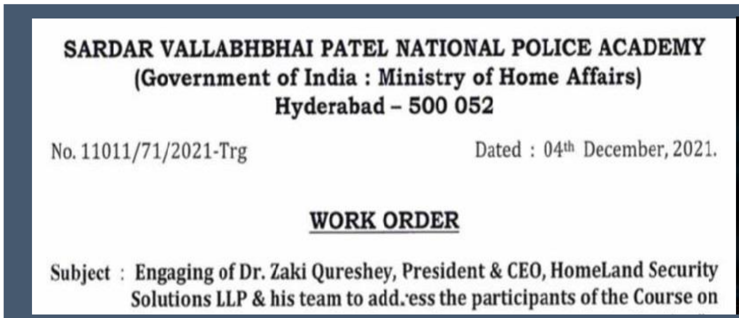
National Police Academy

Cryptocurrency Forensics Investigations Dossier

Index



SARDAR VALLABHBHAI PATEL NATIONAL POLICE ACADEMY
(Government of India : Ministry of Home Affairs)
Hyderabad – 500 052

No. 11011/71/2021-Trg Dated : 04th December, 2021.

WORK ORDER

Subject : Engaging of Dr. Zaki Qureshey, President & CEO, HomeLand Security Solutions LLP & his team to add.·ess the participants of the Course on

Hyderabad Security Cluster & HumanSTAR Collaboration

HumanSTAR & Hyderabad Security Cluster have co-developed a **unique proprietary training program** for Law Enforcement/Compliance Agencies to build their capability and capacity in tackling cryptocurrency crimes. This training program will help LEA's to understand the technology and follow the Standard Operating Procedures (SOPs) in evidence gathering and forensics to successfully achieve the conviction in a cryptocurrency fraud/scam case.

HumanSTAR has got support from **HomeLand Security Solutions – India Cryptocurrency Initiative** for this proprietary training program. BEGIN Indian Think Tank earlier **partnered with United Nations (UNTIL, United Nations Technology Innovation Labs)** in conducting a closed-door conference 'Cryptocurrency: Terror Financing VS Law Enforcement. The conference was attended by enforcement heads of Law Enforcement agencies and forensics Labs on 18th December 2019, at the UN India HQ in New Delhi. The closed-door conference discussed the LEA role and preparation required to handle crimes related to Bitcoins/ cryptocurrency. The meeting was chaired by Dr Subramaniam Swami, Hon'ble Member of Parliament. In the closed-door conference, it was decided to build the capacity of Indian LEA through appropriate training in handling crimes committed through bitcoin scams.

HumanSTAR* is a founding member of HSC, Hyderabad Security Cluster and is working actively to educate stakeholders about cryptocurrency.

Cryptocurrencies are now used for investing, trading and as a means of payment for goods and services. But it is globally accepted that its foremost use is for 'money laundering & funding illegal activity, almost unnoticed. On the one hand, private cryptocurrency poses potential dangers and challenges in its peer-to-peer form of use. That makes it anonymous & untraceable, hence a grave threat to the fiat currency, financial equilibrium & national security of countries.

According to a report published by BEGIN India Think Tank & UNTIL on cryptocurrency crimes in India, Indian individual investors lost close to investment worth US$ 10-12 billion in various cryptocurrency crimes in India from 2016 till 2019. Regrettably, there were no convictions to date

Cryptocurrency Investigations Training @ National Police Academy

About SVPNPA

Sardar Vallabhbhai Patel **National Police Academy** (SVPNPA) is the civil service training institution in India. The institute trains Indian Police Service (IPS) officers before they are sent to their respective state cadres to carry out their duties. It trains officers of the Indian Police Service, who have been selected through an All India based Civil Services Examination. The trained officers will be posted as Assistant Superintendent of Police (ASP) in their respective states under whom the other sub-ranks of police force will be working. The recruitment of sub-ranks such as Constables, Sub-Inspectors, and Deputy Superintendents of Police is each states prerogative, and will be done by respective state Director Generals of Police. The IPS cadre is controlled by the Home Ministry of the Government of India and the officer of this service can only be appointed removed by an order of the President of India

About HSC

The **Hyderabad Security Cluster – India's first Cyber Security Cluster was formed with the support of the Govt of India, Govt of Telangana** and under the leadership of the Founding Fathers, Hyderabad Security Cluster (HSC) is a critical and influential collaboration between 14 global cyber security ecosystems including Hague Security Delta (HSD)-Netherlands, and The Global Ecosystem of Ecosystems Partnership in Innovation and Cybersecurity (Global EPIC).

Established in May 2018, HSC is a replica of the Dutch Cluster called The Hague Security Delta (HSD), the largest cybersecurity cluster in Europe which houses over 200 organizations. Intensifying the Indo-Dutch cooperation, this cluster was endorsed by the **Indian Prime Minister, Narendra Modi & the Dutch Prime Minister, Mark Rutte with signing a "Programme of Corporation" on Cyber Security and was listed among the initiatives that were launched during the visit of Mark Rutte, to India on May 24, 2018.**

Following the 'TRIPLE HELIX MODEL' of academia, industry and Government partnership, HSC brings together security agencies of national and international importance, governments, research and knowledge institutions, cyber security businesses and all relevant stakeholders onto one platform and help in effective collaboration to deal with cyber-crime and warfare, implement cyber security best practices and create skill-ready professionals.

Cryptocurrency: Forensics & Investigations

The growing emergence and use of cryptocurrency in everyday situations bring an ever-growing influx of challenges and opportunities, therefore, law enforcement must keep pace with the challenges posed by novel business models and technologies.

According to a report, Indian individual investors **lost close to investment worth US$ 10-12 billion** in various cryptocurrency crimes in India from 2016 till 2019. Regrettably, there have been convictions to date.

The **HSC** is pleased to share that we have recently delivered a successful **Training on Cryptocurrency Forensics Investigations at the prestigious Sardhar Vallabhabhai Patel National Police Academy** attended by **47 Officers of the rank of ASP to IG from 23 state and central police organizations.**

'Summit for Democracy’
Hosted by US President Biden, PM Modi said, 'We must shape global norms for emerging tech like social media, cryptocurrencies so they are used to empower democracy, not undermine it”

The 3 day Cryptocurrency Investigations Training which was combined with Dark Web Investigations, will help the officers in building their capability and capacity in tackling cryptocurrency & dark-web crimes. This training program will help LEA's to understand the technology and follow the Standard Operating Procedures (SOPs) in evidence gathering and forensics to successfully achieve the conviction in a cryptocurrency fraud/scam case.

Capability Enhancers: Value Add To Existing Knowledge

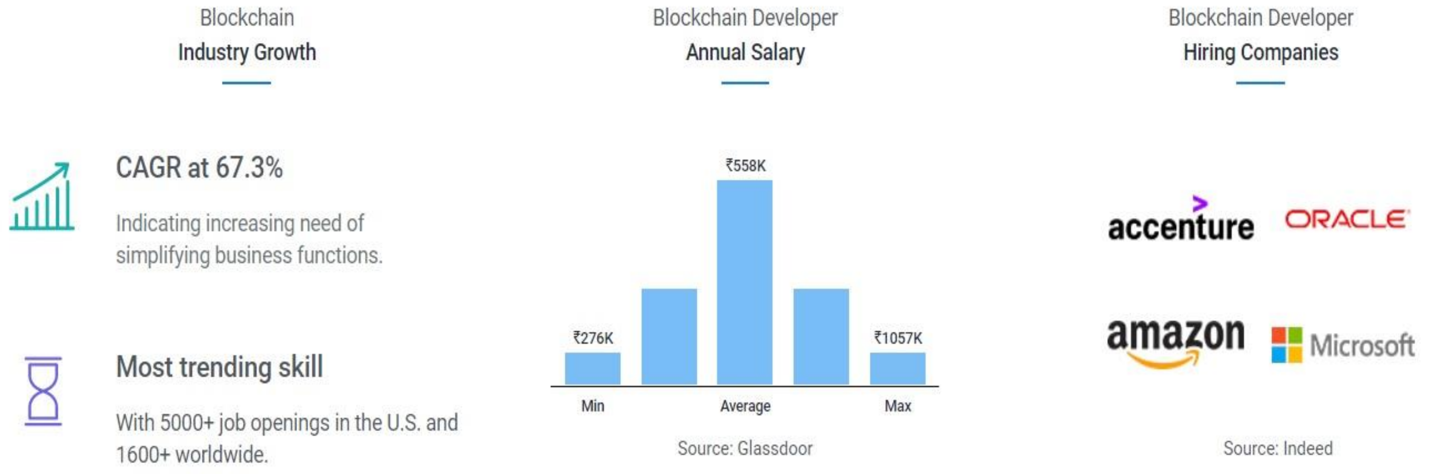
1. Key concepts and technology
2. Recognize the value proposition of cryptocurrencies
3. Understand how to analyze risk assessments drawing on Blockchain analysis/crypto forensics
4. Draw a high impact, globally competitive SOPs for Law Enforcement Agencies in Crypto crimes

Modus Operandi of Sophisticated Cryptocurrency Crimes - Crypto Payments as Indian Rupees (10/10)
DR. ZAKI QURESHEY

Cryptocurrency & Blockchain Market

The global cryptocurrency market size was valued at $1.49 billion in 2020, and is projected to reach $4.94 billion by 2030, growing at a CAGR of 12.8% from 2021 to 2030. Cryptocurrency is known as virtual currency. It is a form of currency that exists digitally only and has no central issuing or regulating authority above. It uses Blockchain technology to authenticate the transactions. Blockchain is a decentralized technology spread across many computers that manages and records transactions. Furthermore, it does not rely on banks to verify the transactions but is used as peer-to-peer system that enable users to send and receive payments from anywhere in the world.

On the other hand, the Blockchain market is expected to reach USD 39.7 billion by 2025, at a growth rate of 67.3 percent, indicating the increased adoption of Blockchain applications.



Blockchain Industry Growth

CAGR at 67.3%

Indicating increasing need of simplifying business functions.

Most trending skill

With 5000+ job openings in the U.S. and 1600+ worldwide.

Source: Glassdoor

Source: Indeed

OUTLOOK

THE WEEKLY NEWSMAGAZINE

By Madhuparna Sukul Published: 31st July 2021

“Digital disruption has brought with it the advent of safe haven for cyber crooks, posing a great threat to personal finance”

Digital disruption has brought with it the advent of a safe haven for cyber crooks, posing a great threat to personal finance

Madhuparna Roy Sukul

Unlike its dubious peers, the instant loan app didn't ask for access to his personal details, and promised to lend Rs 10,000 within two hours of filling up some basic credentials. It took Balaji Vijayaraghavan barely 30 seconds to download SnapIt. And an hour later, he received a text message from his bank, saying that Rs 1 lakh was debited from his account.

It was a typical case of data breach. The criminology graduate handled the situation firmly. He immediately blocked all his bank accounts and got in touch with Save Them India Foundation, a non-government organisation, to investigate the cybersecurity aspects of the incident.

Balaji discovered that although he did not log into the app, neither gave access to any other apps like contacts, camera or gallery, the hackers managed to invade his phone with 59 malwares. The fraudsters actually hijacked his phone and used it to send text messages and read OTPs received. This gave them the access to his bank account.

The bank account was perhaps used for money laundering activities like using cryptocurrency for dark web transactions or, put it simply, to turn dirty money clean. The incident was published in details in a news portal.

Balaji's was just one of the innumerable cybercrime cases reported every year in India and abroad. A raging wave of digitalisation and a life increasingly dependent on apps are largely setting the perfect stage for cybercrime. While SPECOPS data from 2006 to 2020 shows that the US leads the pack of countries hit hardest by cyberattacks, the threat landscape has grown significantly for India during the pandemic. From your identity and bank account details to vaccine or eyes, you think of it, and it's on sale on dark web.

Welcome to the wild world of dark web. Out of bounds for conventional search engines, it needs specific browsers, such as Tor, to reach dark web. The browser provides privacy and secrecy to the user. But the concept of dark web developed into a free space to access anything while staying invisible. From child pornography, illegal drugs and sex trafficking to extortion and hacking – dark web is being used for all the wrong reasons. Not to forget, abetment to suicides, murders and contract killing make dark web a great catalyst for those with hostile intent.

Dark web, also referred to as dark net, is a portion of the internet that requires special software to access and can be difficult to navigate once you do. People may browse and post information on dark web with relative anonymity because of many levels of encryption, which makes it a popular venue for buying and selling illicit products and services.

Tor, which stands for The Onion Router, bounces data through several encrypted layers like an onion to provide greater anonymity to users. On the Tor network, there are onion sites and services and the page addresses end with '.onion' instead of the likes of '.com' or '.net' or '.org'. Tor is just another technology which, when used for a good purpose, can yield some great results like avoiding censorship, accessing illegal markets to get hold of certain pills that

that help access dark net. In reality, there's only about 6.7 per cent of Tor users in India who are accessing dark web and that's despite the infamy of being the hub of criminal activities.

The fact that India leads in terms of population and rising interest of citizens in technology, it is to be seen how the country makes the most of cryptocurrencies and fight the dark threat.

Dark web accounts for nearly 500,000 users that include over 2,400 sellers and 320,000 transactions per year. According to a study on the dark web economy by Armor Threat Resistance Unit, a dark net user could get around $10,000 in cash for Bitcoin worth $800 (*Forbes*).

It is hard to estimate the approximate size of the market for dark web content. According to a recent study on the dark web intelligence market, it is estimated to exceed $840 million by 2026 averaging an annual growth rate of over 20.1 per cent.

A study conducted by the Carnegie Mellon University in 2013, Silk Road netted a whopping $300,000 per day and closing at roughly $100 million a year. While Silk Road was shut down by the FBI in 2013, the model inspired the mushrooming of many such marketplaces like Evolution, Agora, Nucleus and Abraxas, with listings for drugs, fake IDs and firearms. Silk Road was an online black-market platform, popular for money laundering activities. It was replaced by the next largest dark web marketplace, Agora.

ZAKI QURESHEY
Director-General of HSC & Homeland Security Solutions BV

Many large Indian businesses have fallen victims of ransomware attacks that put the average Indian at risk of becoming an easy target of online fraud

The way the dark web marketplace is expanding, the estimated money at stake is beyond our imagination. Based on an analysis conducted on raw data of Bitcoin transactions carried out on 31 of the biggest marketplaces on dark net, the approximate amount of money (in Bitcoin) involved – both sent and received – stands at $4.210 billion.

A Chainalysis (blockchain data platform) report says the dark web market recorded the best profit of $1.7 billion in cryptocurrency last year, although individual purchases dipped from $12.2 million in 2019 to $10 million in 2020. Hydra, perhaps the largest dark web marketplace, constituted over 75 per cent of the profit logged in last year.

While implementing cybersecurity regulations and using anti-malware software or spam filters do assure security to some extent, the rate at which the fraudsters catch up with the latest technology is unthinkable. Leveraging the threat intelligence services can help detect the tools being deployed for cyberattacks as well as to collect threat data.

"There are certain fixed norms where whenever we get our system audited from external auditors, we ensure that our penetration testing is well certified to avoid any injection and ensure data localisation to avoid any customer data to be placed outside the country," says Gautam Sinha, a FACE Member and Vice President for Technology at LoanTap.

Madhusudan Ekambaram, fellow FACE Member and Co-Founder and CEO of KreditBee, assures that proactive measures have been taken by digital lenders, RBI and FinTech Association for Consumer Empowerment (FACE) for the digital lending ecosystem. "Leading digital lenders have set up robust data architecture and technology infrastructure, eliminating their dependence on the customers' galleries or contact lists. They are also ensuring the central storage of the customer's KYC data and are performing information security audits consistently," he says.

The advancement of technology would be impossible to adapt without being aware that there's always a flip side to it. India might be fast turning into a bright spot on dark web, there are cyber cops watching out for any kind of malicious activities on the net. But nothing can ward off the menace unless every individual becomes more proactive to prepare and pre-empt the threat. ◘

The writer is a tech journalist

Flavours of the Web

Clear Web/ Surface Web	Deep Web	Dark Web
The part of the internet accessed by regular users	The part of the internet hidden from users	The part of the Deep Web deliberately and securely made invisible
Contains online content indexed mainly by search engines	Contents are not indexed by the usual web search engines but are accessible	Hosts websites with hidden IP addresses; need specialised software for access like Tor browser
Not involved in illegal activities	Not involved in illegal activities	Being anonymous is important and illegal activities are common
Contains primarily legal content, and illegal activities are limited	Contains mostly benign sites, hosts illegal subscriber databases	Websites are encrypted to offer anonymity
Only 10% of the internet	Enormous compared to Clear Web; contains 90% of all online content	Websites are only in thousands; 0.01% of the Deep Web

Hacking: A Fact Sheet

Common techniques used	Cyber attacks on government and institutions resulting in loss of $1 million or more	Biggest cyber offenders	Most attacked Industries in 2020	Number of attacks in Asia Pacific region	Types of cyberattacks specific to the A-Pac region
1. Script-based, 2. Manual communication hack 3. Phishing Attack, 4. Denial of Service Attack (DoS)	USA **156**, UK **47**, India **23**, Germany **21**, South Korea **18**	China, Russia, Iran, North Korea, India	Manufacturing, energy, finance and insurance	**25%** of all cyberattacks across the world Most attacked - Japan and India	Data theft - **22%**, Ransomware - **19%** Other: Trojans, common vulnerabilities attacks & ransomware

What is Tor?

The Onion Router, Tor, in short, is a free and open-source software that enables anonymous communication. It directs Internet traffic through a free, worldwide, volunteer overlay network consisting of more than 6,000 relays to conceal users' location and usage from anyone conducting network surveillance or traffic analysis

Tor Fact Sheet

- 65,000 URLs with .onion extension available on the Tor network
- Major social media websites and search engines have onion versions of their websites
- More than 2 million active users connected to Tor
- In a recent survey, 26% of respondents confessed to using Tor

Dungeon of the Web

With hackers attacking every 39 seconds, dark web activity surged three-fold in the last three years

Major Financial Data Leaks

- **Air India** - Personal information of 4.5 million passengers hacked worldwide, includes credit card details (February 2021)
- **Upstox** – The trading platform admitted to a breach of KYC data (April 2021)
- **Dominos** - 1 million credit card records compromised (April 2021)
- **Juspay** – Card details of 35 million user accounts (January 2021)
- **State Bank of India (SBI)** – Account details of nearly 3 million customers

Dark Web Activity Stats

- Hackers attack every 39 seconds
- Dark Web activity surged three-fold in the last three years.
- 59% of listings on marketplaces are for illegal drugs and chemicals
- 41% for firearms, hacking tutorials, frauds and pharmaceuticals
- Empire, a leading dark web marketplace, hosts 6,000 products; 50% are drugs
- 50,000 extremist groups are active on dark web

Effect of Dark Web on Individual Finance

- 22 billion records exposed to the dark web in 2020
- Bitcoin transaction shot up by 340% since 2017
- Accounts of 25.9 million Fortune 1000 businesses, 543 million employee credentials available
- Credit card numbers available for just $9 and payment data for $270
- Scanned copy of passport available for just $2
- Driving licences credit history are some popular targets on dark web

Effects of Dark Web on Financial Institutions

- More than 3,50,000 financial services sensitive data gets exposed on dark web regularly
- 19% of the criminal activities online hits finance and the insurance sectors
- The banking sector was hit majorly by dark web in 2018, costing $18.3 million

How is Dark Web Affecting India?

- India is among the top nations with most data breaches per year
- Personal data of 29 million Indian job seekers are on dark web
- 8.2TB (Terabytes) of personal details of 3.5 million Indian users are up for sale
- Email and phone numbers of 7 million Indian debit and credit cardholders are on sale
- 100 GB of Indians' data up for sale on dark web

Telangana Today
FOR LOCAL TO GLOBAL NEWS

US keen to explore ties with Telangana in cybersecurity space

By Y V Phani Rai Published: 6th Sep 2021 8:00 Pm

Hyderabad: The **US government is keen to explore ties with Telangana government in the cybersecurity sector**, particularly in the areas of **cryptocurrency forensics**, capacity building and technology transfer, amidst national security challenges presented by China, Russia and other cyber and emerging technology competitors and adversaries.

Telangana has been a frontrunner in cybersecurity with dedicated efforts / initiatives such as a **State policy, Hyderabad Security Cluster** and Cybersecurity Centre of Excellence.

The deputy assistant to the US President and deputy national security advisor (DNSA) for Cyber & Emerging Technology on the National Security Council Anne Neuberger, who was in India on a short trip recently, exchanged thoughts on potential cooperation and collaboration with the Government of Telangana, represented by Industries & Commerce and IT principal secretary, Jayesh Ranjan.

The meeting, which was also attended by Hyderabad Security Cluster (HSC) director general Dr Zaki Qureshey and representatives of Nasscom, Intel and DNSA, focused on how both sides could address and build plans, resources, and capabilities around the convergence of operational technology and information technology. Representatives from the US Embassy-New Delhi, Consul General in Hyderabad Joel Reifman, two National Security Council staff directors who travelled with Anne Neuberger had also joined along with officials from the Economic Section in the virtual meeting.

Dr Zaki Qureshey, Director General, HSC, told Telangana Today, "We discussed on core cybersecurity concerns such as ransomware attacks, Pegasus revelations, cryptocurrency, phishing, and spyware that have made inroads into the nations that not just corporates, governments and defense forces are feeling the heat, but even small businesses and individuals are impacted."

India has lost $12 billion in cryptocurrency scams in the last four years but not a single prosecution has taken place. Indian States do not have jurisdiction beyond India, even different States in India have jurisdiction issues, Qureshey said this has become a challenge for investigation agencies.

Hyderabad's capabilities

While addressing the cybersecurity challenges, the Hyderabad Security Cluster today focuses on tackling cyber threats to ensure that the emerging technologies such as **artificial intelligence, 5G, cryptocurrency, quantum computing,** networks and related technologies are used for the digital transformation.

Qureshey said, "Hyderabad is on the verge of becoming the cyber security capital of India, under the leadership of KT Rama Rao, Minister for Information Technology, Government of Telangana."

Building resilience

"I would say that more aspects than just threat detection need investments and integration. Education, development, regulations, cooperation, and collaboration all need further investment and integration. This is a core aspiration for both our countries," he added.

It has become important for nations to build resilience and secure supply chains for critical technologies. He added, "We have sought Neuberger and the current US Administration to look at collaborating in several critical areas and share efforts, so that we multiply our outcomes as well as ensure developments don't happen in silos."

"There are 5,00,000 cyber-related jobs available in the US alone. We need to build stronger partnerships between the US and Indian education systems, particularly in the cybersecurity space. There is a rich history of talent exchanges in general between our two countries, and more interestingly in the space of technology. The HSC would be interested to follow up with the US administration on the next steps, share efforts and seek possible cooperation and collaboration," Qureshey emphasized.

https://telanganatoday.com/us-keen-to-explore-ties-with-telangana-in-cybersecurity-space

ACCEPTED HERE
CRYPTO
SCC
Cryptocurrency in India: An Unregulated Safe Haven For Money Laundering?

Outlook

Published: 19 Sep 2021, Updated: 19 Sep 2021 5:52 pm3:02 pm

What Is Forensic In Cryptocurrency Analysis? How Does It Help Law Enforcement Agencies?

Blockchain is a digital and decentralized public ledger with a system that records transactions across several computers linked to a peer-to-peer network. It was originally developed for cryptocurrency assets like Bitcoin in 2008. Blockchain Analysis/ Crypto Forensics creates transparency for a global economy built on blockchains, enabling banks, businesses, and governments to have a common understanding of how people and businesses use cryptocurrency.

Following is a brief on how LEA's can leverage Crypto Forensics to build a charge sheet for successful case closure.

> Visualization and Tracking Tools: Case management solution maintains user-friendly case tracking that has been developed for secure, practical and collaborative use

> Broad Transaction Coverage: Ensures real-time information across all the major blockchains and thousands of entities, currently attributing 90% of all active transactions

> Automated & Evidence-Based: Provides immutable historical data logging with real-time updates and sophisticated risk assessment. Available through API license, Law Enforcement/compliance officers can track and trace potentially illicit activities such as fraud, scams, security breaches, money laundering, or terrorist financing by using crypto forensics tools.

Views and thought on the cryptocurrency concerning retail investors.

In India, there are close to 15 million retail investors, who are registered with various Indian cryptocurrency exchanges. Education is a must for retail investors before investing in cryptocurrency. Most of the cryptocurrency sees 15-20% price volatility in a week or so and it creates anxiety in retail investors. Additionally, the government of India hasn't defined cryptocurrency as a legal entity. However, due to the fundamental nature of peer-to-peer transactions mechanisms of cryptocurrencies, investors can trade in cryptocurrency without any third party knowing about it. How to keep oneself safe from these frauds Retail investors should lookout for the following indicators before buying into any scheme or investment advice:

- Is the company registered in India, if not, avoid any financial transaction or bitcoin transaction
- Who are the owners – You will get the background of all the owners from the internet and if the company hasn't declared their names on their website, stay away from them. Investors should invest 1-2 hours in basic research before putting their hard-earned money
- What is the cryptocurrency they are selling and from which online platform? There are more than 1500 cryptocurrencies across the globe and all of them do not have the technology or use case to further their business needs. Investors should target only the top 10-15 cryptocurrencies for trading.
- Buy cryptocurrency in India from crypto exchanges that have a valid and transparent KYC (Know Your Customer) system in place. There are around 15 crypto exchanges that will qualify
- Do not trust any here say, be prepare to do some research on any new technology and accordingly take actions
- Indian crypto exchanges with valid KYC practice provides investors safety, in case the crypto exchanges are hacked. Do not buy any cryptocurrency from any exchanges that do not protect your digital assets.
- Lastly, there is an umpteen number of wallets available on the market, propagated by the private players. Investors should use at least 3-levels of password protection mechanisms (password, 2FA and google authentication) and do not share passwords on the mail or SMS/ WhatsApp with their loved ones.

Are there any grievance redressal process for fraud victims and what they should do if they fall victim?

Since cryptocurrency has not been legally defined by the Government of India, there is no government redressal system available in India. However, independent bodies likes Hyderabad Security Cluster and BEGIN India Think Tank continue to help investors if they get cheated, on case to case basis. Large fraud has been reported to the police and filed as FIR. However, due to the lack of capacity and capability of Indian LEAs & forensics agencies, digital forensics evidence does not get recorded and most of the culprits got bail in the respective cases.

Chinese Online Gambling Scam Case Study

High Possibility of Cryptocurrency paid as Gambling money By Indian Nationals to Chinese apps

August 2020

A Chinese national and three of his Indian associates have been arrested in a crackdown on an illegal online gambling racket being run by a China-based company, the police said on Thursday. The Chinese national and his associates were arrested by the Hyderabad police from Delhi on Wednesday and brought to Hyderabad on Thursday.

The development comes a day after Chinese individuals and companies were raided by income tax sleuths in Delhi, Gurugram and Noida on suspicion of laundering money. The online gambling was allegedly organised by different companies under the umbrella of China-based "Beijing T Power Company", the police claimed, adding that transactions worth Rs 1,100 crore had been unearthed.

A total of 1.24 crore transactions were found to be paid to Chinese online betting scams websites for a total of INR 11,00 crore by Indian Nationals. The HSBC bank accounts in operation were located in Gurugram One Chinese national, Yah Hao, the online firm's head of operations and three Indian nationals, namely - Dheeraj Sarkar, Ankit Kapoor and Neeraj Tuli were arrested from their office in Gurugram.

How Hyderabad Security Cluster & HumanSTAR Can Help.

In association and guidance from Hyderabad Security Cluster, HumanSTAR can provide exact details of cryptocurrency funds movement from one wallet address to another wallet address.
HSC & HS can provide a detailed data analysis of funds that are transferred to the Online Gambling Chinese app with country and crypto exchange details.

For this to happen, HSC & HS will require a Bitcoin wallet address, transaction id and other cryptocurrency details from police.

The employees of Beijing T Power Company arrested will have all these details in their official communication with the customers or within the office memo.

It may take 20-30 days for HSC & HS to provide evidence of cryptocurrency involvement and detailed data analysis, once respective details are shared by police.

https://www.outlookindia.com/website/story/business-news-what-is-forensic-in-cryptocurrency-analysis-how-does-it-help-law-enforcement-agencies/395054