CRYPTO CRIMES

2017-2022

OPEN SOURCE CASE REFERENCES

PRAVIN MANDLOI [DATA SCIENTIST]

Superintendent of Police, Central Bureau of Investigation, New Delhi

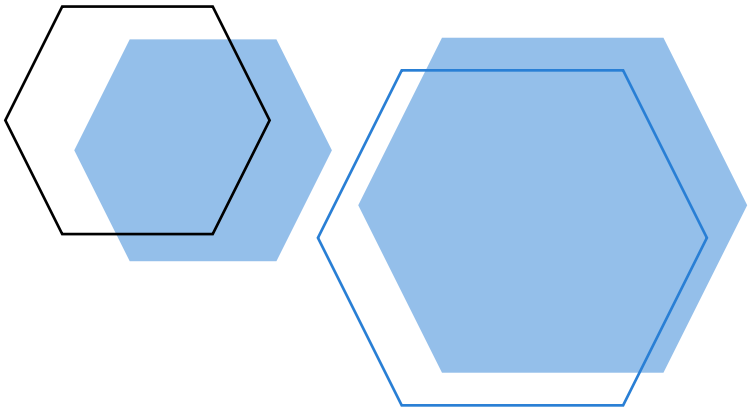
CASE REFERENCES

2017

In late 2017, the operator of the BitConnect Ponzi scheme was arrested in India for defrauding investors out of millions of dollars.

2018

In 2018, the US Department of Justice charged a Russian national with running a large-scale money laundering operation using bitcoin.

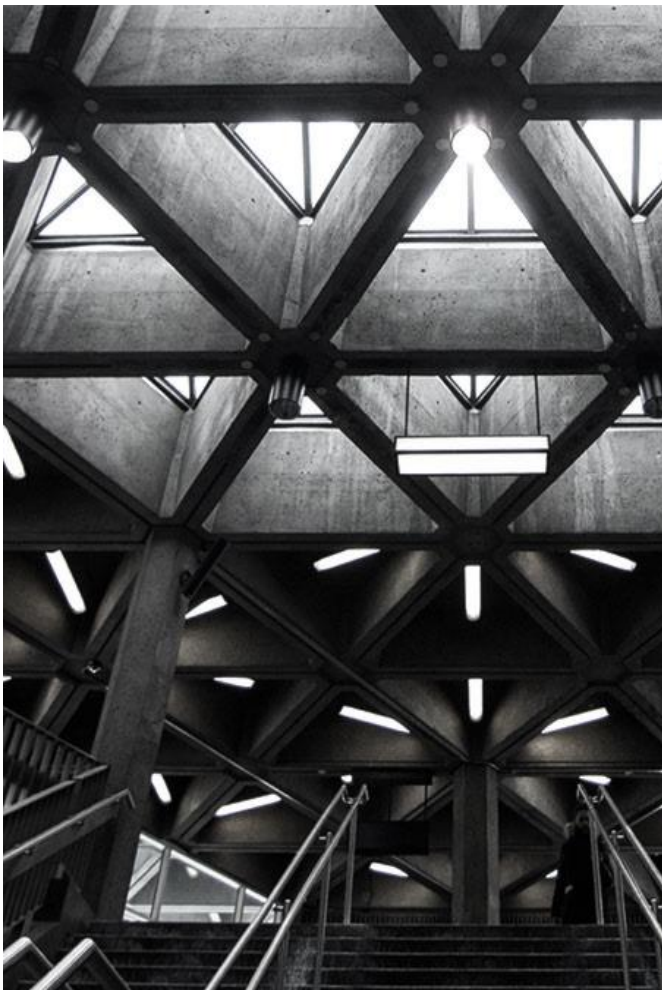


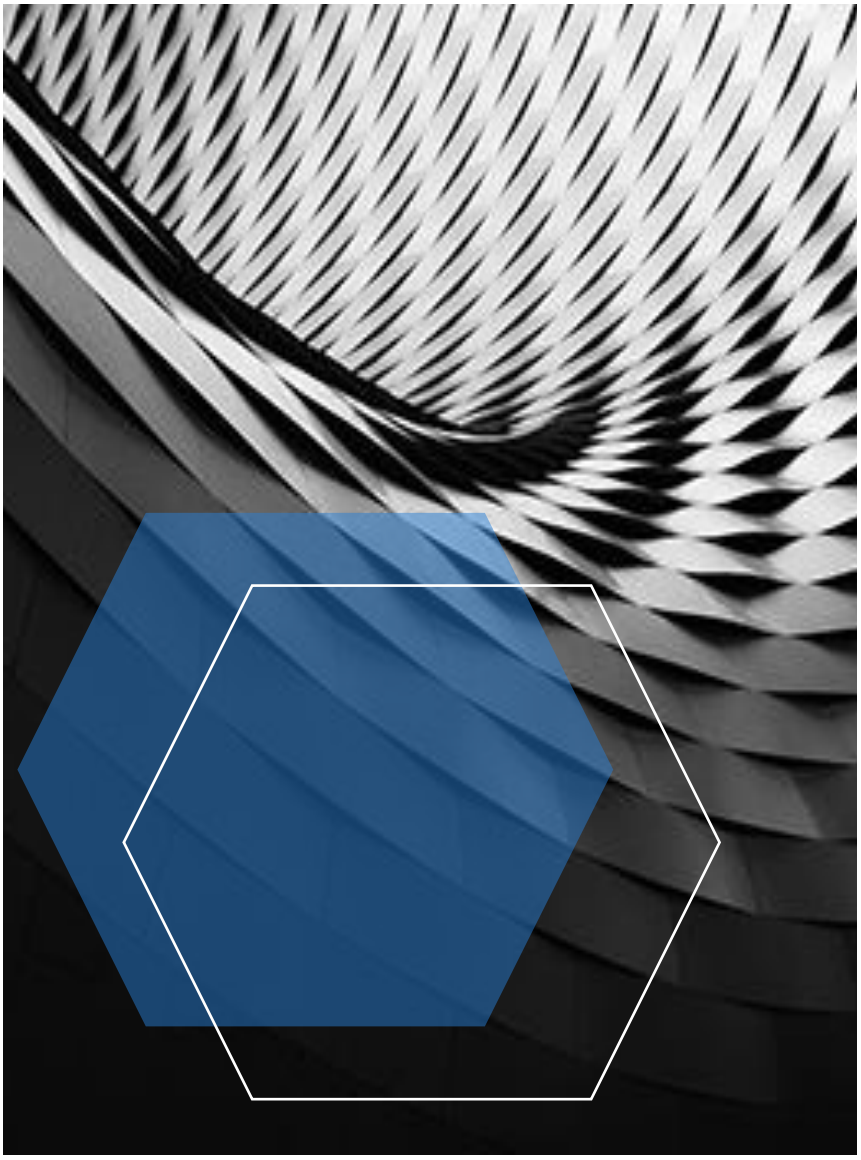
In 2018, a group of hackers stole $534 million worth of cryptocurrency from the Japanese exchange Coincheck.

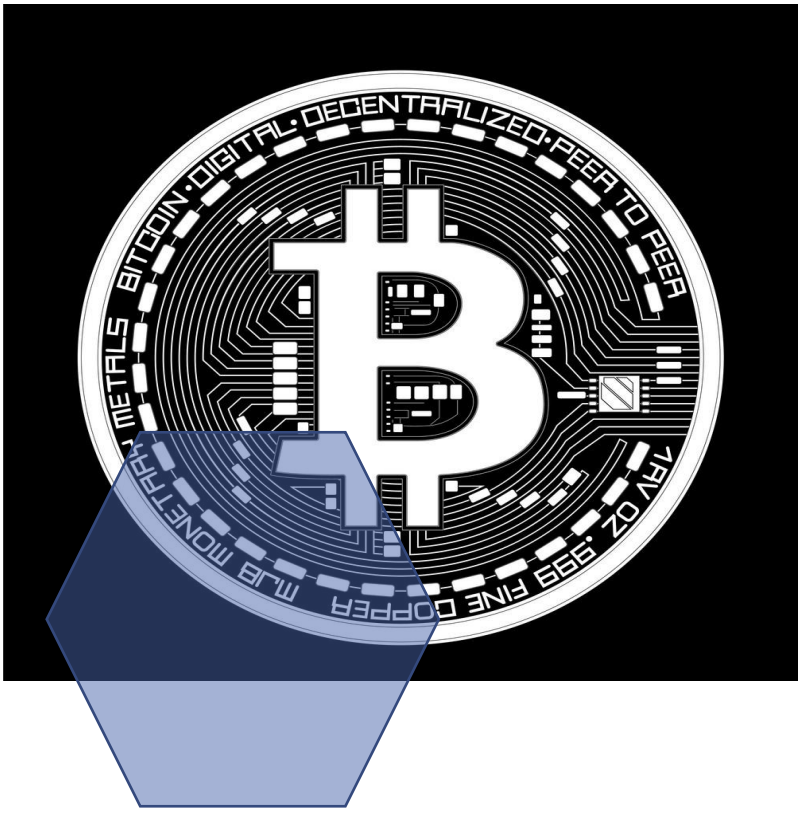
2019

In 2019, a hacker stole $40 million worth of bitcoin from the cryptocurrency exchange Binance. The hacker was later arrested and sentenced to prison.

IN 2019, the us department of justice charged the operator of the btc-e cryptocurrency exchange with money laundering and operating an unlicensed money transmitting business.







2020

In 2020, the founder of the cryptocurrency exchange QuadrigaCX was accused of embezzling millions of dollars from customer accounts. The case is still ongoing.

In 2020, the US Internal Revenue Service (IRS) announced that it had arrested a man for operating a cryptocurrency mixering service that was used to launder millions of dollars on behalf of criminals.

2021

In 2021, the US government seized $2.3 billion worth of bitcoin from the ransomware group known as "DarkSide." The group had been using bitcoin to collect ransom payments from victims of their cyber attacks.

In 2021, the US Securities and Exchange Commission (SEC) charged a man with running a $30 million cryptocurrency investment scam.

In 2021, the US Department of Justice indicted a man for operating a cryptocurrency-based Ponzi scheme that defrauded investors out of millions of dollars.

In 2021, the US Department of Justice charged a group of hackers with stealing over $2.3 million in

cryptocurrency from various individuals and exchanges.

In 2021, the US Federal Bureau of Investigation (FBI) arrested a man for operating a cryptocurrency Ponzi scheme that defrauded investors out of millions of dollars.

In 2021, the US Commodity Futures Trading Commission (CFTC) filed a civil enforcement action against a man and his company for operating a cryptocurrency Ponzi scheme that defrauded investors out of over $7 million.

In 2021, the US Securities and Exchange Commission (SEC) charged a man with running a cryptocurrency investment scam that defrauded investors out of over $15 million.

In 2021, the US Internal Revenue Service (IRS) announced that it had arrested a group of individuals for operating a cryptocurrency money laundering scheme that involved the use of ATMs and prepaid debit cards.

An INTERPOL police operation to tackle online fraud has seen almost 1000 suspects arrested and the seizure of USD 129,975,440 worth of virtual assets.

Fraud investigators around the world worked together over five months (28 June – 23 November) to intercept money and virtual assets linked to a wide range of cyber-enabled financial crimes and money laundering, assisting countries to recover and return illicitly obtained funds to victims.

Specifically targeting voice phishing, romance scams, sextortion, investment fraud and money laundering associated with illegal online gambling, Operation HAECHI III was coordinated by INTERPOL's Financial Crime and Anti-Corruption Centre (IFCACC) which supported 30 countries via their respective INTERPOL National Central Bureaus (NCBs)

C B I

NEW DELHI, INDIA

2022

the Austrian delegation has appreciated the Central Bureau of Investigation (CBI) officials for prompt action against a call centre through which foreign nationals were being duped by the persons posing as law enforcement and Europol officers. Owing to the investigation, there was a drastic reduction in the cases of frauds in Austria and its neighbouring countries, they told the agency.

Acting on the inputs received from some countries, the CBI had recently registered a case and searched a call centre in Delhi's Shadi Khampur village that had been targeting foreigners. Posing as law enforcement and Europol officers, they would tell the prospective victims that their identities had been stolen and used for committing crimes related to narcotics drugs in their names.

“In order to clear themselves of this suspicion, the victims were compelled to transfer their assets/money to a trust account through bank transfers, crypto wallets, gift card codes or voucher codes. Another call centre located in Noida was traced and raided. During the operation, about 25.83 Bitcoins and over ₹30.92 lakh stored in different wallets of the accused were frozen along with about ₹30.43 lakh lying in a bank account,”