International Journal of Cybersecurity Intelligence & Cybercrime

Volume 7 | Issue 1 Article 4

2-29-2024

# Book Review: Tracers in the Dark: The Global Hunt for the Crime Lords of Cryptocurrency

cryptocurrency, law enforcement, privacy, cybercrime

Jones (2024). *International Journal of Cybersecurity Intelligence and Cybercrime, 7*(1), 44-47.

# Book Review: Tracers in the Dark: The Global Hunt for the Crime Lords of Cryptocurrency

Marion Jones*, CISSP, Cybersecurity Consultant, U.S.A.

*Keywords: cryptocurrency; law enforcement; privacy; cybercrime*

**Abstract:**
Doubleday released Andy Greenberg's Tracers in the Dark: The Global Hunt for the Crime Lords of Cryptocurrency in November 2022. Through vivid case studies of global criminal investigations, the book dispels myths about the anonymizing power of cryptocurrency. The book details how the ability to identify cryptocurrency users and payment methods successfully brought down several large criminal empires, while also highlighting the continuous cat-and-mouse game between law enforcement officials and criminal actors using cryptocurrency. The book is an excellent resource for law enforcement officials, academics, and general cybersecurity practitioners interested in cryptocurrency-related criminal activities and law enforcement techniques.

## Introduction

Cryptocurrency has been surrounded in a shroud of mystery and privacy assumptions since Satoshi Nakamoto released his seminal 2008 paper that outlined the concept of Bitcoin (Nakomoto, 2008). In Tracers in the Dark: The Global Hunt for the Crime Lords of Cryptocurrency, Andy Greenberg (2022) dispels many of the myths surrounding the perceived anonymity cryptocurrency offers to its users and describes with insider detail how law enforcement officials around the globe are using sophisticated techniques to identify, track, and apprehend criminals who are using cryptocurrency to fuel illegal activities.

The book does an excellent job describing the keys to a successful cryptocurrency-related investigation and also shows the role academia and the private sector have played in the ever-evolving cat-and-mouse game between enforcement officials and cybercriminals. The book assumes a basic understanding of cryptocurrency technologies and law enforcement methods. Some readers may find Greenberg paid too little attention to the larger implications of the increasingly mainstream adoption of cryptocurrency, such as nation states adopting cryptocurrency or the potential impact of increasing government regulation.

The book can be a great resource for law enforcement officials pursuing cryptocurrency-related crime, academics who are interested in seeing how their work can affect real-world issues, or the layperson who is interested in the technology arms race between law enforcement and criminal entities.

## Overview

Greenberg divides his book into five parts that center on three cryptocurrency-focused U.S. law enforcement investigations. Interwoven in these case studies are details of the academic community and private sector's efforts to study and de-anonymize cryptocurrency. Greenberg closes the book by examining the evolution of cryptocurrency and considering its future involvement in criminal efforts and geopolitics.

*Corresponding author
Marion Jones, Cybersecurity Consultant, 500 North Akard Street, Dallas, Texas, 75201, U.S.A.
Email: Mjones5876@proton.me

Greenberg begins the book by examining the Silk Road criminal network and U.S. law enforcement's efforts to identify and arrest its founder, Ross Ulbricht. Greenberg provides a brief overview of the Silk Road investigation, and readers interested in more in-depth coverage of the investigation should refer to Bilton (2017). Whereas Bilton provided a biography of Ulbricht and followed the Silk Road from its creation, Greenberg largely picks up after the collapse of the Silk Road and covers the Internal Revenue Service (IRS)'s efforts to identify and arrest Secret Service and Drug Enforcement Administration (DEA) agents who stole Silk Road cryptocurrency during the investigation.

Greenberg then examines the DEA's investigation into Alpha Bay, which became the major illicit, crypto-currency-fueled narcotics network operating after the Silk Road's takedown in 2013. Greenberg's access to law enforcement officials and information is superb throughout the book, but it particularly shines during this section, and his detailed explanation of the global cooperation by U.S., Thai, and Dutch law enforcement officials all targeting the same Alpha Bay network is riveting.

The last major case study in the book revolves around the website Welcome to Video, which housed child sexual abuse videos in exchange for cryptocurrency payments. While at times difficult to read due to the nature of the offenses involved, this last section is particularly interesting, as it diverges from the narcotics-focused Silk Road and Alpha Bay investigations to show how cryptocurrency is being leveraged in other types of crimes.

Interspersed throughout the three case studies, Greenberg traces the work of academia and the private sector in understanding cryptocurrency and its perceived anonymity. The book begins by discussing the academic paper that was one of the first to show that cryptocurrency transactions could be traced (Meiklejohn et al., 2013) and goes on to explain academic studies that have shown how seemingly disparate cryptocurrency transactions can be lumped together and readily traced to single entities.

The private crypto analysis firm Chainalysis is another character detailed throughout the book, and Greenberg describes its evolution from a two-person company into one of the major cryptocurrency tracking and evaluation companies in existence today. Chainalysis plays a crucial role in assisting U.S. law enforcement efforts throughout the book.

**The Book Provides a Solid Foundation**

Tracers in the Dark can serve as a great reference for law enforcement officials who are interested in understanding the inner workings of cryptocurrency-related investigations. The book also thoroughly explains the evolving cat-and-mouse game between regulators and criminals that those interested in criminal trends and law enforcement techniques would find fascinating. Lastly, the book can serve as an example to those in the academic community who wonder how their work can have real-world impact.

Law enforcement officials can use Tracers in the Dark as an easy-to-read guide on how cryptocurrency investigations can be conducted. The book details how techniques—largely drawn from Chainalysis's work and partnership with U.S. law enforcement—can trace cryptocurrency transactions despite complicated obfuscation efforts from criminals. The book explains how traditional law enforcement tools, such as subpoenas and search warrants, can be used to identify account owners. It also explains why crypto companies not based in the United States are increasingly compliant with the U.S. legal process in an effort to appear above-board, as cryptocurrency regulation becomes a focus of the financial regulation industry.

Arguably the most important thing Tracers in the Dark can provide law enforcement officials is recognition that a technical background or cybersecurity proficiency is not a prerequisite to conduct cryptocurrency investigations. Notably, none of the IRS, FBI, or DEA agents profiled in Greenberg's book had extensive cybersecurity or cryptographic experience prior to launching their investigations. No doubt they had the support of experts in these fields along the way, but officials should not be daunted by a perceived lack of knowledge. The book also explains other cybersecurity tools and concepts, such as Tor browsers, the Dark Web, encryption, and internet protocol (IP) routing and identification, which could be helpful to law enforcement agents who are new to the world of cryptocurrency investigations.

Those in the field of academia may also find Tracers in the Dark an interesting read, as it shows the real-world impact that academic work can have. The book shows that Meiklejohn's and other academic writings were the first to show cracks in the perceived anonymity of cryptocurrency. While Meiklejohn turned down an offer to work for Chainalysis during its early days, the crypto field is rife with academics who decided to take their extensive knowledge into the private sector (Cadogan, 2021; Vora, 2020).

**But Misses Some Bigger Questions**

Tracers in the Dark can serve as a helpful introduction to cryptocurrency investigations and criminal activities, but it also misses larger questions surrounding these issues. The topic of cryptocurrency facilitating ransomware attacks is addressed briefly by Greenberg towards the end of the book, but the analysis leaves the reader wanting more after such detailed case studies earlier. Greenberg may have been light on ransomware in the book because it was covered more extensively, and quite effectively, in his previous work focused on Russian cyberwarfare activity in Ukraine, and interested readers should turn there for more information (Greenberg, 2019).

The right to anonymity has been a tenant of cryptocurrency since its initial conception (May, 1988), but Greenberg covers the ethical questions surrounding cryptocurrency and the right to privacy in light detail, and a deeper discussion on this issue is certainly warranted.

Lastly, the book mentions the problem that state actors—such as Russia and North Korea—pose in providing safe harbor to cryptocurrency criminals; however, given the size of the problem, it is not discussed in the detail it deserves. It is difficult for U.S. prosecutors to act against cryptocurrency criminals living in these countries unless these criminals travel to, or through, nations that cooperate with U.S. law enforcement agencies. Greenberg does little to identify alternatives that this leaves law enforcement officials, perhaps because there are none.

**An Entertaining Read for Anyone**

Through in-depth reporting of real-life case studies, Greenberg builds the seemingly niche topic of cryptocurrency crime into a fascinating account of law enforcement battling criminals. Law enforcement officials, academics, and laypersons interested in true crime will find Tracers in the Dark worthwhile reading.

**References**

Bilton, N. (2017). *American kingpin: The epic hunt for the criminal mastermind behind the silk road.* Penguin.

Cadogan, M. (2021, February 9). Startup Spotlight: Cornell Professor Founds Crypto Startup With Two Graduate Students. *The Cornell Daily Sun.* https://cornellsun.com/2021/02/09/startup-spotlight-cornell-professor-founds-crypto-start-up-with-two-graduate-students/

Greenberg, A. (2019). *Sandworm: A new era of cyberwar and the hunt for the kremlin's most dangerous hackers.* Anchor.

Greenberg, A. (2022). *Tracers in the dark: The global hunt for the crime lords of cryptocurrency.* Doubleday.

May, T. (1988). The Crypto Anarchist Manifesto. *The Nakamoto Institute.* Retrieved May 23, 2023, from https://nakamotoinstitute.org/crypto-anarchist-manifesto/

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., & Savage, S. (2013). A fistful of bitcoins: Characterizing payments among men with no manes. *The Magazine of USENIX & SAGE, 38*(6), 10–14. https://dblp.uni-trier.de/db/journals/usenix-login/usenix-login38.html#Meiklejohn-PJLMV13

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system.* Bitcoin.com. https://bitcoin.org/bitcoin.pdf

Vora, R. (2020, September 18). *MIT & Stanford professors to create cryptocurrency, Unit-e.* CryptoNewsZ. https://www.cryptonewsz.com/mit-stanford-profs-to-develop-an-improved-cryptocurrency-than-bitcoin/