

Putting Lipstick on a Pig

A Deep Dive into Pig Butchering Scams in Crypto



Overview	3
Introduction	4
What is Authorized Fraud	6
Pig Butchering (Shā Zhū Pán - 杀猪盘):	6
How Pig Butchering Fits into the Broader Authorized Fraud Landscape	8
Cyvers Case Study: A Glimpse into the Scope of the Pig Butchering Phenomenon	10
Impact on Crypto Platforms	10
Trends and Growth in 2024	12
Pig Butchering Activity per Coin	13
Pig Butchering: How Does It Work On-Chain	14
1. Movement of Funds	14
2. Laundering Techniques	14
3. Cashing Out and Monetization	14
Recent Regulatory Moves	16
United Kingdom: Authorized Push Payment (APP) Fraud Reimbursement	16
Singapore: Shared Responsibility Framework (SRF)	17
European Union: Proposed Payment Services Directive (PSD3) and Payment Services Regulation (PSR)	18
Australia: Scam Prevention Framework	18
United States: CFPB Proposal	18
Global initiatives to combat pig butchering	20
Operation Shamrock	20
INTERPOL's Global Financial Fraud Assessment	20
U.S. Commodity Futures Trading Commission (CFTC) Alliances	20
Tech Against Scams	20
Implications of Pig Butchering exposure for crypto companies	22
Reputational impact	22
Regulatory scrutiny	22
Lawsuits	23
Methods for Combating Pig Butchering	24
Disrupting the victim-perpetrator communication	24
Criminal and legal enforcement against the perpetrators	24
Preventing fund transfers to scammer addresses	25
Cyvers solution	27
Our Solutions	28

Overview

Fraudulent activity in the crypto space takes various forms and definitions. In many cases, a single fraud scheme may exhibit characteristics that fit multiple classifications.

This report focuses on Authorized Fraud - a type of fraud where the user willingly initiates a payment, albeit based on false and misleading information. This stands in contrast to Unauthorized Fraud, in which attackers extract funds from users without their consent or approval. Within the realm of Authorized Fraud, this report will primarily examine Pig Butchering scams - one of the most pervasive and organized fraud techniques in the crypto industry.

The findings presented in this report are based on a comprehensive analysis of Cyvers's unique data, the latest academic research on authorized fraud and Pig Butchering in cryptocurrency, various OSINT sources (including media reports, expert publications, and industry analyses), as well as exclusive insights gathered from Cyvers's clients.

Get started with Cyvers today!

[Book a Demo](#)

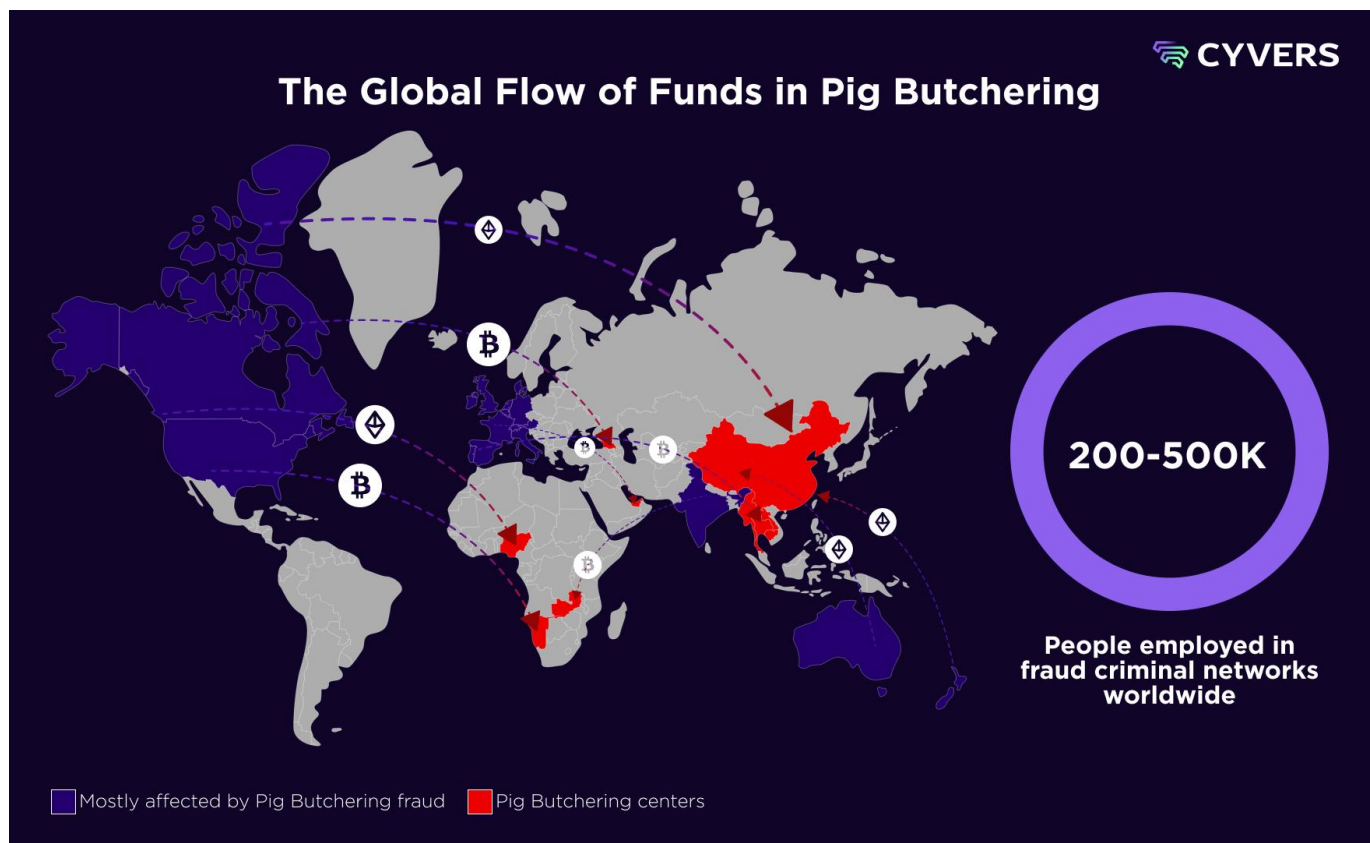
Introduction

At the time of writing, cryptocurrency is experiencing a strong resurgence. After a prolonged crypto winter that lasted until mid-2023, token prices have rebounded, fueled by the landmark approval of crypto-ETFs.

This January, the markets received yet another boost with U.S. President Donald Trump stepping into the Oval Office, pledging to become the most crypto-friendly president in history.

But this influx of retail and institutional capital has attracted more than just investors and innovators. Cybercrime is thriving, with billions of dollars stolen each year through hacks, scams, and fraud. Cryptocurrency fraud is rapidly escalating, shaping up to be one of the biggest threats to crypto holders, platforms, and the industry as a whole. Among the most notorious fraud techniques is pig butchering - a highly sophisticated and organized scam operation.

The latest Economist podcast series, [Scam Inc.](#), estimates that the true scale of crypto fraud could be as big as that of major U.S. corporations like McDonald's. The report even defines crypto fraud as: "An industry that now rivals the size of the illicit drug trade."



The numbers are staggering. Anywhere between \$20 billion and \$45 billion in lost funds vanished into criminal networks. One telling indicator of this industry's scale is the number of individuals involved - estimated between [200,000](#) and [500,000](#) people worldwide, primarily operating out of Southeast Asia. The flow of stolen funds typically moves from Western countries with high purchasing power into emerging markets.

A toxic mix of clever scam tactics, emerging technologies, and widespread user ignorance has bred a global fraud industry, complete with thousands of criminal enterprises and an entire ecosystem of adjacent services enabling these schemes.

On an individual level, pig butchering has already victimized hundreds of thousands worldwide, wiping out a significant portion of their net worth - often pushing them into debt. But the impact extends beyond retail investors. Crypto platforms - especially centralized exchanges - are hemorrhaging millions, grappling with reputational crises, struggling to maintain banking relationships, and increasingly facing regulatory scrutiny.

As the scale of this fraud continues to grow, both the crypto industry and the public sector are under pressure to develop comprehensive countermeasures - whether by targeting individual scammers or dismantling entire fraud networks.

Efforts to combat this phenomenon are underway, ranging from industry-led initiatives to government-driven regulatory actions and enforcement efforts. The latter has caught many crypto platforms off guard, as they are now expected to provide historical scam data and implement measures to prevent future fraud.

However, these platforms can only scratch the surface of the scam's off-chain elements, as the majority of victims do not report these incidents. In fact, according to data from TRM Labs, only 15% of the victims actually complain. Additionally, raising awareness through on-platform educational initiatives and warnings has proven to be of limited effectiveness due to the deeply manipulative social engineering tactics used in these scams.

As a result, platforms are deemed to rely on on-chain threat detection and investigative methods. Yet, when they do, they quickly realize that existing crypto intelligence and analytics tools are largely inadequate for tackling this growing challenge.

What is Authorized Fraud

Authorized fraud in cryptocurrency refers to financial fraud where victims **voluntarily** authorize transactions under false pretenses, often due to deception, manipulation, or coercion. Unlike unauthorized fraud (such as hacking or direct wallet theft), victims willingly transfer funds, believing they are engaging in legitimate investments, payments, or transactions. This type of fraud is typically facilitated through **social engineering tactics, misinformation, and psychological manipulation**, making it particularly difficult to detect and recover losses.

Authorized fraud in crypto is distinct from unauthorized fraud because the victim's own actions - rather than direct technical breaches - lead to the loss of funds. This distinction often complicates legal and financial recourse, as many jurisdictions consider authorized transactions as non-reversible, even if they result from deception.

Pig Butchering (Shā Zhū Pán - 杀猪盘):

Typically, a combination of romance and investment fraud, where scammers spend weeks or months grooming victims before introducing a fake investment opportunity. Victims are convinced to repeatedly deposit funds until they are completely drained.

- o Scammers often pretend to be wealthy, successful traders.
- o They introduce victims to fake trading platforms, where small, initial profits are shown to build trust before large losses occur.
- o Many scams originate from human trafficking rings, forcing individuals to perpetrate fraud against Western targets.

Initially, scammers establish contact through social media, dating apps, or even mistaken text messages, gradually fostering a sense of trust and emotional connection with the victim. This long-term grooming process is designed to lower the victim's defenses, making them more susceptible to investment suggestions.

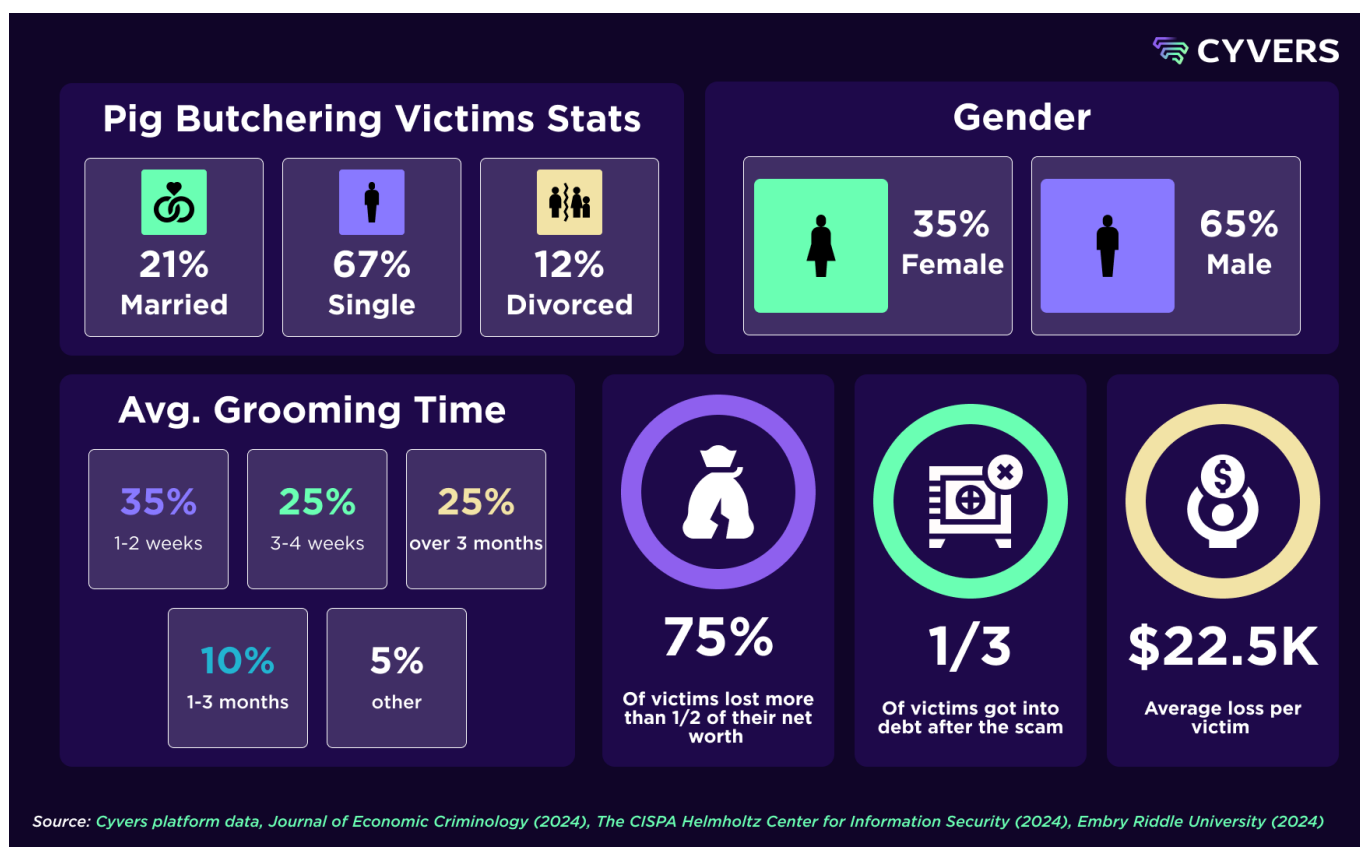
In case of an investment scam, the scammer, often posing as a successful trader or financial expert, introduces the victim to a seemingly legitimate cryptocurrency trading platform or investment opportunity. The victim sees fictitious profits accumulating on the fake platform, leading them to invest even more money.

However, once the victim attempts to withdraw funds or stops investing, they encounter barriers such as fabricated transaction fees or account restrictions.

Eventually, the scammer cuts off communication, leaving the victim financially devastated and psychologically distressed, often ashamed to report the crime.

The demographic profile of pig butchering victims, as depicted in the graph below, reveals a troubling trend. While traditional financial scams have disproportionately affected older individuals, pig butchering scams have expanded to target a younger, tech-savvy demographic. Data indicates that victims between the ages of 30 and 49 are the most affected, comprising the largest segment of reported cases.

Additionally, these scams disproportionately target individuals who are emotionally vulnerable - such as recent divorcees or those experiencing loneliness - by exploiting their personal struggles and trust-seeking behavior. The psychological manipulation tactics employed by scammers, including flattery, fabricated urgency, and social engineering, make it exceedingly difficult for victims to recognize the scam before it is too late.



Pig butchering scams are also uniquely intertwined with human trafficking, where scammers are often victims themselves - coerced into fraudulent activities under duress. These so-called "account managers" (a term imposed by their captors) are held in large compounds, forced to work long hours under harsh conditions, often under armed supervision.

This brutal system exists because pig butchering scams rely on high-engagement, intensive communication between scammers and their victims. Many victims describe their interactions as resembling the early stages of a romantic relationship - where both parties communicate constantly, fostering a deep emotional connection. To maintain the illusion, scammers must juggle multiple victims at once, remaining online nearly 24/7 to sustain the deception.

Yet, these individuals are only the tip of the spear in the pig butchering industry. Behind them lies a vast, [sophisticated network of service providers](#), that enable the scam's operation. This includes hosting services, deepfake tools, financial services (such as money exchange, escrow, and OTC services), as well as design, marketing, translation, and more. Some of them are even offering end-to-end "[Pig Butchering kits](#)" solutions. Together, these elements form a well-organized, highly profitable ecosystem, allowing pig butchering scams to thrive on a global scale.

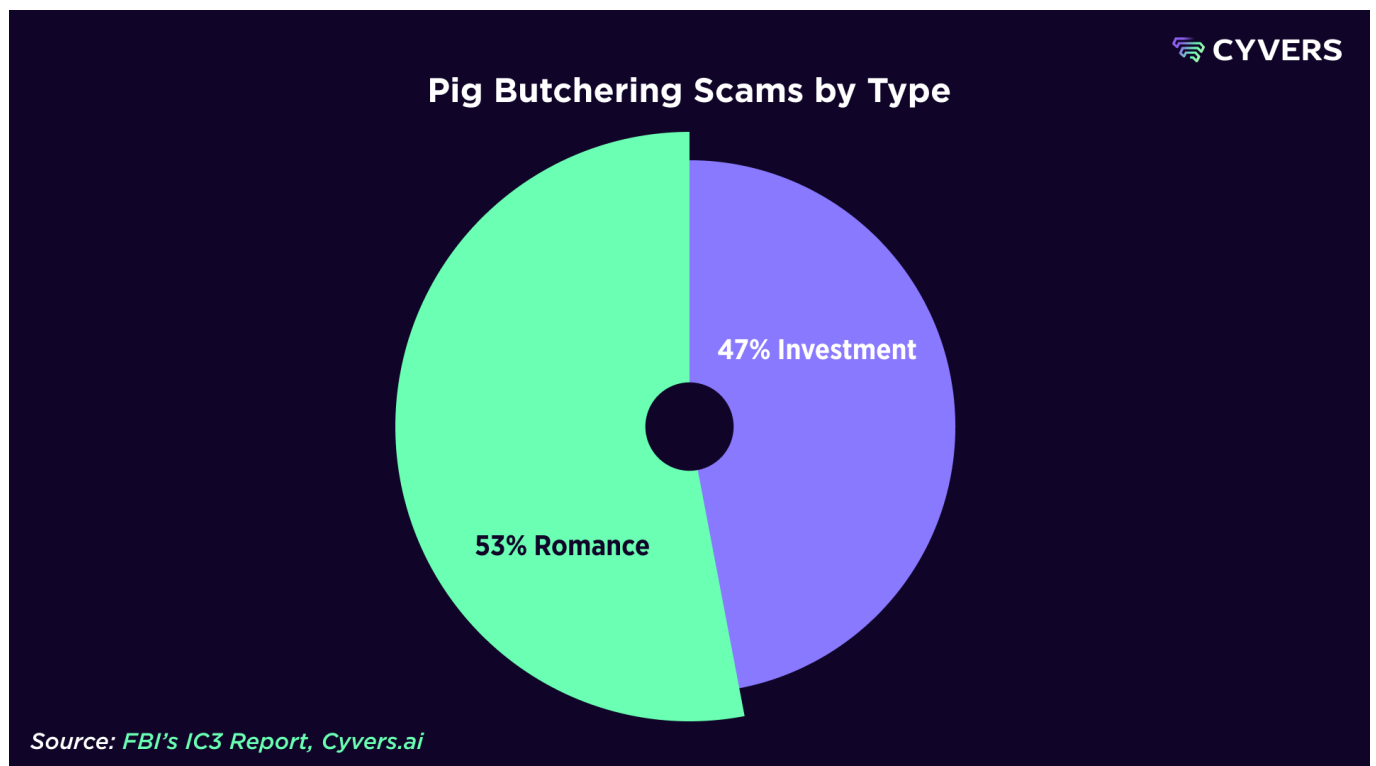
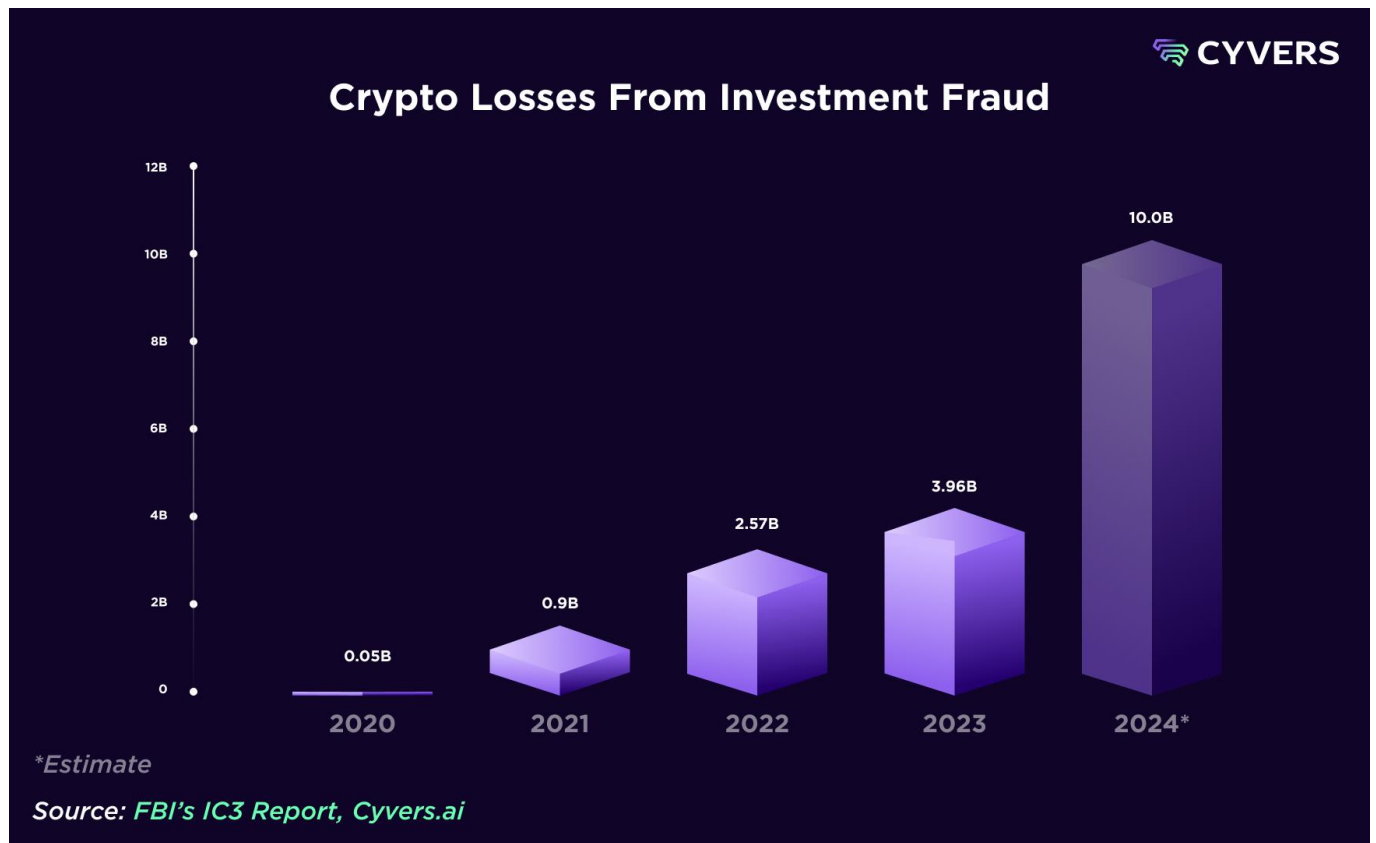
How Pig Butchering Fits into the Broader Authorized Fraud Landscape

Pig Butchering now dominates the fraud scene in crypto and is responsible for over 60% of all authorized fraud in crypto. It is the "Swiss knife" of fraud, given that it is often **a hybrid of romance fraud and investment scams**, making it particularly **destructive**. Unlike traditional Ponzi schemes or rug pulls, Pig Butchering operates on **long-term psychological grooming** rather than quick deception.

It shares characteristics with:

- **Romance scams** → Uses emotional manipulation to establish trust.
- **Investment fraud** → Encourages victims to invest in fake trading platforms.
- **Ponzi schemes** → Creates the illusion of high returns before the final financial drain.





Cyvers Case Study: A Glimpse into the Scope of the Pig Butchering Phenomenon

Cyvers actively monitors blockchains to detect Pig Butchering scams, uncovering fraudulent networks and their affiliated wallets. Below, we present a study conducted in 2024 on 150 leading crypto platforms, including centralized exchanges, payment service providers (PSPs), and on/off-ramp platforms, banks and more - with a focus on the Ethereum blockchain.

Our findings reveal the staggering scale of this fraud:

- Over 200,000 cases of Pig Butchering scams were identified.
- More than \$5.5 billion was stolen across 1.15 million fraudulent transactions.

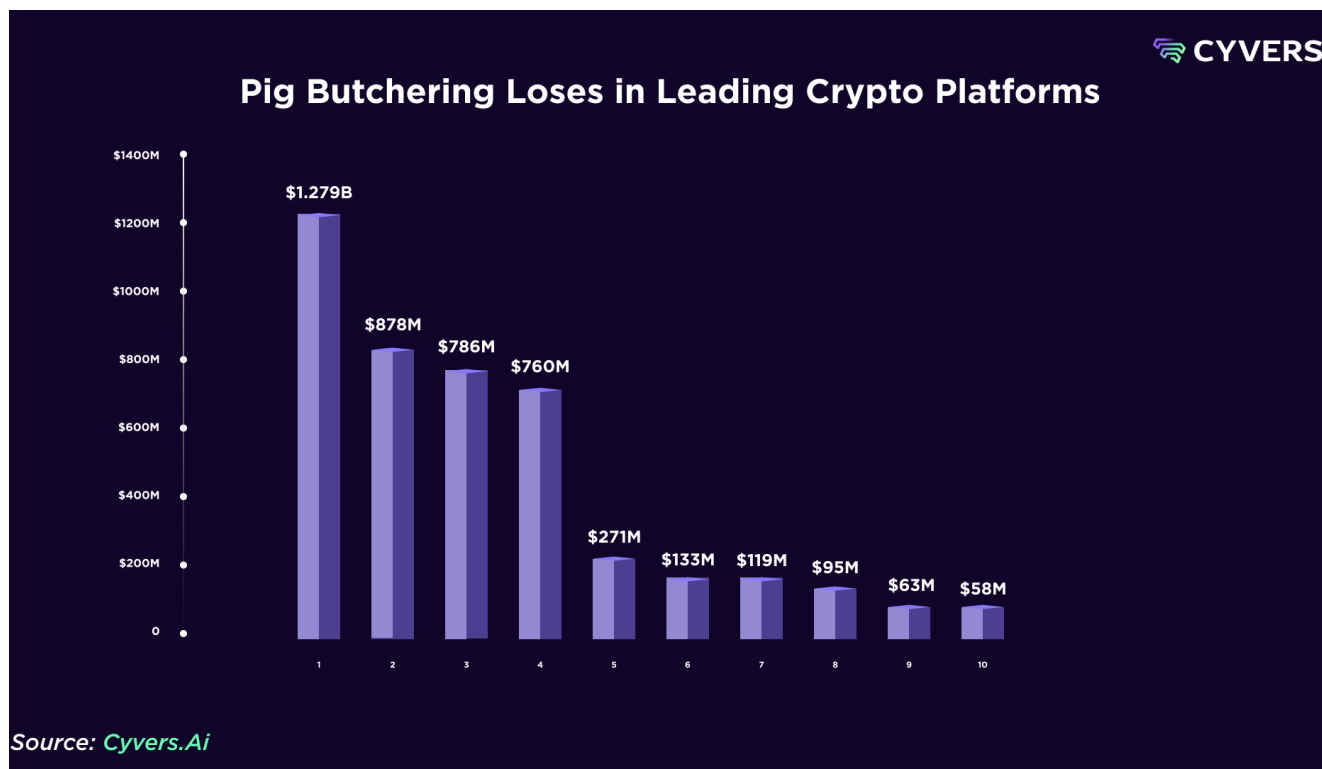


Impact on Crypto Platforms

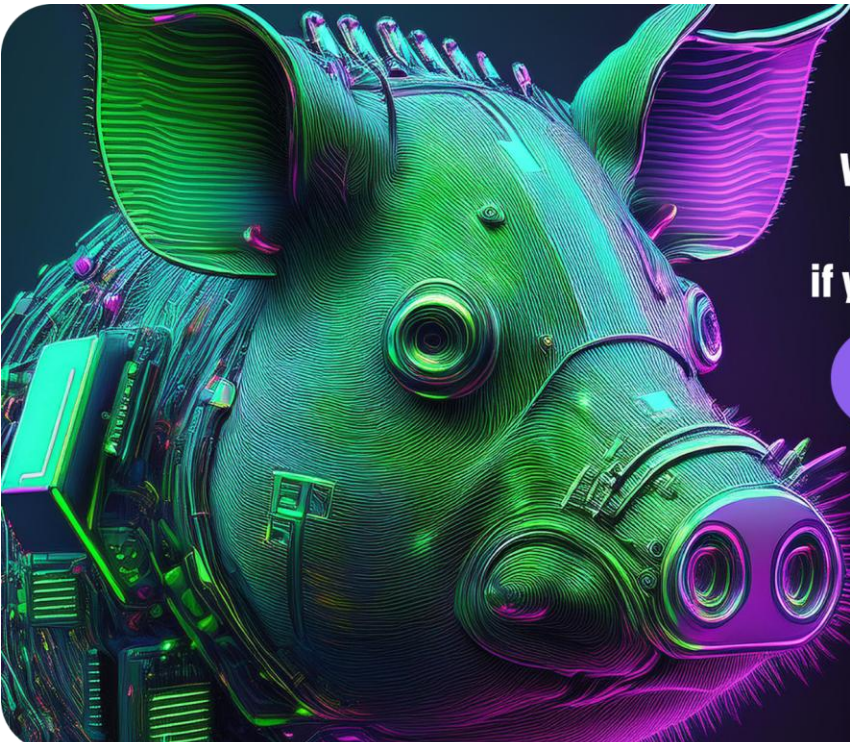
The severity of Pig Butchering fraud varies significantly across platforms. While some exchanges and service providers experienced widespread fraud, with thousands of victims and billions in stolen funds, others showed minimal Pig Butchering activity.

Among the top 10 most affected platforms, we identified:

- Three of the five largest crypto exchanges (by trading volume).
- A crypto-friendly bank.
- An institutional trading platform.



]



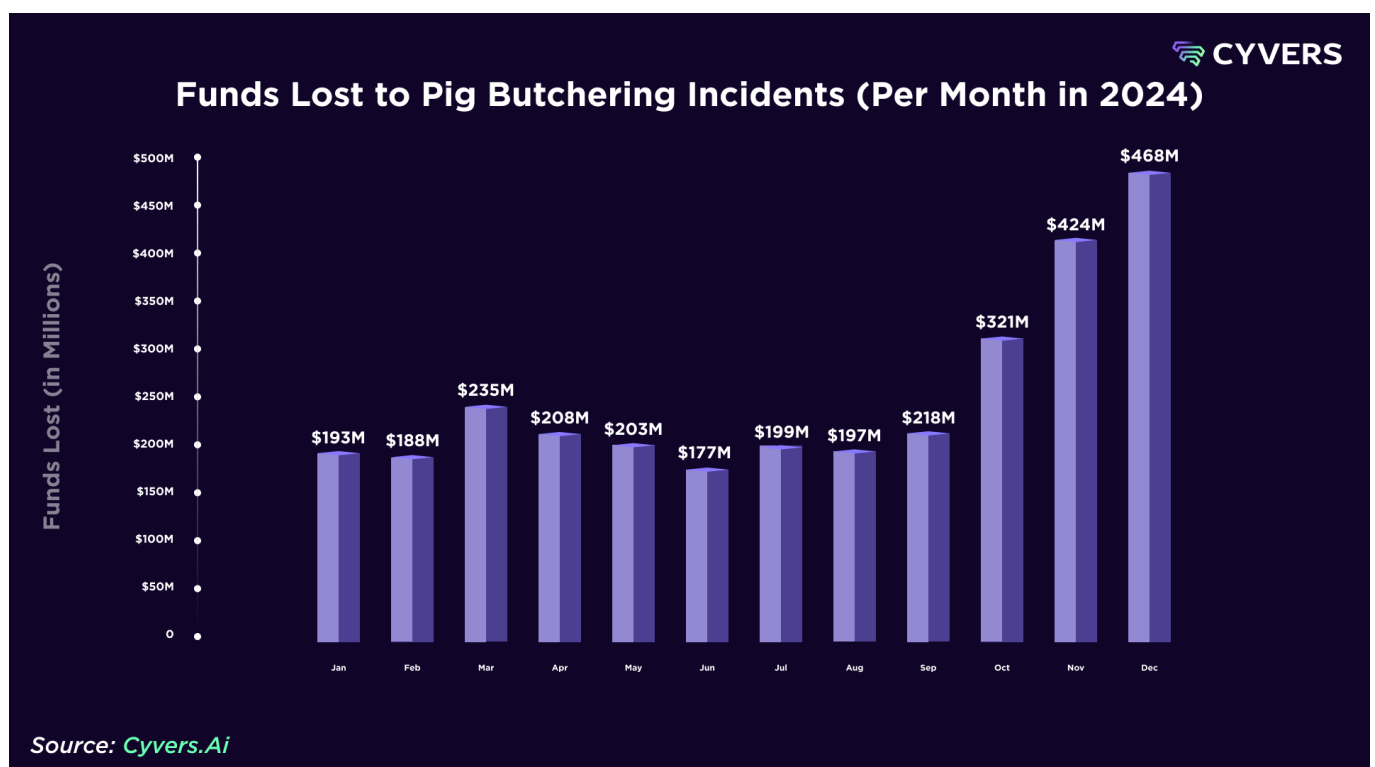
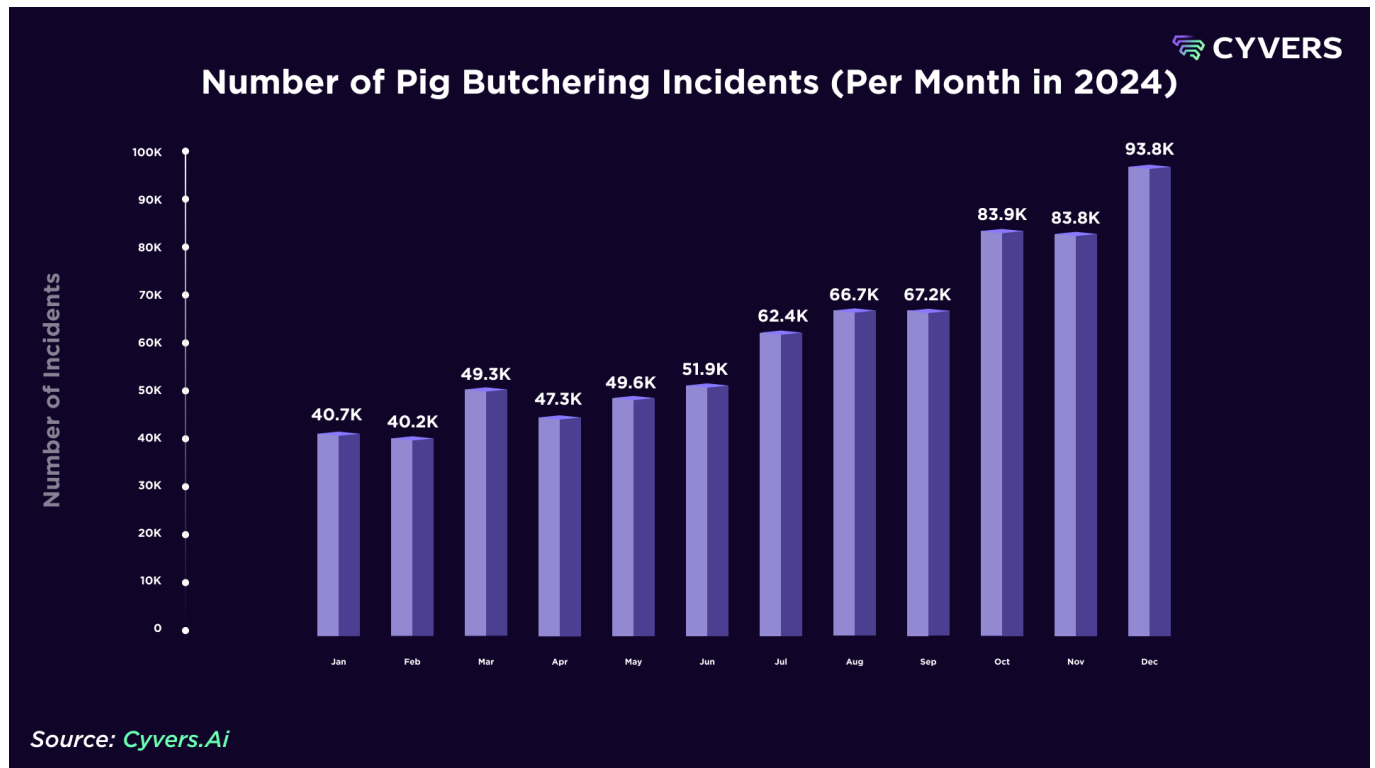
Want to see which platforms made the list - and find out if your platform is among them?

Click Here

to uncover the names behind these staggering losses.

Trends and Growth in 2024

Our study also observed a steady increase in Pig Butchering activity throughout the year, partially correlating with market sentiment and rising crypto inflows. This growth was reflected in both the number of reported incidents and the total value of stolen funds.

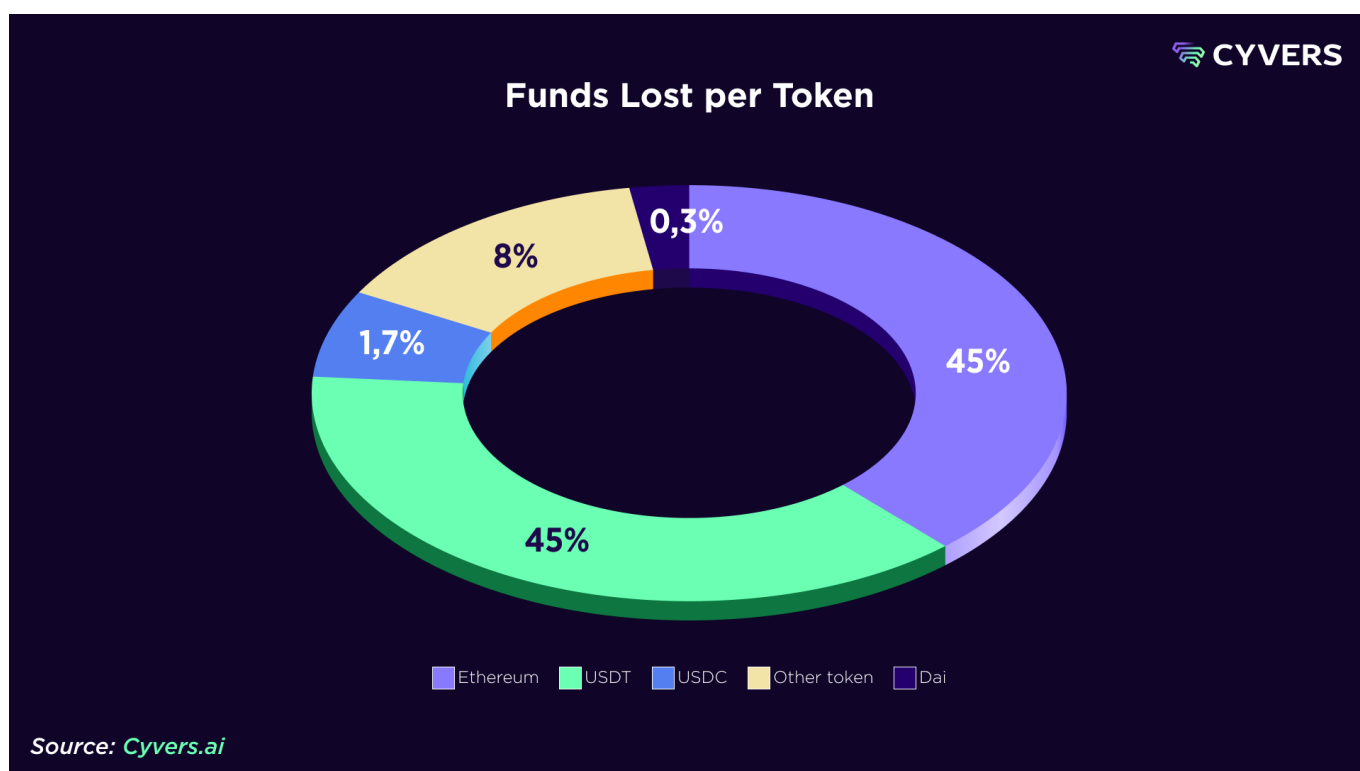


Pig Butchering Activity per Coin

The majority of funds stolen in Pig Butchering scams are concentrated in just a few coins. While fraudsters exploit various coins and tokens, certain coins stand out as the primary vehicles for illicit transactions. The breakdown reveals a strong preference for high-liquidity and widely accepted assets, making them the top targets for laundering stolen funds.

Stablecoins, particularly those with deep market penetration, play a critical role in scam operations due to their ease of conversion and perceived stability. Meanwhile, major smart contract platforms also see significant fraudulent activity, given their dominance in decentralized finance (DeFi) and large transaction volumes.

This chart illustrates the distribution of stolen funds across different cryptocurrencies, highlighting which assets are most frequently exploited in these scams.



Pig Butchering: How Does It Work On-Chain

The operators of the fraud networks are aware of the fact that they can get caught and exposed, given the transparency of the blockchain network and the existence of transaction monitoring tools. Scammers use various methods to obfuscate their activities, including multiple transactions, swapping between cryptocurrencies via DeFi smart contracts, and bridging assets across blockchains.

1. Movement of Funds

- **Multiple Small Transactions:** Scammers engage in multiple micro-transactions to build trust with victims and avoid suspicion.
- **Layering through Exchanges:** Funds are transferred across multiple wallets before reaching major exchanges, making tracking difficult.
- **Use of Centralized Exchanges (CEXs):** Major platforms like Binance, Huobi, and OKX are frequently used as cash-out points.
- **Exploitation of DeFi Protocols:** Smart contracts and decentralized exchanges (DEXs) are leveraged for laundering funds.

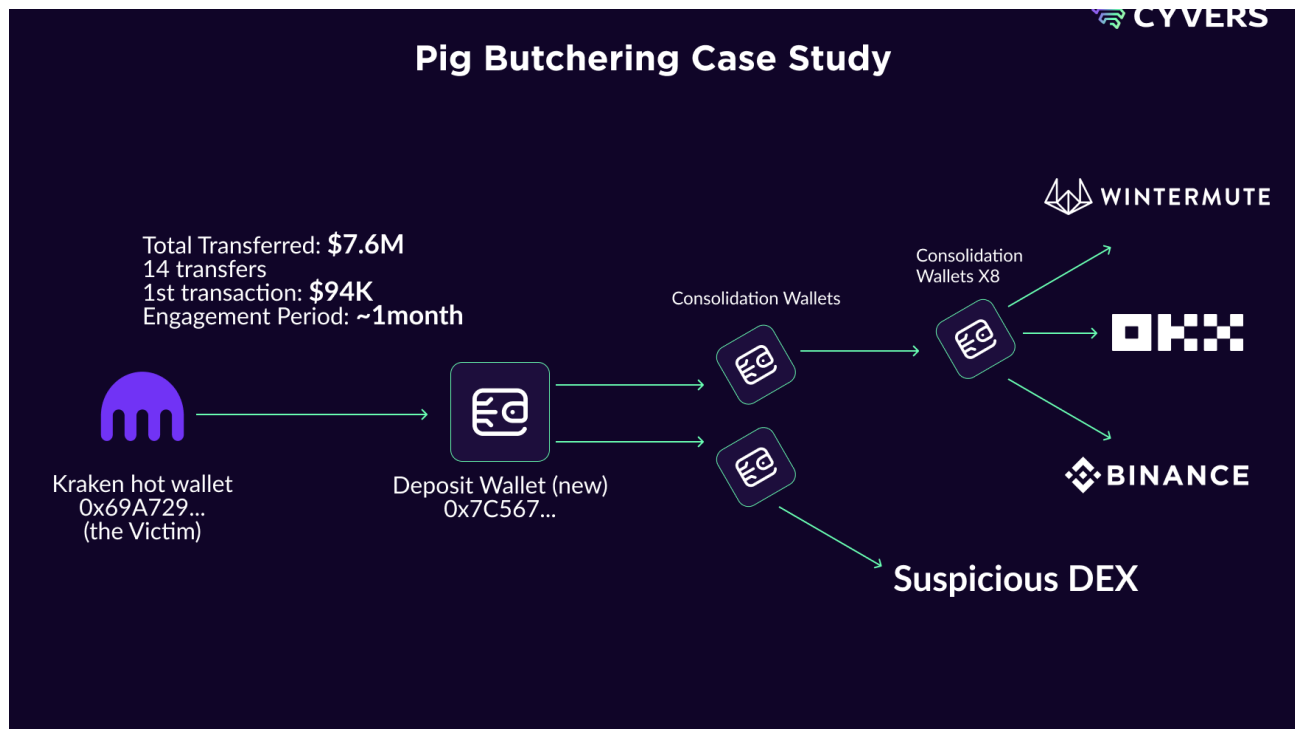
2. Laundering Techniques

- **Cross-Chain Bridging:** Scammers move stolen assets between different blockchains (Ethereum, Binance Smart Chain, etc.) to break tracking chains.
- **Token Swaps in DeFi:** Cryptocurrency is exchanged for privacy-oriented tokens like Monero (XMR) via decentralized platforms.
- **Tether (USDT) as a Key Asset:** Stablecoins like USDT are often used for their liquidity and ease of conversion into fiat currency.

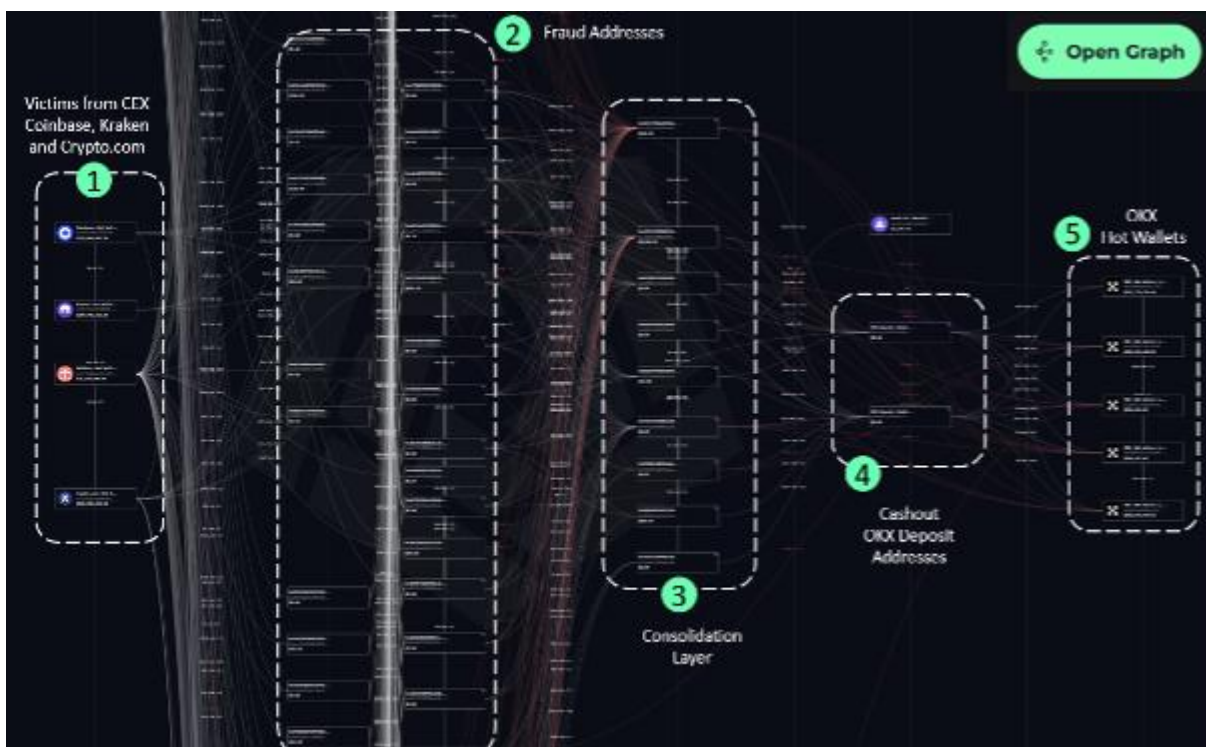
3. Cashing Out and Monetization

- **OTC (Over-the-Counter) Markets:** Scammers prefer OTC brokers who operate without strict KYC policies.
- **Money Mules:** Recruited individuals withdraw fiat currency from cryptocurrency exchanges to avoid direct tracing to scammers.
- **Gift Card and Prepaid Card Conversions:** Stolen crypto is sometimes converted into digital gift cards, which can be resold for fiat money.

Below, you can see a simplified chart of a real use-case of pig butchering scam and the money trail, starting from the victim and all the way to the perpetrator, as uncovered by cyvers.



If we zoom out and look at the pig picture, we can see a very complex map of fund transfers, with multiple layers.



Recent Regulatory Moves

In response to the escalating sophistication of digital fraud, various jurisdictions have implemented regulatory frameworks to enhance consumer protection and assign accountability among financial institutions, telecommunications companies, and consumers.

While most of these regulatory moves apply mostly to TradFi institutions and PSPs, the repercussions of this step have a spill-over effect that goes beyond these realms and is gradually affecting exchanges and other crypto platforms.



United Kingdom: Authorized Push Payment (APP) Fraud Reimbursement

In the United Kingdom, the regulatory framework for combating Authorized Push Payment (APP) fraud has been significantly strengthened with the implementation of mandatory reimbursement rules. These measures, effective from 7 October 2024, aim to enhance consumer protection and hold Payment Service Providers (PSPs) accountable for fraudulent transactions.

This step represents a significant advancement in consumer protection, with potential implications for broader financial services, including the cryptocurrency industry.

Key Provisions of the Legislation:

- **Mandatory Reimbursement:** PSPs are required to reimburse victims of APP fraud for qualifying transactions conducted via the Faster Payments System (FPS) and CHAPS. This mandate replaces the previous voluntary Contingent Reimbursement Model (CRM) Code, ensuring more consistent protection for consumers.
- **Reimbursement Cap and Excess Fee:** The legislation sets a reimbursement cap of £85,000 per claim. Additionally, PSPs have the discretion to apply an excess fee of up to £100 per claim, though this is not mandatory and varies among institutions. Vulnerable consumers are exempt from this excess fee.

While the current APP fraud reimbursement rules primarily target traditional banking transactions, the evolving regulatory landscape indicates a growing emphasis on consumer protection across all financial services, including the crypto sector.

Crypto exchanges and service providers should proactively consider implementing robust fraud detection and prevention measures to align with these regulatory trends and to protect their customers from potential scams.

Singapore: Shared Responsibility Framework (SRF)

Effective from 16 December 2024, Singapore's SRF delineates duties and liabilities among financial institutions, telcos, and consumers to combat phishing scams. Key obligations for specified financial institutions include:

- **Real-Time Notification Alerts:** Providing immediate alerts for activities such as digital token activations, new device logins, high-risk transactions, and outgoing payments.
- **Accessible Reporting Channels:** Offering customers channels to report and block unauthorized transactions, including self-service options to restrict account access.
- **Real-Time Fraud Surveillance:** Establishing systems to detect and prevent unauthorized transactions associated with phishing scams.

European Union: Proposed Payment Services Directive (PSD3) and Payment Services Regulation (PSR)

The European Union is advancing efforts to bolster consumer protection through the proposed PSD3 and PSR. These proposals aim to expand the liabilities of PSPs, requiring them to reimburse consumers for fraud losses. These initiatives signify the EU's dedication to enhancing accountability and security within its payment services framework.

Australia: Scam Prevention Framework

In November 2024, the Australian government introduced legislation establishing a "scams prevention framework," imposing fines up to \$50 million on banks and social media companies that fail to prevent scams. This framework distributes liability among telecommunications companies, social media platforms, and banks, marking a comprehensive approach to combating digital fraud. Additionally, it provides victims with clear pathways to compensation if regulated entities fail in their duties to prevent, detect, report, disrupt, and respond to scams.

United States: CFPB Proposal

In the United States, discussions are ongoing regarding the allocation of liability for cyber scams. While some advocate for making banks partially liable, similar to approaches in the UK and Australia, there is currently no federal mandate requiring banks to reimburse scam victims. The debate continues as stakeholders consider the balance between consumer protection and the responsibilities of financial institutions and technology companies.

On January 10, 2025, the CFPB proposed a rule that would require crypto asset service providers to reimburse users for funds lost due to illicit activities, including hacks and unauthorized transactions. This proposal seeks to extend the protections of the Electronic Fund Transfer Act (EFTA) to encompass digital assets such as stablecoins and other fungible cryptocurrencies used as mediums of exchange or payment. The CFPB interprets the term "funds" within the EFTA to include assets that function like money, thereby granting consumers transacting in cryptocurrencies similar rights to those of traditional bank account holders.

The proposed rule is currently open for public comment until March 31, 2025, after which the CFPB will decide on its final implementation. If enacted, this rule would mandate that cryptocurrency companies enhance their security measures and

maintain sufficient reserves to cover potential losses from unauthorized transactions, aligning their responsibilities with those of traditional financial institutions.

It is yet to be seen how the new president's administration and **its de-regulation and crypto-friendly approach will affect this initiative.**



Global initiatives to combat pig butchering

Operation Shamrock

Operation Shamrock is a collaborative initiative that unites law enforcement agencies, financial institutions, technology companies, and non-governmental organizations to combat cyber scams, including pig butchering. The operation focuses on educating the public, seizing assets from scammers, and disrupting the infrastructure supporting these fraudulent activities. By streamlining reporting processes and building coalitions across various sectors, Operation Shamrock aims to dismantle cybercriminal networks and provide real-time support to victims.

INTERPOL's Global Financial Fraud Assessment

INTERPOL has conducted a comprehensive assessment highlighting the role of technology in enabling organized crime groups to target victims worldwide through scams like pig butchering. The organization emphasizes the need for international cooperation among law enforcement agencies and the private sector to address these crimes effectively. INTERPOL's initiatives include raising awareness, enhancing information sharing, and coordinating cross-border operations to dismantle scam networks.

U.S. Commodity Futures Trading Commission (CFTC) Alliances

The CFTC has formed partnerships with federal and state regulators, as well as consumer protection groups, to address the rise of pig butchering scams. These collaborations focus on educating the public, sharing information, and coordinating enforcement actions to dismantle fraudulent operations.

Tech Against Scams

In May 2024, leading technology and crypto companies formed the Tech Against Scams coalition to combat online fraud and financial schemes. Spearheaded by Coinbase, the coalition includes prominent members such as Meta, Match Group (the parent company of Tinder and Hinge), Kraken, Ripple, Gemini, and the Global Anti-Scam Organization (GASO).

The coalition focuses on:

- **Collaboration Across Industries:** The coalition aims to unite various sectors - including social media, dating platforms, financial institutions, and cryptocurrency firms - to address the pervasive issue of online scams.
- **Sharing Best Practices:** Members will exchange insights and strategies to enhance detection and prevention mechanisms against fraudulent activities.

- **Consumer Education:** A significant focus is on informing users about common scam tactics, such as "pig butchering" and romance scams, to empower them to recognize and avoid potential threats.
- **Disrupting Scam Networks:** By pooling resources and intelligence, the coalition seeks to dismantle the infrastructure that enables scammers to operate across multiple platforms.



Implications of Pig Butchering exposure for crypto companies

Reputational impact

Centralized exchanges, brokers, and on-ramp services play a pivotal role in the crypto ecosystem, acting as the primary interface between the crypto space and mainstream users. Their **ease of use, brand recognition, and “bank-like” user experience** makes them the go-to platforms for newcomers and non-savvy investors entering the crypto space.

This accessibility, however, also makes these platforms the primary conduit for **pig butchering scams**, as victims unknowingly transfer funds through them before being defrauded by perpetrators. The increasing prevalence of such scams - and their **high-profile exposure in media and regulatory discussions** - has led to **severe reputational damage** for these platforms and the broader crypto industry. This damage is particularly evident in:

- **Erosion of Trust** – Victims often associate legitimate exchanges with fraudulent activity, leading to a wider perception of crypto platforms as unsafe.
- **Perceived Inaction** – Many users believe that exchanges are not doing enough to combat fraud, deterring retail investors from engaging with these platforms.

As a result, a growing number of potential users avoid **crypto altogether** or **choose to disengage from platforms linked to fraud cases**, creating a **negative feedback loop that stifles mainstream adoption**.

Regulatory scrutiny

Fraud targeting users of crypto platforms often place **unwanted regulatory attention** on the companies operating these services. Platforms perceived as **facilitating fraudulent activity** - whether through lax oversight or insufficient preventive measures - risk being flagged by regulators, leading to **heightened scrutiny and potential enforcement actions**.

This can result in:

- **Regulatory Labelling** – Platforms suspected of enabling scams may be publicly identified as high-risk by financial watchdogs, damaging their credibility.
- **Enforcement Actions** – Authorities may impose fines, operational restrictions, or even revoke regulatory licenses, severely impacting a platform’s ability to operate in key markets.

As global regulators increase their focus on consumer protection and anti-fraud measures, crypto platforms that fail to proactively address these concerns may find themselves facing crippling legal and compliance challenges.

Lawsuits

Crypto platforms, particularly centralized exchanges, and even traditional banks are often perceived as primary enablers of Pig Butchering scams due to their failure to protect users. This perception frequently leads victims to file lawsuits - both individual and class-action - against these platforms.

For example, in May 2023, Binance and several financial institutions, including TD Bank, [were sued by a Texas woman](#) who fell victim to a Pig Butchering romance scam. The scam began with an interaction on Tinder and ultimately led to the victim losing \$8 million.

In another case, [a California victim filed a lawsuit in January 2024](#) against three banks, alleging "willful blindness" to the fraud. The victim claimed that the banks failed to implement adequate fraud prevention measures, allowing the scam to take place.

But these lawsuits aren't just coming from individual victims. In December 2023, [the Consumer Financial Protection Bureau \(CFPB\) sued](#) Bank of America, JPMorgan Chase, and Wells Fargo, accusing them of failing to protect customers from fraud on Zelle, a widely used instant payment network.

Many of these lawsuits end in settlements or result in court rulings that sometimes favor the companies, reinforcing the argument that platforms and banks cannot be held accountable for every fraudulent transaction. However, the evolving regulatory landscape is increasingly shifting responsibility onto financial institutions. As legal frameworks tighten, these lawsuits are expected to become more frequent and more likely to result in rulings against banks and crypto platforms.

Methods for Combating Pig Butchering

Given the complex and multi-faceted value chain of pig butchering schemes, the scam process can be stopped by targeting various parts of this mechanism.

Disrupting the victim-perpetrator communication

One way to disrupt the fraud value chain is by targeting the points of contact between the victims and the perpetrators. This can be done mostly by social media platforms that can act against fake profiles targeting the victims.

In May of last year, leading tech companies such as Meta, Match Group (the company behind Tinder), along with leading crypto companies like Coinbase, Gemini and Kraken – have announced the establishment of Tech Against Scams initiative. The initiative includes sharing data on scammers and collaborating on various prevention efforts. Efforts such as deleting fake profiles, deplatforming scam apps and more. [Meta announced](#) last November that it removed two million accounts related to pig butchering scams.

Google went beyond just deplatforming and [sued developers](#) that built fraudulent apps that were downloaded by more than 100,000 people.

But the efficiency of these steps is limited due to the fact that the scammers will find ways to create new fake profiles and to approach their potential victims on less cooperative platforms (like Telegram and TikTok).

Criminal and legal enforcement against the perpetrators

Another approach to combating pig butchering scams is to focus on the perpetrators and beneficiaries of these fraudulent activities. This requires a coordinated effort by global law enforcement agencies and governments to dismantle scam campuses in Southeast Asia and their international networks. However, large-scale enforcement efforts have been limited, either due to feasibility challenges or a lack of political will within the international community.

To take meaningful action, law enforcement agencies need precise and actionable data on fraudulent transactions. More importantly, they must be able to trace the flow of funds to identify and apprehend the perpetrators. This process requires comprehensive, verifiable data - both on-chain and off-chain - that meets legal evidentiary standards for prosecution. Without such robust intelligence, investigations and legal actions face significant hurdles in achieving successful convictions.

Moreover, given the scale of this phenomenon and the resource constraints faced by law enforcement, fraud detection and investigative tools must be automated, scalable, and easy to deploy. Automated intelligence solutions can streamline evidence collection and forensic analysis, ensuring that investigations remain efficient, scalable, and capable of handling the vast complexity of pig butchering schemes.

For example, last year, the US government issued a forfeiture process for more than \$2.5 million in USDT linked to pig butchering scams. The court complaint highlights the length and complexity of tracing the money trail and identifying affiliated wallets. The investigation involved:

- Multiple subpoenas
- Forensic accounting and financial analysis
- Collaboration with international law enforcement agencies, including the Royal Thai Police
- Specialized investigators dedicated to tracking illicit crypto transactions

This case underscores the significant challenges law enforcement faces in tackling crypto fraud and the need for advanced investigative tools to combat these schemes effectively.

Preventing fund transfers to scammer addresses

Finally, there's the possibility of blocking fund transfers issued by users to scammer addresses. This is not a new concept that requires building solutions from scratch. Traditional finance (TradFi) and fiat-based companies have successfully prevented financial fraud for decades, primarily through payment providers such as Mastercard and [Visa](#). These companies achieve fraud prevention by monitoring user accounts, transactions, and fund transfer destinations to identify anomalies and respond accordingly.

This process involves analyzing key parameters, such as:

- Transaction velocity and recurrence (frequency and speed of transactions)
- Iterations of destination accounts (patterns in repeated transfers)
- Other behavioral indicators that suggest fraudulent activity

Moreover, the integration of artificial intelligence (AI) in fraud detection and prevention has enabled faster and more precise tools for monitoring, labelling, and detecting suspicious activity. Mastercard, for instance, has emphasized the critical role

of AI in its [recent vision for the payments landscape](#), highlighting its effectiveness in fraud detection.

In theory, these fraud detection practices should be even easier to implement in the blockchain space. Since blockchains are open ledgers, all wallets, token balances, and transactions are publicly visible for anyone to review.

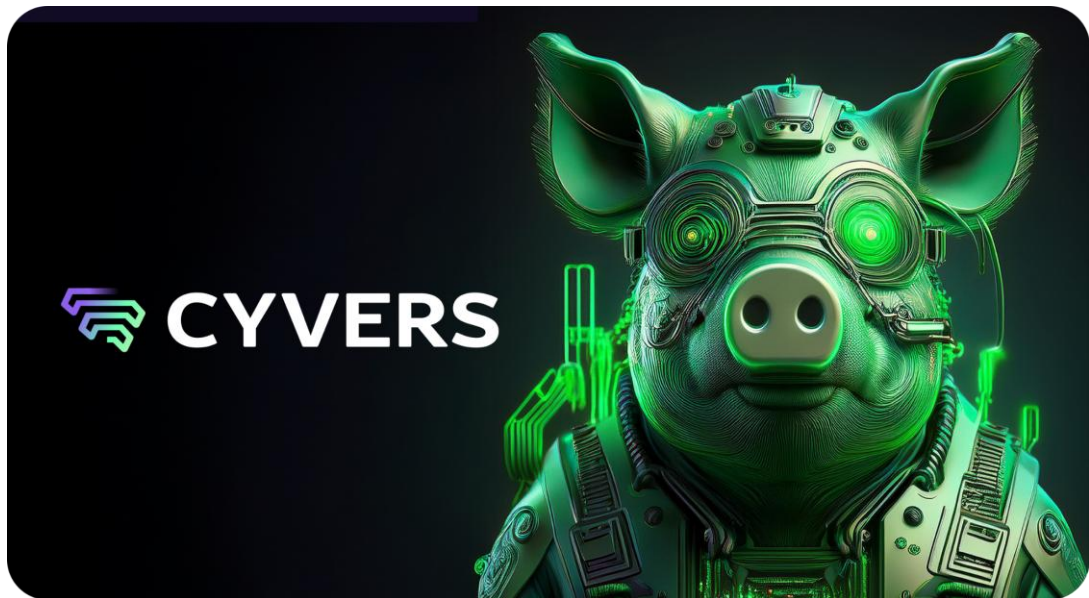
However, there is a major caveat: while blockchain is data-rich, it is context-poor. The relative anonymity of crypto wallets and the ease of creating new wallets make it extremely challenging to differentiate between legitimate and fraudulent transactions. As a result, identifying and blocking illicit activity in blockchain ecosystems remains a highly complex task.

The primary enforcement agents in this process should be centralized crypto entities - including exchanges, brokers, payment service providers (PSPs), and on/off-ramp platforms. These entities act as the key touchpoints between victims and scammers, processing the majority of the funds flowing through pig butchering schemes. Additionally, they possess the technical capability to detect and block suspicious transactions in real-time.

However, these platforms face two major obstacles:

- 1. A lack of actionable intelligence** - They struggle to access real-time, high-quality fraud data to distinguish between the vast majority of legitimate transactions and the small minority of malicious ones.
- 2. Balancing security with user freedom** - They are caught between their mission to facilitate seamless value exchange and their responsibility to protect users from financial harm.

To effectively combat pig butchering, centralized platforms must bridge this gap - leveraging advanced fraud detection tools, strengthening industry collaboration, and integrating blockchain intelligence to proactively prevent illicit transactions.



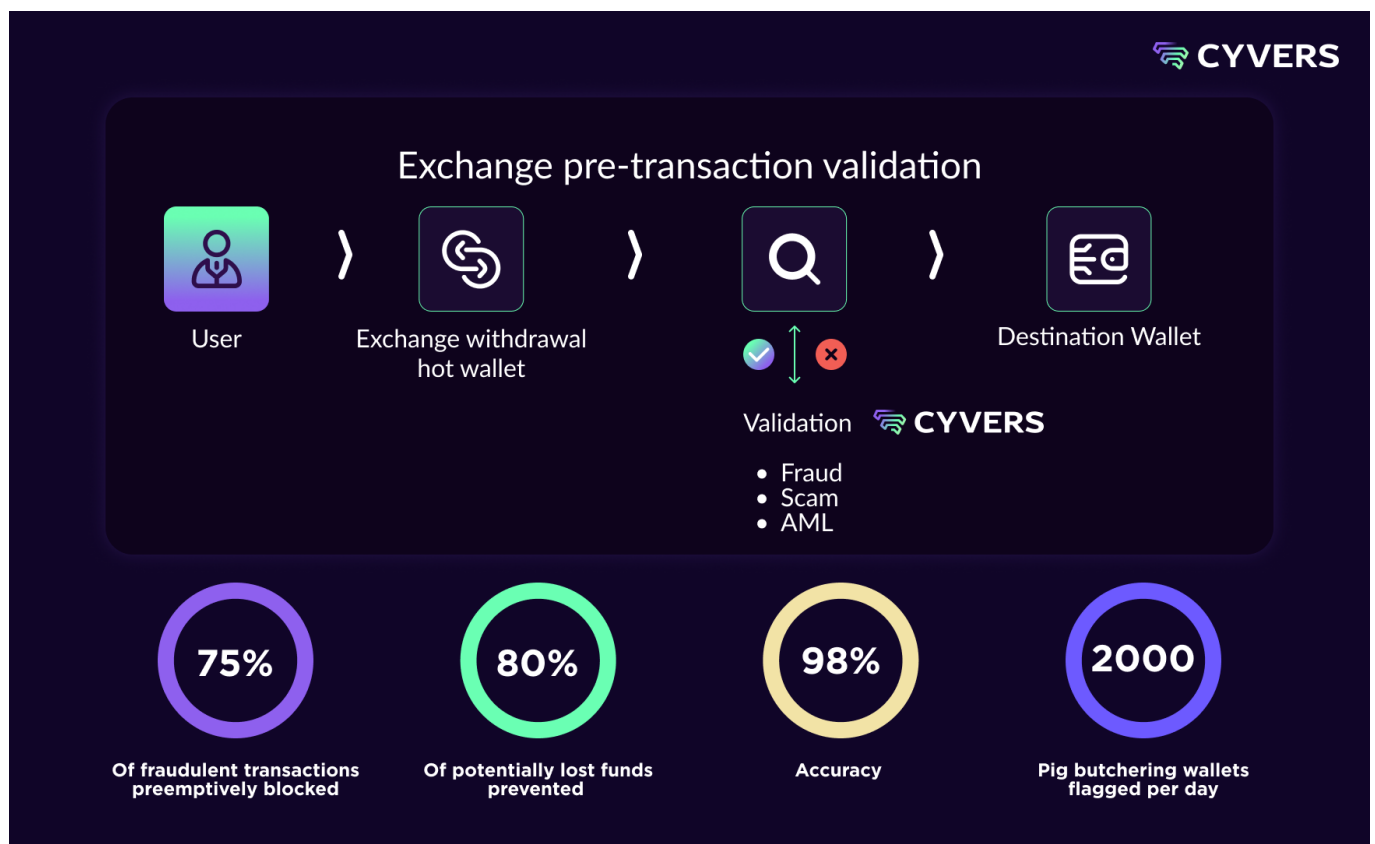
Cyvers solution

Cyvers.ai is a leading Web3 threat prevention and risk mitigation platform, specializing in proactive fraud prevention for cryptocurrency platforms, financial institutions, and public sector entities.

Cyvers provides a unique solution to detect and disrupt Authorized Fraud, with a specific focus on Pig Butchering scams. By leveraging advanced topological AI, geometric anomaly detection, and various clustering techniques, Cyvers analyzes blockchain activity at scale to identify fraudulent patterns.

With a daily impact of:

- ✓ Over 2,000 wallets labeled
- ✓ Dozens of fraudulent networks uncovered
- ✓ More than \$20 million in fraud losses identified per day



Cyvers collaborates with industry leaders such as Crypto[.]com, enabling exchanges, payment service providers (PSPs), banks, and crypto platforms to protect users from fraud in real-time. Through mapping the on-chain activity of global fraud networks, Cyvers helps platforms strengthen user trust, enhance security, ensure compliance, and minimize regulatory exposure.

Beyond the private sector, Cyvers also partners with public sector entities, regulators, and law enforcement agencies by providing real-time fraud intelligence, statistical insights, and forensic data to combat financial crime. These efforts support both policy-making and criminal/regulatory investigations, equipping authorities with the tools needed to track illicit funds and build strong legal cases against perpetrators.

Our Solutions

 **Continuous Monitoring & Alerting:** Real-time monitoring of hot wallets for exchanges, PSPs, public sector institutions, and other platforms to detect exposure to Pig Butchering networks.

 **Pre-withdrawal screening:** Assessment of destination addresses for exposure to fraudulent networks. Delivered via API integration for seamless use within existing transaction security/compliance mechanisms.

Comprehensive Reporting

- Audit-ready compliance reports tailored for global regulatory standards.
- User-friendly insights to improve explainability and transparency for end users.
- Public sector reports to assist government agencies in monitoring large-scale fraud trends and threats.

Investigation & Law Enforcement Support

- Expert assistance for investigative teams in gathering forensic data and tracing money flows in fraud-related cases.
- Collaboration with regulators and law enforcement to provide case-specific evidence and intelligence for prosecutions and asset recovery efforts.

Get started with Cyvers today!

[Book a Demo](#)