Written Testimony of Jonathan Levin
Co-Founder and Chief Strategy Officer
Chainalysis Inc.

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

Hearing on
Under the Radar: Alternative Payment Systems and the National Security Impacts of Their Growth

September 20, 2022

Chairman Himes, Ranking Member Barr, and distinguished members of the Committee. Thank you for inviting me to testify before you today. My name is Jonathan Levin and I am the Co-Founder and Chief Strategy Officer of Chainalysis. Chainalysis, founded in 2014, is the blockchain data platform. Chainalysis has served the cryptocurrency ecosystem for nearly a decade, developing investigative, compliance, and business intelligence solutions and building trust in blockchains.

I am honored to testify before you today on this important topic. I began studying cryptocurrencies ten years ago through my research as an economist at the University of Oxford. I was interested in the way that the internet could create brand new markets and impact developing economies.

In the '90s, many thought the idea that all companies would one day become internet companies was impossible. Now, it simply feels inevitable. We live in an increasingly digital world – in recent research, the Interactive Advertising Bureau found that the internet economy grew seven times faster than the total U.S. economy during the past four years, a sign that more commerce continues to happen online, whether it be through advertising, e-commerce, or other forms.

This transformation has brought citizens of the world closer together in terms of global connectivity, but it has not been accompanied by as many economic opportunities that were promised to individuals. Cryptocurrency technology provides a new way for people to interact and conduct global commerce, providing economic opportunities for people across the world. One day in the near future, all companies will be web3 companies and cryptocurrencies will be fully integrated into their businesses.

Web3 and the crypto rails upon which it is built will serve as the foundation for future e-commerce and it is vital that the U.S. understand the strategic relevance of these payment systems as payment rails shift. Our payment systems will need to be native to the internet in order to compete directly with China and other nations who are already embracing this future.

The United States has built and facilitated the safest and most mature financial system in the world by creating the guardrails upon which individuals and corporations have clear knowledge of property rights, counterparty risks and the cost of transacting. This has been established over decades by deputizing the creation of money through credit and the establishment of many alternative payment instruments to consumers that have ensured greater financial inclusion, lower costs and more options for online payments.

Cryptocurrencies provide entrepreneurs, creators and individuals with technology to create, interact, and transact in ways that are consistent with the U.S. values of individual creativity and economic freedom. This is in stark contrast to the alternative payment systems that are being proposed by China and other authoritarian regimes which may have very low costs but ultimately end in a state of surveillance and a lack of individual freedom. This becomes a geopolitical threat to the United States when these state-controlled digital currencies grow large enough to compete with the U.S. dollar.

The transparent, accessible, frictionless and borderless characteristics of cryptocurrency and web3 technology are the antidote to the goals of countries like China and their adoption of digital currencies: surveillance and total control of economic activity. However, this only happens if the U.S. embraces this technology.

Even in this 'crypto winter', our research shows that adoption of cryptocurrencies continues to grow, especially in emerging markets. As more people put a higher percentage of their net worth into cryptocurrency, they'll want the ability to use cryptocurrency for the full range of transactions they can currently carry out with fiat, such as lending and borrowing, trading assets, and payments. Web3 will enable them to do that with cryptocurrency faster and more easily than they can today.

Let's use mortgage approvals as an example. Today, borrowers need to go through a cumbersome mortgage application process that relies heavily on human judgment — judgment that studies show often reflects human biases and unfairly punishes marginalized communities. In a web3 world, that process becomes faster and fairer.

With the evolution of web3, we have seen new types of products and contracts taking advantage of the composability that blockchain technology affords. Web3 won't just streamline existing financial activity. It will also unlock new use cases in finance that currently aren't possible with traditional assets. We've only begun to scratch the surface of all that web3 can enable, but already we see a variety of different applications, including investing, borrowing, lending, art, entertainment, culture, decentralized autonomous organizations (DAOs), and digital identity.

The recent Biden Administration Executive Order on Ensuring Responsible Development of Digital Assets, which called for U.S. government agencies to come together and develop clear frameworks and policies around cryptocurrencies is an important start to U.S. leadership in this space. We have seen many reports in just the last week coming out of a

number of agencies, including the U.S. Department of Treasury, U.S. Department of Commerce, and U.S. Department of Justice, highlighting the important work they are doing in this space and their plans and recommendations for future coordinated interagency action to promote responsible innovation, reinforce the U.S. role in leadership in the global financial system, mitigate risks associated with cryptocurrency, protect global financial stability, and promote access to safe and affordable financial services. In addition, the recently-passed CHIPS and Science Act establishes a new position within the Office of Science and Technology Policy to advise the President on matters related to blockchain and cryptocurrencies. These are important steps and Congress and this administration should build upon them.

The U.S. must embrace blockchain and web3 technology in order to maintain economic dominance and ensure its national security. We have the opportunity to lead on this front and ensure that future payment systems are built by U.S. companies with U.S. principles in mind, and that these new payment rails, like past payment rails, become the new global standard. If the U.S. does not act quickly, it runs the risk of falling behind adversarial countries like China and Iran, which have already embraced this technology. Lawmakers and regulators should work with industry to implement reasonable regulations that will allow blockchain and web3 to flourish here in the United States. This will help to grow the cryptocurrency industry here, keeping high-paying jobs and economic activity here. Chainalysis, for example, has 850 employees, approximately 500 of whom are here in the U.S.

As with any new technology, cryptocurrency can be used by both good and bad actors. As such, preventing cryptocurrency from being abused by our adversaries is intricately linked to our continued ability to project prosperity around the world and maintain our national security. Embracing this industry will also help to ensure that businesses stay within the U.S.'s regulatory parameters, rather than moving to jurisdictions that do not regulate cryptocurrency businesses or are viewed as "friendlier" regulatory environments. This is critical from a national security perspective. In government investigations into the illicit use of cryptocurrency, it is important that they be able to identify cash out points in regulated countries in order to obtain identifying information about suspects. In a recent report from the U.S. Department of Justice, titled *How To Strengthen International Law Enforcement Cooperation For Detecting, Investigating, And Prosecuting Criminal Activity Related To Digital Assets*, they note "To effectively combat crime involving cryptocurrency and other digital assets, law enforcement must be able to rapidly obtain evidence concerning the crimes." The report specifically cites different record keeping standards and anti-money laundering/countering the financing of terrorism (AML/CFT) standards for cryptocurrency businesses abroad as a challenge that can impede or stall criminal investigations. It is important to government investigations that law enforcement be able to obtain information from cryptocurrency businesses when alternative payment systems like cryptocurrency are exploited by criminals. When these businesses are in unregulated countries, this process becomes much more difficult and is not always possible.

One point I want to make sure I highlight to the members of this Committee, is that the transparency of cryptocurrency blockchains enhances the ability of policymakers and government agencies to detect, disrupt and, ultimately, deter illicit activity. By mapping a single illicit actor to a cryptocurrency wallet address– for example from a payment made to a ransomware group– law enforcement unlocks immediate insight into the network of wallet addresses and services (e.g., exchanges, mixers, etc.) that facilitate the illicit actor. In contrast, in a traditional finance investigation, a similar tip linking an illicit actor to a bank account is just the beginning of a long, extensive process to request and subpoena records that are manually reviewed and reconciled to generate a comparable amount of insight.

In my testimony, I discuss global trends in cryptocurrency, provide background on Chainalysis, outline how blockchain analysis can be leveraged in investigations, and provide an overview of some of the national security threats we see related to cryptocurrency, including from nation-state actors aligned with North Korea, Iran, Russia, and China. I also provide recommendations for improving the government's national security position in relation to cryptocurrency.

Global Trends in Cryptocurrency

Along with the evolution of different use cases in this space, we have seen global adoption of cryptocurrency evolve around the world. Global adoption of cryptocurrency reached its current all-time high in Q2 2021. Since then, adoption has moved in waves – it fell in Q3, which saw crypto price declines, rebounded in Q4 when we saw prices rebound to new all-time highs, and has fallen in each of the last two quarters as we've entered a bear market. Still, it's important to note that global adoption remains well above its pre-bull market 2019 levels. Our data suggests that many of those attracted by rising prices in 2020 and 2021 stuck around, and continue to invest a significant chunk of their assets in cryptocurrencies.

Emerging markets dominate our 2022 Global Crypto Adoption Index, which is designed to measure grassroots adoption of cryptocurrencies. The World Bank categorizes countries into one of four categories based on income levels and overall economic development: high income, upper middle income, lower middle income, and low income. Using that framework, we found that the middle two categories dominate the top of our index. Out of our top 20 ranked countries, the majority are middle or upper middle income countries:

- Middle income: Vietnam, Philippines, Ukraine, India, Pakistan, Nigeria, Morocco, Nepal, Kenya, and Indonesia
- Upper middle income: Brazil, Thailand, Russia, China, Turkey, Argentina, Colombia, and Ecuador
- High income: United States and United Kingdom

Users in lower middle and upper middle income countries often rely on cryptocurrency to send remittances, preserve their savings in times of fiat currency volatility, and fulfill other

financial needs unique to their economies. These countries also tend to lean on Bitcoin and stablecoins more than other countries.

Around the world, not only have we seen cryptocurrencies and digital assets embraced, but many countries are developing their own digital versions of their central bank money. According to the Atlantic Council, 11 countries have launched central bank digital currencies (CBDCs), while another 14 countries (including China) are in the pilot phase of their CBDC project, and another 73 are either developing or researching a CBDC.

Here in the U.S., according to a study conducted by Pew Research, 16% of Americans say they personally have invested in, traded or otherwise used cryptocurrency. According to the recent *Economic Well-Being of U.S. Households in 2021* survey from the Federal Reserve System Board of Governors, while only 3% of people used cryptocurrencies for payments or transfers, 13% of those people who used cryptocurrency for payments or transfers did not have a bank account. This shows how cryptocurrency is already being explored as a means for the underbanked and unbanked to attain greater financial inclusion. Cryptocurrencies are also increasingly used as a fast, low-cost way to send remittances using solutions like the one that Stellar has developed. This rapid and far-reaching expansion of cryptocurrency adoption around the world further demonstrates the importance of U.S. leadership in this space.

Background on Chainalysis

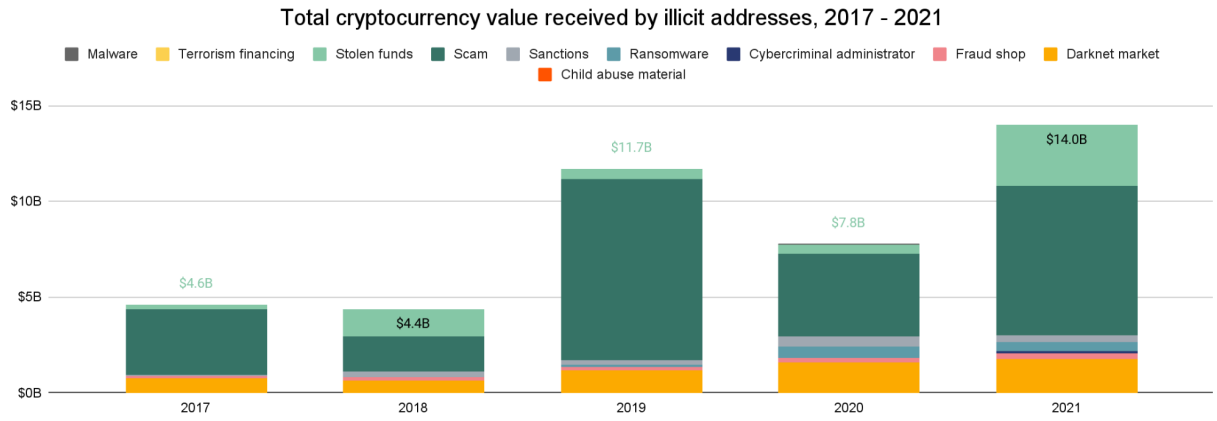
Chainalysis is the blockchain data platform. We provide data, software, services, and research to government agencies, exchanges, financial institutions, and insurance and cybersecurity companies. Chainalysis currently has over 850 customers in 70 countries. Our data platform powers investigations, compliance, and risk-management tools that have been used to solve many of the world's most high-profile cyber-crime cases and grow consumer access to cryptocurrency safely. We have worked closely with law enforcement and regulators as they have worked to disrupt and deter illicit uses of cryptocurrency.

Chainalysis's partnerships with law enforcement and regulators are consistent with our corporate mission: to build trust in blockchains. Fundamentally, we believe in the potential of open, decentralized blockchain networks to drive new efficiencies, reduce barriers for innovators to create new financial and commercial products, encourage innovation, enhance financial inclusion, and unlock competitive forces across financial services and other markets. Our goal is to contribute our data, tools and expertise to drive illicit finance and other risks out of the cryptocurrency ecosystem, enabling the realization of the technology's potential.

Chainalysis's data powers both investigative and compliance tools. Our investigative tool, Reactor, enables government agencies and investigative teams to trace the illicit uses of cryptocurrency, including money laundering, theft, scams, and other criminal activities. Our compliance tool, KYT (Know Your Transaction), provides cryptocurrency businesses and financial institutions the ability to screen their clients' transactions and ensure that they are

not attempting to interact with illicit services. This transaction monitoring tool provides ongoing insights for cryptocurrency businesses so that they can protect their businesses and clients and meet their regulatory obligations.

Chainalysis also leverages our data to conduct research into the cryptocurrency ecosystem, including the illicit use of cryptocurrency. We publish a number of reports, including our annual Crypto Crime Report. Based on this research, we reported in our 2022 Crypto Crime Report that cryptocurrency-based crime hit a new all-time high in 2021, with illicit addresses receiving $14 billion over the course of the year, up from $7.8 billion in 2020. Top categories include scams, stolen funds, darknet markets, and ransomware. We always caveat these figures, noting that these numbers are the floor, not the ceiling. Our data improves as we learn more about different activities and map out more services, and these numbers will change as we incorporate new information into our data. These numbers also only account for funds derived from "cryptocurrency-native" crime, meaning cybercriminal activity such as darknet market sales or ransomware attacks in which profits are virtually always derived in cryptocurrency rather than fiat currency.



Despite this large increase in illicit transaction volume, illicit activity as a percentage of total volume has actually fallen since 2019. In 2019, the illicit share was about 3%, in 2020 it was just over 0.5%, and in 2021 it was 0.15%. The reason for this is that cryptocurrency usage is growing faster than ever before, so while cryptocurrency-related crime is definitely increasing, the legitimate use of cryptocurrency is far outpacing its use by illicit actors. This is good news for the cryptocurrency ecosystem, but government and industry must still put in place and implement the appropriate controls to mitigate risks in the system.

How Blockchain Analysis Can Be Leveraged in Investigations

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 that of other traditional forms of value transfer. Cryptocurrencies like Bitcoin operate on public, immutable ledgers known as blockchains. Anyone with an internet

connection can look up the entire history of transactions on these blockchains. The ledger shows a string of numbers and letters that transact with another string of numbers and letters. Chainalysis maps these numbers and letters – cryptocurrency addresses – to their real-world services. For example, in Chainalysis products, we are able to see that a given transaction was between a customer at a specific exchange, with a customer at another exchange, between a customer 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 empowering government and private sector 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 addresses to identify the origination and/or cashout points at cryptocurrency exchanges. Law enforcement can serve legal process to these cryptocurrency exchanges, which are required to register as money services businesses (MSBs) here in the United States and collect Know Your Customer (KYC) information from their customers. In response to a subpoena, the exchange will provide law enforcement with any identifying information that it has related to the cryptocurrency transaction(s) in question, such as name, address, and government identification documentation, allowing authorities to further their investigation.

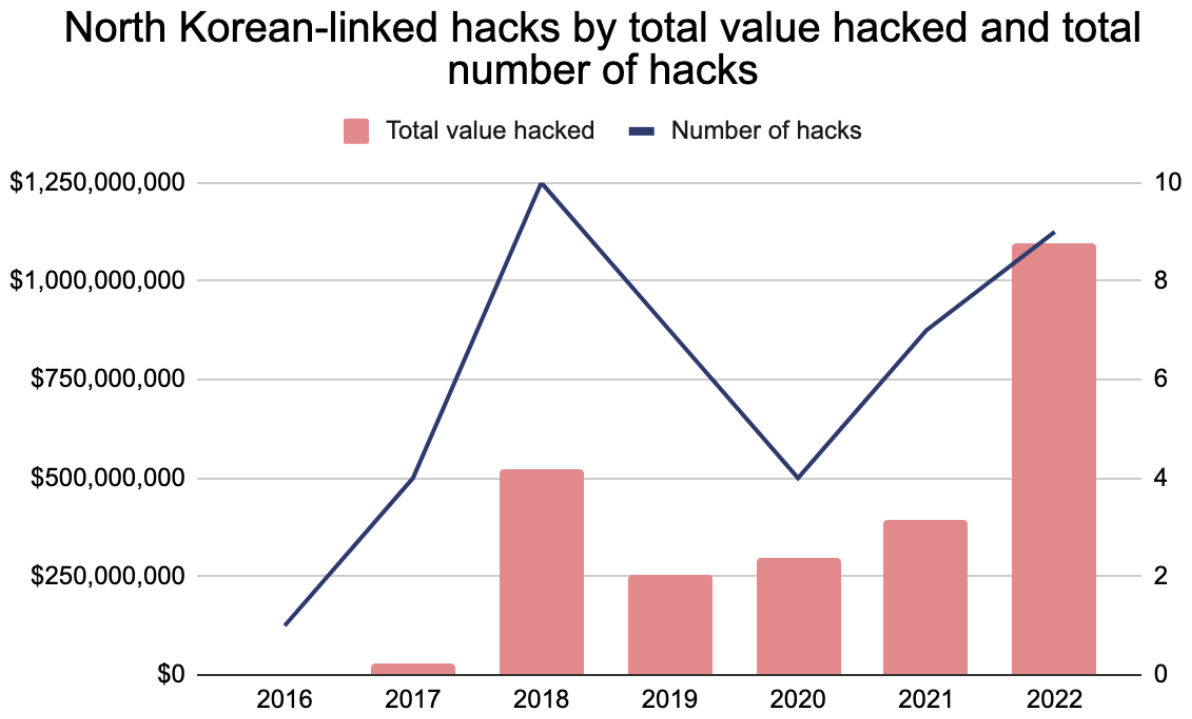
Starting with one cryptocurrency address, from a ransomware payment for example, an investigator can identify not only which address currently holds the funds, but which other addresses are associated with that ransomware actor, as well as which facilitating tools and services enable their attacks, such as access brokers, VPN providers or bulletproof hosting services, and which other groups these actors may be collaborating with. We can tell when members of one group are tied to a new group, whether that is a rebrand, or simply collaboration with another group. This provides invaluable insight into criminal networks and allows government agencies to better prioritize their efforts - and the blockchain trail has time and time again led to outcomes like attribution and even arrest of the perpetrator and asset seizure.

National Security and Cryptocurrency

While, as I have already noted, the overall percentage of illicit activity in cryptocurrency is very small, we do see a number of different adversaries engaged in illicit activities. This is concerning from a national security perspective and should be taken seriously. We must arm our government intelligence and investigative agencies with the right resources and tools to effectively go after these malign foreign actors and mitigate the threat they pose to our national security. I will cover four adversarial countries in my testimony and how they are using cryptocurrencies: North Korea – or the Democratic People's Republic of Korea (DPRK), Iran, Russia, and China.

North Korea

North Korean cybercriminals launched numerous attacks on cryptocurrency platforms over the past few years. Chainalysis estimates that DPRK actors were able to extract nearly $400 million worth of cryptocurrency last year. In 2022, they have already surpassed this number, stealing more than $1 billion from cryptocurrency platforms. Given that North Korea's trade was just $710 million in 2021, the amount of cryptocurrency they are able to steal in these thefts is alarming. And according to the UN security council, the revenue generated from these hacks goes to support North Korea's WMD and ballistic missile programs.



These attacks target investment firms, centralized exchanges, and, increasingly, decentralized exchanges and protocols using phishing lures, code exploits, flash loan attacks, malware, and advanced social engineering to siphon funds out into DPRK-controlled addresses. Once North Korea gains custody of the funds, they begin a careful laundering process to cover up and cash out.

These complex tactics and techniques have led many security researchers to characterize cyber actors for the DPRK is especially true for North Korean hacking group, the "Lazarus Group," which is led by DPRK's primary intelligence agency, the U.S.- and UN-sanctioned Reconnaissance General Bureau. While we will refer to the attackers as North Korean-linked hackers more generally, many of these attacks were carried out by the Lazarus Group in particular.

Lazarus Group first gained notoriety from its Sony Pictures and WannaCry cyberattacks, but it has since concentrated its efforts on cryptocurrency crime—a strategy that has proven

immensely profitable. From 2018 on, the group has stolen and laundered massive sums of virtual currencies every year, typically in excess of $200 million. In March 2022, DPRK was responsible for a theft of more than $600 million from Ronin Network, a sidechain built for the web-based NFT game Axie Infinity. In April 2022, the U.S. Department of Treasury's Office of Foreign Assets Control (OFAC) updated the SDN List to include cryptocurrency addresses as identifiers for the Lazarus Group. This update confirmed that North Korea had been responsible for the hack of the Ronin bridge attack.

Cryptocurrency's transparency is instrumental to investigating hacks like the one suffered by Axie Infinity. Investigators with the right tools can follow the money to understand and disrupt a cybercrime organization's laundering activities. This would never be possible in traditional financial channels, where money laundering usually involves networks of shell companies and financial institutions in jurisdictions that may not cooperate.

In fact, because of the transparency of cryptocurrency, Chainalysis can tell you exactly what happened in the Ronin hack and how the stolen funds were laundered. The attack began when the Lazarus Group gained access to five of the nine private keys held by transaction validators for Ronin Network's cross-chain bridge. They used this majority to approve two transactions, both withdrawals: one for 173,600 ether (ETH) and the other for 25.5 million USD Coin (USDC). They then initiated their laundering process – and Chainalysis began tracing the funds. The laundering of these funds has leveraged over 12,000 different crypto addresses to-date, which demonstrates the hackers' highly sophisticated laundering capabilities.

There is good news here – law enforcement was able to seize more than $30 million worth of cryptocurrency stolen by these North Korean-linked hackers in this case. This marks the first time ever that cryptocurrency stolen by a North Korean hacking group has been seized, and we're confident it won't be the last.

These seizures would not have been possible without collaboration across the public and private sectors. Much of the funds stolen from Axie Infinity remain unspent in cryptocurrency wallets under the hackers' control. This example underscores the importance of public-private partnerships in promoting our national security.

Iran

Iran's Use of Cryptocurrency in Cross-Border Payments

Iran faces some of the most extensive US sanctions of any country. The Iranian government, including former Iranian President Hasan Ruhani, and several Islamic Revolutionary Guard Corps (IRGC) generals have publicly

endorsed the use of cryptocurrency, including the launch of a central bank digital currency (CBDC), for the explicit purpose of circumventing sanctions.

On August 9, 2022, Iran's Deputy Minister of Industry, Mine & Trade Alireza Peyman-Pak tweeted that Iran had placed its first import order using $10 million worth of cryptocurrency and that, "By the end of September, the use of cryptocurrencies and smart contracts will be widely used in foreign trade with target countries." While Iran's imports using cryptocurrency have not yet been confirmed, two weeks later, on August 29, 2022, Iran's government approved regulations for trading with cryptocurrencies, a move that potentially allows the country to skirt some U.S. financial sanctions imposed over Tehran's nuclear program.

Iran & Cryptocurrency Mining

As one of the world's largest energy producers, Iran has the low-cost electricity needed to mine digital assets like Bitcoin cheaply, providing an injection of monetary value that sanctions can't stop. Our research indicates Iranian Bitcoin mining is well underway at a surprisingly large scale. From 2015 to 2021, we found that Bitcoin mining funneled more than $186 million into Iranian services, most of it within the past year. Iranian state actors are well aware of the opportunity. In 2019, the Iranian government created a licensing regime for cryptocurrency mining. And in March 2021, a think tank tied to the President's office released a report stressing its benefits. The government has actively solicited mining projects to set up shop in the country and take advantage of its low-priced power. They've granted over 1000 licenses to mining operations and according to our data, nearly 17% of funds moving to local Iranian services come from mining entities, compared to just 5% for Middle East-based services overall.

Iranian Ransomware Actors

Iranian ransomware attackers also pose a national security threat. Cybersecurity analysts at Crowdstrike and Microsoft have concluded that many attacks by ransomware strains affiliated with Iran, mostly targeting organizations in the U.S., the E.U., and Israel, leveraging ransomware for financial gain, or objectives of causing disruption or serving as a ruse to conceal espionage activity. Generally speaking, Chainalysis has seen significant growth over the last year in the number of ransomware strains attributed to Iranian cybercriminals in the past year.

Earlier this month, OFAC designated Iran's Ministry of Intelligence and Security (MOIS) and its head, Esmail Khatib, citing their involvement in "cyber espionage and ransomware attacks in support of Iran's political goals." Just last week, the OFAC designated ten individuals and two entities affiliated with Iran's IRGC for their roles in conducting malicious cyber acts, including ransomware activity. According to OFAC, "this IRGC-affiliated group is known to exploit software vulnerabilities in order to carry out their ransomware activities, as well as engage in unauthorized computer access, data exfiltration, and other malicious cyber activities."

In the designation, OFAC listed six cryptocurrency addresses as identifiers for two of the IRGC-affiliated individuals designated for their roles in targeting various networks–including attacks on critical infrastructure–by exploiting well-known vulnerabilities to gain initial access in furtherance of malicious activities, including ransom operations. OFAC specifically cited their role in a February 2021 cyber attack on a New Jersey municipality, a June 2021 system compromise of a U.S.-based children's hospital, and other attacks targeting transportation providers, healthcare practices, emergency service providers, and educational institutions. At the same time, the Federal Bureau of Investigation announced the indictment of three of these Iranian nationals for their roles in a multi-year scheme to compromise the networks of hundreds of companies.

While some Iranian ransomware strains may be used in conventional, financially-motivated attacks by cybercriminals operating in the country, other strains behave more like tools of espionage, extorting negligible amounts of cryptocurrency from victims. Ransomware is a useful cover for strategic denial and deception against enemy states because attacks can be carried out cheaply, and it gives the attacking nation some measure of plausible deniability, as they can always claim the attack was carried out by mere cybercriminals or another nation state.

Earlier this month, a joint Cybersecurity Advisory was released by the Federal Bureau of Investigation, the Cybersecurity and Infrastructure Security Agency, the National Security Agency, U.S. Cyber Command-Cyber National Mission Force, the Department of the Treasury, the Australian Cyber Security Centre, the Canadian Centre for Cyber Security, and the United Kingdom's National Cyber Security Centre on malicious cyber activity by advanced persistent threat (APT) actors affiliated with the IRGC, highlighting the continued threat to national security these actors pose.

It is important to remember that even ransomware attacks carried out for non-financial reasons leave a trail on the blockchain. For that reason, it's crucial that agencies focused on national security understand how to trace funds using blockchain analysis, as this is the key to identifying the individuals involved in the attacks themselves, the tools they use, and how they launder any funds obtained from victims.

Russia

Russian Use of Cryptocurrencies and CBDCs in Cross-Border Payments

While cryptocurrency is technically banned in Russia, like Iran, Russian plans to use cryptocurrency for cross-border transactions. Just this month, Russian Prime Minister Mikhail Mishustin officially instructed the government to come to a consensus regarding cryptocurrency regulation in Russia by December 19, 2022. He has called for coordinated policies on regulating the issuance and circulation of cryptocurrencies in Russia and asked regulators to finalize regulations for cryptocurrency mining and cross-border transactions in cryptocurrencies. In addition, according to the last monetary policy update from the Bank of

Russia, Russia is also planning to roll out the digital ruble in the next few years, and will begin to connect banks to the digital ruble platform in 2024.

Now-sanctioned oligarch Vladimir Potanin has said the digital ruble and tokens may replace "unregulated" cryptocurrency. He made these comments after Russia's Central Bank gave the local blockchain platform, Atomyze, a license to issue and exchange digital financial assets. Atomyze platform uses blockchain to digitize real assets (like real estate or metals) and convert them into tokens that can be easily exchanged, which allows them to organize the circulation of tokens backed by goods or money on its blockchain platform. These sorts of capabilities may enable Russia's ability to circumvent sanctions to some degree.

Russia-Based High-Risk Exchanges

Interestingly, in spite of the supposed cryptocurrency ban, Russia still ranks #9 on the Chainalysis 2022 Global Crypto Adoption Index, which we released last week. We also know from our research that there are a number of cryptocurrency exchanges based in Moscow City, Russia. Many of these exchanges facilitate significant amounts of money laundering. OFAC has sanctioned several of these exchanges, including Suex, Garantex, and Chatex, which both operated out of the same Moscow City skyscraper: Federation Tower East. While Suex and Chatex have both ceased to operate following their designations by OFAC, Garantex still has existing operations. Nothing is more emblematic of the growth of Russia's crypto crime ecosystem, and of cybercriminals' ability to operate with apparent impunity, than the presence of so many cryptocurrency businesses linked to money laundering in one of the capital city's most notable landmarks.

For some Moscow City cryptocurrency businesses, illicit funds make up as much as 30% or more of all cryptocurrency received, which suggests those businesses may be making a concerted effort to serve a cybercriminal clientele. These sorts of high-risk exchanges are favored by criminal groups, including ransomware groups, as cash out points because they provide an unregulated venue for converting cryptocurrency to fiat without going through the customer due diligence and recordkeeping obligations that exchanges require in parts of the world that regulate cryptocurrency businesses. The use of these sorts of exchanges can stymie investigations in which law enforcement officers seek to find the identity of illicit actors to bring them to justice.

Russian Ransomware actors

As with Iranian ransomware attacks, some Russian ransomware attacks appear to align with geopolitical objectives or employ ransomware as a cover for these goals and Russian ransomware actors are some of the most prolific. Individuals and groups based in Russia — some of whom have been sanctioned by the United States in recent years — account for a disproportionate share of activity in several forms of cryptocurrency-based crime. Chainalysis data suggests roughly 75% of ransomware revenue in 2021 went to strains we can say are highly likely to be affiliated with Russia in some way.

One indication of geopolitical motivations in ransomware attacks is that some of the most pervasive ransomware strains avoid targeting Commonwealth of Independent States (CIS), including Russia, and will fail to encrypt if they detect the operating system is located in a CIS country. Where that fails, ransomware operators have been identified returning decryptors in cases of inadvertent targeting of Russian entities. This suggests at least a tacit tolerance of ransomware activities by the Russian government. In addition, the Russian government has been very reluctant to pursue these groups. In January 2022, Russia arrested 14 alleged members of the REvil ransomware gang, but in June 2022, reports indicated that they intended to drop most of the charges and were "mulling a deal to put the hackers to work for state security services 'in the fight against hackers from Ukraine.'" In other cases, ransomware groups like Evil Corp have been explicitly tied to the Russian government.

In cases where a ransomware strain contains no mechanism to collect payment or allow victims to recover their files, we can be more certain that money isn't the attackers' primary motivation. That's exactly what we saw in a ransomware attack on Ukrainian government agencies by hackers believed to be associated with the Russian government. As the Computer Emergency Response Team of Ukraine (CERT-UA) describes here, a cyber attack occurred on January 13, 2022, disrupting several government agencies' ability to operate. The attack appeared like a ransomware incident, replete with a note and cryptocurrency address provided for payment, that actually belied a malicious wiper known as WhisperGate, that was deleting data at Ukrainian entities. Interestingly, CERT-UA released a report showing that the wiper contains code repurposed from WhiteBlackCrypt, a ransomware strain active in 2021 that was also designed to wipe victims' systems rather than extort them for money.

As the Russian war with Ukraine has continued, there have been an increase in attacks targeting Ukraine that appear aligned with Russian geopolitical goals. An analysis from the Threat Analysis Group (TAG) outlined five different campaigns carried out between April and August 2022 whose activities overlap with a group that the CERT-UA tracks. TAG believes that this group is made up of "former members of the Conti cybercrime group repurposing their techniques to target Ukraine."

We saw a similar situation unfold in 2017, when the Russia-based NotPetya ransomware strain, which contained no viable payment mechanism, targeted several Ukrainian organizations and was also widely judged to be a geopolitically motivated disruption attempt by the Russian military rather than a money-making effort.

Cryptocurrency Fundraising by Pro-Russian Groups

As Russia's war in Ukraine has continued, Russian forces have been accompanied by various militia groups and emboldened by war propaganda. A number of volunteer groups and their supporters have taken to social media to crowdfund military purchases and the spread of disinformation by soliciting cryptocurrency donations. Since the start of the war, Chainalysis has identified 54 such organizations that have collectively received over $3.5

million worth of cryptocurrency, primarily from Bitcoin and Ether donations. Considerable quantities of Tether, Litecoin, and Dogecoin have been sent as well. Roughly half of the donation-collecting accounts have publicly solicited support for militias located in the Donbas region of Ukraine, specifically Donetsk and Luhansk – two territories subject to comprehensive OFAC sanctions as of February 22.

Most of the cryptocurrency donated thus far have been sent to just a few organizations in particular. The cryptocurrency donations sent to these organizations have reportedly been used to support everything from the financing of pro-Russian propaganda sites to the purchase of military items, like drones, weapons, bulletproof vests, communication devices and various other supplies.

Because public blockchains are transparent, we can follow each transfer in these accounts' chains of payments, gleaning insights into pro-Russian activities that would be harder to extract from fiat money investigations. In fact, just last week, OFAC sanctioned Task Force Rusich, one of the above-referenced Russian paramilitary organizations affiliated with Wagner Group, operating in Ukraine — five cryptocurrency addresses we analyzed then were included as identifiers in Rusich's OFAC designation.

Chainalysis continues to work with our partners in the public and private sectors to track these accounts and add new ones as they are identified. We also continue to pay close attention to further indicators of Russian sanctions evasion and cryptocurrency-based money laundering.

China

China and Cryptocurrency

China has historically been one of the largest cryptocurrency markets that Chainalysis studies. China's cryptocurrency industry and user base is one of the most active in the world. China has also historically dominated cryptocurrency mining. At times, China-based mining operations have controlled as much as 65% of Bitcoin's global hashrate — the measurement of how much computing power goes toward mining Bitcoin — which has led to increased liquidity for cryptocurrency services serving China and Asia as a whole, but also concerns that the Chinese Communist Party (CCP) could leverage this control to harm the Bitcoin network. Historical transaction data also suggests that some Chinese cryptocurrency businesses, especially over-the-counter (OTC) brokers, have played an outsized role in facilitating money laundering for those involved in cryptocurrency-based crime.

However, in September 2021, government officials cracked down on cryptocurrency mining and trading, with the global hashrate falling as many Chinese miners paused operations. Interestingly, in spite of the supposed crackdown in China on cryptocurrency trading, China still ranks #10 on Chainalysis 2022 Global Crypto Adoption Index. Our sub-indexes show that China is especially strong in usage of centralized services, placing second overall for purchasing power-adjusted transaction volume at both the overall and retail levels. This is

especially interesting given the Chinese government's crackdown on cryptocurrency activity, which includes a ban on all cryptocurrency trading announced in September 2021. Our data suggests that the ban has either been ineffective or loosely enforced. The industry is generally in agreement that China has dramatically diverted from bitcoin use to altcoins and stablecoins and it's likely that an extensive amount of the activity is conducted on blockchains other than Bitcoin or Ethereum.

China's Digital Yuan

In April 2020, China began testing the digital yuan, becoming one of the first governments to issue a CBDC. CBDCs like the digital yuan (also called the e-CNY) are government-issued, digital versions of a country's national currency. Like most conventional cryptocurrencies, CBDCs would provide greater transparency into how people spend in the aggregate, as the currency's blockchain would act as a permanent, immutable ledger of all transactions. China is rolling out the digital yuan through state-owned banks and digital payment apps like WeChat Pay and AliPay, which are much more widely used in China than their American or European counterparts. Digital yuan trials are ongoing, and many pointed to Beijing's 2022 Winter Olympics as the government's occasion to unveil its new CBDC to the world, as it planned to issue the digital yuan to visiting athletes. According to reports, the digital yuan was used to make 2 million yuan ($315,761) or more of payments a day at the Beijing Winter Olympics, per an official from the Chinese central bank.

According to the Economist, 260 million people and 4.5 million businesses can now use the digital yuan. "Thanks to promotions and handouts, the digital currency has been used in over 260m transactions worth about 83bn yuan ($12bn) since its inception until the end of May, with an average transaction size of about 300 yuan." The digital yuan was designed for retail use so as to be able to rival private payment platforms like Alipay and WeChat Pay. It could improve the government's ability to manage the Chinese economy, but many have expressed concern that the digital yuan will be used as a tool for financial surveillance, and could be a means of subverting U.S. imposed sanctions, as well as the U.S. dollar's position as the world's reserve currency.

Chinese Cyber Actors

Like Iran and Russia, China employs cyber attacks as a geopolitical tool. According to a Bloomberg article, "For more than a decade, Chinese hackers have waged a persistent cyber offensive against Taiwanese government, non-government and corporate targets. Taiwan also happens to be home to some of the electronics, semiconductor and military technology that China desperately wants to get its hands on." These attacks are often used as means to steal sensitive information, such as trade secrets, rather than to demand ransom. However, analysts have also identified instances of ransomware strains affiliated with China, such as ColdLock, carrying out geopolitical attacks on Taiwanese organizations, and Taiwanese authorities have indicated they believe Chinese hackers to be behind attacks on Taiwan's state oil company.

Recommendations

In order to promote U.S. national security, the U.S. can take a number of steps. These include 1) embracing web3 technology and providing regulatory clarity, 2) ensuring U.S. government agencies have the tools, training, and resources they need to conduct and coordinate investigations into the criminal use and national security impacts of cryptocurrency, and 3) improve public-private partnerships. I will detail these recommendations further below.

Embrace web3 technology and provide regulatory guidelines that enable industry to flourish.

The U.S. must embrace this technology and provide clear, workable guardrails for industry participants. While cryptocurrency businesses have been subject to anti-money laundering laws since at least 2013, there are other aspects of the market that still require additional clarification, including direction from Congress. Providing market clarity will support the goals of economic growth and leadership in the U.S. If the U.S. wants to lead in the cryptocurrency sector, we must lead in clear, reasonable cryptocurrency regulation. Clarifying roles around cryptocurrency regulation at the federal level would be a very important step for this market and would help to lend a greater degree of order and enable the industry to grow safely in the U.S.

Ensure adequate funding, resources, and training for government agencies charged with investigating and analyzing the illicit use of cryptocurrency and improve coordination.

As criminals, nation states, and adversaries adopt cryptocurrencies and cryptocurrency technology, governments must keep up with the latest techniques and tactics. Governments that have already embraced blockchain analysis tools have gained invaluable insight and been able to analysis networks and seize millions of dollars in cryptocurrency—further evidence that with the proper tools, investigators can cut off terrorist organizations the funds they need to survive, operate, procure weapons, and carry out attacks. Many government agencies have limited or inconsistent personnel dedicated to investigating and analyzing the illicit use of cryptocurrency. This is often because of a lack of training resources and a lack of funding for new personnel and tools. Allocating appropriate financial and personnel resources to these efforts would ensure that investigators can trace illicit transactions, seize funds, and help bring criminals to justice when criminals exploit cryptocurrency.

In addition to ensuring adequate resourcing, improving coordination among agencies is key. 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 Coordination Center. This would house representatives from many U.S. government agencies, working together to investigate and 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 have been exploited, publish resources and reports on trends and how criminal techniques are changing, as well as best practices in investigations, and serve as an information sharing venue private sector liaison efforts.

Improve and augment 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. The U.S. Department of Treasury's Financial Crimes Enforcement Network ("FinCEN") Exchange program, which brings together representatives from FinCEN, law enforcement, regulators, and industry members in a voluntary public-private information-sharing partnership is an example that should be looked to and expanded upon wherever possible. These exchanges enable FinCEN to collect and share information in a less formal setting, as well as learn about challenges faced by industry members in their efforts to prevent illicit finance. These sorts of public-private partnerships help to build and improve relationships and sharing mechanisms between the involved parties, with the shared goal of preventing illicit financing and protecting national security. They are also key in an industry that is fast growing and fast evolving – these relationships enable the public sector to better understand what is happening in the private sector and gain key insights that would not be possible without these interactions. Expanding public-private information sharing opportunities among Federal agencies, financial institutions, and private sector experts in banking, national security, and law enforcement is key to improving the U.S. response to illicit financing.

Conclusion

Today, we are living in an increasingly digital world and web3 technology will be foundational to addressing people's desire for fast, frictionless payment systems. These technologies are also some of the best available tools in the toolkit that the United States has to compete with potential national security threats, like ransomware attacks and North Korean hackers. The entrepreneurial dynamism that cryptocurrencies present allows for innovators and builders to create universal access to financial products and re-engineer web2 business models to serve individuals and their data in a way that protects privacy and helps our communities. This technology is consistent with our American values and has the potential to be strategically more important in great power competition over the next few decades. Of course, we understand concerns about risk and that is why we are here today, but at Chainalysis we know that the inherent open nature of this technology can be leveraged to mitigate the risks associated with it. Cryptocurrency's transparency allows for not only the disruption of illicit financing networks, but also the identification, arrest, and prosecution of bad actors. By providing the resources necessary to understand this threat, law enforcement, the intelligence community, and the U.S. government as a whole will be better equipped to mitigate risks and investigate and disrupt national security threats.