nSure.ai

USE CASE

You've Been Hacked: **An Overview of Crypto Exchange Fraud**

Gain insight into the volatility of crypto and how to protect yourself with nSure.ai solutions.

Use Case Scenario

The problem of payment fraud has intensified in the past couple of years, and the crypto space isn't immune to its spread.

As the market continues to grow in size, so does the level of fraudulent activity. Losses caused by DeFi exploits totaled $12B in 2021. Fraud and theft account for $10.5 billion of that sum — a seven-time increase from 2020.

Fraud and theft account for $10.5 billion of that $12B in losses caused by DeFi in 2021

Crypto exchanges are frequently under attack and **once the money is gone, it's gone for good**. What goes along with it are positive aspects the exchange's reputation.

The crypto space has a huge desire to be widely accepted and used in the mainstream, but as long as it is perceived as unsafe, its massive potential will not be realized.

It doesn't have to be as bad.

Potential Impacts

The high-tech world of crypto means there are many new and evolving risks, all thanks to the nature of these digital assets.

Decentralization

Because cryptocurrencies are distributed across a large number of computers, they exist in a decentralized structure that allows them to exist outside the control of governing bodies.

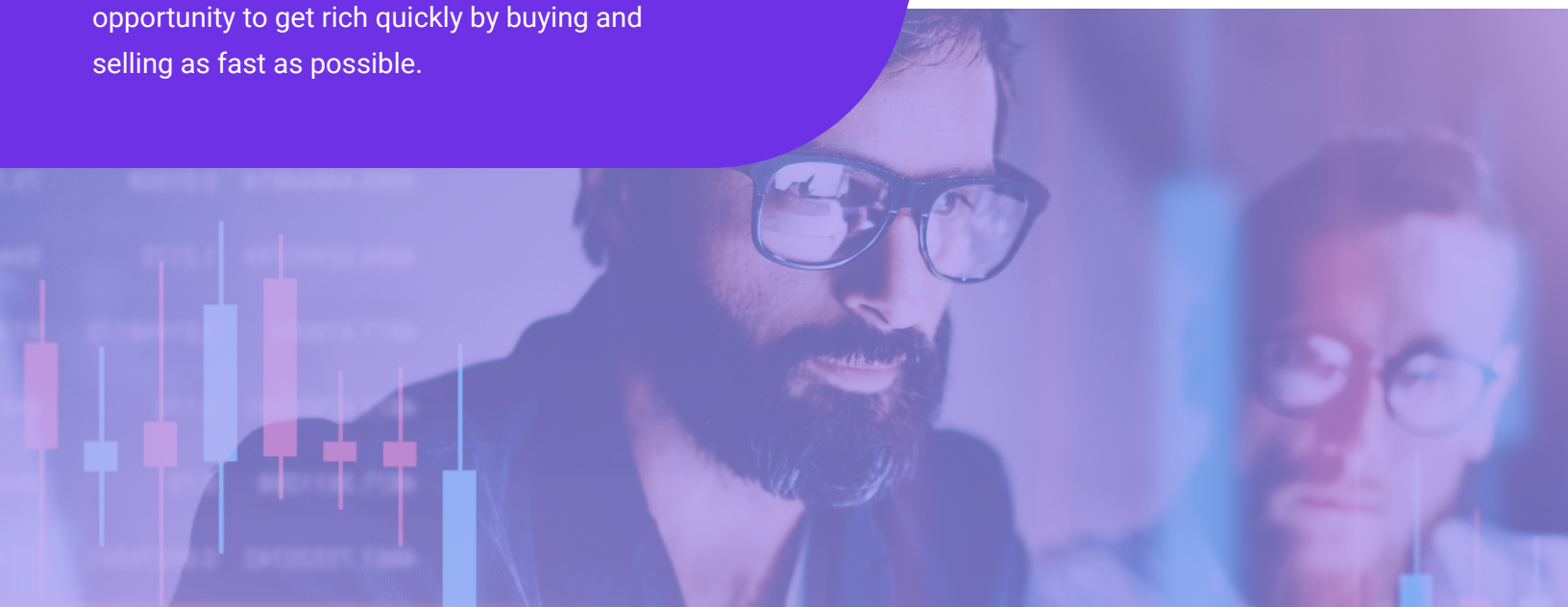
Irreversibility

Unlike fiat currencies (such as the US dollar), there usually aren't legal protections for cryptocurrencies. Crypto payments generally aren't considered reversible as the only way to get money back is if the person you paid returns it.

Pseudonymity

Although they offer a decent amount of anonymity as a user can hold a crypto address without revealing anything about their identity, cryptocurrency transactions are permanent and public hence, sending and receiving virtual currency is a lot like writing under a pseudonym where one person can hold multiple addresses, create multiple wallets, or use tumblers/mixers to obfuscate their trail.

On top of these reasons, the fact that crypto is a volatile and complex technology that is far from easy to understand is helping the fraudsters' cause. Scams such as fake coins, fake exchanges, and similar present an appealing opportunity to get rich quickly by buying and selling as fast as possible.



The nSure.ai Solution

1 Lack of Checks → KYC

Unlike its banking counterpart, blockchain lacks common KYC (Know Your Customer) and anti-money laundering checks. These are two sets of standards that make sure customers are who they say they are and prevent criminals from depositing or transferring funds that came from illegal activity.

Our Dynamic KYC™ lets you know who your customer is and what their intentions are.
As detected by advanced behavioral analysis, crypto exchanges no longer need to worry about leaving money on the table with fraudulent transactions.

2 Chargeback Fraud → Chargeback Guarantee

The all too familiar type of fraud mostly happens when converting a fiat currency to crypto.
A fraudster purchases a cryptocurrency via a stolen credit card number and sends it to another wallet, which triggers a chargeback request from the actual cardholder. The exchange then issues a refund while still the fraudster keeps the stolen goods.

In some cases where phishing is involved, a user buys a cryptocurrency with their credit card and thinks they are sending it to their own wallet. However, they actually click a link that sends the cryptocurrency to someone else (a fraudster's wallet), which is a reason enough to request a chargeback — yet another way crypto exchanges can be hurt.

Don't suffer the consequences fraudsters cause. With nSure.ai, we guarantee low chargebacks with a fraud CB rate no higher than 0.5%. You get coverage for all chargebacks, regardless of the reason.

3 Unbalanced Friction and Protection → Less Friction, More Protection

In the near future, experts predict compliance will become stricter, and not enforcing checks such as two-factor authentication or allowing weak passwords will yield severe penalties.

The process will require revisiting with minimal friction and maximal protection to strike a proper balance.

Doing so with nSure.ai contractually guarantees an SLA of 500ms on every decision we provide.
No need for user verification, 3D Secure, or other SCA.

Result

Going forward, crypto payment fraud isn't a problem you can ignore. The repercussions of allowing fraudsters into your site, either as registered users or through backdoor hacking, can be catastrophic.

Right now, many crypto exchanges that fell victim to fraudulent attacks just chalk it up to the cost of doing crypto.

This is bad.

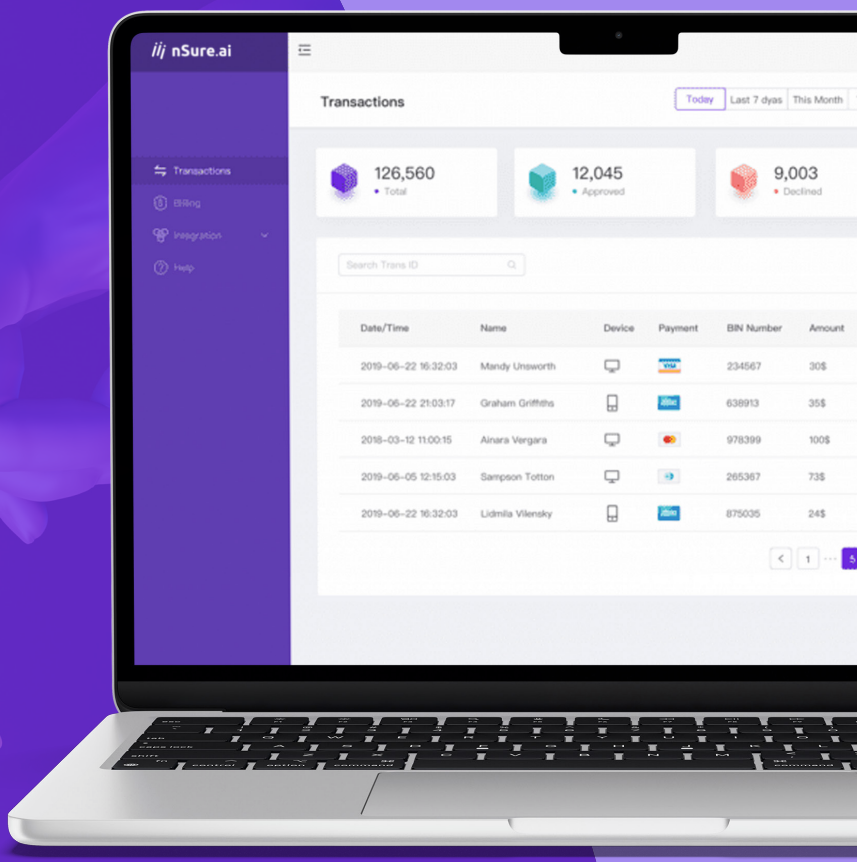
Fraud should never, ever be accepted as part of the cost of doing business.

A lot of this activity can be cut off at the pass with tools that match customer data with cryptocurrency transaction histories. This can make it easy to identify high-risk customers remain AML compliant and avoid the stigma associated with crypto money laundering.

Anything else is a risk not worth gambling.

Stay Proactive and Secure With nSure.ai's Fraud Prevention Solutions

While there are many unknowns about the future of crypto, one thing is for certain — nSure.ai's fraud prevention is a tool you need in your toolbelt. Get predictability and peace of mind with our full liability shift for crypto today.



nSure.ai