Chainalysis

# The Role of Cryptocurrency Analysis in Decision Dominance on the Blockchain

**Prepared for:**

TechNet Indo-Pacific 2022

Submitted by:
**Customer POC:** Paul Bence, DoD Account Executive
paul.bence@chainalysis.com
(770 )363-2491
**Technical POC:** Connor McAuliffe, Solutions Architecture
connor.mcauliffe@chainalysis.com
www.chainalysis.com

*This response includes data that shall not be disclosed outside the Government and shall not be duplicated, used, or disclosed—in whole or in part—for any purpose other than to evaluate this submission. However, if a contract is awarded to Chainalysis as a result of—or in connection with—the submission of these data, the Government shall have the right to duplicate, use, or disclose the data to the extent provided in the resulting contract. This restriction does not limit the Government's right to use information contained in these data if they are obtained from another source without restriction.*

**Executive Summary:** Chainalysis data is used by the DoD/IC to understand the interwoven cyber and physical operational environment. National security threats, including state and non-state actors, use cryptocurrency to facilitate ransomware payments, conduct cyber operations, and evade sanctions, but the exchange of digital assets leaves key intelligence for analysts to collect. Additionally, Chainalysis has an award-winning capability to combine blockchain data with other forms of cyber data to provide a holistic understanding of the relationships, patterns, behaviors and activities of our adversaries. This data fusion provides a foundation for cyber teams to proactively mitigate ransomware risks and act swiftly to neutralize even the most advanced cybercriminals. Moreover, Chainalysis has worked collaboratively with industry partners in the past to bring the right solution to the customer, and remains open to taking that approach if the case arises.

Cryptocurrencies present a new and emerging threat to national security. Speed, accuracy and reliability are essential elements to data and information in the digital age. Access to blockchain data is a quintessential next step for the DoD/IC to take as it looks to integrate cutting-edge data streams.

Chainalysis seeks to support the DoD/IC in its efforts to integrate and conduct cyberspace operations by ensuring decision dominance on the blockchain while denying the same to our adversaries. Cryptocurrencies empower our enemies with ever-greater ways to exchange value, and having analytic processes to synthesize, filter and make sense of this value transfer data in real time is essential. This whitepaper outlines how Chainalysis leverages its best in class datasets to affect national security through our clientele, outlines our proposed work with our customers, highlights a growing list of operational achievements, and introduces a case study on how cryptocurrency analysis was integral in identifying weapons, ammunitions, and the risk of Chinese cryptocurrency mining despite its nationwide crackdown in May 2021.

**Technology Concept:** Chainalysis maintains the world’s largest database mapping cryptocurrency transactions to real world entities. As the first movers in this space, Chainalysis has been collecting and enriching blockchain data and linkages to real world entities since 2014. Our Bulk Data and Investigations API (IAPI) consists of $13.6T in named received value, 10,930 unique entities, and 30,510 named entities across all assets. Additionally, Chainalysis implements a robust and multi-layered validation process that includes ground-truth manual review to mitigate false positives. This saves time and prioritizes your efforts on the most critical analysis. Furthermore, all Chainalysis data attributions and labeling is auditable.

Chainalysis examines public blockchain data from its beginning to assess the entire history of transactions. Using deterministic methodology and clustering heuristics, we identify which addresses are managed by the same entity and should therefore be grouped together in a cluster. Additionally, some of our cryptocurrency exchange clients have agreed to share with us their on-chain transaction data. This provides unique insights into cryptocurrency services and informs our clustering methods.

Chainalysis leverages four key clustering heuristics: co-spend clustering, behavioral clustering, intelligence-based clustering, and detection of coinjoin and mixing activity. The co-spend technique groups addresses that are contributing inputs to a single transaction. This is an automated process, and when multiple cryptocurrency addresses are used as inputs in the same transaction, clustered ownership is attributed with a high degree of accuracy. Additionally, Chainalysis clusters co-spending across forks. For example, addresses that existed on the Bitcoin blockchain before the split with Bitcoin cash appear on both blockchains.

Behavioral clustering refers to detecting patterns in the timing or structure of transactions to identify a specific wallet software. Wallets have distinct ways of handling fees and change addresses, and can help identify Virtual Asset Service Providers (VASP's) or specific wallet software. Chainalysis is able to apply AI/ML and specific algorithms to map addresses belonging to a particular service. Chainalysis also investigates a service's particular transaction patterns to develop clustering algorithms specific to that service, further increasing our data coverage.

Chainalysis gathers information from other sources to enable intelligence based clustering. Our intelligence operations team collects information from data-leaks, court documents, data partnerships, and manual analysis to supplement our clustering. Similarly, we are also able to cluster addresses based on the detection of a mixing service.

These clustered entities are presented graphically in our tools, and they are also accessible through our investigations API. Users can also form their own clusters by merging or creating entirely unique entities based on their own specific knowledge.

Chainalysis also has the ability to deploy sensitive proprietary technologies developed for and available only to our government customers. Chainalysis IAPI and Reactor are both TRL level 9 Solutions. Both are actual applications of the technology in its final form and are used under operational mission conditions within the DoD and IC.

**Proposed Work As it Relates to DoD/IC Capability Desirements:** IAPI will enable DoD/IC data engineers and scientists to search their own enterprise data and enrich that with Chainalysis insights to enhance large scale analysis, surface new leads and uncover previously unknown connections between different selectors for deconfliction. Finally, DoD/IC can use the IAPI to integrate Chainalysis data into internal tools such as query engines or threat intelligence platforms where analysts can glean quick insights on cryptocurrency data and determine if a deeper analysis/investigation is needed in Reactor. Some specific examples of workflows Chainalysis envisions for our customers are:

1. **Programmatic Prioritization & Target Development:** Analysts within specific organizations currently, and will eventually have even greater amounts of cryptocurrency addresses and transaction hashes linked to thousands of selectors. Pursuing each data point is nearly impossible. With the IAPI, analysts can quickly prioritize selectors and

leads with the highest amount of suspicious activity, streamline manual effort and focus on the most important pieces of intelligence with the highest likelihood of success. Typical examples include Darknet Market takedowns and sifting through SAR data at scale to quickly identify the most important vendors and surface the most egregious threat actors respectively.

2. **Enriching and identifying connections across disparate datasets to build comprehensive pictures of threat actors:** Our customers have  access to different datasets, but it can be impossible to see what data is connected. IAPI uncovers which existing datasets can be joined to Chainalysis data using various selectors such as IP addresses, cryptocurrency addresses and other entity-level data to enrich these datasets and create a full picture of an actor's financial activity and do deconfliction. One current Chainalysis customer, the cyber division of a gov't agency, uses this workflow to enrich existing digital forensics data and identify connections between different targets. Specifically, this workflow was leveraged in our analysis of Conti administrative payments. Following this lead, Chainalysis was able to uncover that Conti administrators likely brokered a revenue sharing model with an adjacent organization, Trickbot Group, also known as Wizard Spider.
3. **Access to & enrichment of cryptocurrency data at enterprise scale:** Analysts come across cryptocurrency data in their own internal tools on a daily basis but have no way of deriving insights from this data without blockchain analytics tools like Chainalysis Reactor. IAPI can solve this problem by integrating Chainalysis data into internal tools, providing enterprise-level access to our insights. An example of this is a team of ~100 intelligence analysts at a U.S. intelligence agency who use an internal tool to put together intelligence reports on a daily basis.

Ultimately, using Chainalysis' blockchain intelligence data, the DoD/IC can continue to ensure decision dominance through:

**Access To New And Emerging Data Streams:** In support of governments around the world, our data is integral in supporting our clientele uncover crypto nexus to the Pandora Papers; and uncover the most advanced ransomware actors to include Conti, which brought in at least $165 million in 2021 alone making it the most successful identified ransomware variant in 2021.

**Insights Allowing analysts To Make Data-Informed Decisions On Various Time Horizons And In Various Mission Areas:** Chainalysis curates blockchain intelligence data, leveraging Artificial Intelligence and Machine Learning (AI/ML), to drive decision making and guide our partners in an otherwise opaque ecosystem. Aligning Chainalysis capabilities with your intelligence lifecycle ensures your analysts will immediately be able to exploit this emerging dataset in a targeted fashion.

**The Standardization of Data Across Multi Domain Ops / Orgs:** Chainalysis serves as the single-source and ground truth dataset for the blockchain. Our data and blockchain intelligence will allow the government to influence the highly contested cyber environment. Corroborating vast datasets to produce actionable information is the most difficult challenge in the science and art of intelligence generation. Chainalysis offers access to 150 million unique digital addresses and relevant publicly available information (PAI) in a standardized format in our system.

**Past and Ongoing Efforts Where Chainalysis Has Addressed the Known Capability Desirements:** In 2021, Chainalysis provided both bulk data as well as our API to the USG in order to provide intelligence on issues of national security, ransomware, cyber threats, dark net markets, and money laundering networks. Specific examples include:

*Cyber*

- Identified infrastructure payments associated with Solarwinds via cross chain graphing.
- Identified a malware operation run by nation-state actors leveraging privacy coins.
- Identified infrastructure payments from a threat actor hijacking BGP (Border Gateway Protocol) certificates to target cryptocurrency platforms in a supply chain attack.
- Supported cyber extortion group and demixed funds moving through mixing service, Bitblender, to launder their extortion payments from victims and sales from the darkweb.

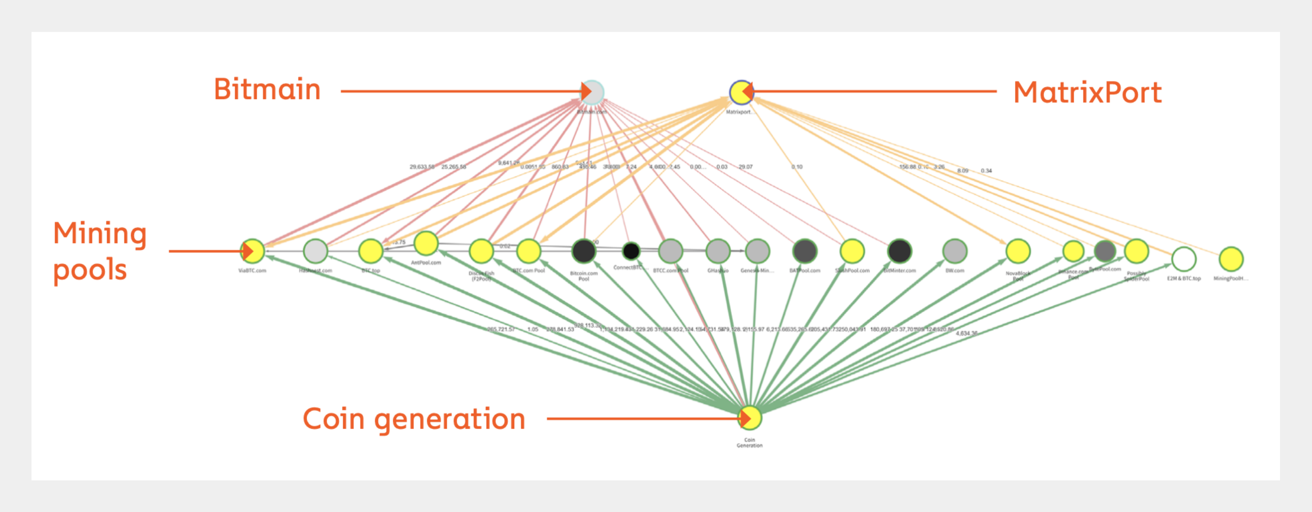
*Ransomware*

- Provided extensive insight into the Netwalker Administrator and Affiliate payments. For example, Netwalker very likely designed their ransomware operations to incorporate a mixing service, Bitmix.biz's, infrastructure; meaning the affiliates received their cut of the given attack as multiple withdrawals from the mixer rather than from the direct distribution of the victim payments.
- Traced and demixed funds tied to the Colonial Pipeline ransom resulting in a $2.3 Million USD seizure. Provided update and demix of previously dormant funds originating from the DarkSide ransomware group where funds were then transferred into cryptocurrency mixing service CryptoMixer.
- Identified the Avaddon ransomware payment network and Administrator(s).
- Demixed deposit transactions into mixing service, Blender[.]io, that were linked to Sodinokibi ransomware strain which was responsible for the JBS ransomware attack.
- Advised the National Security Council on the $600M Ronin hack to include the Tornado.cash outputs.
- Provided intelligence agencies insights into Conti RaaS operating model. Most Conti infections derive from Trickbot compromises. Trickbot malware enables stealing, infiltration, access, and malware delivery, and Trickbot receives a percentage of the overall extorted funds. Trickbot is a trojan that first appeared in 2016; it was originally used to steal financial information from victims but has evolved for broader criminal purposes

*Dark Net Markets*

- Identified the servers for the dark net market, World Market, with a transactional volume of over $36 Million USD.
- Developed lead package for Wall Street Market vendors and their cash out points.

**Cryptocurrency and China:** China was the historic leader in cryptocurrency mining, with Chinese miners at one point controlling an estimated 65% of Bitcoin's global hashrate. Moreover, it also dominated the mining equipment industry, and the machines produced by one Chinese company, Bitmain, have at times accounted for as much as 80% of all Bitcoin mined. Bitmain also owns Antpool, which is one of the world's largest mining pools. On-chain data gives us a view of Bitmain's importance to the mining industry. The Chainalysis Reactor graph below shows Bitmain's transactions with several of the largest mining pools. Green arrows represent newly mined Bitcoin moving to mining pools, while red lines represent mining pools sending funds to Bitmain, likely to purchase mining equipment.



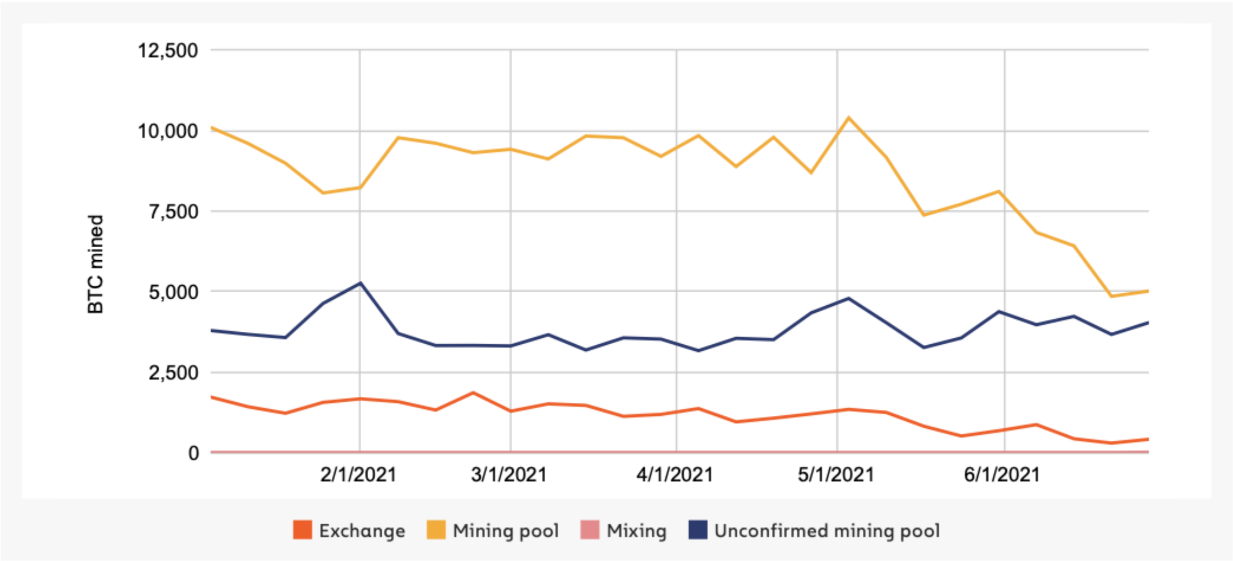
You'll also see a wallet for a firm called MatrixPort next to Bitmain. MatrixPort offers several different cryptocurrency services, and in 2019, Bitmain stopped accepting payments for mining equipment directly and began receiving them through MatrixPort's merchant services solution. Those payments are represented by orange lines, and show that the same mining pools are still purchasing from Bitmain.

Interestingly, MatrixPort spun off as an independent business unit from Bitmain in 2019, with a key Bitmain executive, Ge Yuesheng, becoming a cofounder of MatrixPort. These connections and their importance will be discussed later in this section.

China's status as the top cryptocurrency mining country changed drastically in May 2021, when the CCP announced its intent to clamp down on cryptocurrency mining and trading, citing concerns around financial stability and environmental impact. While this isn't the first time the CCP has adopted anti-cryptocurrency policies, previous enforcement only pushed exchanges and other cryptocurrency businesses out of the country, while traders and miners could still operate. Since the crackdown began in May 2021, Bitcoin's overall hashrate has fallen by more than 50%, as authorities have begun shutting down mining operations in many Chinese provinces.

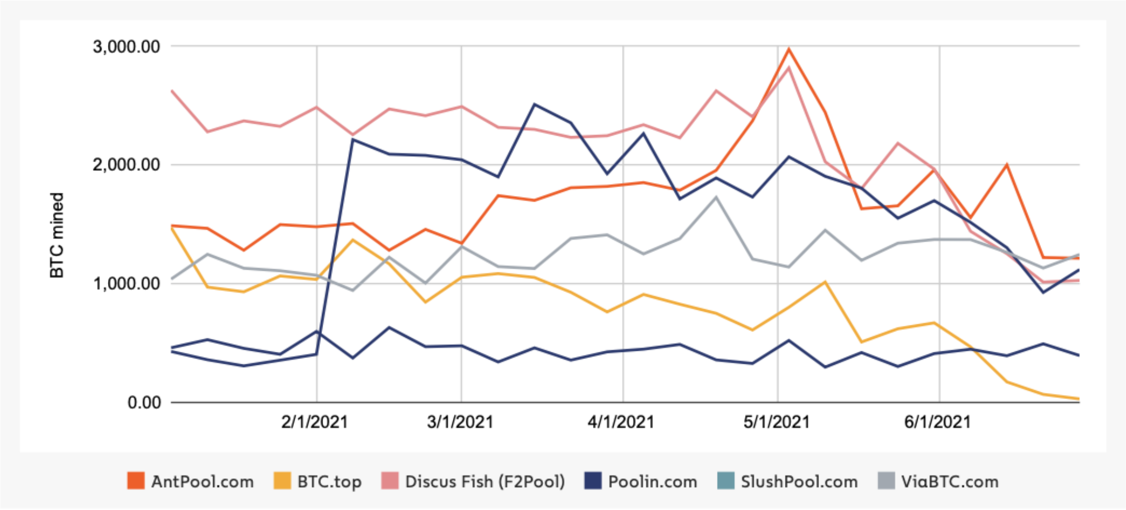
On-chain data reflects these changes. Starting in mid-May, soon after the announcement of China's crackdown, mining pools began receiving less newly mined Bitcoin, with weekly volume falling from roughly 10,000 BTC per week to under 5,000.

**Destination of Bitcoin mined by week** | Jan '21 - Jul '21



Digging deeper, it appears that mining pools headquartered in China or connected to Chinese cryptocurrency businesses were hit harder than others.

**Bitcoin mined by mining pools** | Jan '21 - Jul '21



All of this begs the question: Why is the CCP cracking down on cryptocurrency? We spoke to a China-based cryptocurrency operator who asked to remain anonymous. They named a few practical reasons for the government to move against cryptocurrency, such as preventing capital flight and stopping illegal money services businesses (MSBs) from operating. However, they positioned the CCP's opposition to cryptocurrency as primarily ideological.

"To understand this, you need to understand the CCP's governance philosophy," our expert says. "They take a top-down approach, and the goal is to maintain stability and unity. So when government officials see people like early Bitcoiners getting ultra rich and advocating for liberty and self-sovereignty, the natural inclination is to see them as dissidents."

Indeed, this ideological conflict has driven the CCP to take actions beyond just cracking down on mining and trading, such as campaigning against cryptocurrency in state-sponsored media, placing official warning messages on cryptocurrency-related apps, and potentially leaning on social media companies to suppress cryptocurrency-related content. Our expert stressed that while rebuilding mining infrastructure would be a long, difficult process, Chinese miners can move to new countries to resume work. They cited Kazakhstan as a likely destination, as well as regions of Africa whose economies have become intertwined with China's through programs like the Belt and Road initiative.

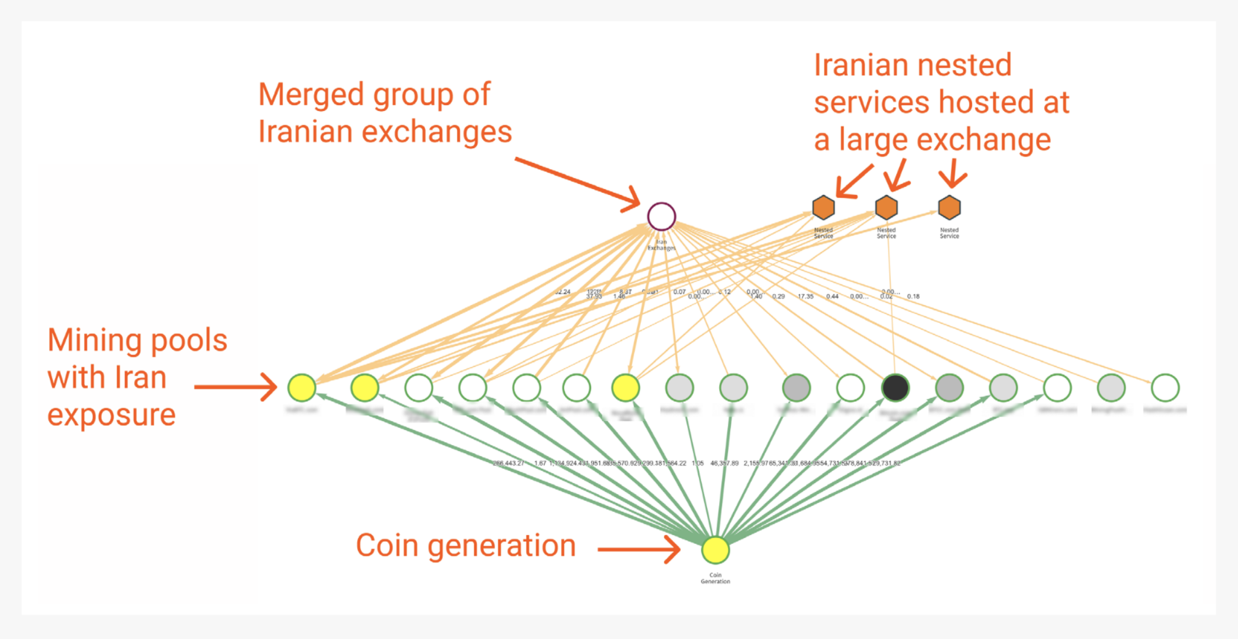
The ability to pick up and move means many Chinese miners will get to continue operating even as the CCP bans their activity. However, this may create risk for countries where miners are moving in cases where mining companies or their executives have connections to the CCP. We'll look at an example case here involving a partnership between a U.S. business and a Chinese business to set up mining operations in Texas.

Though based in Texas, Dory Creek LLC lists Jihan Wu, a cofounder of Bitmain and MatrixPort, as one of its managers. Dory Creek is partnering with a Chinese company called BIT Mining Limited to set up mining operations in Texas. BIT Mining Limited was primarily a gambling company until recently pivoting to mining. Publicly available information indicates that BIT Mining Limited is majority owned by an entity with close ties to the Chinese government.

Wu and other business partners sold two mining pools and related assets — BTC.com and BitDeer — to BIT Mining Limited in exchange for a stake in the company. SEC filings show approximately 75% of BIT Mining Limited shares are owned, either directly or through affiliates, by Tsinghua Unigroup (TU) or members of its senior leadership. TU is one of China's largest technology conglomerates, and is financially backed by the Chinese government. TU owns shares in Semiconductor Manufacturing International Corporation (SMIC), a Chinese semiconductor business that was added to the Bureau of Industry and Security (BIS) sanctions list in 2018.

The ownership of TU itself is also a matter of concern. A majority of its shares are held by Tsinghua University, a major Chinese university whose infrastructure has reportedly been used by hackers carrying out cyber intrusions, according to former Defense Intelligence Agency official Nicholas Eftimiades. While the CCP sees a cryptocurrency mining ban as within its own best interests, companies with ties to the CCP can still benefit from mining by moving overseas. However, these moves can create risk for the countries taking in Chinese mining companies and any domestic companies they partner with. In this case, Dory Creek is taking on risk by partnering with a business with ties to a sanctioned entity and a university that has been used by hackers to carry out cyber espionage attacks. Under such an arrangement, the CCP and its allies can benefit at the United States' expense.

*Mining and Sanctions Risk:* Cryptocurrency mining is a great way for heavily sanctioned countries to get money into their economy, because anybody with an internet connection and enough power can mine regardless of their location. Iran in particular has embraced cryptocurrency mining for this very reason, often partnering with Chinese mining companies to set up operations. We can get a high-level view of this activity using Chainalysis Reactor.


Merged group of Iranian exchanges
Iranian nested services hosted at a large exchange
Iran Exchanges
Nested Service
Nested Service
Nested Service
Mining pools with Iran exposure
Coin generation
Coin Generation

Above the entity labeled "Coin Generation," we see several Chinese mining pools receiving Bitcoin from mining, which is denoted by the green lines. Many of them send significant funds to cryptocurrency wallets and services known to be located in Iran, as denoted by the orange lines. Iranian cryptocurrency businesses included in that group are:

- iMiner - a Turkey based company with several mining farms in Iran

- Iranian cryptocurrency exchanges such as Nobitex.ir, Coinex.ir, EXIR.io, and Farhad Exchange

- Iranian OTCs and other nested services with addresses hosted at mainstream exchanges

While most of this activity is likely benign, it also represents potential sanctions circumvention by blacklisted individuals and entities in Iran.