Written Testimony of Jesse Spiro
Chief of Government Affairs
Chainalysis

Before the
House Financial Services Committee
Subcommittee on National Security, International Development and Monetary Policy

Hearing on
Schemes and Subversion:
How Targets of Sanctions Undermine and Evade Sanctions Regimes

Wednesday, June 16, 2021

Chairman Himes, Ranking Member Barr, and distinguished members of the Committee. Thank you for inviting me to testify before you today on this very important topic.

My name is Jesse Spiro and I am the Chief of Government Affairs at 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. I am very glad to be here today to speak about sanctions. Every year, Chainalysis publishes a widely-read annual Crypto Crime Report, and sanctions are one of the items we focus on in the report.

Chainalysis' mission is to build trust in blockchains, and we provide blockchain data and analysis that enables law enforcement to investigate illicit activities, and regulators to ensure compliance with anti-money laundering and sanctions requirements. We also serve customers in the cryptocurrency and financial sectors, enabling them to remain in compliance with all of the latest regulatory developments, including guidance from the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC). As this rather new ecosystem grows, it is important that people have confidence in it.

Today I would like to discuss:

1. How blockchain data and analysis can benefit investigations into sanctions evasion using cryptocurrency,
2. Sanctions and cryptocurrency,
3. Examples of illicit actors and adversarial groups that have have employed cryptocurrency to evade sanctions,
4. Challenges and successes under the current sanctions regime, and
5. Recommendations for ways to improve the current sanctions regime with regards to cryptocurrency.

I would like to note that while the focus of today's hearing is sanctions, and cryptocurrency is one way that illicit actors evade sanctions, the vast majority of cryptocurrency transactions are legitimate. According to our analysis, in 2020, the illicit share of all cryptocurrency activity was just 0.34%, or $10.0 billion in transaction volume. This was a decrease from 2019, when illicit activity represented 2.1% of all cryptocurrency transaction volume, or roughly $21.4 billion worth of transfers. We do expect 2020's reported illicit activity numbers to rise slightly over time as we learn more about scams, fraud, and other illicit activity that have not yet been identified, but it is clear the vast majority of transactions are legitimate in nature.

How Blockchain Data and Analysis Can Benefit Investigations into Sanctions Evasion Using Cryptocurrency

It is a common misconception that cryptocurrency is completely anonymous and untraceable. In fact, the transparency provided by many cryptocurrencies' public ledgers is much greater than other traditional forms of value transfer. Cryptocurrencies like Bitcoin operate on public, immutable ledgers known as blockchains. Anyone can look up the entire history of transactions on these blockchains. The ledger shows a string of random numbers and letters that transact with another string of random numbers and letters. At its core, Chainalysis is a data company, and our data set maps these random numbers and letters – cryptocurrency addresses– to their real-world entities. For example, in Chainalysis products, we are able to see that a given transaction was between a user at a specific exchange, with a user at another exchange, or between a user at an exchange and a sanctioned entity, or any other illicit or legitimate service using cryptocurrency.

Our data set and investigative tools are invaluable in allowing investigators to trace cryptocurrency transactions, identify patterns, and, crucially, see where cryptocurrency users are exchanging cryptocurrency for fiat currency. Using blockchain analysis tools, law enforcement can trace cryptocurrency to identify its origination and/or its cashout points at cryptocurrency exchanges. Law enforcement can serve subpoenas to these cryptocurrency exchanges, which are required to register as money service businesses here in the United States and collect Know Your Customer (KYC) information from their customers. In their response to legal process, the exchange will provide any identifying information that they have related to the cryptocurrency address, such as name, address, and government identification documentation, to law enforcement, allowing them to further their investigation.

In part due to the ability to leverage the transparency of cryptocurrencies and blockchain analytics, law enforcement has been able to disrupt terrorist financing campaigns, dismantle child sexual abuse material websites, and seize the ill-gotten proceeds of Darknet marketplace administrators.

Blockchain analysis tools like ours are also used by financial institutions and cryptocurrency exchanges to ensure they are meeting their anti-money laundering requirements. These tools can detect and alert users to patterns of potential high-risk activity among their

customers. Using these tools, businesses can identify whether their customers are attempting to transact with OFAC sanctioned individuals, entities, or jurisdictions, or cashing out funds generated from Darknet markets, scams, fraud, and other forms of illicit activity.

Blockchain and investigative analyses can be used to determine ownership or control of additional addresses associated with sanctioned individuals or entities based on information OFAC has provided publically. For example, if OFAC lists a cryptocurrency address as an identifier associated with a particular individual, using blockchain analytics, we can identify other wallet addresses likely controlled by the same individual and label them so that they are also identified as belonging to the sanctioned individual. Likewise, additional assets, such as tokens or forks of blockchains, associated with the addresses and entities identified by OFAC can be determined through blockchain analytics.

When OFAC lists cryptocurrency addresses as identifiers associated with sanctioned entities, they are labelled in our tools as sanctions-related and our customers receive alerts on historical or future exposure to these addresses. This means our technology enables cryptocurrency exchanges and financial institutions to ensure that their customers are not interacting with addresses associated with sanctioned persons and identify and freeze any accounts that attempt to do so.

Blockchain analytics can also be used to identify trends and develop intelligence about who may be facilitating the evasion of sanctions. Using tools like the ones that Chainalysis develops, it's possible to quantify how much sanctions evasion has occurred in the past, something that would not be possible in traditional finance. For example, by tracking their payments, our customers can identify virtual private network (VPN) services, bulletproof web hosting services, and other providers sanctioned malicious actors are using. All of this information is valuable intelligence that can allow investigators to determine new trends and patterns in sanctions evasion so that they can combat them.

Because of its inherent transparency and traceability, there are many advantages to cryptocurrency when it comes to investigating sanctions evasion. Traditionally, criminals and money launderers have attempted to use misspellings, code words, and other techniques to evade sophisticated sanctions screening. But with cryptocurrency, the unforgeable addresses represent unavoidable, definitive evidence on a transparent record. Additionally, unlike some forensic evidence that degrades over time, blockchain evidence is permanent and immutable. What's more, our ability to analyze this evidence is only getting more sophisticated. Criminals who thought they evaded detection in months and years past often find they've left a permanent trail for law enforcement to follow.

Sanctions and Cryptocurrency

OFAC is charged with administering and enforcing economic and trade sanctions. This includes sanctions against terrorists, transnational criminal organizations, those engaged in activities related to the proliferation of weapons of mass destruction, and foreign countries that pose a threat to our national security. OFAC creates and maintains the Specially

Designated Nationals and Blocked Persons List (SDN List), which financial institutions screen their customers against. In addition to the SDN List, there are comprehensive country and regional embargoes. U.S. persons are prohibited from engaging in a wide range of activity in connection with individuals or entities on OFAC's SDN List and those covered by comprehensive country or region embargoes.

In 2015, then-President Obama issued Executive Order 13694, titled "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," and OFAC began designating malicious cyber actors. Since then, OFAC has implemented a cyber sanctions program and designated many malicious cyber actors, including perpetrators of ransomware attacks, actors who have stolen millions in cryptocurrency from users in exchange hacks, and those who facilitate ransomware or theft proceeds by exchanging them for fiat.

In March 2018, OFAC released public guidance [FAQs #559, 560-594] related to cryptocurrencies and indicated they would start listing "digital currency addresses" on the SDN List as identifiers associated with sanctioned individuals and entities. In November 2018, OFAC designated two Iran-based financial facilitators of malicious cyber activity for their alleged involvement in the SamSam ransomware, and for the first time included digital currency addresses as identifiers.

On the SDN list, OFAC lists cryptocurrency addresses under sanctioned entities or individuals as identifier "Digital Currency Address" as shown in the example below.

Example of OFAC "Digital Currency Address" Listing

Details:

Type:	Individual	**List:**	SDN
Last Name:	KHORASHADIZADEH	**Program:**	CYBER2
First Name:	Ali	**Nationality:**	Iran
Title:		**Citizenship:**	
Date of Birth:	21 Sep 1979	**Remarks:**	
Place of Birth:	Tehran, Iran		

Identifications:

Type	ID#	Country	Issue Date	Expire Date
Passport	T14553558	Iran	28 Oct 2008	29 Oct 2013
Digital Currency Address - XBT	149w62rY42aZBox8fGcmqNsXUzSStKeq8C			
Gender	Male			
Email Address	iranvisacart@yahoo.com			
Email Address	alikhorashadi@yahoo.com			
Email Address	mastercartaria@yahoo.com			
Email Address	toppglasses@gmail.com			
Email Address	iranian_boy5@yahoo.com			
Additional Sanctions Information -	Subject to Secondary Sanctions			

Aliases:

Type	Category	Name
a.k.a.	weak	Mastercartaria
a.k.a.	weak	Iranvisacart

Since November 2018, OFAC has included 97 digital currency addresses in eight different designations. This has included designations against Chinese nationals for narcotics trafficking and money laundering, associates of the Democratic People's Republic of Korea (DPRK) Lazarus Group, Russian nationals for their involvement in disinformation campaigns, and Russian cyber actors involved in cryptocurrency exchange hacks. In April of this year, the Biden Administration announced several new sanctions against Russian intelligence service disinformation outlets and designated a Pakistani organization that provided cyber actors, including Russian disinformation actors, fraudulent identity documents used in the digital onboarding process at financial institutions.

In October 2020, OFAC issued an "Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments." The advisory warned, "Companies that facilitate ransomware payments to cyber actors on behalf of victims, including financial institutions, cyber insurance firms, and companies involved in digital forensics and incident response, not only encourage future ransomware payment demands but also may risk violating OFAC regulations." OFAC's alert bolstered previous government guidance not to pay ransomware attackers, who typically demand ransom be paid in cryptocurrency, as this incentivizes future attacks and goes a step further in warning that ransomware victims and consultants who help them make payments could face the heavy penalties associated with sanctions violations. It also noted that license applications made to OFAC that involve ransomware payments demanded as a result of malicious cyber-enabled activities would be reviewed by OFAC, but with a presumption of denial.

Under 2013 guidance from FinCEN, cryptocurrency exchanges must register as money services businesses ("MSBs"). They therefore must meet certain anti-money laundering/countering the financing of terrorism (AML/CFT) requirements under the Bank Secrecy Act, including (i) establishing AML programs, (ii) adhering to certain regulatory reporting requirements, and (iii) maintaining certain books and records. This includes complying with sanctions regulations. This has led US-based cryptocurrency exchanges to establish KYC programs to verify the identity of their customers and use transaction monitoring solutions to detect suspicious activity, making it more difficult for illicit actors or those trying to evade sanctions to cash out their ill-gotten cryptocurrency for fiat currency.

More recently, after a number of high-profile ransomware attacks, including those on Colonial Pipeline and JBS, National Security Advisor Jake Sullivan confirmed the Administration would be addressing the issue of ransomware and "countries, including Russia, that are harboring or permitting cyber criminals to operate from their territory" at the G7 Summit. While the addition of cryptocurrency addresses as identifiers for sanctioned individuals and entities is a relatively new advent, we see based on blockchain data how impactful these inclusions are. The data on ransomware specifically suggests that blockchain analysis will be crucial to fighting cybercrime from groups aligned with Russia and other hostile nation states.

Examples of Illicit Actors and Adversarial Groups That Have Employed Cryptocurrency to Evade Sanctions

Terrorist Groups

While terrorist financing using cryptocurrency is a small portion of the illicit activity we see on the blockchain, it does occur. Cryptocurrency as a terrorism financing tool presents particular challenges. Unlike social media profiles and bank accounts, a cryptocurrency address is much more difficult to shut down due to the decentralized nature of blockchains. Here I outline several examples of terrorist organizations that have exploited cryptocurrency as a means of evading sanctions and raising money for their violent efforts.

Terrorist Groups: Hamas

Recently, a representative from Palestinian militant group Hamas confirmed that they have seen an increase in cryptocurrency donations. The group is able to use cryptocurrency to circumvent international sanctions to fund its military operations. This is not a new trend for the group, which has exploited cryptocurrency in the past to raise money.

The Izz ad-Din al-Qassam Brigades (AQB) is the military wing of Hamas, a U.S.- and European Union-designated terrorist organization. Chainalysis has written previously about AQB's use of cryptocurrency in donation campaigns in our 2020 Crypto Crime Report and in August 2020, the U.S. federal authorities seized more than $1 million in cryptocurrency tied to AQB financial facilitators.

AQB's campaign started in 2019, when they posted a call on their social media page and official websites asking for Bitcoin donations. According to the DOJ's press release, "The al-Qassam Brigades boasted that Bitcoin donations were untraceable and would be used for violent causes. Their websites offered video instruction on how to anonymously make donations, in part by using unique Bitcoin addresses generated for each individual donor." Federal investigators were able to employ blockchain analysis to track the donated cryptocurrency and take action by identifying individuals who had violated U.S. sanctions by donating to the terrorists or individuals who received Bitcoin from the campaign.

Terrorist Groups: Al-Qaeda

Al-Qaeda, another U.S.- and European Union-designated terrorist organization, along with affiliated groups, operated a cryptocurrency terror finance campaign, evading U.S. sanctions. The campaign was conducted using Telegram and other social media platforms to solicit donations to fund violent terrorist attacks and equip terrorists in Syria. U.S. law enforcement was able to identify 155 virtual currency addresses associated with the terrorist campaign.

According to the criminal complaint, these al-Qaeda and affiliated groups used multi-layered transactions to obfuscate the movement of these donations to a central hub of

addresses, from which funds were then redistributed to the individual groups. Through blockchain analysis, Chainalysis identified the BitcoinTransfer Office in Idlib, Syria as the central hub described in the criminal complaint. BitcoinTransfer purports to be a cryptocurrency exchange but has been implicated in several terrorism financing schemes and appears to be fully under the control of terrorist groups. Since the service became active in late December 2018, more than $280,000 worth of Bitcoin has passed through BitcoinTransfer, much of it related to terrorism financing.

While multiple terrorist groups ran their own individual donation pushes, nearly all of them followed a similar strategy. The groups presented themselves as charitable organizations operating in Syria to solicit Bitcoin donations on social media and messaging platforms — mostly Telegram and Facebook. However, despite the charity facade, these groups often published posts indicating that donations would go towards purchasing weapons for militant groups.

In May 2019, U.S. law enforcement monitoring the Telegram page of one such group, Tawheed & Jihad Media, saw the administrators promoting a funding campaign for "bullets and rockets for the *mujahideen*" with a single Bitcoin address listed. Law enforcement monitored that address as donations came in, and noticed that the group administrators eventually moved the funds to an address associated with BitcoinTransfer.

Using similar analytical techniques, law enforcement observed terrorism financing campaigns conducted by other al-Qaeda-affiliated groups, most of whom solicited donations in similar ways — pretending to be charities while actually funding militant activity — before sending the proceeds on to al-Qaeda's BitcoinTransfer addresses. Those groups include:

- Malhama Tactical - a jihadist military company that trains Hay'at Tahrir al-Sham (HTS) fighters and has solicited Bitcoin to finance HTS operations in Syria.
- Al Sadaqah - "charity" in Arabic, is a Syrian organization that operates social media accounts on multiple platforms which seek to finance terrorism via Bitcoin solicitations.
- Al Ikhwa - the group's profile describes them as an "independent charity on the ground in Syria" and that they "do not support any acts of terrorism;" however, blockchain analysis and a review of related social media posting demonstrates otherwise.
- Reminder from Syria - a Telegram channel affiliated with terrorist groups that frequently interacts with and boosts content from Al Ikhwa on social media.

Given these instances, it's crucial that cryptocurrency businesses and financial institutions monitor transactions to address any possible exposure to terrorist financing campaigns.

Nation States

At both the government-level and the individual-level those in nation states impacted by sanctions have embraced cryptocurrency adoption for various reasons. For some it is simply

out of curiosity or investment, for others it is about wealth preservation to hide from their government's reach, and then there are those who are using it as a way to evade sanctions, or facilitate financial cyber crimes. Below I outline examples from Iran, Russia, North Korea, and Venezuela.

Nation State Actors: Iran

Iranian officials have discussed the use of cryptocurrencies to evade sanctions, with Iranian researchers preparing whitepapers on the topic. The Central Bank of Iran has piloted research and development of a Central Bank Digital Currency (CBDC). Recently, Iranian President Hassan Rouhani requested his government start developing a framework to regulate cryptocurrencies. Beyond the government level, Iran's citizens have embraced cryptocurrency and are considered early adopters. The two main ways Iran can use cryptocurrency to evade sanctions, or weaken the impact of sanctions, is to acquire wealth by mining or theft of cryptocurrencies, or to use cryptocurrencies to conduct economic business to bypass traditional screening.

Iran is heavily involved in mining cryptocurrencies. By mining cryptocurrencies, Iran is able to acquire wealth by validating cryptocurrency payments for individuals globally - including U.S. citizens. They can then transact via non-traditional financial institutions, including high risk exchanges or individual peer-to-peer traders, to bypass screening. Iran's cyber actors have been involved with deploying ransomware and receiving cryptocurrency payments from U.S. companies.

While there has not been substantial reporting on exact use cases for economic trades involving cryptocurrency, Iran could use cryptocurrency to send and receive payments for oil or other goods to evade sanctions. According to a report from the English-language Iranian economic news source Financial Tribune, the Central Bank of Iran is authorizing banks and licensed exchanges to use cryptocurrency as payments for imports.

Chainalysis research has identified over 20 Iranian exchanges that have received cryptocurrencies worth over $820 million since May 2013. Substantial amounts of the Bitcoin received at these exchanges can be traced back to mining operations or exchanges not based in Iran, while substantial amounts of the outgoing Bitcoin can be traced to various exchanges located around the world.

Nation State Actors: Russia

Russian cybercriminals are involved in developing and deploying ransomware, cryptocurrency thefts from individuals and exchanges, and cryptocurrency scams aimed to defraud cryptocurrency users. The GRU, a Russian military foreign intelligence service involved with disinformation campaigns and other cyber activities, have used cryptocurrency to acquire cyber infrastructure.

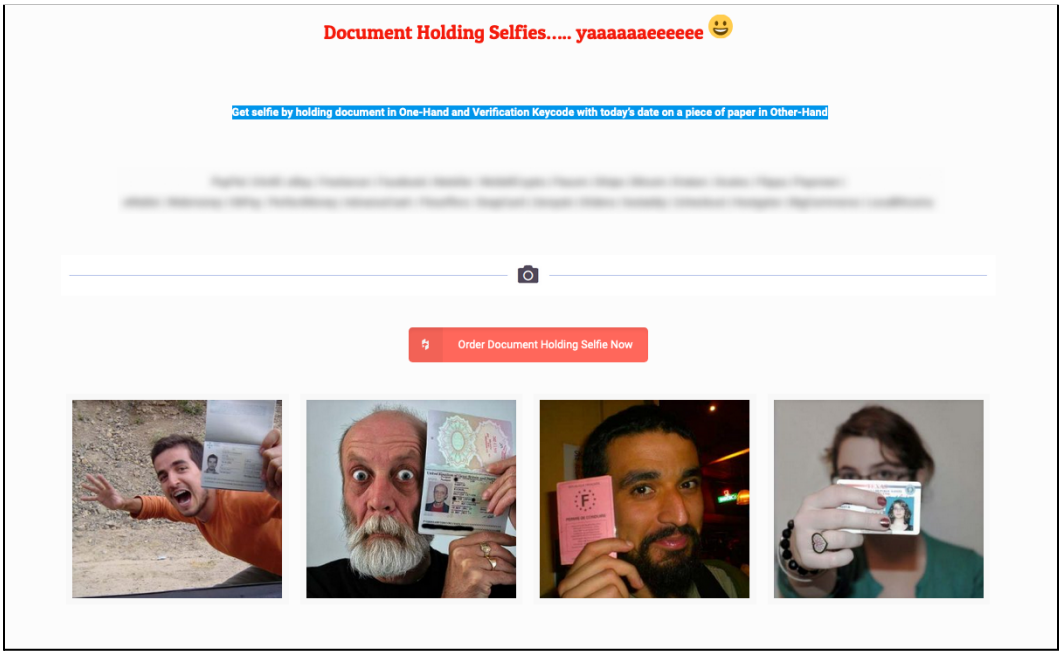
In 2020, OFAC designated Russian nationals involved with the previously designated Internet Research Agency (IRA) disinformation campaign and in a separate action they designated Russian cybercriminals involved with stealing cryptocurrencies. In April 2021, in coordination with the issuance of a new Executive Order and a six-count federal indictment from the Department of Justice, OFAC took sweeping action against 16 entities and 16 individuals who attempted to influence the 2020 U.S. presidential election at the direction of the leadership of the Russian Government. Second Eye Solution (SES), an entity designated on this date, highlights the weaknesses for digital onboarding and sanctions screening.

SES is a Pakistan-based synthetic identity document vendor that provided fake identity documents for people to sign up for accounts with cryptocurrency exchanges, payment providers, banks, and more under false identities. SES assisted the IRA in concealing its identity to evade sanctions. According to the Department of Justice indictment, SES provided documents to over 200 countries and territories. These documents can be used to bypass sanctions screening.

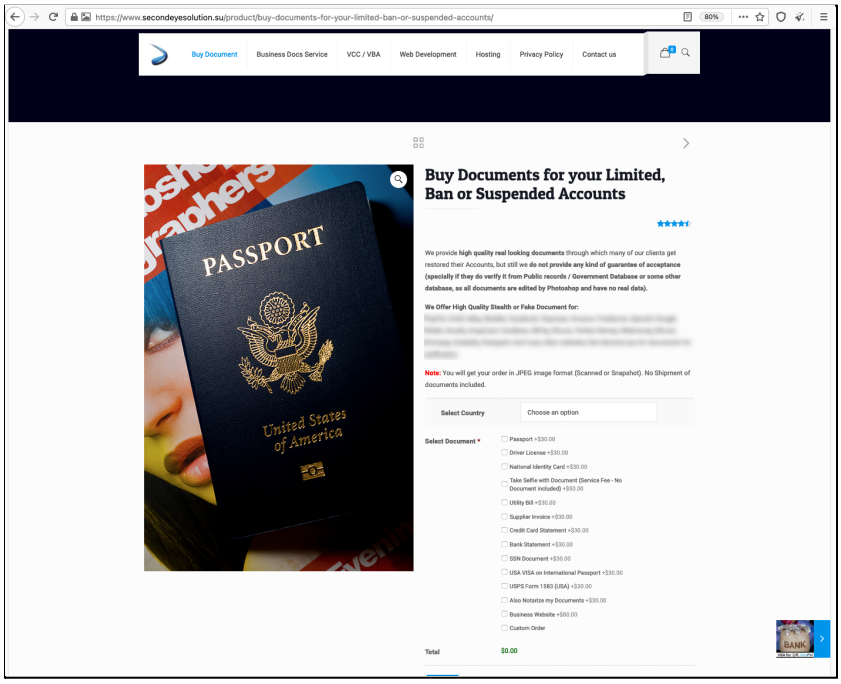
SES operated openly on the Clearnet, rather than on the Darknet like many other fraud shops and illegal businesses Chainalysis studies. The company promoted its products to people looking to sign up for financial technology (fintech) and cryptocurrency platforms using falsified documents. In fact, SES's documents were only in digital JPEG format, with no physical documents provided, making it difficult to imagine use cases other than fooling remote photo or video-based KYC checks. The company even offered users fake selfies in which they appear to be holding identifying documents — a common requirement for remote KYC checks during onboarding.

SES also helped its customers carry out synthetic identity fraud as opposed to stolen identity fraud, a rarity in fraud shops. Whereas stolen identity fraud involves the use of stolen information to steal an existing person's identity, perpetrators of synthetic identity fraud typically use a mix of real and fake information, such as social security numbers and names, to create new false identities in order to commit fraud.

Example of Second Eye Solution's Advertised Selfie Offerings



Example of Second Eye Solution's Advertised Fake Documents for Sale



After customers chose the documents they wanted to purchase, SES would ask them to specify the services at which they planned to use them so that the documents could be tailored accordingly. Most fake documents were priced between $30 and $80. Customers could pay using cryptocurrencies like Bitcoin, Ethereum, Litecoin, and Bitcoin Cash, or with online payment services like WebMoney, PerfectMoney, and Payoneer.

The DOJ indictment notes that threat actors associated with Russia's IRA bought fake identification documents from the company in order to set up online accounts under assumed identities. The IRA is a "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. OFAC previously sanctioned the IRA in March 2018, September 2019, and September 2020, and according to the Treasury, selling to the IRA is the specific offense that has now landed SES on the SDN List.

Using blockchain analytics to analyze the cryptocurrency addresses cited in OFAC's designation and those we have identified through co-spending patterns, we see that SES received over $2.5 million worth of cryptocurrency across 31,000 transactions since becoming active in 2013.

Nation State Actors: Democratic People's Republic of Korea (DPRK)

The Democratic People's Republic of Korea (DPRK) trains cyber actors to target and launder stolen funds from financial institutions. Of note is Lazarus Group, a U.S.-designated North Korean state-sponsored malicious cyber group. Lazarus Group is an infamous cybercriminal syndicate sponsored by the North Korean government. Considered an advanced persistent threat by cybersecurity experts, Lazarus Group is accused of being behind the 2014 hack of Sony Pictures; the 2017 WannaCry ransomware attacks, which affected at least 150 countries around the world and shut down approximately three hundred thousand computers; the $81 million Bangladesh Central Bank SWIFT hacking; as well as a number of cryptocurrency exchange attacks. Overall, the group is believed to have stolen more than $1.75 billion worth of cryptocurrency in the time it's been active. According to OFAC, "North Korea's malicious cyber activity is a key revenue generator for the regime, from the theft of fiat currency at conventional financial institutions to cyber intrusions targeting cryptocurrency exchanges" and the stolen funds allow "the North Korean regime to continue to invest in its illicit ballistic missile and nuclear programs."

In March 2019, the DragonEx cryptocurrency exchange was hacked by Lazarus Group and lost over $7 million worth of cryptocurrency, including Bitcoin, Ripple, and Litecoin. DragonEx responded quickly, announcing on various social media platforms that it had been hacked and releasing a list of 20 wallet addresses to which its funds had been transferred. That allowed other exchanges to flag those wallets and freeze accounts associated with them, making it harder for the attackers to move the funds. Also in 2019, Lazarus hacked the UpBit cryptocurrency exchange, which netted them more than $49 million worth of cryptocurrency. Then in 2020, Lazarus Group managed to pull off the biggest cryptocurrency theft of the year, stealing roughly $275 million worth of cryptocurrency from the exchange KuCoin. According to KuCoin's CEO, the hack occurred after cybercriminals gained access to the private keys to the exchange's hot wallets. Soon after, he claimed that the exchange had recovered $204 million worth of the stolen funds.

Lazarus Group's hacking techniques have advanced over time, as evidenced in the DragonEx instance. Initially, Lazarus Group relied on social engineering to attack exchanges,

typically fooling employees into downloading malicious software that gave Lazarus access to users' funds. Lazarus took this strategy a step further and executed one of the most elaborate phishing schemes we've seen to gain access to users' funds in the 2019 DragonEx exchange hack.

While the DragonEx hack was relatively small, it was notable for the lengths Lazarus Group went to in order to infiltrate the exchange's systems in a sophisticated phishing attack. Lazarus created a fake company claiming to offer an automated cryptocurrency trading bot called Worldbit-bot, complete with a slick website and social media presence for made-up employees. Lazarus even went so far as to build a software product resembling the trading bot they claimed to be selling. The key difference, of course, was that the program contained malware giving the hackers access to the computer of anyone who downloaded it. Lazarus Group hackers pitched a free trial of the software to DragonEx employees, eventually convincing someone to download it to a computer containing the private keys for the exchange's wallets. From there, the hackers were able to make off with millions.

Similarly, Lazarus Group's money laundering techniques have advanced over time. For example, in 2018, 98% of all funds Lazarus stolen from exchanges were moved to exchanges with minimal KYC requirements. By 2019, 48% of funds stolen by Lazarus moved to mixers or CoinJoin wallets, while 50% sit unspent in the hackers' original wallet. Mixers obfuscate the path of funds by pooling cryptocurrency from multiple users, and giving each one back an amount from the pool equal to what they initially put in, minus a 1-3% service fee. Everyone ends up with a "mix" of the funds everyone else put in, which makes it more difficult to connect the inputs to an output on the users' transactions. Many criminals use mixers to hide the source of illicit cryptocurrency before moving it to other services. CoinJoin wallets (named for the underlying CoinJoin protocol), such as Wasabi Wallet, accomplish the same thing by providing a wallet service that allows multiple users to trustlessly join their payments into a single transaction with multiple recipients.

The advances Lazarus Group has made in both their hacking and money laundering techniques reveal the time and resources Lazarus has at its disposal, as well as the deep knowledge of the cryptocurrency ecosystem necessary to successfully impersonate legitimate participants and adapt to investigative techniques.

In February 2019, OFAC sanctioned Lazarus Group, as well as two of their subgroups, "Bluenoroff" and "Andariel." In the announcement of the designation, OFAC noted that, "Lazarus Group targets institutions such as government, military, financial, manufacturing, publishing, media, entertainment, and international shipping companies, as well as critical infrastructure, using tactics such as cyber espionage, data theft, monetary heists, and destructive malware operations." The following year, in March 2020, U.S. Treasury's Office of Foreign Assets Control (OFAC) sanctioned two Chinese nationals, Tian Yinyin and Li Jiadong, for their role in helping Lazarus Group launder funds stolen in four separate cryptocurrency exchange hacks between 2017 and 2019. In this latter designation, 20 cryptocurrency addresses associated with sanctioned entities were added as identifiers.

Nation State Actors: Venezuela

Venezuela is suffering through one of the worst economic crises in modern history. In 2020, the annual inflation rate reached 6,500%. Under these circumstances, cryptocurrency has taken on an important role in Venezuela's economy. Many Venezuelans rely on cryptocurrency to receive remittances from abroad and preserve their savings against hyperinflation. At the same time, Venezuela's contested government, led by OFAC-sanctioned Nicolas Maduro and known for its corruption and human rights abuses, has launched its own cryptocurrency projects it claims will mitigate poor economic conditions for its citizens. However, officials have also stated that bypassing sanctions — a point of concern around cryptocurrency for the U.S. and its allies — is a key goal of these projects.

In 2018, the Venezuelan government started the Petro: a national cryptocurrency said to be backed by the country's oil reserves. In March 2018, then-President Trump issued Executive Order 13827, banning U.S. persons from transacting in the Petro. While the goal of the project is ostensibly to combat the currency devaluation hurting Venezuela today, government officials have also stated that evading sanctions is another goal. In addition to creating the Petro, the Maduro regime also gave seven cryptocurrency exchanges permission to operate in the country, their goal being to facilitate the exchange of the Petro so that it can circulate in the global cryptocurrency economy. These exchanges aren't limited to the Petro, of course — just like any other exchange, users can buy and sell popular cryptocurrencies like Bitcoin. In addition to the cryptocurrency exchanges, Caracas recently got its first Bitcoin ATM. The exchanges and Bitcoin ATM represent a risk of sanctions evasions, as individuals connected to the Maduro regime could theoretically use them to receive transfers from citizens of the U.S., E.U., or other jurisdictions that have implemented Venezuela-related sanctions.

Malicious Cyber-Enabled Actors

OFAC has sanctioned malicious cyber-enabled actors, including ransomware developers and attackers. Because of this, victims and financial intermediaries who facilitate ransomware payments on their behalf should be aware that making ransomware payments to sanctioned actors could be a violation. Ransomware victims may be forced to choose between paying the ransom and possibly suffering an additional penalty in the form of an OFAC violation, or not paying the ransom and suffering the loss of their data and the resulting financial costs of business disruption, or even death in the event that hospitals are attacked.

Ransomware payments increased in 2020, and are on pace to grow again in 2021. We are aware of ransomware strains related to sanctioned entities that have very likely rebranded, changing the ransomware names to obfuscate their connection to sanctions so that victims will continue to make ransom payments. We may see increases in ransomware payments with sanctions risk, if emerging strains receiving payments are connected to potential sanctions nexuses, or if OFAC designates additional ransomware groups. For instance,

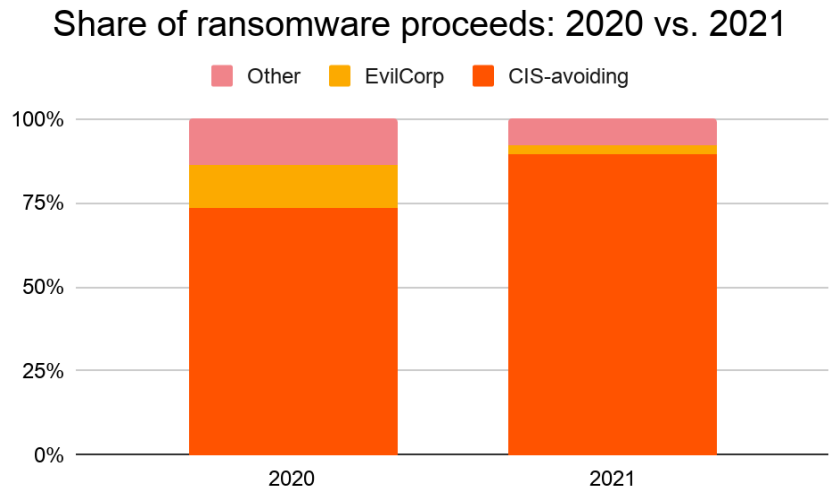
we've noticed that some Iranian ransomware strains have resurfaced under new names to disguise their connections to organizations and individuals with sanctions risk. It is therefore imperative that ransomware victims and those assisting them conduct due diligence using blockchain analytics to ensure that they are not violating sanctions should they choose to pay ransom.

Many ransomware strains are associated with sanctioned cybercriminal groups based in or affiliated with Russia, such as the sanctioned group Evil Corp, whose leadership reportedly has ties to the Russian government. Generally speaking, cybercriminals affiliated with Russia and other Russian-speaking countries in the Commonwealth of Independent States (CIS) — an intergovernmental organization of former Soviet countries — have been among the most prolific in the world. Russian-affiliated services received more cryptocurrency from illicit addresses than those in any other country, suggesting that Russian-affiliated cybercriminals are some of the biggest financial beneficiaries of cryptocurrency-based crime. Much of this activity is driven by Hydra, a Russia-based Darknet market, which, in addition to drugs, sells stolen data that can be useful to ransomware attackers.

In 2021, ransomware strains associated with Russia and other CIS countries are accounting for a larger share of overall ransomware activity. We show this on the graph below by comparing activity in 2020 and 2021 for two categories of ransomware strains:

- Strains associated with Evil Corp.
- Strains with code that prevents encryption if the ransomware detects the victim's operating system is located in a CIS country, labled "CIS-avoiding" in the below graph. These strains can generally be assumed to have originated in Russia or other CIS countries.

The numbers are clear: Taken together, these ransomware strains are accounting for more activity in 2021 compared to 2020.



Please note: This graph reflects the total amount of ransomware activity accounted for by the ten most prolific strains in 2020 and 2021. While this excludes many individual strains, it still reflects the majority of activity in both years.

In 2020, roughly 86% of ransomware proceeds studied could be attributed to ransomware strains that are either associated with Evil Corp or are designed to avoid CIS countries. So far in 2021, that figure is at 92%.

Transnational Criminal Organizations

We see a number of transnational criminal organizations (TCOs) exploiting cryptocurrency as a method of money laundering. This includes designated Mexican TCOs like the Cartel de Jalisco Nueva Generacion (CJNG) and the Sinaloa Cartel, which have turned to cryptocurrency to launder their illicit proceeds. In the past two years, OFAC has continued levying sanctions against these types of organizations, and has taken the step of listing their associated cryptocurrency addresses as identifiers in the designations.

In August 2019, OFAC announced sanctions against three Chinese nationals and the Zheng drug trafficking organization (DTO) for manufacturing and distributing hundreds of controlled substances, including fentanyl analogues, which they sold online. In the designation, 12 cryptocurrency addresses were included as associated identifiers. The Zheng DTO laundered their illicit proceeds using cryptocurrencies and, according to OFAC, "transmitted drug proceeds into and out of bank accounts in China and Hong Kong, and bypassed currency restrictions and reporting requirements." According to the Department of Homeland Security, the group was responsible for shipping fentanyl analogues and 250 other drugs to at least 25 countries and 37 states and the drugs sold by the group directly led to the fatal overdoses of two people in Akron, Ohio.

In December 2020, OFAC designated Wan Kuok Koi, aka "Broken Tooth," as well as three entities owned or controlled by him. According to OFAC, Wan "is a member of the Communist Party of China's (CCP) Chinese People's Political Consultative Conference, and is a leader of the 14K Triad, one of the largest Chinese organized criminal organizations in the world that engages in drug trafficking, illegal gambling, racketeering, human trafficking, and a range of other criminal activities." Wan was designated for corruption related to government contracts, bribery, and the expropriation of private assets for personal gain. Wan's World Hongmen History and Culture Association, which was also designated in this action, has spread across Southeast Asia, establishing a powerful business network involved in real estate, a security company specialized in protecting Belt and Road Initiative investments, and even the development and launching of cryptocurrencies. OFAC noted that Wan's activities meet "a pattern of overseas Chinese actors trying to paper over illegal criminal activities by framing their actions in terms of China's Belt and Road Initiative (BRI), the China Dream, or other major initiatives of the CCP." The Chinese enterprises behind the BRI projects, like Wan's, are often linked to criminal networks, and engage in money laundering using casinos and cryptocurrencies.

Challenges and Successes Under the Current Sanctions Regime

While we have seen sanctions have an impact against those exploiting cryptocurrencies and those seeking to use cryptocurrencies to evade sanctions, there is no denying that there are some challenges associated with the use of cryptocurrency to evade sanctions. As with any new technology, there is a learning curve. Investigators have had to develop the skills, tools, and capabilities necessary to go after these criminals. This sort of development takes time and money and requires agency leaders to prioritize these resources and efforts. Investigative techniques, training, and domain knowledge within the U.S. Government must continue to advance in line with the evolving technologies and the tactics deployed by bad actors attempting to abuse the digital financial ecosystem.

Financial screening and KYC checks can also pose a challenge for cryptocurrency exchanges. As the SES case underscores, even if exchanges have strong compliance regimes, there exist criminal groups willing to sell fake documents that allow illicit actors to pass KYC checks. These fraudulent identification documents, which can be enhanced with photo editing and deepfake video technology, can be used during the digital onboarding process to bypass sanctions screening. Chainalysis has begun to map out at least 50 other vendors like SES that provide fraudulent identity documents used during the digital onboarding process. While this challenge is not unique to cryptocurrency exchanges — there are an increasing number of online banks that must also confront this issue — it's vital that cryptocurrency businesses recognize this threat and adopt rigorous compliance measures to ensure their platforms aren't abused by those looking to skirt identification requirements to evade sanctions.

In addition, there are no comprehensive, international standards for digital identification documents, though some countries have proposed legislation to change that. That lack of standards has created a global cybersecurity risk. Whether they fall into the synthetic or stolen category, fake digital identity documents allow cybercriminals — including nation state threat actors — to abuse cryptocurrency businesses by skirting their compliance processes and evading bans put in place to prevent money laundering and terrorist financing. As cryptocurrency and other digital payments systems continue to grow, the Financial Action Task Force (FATF) has recognized the problem and called for a more standardized digital identification system. The shutdown and sanctioning of SES reinforces the need for such measures.

In spite of these challenges, there have been clear successes in this area. FinCEN's 2013 guidance clarified that cryptocurrency exchanges must register as MSBs and maintain compliance programs in the United States. The 2015 initiative to include Malicious Cyber-Enabled designations and the 2018 initiative to include digital currency addresses as identifiers associated with designated individuals or entities have both been impactful. Using blockchain analysis, Chainalysis can see the effectiveness of including digital currency addresses as identifiers in designations. Our data demonstrates that after digital currency identifiers are included, little to no more money flows to these addresses, indicating the positive impact of blacklisting wallet addresses. The figure below demonstrates this.

Chart Showing Impact of OFAC Including "Digital Currency Addresses" As Identifiers in Designations of Individuals and Entities

Designating body	Sanction type	Sanctioned Entity	Sanction date	Cryptocurrency value received pre-sanction	Cryptocurrency value received post-sanction
OFAC	SDN	Anton Nikolaeyvich Andreyev	9/10/2020	$1,205.07	$0.00
OFAC	SDN	Danil Potekhin (ETH)	9/16/2020	$2,047,908.63	$0.00
OFAC	SDN	Danil Potekhin (BTC)	9/16/2020	$5,023,874.52	$0.00
OFAC	SDN	EnExchanger	11/28/2018	$1,219,123.55	$0.98
OFAC	SDN	Fujing Zheng	8/21/2019	$23,300.02	$1.21
OFAC	SDN	Iranvisacart	12/4/2018	$2,974,970.15	$6.66
OFAC	SDN	Mujtaba Ali Raza	4/20/2021	$9,128.03	$0.00
OFAC	SDN	Secondeye Solution	4/15/2021	$130,878.61	$0.00
OFAC	SDN	Xiaobing Yan	8/21/2019	$1,057,546.71	$7.79

Two bureaus within the U.S. Department of the Treasury– the Office of Foreign Assets Control (OFAC) and the Financial Crimes Enforcement Network (FinCEN)– have issued advisories related to facilitating ransomware payments and the sanctions risk that this poses. OFAC has also taken action against cryptocurrency exchanges that have violated sanctions. In December 2020 and February 2021, respectively, OFAC entered into settlements with cryptocurrency exchanges BitGo and BitPay for violations of multiple sanctions programs.

Recommendations for Ways to Improve the Current Sanctions Regime with Regards to Cryptocurrency

I would like to provide some recommendations for ways to improve the efficacy of the current sanctions regime with regards to cryptocurrency. These include 1) encouraging collaboration and information sharing with international partners, 2) increasing public-private partnerships, 3) increasing OFAC's resources to support more comprehensive targeting and designations of individuals, organizations, and services that facilitate sanctions evasion using cryptocurrency, and 4) the creation of a National Cryptocurrency Targeting Center to improve cross-agency collaboration to combat the illicit use of cryptocurrencies.

Recommendation 1: Encourage Collaboration and Information Sharing with International Partners

Collaboration and information sharing with our international partners is critical in this space and concerted efforts to improve international partnerships should be made. Increased cross-border cooperation between law enforcement agencies can go a long way towards mitigating sanctions evasion and other illicit uses of cryptocurrency, such as cryptocurrency exchange hacks and ransomware attacks. If financial intelligence units (FIUs) around the world can swiftly share the information they get, they may be able to freeze funds before illicit actors are able to move them to a mixer or low-KYC exchange.

Additionally, OFAC is currently the only sanctioning body that lists digital currency addresses. There is an opportunity to work with other international sanctioning bodies to help them initiate similar efforts. This would improve the impact of these sanctions. As our data demonstrates, when OFAC does include a digital currency address as an identifier for a sanctioned individual or entity, there are rarely future payments to that address. The inclusion of these identifiers is incredibly effective and should be increased. The more sanctions that are levied that include these sorts of identifiers, the more difficult it will be for these malicious actors to operate.

Recommendation 2: Increase Public-Private Partnerships

We recommend increasing and improving public-private partnerships in this space. The more information that is shared, the better able we are to combat illicit activities like sanctions evasion. There have been a number of legislative proposals, including the "Combating Illicit Finance Public-Private Partnerships Act'' and proposed OFAC Exchange Act, which would improve public-private information sharing opportunities among Federal agencies, financial institutions, and private sector experts in banking, national security, and law enforcement. We believe that these sorts of partnership proposals would be effective in improving the U.S. response to sanctions evasion, money laundering, terrorist financing, and other financial crimes.

Recommendation 3: Increase OFAC's Resources to Support More Comprehensive Targeting

We would also encourage more designations of illicit actors and those who facilitate their criminal activities. In order to enable this, OFAC's funding and resources should be increased. This would support their efforts to engage in more comprehensive targeting and designations of individuals, organizations, and services that facilitate sanctions evasion using cryptocurrency. We know that in the case of malicious cyber actors, such as ransomware attackers, bulletproof hosting services, VPN providers, Darknet markets, and/or online fraud shops are critical to their success. OFAC should designate more facilitators, much as they did with SES for providing fraudulent identification documents to malign foreign actors. OFAC routinely designates facilitators of terrorists and TCOs, and should employ the same tactic with those who enable malicious cyber actors. Since the

components of ransomware are often sold on Darknet markets and online fraud shops, OFAC should also consider designating those groups.

Recommendation 4: National Cryptocurrency Targeting Center

Finally, while there are a number of law enforcement agencies that have been building up their blockchain analysis capabilities, these efforts have been siloed and largely uncoordinated. To increase collective impact and achieve large-scale objectives, the U.S. should consider the creation of a National Cryptocurrency Targeting Center. This would house representatives from many U.S. government agencies, working together to combat the illicit use of cryptocurrencies. The center could also provide training opportunities to the member agencies to raise awareness of what indicators exist in an investigation to indicate that cryptocurrency might be being exploited, publish guides and reports on trends and how criminal techniques are changing, as well as best practices in investigations, and serve as an information sharing venue for law enforcement.

Conclusion

In closing, we applaud your efforts to improve the effectiveness of our sanctions. Cryptocurrency and blockchain technology offer the promise of bringing more people into the global financial system, but it's important to ensure malicious actors aren't abusing that promise. I therefore encourage you to consider the impact any potential legislation could have on technical innovation. While adversaries have quickly embraced cryptocurrency, sometimes for illicit purposes, we have found that not only are the vast majority of cryptocurrency transactions legitimate, the percentage of illicit use of cryptocurrencies is dropping. This may be due to greater awareness about blockchain analysis, which provides insights into transactions and trends that are invaluable to investigators. This sort of visibility is not possible with other forms of value transfer. We hope to see the United States lead on the cryptocurrency front — because if we don't, others will. Thoughtful regulation that promotes American innovation while supporting law enforcement and financial regulators will be crucial for the United States to maintain its position as the leader of the global financial system.

# # # # #