# [ PDF Database Document ] - BTCC Cryptocurrency Exchange

Original:
https://www.btcc.com/en-US/academy/research-analysis/criminals-still-find-it-easier-to-hide-in-fiat-than-crypto

**Criminals Still Find it Easier to Hide in Fiat Than Crypto**

Contrary to popular lore, cryptocurrencies are not a haven for anonymous criminals. Lawbreakers can run, but not hide, in transparent cryptocurrency networks.

In fact, because of smart blockchain analytics, it's easier to follow money trails on blockchains than it is on legacy payment networks, however a circuitous route they may take.

What's still hard to figure out – at least for the time being – is the identity of the criminals using various blockchain addresses to move stolen funds. This is especially true if they use self-hosted wallets.

## Blockchains are Much More Transparent for Tracking Criminal Payments Than Fiat

Transparent blockchains are much easier platforms for tracking criminal payments than siloed legacy payment systems ever were. Today, about 23 public blockchains make up about 99% of the total cryptocurrency market cap. That means that blockchain fraud detection systems must integrate with just 23 transparent platforms rather than thousands of siloed enterprise and fiat payment networks.

The hard part is turning nondescript blockchain metadata into meaningful information. If done well, using scalable real-time analytics, automated insights can help users see across all blockchain platforms at once, trace criminal and suspect payments and addresses and identify abnormal money movement patterns that are often repeated.

## Emerging Blockchain Network

Vendors like Chainalysis Ciphertrace, Elementus and TRM Labs provide insights on money trails to authorities investigating hacks. Their services are increasingly used by exchanges and decentralized finance (DeFi) protocols to prevent fraud in the first place.

In 2021, high-profile hacks resulted in criminals returning stolen funds or law enforcement clawing them back. Criminals are finding it difficult to hide from investigators who identify addresses where stolen funds are parked. Once stolen funds are marked, they cannot be easily moved off the blockchain without being seized by watchful parties and law enforcement.

It is simply getting harder for criminals to move stolen funds off crypto networks. We see this repeatedly, for example in the hacks of Poly Network and BadgerDao and the freeze of the tether stablecoin.

## Connecting Addresses to Identities: the Missing Link

Detecting blockchain addresses used by criminals doesn’t yield the identity of the address’ owner. No KYC (or know-your-customer procedure) is required to use a blockchain unless a user onboards through a virtual asset service provider (VASP) that complies with regulations. Most criminals use self-hosted wallets and are their own “banks.”

Several startups fill this identity-knowledge gap for law enforcement targeting criminals or investors analyzing successful investment strategies. These startups identify address owners by scraping websites and using analytics to associate addresses with multiple user attributes, like social network profiles, geolocations, mobile numbers and email addresses. They collect data from darknets, social networks and open-source forums, and purchase data from proprietary sources when possible.

Hundreds of companies already engage in similar Web 2 data aggregation to support threat intelligence, marketing, loan approval and other use cases, generating profitable data markets worth

billions of dollars.

Over time, users will increasingly authenticate to Web 3 apps using blockchain wallets. Service providers will need to rely on blockchain data analytics for risk mitigation, marketing, crypto-market monitoring and more. Blockchain data analytics will grow into a large profitable market, subject to regulatory constraints.

## Blockchain Addresses' Privacy Protocols

Blockchain addresses are key to Web 3 identities, and so privacy-sensitive cryptocurrency traders take measures to maintain address anonymity. For example, they spread holdings out across multiple addresses, use mixers for transacting or trade in privacy coins like monero, pivx or zcash.

New proprietary privacy protocols go further and hide individual addresses and balances from public view. Soon we will see privacy "services" allow crypto traders to transact without revealing addresses. However, these services will likely be centralized and not necessarily trustworthy.

As privacy protocols that hide user addresses gain more adoption, blockchain intelligence firms will rely on alternative identity indicators to follow money trails. For example, they can pinpoint a transacting endpoint and use social graphs to link its activity – e.g., text and call metadata, interaction frequencies and size – to open source intelligence that can lead to an email or mobile phone number tied to an address.

Criminals will move more communications to encrypted private channels, making their real-world identity harder to determine. The cat and mouse game will continue, and agile bad guys will likely stay steps ahead of good guys bogged down by bureaucratic processes.

## Criminals Can Not Hide

It's a myth that blockchain networks are criminal havens. Reports from Financial Action Task Force (FATF) and blockchain intelligence providers confirm this fact with hard numbers.

No doubt, criminals will increasingly find it easier to hide in the spaghetti code of thousands of legacy systems than in transparent and far fewer blockchain networks.

Finally, the notion that users control their Web 3 identity goes only so far. Individuals, criminal or not, have zero control over public metadata used to determine real-world identities. Databases are

building up quickly to tie identities to blockchain addresses. New regulations, such as FATF's "Travel Rule," further reduce address privacy by forcing exposure of associated personal identifiable information (PII) data.

In the end, most criminals will lose on both levels, in hiding blockchain transactions and in hiding their real-world identities.