TRM

All Roads Lead to China

North Korean hackers, fentanyl, cartel money laundering, and global organized crime

MAY 2025

TRMLABS.COM

Introduction

Chinese underground banking networks — often operating in the shadows of the global financial system — have become critical conduits for transnational organized crime.

These informal banking channels, sometimes dubbed "fei qian," or flying money, operate outside traditional banking regulations to move value across borders. They enable a vast range of illicit enterprises — from cyber-enabled financial crime and sanctions evasion to drug trafficking — by converting and transferring funds in ways that frustrate law enforcement oversight.

In recent years, these networks have increasingly turned to cryptocurrency to facilitate rapid, pseudonymous cross-border transactions. As a result, Chinese underground bankers and their criminal clients (including North Korean hackers, Mexican cartels, Russian crime syndicates, and Triad gangs) have built a sprawling illicit finance ecosystem that exploits crypto assets and underground financial systems to launder dirty money on a global scale.

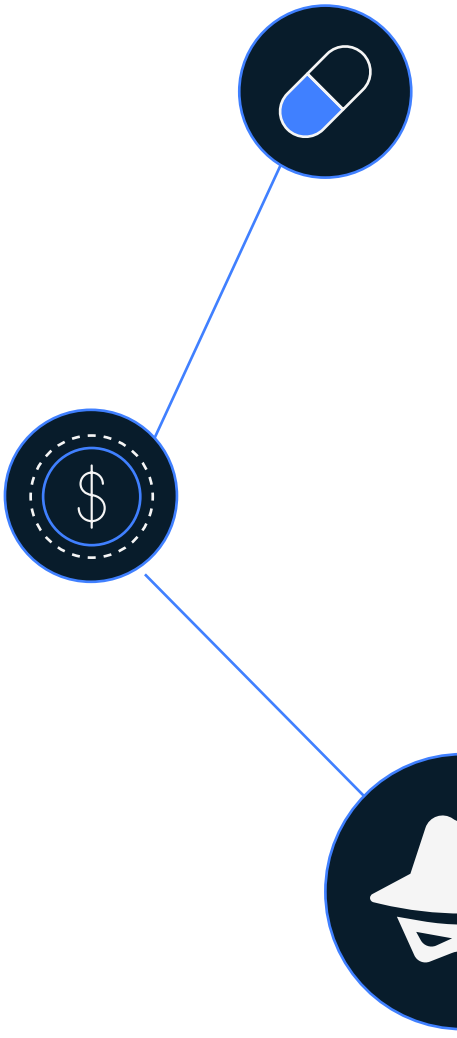
This report investigates how these networks function, examines case studies drawn from TRM Labs' blockchain intelligence, and discusses strategies to disrupt their operations.

Some of the insights found in this report were originally published in *Lawfare*. See Sujit Raman and Nick Carlsen, "The World's Underground Bankers," (May 5, 2025).

The role of Chinese underground banking networks in global

Chinese underground banking networks serve as a financial lifeline for criminals worldwide, effectively operating a parallel banking system that skirts official scrutiny. These networks typically involve **brokers** who can seamlessly swap funds across jurisdictions without leaving a trace in regulated bank accounts.

For example, US drug dollars can be exchanged for Chinese yuan through an **informal value transfer**: a broker in the US collects cartel cash and mirrors the transaction by providing equivalent value to a counterpart in China, often via crypto or other off-record methods.



The advantage of this "mirror exchange" is that no cross-border wire ever occurs — dollars stay in the US and yuan remain in China — minimizing red flags for regulators. Instead, brokers settle accounts through creative means like **trade-based money laundering (TBML)**: using the yuan to purchase goods in China, exporting those goods to cartel affiliates in Latin America, and selling them for local currency to recoup the broker's funds. This web of currency swaps and trade deals, facilitated increasingly by cryptocurrency, is highly effective at moving criminal profits under the radar.

According to TRM, Chinese underground banks have a symbiotic relationship with organized crime groups worldwide, including Mexican cartels. They provide a service that both circumvents China's strict capital controls (helping wealthy Chinese move money abroad illicitly) and helps foreign criminals repatriate or reposition their illicit earnings.

US authorities have uncovered numerous instances of these networks laundering drug proceeds for cartels. In one case, a Los Angeles-based ring led by cartel operatives laundered over USD 50 million in narcotics revenue via Chinese underground bankers, using trade-based schemes and crypto transactions to conceal the money's origins. Large seizures of cash and drugs in that investigation underscored the extensive collaboration between cartel operatives and Chinese underground banks in concealing and transferring illicit drug proceeds.

Such networks effectively bridge the gap between the cash-intensive criminal underworld and the formal economy, offering criminals a reliable way to convert dirty cash into usable assets. This same Chinese money laundering infrastructure has also been repurposed to assist cybercriminals and sanctioned regimes, proving its versatility as a global crime enabler.

Case studies and key networks: Chinese criminal organizations in action

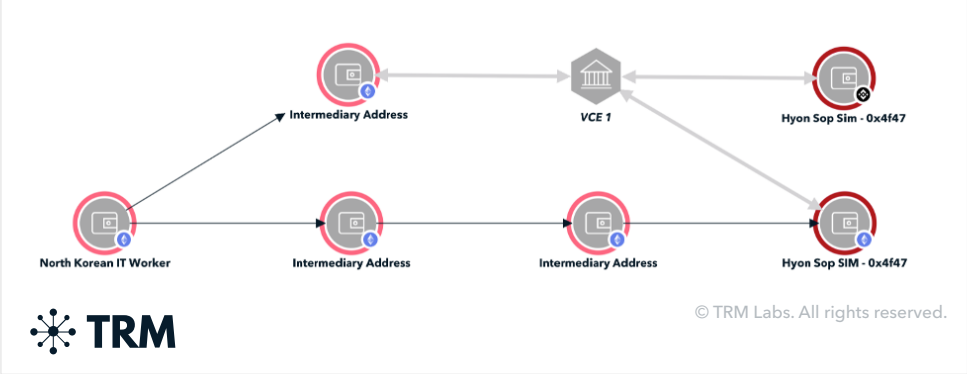
North Korean crypto heists and Chinese laundering networks

North Korea's state-sponsored hackers have stolen billions of dollars in cryptocurrency through exchange hacks and cyber-heists. But stealing crypto is only half the challenge. Converting those digital assets into money that Pyongyang can use (e.g. to fund its weapons programs) requires a laundering pipeline that circumvents global sanctions.

Chinese underground banking networks and loosely regulated crypto brokers have provided exactly that. TRM Labs and US authorities have uncovered how North Korean operatives rely on Chinese over-the-counter (OTC) crypto brokers and financial facilitators to wash stolen coins into fiat currency or commodities.

The middlemen: Chinese OTC brokers

In a 2023 US indictment, North Korean banker Sim Hyon Sop was charged alongside three OTC brokers — Wu Huihui, Cheng Hung Man, and a broker using the moniker "Jammy Chen" — for conspiring to launder cryptocurrency pilfered by Pyongyang's hackers.



TRM Graph Visualizer showing the flow of the biweekly salary of one North Korean IT worker and hacker, which TRM Labs has been tracking, to the address publicly revealed to be controlled by Sim Hyon Sop on behalf of North Korea's Foreign Trade Bank (FTB) / Korea Kwangson Banking Corporation (KKBC)

According to court documents, Sim (a representative of North Korea's Foreign Trade Bank) worked with these mainland China and Hong Kong-based brokers to convert stolen crypto into US dollars by funneling it through exchanges and shell companies, then using the funds to purchase goods via Hong Kong front firms for North Korea's benefit. This scheme effectively turned hacked crypto into sanctioned commodities, illustrating the marriage of cybercrime proceeds with underground trade channels.

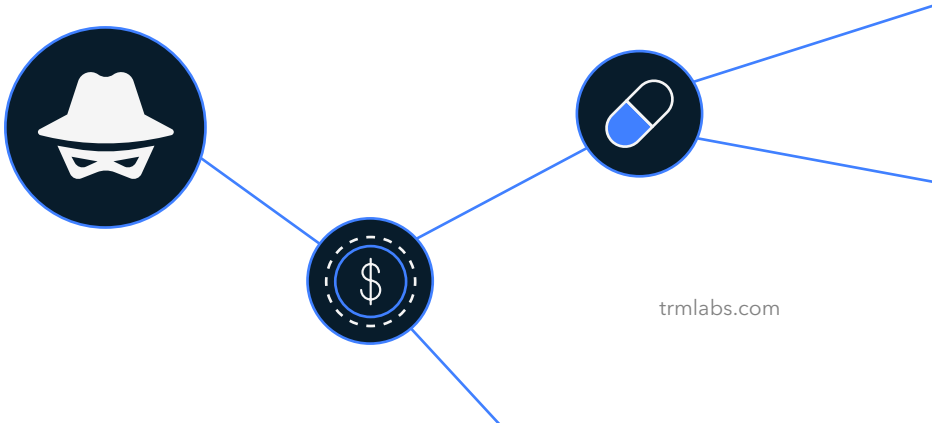
TRM analysis shows that OTC brokers like Wu and Cheng act as critical middlemen in North Korea's laundering playbook. They use their access to major crypto exchanges and bank accounts to swap illicit crypto for fiat under the cover of legitimate high-volume trading. Once funds enter traditional banks (often via accounts of offshore companies in lax jurisdictions), they are layered through a maze of transfers to obscure their North Korean origin.

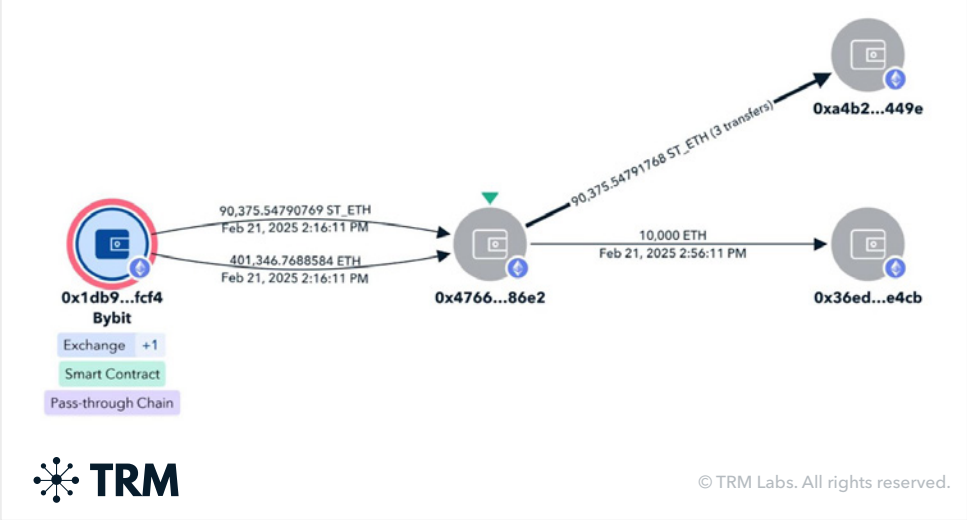
China — historically North Korea's largest trading partner — often serves as the geographic hub for these operations, with key facilitators based in Chinese territory. Notably, Sim Hyon Sop himself relocated to Dandong, China, a border city long known as a nexus for North Korean illicit commerce. This highlights how Pyongyang's financial emissaries embed within China to exploit its financial system's gray areas.

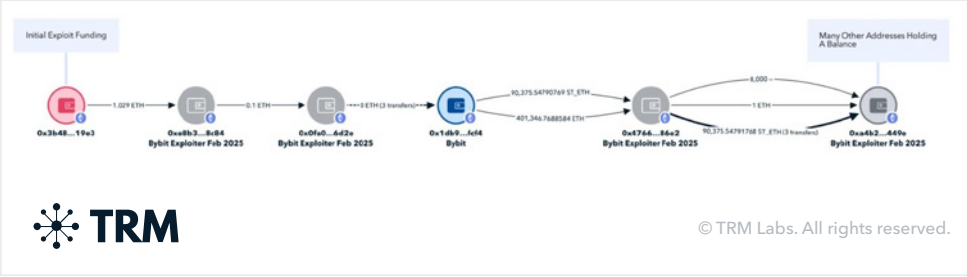
North Korea's expanding laundering infrastructure

North Korea's crypto laundering methods have evolved to maximize speed and anonymity. After major hacks, Pyongyang's hackers rapidly move stolen coins into complex chains of transactions — using decentralized exchanges, cross-chain "bridges" between blockchains, and mixers — before handing off to OTC brokers for the final cash-out.

A recent example is the Bybit exchange hack in February 2025 — North Korea's largest crypto exploit to date, in which North Korea stole USD 1.5 billion from the world's second largest exchange. TRM Labs investigators noted the "unprecedented level of operational efficiency" in the Bybit laundering: within days of the theft, the hackers bridged nearly all stolen Ether into Bitcoin via decentralized protocols, then started funneling the Bitcoin through mixers.

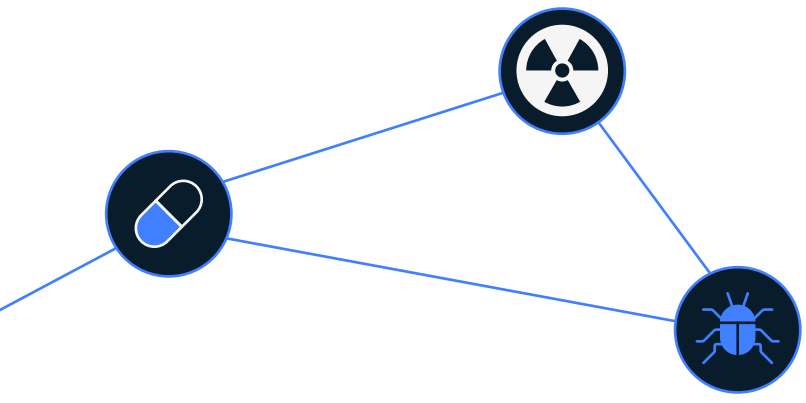


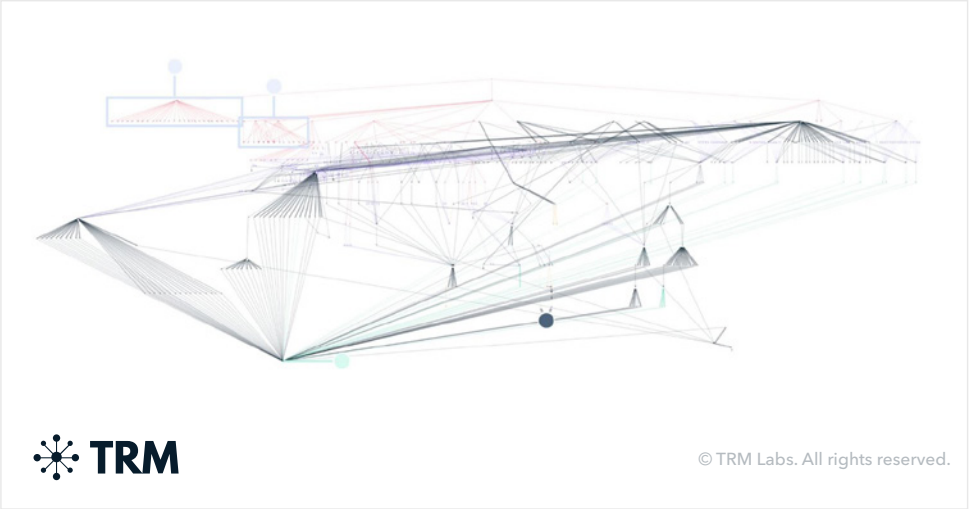




Funds moving off of Bybit after the initial hack, as shown in TRM Graph Visualizer

Such rapid layering suggests an expansion of North Korea's laundering infrastructure — likely with greater support from underground networks in China to absorb and process the funds. Indeed, once the initial obfuscation was done, a large portion of the Bitcoins sat idle, presumably awaiting liquidation through OTC channels that can handle converting tens of millions without detection.





The rapid laundering process, as of February 26, 2025, includes transfers through multiple intermediary wallets, conversion into different cryptocurrencies, and the use of DEXs and cross-chain bridges to obfuscate the trail

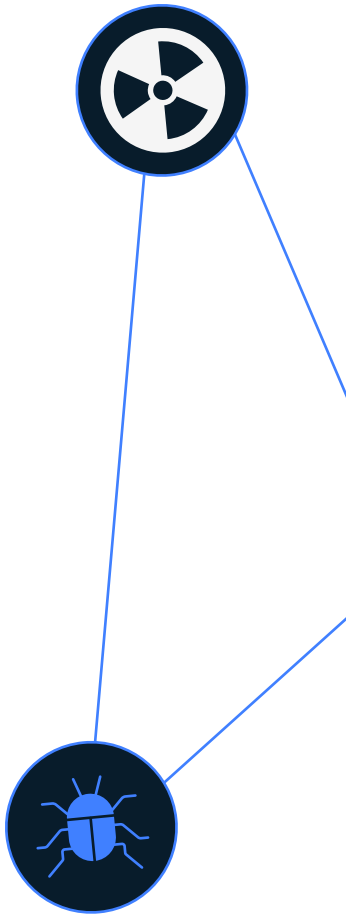
Chinese laundering networks (from crypto brokers to complicit banks) are the linchpin that enables Pyongyang to transform hacked crypto into tangible resources. Their collaboration presents a formidable challenge to sanctions regimes, as North Korea leverages both cutting-edge cyber tactics and age-old underground banking to sustain its illicit finances.

Triads, crypto casinos, and trade-based laundering

The Chinese Triads — long established as powerful organized crime syndicates — have aggressively embraced underground banking and cryptocurrency to launder their illicit proceeds. These groups (such as 14K and Sun Yee On) historically controlled Hong Kong and Macau gambling junkets and extensive smuggling networks, which they used to clean cash from activities like drug trafficking.

In the modern era, Triad-affiliated networks have extended this model across Southeast Asia, operating casinos (both physical and online), scam call centers, and shell companies that function as laundering hubs. During the COVID-19 pandemic, many land-based casinos in the region shifted to online operations, and criminal groups repurposed their infrastructure to run cyber-scam centers in special economic zones along the Mekong and Myanmar border.

These scam compounds — often involved in "pig-butchering" romance and investment frauds — generate massive crypto profits that require washing. Triad gangs have turned the region's casinos and underground bankers into an "underground banking system," super-charging the illicit economy by enabling criminals to move money freely through casino accounts, betting credits, and cryptocurrency transactions.



Common laundering techniques leveraged by Triad gangs

According to the UN Office on Drugs and Crime, Chinese triads and affiliated gangs leverage casino-based networks to move funds in "much bigger and more untraceable ways than in the past," making it incredibly difficult for authorities to track the money.

One common Triad technique is to integrate cryptocurrency into casino and **trade-based money laundering (TBML)** schemes. For instance, a Triad-linked underground bank might accept criminal funds (from drug sales, human trafficking, etc.) and issue the equivalent value as gambling credits in a special economic zone (SEZ) casino or as cryptocurrency that can be gambled online. The funds can then be circulated through high-volume betting (often mixing illicit money with legitimate gamblers' funds) and eventually cashed out as "casino winnings" or business revenues, obscuring their origin.

Triad networks also **exploit international trade to launder money** — a practice where crypto is increasingly playing a role. They may use illicit proceeds to purchase valuable commodities (through fronts) which are shipped overseas and sold, or simply exchange dirty money for crypto, then use that crypto to buy goods that are hard to trace to the original crime.

The role of Chinese precursor manufacturers in trade-based schemes

According to TRM Labs, Chinese chemical manufacturers have been a key node in such trade-based schemes, especially in the drug trade. Of over 120 Chinese companies supplying precursors for fentanyl and methamphetamine (a trade in which Triads are deeply involved), **97% were willing to accept payment in cryptocurrency.**

This finding underscores how crypto has been integrated into the supply chains of illicit commerce. The Triads can pay Chinese precursor suppliers in Bitcoin or Tether, receive chemicals which are turned into narcotics, and then sell those drugs for cash that enters the underground banking cycle again.

A broad scope of criminal finances: From fraud to wildlife trafficking

Beyond drugs, Triad-connected laundering rings handle a range of criminal finances. They aid **fraud and scam networks** by providing channels to move stolen funds offshore. They have also been implicated in **wildlife and illegal goods trafficking**, using some of the same underground payment methods.

In all these ventures, the convergence of crypto and underground banking amplifies the scale. Triad money launderers have even stood up **unlicensed crypto exchanges and OTC desks** of their own to service clientele, often advertising via encrypted apps like WeChat or Telegram which are "resistant to surveillance" by authorities.

By blending traditional underground banking methods with cryptocurrency transactions, Triad-affiliated networks create multiple layers of anonymity. For example, a single laundering operation might involve swapping cash for crypto through a broker, gambling that crypto on an online casino the gang controls, then withdrawing it in another form elsewhere. Each hop makes it harder to connect the final "clean" money back to the crime.

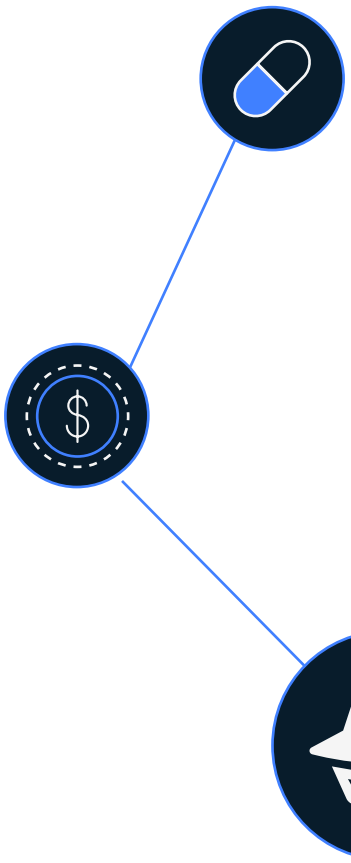
These complex schemes illustrate the adaptability of Triads in the face of new technology: they have essentially turned cryptocurrency into another tool for their age-old money laundering machine, alongside casinos, shell companies, and trade fraud.

The "mirror exchange" between cartels and Chinese money brokers

A particularly sophisticated method by which Chinese underground bankers facilitate cartel money laundering is through a **mirror exchange** system that largely bypasses formal banking altogether. In this arrangement, Chinese money laundering organizations (CMLOs) effectively swap assets with cartel associates to satisfy both parties' needs while minimizing any actual cross-border fund transfers.

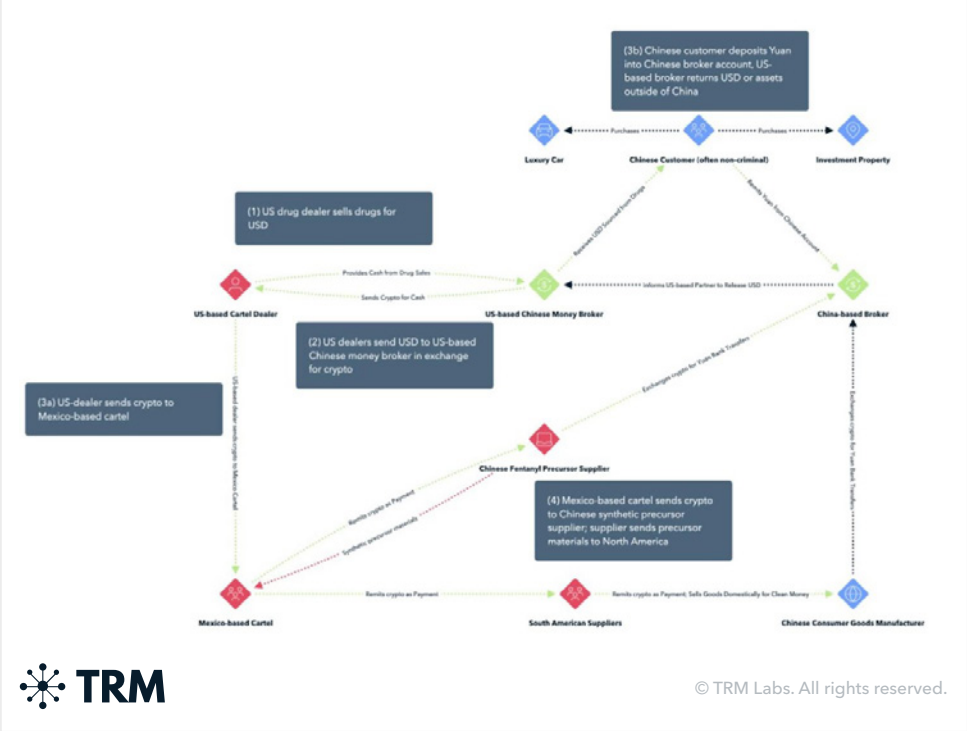
How the mirror exchange system works

- A Mexican cartel has millions in US cash from drug sales that it needs to get into Mexico or otherwise usable form, while wealthy Chinese individuals in China want US dollars outside of China (to invest abroad or evade China's currency controls).
- A Chinese underground broker steps in as the intermediary. The broker will buy the cartel's bulk dollars in the US (thus taking possession of the illicit cash) and, in return, provide the equivalent value to the cartel's people in Mexico — not in dollars, but in local Mexican pesos or other assets — by tapping funds that the broker already controls (or can access) in Mexico.
- Conversely, the Chinese broker "sells" those US dollars to a Chinese client who is seeking dollars in US; that client pays the broker the matching amount in yuan back in China.
- In the end, the cartel's dollars never physically leave the United States (they end up with the Chinese customer) and the Chinese yuan never leave China (they stay with the broker) — yet value has been transferred: the cartel got its money in Mexico, and the Chinese investor got money in the US, all via an off-ledger swap.



Cryptocurrency adds a modern twist to this mirror exchange system. Instead of relying solely on cash deliveries and commodity shipments to settle accounts, brokers increasingly use crypto as the intermediary value transfer. This innovation now allows for a **trustless network**. Whereas before, Chinese underground banking brokers relied on trusted associates in each geographical location they served, crypto now allows for a much looser confederation. There is no trust required or even a shared ledger when stablecoins form the medium of exchange.

For example, in some cases documented by TRM Labs, drug traffickers or their brokers deposit bulk cash into crypto ATMs or exchanges in the US, converting it to Bitcoin, which is then sent to a wallet controlled by a Chinese network.



TRM Graph Visualizer, with explanations, showing how the cartels and Chinese brokers use cryptocurrencies to launder drug money

The Chinese facilitators can then either convert that cryptocurrency to fiat in a jurisdiction of choice, or use it to purchase goods (like precursor chemicals or luxury items) that ultimately credit the cartel's account. One TRM investigation described a Sinaloa Cartel-linked money launderer in the US who directed couriers to pick up drug cash and deposit it into various virtual currency wallets – effectively paying the cartel in crypto, which could be reinvested into fentanyl production back in Mexico.

In such a setup, neither the cash nor a wire crosses the US-Mexico border; the value moves via blockchain. This achieves the same goal as the traditional mirror exchange – keeping dirty money out of sight – but with even greater speed and obscurity. Digital assets can be transferred globally in seconds, and when handled through opaque OTC trades, peer-to-peer exchanges, or privacy coins, leave little trace for law enforcement.

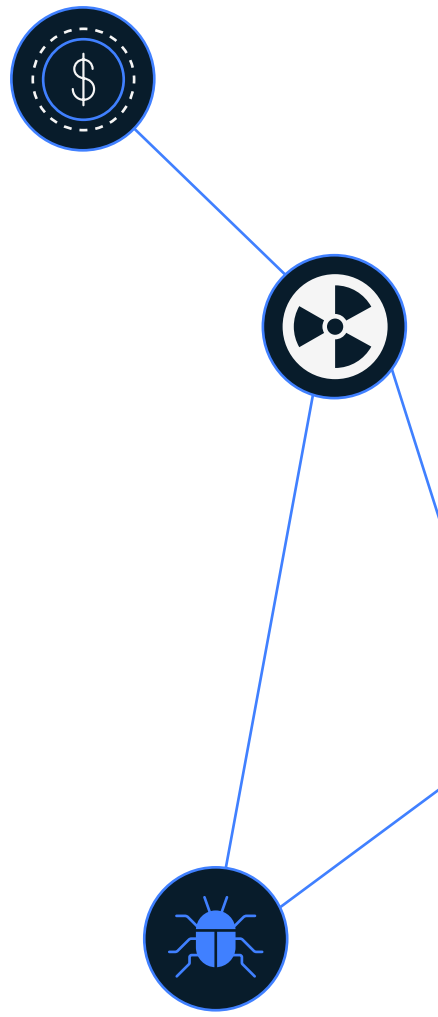
The shadow financial pipeline between the Americas and China

The mirror exchange method is powerful because it leverages mutual needs: Chinese brokers profit by collecting fees and gaining access to hard currency, Chinese elites get their capital flight accomplished, and cartels get their

narco-dollars laundered into usable form. And all of this happens outside regulated channels. As a former US DEA official noted, these CMLOs use encrypted communication (often **WeChat**) to quickly match buyers and sellers of currency, making transactions instant and difficult to intercept.

By keeping each currency largely within its home country (dollars in the US, yuan in China, pesos in Mexico) and using crypto and trade as balancing mechanisms, the scheme avoids the need for international bank wires that might trigger AML alarms. This "exchange without exchange" system has enabled cartels like Sinaloa to launder enormous sums. US investigators estimated that one such Chinese money ring launders hundreds of millions annually for cartels, taking only a small commission (often 1-2% of funds) to undercut traditional money brokers.

The result is a shadow financial pipeline between the Americas and China that moves illicit drug profits with incredible efficiency. As long as Chinese underground banks can freely trade in cryptocurrency and settle debts with goods or internal offsets, they will remain a formidable challenge to drug enforcement efforts.



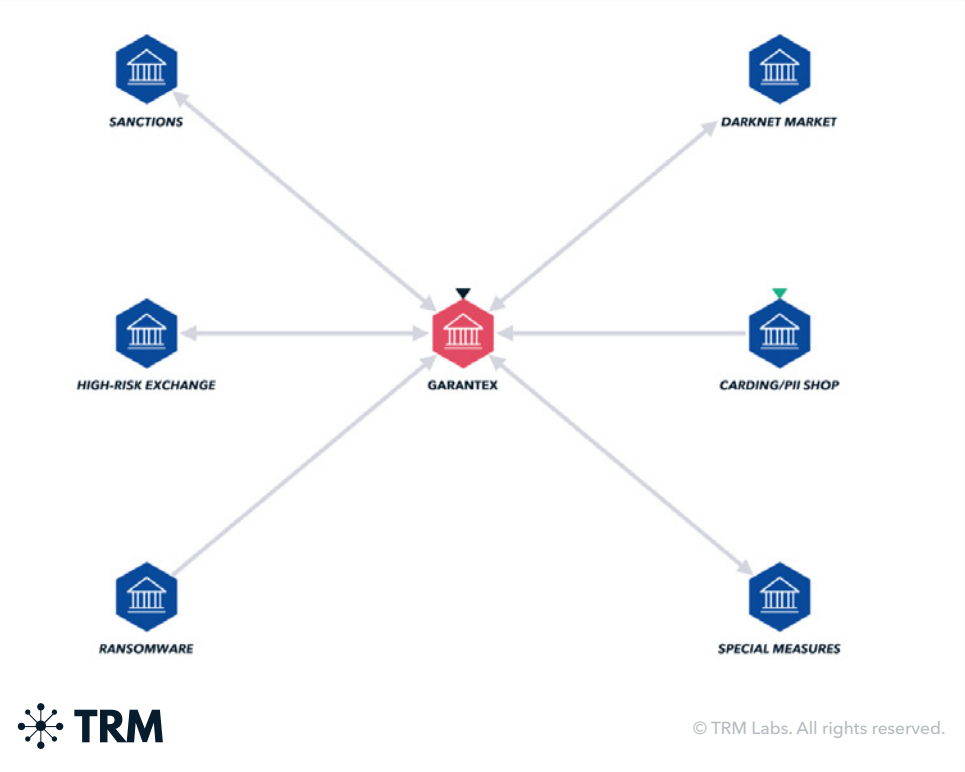
The nexus of North Korea, China, and Russia in illicit finance

Perhaps the most alarming development is how North Korea, China, and elements of Russian organized crime form an interconnected nexus in the illicit financial system. These actors each bring different capabilities to the table:

- North Korea contributes elite cybercriminals (the Lazarus Group and others) who steal vast sums of crypto
- Chinese underground networks provide the laundering channels and financial infrastructure
- Russian actors (whether state-linked or organized crime) offer additional safe havens and tools like rogue crypto exchanges and ransomware ecosystems

The coordination may not always be explicit, but their activities often complement each other on the blockchain. For instance, North Korean hackers have been known to funnel stolen cryptocurrency into services popular with Russian cybercriminals. US authorities noted that the Russia-based crypto exchange Garantex – an exchange later sanctioned and shut down – was a favored "money laundering destination for Russian and North Korean hackers."

In other cases, North Korean-linked wallets have sent funds to accounts on Russian-run exchanges and mixers, suggesting collaboration – or at least shared facilitators. This makes sense: an exchange like Garantex (or the defunct darknet market Hydra) had an established network to convert crypto into cash with little oversight, which any sanctioned actor would find valuable.



Garantex, before and after sanctions, has facilitated sanctions evasion, darknet market activity, ransomware, and other illicit activity

On the flip side, Chinese networks have also helped Russian entities evade sanctions and move funds. A notable example exposed by TRM Labs is the **financing of Russia's war machine** through crypto channels. Chinese companies manufacturing military equipment (such as drone and optical tech) have been selling to Russia, and cryptocurrency has been used to pay for these sanctioned transactions.

TRM identified at least USD 85 million sent since 2021 to crypto wallets linked to Russian and Chinese entities involved in the trade of military and dual-use equipment — effectively a cross-border sanctions evasion pipeline using digital assets.

In this scheme, Russian intermediaries likely obtained crypto (potentially from sources like ransomware proceeds or illicit exchanges) and transferred it to Chinese suppliers, who could then cash out in China, thereby skirting Western financial sanctions. Such activity underlines how Chinese underground finance isn't limited to just profiteering criminals; it can also facilitate state-level sanction busting. North Korea has engaged in similar tactics by using stolen crypto to acquire sanctioned goods via China, as seen with the Hong Kong front companies used to buy luxury items and raw materials for Pyongyang.

Moreover, these actors learn from each other. North Korean hackers, for example, have emulated Russian cybercriminal techniques — from using ransomware as a fundraising tool to employing Russian-developed malware — and then laundered the proceeds through Chinese brokers. Russian darknet drug markets have flourished with Chinese precursor chemicals (like ingredients for meth and fentanyl) keeping their supplies flowing.

Those Chinese chemical suppliers, in turn, readily accept crypto payments, feeding the cycle of crypto-fueled crime. **In essence, North Korea, China, and Russia have formed a *de facto* illicit finance alliance.**

- North Korea contributes to financial cybercrime and demands for sanctions evasion
- Russia provides criminal marketplaces and technical tools
- Chinese networks furnish the monetary plumbing to wash and move funds

Each one benefits: North Korea gets cash for its regime, Russian actors get partners in crime and access to Chinese markets, and corrupt Chinese brokers and businesses earn hefty fees. This nexus poses a multifaceted threat that spans cybercrime, narcotics, and sanctions evasion, all stitched together through blockchain networks that ignore national boundaries.

Analysis: How underground networks evade detection

Chinese underground banking networks and their criminal partners employ a sophisticated arsenal of tactics to evade detection and outmaneuver law enforcement and compliance controls. A core strength of their operations is **jurisdictional arbitrage**: they base critical steps of the laundering process in countries or platforms where oversight is weak. For example, Chinese OTC brokers laundering North Korean crypto often transact on exchanges with lax Know Your Customer (KYC) rules or in jurisdictions that don't strictly enforce sanctions.

By the time funds reach a well-regulated environment, they have been layered through multiple hops (often via shell companies or obscure bank accounts) to obscure their true origin. This cross-border shell game makes it challenging for any single agency or bank to piece together the full trail.

Mixers, cross-chain bridges, and other obfuscation methods

Cryptocurrency has become a double-edged sword in this cat-and-mouse game. On one hand, crypto transactions are recorded on public blockchains, offering investigators new ways to trace money. On the other hand, underground networks exploit tools to muddy the waters: **using mixers, cross-chain bridges**, privacy coins, and hundreds of **micro-transactions** to break the links that investigators follow. North Korea's "flood the zone" technique is a prime example, involving moving stolen crypto through rapid, high-frequency transactions across multiple platforms to overwhelm trackers.

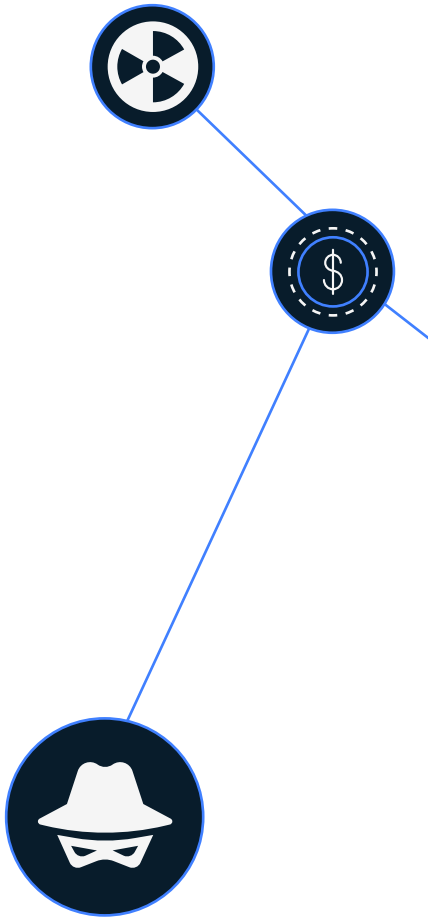
By hopping across different blockchains (Ethereum to Bitcoin to TRON, etc.) and using decentralized exchanges, the launderers slip through gaps between regulatory perimeters. In the Bybit hack, the thieves bridged assets via THORChain and immediately funneled them into mixers like Wasabi Wallet and others.

Such DeFi and mixer usage creates significant tracing challenges, often generating false leads for investigators as unrelated funds intermingle. Only advanced analytics tools and highly trained investigators can follow these complex paths with confidence.

Trade-based money laundering (TBML)

The "old school" methods of underground banking continue to allow the movement of funds without detection by authorities. **Trade-based money laundering (TBML)**, used by Triads and cartel brokers alike, obscures illicit funds within the huge volume of international trade. Falsified invoices, front companies, and commodity swaps make it appear as if money is simply the proceeds of legitimate trade.

When combined with crypto, TBML becomes even harder to spot. Payments for fake "goods" may be made in cryptocurrency and never touch the banking system, or crypto earnings from crime can be masked as proceeds from selling under- or over-valued shipments. Traditional anti-money laundering (AML) systems (which rely on flagging unusual bank transfers) are blind to value moving via a container ship or a crypto wallet. Chinese underground networks take full advantage of this by operating in the seams between systems: **they settle balances with whatever method draws least attention**, be it Bitcoin or a shipment of electronics.



Encrypted communications, language barriers, and constant innovation

Another key evasion tactic is the use of **encrypted communications and clandestine networks** that enable trust among criminals without exposing transactions.

Chinese brokers and their clients coordinate deals through encrypted messaging apps (WeChat, Telegram, WhatsApp with end-to-end encryption). They often use code words or refer to transactions obliquely, and because the actual currency exchanges happen off the books (or within crypto wallets), a surveillance agency might only see innocuous chatter about "buying merchandise" or "investing in projects."

The human element – **language and cultural barriers** – also plays a role. Western law enforcement agencies require specialized translators and cultural knowledge to penetrate Chinese underground circles. Without those, even intercepted messages may go unrecognized for what they are.

Finally, these networks actively **adapt and innovate** in response to enforcement efforts. When one exchange or mixer is shut down, they migrate to a new one. If banks increase scrutiny on large wire transfers, they break transfers into smaller "smurfed" amounts or pivot more into crypto. A glimpse of progress can be seen in cases where enforcement pressure had an impact – for example, when Binance's compliance team identified and froze OTC broker Wu Huihui's accounts in 2022, he complained publicly about being cut off.

This shows that vigilant compliance by crypto exchanges can disrupt launderers' activities. But such victories are often temporary. The launderers find other platforms or use straw account holders to get back online. Chinese underground bankers and their criminal clients exploit every available gap: regulatory blind spots, technology loopholes, and international divides. They blend age-old hawala-like techniques with 21st-century fintech, staying one step ahead of authorities who must coordinate across borders and specialties to catch them.

Conclusion

Chinese underground banking networks and their crypto-laundering schemes represent a complex, global challenge at the nexus of cybercrime, drug trafficking, and sanctions evasion. Yet, as this report has shown, they are not invisible. Through diligent blockchain analysis, interagency collaboration, and bold strategies — including going on the offensive in cyberspace — authorities can illuminate these shadowy networks.

The same features that make cryptocurrency attractive to criminals (speed, global reach, pseudonymity) can be leveraged by investigators to track and freeze illicit assets in ways not possible before. By tightening the net around key nodes and fostering international unity against underground financiers, law enforcement can begin to staunch illicit financial flows — with the cases of successful indictments and sanctions thus far offering a valuable blueprint.

Ultimately, combating this threat will require agility and innovation to match the criminals' own — but it is a fight that is well underway, aiming to safeguard the integrity of the global financial system from the dark alleys of underground banking.

About TRM Labs

TRM Labs provides blockchain analytics solutions to help law enforcement and national security agencies, financial institutions, and cryptocurrency businesses detect, investigate, and disrupt crypto-related fraud and financial crime. TRM's blockchain intelligence platform includes solutions to trace the source and destination of funds, identify illicit activity, build cases, and construct an operating picture of threats. TRM is trusted by leading agencies and businesses worldwide who rely on TRM to enable a safer, more secure crypto ecosystem. TRM is based in San Francisco, CA, and is hiring across engineering, product, sales, and data science.

To learn more, visit www.trmlabs.com