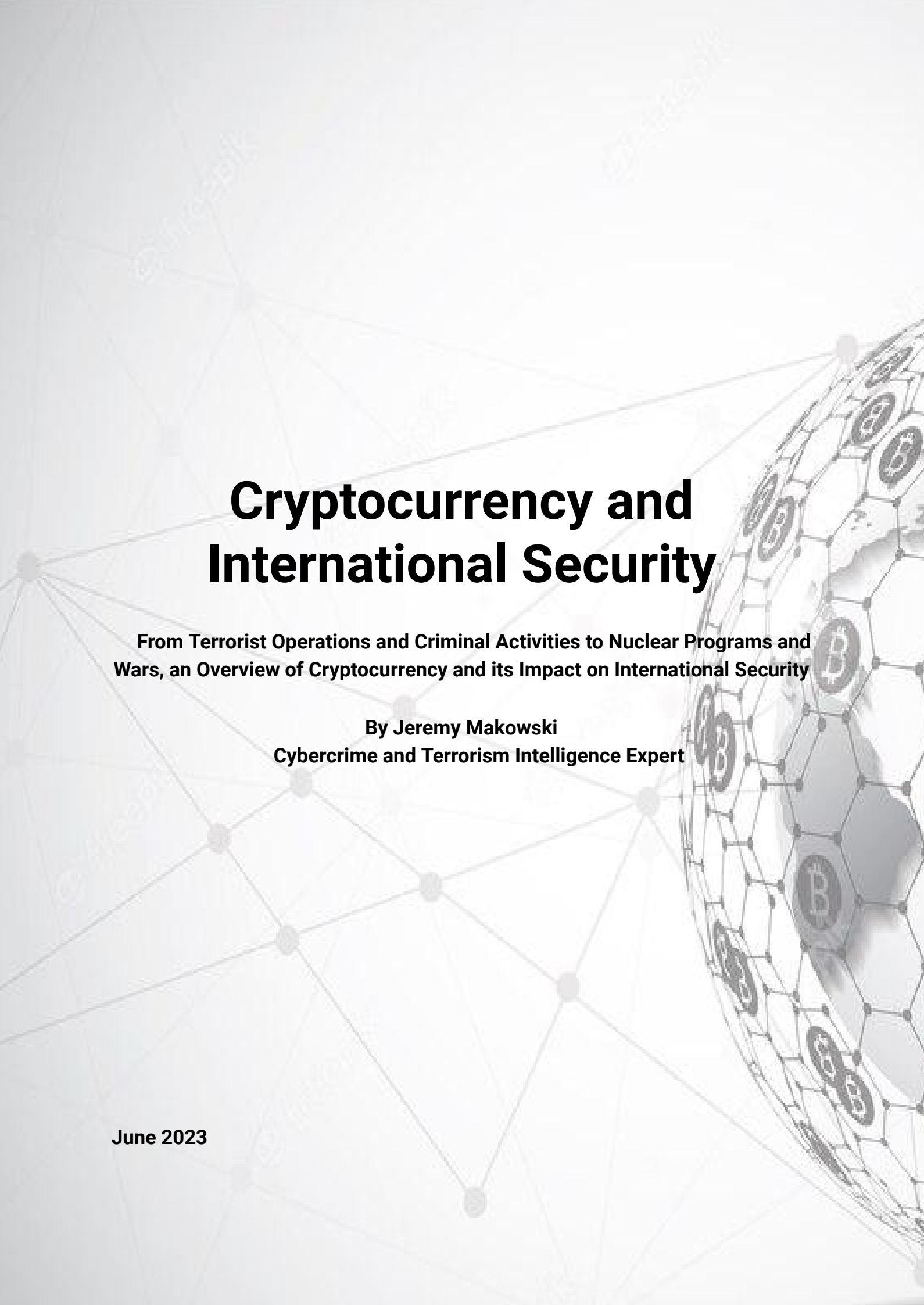
# Cryptocurrency and International Security

**From Terrorist Operations and Criminal Activities to Nuclear Programs and Wars, an Overview of Cryptocurrency and its Impact on International Security**

**By Jeremy Makowski**
**Cybercrime and Terrorism Intelligence Expert**



**June 2023**

# Table of Content


Executive Summary 3
1. Cryptocurrency: Concept and Operation 4
    1.1. What is Cryptocurrency? 4
    1.2. Blockchain and Cryptocurrency 5
    1.3. How to Trade Cryptocurrency? 8
2. Criminal Activities 13
    2.1. Traditional Crime 13
    2.2. Cybercrime 16
    2.3. Money Laundering 20
3. Terrorist Operations 21
4. War and Nuclear Program 24
    4.1. Nuclear Program 24
    4.2. War and International Sanctions 25
5. Cryptocurrency and Anonymity 28
    5.1. Mixing Services 29
6. Tracking Cryptocurrency on the Blockchain 30
7. Impact on States and International Security 34
About The Author 36
References 37
OSINT Resources for Cryptocurrencies Investigation 39

# Executive Summary

Since its creation in 2009, cryptocurrency has consistently developed and gained momentum on the international scene. Cryptocurrency transactions established themselves as plausible alternatives to the traditional financial system; however, the elusive nature of crypto payments has been widely leveraged to finance illegal activities. From crime to terrorism, through war and nuclear programs, cryptocurrency is used by many threat actors who have understood the benefit they can derive from its anonymous and secure nature. Cryptocurrencies allow threat actors greater leeway and reduce the risk of being identified, despite many technological advancements in the fight against the illegal use of cryptocurrencies. The real problem with cryptocurrency lies in a crucial lack of regulation and legislation at the state and international levels. Cryptocurrency can be used to avoid international sanctions imposed on a state because there is currently no consensus on the issue, despite some regulations, especially in the European Union. The problem might become even more widespread in the future if states and international organizations continue to neglect it.

# 1. Cryptocurrency: Concept and Operation

## 1.1. What is Cryptocurrency?

Cryptocurrency is a digital financial asset that does not rely on banks to authorize and verify financial transactions. Cryptocurrency is based on a peer-to-peer system that allows anyone to send and receive funds anywhere in the world. Unlike physical money in the real world, cryptocurrency payments exist only as digital entries in an online database describing specific transactions. When one transfers cryptocurrency funds, the transactions are recorded in a public ledger and usually stored in digital wallets. The concept of cryptocurrency is also based on the encryption of transactions. An encryption algorithm is involved in storing and transmitting cryptocurrency data between wallets and public ledgers. The purpose of encryption is to guarantee transaction security and anonymity.

Cryptocurrencies are a decentralized cash flow and payment exchange system that maintains ownership logs through a decentralized blockchain record (Figure 1). They were created to avoid the control of banks and states and to eliminate the fees associated with traditional financial transactions. However, like any newly implemented technology, this one was very quickly spotted by groups of cybercriminals or terrorists who saw cryptocurrencies as an excellent way to transfer funds anonymously and securely. Security is precisely what has made the reputation of cryptocurrencies.

While traditional currencies (Dollar. Euro, Pound, Yen...) operate on the principle of centralized exchanges, which record all transactions on a central server, cryptocurrencies operate in a so-called decentralized mode, allowing cryptocurrency users to have pseudo-anonymity and to carry out transactions without being easily identified. This pseudo-anonymity and the decentralization of these exchanges threaten international security. Criminal and terrorist organizations have constantly been searching for this pseudo-anonymity taking advantage of social networks and other encrypted chat applications to carry out their illegal activities.

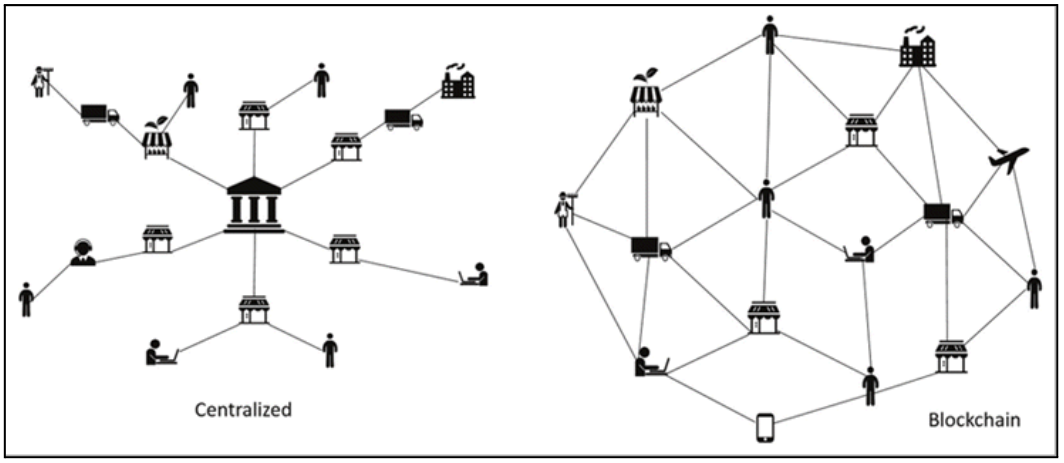



*Figure 1 - Topology of centralized and decentralized financial networks*

In January 2009, Satoshi Nakamoto, a pseudonym used by the person or persons who created Bitcoin, the first cryptocurrency available for public purchase. A few years after its creation, Bitcoin has gradually become popular and inspired many other cryptocurrencies that followed its course.

Apart from Bitcoin, there are many other cryptocurrencies. As of March 2023, there have been created about 23,000 types of cryptocurrencies. However, not all of them are active or valuable. Moreover, as of today, the most used cryptocurrencies in the world are:

- Bitcoin (BTC)
- Ethereum (ETH)
- Tether (USDT)
- Binance (BND)
- USD Coin (USDC)
- Ripple (XRP)

## 1.2. Blockchain and Cryptocurrency

A blockchain is a distributed database or ledger shared between nodes in a computer network. They are primarily (but not only) used in cryptocurrency systems to maintain a secure and decentralized record of transactions, but they are not limited to cryptocurrency uses. Blockchains can be used to make data immutable in any industry. Because there is no way to modify a block, the only trust needed is when a user or program inputs data. This aspect reduces the need for trusted third parties, usually auditors or others who add costs and can make mistakes. Cryptocurrencies and the blockchain technology that powers them make it possible to transfer value online without an intermediary, just like a traditional money transfer system. Almost all cryptocurrencies are secured using blockchain networks, which makes it possible to

verify the accuracy of transactions thanks to very high computing power. Blockchain can be categorized into four broad categories (Figure 2):

- ➢ Public Blockchain.
- ➢ Private Blockchain.
- ➢ Hybrid Blockchain.
- ➢ Consortium Blockchain.

**Public Blockchain**

This type of blockchain is utterly open to following the idea of decentralization. They have no restrictions, as anyone having a computer and an internet connection can be part of the network.

**Private Blockchain**

These blockchains are not as decentralized as the public blockchain; only selected nodes can participate in the process, which makes them more secure than others.

**Hybrid Blockchain**

This type of blockchain is a mix between a private and public blockchain, where an organization controls some part, and other marks are visible as a public blockchain.

**Consortium Blockchain**

This type of blockchain is a creative approach that addresses the organization's needs. This blockchain validates the transaction and also initiates or receives transactions.

| | **Public** (permissionless) | **Private** (permissioned) | **Hybrid** | **Consortium** |
|---|---|---|---|---|
| ADVANTAGES | + Independence<br>+ Transparency<br>+ Trust | + Access control<br>+ Performance | + Access control<br>+ Performance<br>+ Scalability | + Access control<br>+ Scalability<br>+ Security |
| DISADVANTAGES | – Performance<br>– Scalability<br>– Security | – Trust<br>– Auditability | – Transparency<br>– Upgrading | – Transparency |
| USE CASES | ■ Cryptocurrency<br>■ Document validation | ■ Supply chain<br>■ Asset ownership | ■ Medical records<br>■ Real estate | ■ Banking<br>■ Research<br>■ Supply chain |

*Figure 2 - Comparative table of different blockchains (Source: Techtarget)*

Cryptocurrencies like Bitcoin or Ethereum are based on public blockchain technology. This technology is a list of transactions anyone can view and verify. The Bitcoin blockchain contains a record of every transaction made. The list of transactions in the blockchain is one of the fundamental cryptography concepts for most cryptocurrencies, as it makes it possible to secure financial exchanges between two entities that do not know each other (Figure 3).

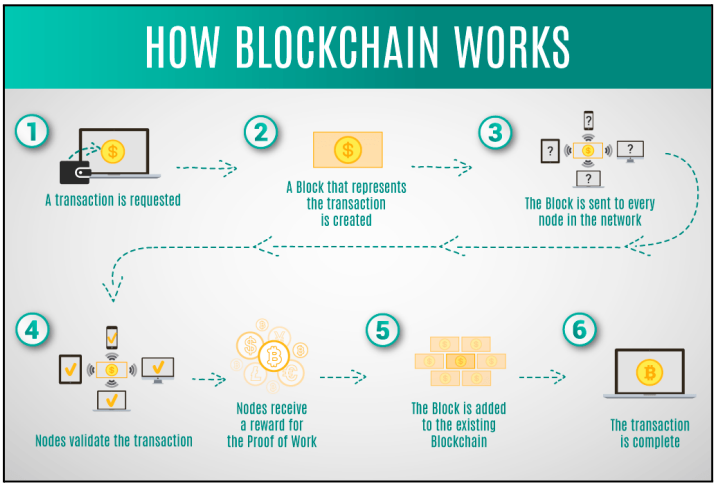



*Figure 3 - Blockchain operating mode*

A public blockchain network usually comprises several components, including nodes. There are three types of nodes: full, light, and minor. Full nodes store a copy of the blockchain ledger, while light nodes only store the data needed to verify transactions. The nodes communicate with each other via a peer-to-peer network, which allows them to exchange information and maintain consensus on the state of the Blockchain. Node operators can earn rewards for network participation through block rewards or transaction fees. The role played by node operators is vital in maintaining network security. They help prevent “double spending” by checking transactions and rejecting invalid ones. Operating a node requires technical knowledge and resources, such as computing power and storage space. However, there are tools that make it easier for users to configure and manage their own nodes. Blockchain nodes are essential to the blockchain network, as they help ensure network security and reliability (Figure 4).

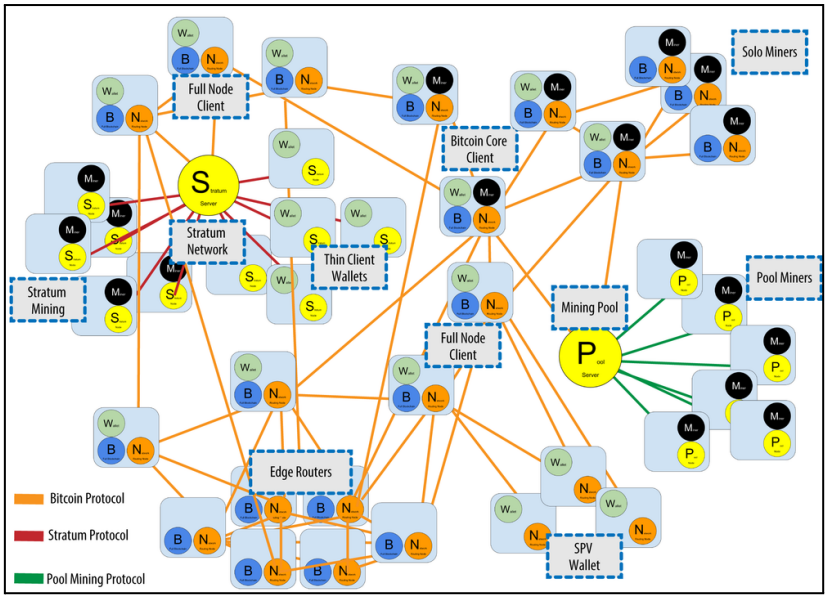



*Figure 4 - The Bitcoin network shows various node types, gateways, and protocols*

## 1.3. How to Trade Cryptocurrency?

Today, buying, selling, and trading cryptocurrencies is easy and accessible to most people worldwide. However, their possession and use are not subject to the same laws and regulations in all countries. The legal status of cryptocurrencies varies significantly from country to country. While in the vast majority of countries, the possession and use of cryptocurrency are not per se illegal, its status and usability as a form of payment (or commodity) vary, with different regulatory implications (Figure 5).

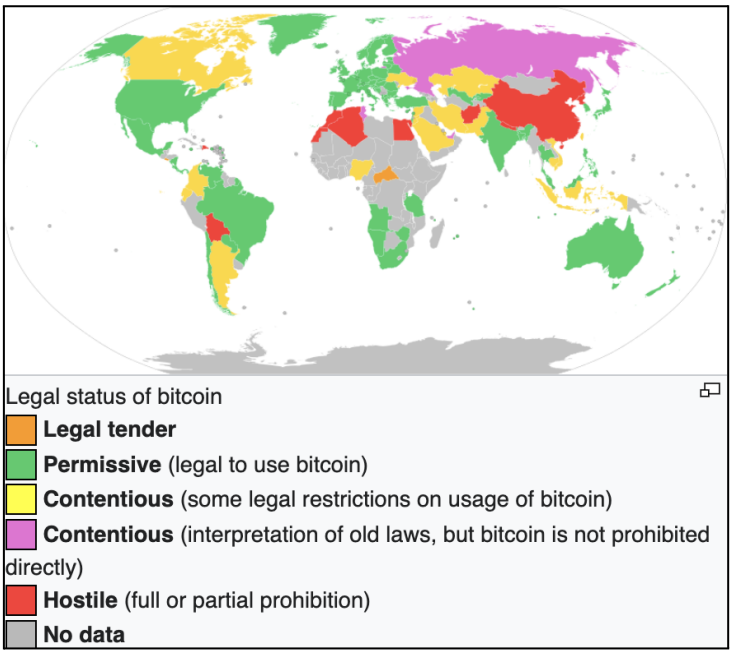



*Figure 5 - Legal status of Bitcoin Worldwide*

There are several ways to buy cryptocurrency; some are easier than others. Purchasing cryptocurrency is also subject to specific regulations. These regulations may or may not facilitate the acquisition and trade of cryptocurrencies. In general, these are the different ways to buy cryptocurrencies:

**Peer-to-peer exchange platforms**

These platforms are a network of worldwide sellers and buyers, allowing the purchase of cryptocurrencies by different financial means (cash, bank transfer, credit cards, etc.) (Figure 6). Their level of identification requirement depends on the country in which it is hosted and its compliance and anti-money laundering laws.

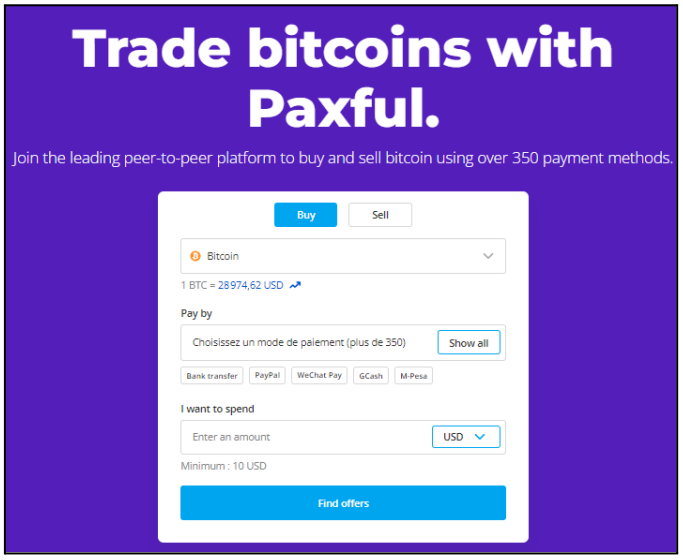



*Figure 6 - The Paxful peer-to-peer platform*

**Online trading Platform**

These exchange platforms (e.g., Coinbase, Kraken, Binance) allow users to create an online account and open a wallet to buy cryptocurrencies using different means of payment (e.g., credit cards, bank transfer, Apple Pay, Google Payer). These platforms usually require some form of identification when registering on them. As with peer-to-peer platforms, their level of identification requirement depends on the country in which it is hosted and the country's compliance and anti-money laundering laws (Figures 7, 8, and 9).

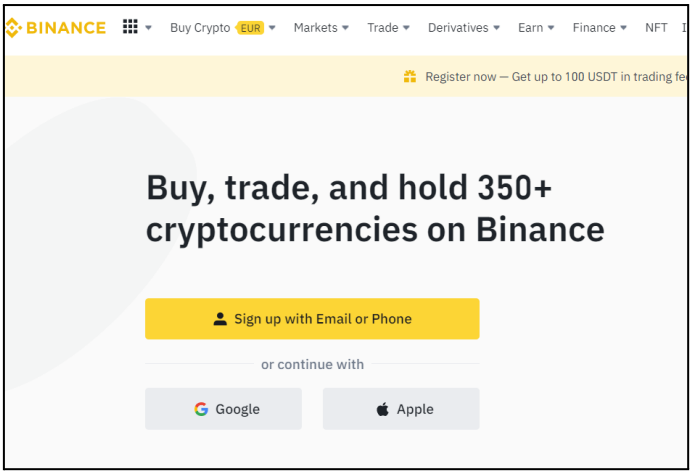



*Figure 7 - The Binance exchange platform*

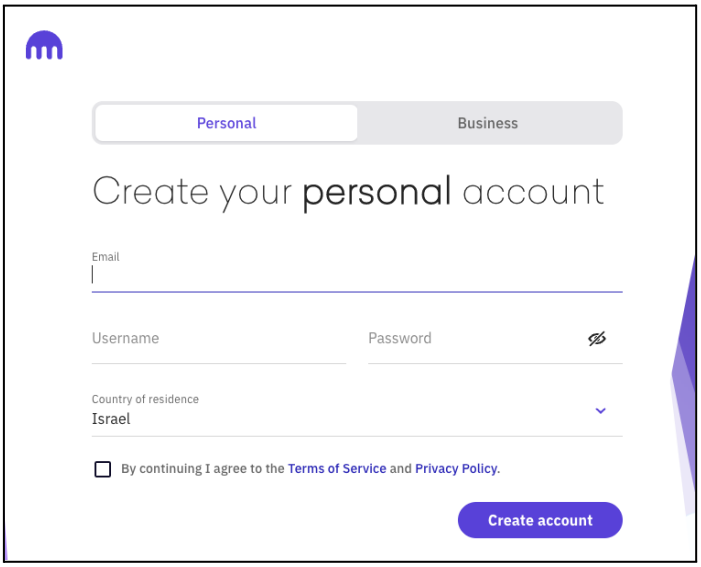



*Figure 8 - The Kraken exchange platform*

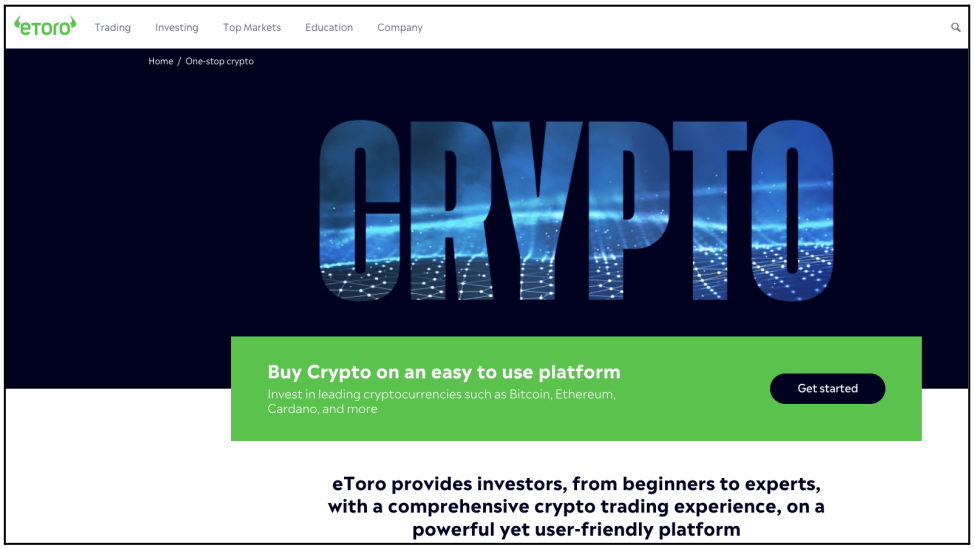



*Figure 9 - The etoro trading platform*

**Bitcoin ATM Machines**

Bitcoin ATMs allow people to buy bitcoins and other cryptocurrencies using cash or debit cards. Unlike traditional ATMs, Bitcoin ATMs allow customers to manage funds in their accounts. Bitcoin ATMs are simply tools through which one can make Bitcoin purchases. Unlike cryptocurrency exchanges, Bitcoin ATMs allow users to hold their own purchased Bitcoin by connecting the coins directly to a crypto wallet of their choice (Figure 10).




*Figure 10 - Examples of Cryptocurrency ATMs*

The regulation concerning the purchase of cryptocurrency in cash using an ATM mainly depends on the legislation in force in each country. Indeed, each country generally has a legal framework concerning the purchase of cryptocurrency in cash.

**United States**

In the United States, to be operational, Bitcoin ATM operators must register with the Financial Crimes Enforcement Network (FinCEN), the authority responsible for ensuring compliance with the banking secrecy law. Each Bitcoin ATM operator implements a set of Know Your Customer (KYC) procedures to ensure compliance, as well as independent audits and a dedicated compliance officer. The maximum amount of a transaction is generally around $3,000 every 24 hours. Different reporting requirements depend on the total amount and purchase method.

**United Kingdom**

In the United Kingdom, the legislation concerning cryptocurrency ATMs is stringent. In 2019 the UK government made a policy statement through the Financial Conduct Authority (FCA) regarding online crypto businesses and Bitcoin ATMs. All crypto transactions over £150 require KYC verification.

### European Countries

In most European countries, the daily transaction limits for Bitcoin ATMs are between €2,000 - €3,000. However, this limit depends on the country and the Bitcoin ATM operator. You will not have to submit KYC requirements in most countries if the amount is below €150. Bitcoin ATM operators must be registered and licensed by the appropriate local authorities. In many European countries, there is still a lack of a clear legal framework regarding cryptocurrency. Some countries define it as a currency, while others as a commodity.

### Asian Countries

Independent sellers generally operate on less mainstream channels than exchange or peer-to-peer platforms, such as encrypted chat applications like Telegram. There are many channels, with dealers generally offering cryptocurrencies, such as Bitcoin and Ethereum. These cryptocurrency dealers are not concerned about the buyer's identity because they usually deal with money from illegal activities.

## Independent Sellers

Independent sellers are arguably the most anonymous way to source cryptocurrencies. Most of these sellers operate on less mainstream channels than traditional platforms. On the Telegram application, there are many channels where dozens of cryptocurrency sellers offer Bitcoin for sale. Ethereum or Tether. These sellers do not require identification; transactions are generally carried out locally and in cash (Figure 11).

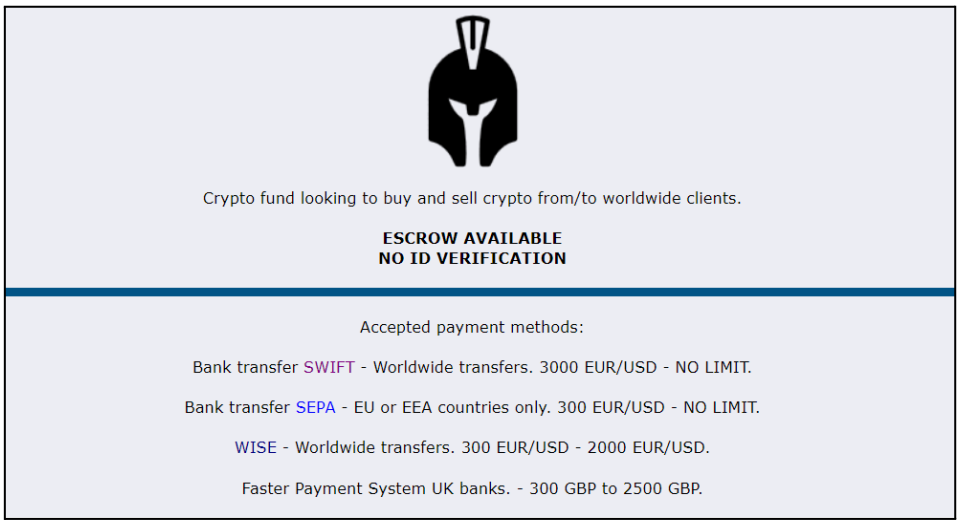



*Figure 11 - Independent worldwide crypto service with no ID verification*

While many people use cryptocurrency in a legal framework for investing, trading, and exchanging consumer goods, it is nevertheless widely used by multiple threat actors for the following purposes:

- ➢ Money laundering
- ➢ Fraud
- ➢ Drug, arms, and human trafficking
- ➢ Exploitation of children
- ➢ Darknet market trading
- ➢ Cybercrime
- ➢ Terrorism funding
- ➢ Nuclear program and war funding

Cryptocurrency has thus become one of the preferred means of threat actors for financing illegal activities and such due to its complexity. This document explains why cryptocurrency is so popular with these threat actors and its impact on security.

# 2. Criminal Activities

## 2.1. Traditional Crime

As cryptocurrencies have grown in popularity over the past decade, their use for criminal purposes has increased dramatically, making the work of law enforcement and intelligence agencies more complex. For several years now, cryptocurrencies have posed a new security issue. How can states prevent the financing of international criminal and terrorist activities when the transactions are difficult to trace, if not impossible?

The use of cryptocurrency in classic criminal activities and cybercrime is a significant means of payment for the sale and purchase of illegal physical and digital assets online. Consider that the dark web has greatly contributed to democratizing online trading. Cryptocurrencies have been the tipping point making this trading harder to identify and track (Figures 12, 13, and 14). While on some dark web sites or applications like Telegram, the prices displayed are in dollars, the means of payment remain in cryptocurrency, mainly in Bitcoin. Trading illicit goods using cryptocurrency generates significant fluctuating profits depending on the intensity of law enforcement activity against it (Figure 15).

Criminals are constantly looking for new ways to avoid law enforcement and cover up their illegal activities, so they have become more sophisticated in using cryptocurrencies. However, according to a report published by the European Law

Enforcement Agency, Europol, the extent and share of the illicit use of cryptocurrencies in criminal activities is difficult to estimate. Criminals involved in organized crime also continue to rely significantly on fiat currencies and traditional transactions, in addition to new value transfer opportunities. Furthermore, Europol underlines that if the use of cryptocurrency in the context of criminal activities increases, it would appear that the total number and value of cryptocurrency transactions related to criminal activities still represent only a small share compared to cash and other forms of transactions.

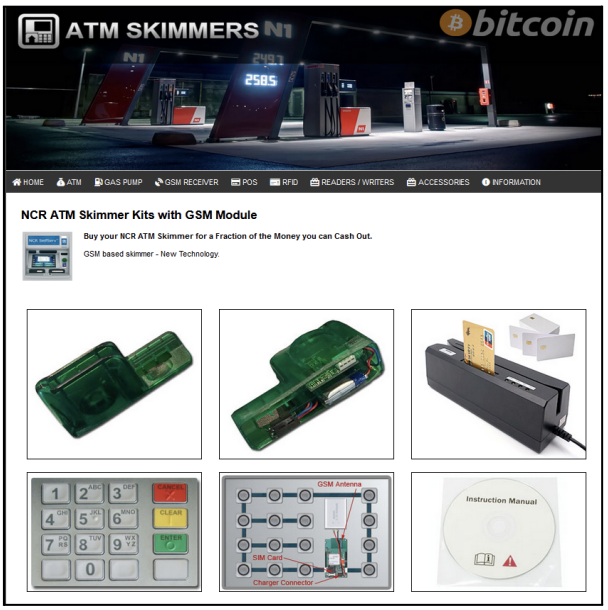



*Figure 12 - A dark web market selling ATM Skimmers*

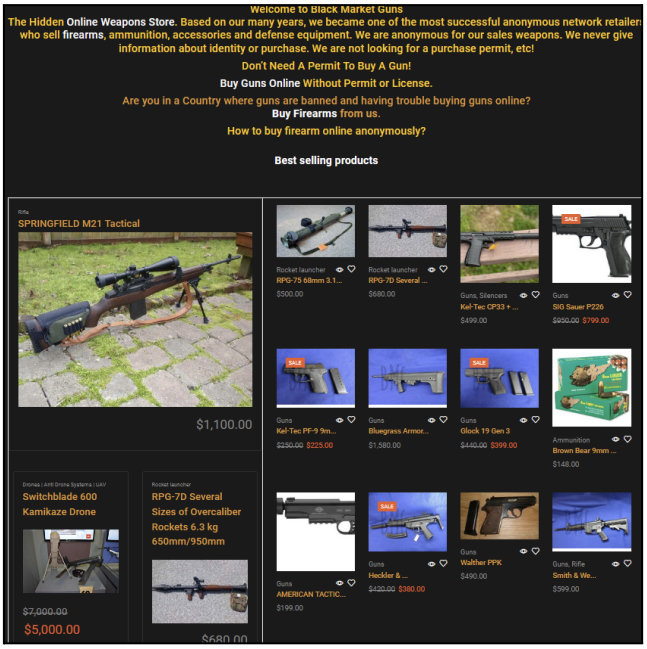



*Figure 13 - A dark web market selling weapons*

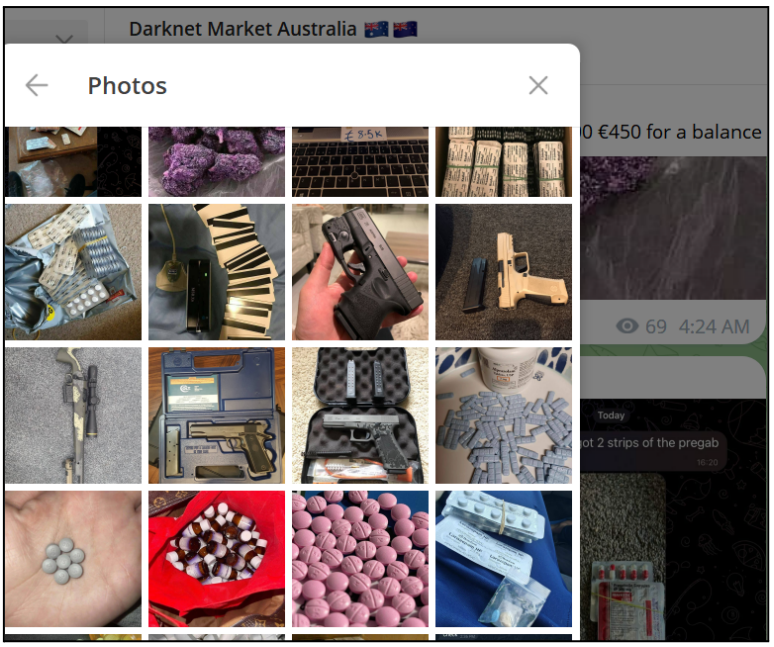



*Figure 14 - Illegal Items for Sale on a Telegram darknet market*

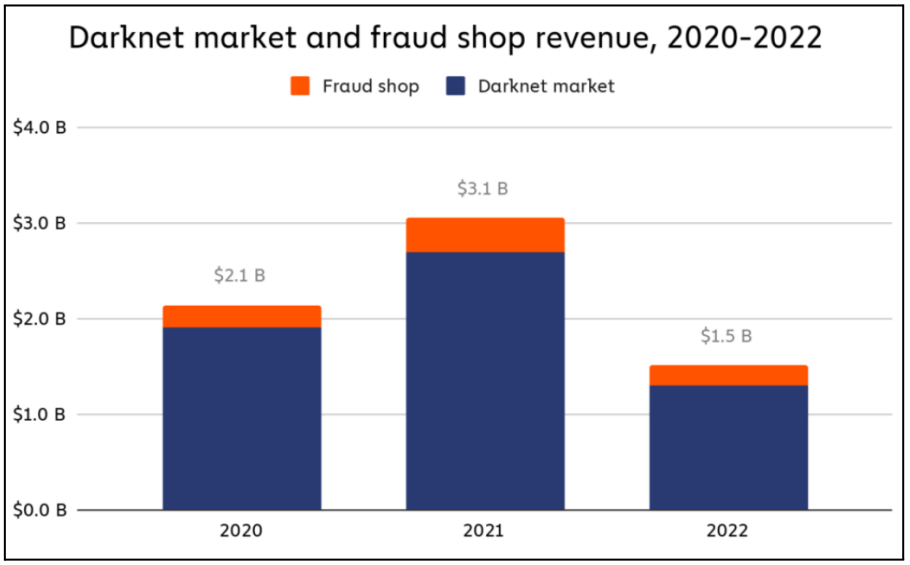



*Figure 15 - Darknet market and fraud shop revenue 2020-2022 (Source: Chainalysis)*

Today, the most popular cryptocurrencies cybercriminals use are the following:

**Bitcoin:** As the first and best-known cryptocurrency, Bitcoin remains the most popular currency among cybercriminals today as it has the highest level of liquidity and is the most widely accepted payment method on the dark web market. Although Bitcoin transactions are recorded on the blockchain, allowing law enforcement to track transactions, it is still much more complex than tracking traditional forms of currency.

**Ethereum:** Ethereum is another cryptocurrency that offers some level of privacy. Even if Ethereum transactions are trackable, they are not as easy as the Bitcoin ones and remain a popular choice among cybercriminals.

**Monero:** Due to its built-in privacy features, Monero is a popular cryptocurrency among cybercriminals. Monero transactions are designed to be private, making it much harder for law enforcement to trace transactions. Additionally, Monero uses a technique called ring signatures, which makes it difficult to determine the identity of the entity behind a transaction.

## 2.2. Cybercrime

In the world of cybercrime, there are four main types of cyberattacks based on the use of cryptocurrencies such as Bitcoin, Ethereum, and Monero:

- ➢ Ransomware
- ➢ DDoS Extortion
- ➢ Cryptojacking
- ➢ Cryptocurrency Theft

**Ransomware** is a type of malware that encrypts files to extort victims into paying a ransom (usually using cryptocurrency like Bitcoin). The price of the ransom is usually based on the annual revenue of the targeted company and can increase if the payment deadline fixed by the threat actor has passed. A common type of ransomware operation called “double extortion” involves threat actors threatening the victim to expose the stolen files publicly if the ransom is not paid (Figure 16). Receiving payments in cryptocurrency allows cybercriminals to maintain anonymity and not be traced.

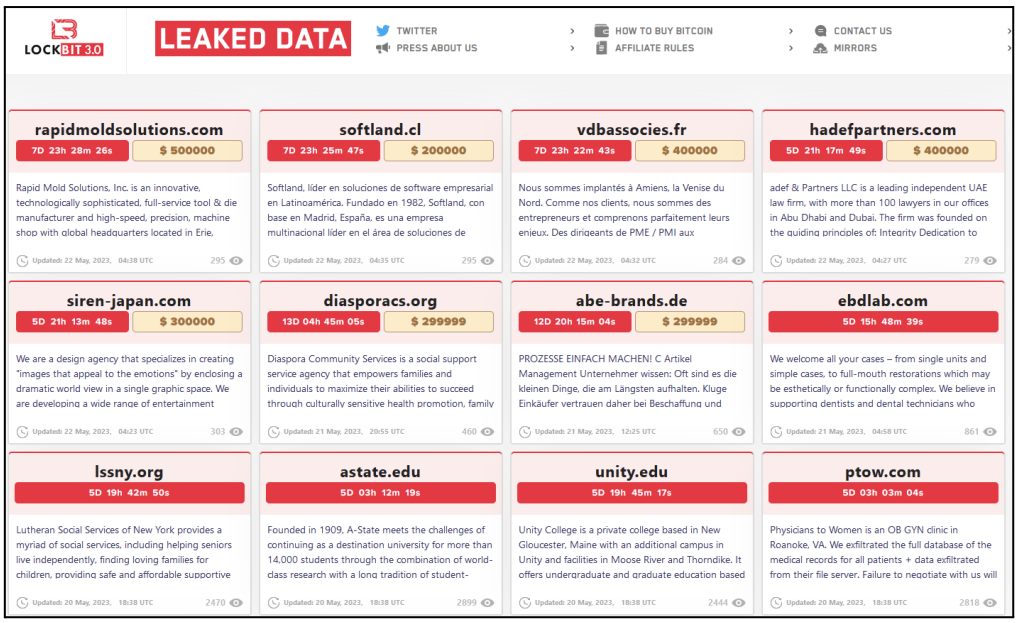



*Figure 16 - The LockBit ransomware group double extortion website*

**DDoS Extortion** is a technique similar to ransomware, except that threat actors launch a sustained distributed denial-of-service (DDoS) attack instead of gaining access to internal files and encrypting them until a cryptocurrency ransom is paid. Some threat actors send a letter to the victim, threatening to be targeted if they do not pay (Figure 17).

Subject: DDoS Attack

We are the Lazarus Group and we have chosen [redacted] as target for our next DDoS attack.

Please perform a google search for " Lazarus Group" to have a look at some of our previous work. Also, perform a search for "[redacted]" or "[redacted]" in the news. You don't want to be like them, do you?

Your whole network will be subject to a DDoS attack starting [redacted] next week. (This is not a hoax, and to prove it right now we will start a small attack on a few of your IPs from AS[redacted] block that will last for about 60 minutes. It will not be heavy attack, and will not cause you any damage, so don't worry at this moment.) There's no counter measure to this, because we will be attacking your IPs directly and our attacks are extremely powerful (peak over 2 Tbps)

This means that your websites and other connected services will be unavailable for everyone. Please also note that this will severely damage your reputation among your customers who use online services.

Worst of all for you, you will lose Internet access in your offices too!

We will refrain from attacking your network for a small fee. The current fee is 20 Bitcoin (BTC). It's a small price for what will happen when your whole network goes down. Is it worth it? You decide!

We are giving you time to buy Bitcoin if you don't have it already. And hopefully for this message to reach somebody who can handle it properly.

If you don't pay the attack will start and fee to stop will increase to 30 BTC and will increase by 10 Bitcoin for each day after the deadline that passed without payment.

Please send Bitcoin to the following Bitcoin address: [redacted]

Once you have paid we will automatically get informed that it was your payment.
Please note that you have to make payment before the deadline or the attack WILL start!

If you decide not to pay, we will start the attack on the indicated date and uphold it until you do. We will completely destroy your reputation and make sure your services will remain offline until you pay.

Do not reply to this email, don't try to reason or negotiate, we will not read any replies.

Once you have paid we won't start the attack and you will never hear from us again.

Please note we will respect your privacy and reputation, so no one will find out that you have complied.

*Figure 17 - A sample of a DDoS ransom letter (Source: Radware)*

**Cryptojacking** is the illegal use of people's computers' power to mine cryptocurrency. This type of attack is done with the help of malware that uses the CPU resources for that purpose. Unlike other cybercriminals, crypto hackers do not directly steal money or threaten victims but rather steal computer resources. This results in higher energy costs, lower performance for users, and an accelerated drop in battery performance (Figure 18).

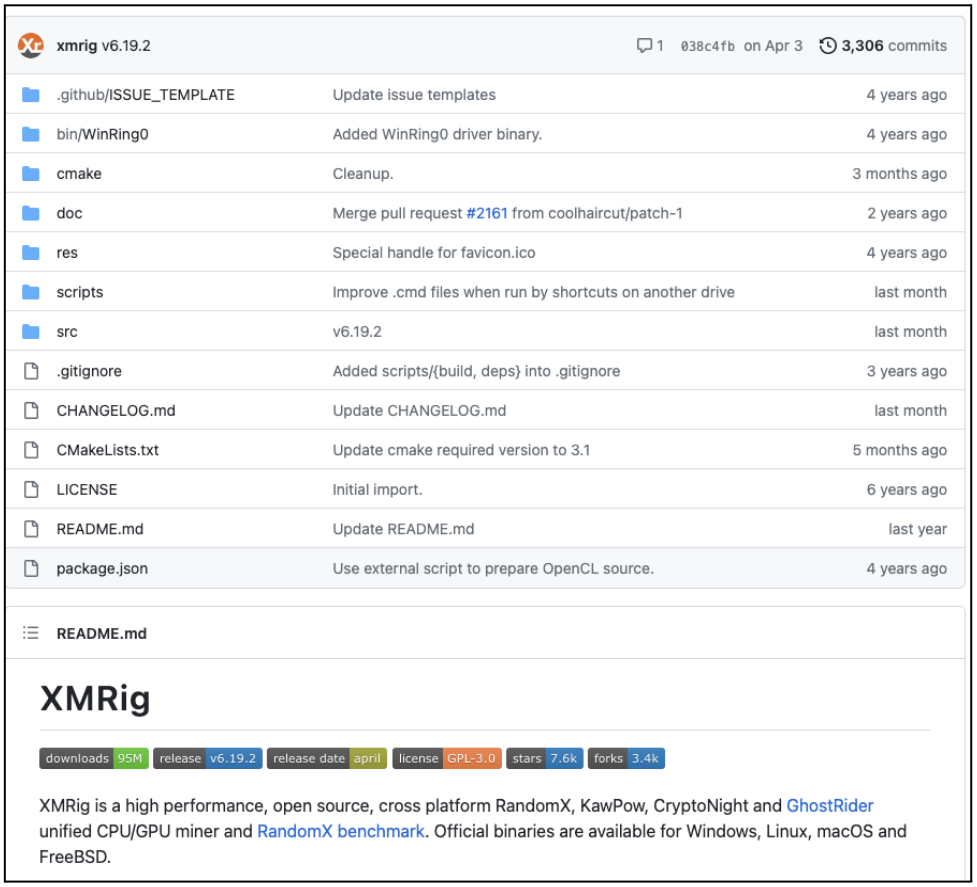



*Figure 18 - The XMRig crypto mining malware*

**Cryptocurrency Theft** is stealing money directly from their rightful owners. This type of attack is usually carried out using malware called Stealer (Figure 19) which can work in two different ways. The first is based on an address modification mode.; the malware detects when the victim performs a cryptocurrency transaction and replaces the recipient's address with the hacker's address without the victim's knowledge. The second way is to collect the connection logins to the victim's wallet to access and transfer the money.




*Figure 19 - A stealer with cryptocurrencies features for sale*

Beyond cyberattacks carried out by cybercriminals for profit, other threat actors, such as the Anonymous Sudan hacktivist group, are launching financial support campaigns using cryptocurrencies to fund their cyber operations (Figure 20).




*Figure 20 - Anonymous Sudan message on Telegram for financially supporting their cyber operations with cryptocurrencies*

## 2.3. Money Laundering

Money laundering is the process of illegally acquiring money and hiding it to give the impression that it was generated from legitimate sources. Money laundering usually comes from activities such as drug and sex trafficking, terrorist activities, and other illicit means. In a traditional money laundering system, we can distinguish different stages to conceal money acquired illegally. The following steps are usually part of the money laundering process:

**Investment:** Money is brought into the financial system by dividing it into different deposits and investments.
**Layering:** The money is mixed together to create distance between it and the perpetrators.
**Integration:** The money is returned to the owners as legitimate income or own money.

Since the emergence of cryptocurrencies, hackers, criminals, and terrorists quickly realized that these virtual currencies would facilitate money laundering despite specific state regulations set over the years. Owning, exchanging, and investing cryptocurrencies can be helpful for threat actors who do not lack the imagination to transform dirty money into proper and legal funds. Money launderers can convert their cryptocurrencies into private coins to conceal their operations since digital assets like Monero and ZCash are harder to track. While many exchanges and governments prohibit using private coins, money launderers can always find ways to transfer these tokens and hide their funds. Based on the data analyzed by the blockchain compliance company Chainalysis, between 2017 and 2021, cryptocurrency laundering has experienced variation from one year to another, increasing since 2019 (Figure 21).[1]

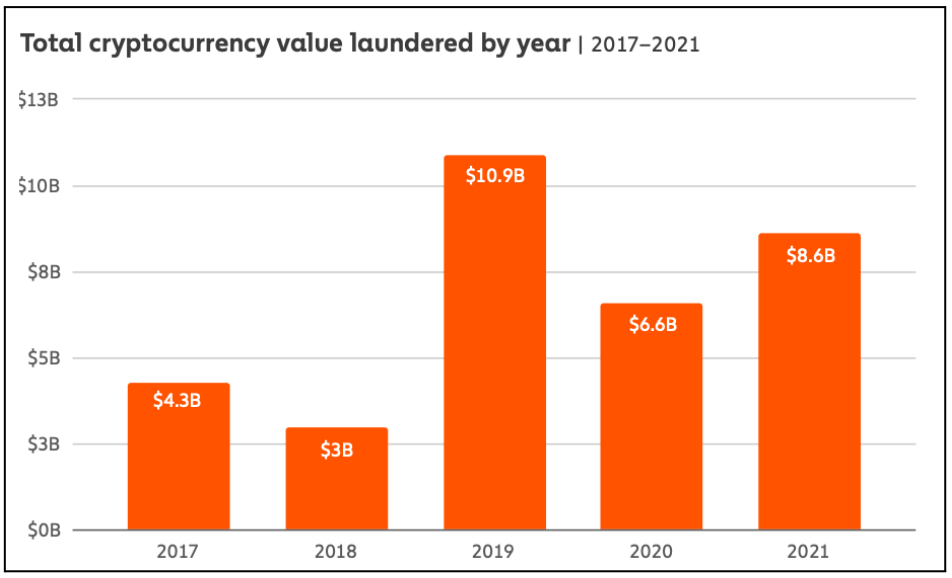



*Figure 21 - Cryptocurrency value laundered by year between 2017-2021 (Source: Chainalysis)*

[1] https://blockbr.com.br/wp-content/uploads/2022/06/2022-crypto-crime-report.pdf

Money launderers have been increasingly using Initial Coin Offerings (ICOs), a popular fundraising method used primarily by start-ups wishing to offer products and services. Some ICOs have generated massive returns for investors. However, other ICOs have become frauds or were financed using illegal funds. Unlike investments with traditional funds, it is more complicated or almost impossible for start-up creators to verify the source of their investor's cryptocurrency funds. In addition, some founders open the capital to anyone who wants to invest in their project, which makes things even easier for money launderers (Figure 22).

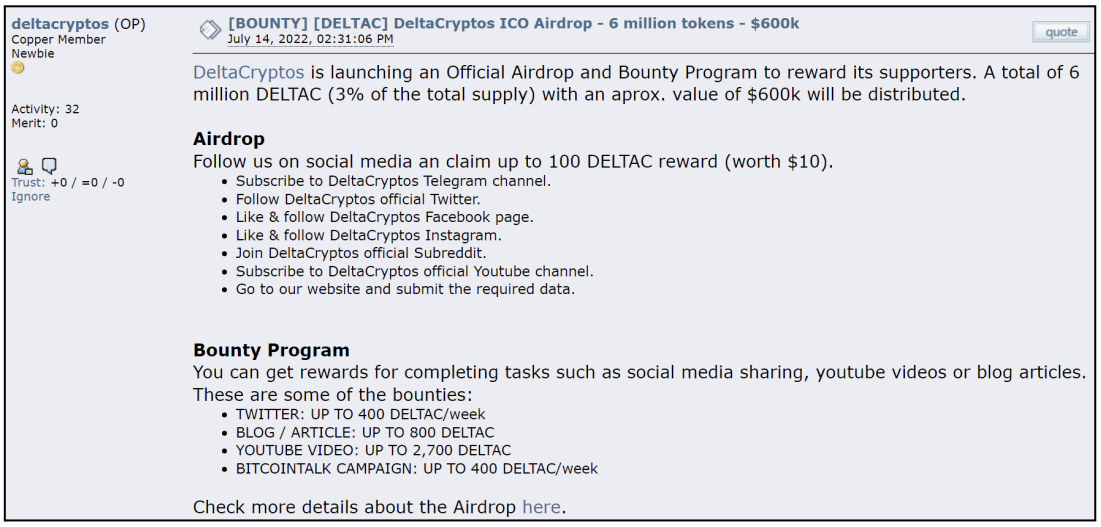



*Figure 22 - Example of an ICO project initiated in 2022 on a cryptocurrency forum*

## 3. Terrorist Operations

Decades ago, terrorist financing relied on traditional methods until terrorist groups started using cryptocurrencies to send and receive funds anonymously and securely. The same anonymity that is good for committing a crime can also be good for funding terrorist organizations. Most of the funders of terrorist activities are blacklisted by banks, which makes digital currency a very attractive alternative. While hackers have quickly embraced the crypto movement, terrorists are slower to use this venue for illicit purposes since, in many cases, terrorists, especially jihadists, operate in areas that do not allow them to use cryptocurrencies. However, several jihadist fundraising campaigns were previously identified on social networks. For example, until April 2023, Hamas and its affiliates had an active Bitcoin fundraising campaign on their website.



They allowed their supporters to donate anonymously and securely via a unique Bitcoin address that was automatically generated for each donor. Once received, the funds were often transferred from wallet to wallet to conceal the source and path of payment. The funds were then withdrawn using mediators with money (money mules). For those who preferred to make a more traditional donation, Hamas also provided an email address for making more direct contact (Figures 23 and 24). Recently, Hamas has decided to stop receiving fundraising via Bitcoin; however, Hamas' armed wing, the Izz el-Deen al-Qassam Brigades, renewed its call for continued dedication to Qassam and resistance by all means.

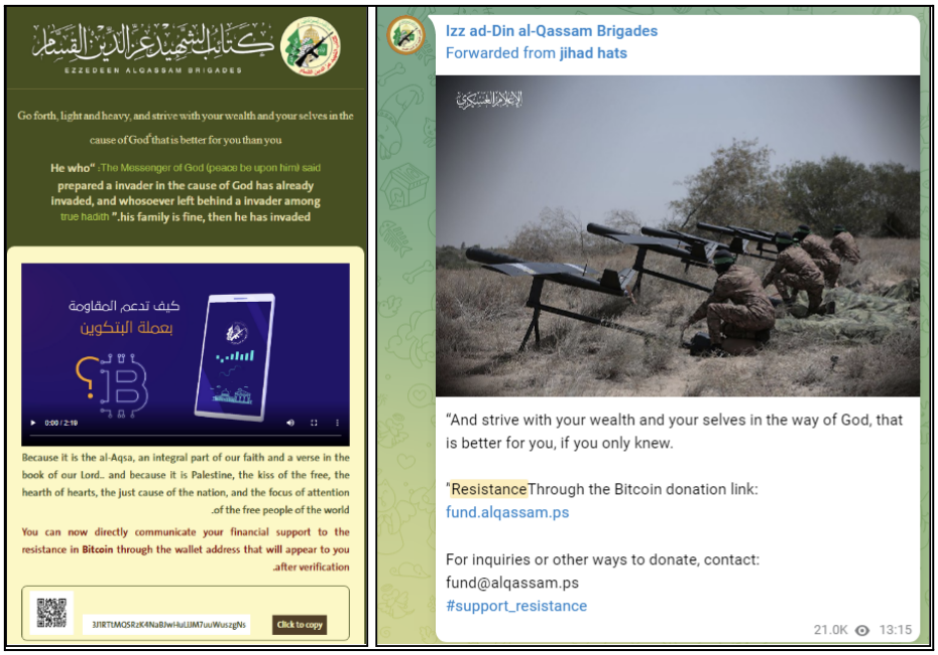



*Figure 23 - Messages on the Hamas website and Telegram for people who want to financially support them by sending Bitcoin or contacting them by email*




*Figure 24 - A post from the Jerusalem Electronic Army on Telegram with a Bitcoin address for donations (Source: Telegram)*

In May 2023, Israel's National Counterterrorism Funding Board (NBCTF) announced that it had seized around 190 cryptocurrency accounts on the Binance exchange due to alleged ties to Hamas. According to a Reuters report based on documents released by the country, Israel also claimed that two of the accounts belonged to the extremist group ISIS.

Hamas is far from being the only terrorist organization to use Bitcoin as a means of financing operations. A New York woman has been accused of providing financial support ($5000) using cryptocurrency to terrorist groups in Syria (Figure 25). This lawsuit appears to be one of the few involving virtual currency to finance terrorism in the United States. The 11-count indictment charged the 43-year-old American woman, Bakhrom Talipov, with supporting an act of terrorism, money laundering, and other crimes. Apart from the American government and Israel, this mode of financing terrorism is taken very seriously by the authorities of other countries, which often leads to convictions.

In 2022, France sentenced two men to prison for sending $280,000 worth of cryptocurrency to jihadists in Syria. Two years earlier, in September 2020, French authorities had arrested 29 people linked to the complex financing of Islamic extremists in Syria using cryptocurrencies.

In February 2023, a 31-year-old Uzbek and a 29-year-old Kazakh were arrested for sending cryptocurrency to Katibat al Tawhid wal Jihad, a Syrian anti-government terrorist group affiliated with Al-Qaeda.



NEWS • PRESS RELEASES

D.A. Bragg, NYPD Commissioner Sewell Announce Indictment of Upper East Side Woman for Using Cryptocurrency to Fund Syrian-Based Terrorist Groups; Launder Supporters' Contributions

JANUARY 31, 2023

Manhattan District Attorney Alvin L. Bragg, Jr., and New York City Police Commissioner Keechant L. Sewell today announced the indictment of VICTORIA JACOBS a/k/a BAKHROM TALIPOV, 43, for using cryptocurrency to provide financial support to violent terrorist groups operating in Syria. JACOBS is charged in a New York State Supreme Court indictment with Soliciting or Providing Support for an Act of Terrorism in the First Degree, as a Crime of Terrorism; Money Laundering; and other charges.[1]

The indictment follows a year-and-a-half-long investigation by the NYPD Intelligence Bureau and the Manhattan District Attorney's Office's Counter Terrorism Program, which was created in June 2015 to identify and pursue investigative leads related to homegrown terror plots, extremist activities, and terror-financing.

"This case marks the first time that terrorism financing is being prosecuted in New York State Court and is one of the rare cases worldwide where cryptocurrency is alleged to have financed terrorism," said District Attorney Bragg. "This complex case demonstrates the depth of knowledge and resources this Office has to combat terrorism and extremism in New York and throughout the globe. I thank our partners at the NYPD for their continued partnership to root out terror threats in any form they take."

"International terrorism remains a grave threat to safety and freedom around the world," said NYPD Commissioner Sewell. "Our department remains vigilant, and this indictment reinforces the NYPD's unwavering commitment to bringing terrorists and all those who support them to justice. I want to thank the Manhattan District Attorney's Office, our NYPD investigators, and everyone else who worked on this critical, wide-ranging case."

According to the indictment and other documents filed in court, from September 2018 through June 2019, JACOBS provided material support to Hay'at Tahrir al-Sham, a U.S. State Department-designated foreign terrorist organization, while living in New York City. JACOBS allegedly provided more than $5,000 to the terrorist training group "Malhama Tactical," which fought with and provided special tactical and military training to Hay'at Tahrir al-Sham.

JACOBS also allegedly laundered $10,661 on behalf of Mahalma Tactical by receiving cryptocurrency and Western Union and MoneyGram wires from supporters around the globe and sending the funds to Bitcoin wallets controlled by Mahalma Tactical. In addition to sending cryptocurrency, she also purchased Google Play gift cards for the organization.

In December 2019, JACOBS provided a comprehensive U.S. Army Improvised Munitions Handbook to an online group – which she believed was associated with both Hay'at Tahrir al-Sham and al-Qaeda affiliated Jihadist group Hurras al-Din – to facilitate their bomb-making efforts in Syria.

In August 2021, JACOBS purchased military-style combat knives, metal knuckles, and throwing-stars, posting in online forums that she was a "brother" who was "behind enemy lines," and asking for prayers for the "courage, strength, guidance, and wisdom to carry out certain missions."

*Prior Anti-Terror Prosecutions*

*Figure 25 - Press release from the Manhattan District Attorney*

The use of cryptocurrency in the financing of terrorist operations has been dramatically democratized in recent years. However, since the authorities have looked into this problem and started to track suspicious transactions, some groups have been more reluctant to use this means of financing. While cryptocurrency funding seems safer than other, more traditional means, it remains limited among terrorist groups. That said, terrorists will likely continue to use cryptocurrency as one of many ways to finance their activities.

# 4. War and Nuclear Program

As previously observed with terrorist operations and criminal activities, cryptocurrency funds significant illegal activities. Apart from that, it is also used to finance war and nuclear programs. Some authoritarian regimes have found cryptocurrency an excellent method to finance offensive activities while avoiding international sanctions.

## 4.1. Nuclear Program

North Korea is undoubtedly the most active and visible country that uses cryptocurrency to fund its nuclear programs. The North Korean regime has conducted multiple cyber operations to steal cryptocurrencies for several years. Gains accrued fraudulently by the regime appear to have been increasing since 2019. According to a report submitted to the UN Security Council, North Korea allegedly stole more than $300 million in virtual assets between 2019 and 2020. In addition, a report published by the cryptocurrency compliance firm Chainalysis in 2021 stated that North Korean hackers launched numerous cyberattacks against cryptocurrency exchanges and stole approximately $400 million worth of digital assets. Finally, based on the claim of South Korean intelligence, North Korean hackers allegedly stole around $1.2 billion in cryptocurrency and other virtual assets over the past five years.[2] These attacks were primarily directed against investment companies and used different techniques, including phishing, code exploits, malware, and social engineering operations. According to a senior White House official, these stolen digital assets would be used to fund part of North Korea's nuclear program. For some time now, US intelligence has been trying to identify North Korean agents and track cryptocurrencies stolen by the regime.



[2] https://www.financialexpress.com/business/blockchain-seoul-north-korean-hackers-stole-1-2b-in-virtual-assets-2923486/

In April 2023, the US Department of Justice accused a North Korean man of concocting a money laundering scheme, using employees of US cryptocurrency companies, to help fund the North Korean regime. According to Deputy National Security Advisor Anne Neuberger, the North Korean regime is carrying out cyber cryptocurrency theft operations to earn an estimated one-third of its funds to finance its missile program.

## 4.2. War and International Sanctions



Apart from funding offensive nuclear programs, cryptocurrency has also become a way for some states trying to avoid international economic sanctions. In recent years, some states have tried to circumvent economic sanctions imposed on them using cryptocurrency. Iran is one of the countries that mostly use cryptocurrency, especially Bitcoin, to evade US economic sanctions and export millions of oil barrels. According to cryptocurrency compliance firm Elliptic, 4.5% of all Bitcoin mining occurs in Iran.[3] This number is based on data from miners by the Cambridge Center for Alternative Finance and statements from Iran's state-controlled power generation company. Iran circumvents trade embargoes and earns hundreds of millions of dollars in crypto assets (Figures 26 and 27).



*Figure 26 - A Bitcoin mining site outside Tehran's desert (Credit: New York Times)*

[3] https://www.elliptic.co/blog/how-iran-uses-bitcoin-mining-to-evade-sanctions



*Figure 27 - A Bitcoin mining site in an Iranian Mosque*

According to a report published in 2021 by the Iranian Presidential Center for Strategic Studies, Bitcoin mining is significant in generating additional revenue for Iran. The report explains that cryptocurrency mining could benefit different sectors of the Iranian economy and highlights the fact that by heavily investing in cryptocurrency mining, the state could generate $2,000,000 per day and $700,000,000 per year in direct revenue.[4]

Money usually plays an essential role in wars and armed conflicts. However, the Russo-Ukrainian war was the first where cryptocurrency was heavily used for funding purposes while avoiding sanctions. Since the Russian forces invaded Ukraine in February 2022, the United States and its allies have imposed an unprecedented series of sanctions on Russia. In the context of Russia's invasion of Ukraine, some members of the crypto community claim that cryptocurrencies offer an alternative to the Russian ruble, which would facilitate the evasion of funds from Russia. Indeed, it is easy to transfer funds in cryptocurrency and get the money in a foreign account in a tax haven or through a third party.




[4] https://iranwire.com/en/features/69084/

The decentralized structure and lack of regulation of cryptocurrencies allow Russian individuals and entities to circumvent sanctions. Based on data collected by blockchain compliance firm Chainalysis, many donations have been made to pro-Russia social media accounts since the invasion of Ukraine (Figure 28).

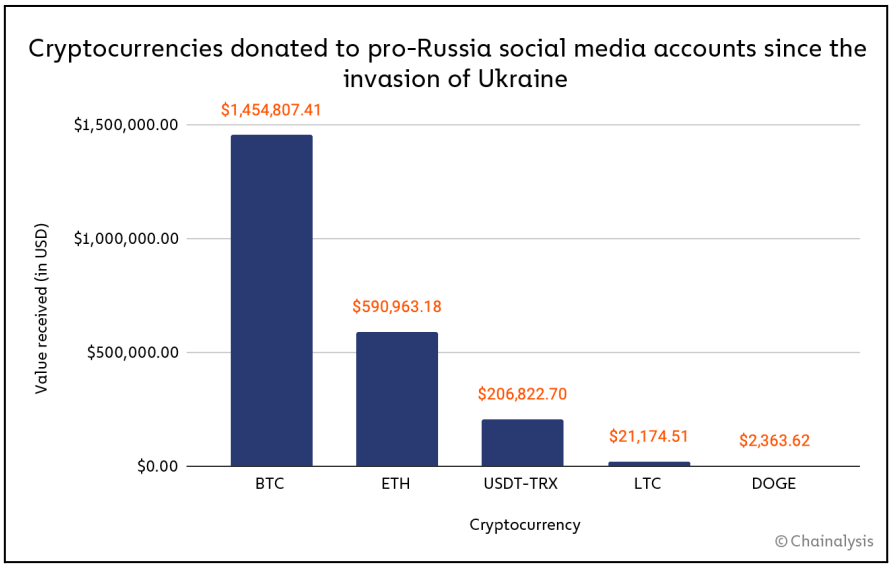



*Figure 28 - Cryptocurrency donations made to pro-Russia social media accounts*

On the opposite side, since the beginning of the war, the Ukrainian government appears to have used cryptocurrency to facilitate donations worldwide for military and other purchases. On February 26, 2022, the Ukrainian government began publicly soliciting crypto donations online (Figure 29). After initially only accepting Bitcoin, Ethereum, and Tether, the Ukrainian government expanded donations to other forms of cryptocurrencies.

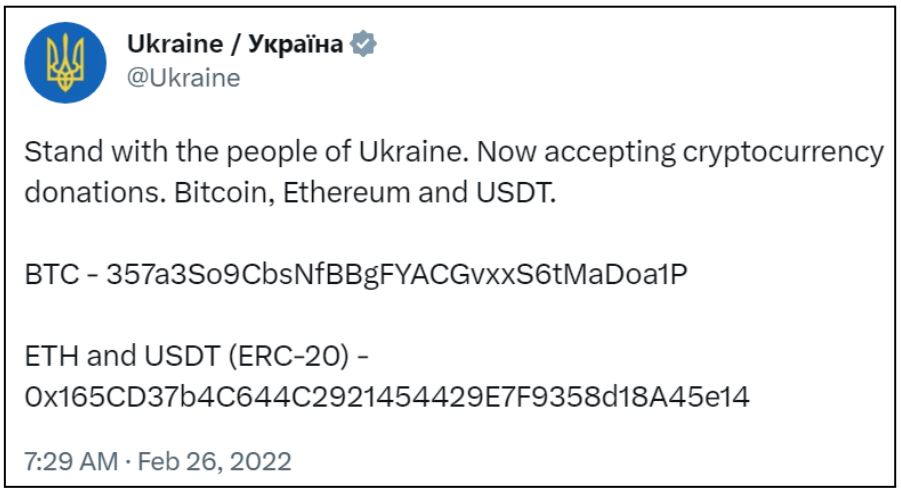



*Figure 29 - Message from the Ukrainian government on Twitter asking for donations in BTC, ETH, and USDT*

According to cryptocurrency compliance firm Elliptic, after nearly a year and a half of war pro-Ukraine causes raised over $212.1 million in crypto assets, outnumbering pro-Russia donations with only $5 million.[5] Ukrainians raised about 44 times the amount going to pro-Russia entities.

## 5. Cryptocurrency and Anonymity

The question of anonymity is at the heart of the use of cryptocurrencies. As observed earlier in this report, cryptocurrencies are devoid of uncontrolled financial flows and do not require the clear identification of the sender and the recipient. However, most cryptocurrencies are not entirely anonymous (Figure 30). Most cryptocurrencies are said to be pseudo-anonymous. In a cryptocurrency transaction, instead of having a sender called Mr. X and a receiver Mr. Y, we have an address based on a series of numbers and letters attached to a wallet. This same wallet can generate hundreds of different addresses.




*Figure 30 - Cryptocurrency privacy comparison*

Many criminals and terrorists use cryptocurrencies to finance their activities, even though they know their lack of complete privacy and security. They know that law enforcement and intelligence services are tracking these transactions, and thus they use mixing services to tighten their cloak of anonymity.

[5] https://www.elliptic.co/hubfs/Elliptic_Crypto_in_Conflict_Report.pdf?utm_campaign=Crypto%20in%20Conflict%20Report%20%7C%202023&utm_medium=email&_hsmi=247210816&_hsenc=p2ANqtz-9Q3ydxsBp7dGvi9YBfJrciXt6CmqI2GovrFd_u12ptNoF3_HRj0uNEIi7yXzR3eLwzUqmjxtZqGpdDobfdUDs0uHm4453I5kDAMQOw0j8p6KeWP-I&utm_content=247210816&utm_source=hs_automation

## 5.1. Mixing Services

Mixing services consist of mixing a multitude of transactions from different sources, which means that the funds can come from everywhere, legitimate or not. Threat actors often use these services to anonymize transfers between parties carrying out illegal activities, as they do not require Know Your Customer (KYC) verification. The price of this type of service generally varies depending on the amount to be transferred and the type of cryptocurrency. Some services also offer to change currency along the way to complicate the transaction path (Figure 31).




*Figure 31 - Example of a Bitcoin mixing service*

There are two main types of crypto mixers:

**Centralized mixers:**

Centralized mixers combine funds from different users into a single wallet. Then, they divide the pooled funds and send them through different crypto wallets. This process makes it difficult for a third party to trace the source of the funds (Figure 32).

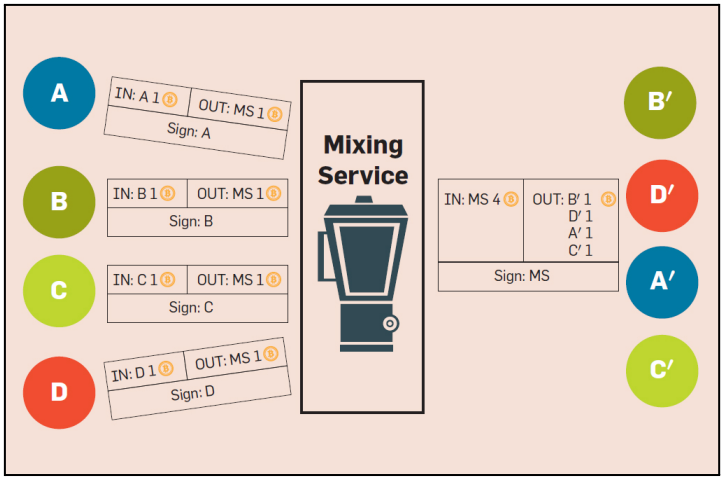



*Figure 32 - Centralized mixing with four participants.*

**Decentralized mixers:**

Decentralized mixers work on the same principle as centralized ones. However, they are not managed by a central entity and instead use peer-to-peer (P2P) strategies to allow people to send crypto funds without relying on third-party services (Figure 33).

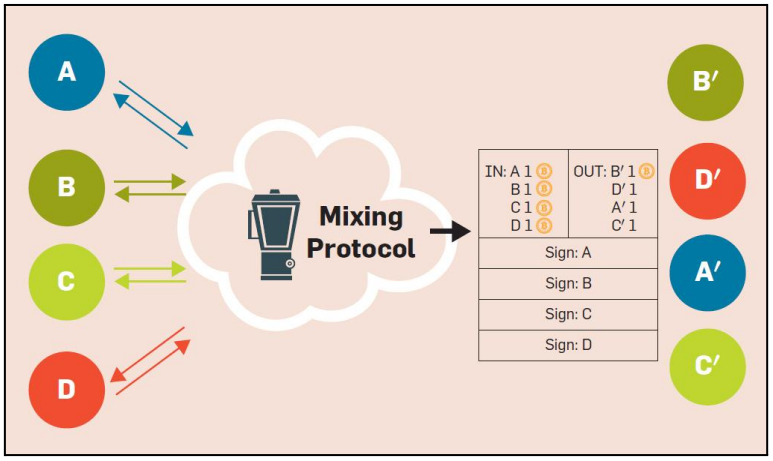



*Figure 33 - Decentralized mixing with four participants.*

## 6. Tracking Cryptocurrency on the Blockchain

Today, it is possible to identify suspicious or illegal transactions using open-source and licensed tools. With the help of OSINT, it is possible to identify addresses and wallets involved in illegal transactions. In addition to blockchain transaction tracking sites, there are also websites for reporting fraudulent addresses that help to identify whether a specific address belongs to a pool of addresses of a known exchange platform (Figures 34 and 35).

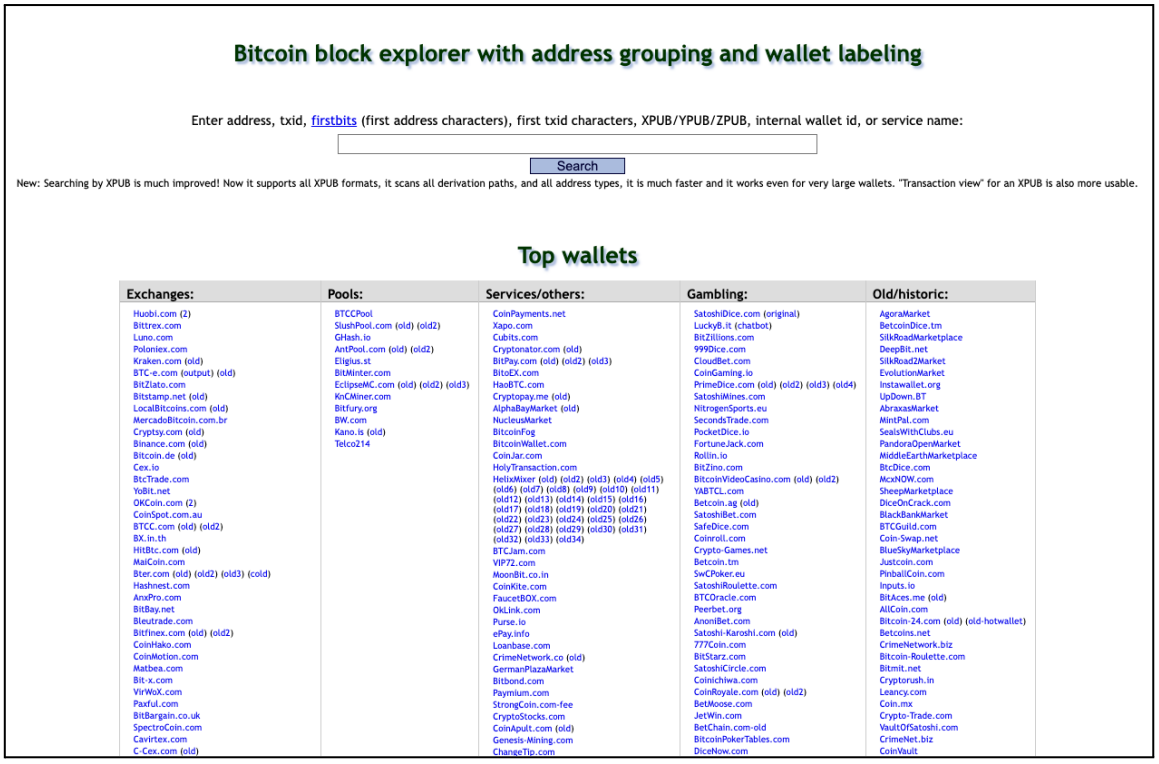



*Figure 34 - A Bitcoin block explorer with address grouping and wallet labeling*

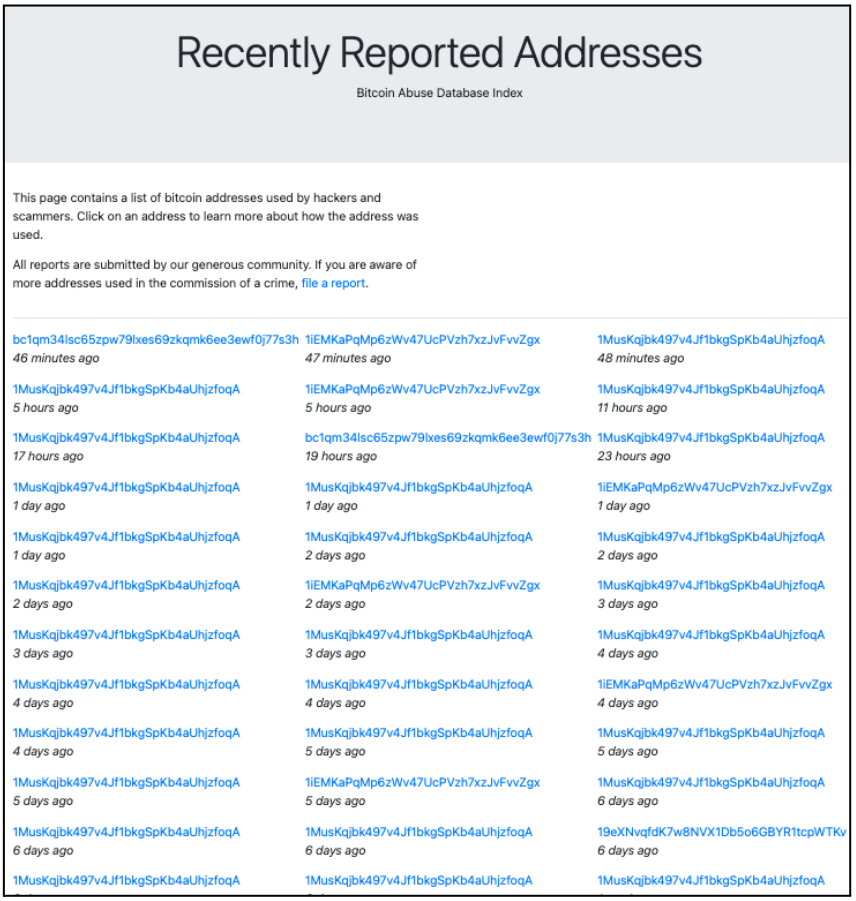



*Figure 35 - A website reporting fraudulent Bitcoin addresses*

There are several solutions on the market for tracking cryptocurrency transactions on the blockchain, particularly Bitcoin (Figure 36). These solutions are mainly used by law enforcement, government agencies, and financial institutions to track transactions and identify the various wallets involved and their respective owners. They usually work on the principle of a mix of blockchain analysis (pattern identification based on different parameters) and OSINT collection. These solutions generally enable a graphical visualization of the different transactions and provide various details, such as the transaction details, the number of addresses used, and statistics. They also provide information on the entity managing the wallet, such as terrorist organizations and darknet market owners (Figures 37 and 38).

| Company | Year Founded | Country Of Origin | Known Customers | No. Of Employees |
|---|---|---|---|---|
| Chainalysis | 2014 | USA | • Gemini<br>• Luno<br>• US FBI | 700 |
| CipherTrace | 2015 | USA | • Banks<br>• Crypto exchanges | <100 |
| Nansen | 2019 | Singapore | • Amber Group<br>• DTC Capital | 100 |
| Coin Metrics | 2017 | USA | • Goldman Sachs<br>• BNY Mellon<br>• Fidelity Investments | 50 |
| Elliptic | 2013 | UK | • Santander<br>• Coinbase<br>• Revolut | 100 |

*Figure 36 - The leading blockchain analysis companies (Source: Milkroad)*

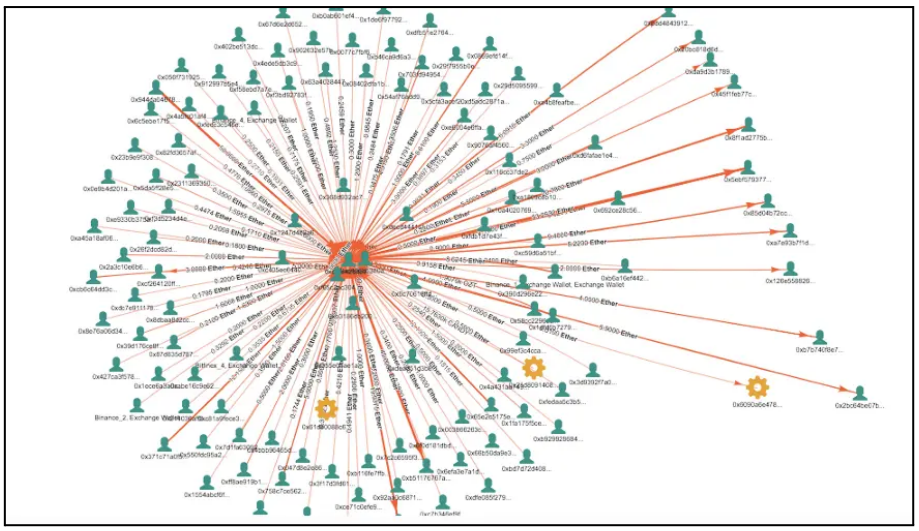


*Figure 37 - Cryptocurrency transactions tracking graph (Source: Ciphertrace)*




*Figure 38 - Interface of a Bitcoin transaction monitoring system (Source: Elliptic)*

# 7. Impact on States and International Security

As this report shows, cryptocurrency has increasingly become a serious alternative to traditional financial systems. The nature of cryptocurrency and its lack of control by states and international financial institutions make it a very useful method for threat actors worldwide to finance their illegal activities. Some economists believe that if cryptocurrency has indeed made it possible to develop a parallel financial exchange system, it might lead to financial instability.[6] Moreover, if we consider that it facilitates online traffic, plays a role in cyberattacks with ransom demands, and in the financing of terrorist and nuclear operations, cryptocurrency can, therefore, also be perceived as a risk to international security.

A vast majority of countries in the world have a different approach to cryptocurrencies. This poses a problem in tracking those using the system illegally. Cryptocurrency policies worldwide range from no regulation to a complete ban on the use of electronic currencies. Currently, each country has its own policy towards cryptocurrency and its own way of approaching it. However, just because a country issues a ban on such transactions, it does not mean it is enforced or monitored. For example, Russia prohibits cryptocurrency use, which can lead to imprisonment. However, as sizable criminal hacking networks show, the country does not seem to enforce this law. The financing of criminal or terrorist operations using cryptocurrencies at the international level can only be dealt with by consensus between states. This requires a certain willingness on the part of the international community to act to regulate the issue of cryptocurrencies. Some international institutions, such as the United Nations, have warned about this problem for some time, asking policymakers to act before the problem escalates further and poses a greater risk.

For some years, the United States has tried to resolve these issues case-by-case by prosecuting individuals and attempting to recover ransom funds. However, these efforts are still too weak. Some businesses that have fallen victim to ransomware attacks have had devastating financial impacts, and some were even forced to shut down due to the inability to recover their systems.

The European Union also takes the issue of cryptocurrencies seriously. In April 2023, MPs approved by 529 votes for, 29 against, and 14 abstentions, the first bill to track transfers of crypto assets like bitcoins and e-money tokens. The bill ensures that crypto transfers, like any other financial transaction, can always be traced and suspicious transactions be blocked.

[6] https://www.cnbc.com/2021/10/13/cryptocurrencies-could-lead-to-financial-instability-author-warns.html

While it is true that cryptocurrency has facilitated the financing of many illegal activities around the world and can potentially pose an economic risk, its use is still very moderate compared to all non-digital currency exchanges. However, if states and international organizations do not mobilize in an attempt to impose some form of standardization and regulation in exchanges, the use of cryptocurrencies for illegal financing purposes might increase in the coming years.

## About The Author



I am a cyber intelligence expert who has worked in various environments over the past twelve years, including academia, high-tech, military, and law enforcement. My field of expertise is cyber intelligence, including strategy, collection, research, and analysis, and the lead of Cyber HUMINT operations on criminal and terrorist activities within cyberspace. I have trained many civilian analysts and Military and Law Enforcement officers on the Deep & Dark Web environments, Cyber intelligence collection, and Cyber HUMINT operations.

## References


1. Terrorist Use of Cryptocurrencies Technical and Organizational Barriers and Future Threats, Cynthia Dion-Schwarz, David Manheim, Patrick B. Johnston, 2019 https://www.rand.org/pubs/research_reports/RR3026.html

2. Funding Tomorrow's Terrorists and Criminals: Cryptocurrency's Impact on the World Stage, Georgetown Security Studies Review. https://georgetownsecuritystudiesreview.org/2023/03/23/funding-tomorrows-terrorists-and-criminals-cryptocurrencys-impact-on-the-world-stage/

3. FORBES BUSINESS, Russia And Iran Eye Up Trade Using Cryptocurrencies To Avoid Dollars And Sanctions, Dominic Dudley, 2023. https://www.forbes.com/sites/dominicdudley/2023/01/18/russia-and-iran-eye-up-trade-using-cryptocurrencies-to-avoid-dollars-and-sanctions/?sh=25a5fafc1a10

4. Arab News, How Iran is cashing in on cryptocurrencies to evade US sanctions, Paul Iddon, 2022. https://www.arabnews.com/node/2199431/business-economy

5. World Economic Forum, Why the role of crypto is huge in the Ukraine war, 2023. https://www.weforum.org/agenda/2023/03/the-role-cryptocurrency-crypto-huge-in-ukraine-war-russia/

6. Financial Times, The two sides of crypto in Ukraine war, Scott Chipolina, 2023. https://www.ft.com/content/a3b59f3b-d0b3-4047-af71-c8ef61aa8d58

7. INTERNATIONAL JOURNAL ON CRIMINOLOGY, Cryptocurrency and National Security, Carolyn Alfieri https://www.criminologyjournal.org/cryptocurrency-and-national-security.html

8. Europol, Cryptocurrencies: Tracing the Evolution of Criminal Finances, 2021 https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf

9. Nuclear Energy Institute, Crypto Goes Nuclear, Mary Carpenter https://www.nei.org/news/2021/crypto-goes-nuclear

10. CNN, Half of North Korean missile program funded by cyberattacks and crypto theft, White House says, Sean Lyngaas, https://edition.cnn.com/2023/05/10/politics/north-korean-missile-program-cyberattacks/index.html

11. Times of Israel, Israel seizes 189 crypto accounts linked to terror groups since 2021, TOI STAFF, 2023. https://www.timesofisrael.com/israel-seizes-189-crypto-accounts-linked-to-terror-groups-since-2021-report/

12. Middle East Eye, Gaza: Armed wing of Hamas no longer accepting Bitcoin donations, 2023. https://www.middleeasteye.net/news/hamas-armed-wing-no-longer-accepting-bitcoin-donations

## OSINT Resources for Cryptocurrencies Investigation

1. GitHub Repository: Cryptocurrencies and NFT  OSINT Tools
   https://github.com/aaarghhh/awesome_osint_criypto_web3_stuff
2. Hackers Arise
   https://www.hackers-arise.com/osint
3. OSINT Framework
   https://osintframework.com/
4. OSINT Techniques
   https://www.osinttechniques.com/osint-tools.html
5. Aware Online
   https://www.aware-online.com/en/osint-tools/cryptocurrency-tools/