Exploring the Advances of Artificial Intelligence in Cryptocurrencies and Darknet Forensics

Ramy El-Kady
http://orcid.org/0000-0003-2208-7576
Dubai Police Academy, UAE

ABSTRACT

This article explores the digital forensics of cryptocurrencies and the dark web, highlighting the role of blockchain, computers, and mobile phones in their formation and evidence gathering. It also discusses the use of artificial intelligence and machine language in dark web forensics. The article highlights the need for immediate research in digital cryptocurrency forensics, particularly in cryptocurrencies like Monero, Ethereum, Verge, and Dogecoin, and the gap in host-based cryptocurrency forensics. Cryptocurrency forensics mostly looks at public blockchains using clustering heuristics and machine learning-based analysis to find anonymous entities or help with investigations. The Elliptic Dataset, a significant resource, has been developed to study machine learning and graph-based methods in Bitcoin forensics based on blockchain technology, providing a wealth of information for researchers in the field. Blockchain-based forensics research is progressing organically alongside technological advancements, offering a promising future.

INTRODUCTION

In recent years, the accelerating integration of modern technologies into everyday life has fundamentally reshaped the landscape of criminal activity. Criminal networks and terrorist organizations have proven particularly adept at exploiting the architecture of the Internet to facilitate recruitment, coordinate operations, launder proceeds, and conceal illicit communications. This technological opportunism has coincided with a marked increase in cyber-dependent and cyber-enabled offences, including identity theft,

DOI: 10.4018/406039

online fraud, ransomware attacks, and large-scale data breaches. Such crimes not only generate substantial economic losses but also undermine public trust in digital infrastructures and threaten national security.

Within this evolving criminogenic environment, digital forensics has emerged as an indispensable pillar of contemporary criminal justice. It is no longer a peripheral technical specialty, but rather a core investigative discipline that bridges technology and law. Through the identification, preservation, analysis, and presentation of electronic evidence, digital forensics enables law enforcement agencies to reconstruct criminal conduct in virtual spaces that are otherwise intangible and transnational. Its evidentiary function is particularly vital in meeting the standards of legality, due process, and evidentiary integrity required in criminal proceedings.

Moreover, the probative value of digital evidence often determines the success or failure of prosecutions in cybercrime cases. Proper forensic methodologies ensure the authenticity, reliability, and chain of custody of electronic data, thereby safeguarding the rights of the accused while strengthening the capacity of the state to combat sophisticated digital criminality. In this sense, investment in digital forensic capabilities is not merely a technical necessity; it is a normative imperative for upholding the rule of law in the digital age (El-Kady, 2023).

Criminal groups develop their methods and skills using emerging technologies, especially the darknet, which, given its unique technological nature, provides them with more facilities to commit illegal activities far from law enforcement agencies.

In this broader technological milieu, successive waves of innovation have precipitated the rise of cryptocurrencies, which have rapidly expanded into diverse spheres of economic and legal interaction. Originally conceived as decentralized financial instruments operating outside traditional banking frameworks, cryptocurrencies have evolved into complex ecosystems supported by blockchain technology, cryptographic protocols, and distributed networks. While these features were designed to enhance security, transparency, and autonomy, they have simultaneously rendered such currencies attractive to criminal groups and terrorist organizations.

Particularly within the environment of the Darknet—accessible through anonymizing technologies and layered encryption—cryptocurrencies have become a preferred medium of exchange for illicit transactions. Drug trafficking, arms sales, ransomware payments, money laundering, and terrorist financing increasingly rely on digital currencies that exploit pseudonymity, cross-border fluidity, and the absence of centralized oversight. The convergence between cryptocurrencies and the Darknet intensifies investigative complexity, as both infrastructures are structured to obscure identity, conceal transactional trails, and frustrate conventional surveillance techniques. Consequently, law enforcement agencies encounter substantial obstacles in identifying perpetrators and attributing criminal responsibility.

Against this backdrop, one of the most pressing challenges concerns evidentiary proof. The inherently technical and decentralized nature of cryptocurrency transactions complicates the processes of seizure, preservation, authentication, and presentation of digital evidence. Questions of jurisdiction, chain of custody, encryption barriers, and forensic integrity further compound these difficulties. It is precisely within this evidentiary dilemma that digital forensics assumes heightened significance (El-Kady, 2025).

This study therefore seeks to examine the digital forensics of cryptocurrencies and the Darknet through a comprehensive analytical lens. It will explore the technical and legal dimensions of foundational elements such as blockchain architecture, digital wallets, computers, and mobile devices as repositories of evidentiary data. Particular attention will be devoted to forensic methodologies employed in tracing cryptocurrency transactions, recovering digital artifacts, and correlating on-chain and off-chain evidence. Furthermore, the study will critically assess the extent to which artificial intelligence (AI) and machine