Criminals on the Chain: Navigating the Landscape of Financial Crimes in Blockchain

Ka-Ho Chow

Assistant Professor

Cyber Security, FinTech and Blockchain Group

https://khchow.com | kachow@cs.hku.hk

SCHOOL OF COMPUTING & DATA SCIENCE
The University of Hong Kong

TECH

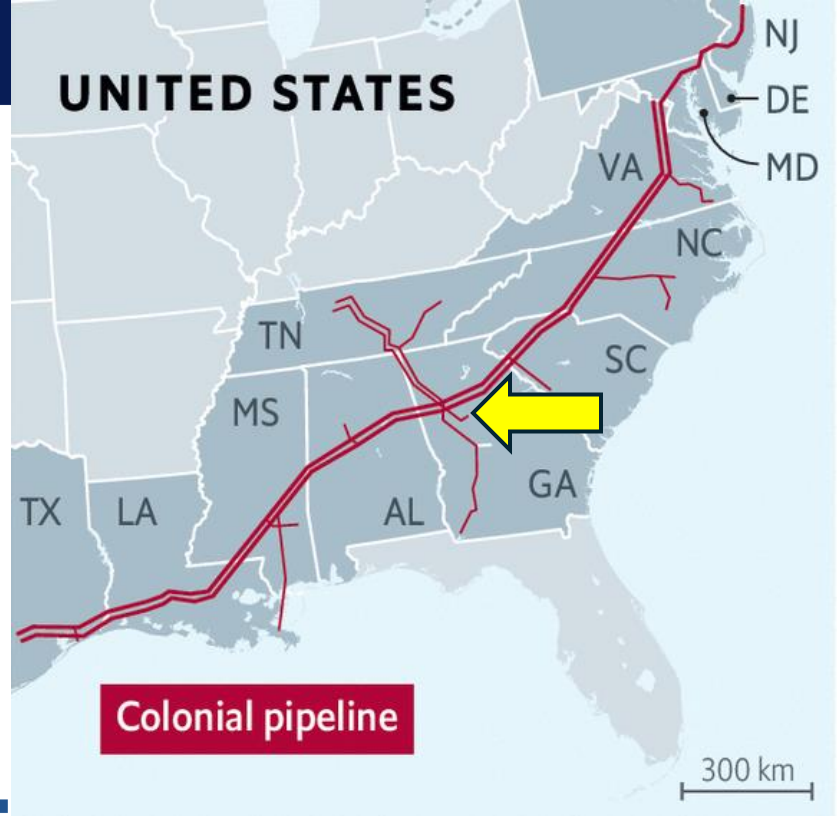
Hackers behind Colonial Pipeline attack reportedly received $90 million in bitcoin before shutting down

PUBLISHED TUE, MAY 18 2021•9:04 AM EDT | UPDATED TUE, MAY 18 2021•4:19 PM EDT

Ryan Browne
@RYAN_BROWNE_

KEY POINTS

- DarkSide, the hacker group behind the Colonial ransomware attack, received $90 million in bitcoin ransom payments, according to blockchain sleuths Elliptic.
- The cybercriminal gang shut down last week after losing access to its servers and as its cryptocurrency wallets were emptied.
- Elliptic said DarkSide's bitcoin wallet contained $5.3 million worth of the digital currency before its funds were drained.



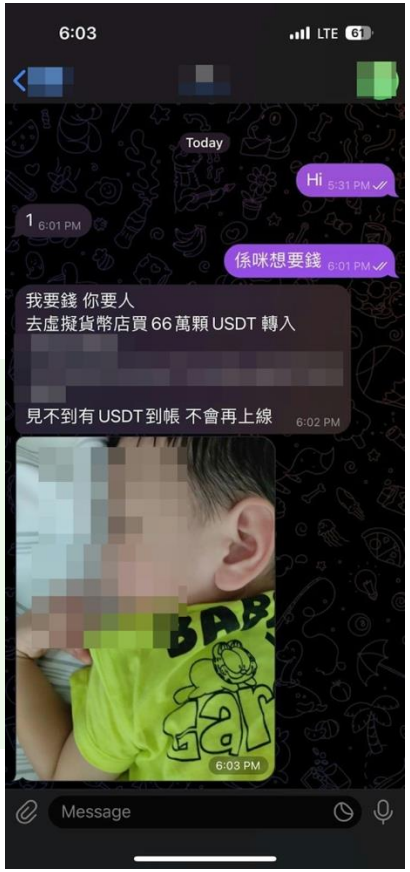
NEWS 3 MIN READ

Kidnappers Demand $600K in Crypto: Hong Kong Parents Forced to Pay USDT Ransom for Toddler's Return

PUBLISHED JULY 4, 2024 3:30 PM
BY LORENA NESSI

Hong Kong Parents Forced to Pay USDT Ransom for Toddler's Return | Source: Chris McGrath/Getty Images

The haunting images from security cameras captured the heart-wrenching moment: the innocent toddler, wide-eyed with fear, abducted in the shopping center.



KEY TAKEAWAYS

- Kidnappers attempt to extort parents in crypto after abducting a child in Hong Kong.
- The case caused an immediate, intense community and media response.
- The police swiftly rescued the child and arrested two men.

01獨家｜港男困緬甸最黑詐騙園區：很多港人受困　家屬付16萬贖人

撰文：蔡苡柔 朱加樟
出版：2024-09-11 17:33　更新：2024-12-16 12:49

東南亞詐騙園區犯罪問題持續受關注，近日《香港01》再次收到有港人被困在緬甸東部詐騙園區的消息，一名26歲香港男子受困「交克園區」五個月，在江蘇常州刑警及內地有相關部門的幫助下，男子家屬在繳付價值約16.3萬港元的泰達幣（USDT） 贖金後，男子始於9月9日獲釋前往泰國，預計11日（周三）從曼谷國際機場搭機返港。

在東南亞長期從事救援行動的華人阿龍斡旋本次的營救行動，他向《香港01》表示，交克園區地處叛軍地盤內，營救難度很大，而且在當地惡名昭彰，為「緬甸東部最黑園區」，「打人，電擊很常見」。

《香港01》在8月底就該個案向香港保安局查詢，保安局稱入境處在接獲家屬求助後，即時透過外交部駐港特派員公署及中國駐緬甸大使館跟進事件，並已按家屬意願提供適切意見及一切可行的協助。

男事主受困「交克園區」5個月後獲釋。（受訪者提供）

CNBC MARKETS BUSINESS INVESTING TECH POLITICS VIDEO INVESTING CLUB PRO

TECH

Hackers behind Colonial Pipeline attack reportedly received $90 million in bitcoin before shutting down

PUBLISHED TUE, MAY 18 2021·9:04 AM EDT | UPDATED TUE, MAY 18 2021·4:19 PM EDT

Ryan Browne
@RYAN_BROWNE_

KEY POINTS

- DarkSide, the hacker group behind the Colonial ransomware attack, received $90 million in bitcoin ransom payments, according to blockchain sleuths Elliptic.
- The cybercriminal gang shut down last week after losing access to its servers and as its cryptocurrency wallets were emptied.

ccn CRYPTO TECHNOLOGY BUSINESS ANALYSIS OPINION

HOME / NEWS / CRYPTO / NEWS / KIDNAPPERS DEMAND $600K IN CRYPTO: HONG KONG PARENTS FORCED TO PAY USD

NEWS 3 MIN READ

Kidnappers Demand $600K in Crypto: Hong Kong Parents Forced to Pay USDT Ransom for Toddler

PUBLISHED JULY 4, 2024 3:30 PM
BY LORENA NESSI

Hong Kong Parents Forced to Pay USDT Ransom for Toddler's Return | Source: Chris McGrath/Getty Images

港聞 娛樂 最平酒店 國際 即時 熱榜 生活 科技 中國 體育 01

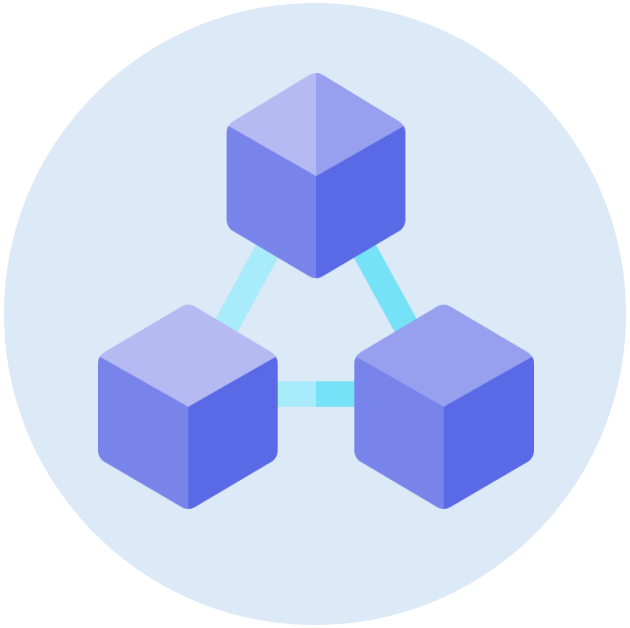
即時中國

獨家｜港男困緬甸最黑詐騙園區：很多港

24-09-11 17:33 更新：2024-12-16 12:49

東南亞詐騙園區犯罪問題持續受關注，近日《香港
困在緬甸東部詐騙園區的消息，一名26歲香港男子
月，在江蘇常州刑警及內地有相關部門的幫助下，
16.3萬港元的泰達幣（USDT）贖金後，男子始於
預計11日（周三）從曼谷國際機場搭機返港。
在東南亞長期從事救援行動的華人阿龍斡旋本次的
01》表示，交克園區地處叛軍地盤內，營救難度很
彰，為「緬甸東部最黑園區」，「打人，電擊很常
《香港01》在8月底就該個案向香港保安局查詢，
屬求助後，即時透過外交部駐港特派員公署及中國
件，並已按家屬意願提供適切意見及一切可行的協

What's wrong with cryptocurrencies like Bitcoin and USDT?



Bitcoin & Blockchain

Crypto Crimes

Countermeasures

Traditional Currencies

- Controlled by central banks & governments
  - Manipulate money supply & interest rates
  - Censorship
- Send and receive money via intermediaries (banks)
- Trust in banks or financial institutions

Get Ready For A World Currency: Bitcoin

Proposed by “Satoshi Nakamoto” in October 2008

Decentralization
No single entity controls it

Financial Freedom
Transactions can be pseudonymous

Fixed Supply
No indefinite money printing

Trustless Transactions
No trust in banks or financial institutions

No Censorship
Governments cannot freeze accounts

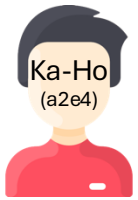
Borderless Transactions
Fast, low-cost international transfers

Bitcoin: A Peer-to-Peer Electronic Cash System

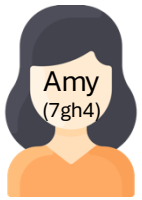
https://bitcoin.org/bitcoin.pdf

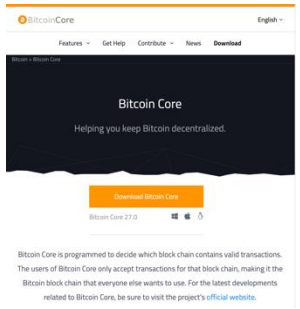
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

A Crash Course on Bitcoin (& Blockchain)



Ka-Ho sends 1 BTC to Amy.





New Transaction:

Sender	Receiver	Amount	Commission
a2e4	7gh4	1 BTC	0.5 BTC

Decentralization

Pseudonymity

Transparency

Immutability

<< Every miner does the same thing >>

Pending Transactions:

Sender	Receiver	Amount	Commission
8754	f511	0.01 BTC	0.0000001 BTC
e7ee	bea4	15 BTC	0 BTC
ad13	85a3	3 BTC	1BTC
be4a	3e4c	0.001 BTC	1 BTC

Proposed New Page (Block):

Maximum Entries : 3

Summary of Previous Page: ....

Sender	Receiver	Amount	Commission
ad13	85a3	3 BTC	1BTC
be4a	3e4c	0.001 BTC	1 BTC
a2e4	7gh4	1 BTC	0.5 BTC

WINNER

+ 3.125 BTC = 5.625 BTC = 2.7m HKD

Statistics of Bitcoin

As of July 2024:

- Number of Blocks: 853,160
  - 560 GB (can fit on your laptop)
  - https://www.blockchain.com/explorer/assets/btc
- Block Reward: 3.125 BTC
  - Around HKD 523,214 every 10 mins
  - Next Halving Date: April 19, 2028
- Profitable?

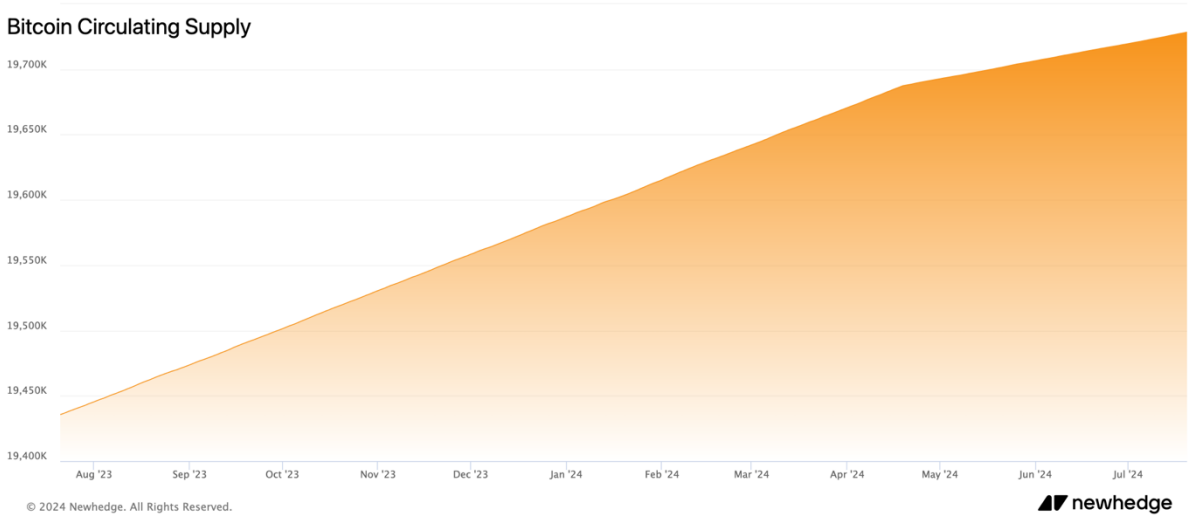
https://bitbo.io/how-many-bitcoin/

19,769,743
Total BTC in Existence

1,230,256
Bitcoins Left to be Mined

94%
% of Bitcoins Issued

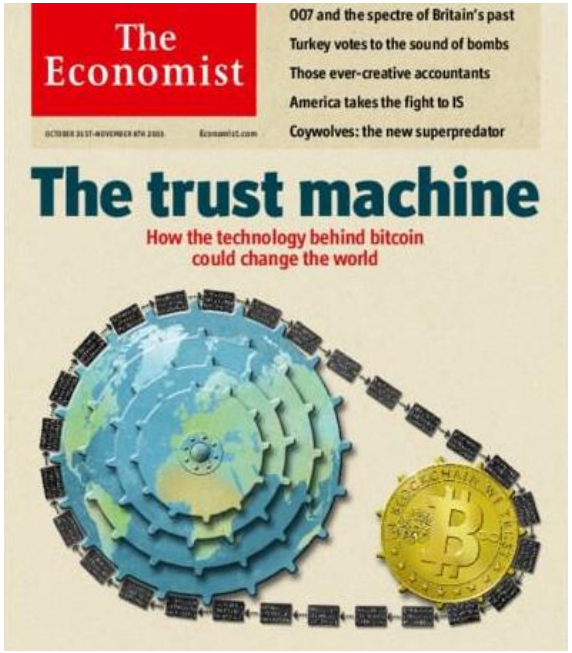
450
New Bitcoins per Day



Why is Bitcoin important?

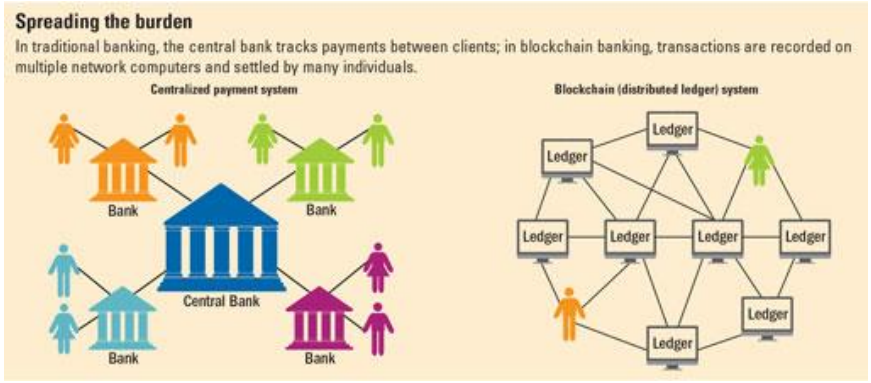
New York Times, January 2014.

"Bitcoin gives us, for the first time, a way for one Internet user to transfer a unique piece of digital property to another Internet user, such that the transfer is guaranteed to be safe and secure, everyone knows that the transfer has taken place, and nobody can challenge the legitimacy of the transfer."



Economist, October 2015.

"The blockchain lets people who have no particular confidence in each other collaborate without having to go through a neutral central authority. Simply put, it is a machine for creating trust."



Altcoins

To improve the limitations of the original digital currency (i.e., bitcoin)

ETH

Allow people to build programs on the blockchain

ADA

Significantly reduce energy consumption

SOL

Achieve high-speed and low-cost transactions

Stablecoins

A type of cryptocurrency whose value is pegged to another asset, such as a fiat currency or gold, to maintain a stable price.

USD

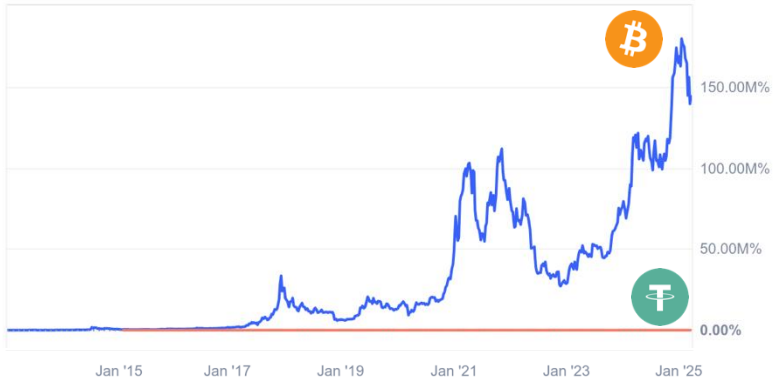
USDT USDC

EURO

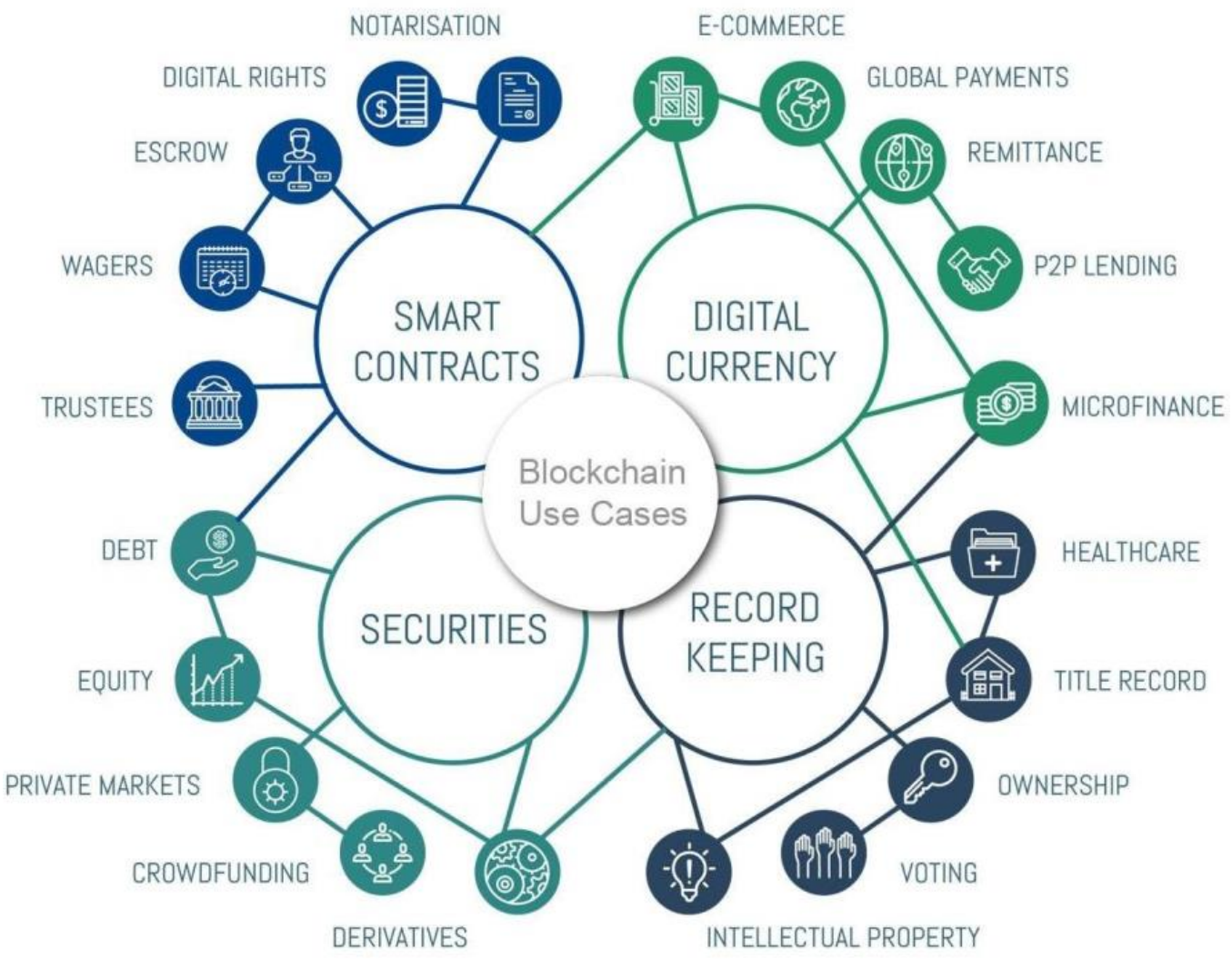
EURS

Gold

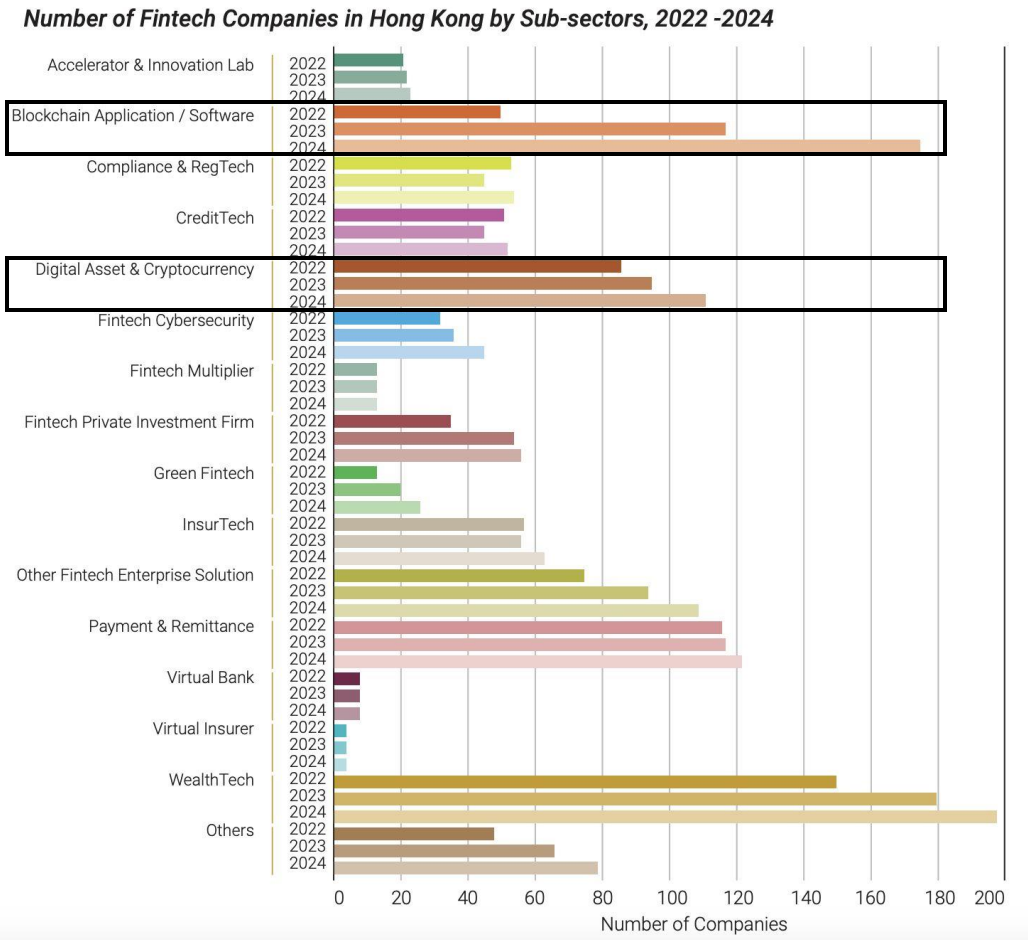
PAXG XAUt



Pervasive Use of Crypto and Its Underlying Tech



The Use Cases of Blockchain That Exist Beyond Crypto Trading
https://www.linkedin.com/pulse/use-cases-blockchain-exist-beyond-crypto-trading-/

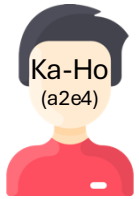


Hong Kong Blockchain Sector Surges 250% Since 2022: Report
https://www.bitget.com/news/detail/12560604642501

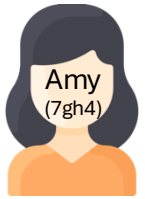
Bitcoin & Blockchain **Crypto Crimes** Countermeasures

Disclaimer: *This part includes inappropriate content, but it is not intended to teach you how to be a smarter criminal. It is to help you recognize and prevent financial crimes.*

Pseudonymity is a Double-Edged Sword



Ka-Ho sends 1 BTC to Amy.



New Transaction:

Sender	Receiver	Amount	Commission
a2e4	7gh4	1 BTC	0.5 BTC

Page (Block) 88917**6**

Sender	Receiver	Amount	Commission
a2d2	211f	1 BTC	0.02 BTC
8754	f511	0.01 BTC	0.0000001 BTC
e7ee	bea4	15 BTC	0.005 BTC
bea4	f15f	3.20 BTC	0.01 BTC
fe1f	5f8a	1.5 BTC	0.1 BTC
ad13	85a3	3 BTC	1 BTC
be4a	3e4c	0.001 BTC	1 BTC
a2e4	**7gh4**	1 BTC	0.5 BTC
ab1e	1ae1	0.2 BTC	0.0001 BTC
... (2000 more entries) ...			

Page (Block) 88917**7**

Sender	Receiver	Amount	Commission
2a3a	2762	0.5 BTC	0.0212 BTC
7gh4	1e23	1 BTC	0.03 BTC
3133	572a	1 BTC	0.023 BTC
5aba	aa3a	1.2 BTC	0.0001 BTC
a78b	8a88	1.1 BTC	0.111 BTC
27ad	51a9	2.1 BTC	0.59 BTC
899a	59e9	3.52 BTC	1.1 BTC
ae36	32e4	0.59 BTC	0.000001 BTC
6a31	55ae	0.97 BTC	0.001 BTC
... (2000 more entries) ...			

- Anyone can create as many accounts as they want.
  - Free of charge
  - No personal information
  - Just get the public key ("username") and the private key ("password")
- Everyone can see all transactions.
  - https://www.blockchain.com/explorer
- Senders and receivers are not directly identifiable.

Crypto Becomes The “Standard Payment Method”

CNBC MARKETS BUSINESS INVESTING TECH POLITICS VIDEO INVESTING CLUB PRO

TECH

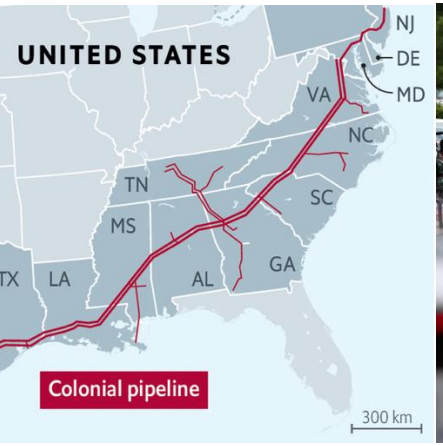
Hackers behind Colonial Pipeline attack reportedly received $90 million in bitcoin before shutting down

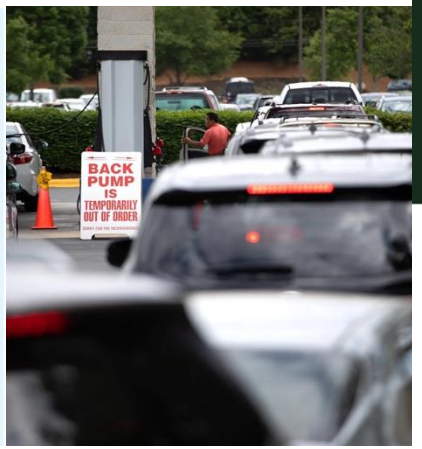
PUBLISHED TUE, MAY 18 2021•9:04 AM EDT | UPDATED TUE, MAY 18 2021•4:19 PM EDT

Ryan Browne
@RYAN_BROWNE_

KEY POINTS

- DarkSide, the hacker group behind the Colonial ransomware attack, received $90 million in bitcoin ransom payments, according to blockchain sleuths Elliptic.
- The cybercriminal gang shut down last week after losing access to its servers and as its cryptocurrency wallets were emptied.





ccn CRYPTO TECHNOLOGY BUSINESS ANALYSIS OPINION E

HOME / NEWS / CRYPTO / NEWS / KIDNAPPERS DEMAND $600K IN CRYPTO: HONG KONG PARENTS FORCED TO PAY USD

NEWS 3 MIN READ

Kidnappers Demand $600K i Crypto: Hong Kong Parents Fo Pay USDT Ransom for Toddler

PUBLISHED JULY 4, 2024 3:30 PM
BY LORENA NESSI

Hong Kong Parents Forced to Pay USDT Ransom for Toddler's Return | Source: Chris McGrath/Getty Images

港聞 娛樂 最平酒店 國際 即時 熱榜 生活 科技 中國 體育 01

即時中國

家｜港男困緬甸最黑詐騙園區：很多港

柔 朱加樟
24–09–11 17:33 更新：2024–12–16 12:49

東南亞詐騙園區犯罪問題持續受關注，近日《香港
困在緬甸東部詐騙園區的消息，一名26歲香港男子
月，在江蘇常州刑警及內地有相關部門的幫助下，
16.3萬港元的泰達幣（USDT） 贖金後，男子始於
預計11日（周三）從曼谷國際機場搭機返港。
在東南亞長期從事救援行動的華人阿龍斡旋本次的
01》表示，交克園區地處叛軍地盤內，營救難度很
彰，為「緬甸東部最黑園區」，「打人，電擊很常
《香港01》在8月底就該個案向香港保安局查詢，
屬求助後，即時透過外交部駐港特派員公署及中國
件，並已按家屬意願提供適切意見及一切可行的協

How Big Was Crypto Crime in 2024?

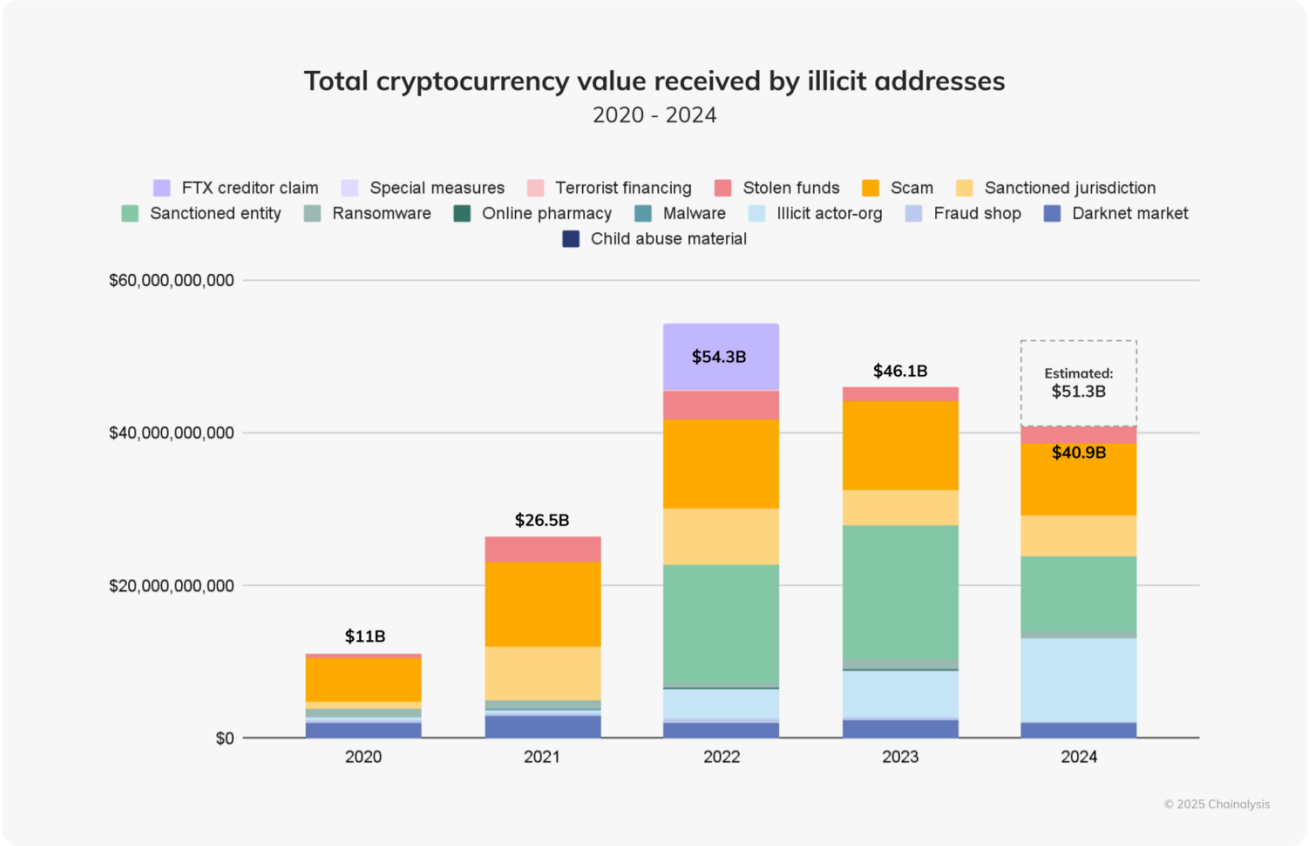
The properties and widespread adoption of crypto give rise to new forms of on-chain criminal activities while also transforming off-chain crimes.

$40B+

received by illicit addresses

0.14%+

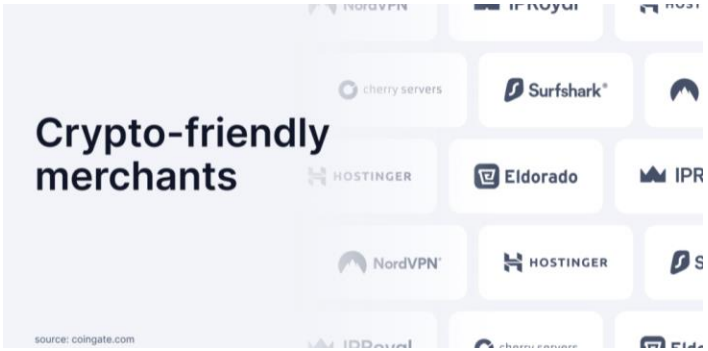
of total on-chain transaction volume

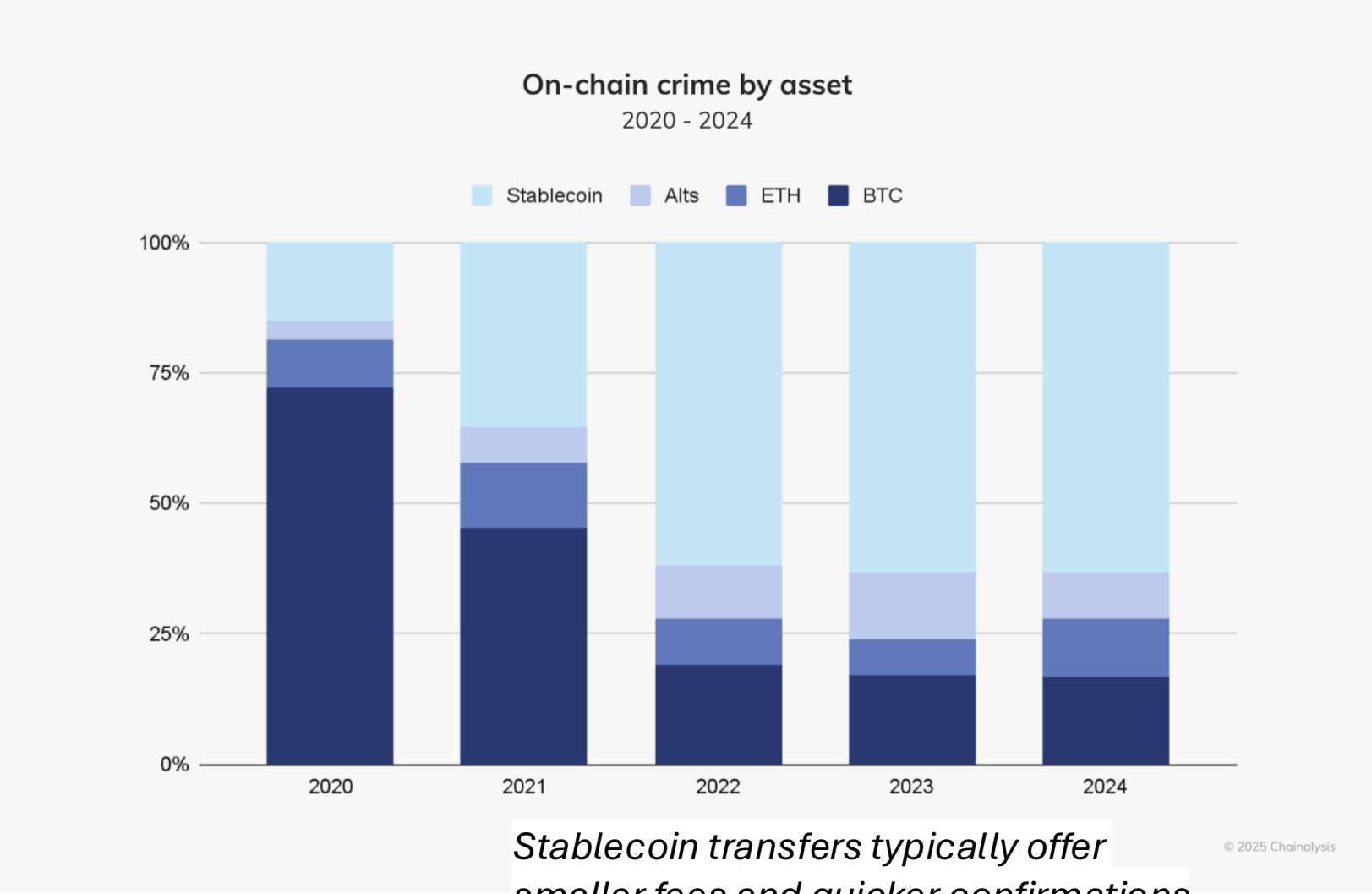


Stablecoins Are Now The Most Popular Currency

- Stability in Value

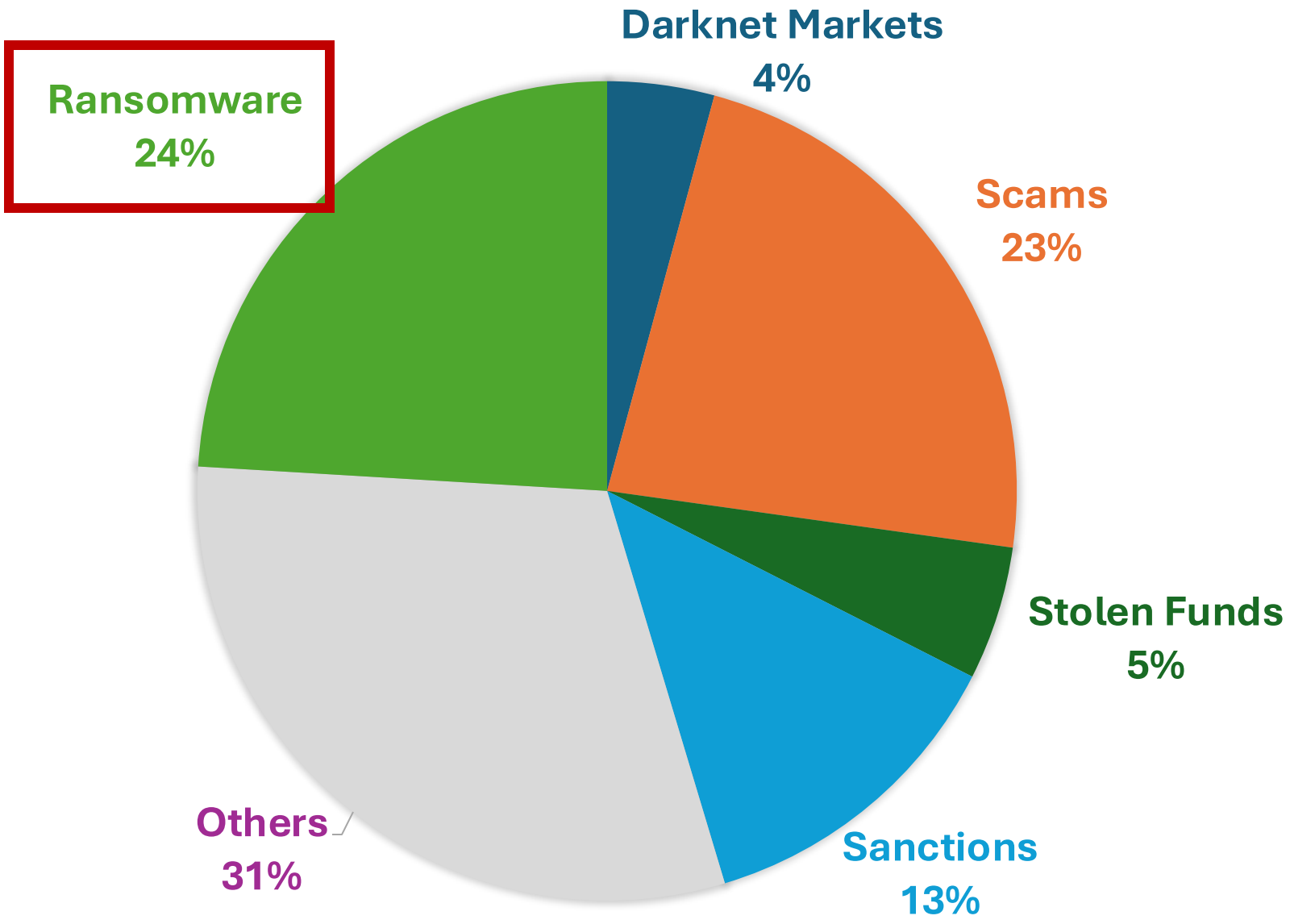
- Liquidity and Wide Acceptance





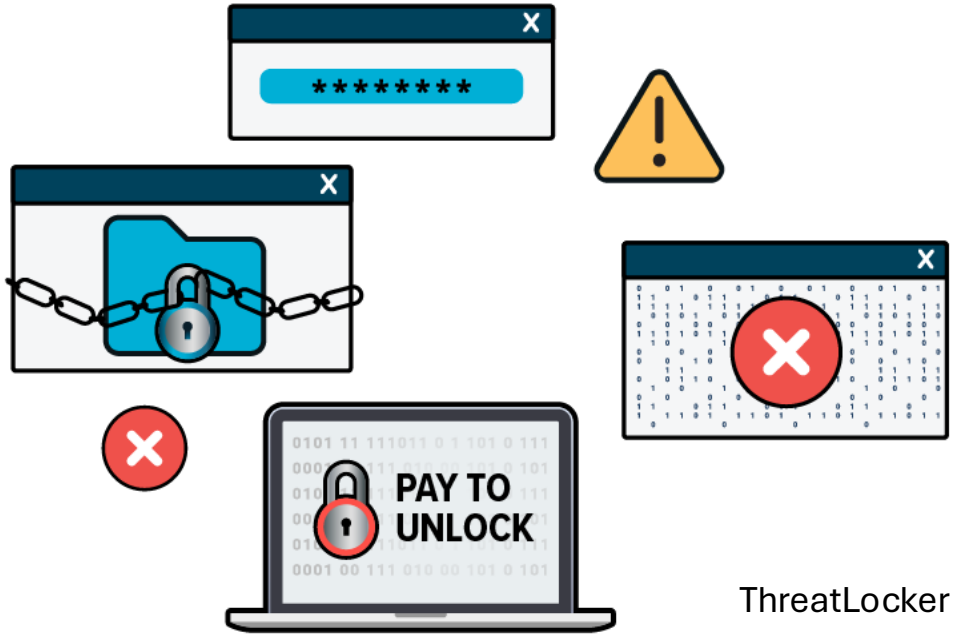
Stablecoin transfers typically offer smaller fees and quicker confirmations

Crypto Value Received By Illicit Addresses in 2024



Ransomware

- Malware that encrypts files and demands a ransom for decryption
  - Spreads through phishing emails, malicious downloads, etc.
  - Often demands payment in cryptocurrency
  - Targets individuals, business, and critical infrastructures
- Common Types
  - **Crypto Ransomware**
    Encrypts files and demands payment
  - **Locker Ransomware**
    Locks the entire system, preventing access
  - **Double Extortion**
    Encrypts data and threatens to leak it



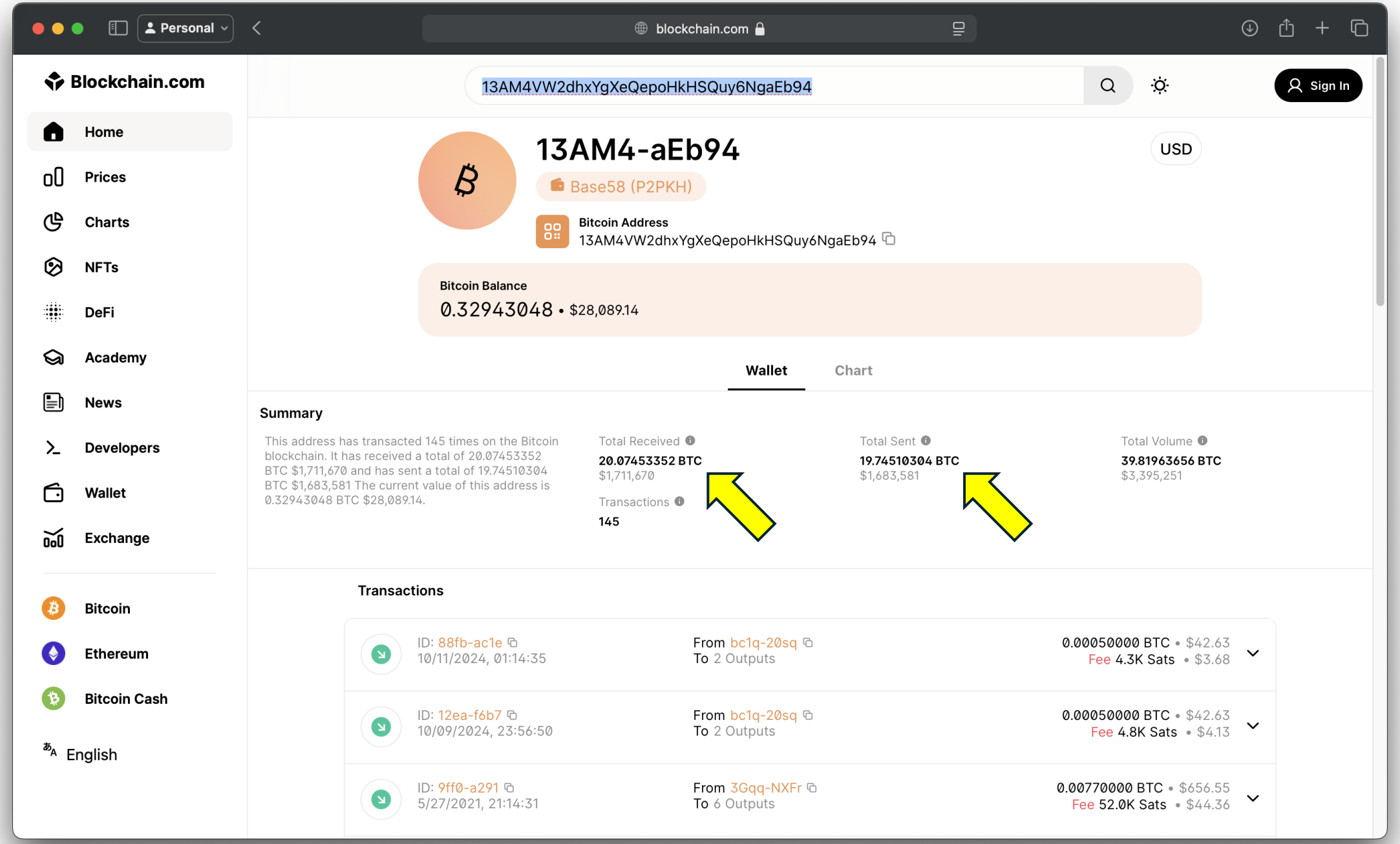
ThreatLocker

WannaCry (2017~Today)

Targets a Windows vulnerability leaked from the NSA

Name	Date	Tags	Size
@Please_Read_Me@.txt	5/13/2017 1:45 PM		1 KB
@WanaDecryptor@.exe	5/13/2017 1:45 PM		1 KB
Chrysanthemum.jpg.WNCRY	7/14/2009 10:22 AM		860 KB
Desert.jpg.WNCRY	7/14/2009 10:22 AM		827 KB
desktop.ini	7/14/2009 10:11 AM		2 KB
Hydrangeas.jpg.WNCRY	7/14/2009 10:22 AM		582 KB
Jellyfish.jpg.WNCRY	7/14/2009 10:22 AM		758 KB
Koala.jpg.WNCRY	7/14/2009 10:22 AM		763 KB
Lighthouse.jpg.WNCRY	7/14/2009 10:22 AM		549 KB
Penguins.jpg.WNCRY	7/14/2009 10:22 AM		760 KB
Tulips.jpg.WNCRY	7/14/2009 10:22 AM		607 KB

Infected more than 230K+ computers (e.g., FedEx, Honda, UK NHS hospital system) in 150+ countries, using 20 different languages to demand ransom from users


Personal
blockchain.com
Blockchain.com
13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94
Sign In
Home
Prices
Charts
NFTs
DeFi
Academy
News
Developers
Wallet
Exchange
Bitcoin
Ethereum
Bitcoin Cash
English
13AM4-aEb94
USD
Base58 (P2PKH)
Bitcoin Address
13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94
Bitcoin Balance
0.32943048 • $28,089.14
Wallet
Chart
Summary
This address has transacted 145 times on the Bitcoin blockchain. It has received a total of 20.07453352 BTC $1,711,670 and has sent a total of 19.74510304 BTC $1,683,581 The current value of this address is 0.32943048 BTC $28,089.14.
Total Received
20.07453352 BTC
$1,711,670
Transactions
145
Total Sent
19.74510304 BTC
$1,683,581
Total Volume
39.81963656 BTC
$3,395,251
Transactions
ID: 88fb-ac1e
10/11/2024, 01:14:35
From bc1q-20sq
To 2 Outputs
0.00050000 BTC • $42.63
Fee 4.3K Sats • $3.68
ID: 12ea-f6b7
10/09/2024, 23:56:50
From bc1q-20sq
To 2 Outputs
0.00050000 BTC • $42.63
Fee 4.8K Sats • $4.13
ID: 9ff0-a291
5/27/2021, 21:14:31
From 3Gqq-NXFr
To 6 Outputs
0.00770000 BTC • $656.55
Fee 52.0K Sats • $44.36

SCAN ME

TECH

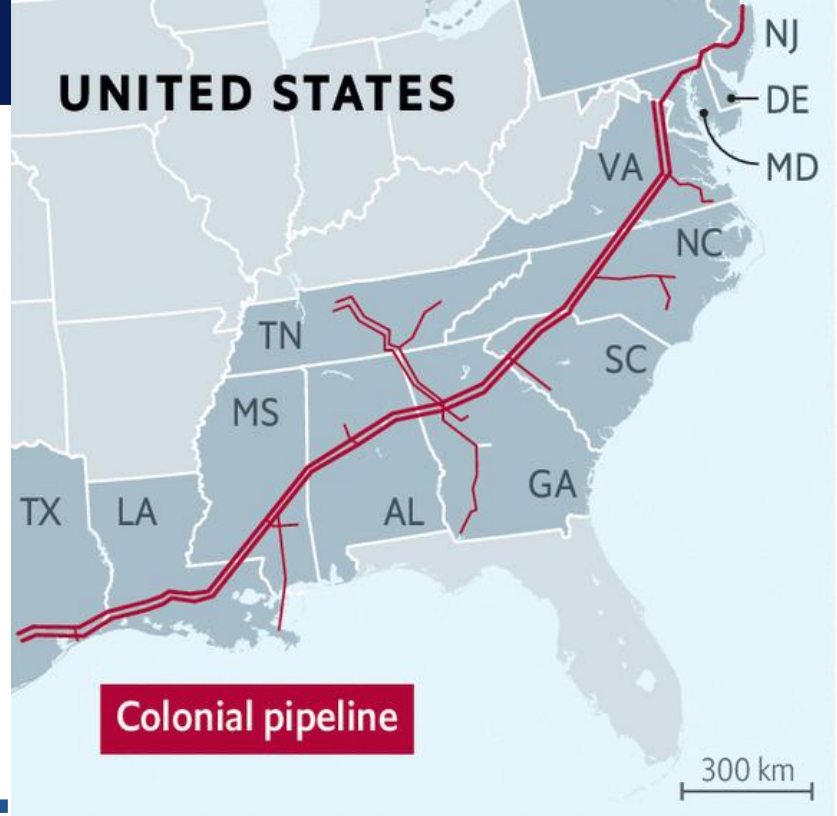
Hackers behind Colonial Pipeline attack reportedly received $90 million in bitcoin before shutting down

PUBLISHED TUE, MAY 18 2021•9:04 AM EDT | UPDATED TUE, MAY 18 2021•4:19 PM EDT

Ryan Browne
@RYAN_BROWNE_

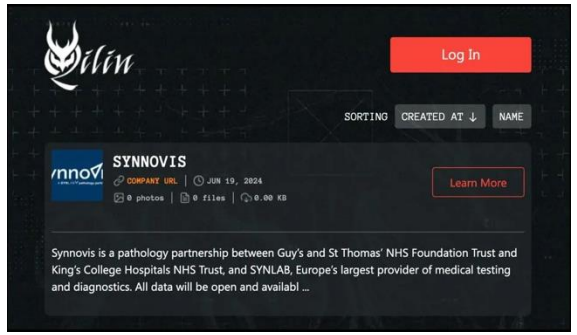
KEY POINTS

- DarkSide, the hacker group behind the Colonial ransomware attack, received $90 million in bitcoin ransom payments, according to blockchain sleuths Elliptic.
- The cybercriminal gang shut down last week after losing access to its servers and as its cryptocurrency wallets were emptied.
- Elliptic said DarkSide's bitcoin wallet contained $5.3 million worth of the digital currency before its funds were drained.



Ransomware Incidents in 2024 (Healthcare)

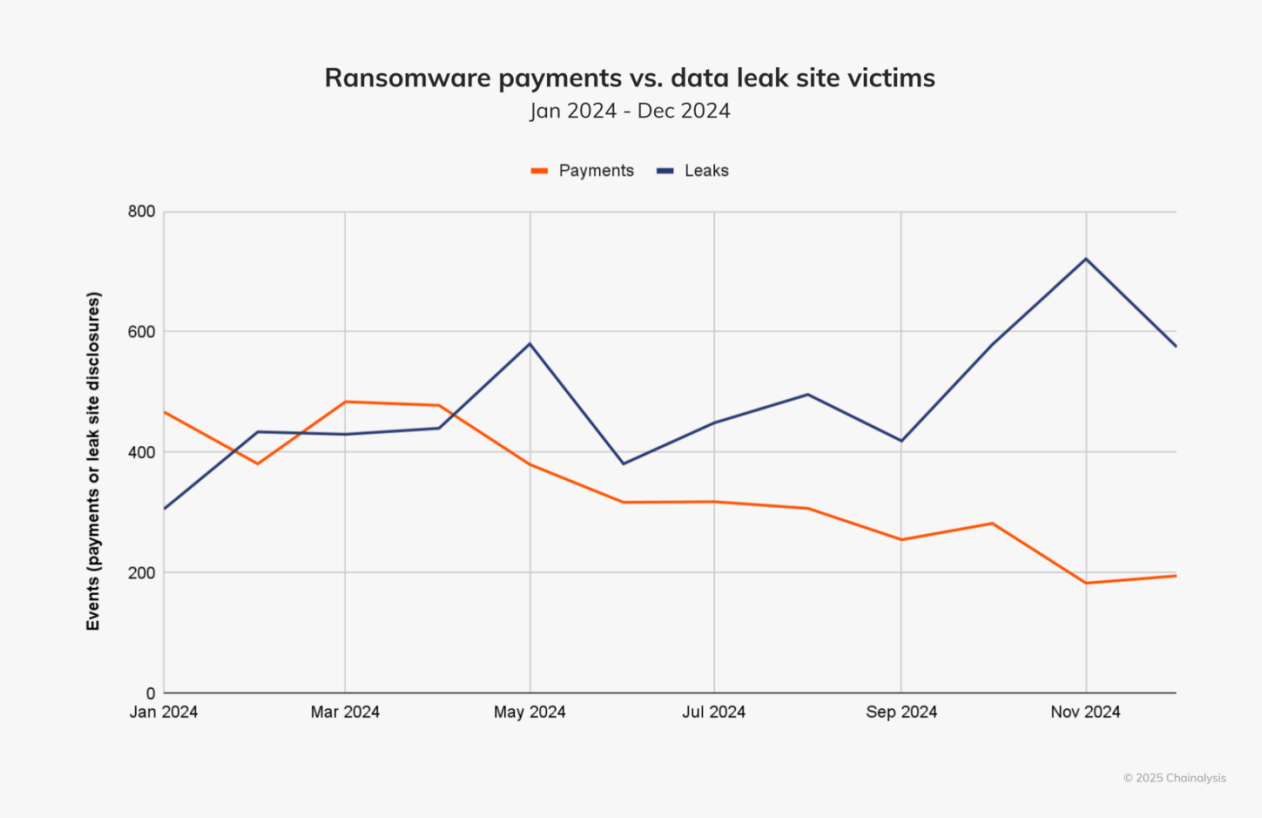
- UnitedHealth (US Health Insurance)
  - Disabled e-payments, stole 6TB of confidential data
  - Paid $22 million ransom
  - Affected over 100 million people
- Ascension (US Healthcare Network)
  - Disrupted EHR access, data breach (5.6 million patients)
  - Costed $1.3 billion and took over 1 month to recover
- Synnovis (UK Pathology Service Provider)
  - All IT systems were affected, encryption of critical data
  - Demanded $50 million ransom, but no payment
  - 800+ surgeries canceled, unable to match donor and patient blood types



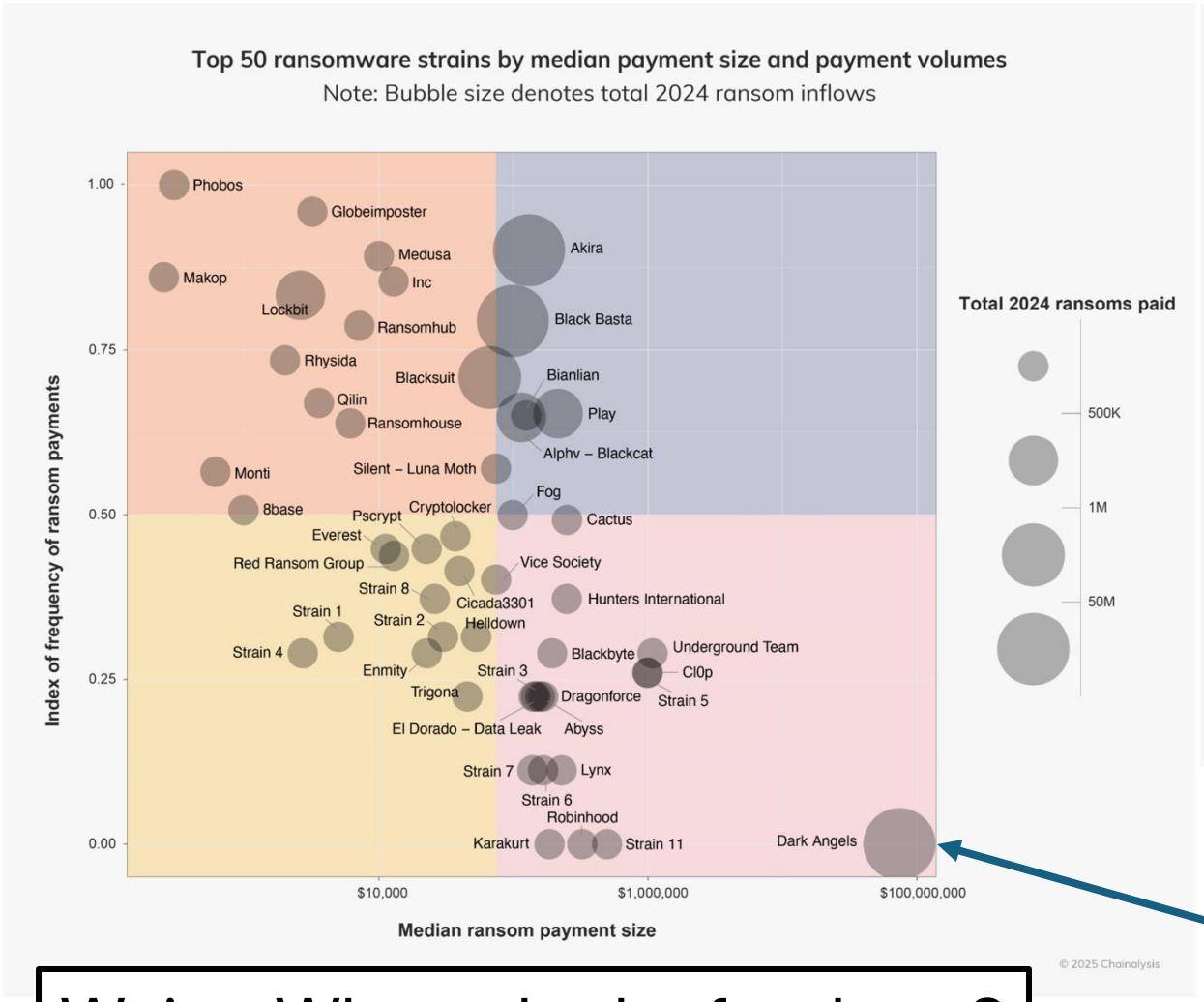
To Pay Or Not To Pay?

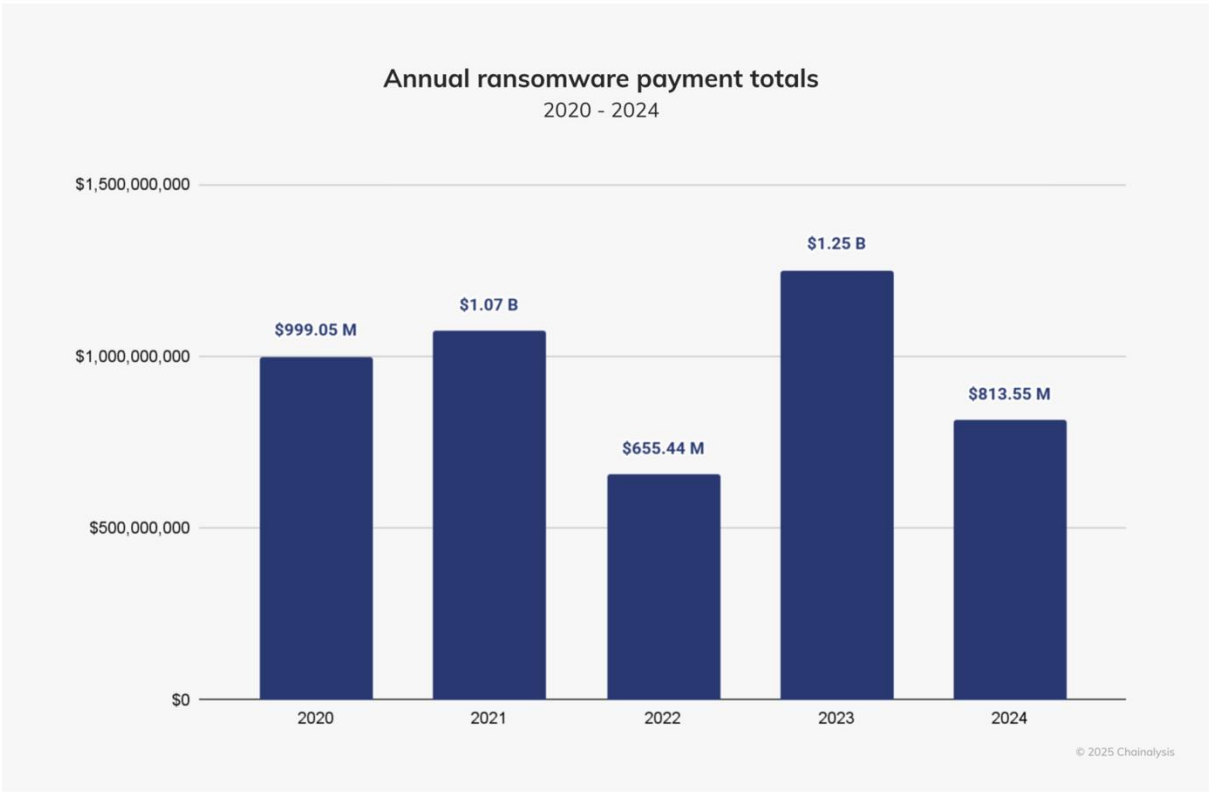
- More victims were targeted, but fewer paid.
- Poor reputation
  - Have been caught overstating or lying about victims
  - Repost claims by old victims
  - Same wallet for different victims(?)
- Better backup mechanisms
- Cannot pay ransom to sanctioned entities by laws and regulations

GARMIN® paid 10 million ransom in 2020, but some critical files were not recoverable.



This Is Still A Sizable Portion





Wait… Where do the funds go?

Crypto Laundering Methods

Crypto Exchange

To ramp-off funds

Coin Mixer

To obscure the movement of funds

Blockchain Bridge

To obscure the movement of funds

Organized crime shows

high level of **professionalization**,

low level of **crypto sophistication**.

Crypto Exchanges

- Platforms that facilitate the buying, selling, and trading of cryptocurrencies and other digital assets.
- Key Features
  - Custodial Services
  - Liquidity
  - Fiat Support
  - Regulation and Compliance

BINANCE

coinbase

Exchanges without KYC?

No-KYC exchanges have no known process for collecting customer information before allowing any level of deposit or withdrawal.

- Crypto-to-crypto
- Fiat-to-crypto

Infosecurity Magazine

Log In Sign Up

News Topics Features Webinars White Papers Podcasts Events & Conferences Directory

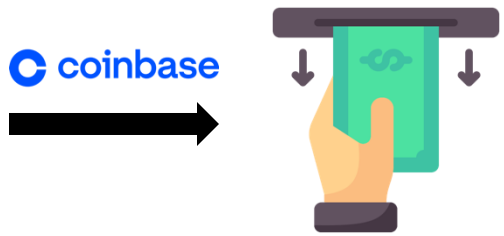
Infosecurity Magazine Home » News » German Police Shutter 47 Criminal Crypto Exchanges

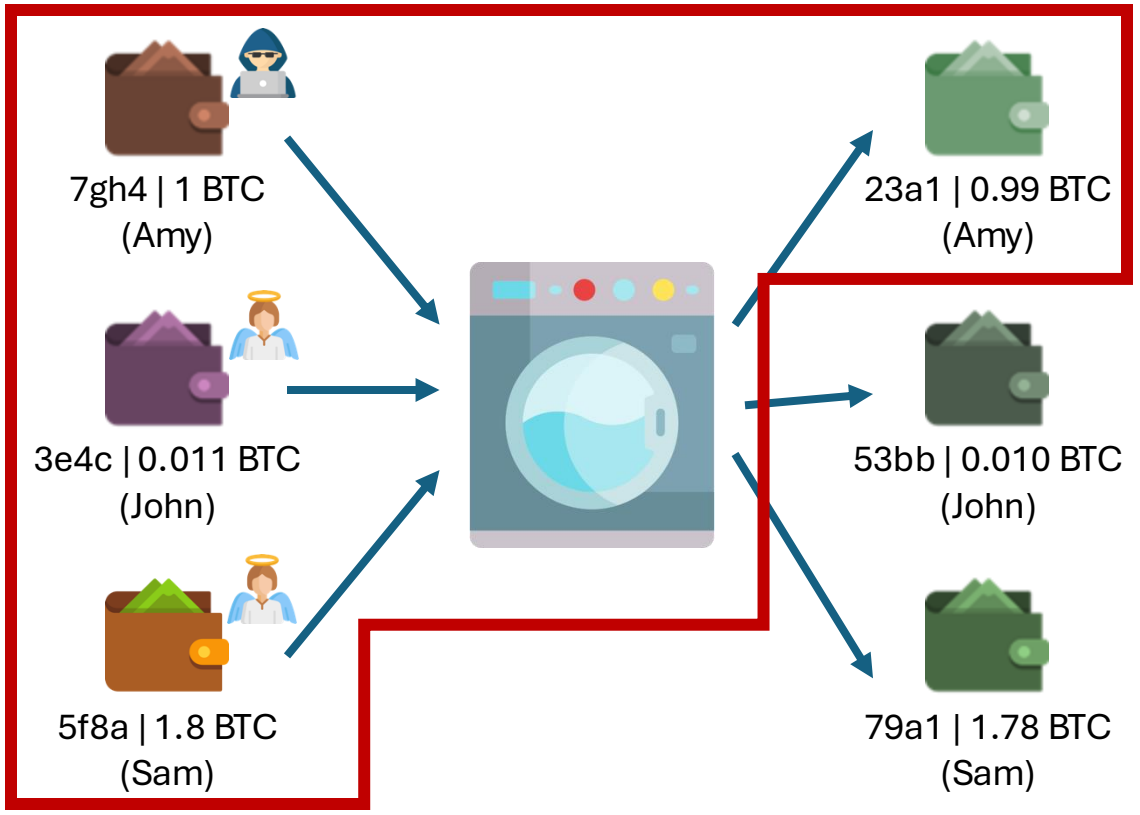
Coin Mixer

If a coin is traced back, there might be multiple possible originators, making it unclear which address is the actual true source.

Page (Block) 889176

Sender	Receiver	Amount	Commission
a2d2	211f	1 BTC	0.02 BTC
8754	f511	0.01 BTC	0.0000001 BTC
e7ee	bea4	15 BTC	0.005 BTC
bea4	f15f	3.20 BTC	0.01 BTC
fe1f	5f8a	1.5 BTC	0.1 BTC
ad13	85a3	3 BTC	1 BTC
be4a	3e4c	0.001 BTC	1 BTC
a2e4	7gh4	1 BTC	0.5 BTC
ab1e	1ae1	0.2 BTC	0.0001 BTC
... (2000 more entries) ...			





Blockchain Bridge

Coin mixers are limited to one blockchain, but blockchain bridges enable cross-chain laundering.

ETH

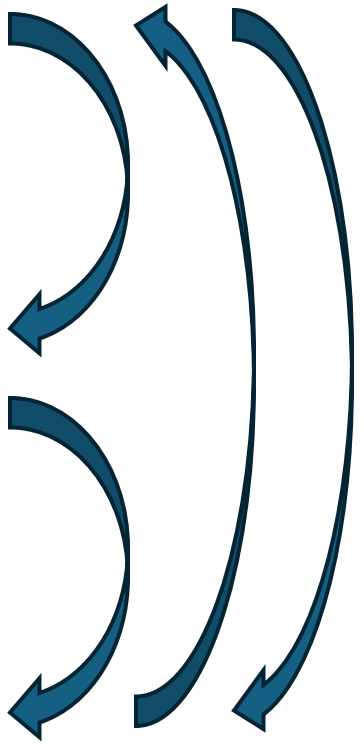
Allow people to build programs on the blockchain

ADA

Significantly reduce energy consumption

SOL

Achieve high-speed and low-cost transactions



Can be used with coin mixing to further obfuscate the illicit funds

Case Study: Lazarus Group

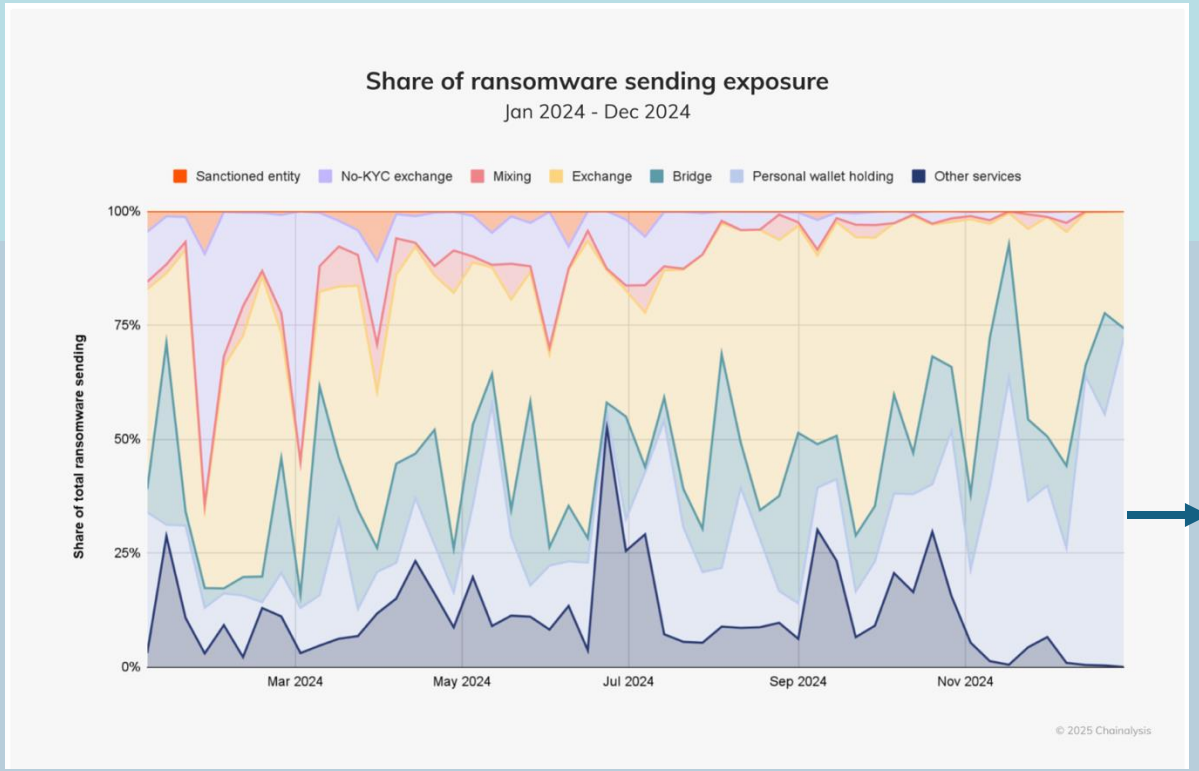
Stole $1.46 billion from Bybit (a Dubai-based crypto exchange)

1. Splitting and dispersing funds (401,000 ETH into 50 wallets)
2. Swapping tokens via exchanges
3. Cross-chain bridges to swap ETH into BTC
4. Mixers to obscure transactions
5. Launched the QinShuhuang token
6. Unregulated over-the-counter brokers to cash out

https://cointelegraph.com/explained/crypto-mixers-and-crosschain-bridges-how-hackers-launder-stolen-assets

Crypto Laundering Methods

Central Exchange



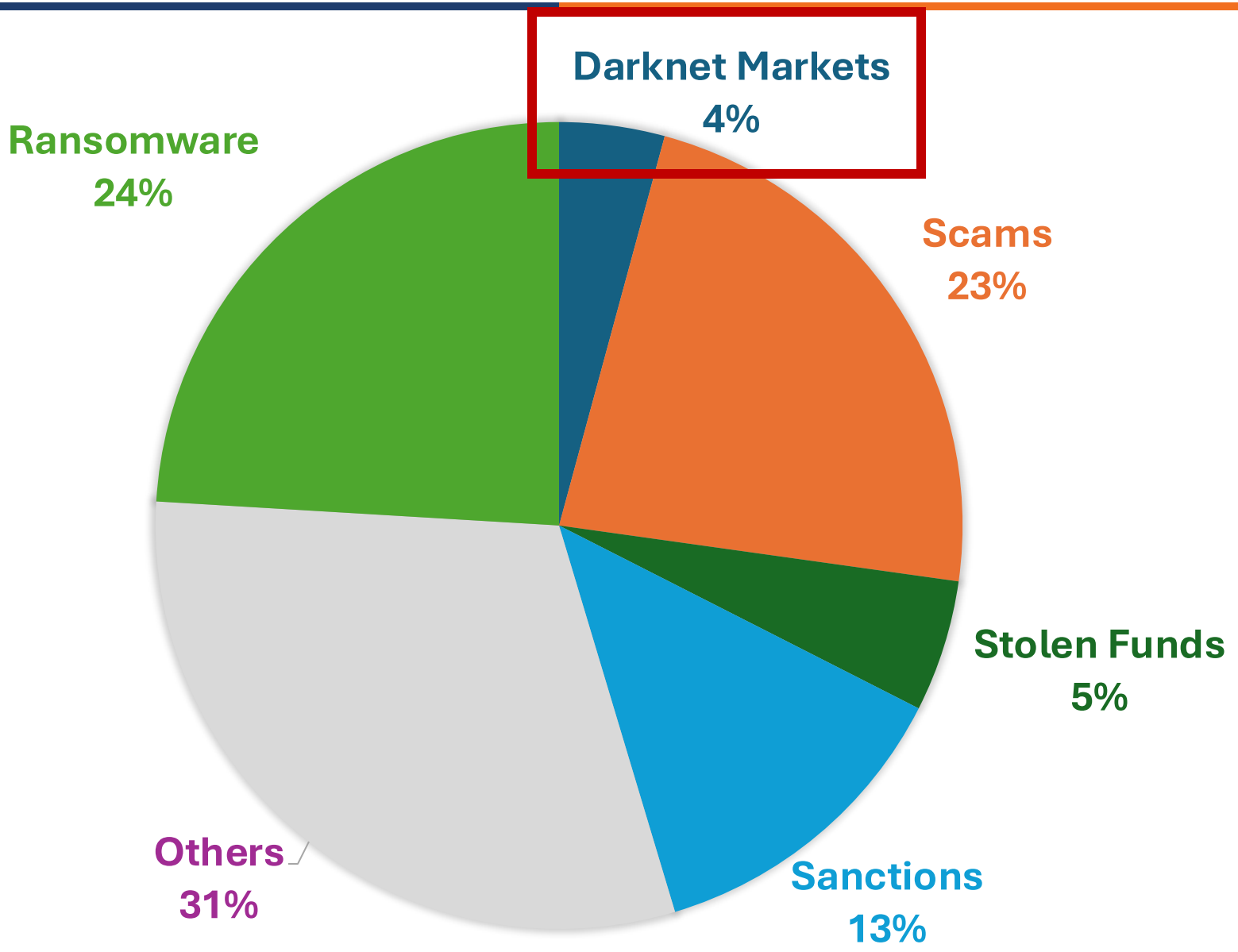
Coin Mixer

To obscure the movement of funds

Personal Wallet

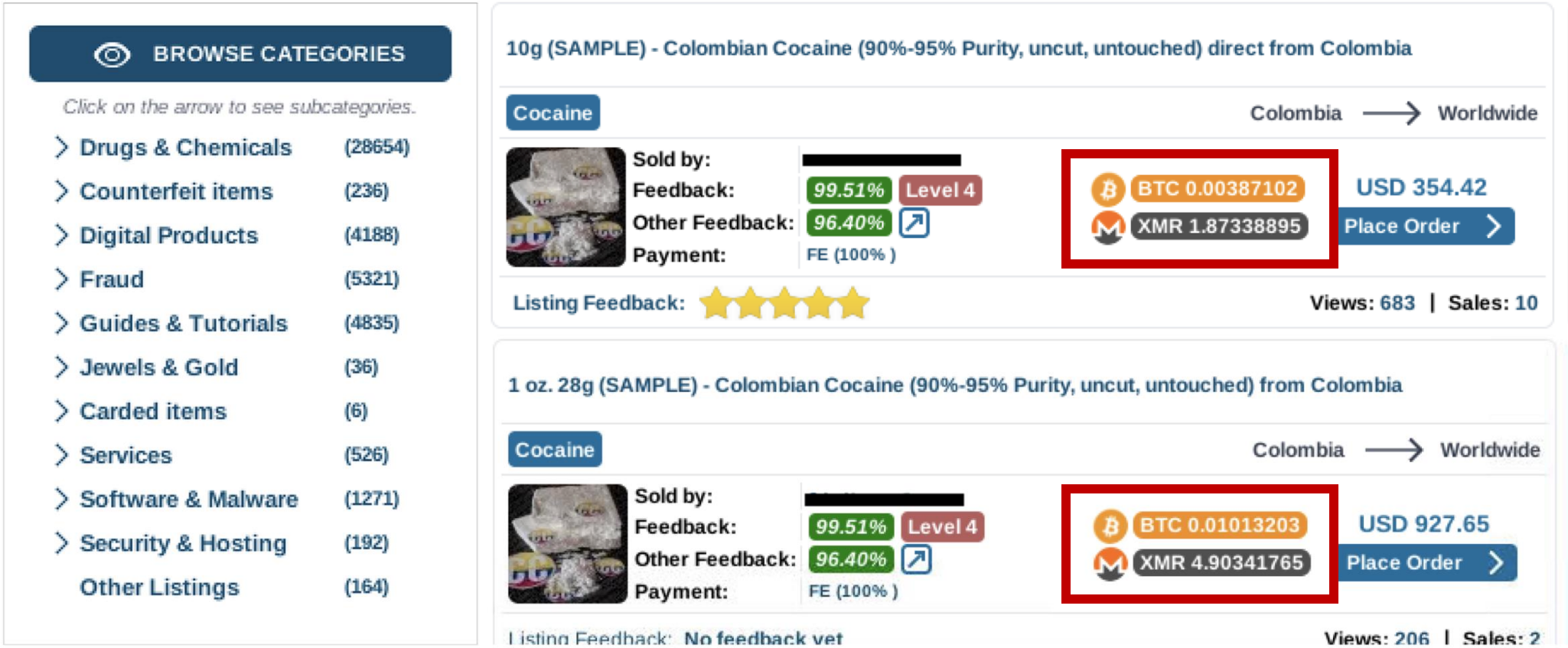
To hold funds

Crypto Value Received By Illicit Addresses in 2024

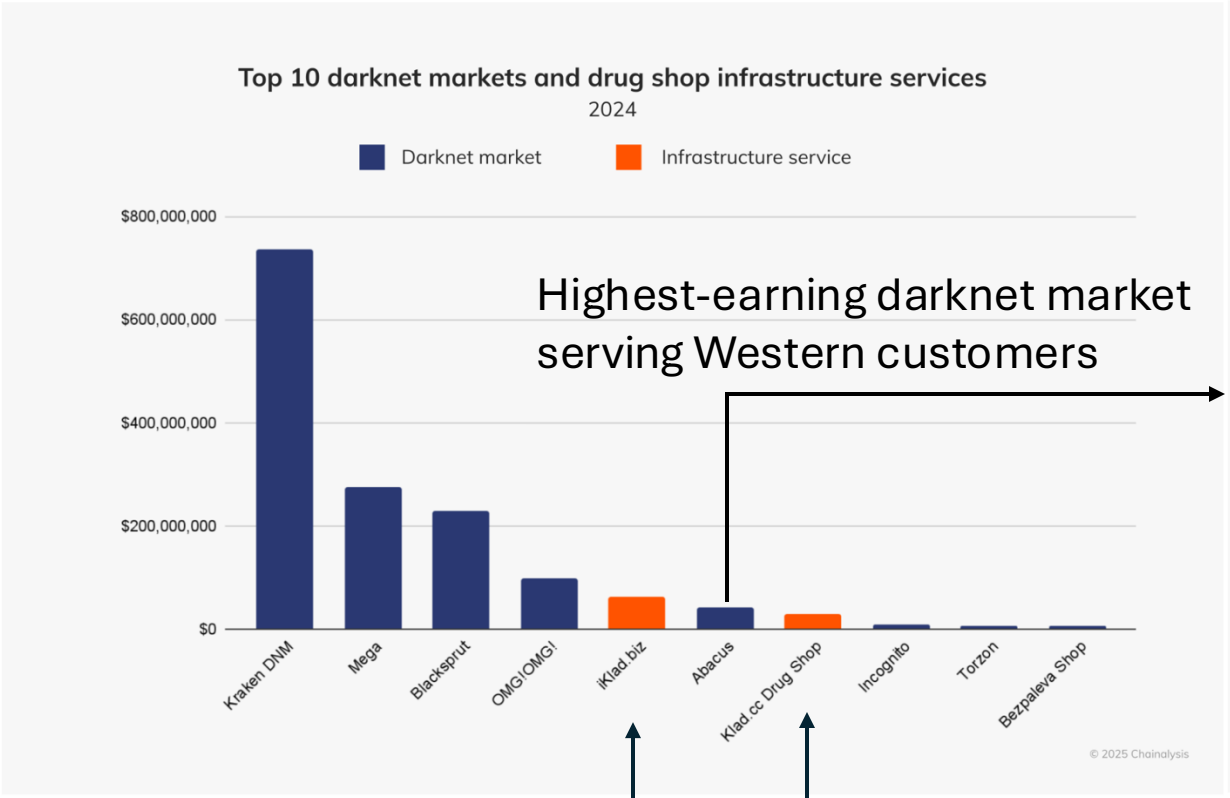


Darknet Markets

Hidden online platforms on the Dark Web where users can buy and sell illegal goods and services (drugs, weapons, and stolen data).

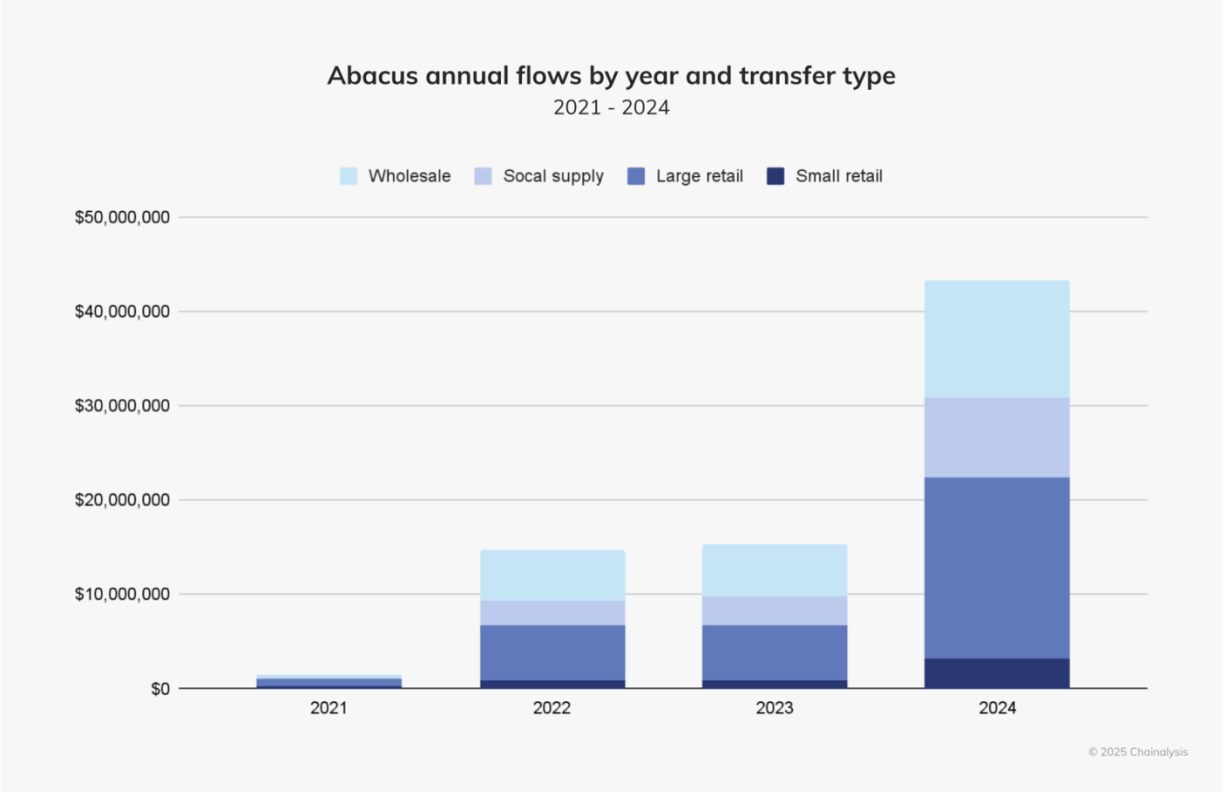


Top Markets



Highest-earning darknet market serving Western customers

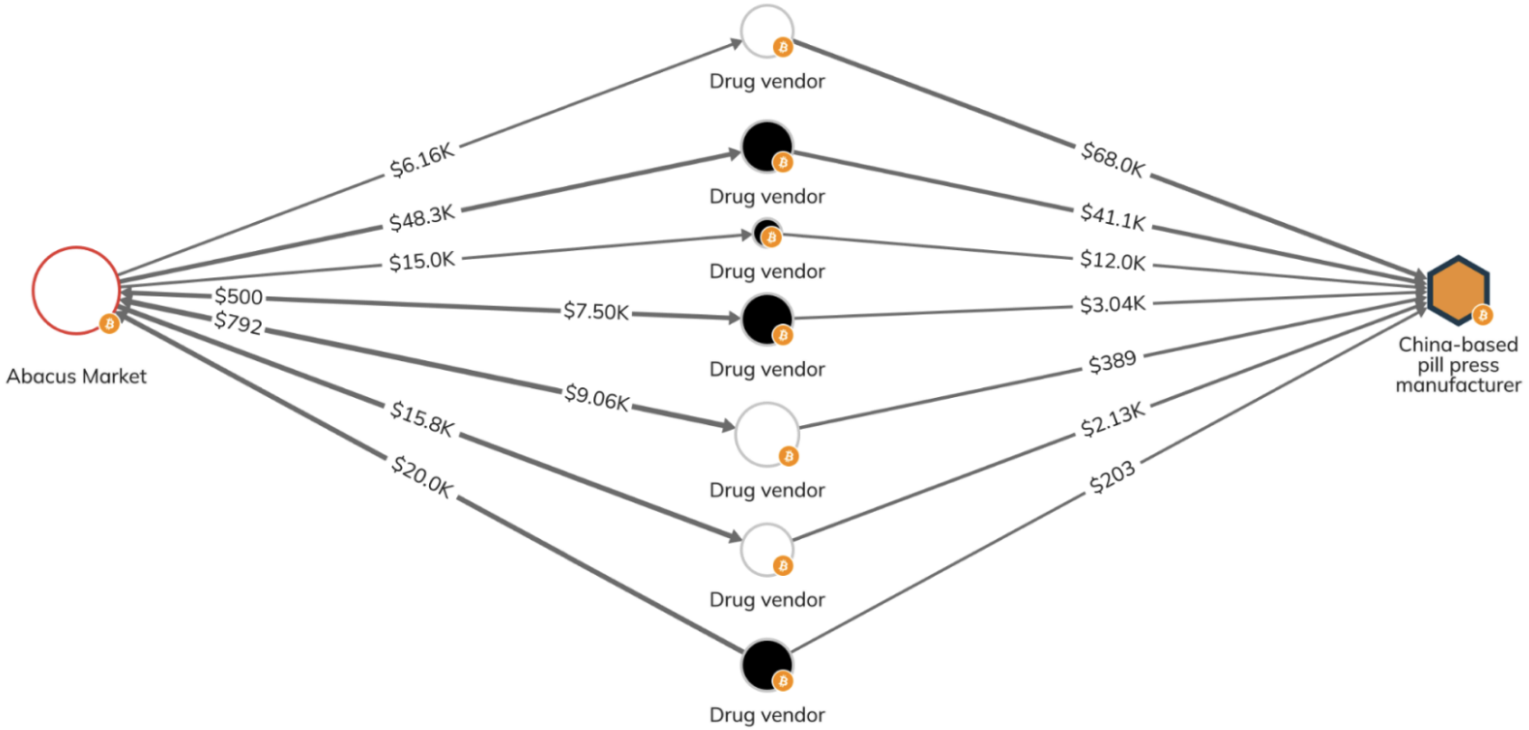
Infrastructure providers (e.g., web hosting, payment processors, etc.)



- **Potential Wholesale:** >$1000, drug sellers and distributors
- **Social Supply:** $500~$1000, sharing drugs in social settings
- **Large Retail:** $100~$500, personal consumption
- **Small Retail:** < $100, personal consumption

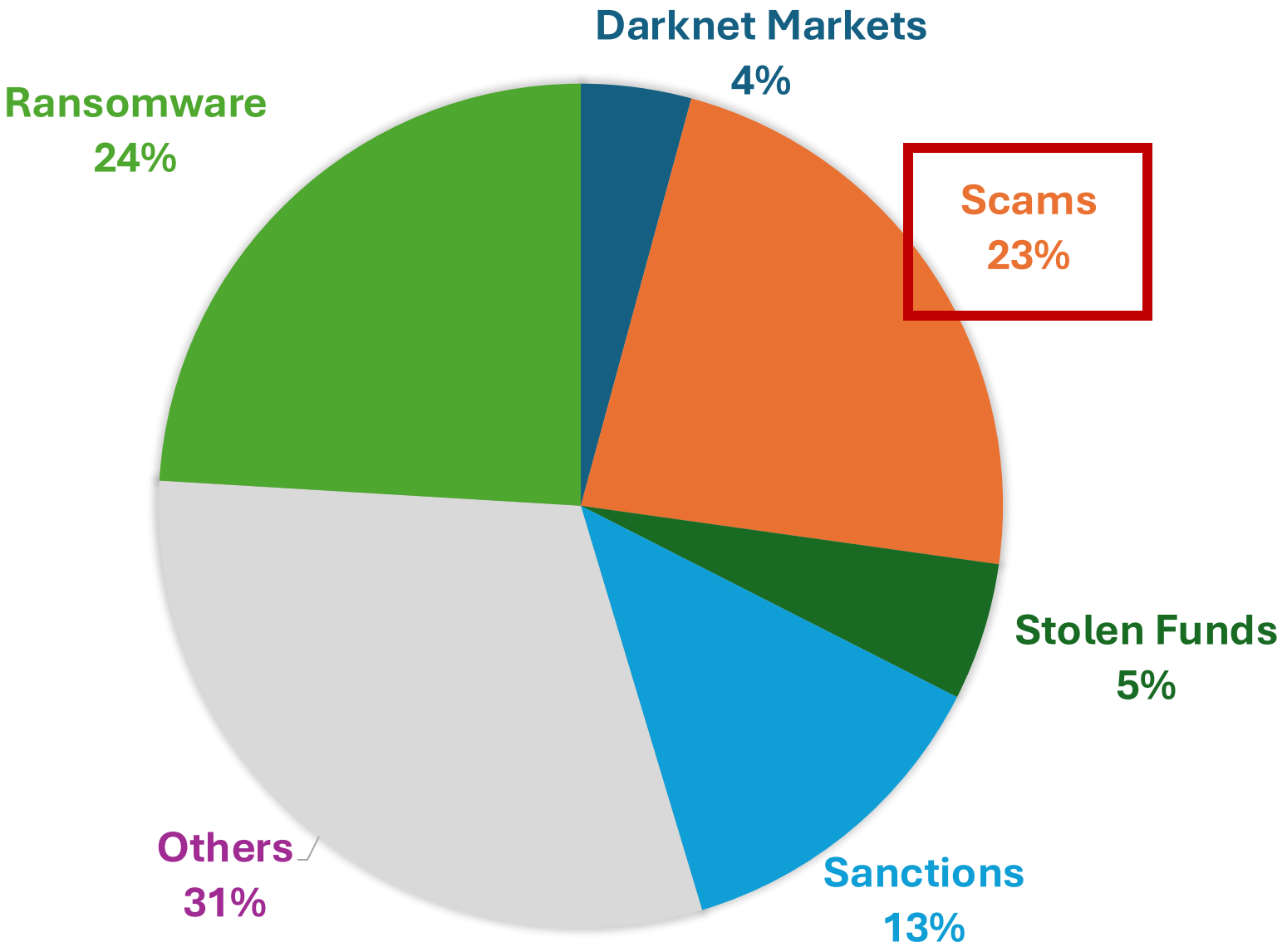
Case Study: Pill Press Manufacturer

A pill press manufacturer has on-chain ties to drug vendors on Abacus Market.



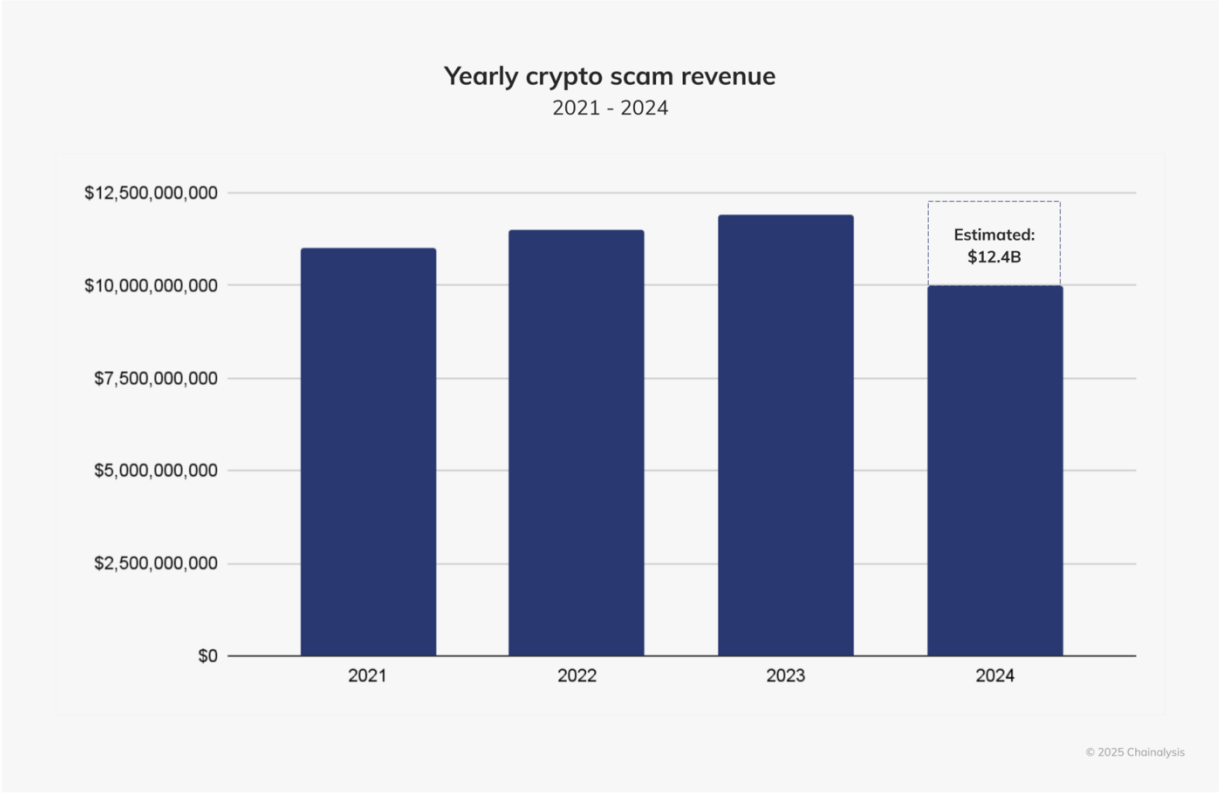
iPharmachine
(Not the one involved in this case study)

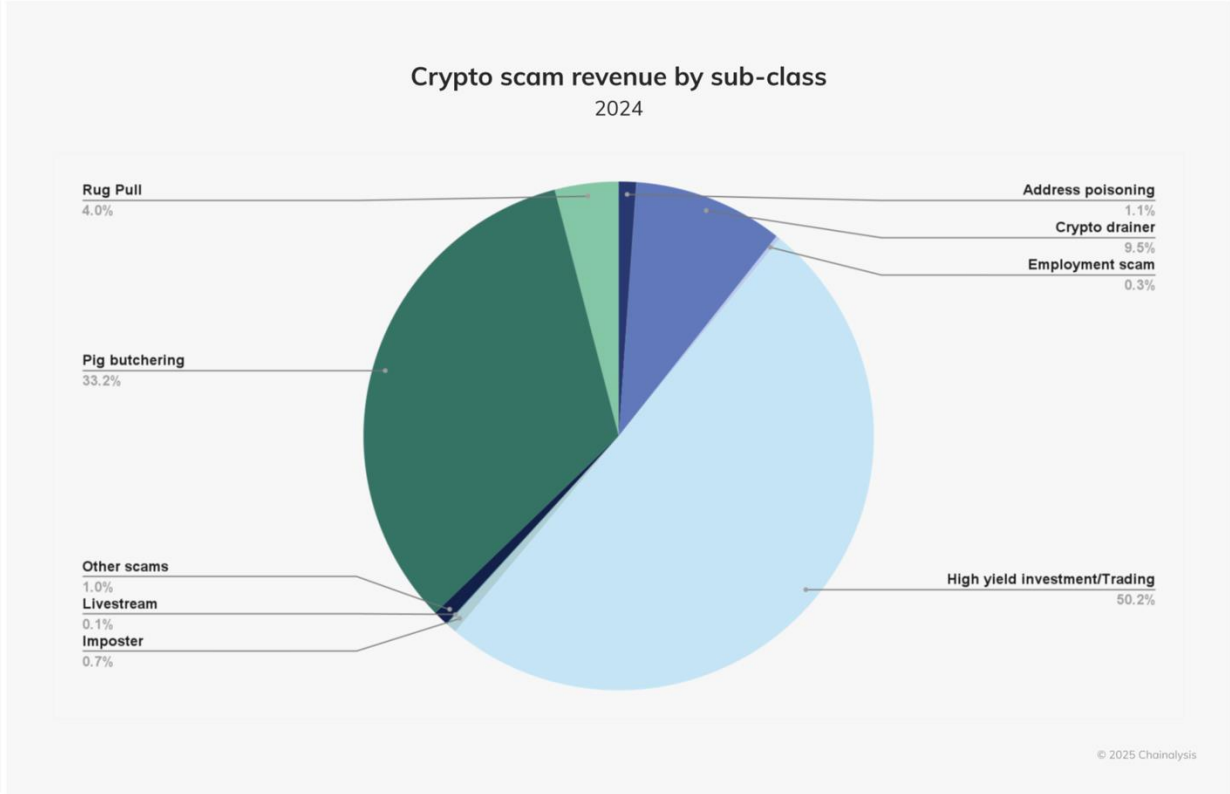
Crypto Value Received By Illicit Addresses in 2024



Scams

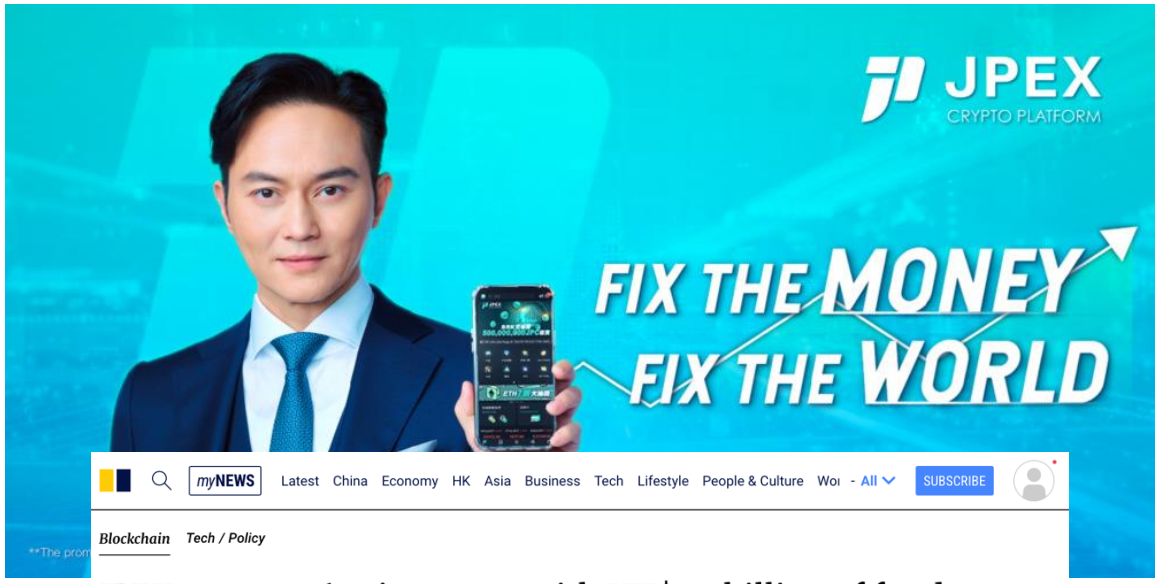
Crypto fraud and scams have continued to increase in revenue and sophistication.





High-yield Investment Scams

- Unrealistic Returns
- Lack of Transparency
- Ponzi Scheme Structure
- Pressure to Invest Quickly
- Use of “Trustworthy” Endorsement
- Withdrawal Difficulties
- Targeting Vulnerable Investors



myNEWS Latest China Economy HK Asia Business Tech Lifestyle People & Culture Wo - All SUBSCRIBE

Blockchain Tech / Policy

JPEX snares 1,641 investors with HK$1.2 billion of funds in Hong Kong’s largest fraud case in history

Police received complaints from 1,641 investors as of Monday evening, involving nearly HK$1.2 billion in assets

Eight people have been arrested in connection with the investigations into alleged fraud by JPEX

Pig Butchering Scams

- Long-Term Relationship Building
  - Use of social media and dating apps
- Fake Investment Opportunities
- Initial Small Gains
- Slaughter

CNN World Subscribe Sign in

World / Asia

Deepfake romance scam raked in $46 million from men across Asia, police say

By Jessie Yeung, CNN

3 minute read · Published 2:12 AM EDT, Tue October 15, 2024

All News DeFi Explore DLNews DLResearch

Regulation

- Hong Kong syndicate used deepfakes to defraud victims of millions of dollars.
- Global pig butchering scams siphoned $4.4 billion in 2023.

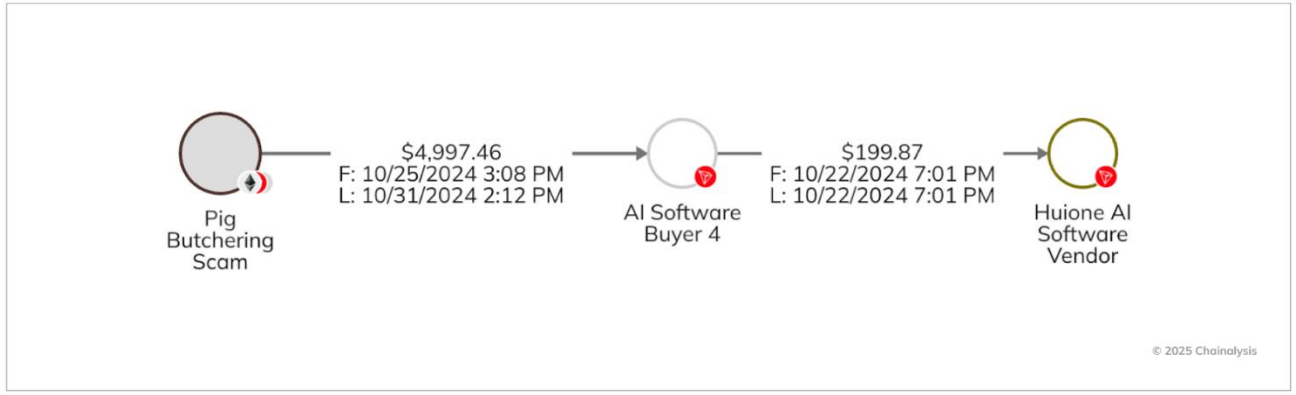
Hong Kong crime ring used deepfake personas and dating apps to steal millions

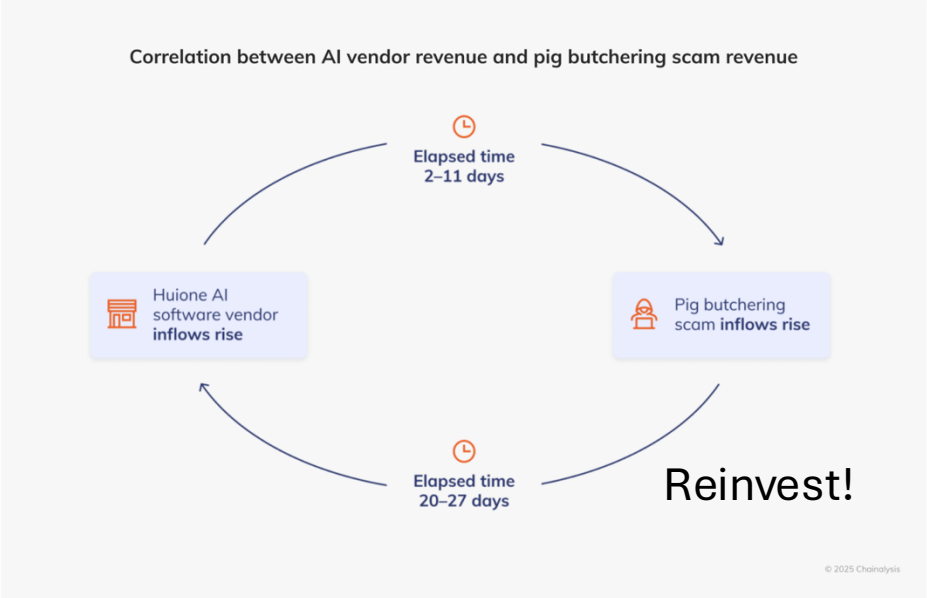
Hong Kong police raid uncovering luxury goods and cash is linked to an AI-powered scam syndicate. Credit: Shutterstock AI

Huione Guarantee: One-stop-shop for Scammers

Offer illicit services that support pig butchering scams and other frauds

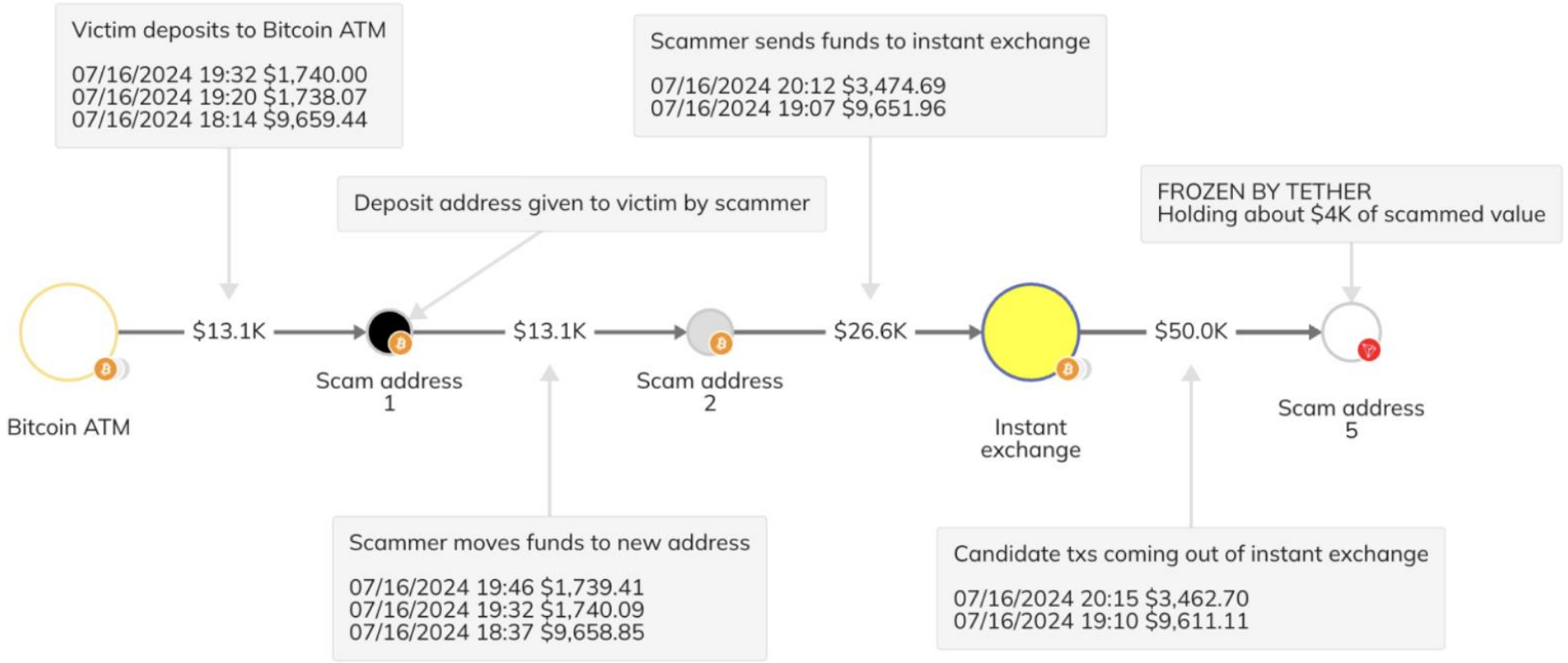
- Tools to initiate scam: workforce, targeted data lists, web hosting, social media account, content creation, AI software, etc.
- Money laundering services and cashing out
  - Processed more than $70 billion in crypto transactions since 2021
  - Mostly support pig butchering scams in Southeast Asia



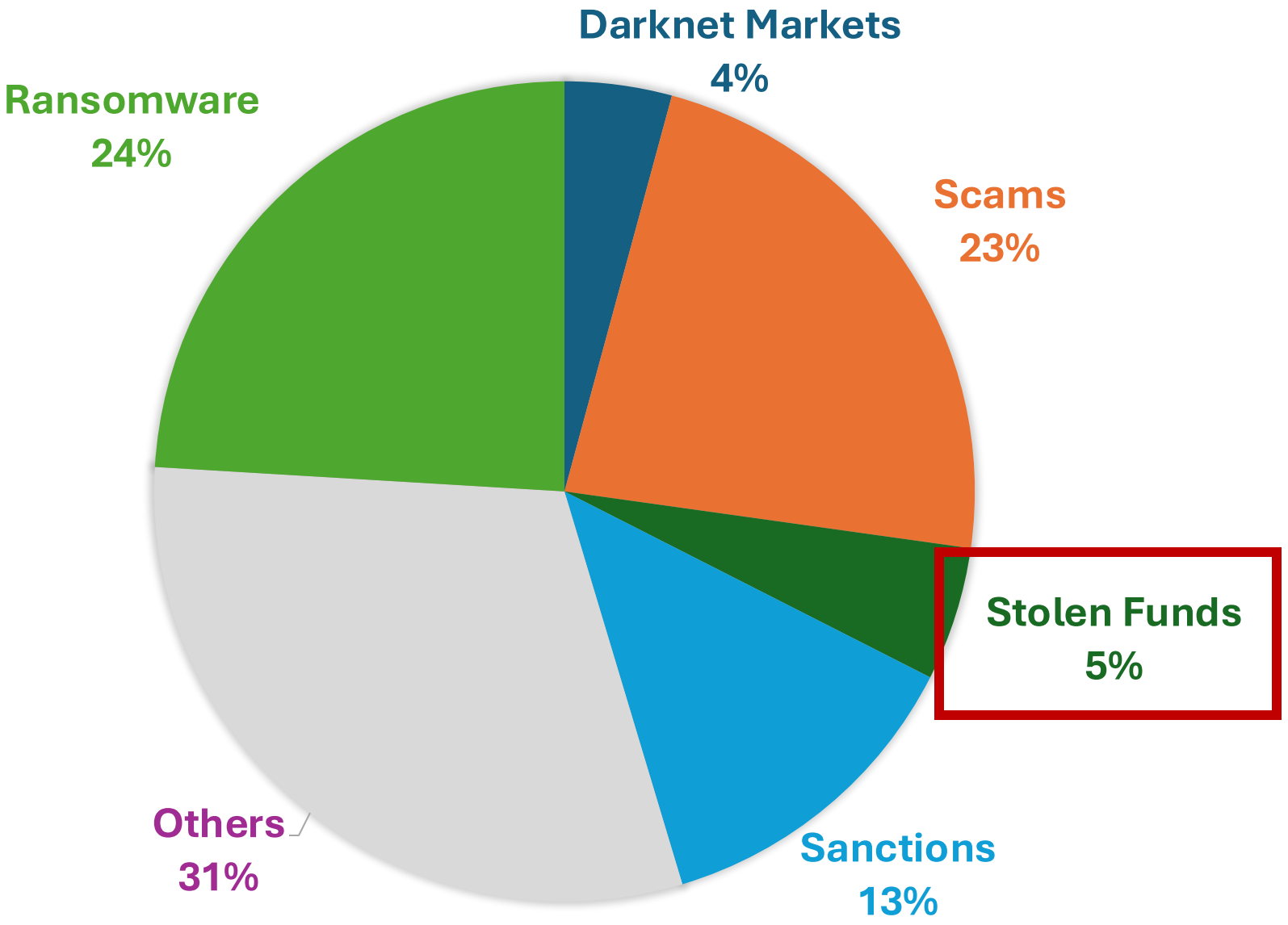


Case Study: Crypto ATM

- The victim had purchased a new laptop compromised by malware.
- The scammer impersonated as a Microsoft tech support and convinced the victim that $15,000 was required to resolve the issue.

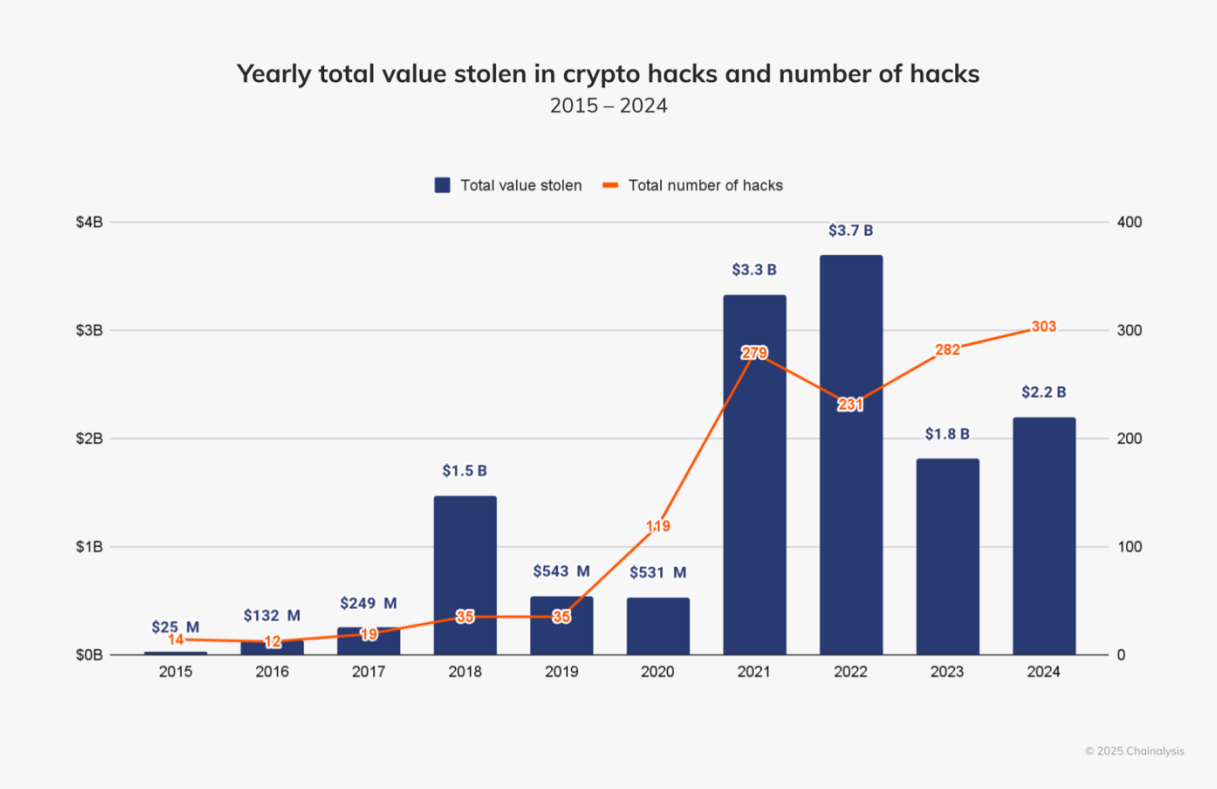


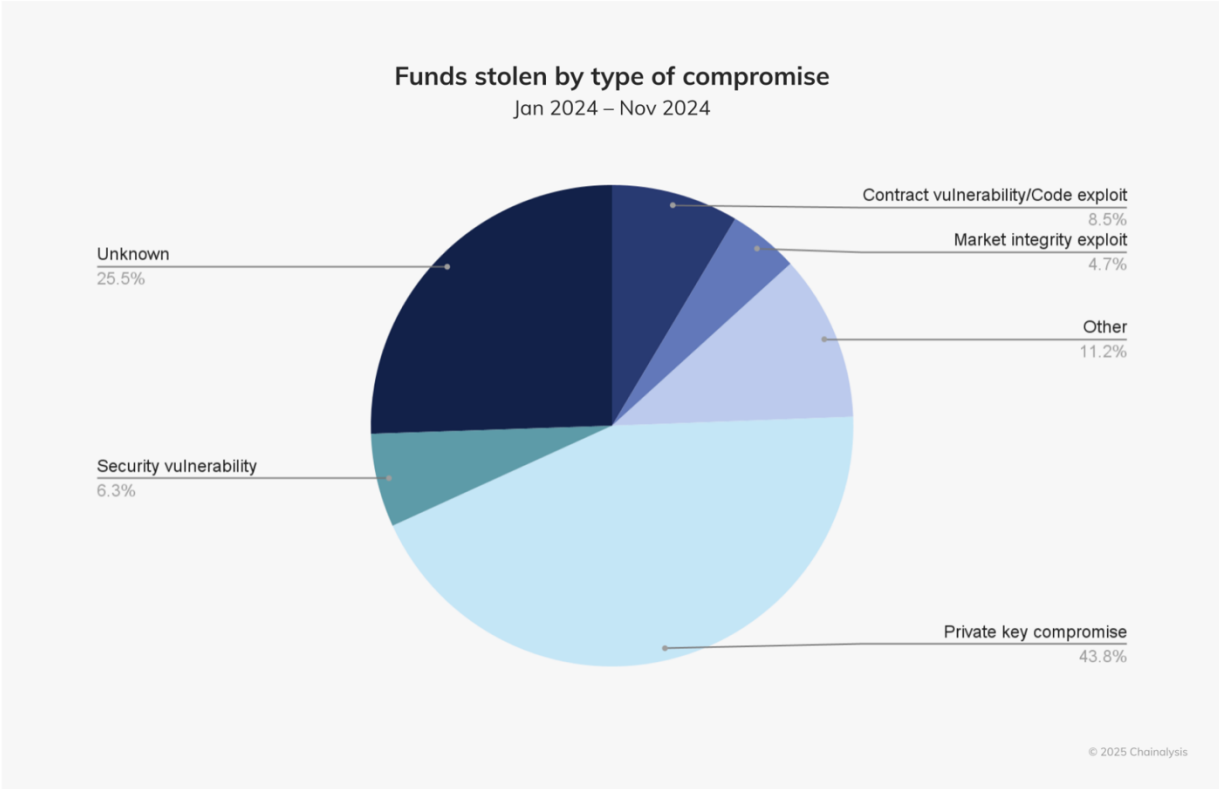
Crypto Value Received By Illicit Addresses in 2024



Stolen Funds

Exchanges are prime targets for attackers as they maintain large pools of customer funds in custodial wallets, rather than immediately transferring them to users' personal wallets.





North Korean Hackers Stole More Than Ever Before

- Employ advanced malware, social engineering, and crypto theft to
  - Fund state-sponsored operations and
  - Circumvent international sanctions
- IT workers infiltrated crypto and Web3 companies and compromised their networks, operations, and integrity.


DOJ Menu

Archives
U.S. Department of Justice

Our Offices | Find Help | Contact Us

Search

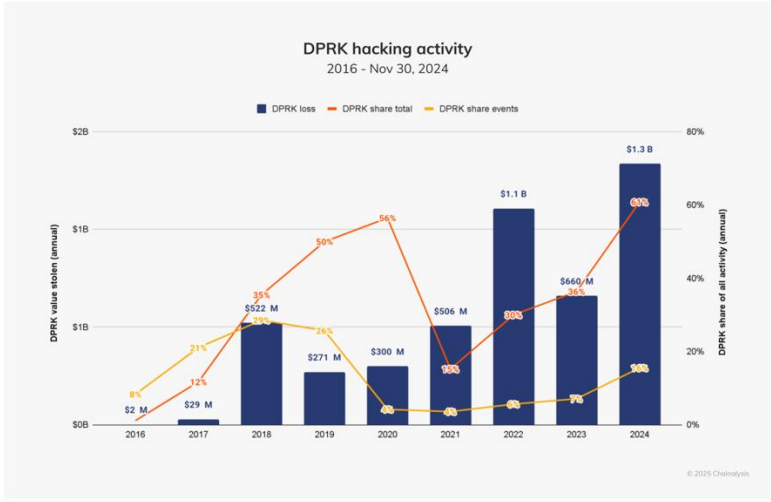
About | News | Documents | Internships | FOIA | Contact | Information for Journalists

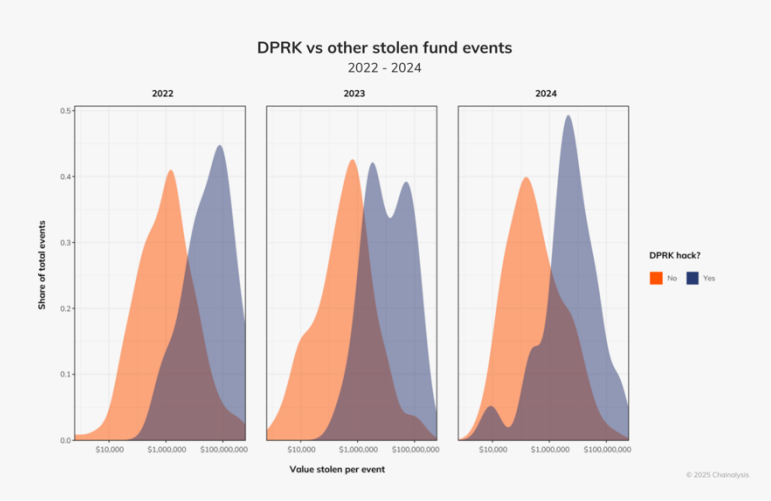
Justice.gov › Office of Public Affairs › News › Press Releases › Fourteen North Korean Nationals Indicted For Carrying Out Multi-Year Fraudulent Information Technology Worker Scheme and Related Extortions

PRESS RELEASE

Fourteen North Korean Nationals Indicted for Carrying Out Multi-Year Fraudulent Information Technology Worker Scheme and Related Extortions

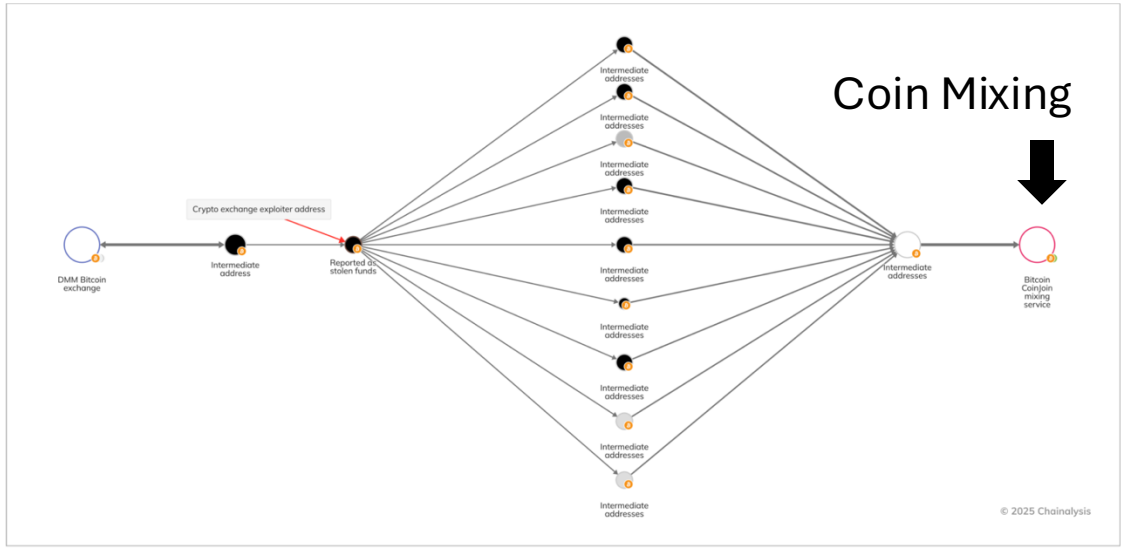
$88+ million throughout the six-year conspiracy

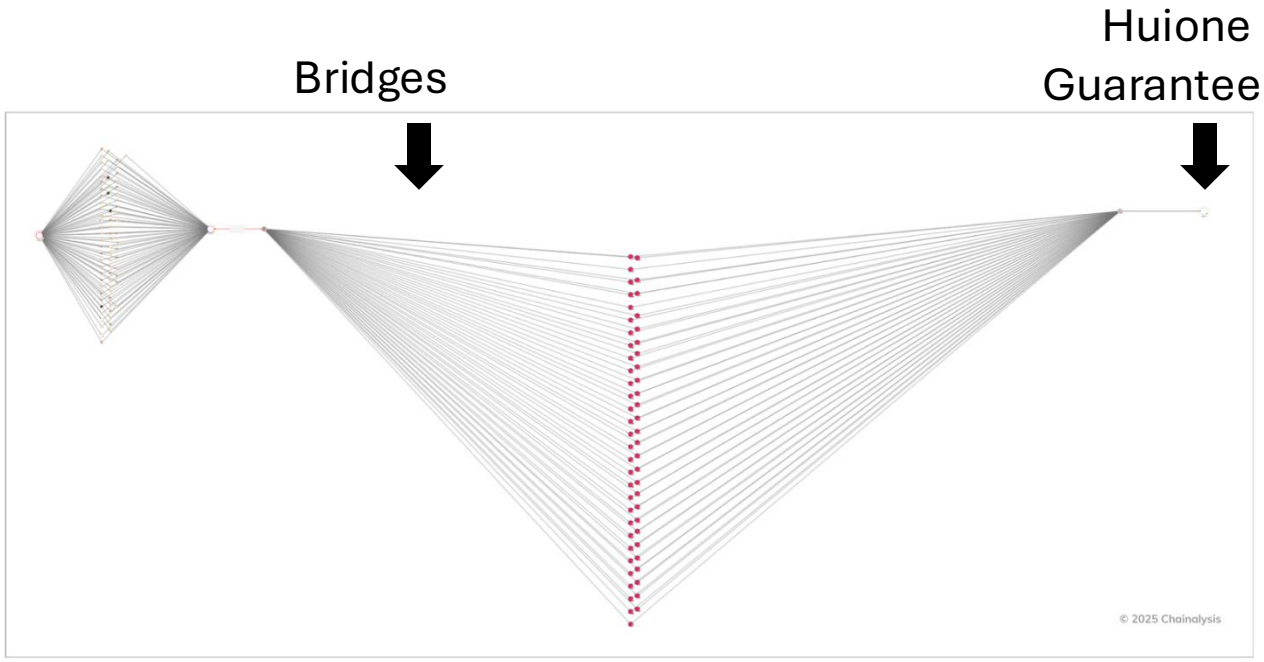




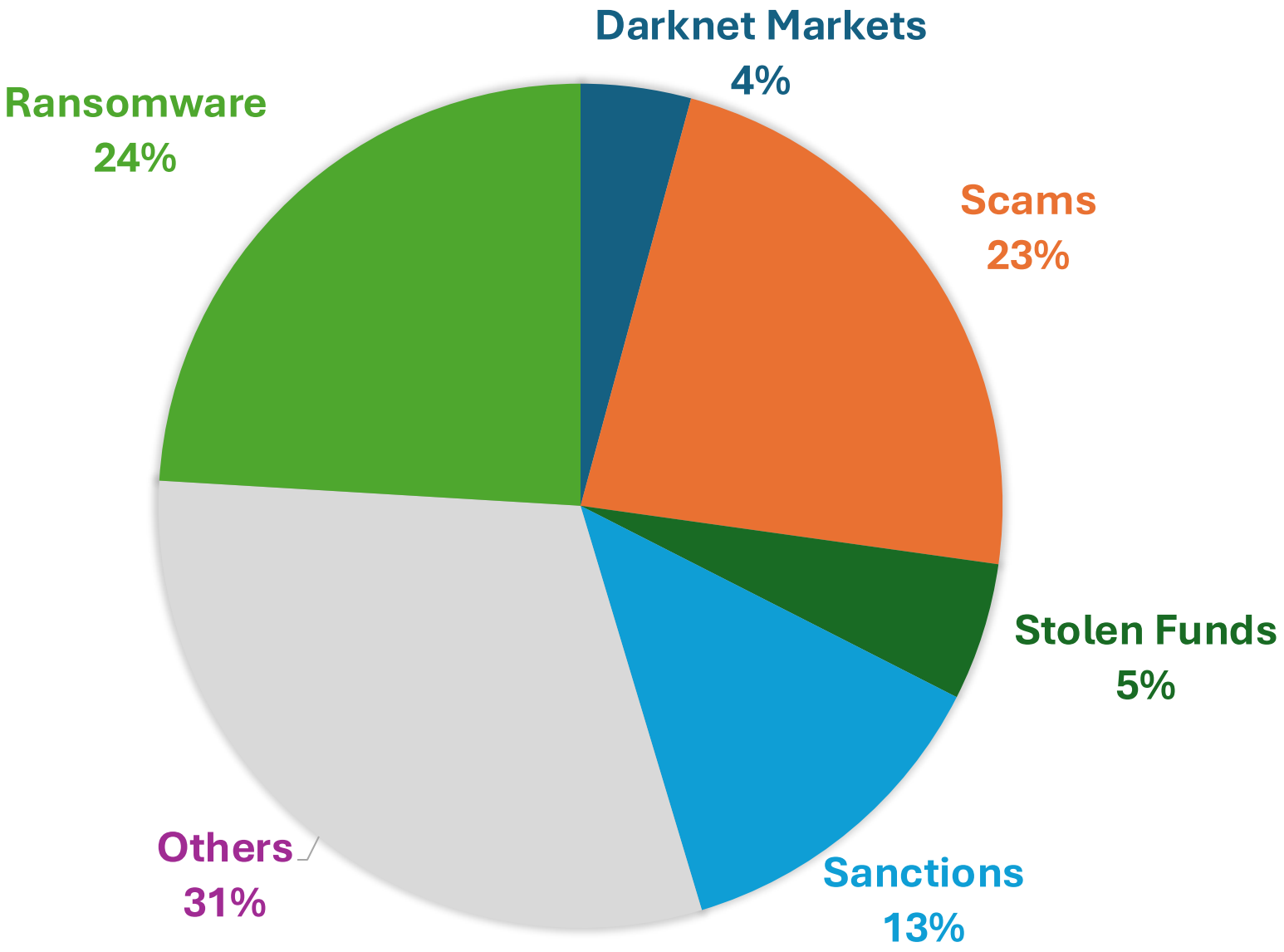
Case Study: DMM Bitcoin

- Japanese crypto exchange suffered a security breach → 4,502.9 Bitcoin
- In response, DMM fully recovered customer deposits by sourcing equivalent funds with the support of group companies.
- Decided to shut down the exchange in December 2024.





Crypto Value Received By Illicit Addresses in 2024



Blockchain

Crypto Crimes

Countermeasures

The **Good** News

You can read every transaction in the blockchain.

Bitcoin Block 866,482

Mined on October 20, 2024 04:17:38 • All Blocks

0	ID: 9b2f-fae8 10/20/2024, 16:17:38	From Block Reward To 3 Outputs	3.21991485 BTC • $220,184 Fee 0 Sats • $0.00
TX	1 ID: caa7-9af8 10/20/2024, 15:19:23	From bc1q-3rfl To 15sq-3vnq	0.00834428 BTC • $570.60 Fee 678 Sats • $0.46
TX	2 ID: b52e-e816 10/20/2024, 15:56:46	From bc1p-m3ya To bc1q-ws3w	0.00000294 BTC • $0.20 Fee 2.6K Sats • $1.78
TX	3 ID: 7613-eed7 10/20/2024, 16:08:32	From bc1q-v5gx To 3 Outputs	0.47799165 BTC • $32,686.13 Fee 1.7K Sats • $1.13
	4 ID: 9229-fbb1	From bc1q-v5gx	0.35750812 BTC • $24,447.20

The **Bad** News

460,000,000 created accounts

1,100,000,000 total transactions

700,000 new transactions per day

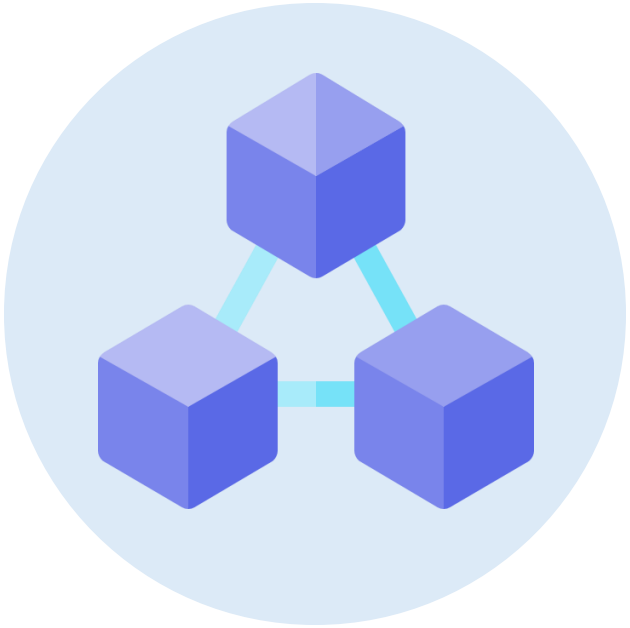
Can artificial intelligence help identify suspicious accounts?

Technological Countermeasures

- Blockchain Analytics and Forensics
  - **Colonial Pipeline Case:** FBI identified a wallet hosted on a US-regulated exchange via tracing technologies and used legal measures to seize $2.3 million of the ransom
  - **Bitfinex Case:** Tracked small movements of stolen funds over the years and led to the arrest of a couple
  - **Lazarus Group Case:** Sanctioned Tornado Cash (a mixer) after being found to help launder stolen funds
- AI and Machine Learning for Fraud Detection
  - **Binance Case:** Used AI-based engine to prevent $2.4 billion in potential user losses

Law Enforcement, Regulators, and Private Sectors

- International Law Enforcement Collaboration
  - **LockBit Case:** A ransomware disrupted by the UK NCA and US FBI had a payment drop by 79%
  - **Chipmixer, Tornado Cash, and Sinbad Case:** Sanctions leading to a substantial decline in using mixers for money laundering
- Enforcing KYC & AML Regulations
  - **Binance Case:** Fined $4.3 billion for failing to implement strong AML controls, leading to CEO's resignation



Bitcoin & Blockchain

Crypto Crimes

Countermeasures

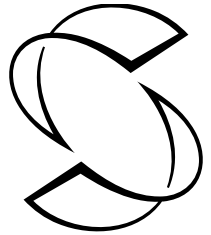
Thank You!

Ka-Ho Chow

Assistant Professor

Cyber Security, FinTech and Blockchain Group

https://khchow.com | kachow@cs.hku.hk



SCHOOL OF
COMPUTING &
DATA SCIENCE
The University of Hong Kong

This slide deck has been designed using icons from https://flaticon.com