ST. KITTS BRANCH
Financial SERVICES Regulatory Commission

NewsLetter

November 2024
Issue No. 125

The Dark Side of Crypto

Crypto and The Criminal Underworld

With the increasing popularity of crypto assets in legitimate circles, also comes its burgeoning use in the criminal underworld. Crypto assets have been reportedly used in money laundering, cybercrime, ransomware and extortion attacks, sanctions evasion, corruption and bribery, terrorist financing and the purchasing of illicit materials and services via the **dark web**.

The Dark Web

The '**dark web'** is an area of the internet inaccessible via traditional search methods and computers, where pages and information are explicitly designed to be concealed from mainline search engines and casual users. The difference between the **surface web** (the "normal" part of the internet) and the **dark web** is that the **dark web** is far more anonymous than the **surface web**. This is also the reason why the **dark web** is often associated with criminality. ***The preferred form of payment on the dark web is cryptocurrency***. Accessing the **dark web** requires specialized software, and accessing it safely and privately requires additional measures.

Crypto Cleansing

'Crypto Cleansing' refers to laundering through the crypto market. Crypto markets offer greater user anonymity when compared to the traditional financial systems since accounts can be set up remotely and pseudonyms are customarily used on exchanges and platforms. However, crypto assets are not completely anonymous or impossible to trace. Crypto assets are largely **tracked via blockchain**. The **blockchain** is a form of distributed ledger technology, decentralized and managed by disparate agents and users across multiple locations, which acts as a virtual tamper-proof ledger, creating a **lasting and irrevocable record** of every crypto transaction ever made. Each crypto transaction therefore leaves a marker on an immutable blockchain which, in turn, can be exposed by forensic and analytical organizations (e.g. Chainalysis) to show the transaction and its ties to a specific wallet. Criminals therefore use various methods to clean/obscure their crypto trail.

Popular Crypto Cleansing Methods

⇒ **Chain Hopping** - Rapidly changing one coin for another to lose online footprint.

⇒ **Coin Cleaning** – Combining laundered crypto with other legitimate crypto before redistributing them.

⇒ **Privacy Wallets** - An obfuscation tool used to move around laundered crypto which includes coin-mixing and extra built-in privacy measures.

DID YOU KNOW?

A combined task force named "**Operation Onymous**" between the Federal Bureau of Investigations (FBI) and the European Cybercrime Centre managed to decrypt large amounts of information and arrested the owner/ operator of the popular **dark web** market, '**Silk Road',** which introduced Bitcoin as an accepted payment. currency.

Case Study

Helix Mixer and Coin Ninja

FinCEN discovered that Larry Dean Harmon, founder of *Helix and Coin Ninja* ***mixing*** *services*, offered his mixing services to criminals; especially vendors on the **dark web** market: '*Alphabay*'. Over a 3-year period, he processed more than one million transactions worth $311 million. Harmon ran Helix on the '*Grams*' onion site (website on the **dark web**) and advertised his services on both the surface web and dark web. He claimed that Helix could allow users to avoid law enforcement detection. Harmon also claimed that by providing users with fresh crypto asset addresses with no trading history, Helix made transactions less susceptible to blockchain monitoring. Transactions were also facilitated on behalf of child exploitation sites, neo-Nazi groups, Iran-based users, and conducted approximately $900,000 of transactions involving BTC-e, a crypto trading platform.

Red Flag Indicators: Crypto Cleansing

- Large/frequent conversions (particularly into multiple crypto assets).
- Immediate withdrawal of funds after initial deposit.
- Exchanges from crypto assets to fiat currency, at a loss (e.g. during times of fluctuation or via high commission fees).
- Use of anonymity through enhanced crypto assets and encrypted, anonymous or temporary emails or through communication platforms such as virtual private networks (VPNs) or Tor (network for anonymous communication.
- Domain registration through proxies/registrars which suppress names.
- Multiple transactions that hover just below the threshold.
- Users with multiple accounts registered under different names.
- Frequent changes of ID information (e.g. email addresses, IP addresses or financial information).
- User attempts to enter multiple service providers from different IP addresses on the same day.
- Incoming transactions from multiple users, especially with the same IP address, with quick turnaround on subsequent transfer or exchange.

Risk Mitigation: How Can Businesses Protect Themselves?

1) Formulating customer risk profiles, sufficiently supported by customer due diligence (CDD) to determine the necessary level and nature of ongoing monitoring.
2) Consideration of geographical risk regarding source and destination of funds relating both to crypto asset provenance and customer's location.
3) A comprehensive red flag list must be drawn up to aid ongoing transaction monitoring which should include suspect language used in message fields that may indicate illicit activity.
4) Screening against industry specific blacklists.
5) Retaining originator & beneficiary information which can be provided on request to all firms involved in a transfer, to enable all agents to build a holistic view of the end-to-end transaction beyond their own, isolated segment.
6) Placing limits on transactions or on the value of privacy coins which may be stored or exchanged. Privacy coins are cryptocurrencies which allow users to conduct transactions privately and anonymously.
7) Imposing time delays on perceived high-risk transactions to limit the rapid movement of funds.
8) Prohibiting transfers between fiat and crypto assets to third parties.

CONTACT US
For More Information

References:

Briefing Note: Money Laundering through Cryptoassets, Themis (February 2021).

Briefing Note: The Dark Side of the Web, Themis (August 2021).

Financial Crime Typologies in Cryptoassets, Elliptic, 2020.

South Independence Square Street, P.O. Box 898, Basseterre, St. Kitts
Tel: (869) 466-5048 | 467-1019/1591 Fax: (869) 466-5317
Website: www.fsrc.kn / Email: info@fsrc.kn