Elliptic Connect

Dogecoin Gaining Traction for Illicit use

Dogecoin may have earned a significant market capitalization from its association with Elon Musk and the fluffy appeal of its Shiba Inu mascot, but that hasn't stopped it being targeted for use by illicit actors in the most serious types of crime.

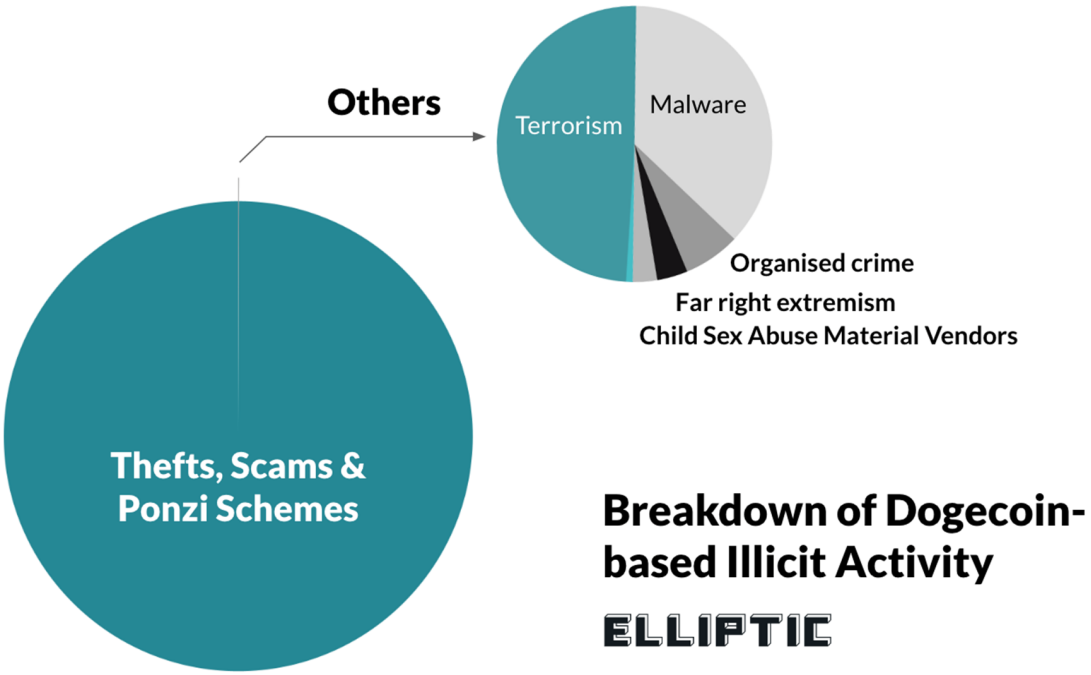
Known as the first of many "meme coins", Dogecoin was created in December 2013 and has since enjoyed a surge in popularity due to promotions from the celebrity circuit including Tesla CEO Elon Musk.

Despite its initial reputation as a joke, the asset has gained significant traction as a method of payment, including being used by the Ukrainian government to accept donations for its defense against the Russian invasion.

Currently, Dogecoin is among the top 10 largest cryptoassets by market capitalization – fast approaching $10 billion in market capitalization.

Dogecoin connected to Illicit Activity

Dogecoin's growing popularity means it has not escaped the notice of criminals. In addition to its use as a means of payment for legal goods and services, Elliptic has identified millions of dollars worth of Dogecoin transactions connected to illicit activity. While the vast majority of this activity consists of fraud, scams and ponzi schemes, it also includes the most serious types of crime, including terrorism financing and vendors of child sexual abuse material (CSAM).

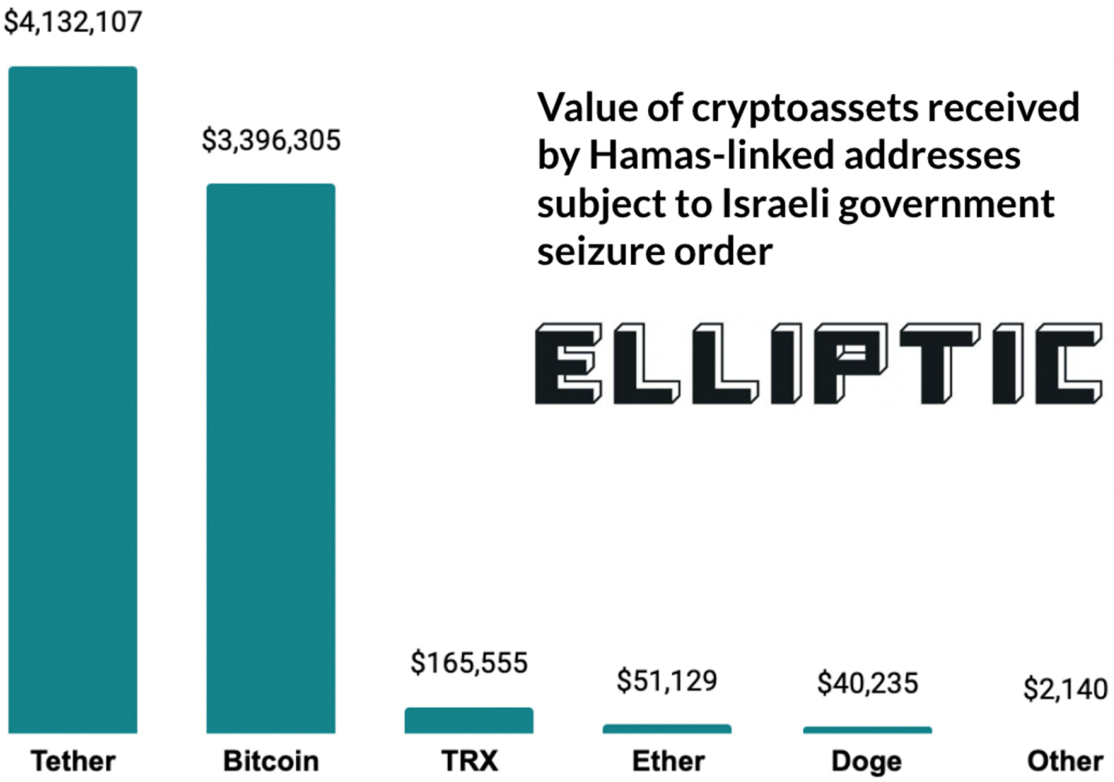


Breakdown of illicit use of Doge.

Terrorism Financing

In July 2021, Israel's National Bureau for Counter Terror Financing issued a seizure order against 84 cryptoasset addresses believed to be controlled by Hamas, or otherwise used in terror-related activity. This included Doge addresses, which had received a total of $40,235.

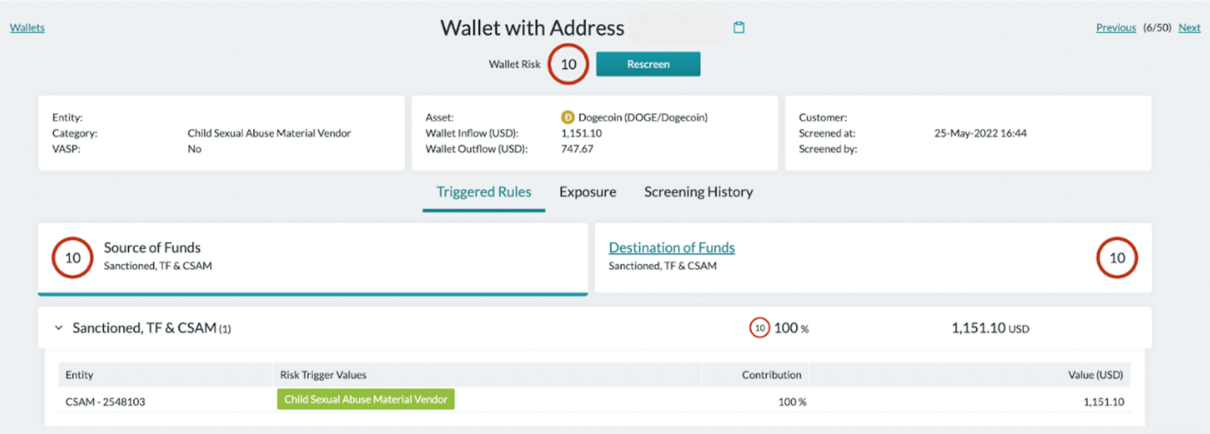
While a small sum compared to Bitcoin and Tether, this example demonstrates the awareness, and increasing adoption, of a wide variety of cryptoassets by groups such as Hamas. It also reinforces the importance of blockchain analytics solutions in a compliance toolkit to enable financial institutions and law enforcement agencies to screen for risk beyond just the most popular cryptoassets.



Child Sexual Abuse Material

In collaboration with industry partners, Elliptic monitors child sexual abuse material (CSAM) vendors operating on both the darknet and clearnet which accept cryptoassets as a method of payment. Again, while the majority of crypto payments to CSAM vendors are made using Bitcoin, a small and growing number of these vendors accept other crypto assets – including Dogecoin.

To be clear, the level of Dogecoin usage within the CSAM community is currently very low, with less than $3,000 in payments globally identified to date. However, the fact that the Dogecoin adoption trend has reached this community further demonstrates the appetite for criminal actors to adopt a wide range of cryptoassets in a bid to avoid notice, and highlights the growing challenge faced by legitimate market participants in mitigating risk across a rapidly growing range of assets.

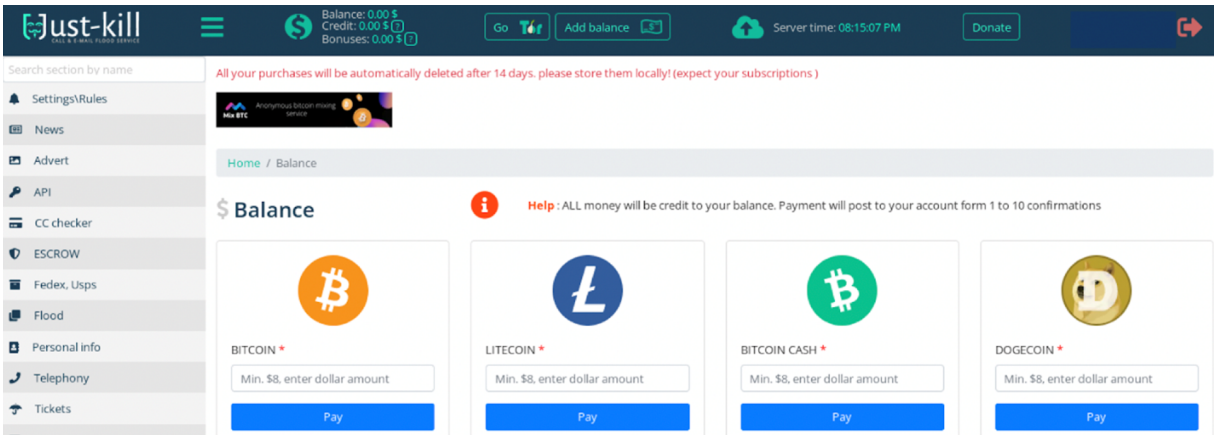


Wallet with Address

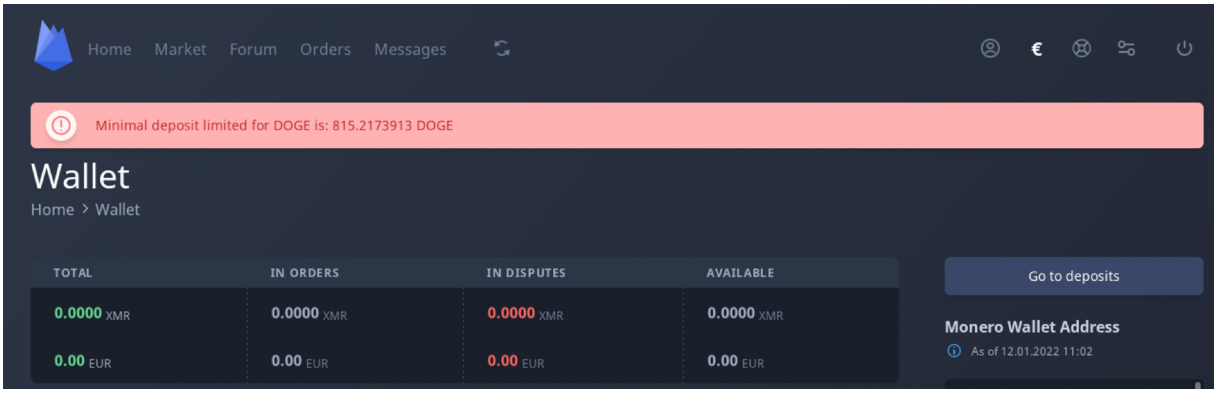
Darknet Markets

Elliptic has identified several darknet markets – including those that sell drugs and stolen data – which accept Dogecoin as a method of payment.

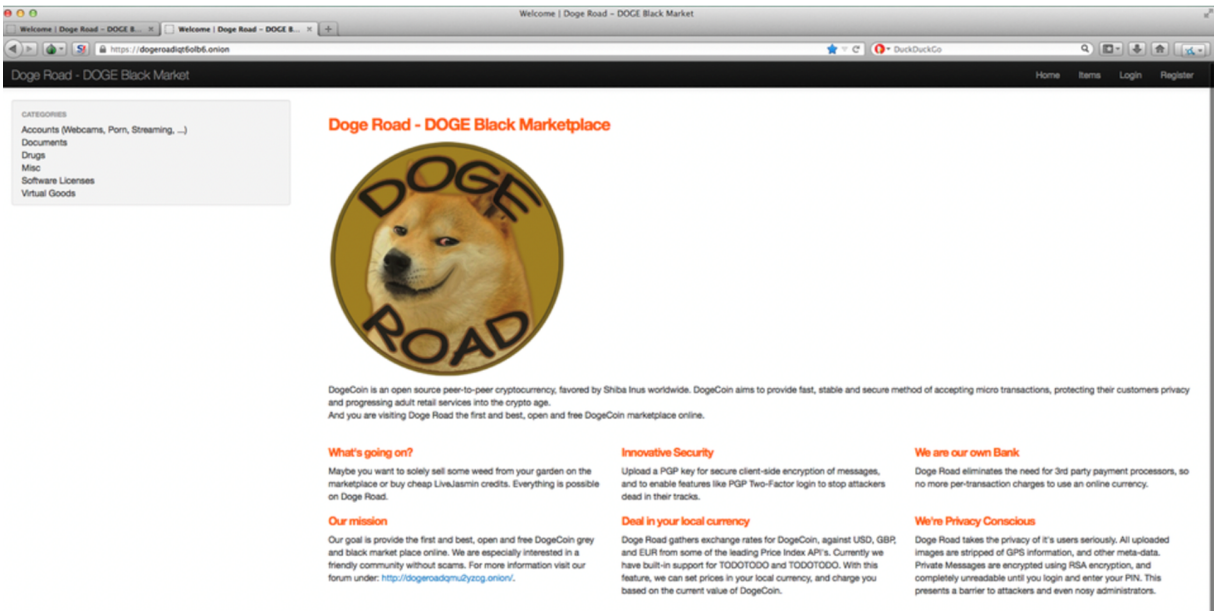
Just-Kill describes itself as a "call & email flood service", which also provides a credit card checker, allowing users to check the validity of purchased stolen credit cards. Just-Kill allows users to both deposit funds and donate to the site using a variety of cryptoassets – including Dogecoin.



DogeCoin is also accepted on some popular darknet drug markets. One, namely Archetyp, previously used a coin swap service to allow users to deposit funds in a range of other cryptoassets – including Doge. The market has since switched to only accepting Monero.



These services build on previous unsuccessful attempts to utilize Doge as a method of payment for illicit goods on darknet markets, including by the now-defunct Doge Road market, which was briefly active in 2014 before it performed an exit scam and the operators disappeared with customer funds.



Screenshot by u/chrono000 Reddit.
Screenshot by u/chrono000 Reddit.

Malware

Several malware campaigns have been identified which involve the theft of Dogecoin. In October 2020, Kaspersky identified a malware family called Cliptomaner which hijacks computers in order to maliciously mine cryptocurrencies. This malware also performs clipboard hijacking, in which crypto addresses copied to a user's clipboard are swapped for addresses controlled by the malware deployers.

Cliptomaner is able to hijack a variety of cryptoasset addresses – including Doge. To date, the Doge address used by Cliptomaner has received almost $29,000,

demonstrating the potential profitability of these campaigns – especially when considering a wide range of assets.

Malware campaigns have also been found to utilize Doge in more creative ways. In July 2020, researchers at Intezer identified a malware campaign dubbed "Doki" which utilized information contained within Doge transactions in order to identify command and control servers, allowing the malware to increase its resilience to law enforcement takedowns. This technique has since been utilized by additional malware campaigns – including the Glupteba botnet – which was the focus of an investigation by Google's Threat Analysis Group in December 2021.

Far-right Extremism

As noted in previous research by Elliptic, far-right extremist groups have increasingly exploited the internet to build followings and raise funds. When faced with exclusion from mainstream financial services, extremists have turned instead to cryptocurrencies.

Numerous news sites, blogs and video sharing platforms have all embraced cryptocurrency payments. Elliptic has identified several far-right entities which have utilized Dogecoin to raise funds such as Infowars. To date, the organization has raised over $1,700 in Doge alone.

Thefts, Scams and Ponzi Schemes

By far the most notable crime type affecting Doge was found to be thefts, scams and ponzi schemes. To date, Elliptic has identified over 50 thefts, frauds and ponzi schemes which have obtained hundreds of millions of dollars worth of Dogecoin.

Just days after Dogecoin launched, Dogewallet – a storage solution for Doge users – suffered a hack resulting in the loss of over $14,000 of users' funds. Additional notable examples include the Plus Token ponzi scheme, which resulted in the seizure of over $20 million in Doge by Chinese authorities, and an alleged theft of $119 million of Dogecoin connected to a Turkish ponzi scheme in 2021.

Expanding crypto coverage to ensure compliance

For retail investors and exchanges, transparency around Dogecoin ownership and its use has become increasingly important. Although it was originally developed as a joke memecoin, Dogecoin has dramatically increased in adoption and value amongst large businesses, including Elon Musk's SpaceX, creating a greater need to validate the coin's origins and payment counterparties.

Elliptic provides full compliance coverage capabilities for Dogecoin in its Elliptic Lens crypto wallet screening and Navigator transaction monitoring solutions, enabling customers to better identify illicit actors, fight financial crime, and achieve anti-money laundering/know-your-customer (AML/KYC) regulatory compliance, making the crypto market safer for all.