A Report on

"Online Awareness Programme on Blockchain and Cryptocurrency Investigation"

For B. Tech CSE (Cyber Security) students

Organized by

Department of Computer Science and Engineering (Cyber Security) On 06.10.2026



Report submitted by:
Mrs. Pagadala Naveena, Assistant Professor & Mr. Goli Nageswararao, Assistant Professor, Department of CSE-Cyber Security.

Resource Person Details:

Dr. Rakesh Kumar Chawla, Deputy Director,
National Crime Records Bureau (NCRB), Ministry of Home Affairs, New Delhi.

Date & Time: 06.10.2026, 11:00 AM to 12:30 PM **Venue:**
Seminar Hall, KKB Block, MITS **Participants:** B. Tech CSE
(Cyber Security) students **Mode of Conduct: Online**

1. **Objectives of the Program**

The primary objective of the programme was to create awareness among B.Tech (Cyber Security) students about blockchain technology, cryptocurrencies, and the investigation of crimes involving digital currencies. The programme aimed to explain how blockchain transactions work, how cryptocurrencies are misused for ransomware, investment frauds and money laundering, and how law-enforcement agencies trace such transactions. The session also aimed to bridge the gap between academic learning and real-world investigative practice by giving students exposure to the experience of a senior officer from the National Crime Records Bureau.

2. **Inaugural Session**

The programme commenced with a warm welcome to the distinguished resource person, Dean – School of Computing, Head of the Department of CSE (Cyber Security), faculty members, and students. The coordinators introduced the resource person, Dr. Rakesh Kumar Chawla, Deputy Director, NCRB, Ministry of Home Affairs, highlighting his Ph.D. from Amity University, the Union MHA Best Trainer Award and the President's Police Medal conferred on him, and his role as guest faculty for Delhi Police, CBI and NICFS.The resource person commenced the technical session by introducing the participants to the fundamentals of blockchain and cryptocurrencies. The session progressively covered cryptocurrency-enabled cybercrimes, investigation and tracing techniques, and the legal and

reporting framework in India. The session was conducted online and streamed live to the students assembled in the seminar hall.





3. **Key Highlights**

- **Blockchain Fundamentals:** Distributed ledger, cryptographic hashing, consensus mechanisms, and why blockchain records are tamper-evident.
- **Wallets and Keys:** Public addresses, private keys, custodial and non-custodial wallets, and the pseudonymous nature of transactions.
- **Cryptocurrency in Cybercrime:** Use of cryptocurrencies in ransomware, fake investment and trading apps, Ponzi-style frauds, and dark-web marketplaces.
- **Money Laundering Methods:** How criminals use mixers, multiple wallets and cross-border exchanges to hide the trail of funds.
- **Investigation Techniques:** Transaction tracing with blockchain explorers, address clustering, and linking wallets to real identities through exchange KYC records.
- **Digital Evidence Handling:** Seizure of wallets, preservation of digital evidence, and maintaining the chain of custody.
- **Legal and Reporting Framework:** Role of NCRB and law-enforcement agencies, the National Cyber Crime Reporting Portal (cybercrime.gov.in), helpline 1930, and anti-money- laundering obligations for virtual digital asset service providers.
- **Interactive Learning:** Students actively participated in the discussion and clarified their queries on careers in cyber forensics and cross-border crypto investigation.
- The program concluded with a vote of thanks expressing gratitude to the resource person, management, Dean, HoD, faculty members, and students for making the programme informative and engaging.

Outcome of the Program:

At the end of the session, participants were able to:

- Explain the basic concepts of blockchain and how cryptocurrency transactions work.
- Identify common patterns of cryptocurrency-enabled fraud, ransomware and money laundering.
- Describe how investigators trace funds on a public blockchain and link wallets to real identities.
- Understand the importance of proper digital evidence handling in crypto-related cases.
- Recognise the reporting mechanisms and legal framework for cyber financial crimes in India.
- Relate blockchain investigation to the broader field of Cyber Security and digital forensics.

The programme provided participants with foundational knowledge of blockchain and cryptocurrency, along with practical awareness of how crypto-related crimes are investigated by national agencies. The insights shared by the resource person enabled students to connect theoretical concepts of cryptography and networks with real-world forensic practice.

The session concluded with a vote of thanks presented by the coordinators, Department of CSE (Cyber Security) at Madanapalle Institute of Technology & Science (Deemed to be University), Madanapalle.