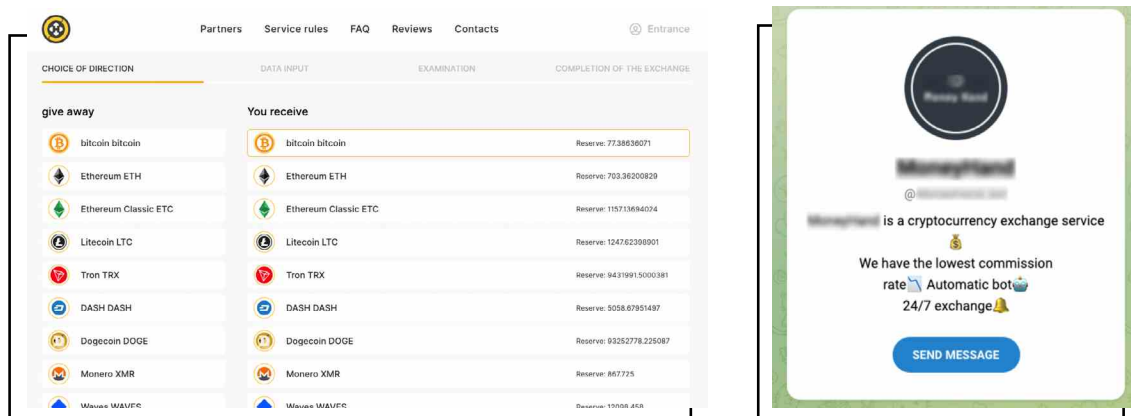
Coin Swaps at a Glance:

- Coin swap services are instant crypto exchange services that swap cryptoassets into other cryptoassets – or into fiat currency – without the need for an account or ID
- Many are anonymous, operate on (predominantly Russian) cybercrime forums and are dedicated to an exclusively criminal clientele
- Elliptic’s “The State of Cross-chain Crime” report has identified over \$1.2 billion in illicit or high risk cryptoassets being sent through coin swap services – including proceeds from dark web markets, sanctioned entities, thefts, ponzi schemes and ransomware

Coin Swap Services in the Criminal Underworld

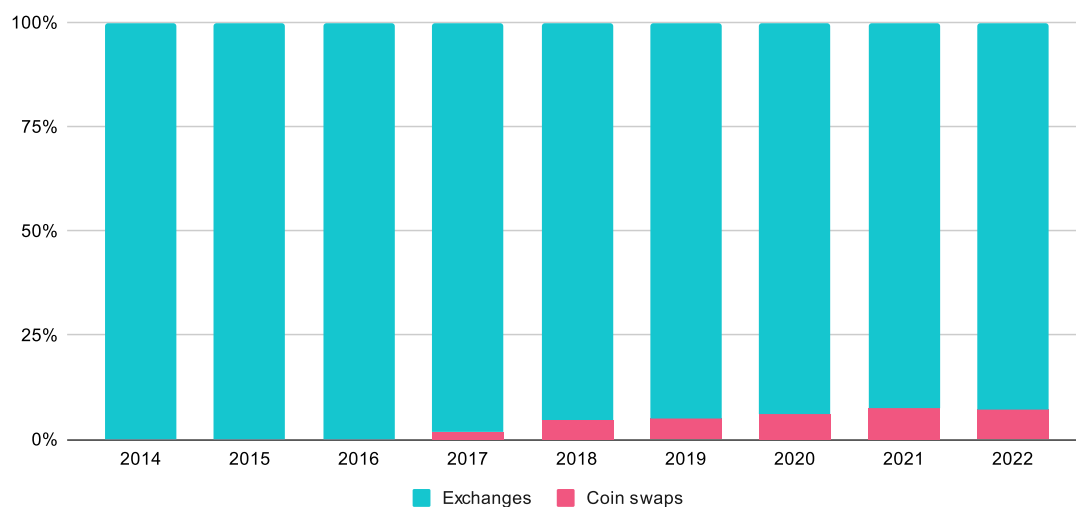
Besides being anonymous and offering anonymous swaps, coin swap services advertised on cybercrime forums have a number of other common characteristics:

- They are predominantly Russian speaking. Countries and currencies for which many of these services offer support include Russia, Ukraine and Kazakhstan. Besides rubles and hryvnia, many also provide Euro and USD cash outs.
- Their crypto reserves are often lower than mainstream exchangers due to the specific nature of their clientele, meaning their commission fees are typically high
- They sometimes offer conversion services to Monero or other privacy-enhanced coins
- They often use a similar site template (pictured below) or operate on Telegram



An example of a coin swap service as a website (left) and Telegram bot channel (right)

Percentage of Illicit Proceeds Laundered through Coin Swap Services Compared to Centralized Exchanges

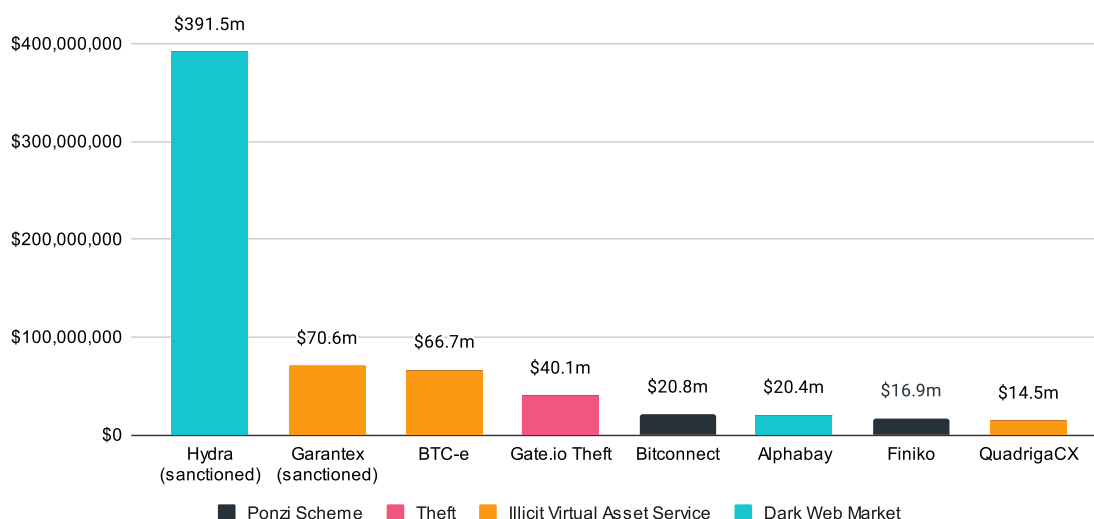


General Usage

The use of coin swap services – including legitimate-facing ones that serve the needs of DeFi investors and other licit users to efficiently swap their assets – has increased over the years. In 2021, coin swap services processed over \$8.1 billion in bitcoin, up over 210% from the year before.

The criminal use and preference of anonymous coin swap services as opposed to more risky AML-compliant centralized exchanges is increasing over time. In 2014, coin swap services barely laundered more than \$70,000. In 2021, they had laundered half a billion dollars worth of illicit or high risk crypto – around 7.5% of the total laundered through centralized and coin swap exchanges.

The Major Illicit Services sending Bitcoin through Coin Swap Services



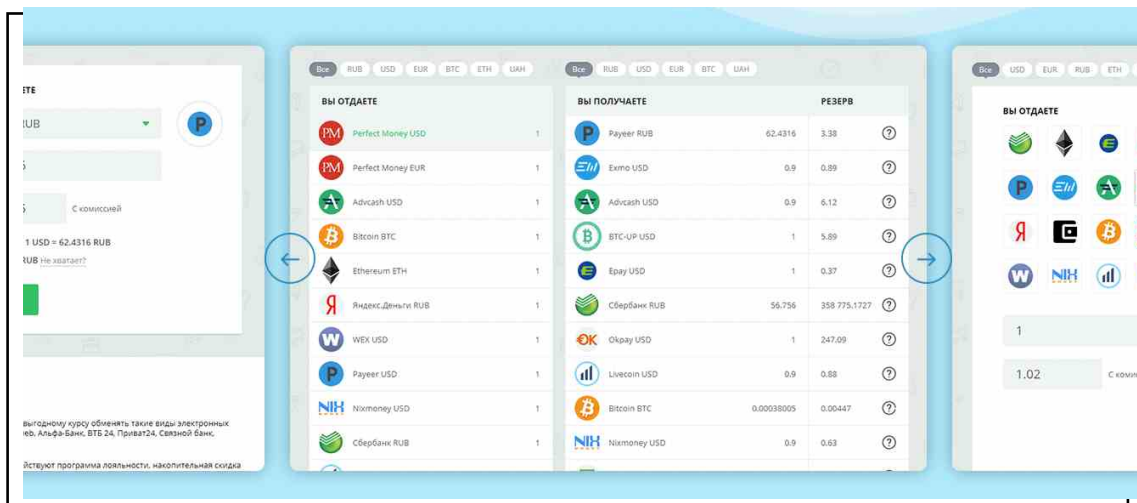
A breakdown of the illicit origin of the \$1.2 billion of crypto laundered through coin swaps is available in Elliptic's "The State of Cross-chain Crime" report. Dark Web markets, such as Hydra (now sanctioned and shut down), Alphabay and more recently Solaris – are prolific users of coin swap services to cash out illicit funds.

Similarly, illicit virtual asset services – such as the now-sanctioned Garantex exchange and the now-seized BTC-e – have made use of coin swap services to further layer illicit assets in their control. Proceeds of crypto thefts from exchanges or DeFi protocols – with some linked to North Korea's "Lazarus Group" – have also been processed by coin swap services.

Operation

Coin Swap Services operate on either websites or Telegram. On rarer occasions, operators can run their services directly through the direct messaging function of a cybercrime forum or through a Jabber messaging address. More popular coin swaps often have multiple modes of operation.

Services that run on sites will typically share a similar template. The design is offered by external providers, which build the front-end website and provide a script for the service. Many also have an instant bot helpline. One service that offers front-end exchanger scripts offers their service for a monthly \$275 or a lump sum of \$7,990 – and claims to be used by over 200 coin swaps.



A Coin Swap UI script provider showcasing their website designs

In the case of direct messaging services such as Telegram, the user typically has to speak to and agree a rate with a live operator. Typically, to avoid scams, a user will initiate a swap using one medium (e.g. Telegram) and confirm the transaction using another medium (e.g. a forum direct message) to ensure that they have not fallen victim to a scam exchanger. Many scammers set up channels bearing similar names to popular coin swap services in an attempt to trap more victims.

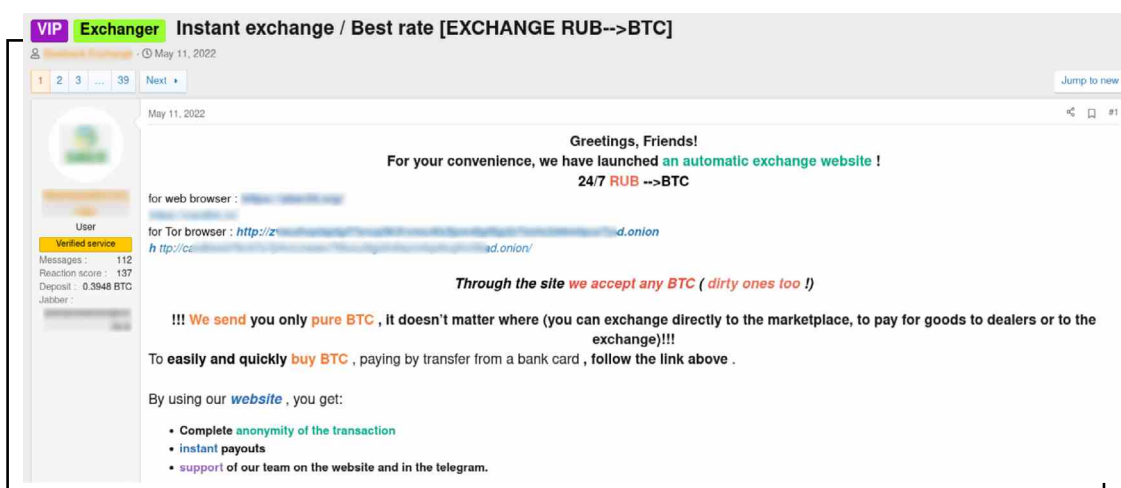
In order to maximise their liquidity to perform high-volume money laundering, many of these services are “nested” in other exchanges. This means that while they advertise themselves as a service on their own, their liquidity or underlying crypto accounts are provided to them by a virtual asset service provider that is either oblivious or turns a blind eye to their activities. Examples include the sanctioned Russian exchange Garantex, which has itself been associated with the laundering of illicit proceeds.

Advertisement

There are entire forums dedicated to cashing out the proceeds of cybercrime. On one such forum, around 40 services pay for advertising, with many more hosting forum threads with links to their services.

Coin Swap service advertisements are typically open about the level of risk they will accept in terms of dirty cryptoassets. Many will charge extra for crypto that is heavily “tainted”, such as those originating directly from a dark web market. Coin swap services that are nested in unwitting virtual asset services may be more conservative with their taint tolerance, often utilizing makeshift blockchain analytics solutions to manage their risk. This is to ensure that the exchange in which they are nested does not block their accounts.

In one blunt advertisement, an exchanger remarked that “what I do with your dirty crypto is my own concern”.




The screenshot shows a forum post from a user named 'VIP Exchanger' on May 11, 2022. The post title is 'Instant exchange / Best rate [EXCHANGE RUB-->BTC]'. The user profile on the left indicates they are a 'Verified service' with 112 messages, a reaction score of 137, and a deposit of 0.9848 BTC. The main text of the post reads: 'Greetings, Friends! For your convenience, we have launched an automatic exchange website ! 24/7 RUB -->BTC'. It provides links for web browser and Tor browser access. A key feature is highlighted: 'Through the site we accept any BTC (dirty ones too !)'. A bold statement follows: '!!! We send you only pure BTC , it doesn't matter where (you can exchange directly to the marketplace, to pay for goods to dealers or to the exchange)!!!'. The post concludes with 'To easily and quickly buy BTC , paying by transfer from a bank card , follow the link above .' and lists benefits: 'Complete anonymity of the transaction', 'instant payouts', and 'support of our team on the website and in the telegram.'

A coin swap service advertises itself on a Russian cybercrime forum, explicitly stating that it can exchange dirty crypto transactions directly from dark web marketplaces

Sanctions Risks

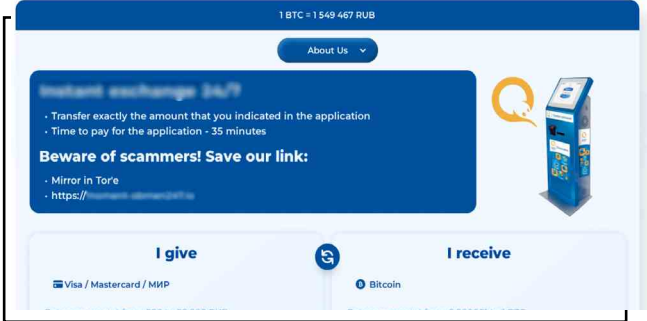
Coin Swap services may pose sanctions risks in three main ways:

1. They may willingly process funds from sanctioned entities: Elliptic’s “The State of Cross-chain Crime” report identified more than \$464 million in Bitcoin originating from sanctioned entities being sent through coin swap services – close to 40% of all illicit funds that they have processed. Dark web market Hydra, illicit exchanges Garantex, Chatex and the crypto-mixer Blender are some of the most prolific users. Separately, terrorist groups such as al-Qaeda and ISIS have made use of coin swap services to process low levels of Bitcoin donations.
2. Some services allow conversions to Russian banks sanctioned by the United States and the EU: In the lead up and response to Russia’s invasion of Ukraine in February 2022, many large Russian financial institutions were sanctioned by the United States, the United Kingdom and European Union. These include Sberbank and Alfa-Bank, both of which are common Ruble account destinations for crypto swapped using coin swap services.
3. Their operators may be affiliated with sanctioned entities: though they typically remain anonymous, operators may use their affiliation with notorious and sanctioned cybercrime services to boost their reputation and coin swap popularity. Some may also use them – in particular sanctioned virtual asset services that still remain operational – to nest their services.

 **The “former exchangers” of Hydra establish a new RUB-BTC service**

On May 5, 2022, an anonymous advertisement for a RUB-BTC exchanger appeared on a popular Russian cybercrime forum, claiming to be the “former exchangers” from Hydra marketplace. The team claimed to have run more than 15 exchangers on Hydra, which had been seized and sanctioned a month before.

In their advertisement, which has been verified by the cybercrime forum, the operators remark that “our team has not changed, our service has not changed, and this is the main thing”. The exchange allows users to swap Bitcoin to Ruble and vice versa.



Elliptic’s internal analysis suggests that the exchanger is used heavily to transact with dark web markets. These markets are the origin of over 82% of Bitcoin (with known sources) being processed by the exchanger. Meanwhile, over 95% of Bitcoin (with known destinations) originating from this exchanger are sent onward to dark web markets.

The Most Prolific Illicit Coin Swap Services

Elliptic tracks over 1,000 coin swap services – both legitimate and illicit-facing. However, only a small number of them maintain a strong degree of popularity across the cybercriminal ecosystem. This section provides an overview of four of the most prolific illicit exchangers that have earned notoriety across dark web criminal forums. These services are chosen to illustrate different functionalities that they may offer.

In order to not serve as inadvertent advertising for these services, their names are anonymised. Elliptic is able to provide details and URLs for these services to law enforcement agencies on request. You can get in touch via www.elliptic.co/contact.



Case Study: Coin Swap 1

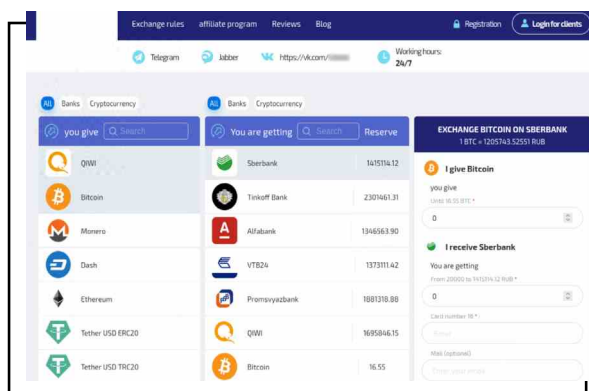
Coin Swap 1 is a service that allows swaps between cryptoassets and Ruble accounts in sanctioned banks. Besides online exchanges, the service also provides cash withdrawal opportunities by providing a QR code to initiate withdrawals at Russian ATMs. Coin Swap 1 claims to also have a courier service that operates “in almost all major cities of the world”.

The pool of Bitcoin used by Coin Swap 1 to fulfil its functions contains incoming funds mainly from dark web markets, though a small proportion also originates from child sex abuse material (CSAM) vendors. The exchange’s operation appears to be heavily integrated with Wasabi Wallet – a privacy enhanced crypto wallet provider.

Coin Swap 1’s dark forum advertisements have been viewed over 200,000 times, with the exchanger enjoying “VIP Service” status on at least one such forum. It operates both a site and direct messaging exchange service. The exchange promises that swapped crypto will have no more than 25% illicit exposure – with a typical illicit exposure of just 2%.

“We mix your coins, but not in the usual sense – we just take away the dirt from you and give away others that are clean according to the AML score.”

In Their Own Words: Coin Swap 1





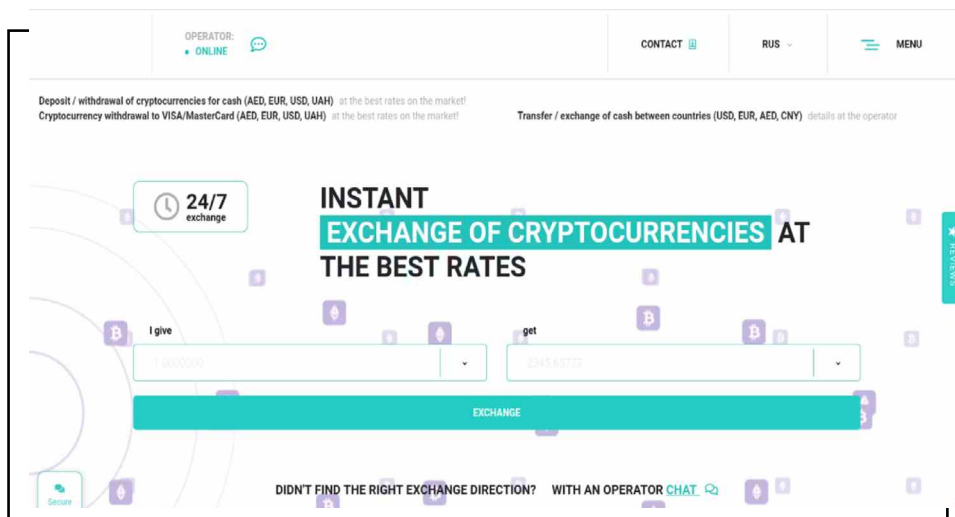
Case Study: Coin Swap 2

Coin Swap 2 is a service that allows the conversion of cryptoassets to fiat currencies such as the Russian Ruble, the Ukrainian Hryvnia, Euro and US Dollar. Uniquely from most other coin swaps, this service provides a larger range of convertible cryptoassets, inviting users with unadvertised assets to arrange a swap via the operator. The service handles assets such as Dogecoin and Shiba Inu (SHIB).

The service is also somewhat integrated with the Decentralized Finance (DeFi) ecosystem. It appears to market its ability to swap tainted cryptoassets from the Bitcoin blockchain to other blockchains through additional use of decentralized exchanges (DEXs) such as PancakeSwap and Uniswap.

The service's advertisements have almost 350,000 views across three different cybercrime forums. It appears to be predominantly used by former vendors or users of the now-sanctioned dark web marketplace Hydra. A significant amount of incoming BTC into the service also originates from All World Cards, a notorious former stolen credit card data vendor that shut down in February 2022. All World Cards had made headlines in June 2021 when it offered over 3 million credit cards for free in a successful illicit publicity stunt.

Elliptic's internal data suggests that the service has processed a small amount of funds from the Conti and Netwalker ransomware groups. Additionally, the site interface of Coin Swap 2 – seen below – has been identified as bearing resemblance to Lockbit ransomware group.





Case Study: Coin Swap 3

Coin Swap 3, which is also a Russia-based service, provides conversions between both cryptoassets and fiat currency, including cash and online accounts of sanctioned Russian banks.

Coin Swap 3's bitcoin reserves show a notable number of clients dealing with sanctioned crypto exchange Garantex, Hydra and other dark web markets. The service has 170,000 views on dark forums.

Like many other coin swaps, this service allows users to retrieve cash throughout Moscow, St Petersburg and most Russian airports through couriers. However, a unique functionality provided by Coin Swap 3 is the ability for clients to count cash using professional equipment in Moscow. When advertising the service, the coin swap's forum advertisement suggests:

You will be able to check cash on professional equipment in an area convenient for you within the Moscow Ring Road. The meeting takes place in armoured vehicles in the presence of security. You are guaranteed security and confidentiality.

In Their Own Words: Coin Swap 3

The screenshot displays the Coin Swap 3 interface. At the top, there are Telegram handles: @jabber.ru and @exploit.im. Below that, a status bar shows the time as 24/7, around the clock, and options for Registration and Authorization. A row of exchange rates is visible: 1 USD = 62.53 RUB, 1 BTC = 19272.11 USD, 1 BTC = 1205083.0383 RUB, 1 DASH = 2607.5394 RUB, 1 LTC = 53.24 USD, 1 ETH = 1308.04 USD.

give away	You receive	Reserve	Exchange
1 Bitcoin BTC	1268836.5379 Cash RUB	183287457.42 RUB	I give → Bitcoin BTC On 0.3. To 100 BTC
1 Ethereum ETH	18819.2114 Cash USD	1167907.42 USD	Your bitcoin wallet Дайте нам и другие кошельки
1 Tether ERC20 USDT	15814.302 Cash EUR	482500 EUR	I receive → the amount Cash RUB www.193207457.4197...
1 Tether TRC20 USDT	1251398.4098 Alfa-Bank cash-in RUB	9910471.36 RUB	Cash RUB
1 Monero XMR	1246519.6436 Russian Standard RUB	16960331.44 RUB	Биткоин-кошелек (для пополнения депозитов)
1 Litecoin LTC	1248983.33 TKC cash-in RUB	997836 RUB	1 Bitcoin BTC = 1268836.5379 Cash RUB
1 Ripple XRP	1073966.8893 QIWI wallet RUB	161001800.99 RUB	
100 Cash RUB	1213209.7065 Яндекс.Деньги RUB	3348974.36 RUB	
1 Cash USD	1079756.6695 Alfa Bank RUB	60308005.12 RUB	
100 QIWI wallet RUB	1084384.7261 Sberbank RUB	370895512.53 RUB	
100 Sberbank RUB	1086755 RUB	141474965.51 RUB	
100 Alfa Bank RUB	1065859.5 RUB	115598105.66 RUB	
100 Tinkoff RUB	1077772.8721 Visa/MasterCard PQ RUB	8188062.11 RUB	
100 BTB RUB	1077772.8721 Visa/MasterCard PQ RUB	8188062.11 RUB	



Case Study: Coin Swap 4

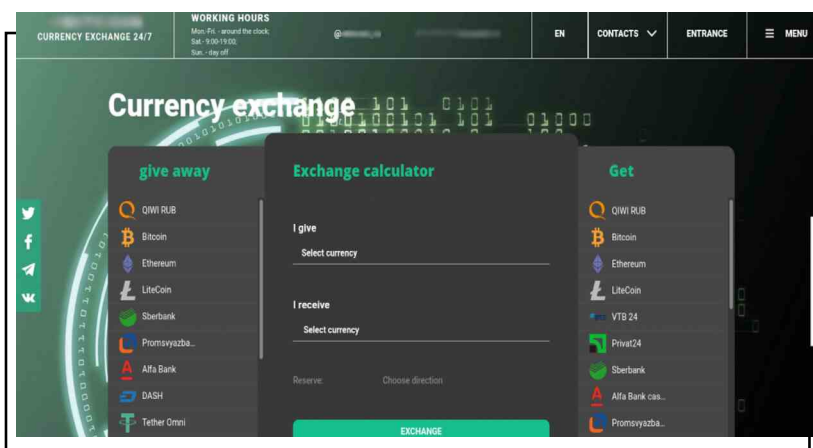
Coin Swap 4 is another service that is popular across the Russian cybercrime ecosystem, receiving around 150,000 views across different dark forums. Its bitcoin liquidity pool suggests that it is used by clients that have previously engaged with Hydra and other dark web markets.

Coin Swap 4 allows funds to be exchanged in both cryptoassets and fiat currency, including cash. It advertises a cash couriering team that provides services to major cities in both Russia (including Moscow and St Petersburg) and Ukraine (including Kyiv, Lviv and Odessa).

The service is unique as it offers an affiliate programme, inviting individuals to create an account and seek referrals in order to win money. The service describes its programme as follows:

Our service is glad to give you the opportunity to earn money with us using an affiliate program, for this, you just need to register on our website, obtain your personalised affiliate link from your account, place it on your website, etc. The more exchanges that follow your link, the more you earn!

In Their Own Words: Coin Swap 4

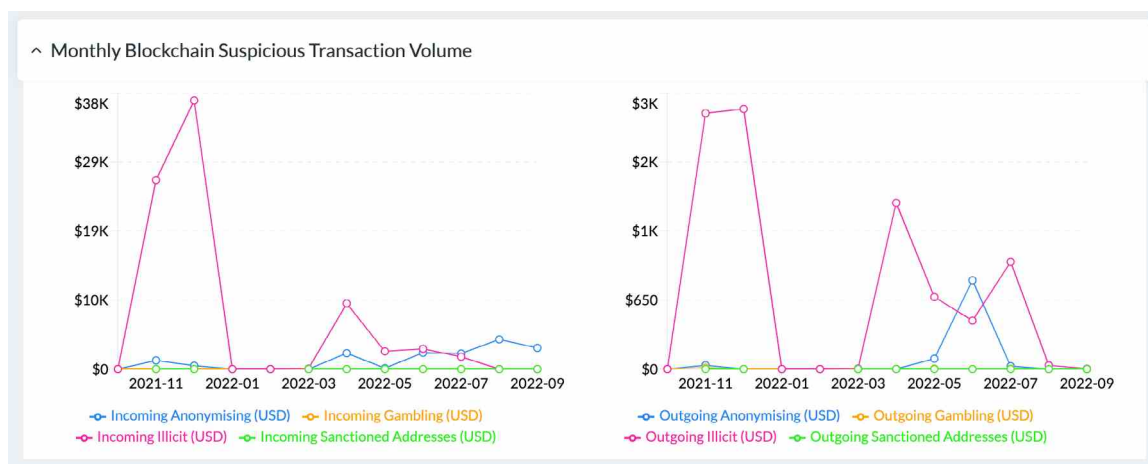


Conclusion

From dark web markets to stolen credit card vending, the underground cybercrime ecosystem is increasingly relying on coin swap services to cash-out their ill-gotten crypto. Equally concerning is the prospect that these services are dispersing illicitly-acquired Bitcoin across other blockchains, perhaps in preparation for investing in decentralized finance (DeFi) protocols or non-fungible tokens (NFTs).

The rise of dedicated cybercrime forums focusing solely on cashing out illicit funds emphasizes that virtual asset services and cybercrime investigators need to effectively manage and mitigate the risks associated with coin swap services. Elliptic provides the following tools to equip investigators with the necessary capabilities to assess and respond appropriately to coin swap-based risks:

- **Elliptic Lens** and **Navigator** allow investigators to screen wallets and transactions (respectively) that are associated with coin swap services or their clients. This can provide crucial information into the nature, scale, origin and destination of the cryptoassets that they process.
- **Elliptic Investigator** allows for transactions to and from coin swap services to be visualised on-chain, offering in-depth insights into transaction patterns, money laundering methods and links with other entities on the blockchain.
- Elliptic's **Holistic Screening** functionality allows investigators to screen coin swap services across all assets and blockchains on which they operate. This allows investigators to identify and manage risk without manually screening services or suspected wallets across individual assets or blockchains at a time, which would be otherwise required by legacy blockchain analytics solutions.
- Finally, **Elliptic Discovery** allows virtual asset services and investigators to conduct entity due diligence on coin swap services and USDT and sent to a number of exchanges including Huobi and OFAC sanctioned Guarantex. Holistic screening allows for the visualisation of these flows despite the cross-asset swaps that sought to obfuscate them:

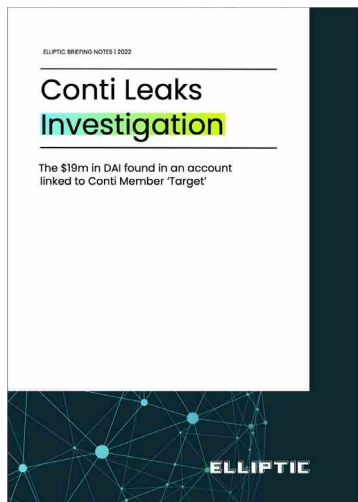


Other Reports by Elliptic



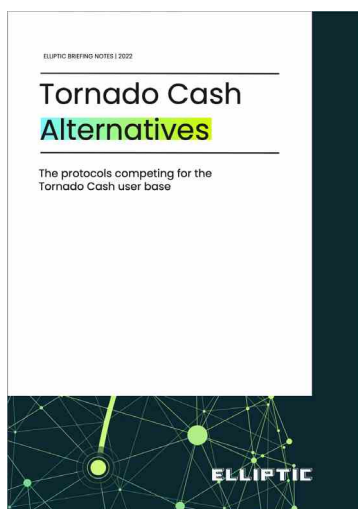
The State of Cross-chain Crime

Blockchains have become increasingly interconnected. New technologies such as decentralized exchanges (DEXs) and cross-chain bridges have removed many of the barriers to the free flow of capital between cryptoassets. However they are also being abused for money laundering by the likes of ransomware groups and hackers, who are moving billions of dollars in crypto between assets and blockchains.



Conti Investigation Briefing Note

Matching communications between high-ranking members of the Conti organisation and blockchain data analysed using Elliptic's Holistic Screening tools, Elliptic identified an account on the Ethereum blockchain that contains \$19m in DAI directly linked to high-ranking Conti member 'Target' and shares of various ransom payments made to Conti in Bitcoin between September 2020 and May 2021.



Tornado Cash Alternatives Briefing Note

On August 8th 2022, the US Treasury Department's Office of Foreign Assets Control (OFAC) sanctioned the popular Tornado Cash decentralized mixer. Processing over \$7 billion worth of cryptoassets throughout its operation, Tornado Cash was used by criminal entities – including North Korea's "Lazarus Group" state cyberhackers – to launder over \$1.54 billion of illicit cryptoassets.

This briefing note details Elliptic's analysis into six prominent alternative Ethereum-based obfuscation protocols that have been mentioned as potentially the next Tornado Cash.