



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

**CRYPTOCURRENCY: CHANGING THE GAME
FOR STATE AND LOCAL LAW ENFORCEMENT**

by

Joseph F. Sembler Jr.

March 2023

Thesis Advisor:
Second Reader:

Kathryn J. Aten
Erik J. Dahl

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			<i>Form Approved OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC, 20503.				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE March 2023	3. REPORT TYPE AND DATES COVERED Master's thesis	
4. TITLE AND SUBTITLE CRYPTOCURRENCY: CHANGING THE GAME FOR STATE AND LOCAL LAW ENFORCEMENT			5. FUNDING NUMBERS	
6. AUTHOR(S) Joseph F. Sembler Jr.				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			10. SPONSORING / MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.			12b. DISTRIBUTION CODE A	
13. ABSTRACT (maximum 200 words) Criminals have increasingly embraced cryptocurrency, accounting for its explosion. This thesis traces cryptocurrency's growth and the government's failure to combat it and provides a guide for state and local law enforcement to identify and curb illegal cryptocurrency. It highlights cryptocurrency's key exploitable characteristics and recommends agency policies and procedures, pinpointing some drivers of organizational change to accelerate state and local law enforcement agencies' preparedness. The thesis offers cases to demonstrate how law enforcement mastered DNA analysis by creating policies and procedures, increasing knowledge, and acknowledging legal precedents. The work reveals a critical need for cryptocurrency training and education at state and local levels. Identifying cryptocurrency in criminal investigations and populating shared databases is a pressing need, so leveraging federal partnerships and educational institutions for training should advance efforts. Collaborating with private companies on cryptocurrency identification software will also change the game. In sum, sharing intelligence, performing community outreach for prevention, and reexamining cold cases through new cryptocurrency intelligence may stem these crimes.				
14. SUBJECT TERMS cryptocurrency, state and local law enforcement, technology, law enforcement training			15. NUMBER OF PAGES 127	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UU	

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. Z39-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

**CRYPTOCURRENCY: CHANGING THE GAME FOR STATE AND LOCAL
LAW ENFORCEMENT**

Joseph F. Sembler Jr.
Lieutenant, New Jersey State Police
BS, Kean University, 2003

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
March 2023**

Approved by: Kathryn J. Aten
Advisor

Erik J. Dahl
Second Reader

Erik J. Dahl
Associate Professor, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Criminals have increasingly embraced cryptocurrency, accounting for its explosion. This thesis traces cryptocurrency's growth and the government's failure to combat it and provides a guide for state and local law enforcement to identify and curb illegal cryptocurrency. It highlights cryptocurrency's key exploitable characteristics and recommends agency policies and procedures, pinpointing some drivers of organizational change to accelerate state and local law enforcement agencies' preparedness. The thesis offers cases to demonstrate how law enforcement mastered DNA analysis by creating policies and procedures, increasing knowledge, and acknowledging legal precedents. The work reveals a critical need for cryptocurrency training and education at state and local levels. Identifying cryptocurrency in criminal investigations and populating shared databases is a pressing need, so leveraging federal partnerships and educational institutions for training should advance efforts. Collaborating with private companies on cryptocurrency identification software will also change the game. In sum, sharing intelligence, performing community outreach for prevention, and reexamining cold cases through new cryptocurrency intelligence may stem these crimes.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
A.	RESEARCH QUESTION	4
B.	LITERATURE REVIEW	4
	1. Technology, Crime, and Law Enforcement.....	5
	2. Technology Adoption and Organizational Change in Law Enforcement	7
	3. Gap Analysis.....	10
	4. Conclusion	10
C.	RESEARCH DESIGN	11
D.	CONTRIBUTION.....	12
II.	KEY CHARACTERISTICS OF CRYPTOCURRENCY.....	13
A.	NATURE OF CRYPTOCURRENCY	13
	1. Blockchain Technology.....	13
	2. Cryptocurrency Wallets	17
	3. Creation of Cryptocurrency.....	21
	4. Cryptocurrency Mining.....	23
B.	LEGITIMATE USES OF CRYPTOCURRENCIES	25
C.	CRYPTOCURRENCY ON THE DARK WEB AND THE TOR NETWORK	28
D.	CRYPTOCURRENCY COUPLED WITH ENCRYPTED MESSAGING SOFTWARE AND APPLICATIONS	32
E.	CONCLUSION	33
III.	CRYPTOCURRENCY CRIMES AND POLICY RESPONSES	35
A.	CRIMES AND POLICY RESPONSES	35
B.	CRYPTOCURRENCY’S USE IN TRADITIONAL CRIMES	38
C.	DARK WEB AND TOR BROWSING CRIMES.....	38
D.	DENIAL OF SERVICE, RANSOMWARE, AND CRIMES COMMITTED WITH CRYPTOCURRENCY	39
E.	NATION-STATE HACKING, TERRORISM AND APPLICATION TO CRYPTOCURRENCY	44
F.	DOMESTIC INSIDER-THREAT HACKING CASES INVOLVING CRYPTOCURRENCY AND THE DARK WEB.....	46
G.	CONCLUSION	50
IV.	DNA CASE ANALYSIS	51
A.	INTRODUCTION TO DNA	51

B.	DNA ANALYSIS.....	53
C.	TIMELINE	54
D.	CONCLUSION	60
V.	GAP ANALYSIS.....	63
A.	DESIRED STATE.....	64
1.	Knowledge Needed.....	65
2.	Organizational Policies.....	68
B.	CURRENT STATE.....	69
1.	Law Enforcement’s Current Knowledge, Training, and Education	69
2.	Law Enforcement Organization	71
C.	RESULTS AND FINDINGS	72
VI.	CHANGING LAW ENFORCEMENT ORGANIZATIONS TO COUNTER CRYPTOCURRENCY CRIME	75
A.	ISSUE SELLING	75
B.	SOCIAL IDENTITY THEORY	77
C.	DISCUSSION, RECOMMENDATIONS, AND CONCLUSION	78
1.	Agency Investment in New Cryptocurrency Identification Technologies	79
2.	Training Law Enforcement on U.S. Regulations for Traditional Financial Crimes.....	80
3.	Leveraging Federal Partnerships and the Educational Sector in Law Enforcement Training	83
4.	Developing a Standard Policy and Procedure for Encountering and Seizing Illegal Cryptocurrency	88
5.	Community Outreach on Cryptocurrency and Crimes	89
6.	Re-examining Historical Investigations for Cryptocurrency Intelligence and Information-Sharing.....	90
D.	CONCLUSION AND FUTURE RESEARCH	90
	LIST OF REFERENCES.....	93
	INITIAL DISTRIBUTION LIST	105

LIST OF FIGURES

Figure 1.	How a Transaction Gets into the Blockchain.	14
Figure 2.	Blockchain versus Database.	16
Figure 3.	Five Simple Ways to Store Private Keys.....	20
Figure 4.	How Bitcoin Is Minted.....	24
Figure 5.	Depiction of the Tor Network.....	31
Figure 6.	Ransomware Infographic.	41
Figure 7.	Average Prices of Cybercrime Services for Sale in 2021.....	43
Figure 8.	GRU Hackers Wanted by the FBI.	45
Figure 9.	DNA Structure	52
Figure 10.	DNA Timeline	60
Figure 11.	Process for Cataloging Digital Evidence.	65
Figure 12.	Coinbase on the Apple App Store.....	82
Figure 13.	Mobile Wallet Examples.....	87

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1.	DNA Analysis.....	61
Table 2.	Comparative Analysis: DNA versus Cryptocurrency.....	73
Table 3.	Policy Example: Seizure of Cryptocurrency.....	88

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

CCU	Cyber Crimes Unit
CPU	central processing unit
DoS	denial of service
FDIC	Federal Deposit Insurance Corporation
FinCEN	Financial Crimes Enforcement Network
IC3	Internet Crime Complaint Center
IP	internet protocol
IPv4	internet protocol version 4
IPv6	internet protocol version 6
NDIS	National DNA Index System
NJSP	New Jersey State Police
PCR	polymerase chain reaction
PERF	Police Executive Research Forum
RCMP	Royal Canadian Mounted Police
SAR	Suspicious Activity Reports (Initiative)
SEC	Securities and Exchange Committee
SIT	social identity theory
VPN	virtual private network

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

Cryptocurrency is becoming more popular among criminals, and research on cryptocurrency has concluded that this rapidly evolving technology forms a significant part of the financial landscape.¹ Although cryptocurrency appears to be a key element of many cybercrimes, criminals increasingly use it in traditional crimes because they can convert it into conventional money. This evolution has given rise to cryptocurrency crime and pressured state and local law enforcement to identify and understand how to solve such offenses. This thesis shows that cryptocurrency is growing in popularity, but the U.S. government is not inhibiting its use in American commerce.

This thesis identifies cryptocurrency's key characteristics or affordances and the ways in which criminals—including enemies of the United States, terrorists, transnational criminal groups, nation-state hackers, and domestic criminals—exploit them. Regarding law enforcement, this thesis provides guidance for state and local law enforcement in recognizing illegal cryptocurrency and formulating policies and procedures, as well as offers recommendations for what to do when it is encountered in a crime. It also identifies some drivers for organizational change, such as social identity and issue selling, to better prepare agencies for responding to and investigating cryptocurrency.

This thesis analyzes cases of another emerging technology, DNA analysis, to examine how law enforcement responded and adapted to it by creating policies and procedures, increasing knowledge, partnering with the educational and private sector, and acknowledging legal precedents. DNA analysis technology has moved from its infancy just 35 years ago to an integral role in securing convictions and exonerations in major crimes today.² Analyzing how law enforcement adapted to an evolving technology can inform recommendations for adapting and investigating crimes involving cryptocurrency.

¹ Eva Su, *Digital Assets and SEC Regulation*, CRS Report No. R46208 (Washington, DC: Congressional Research Service, 2021), <https://www.hsdl.org/?abstract&did=855875>.

² Celia Henry Arnaud, "Thirty Years of DNA Forensics: How DNA Has Revolutionized Criminal Investigations," *Chemical & Engineering News*, September 18, 2017, <https://cen.acs.org/analytical-chemistry/Thirty-years-DNA-forensics-DNA/95/i37>.

This thesis outlines most questions decision-makers might have when trying to enhance an agency's capabilities in dealing with cryptocurrency. Several resources can enable state and local law enforcement's solutions in this complex criminal landscape. Adopting education and training programs in cryptocurrency for state and local governments is critical as is identifying cryptocurrency information in criminal investigations and populating intelligence-sharing databases with it.³ With cryptocurrency and associated crimes increasing, state and local governments need to engage and create new policies where they do not exist.⁴ This thesis recommends the following measures for law enforcement:

- Developing a fundamental understanding of traditional financial crimes,
- Leveraging federal partnerships and educational institutions to provide training,
- Collaborating with private companies on available cryptocurrency identification software to “change the game,”
- Sharing more cryptocurrency-related criminal intelligence,
- Performing community outreach to prevent crimes involving cryptocurrency,
- Re-examining technology-related cold cases that are potentially solvable through new cryptocurrency intelligence, and
- Creating new policies and procedures to investigate cybercrimes effectively.

³ Police Executive Research Forum, *New National Commitment Required: The Changing Nature of Crime and Criminal Investigations* (Washington, DC: Police Executive Research Forum, 2018), <https://www.policeforum.org/assets/ChangingNatureofCrime.pdf>.

⁴ Eric Rosner, “Cyber Federalism: Defining Cyber’s Jurisdictional Boundaries” (master’s thesis, Naval Postgraduate School, 2017), <https://calhoun.nps.edu/handle/10945/56794>.

As Eric Rosner identified in his Naval Postgraduate School thesis, the federal government can no longer be solely responsible for investigating all technology-enabled crimes.⁵ State and local law enforcement agencies in the United States need to equip their organizations to respond to and investigate crimes involving such evolving technologies as cryptocurrency.⁶ This effort will require a complete understanding of how cryptocurrency connects to crime. Then, departments can design education and training for law enforcement that supports organizational policies and procedures.

⁵ Rosner.

⁶ Police Executive Research Forum, *New National Commitment Required*.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

It has been a tremendous honor to be accepted and participate in the CHDS master's program at the Naval Postgraduate School. This program has considerably changed how I think about public safety. The academic standards and commitment have been strenuous and demanded much sacrifice of personal and professional time. The experiences have been captivating from beginning to end. While there are so many to thank for this incredible opportunity, I would like to address the following people.

Above all, I would like to express my sincere gratitude to the New Jersey State Police (NJSP), who identified and recommended me for this program and supported me throughout this time. Lieutenant Colonel (LTC) Scott Ebner (Ret.), a graduate of the Executive Leaders Program at CHDS, presented the opportunity and believed in me. He gave me the confidence to apply and the perseverance to stick with it. LTC Ray Guidetti (Ret.), a CHDS master's program graduate, voiced his strong support and encouragement, along with Major Richard Laverty (Ret.), another CHDS Executive Leaders Program graduate. LTC Fritz Fragé (Ret.) recognized the program's importance and strongly supported this endeavor from the beginning while I was assigned to his office. I also express my sincere gratitude to NJSP Superintendent, Colonel Patrick Callahan. This would not have been possible without your support and commitment to excellence. I would not be where I am professionally if not for the leadership and guidance of these NJSP commanders. You should all know that I will continue to serve the division to the best of my abilities and represent our "outfit" in ways that make you all proud. Thank you all for your leadership.

To the staff of CHDS, you made this an incredible experience. Your commitment to public safety is just remarkable. I am so humbled to have learned from each of you. To my thesis advisors, Dr. Kathryn Aten and Dr. Erik Dahl, you took my ideas and provided me with the wisdom and guidance I needed to learn and explore how to organize them to make the world a little safer. I am forever grateful for your insight and management. To CHDS graduate writing coach Marianne Taflinger, I will continually use the tools and guidance that you offered me to be a more accomplished and confident writer. I am forever

thankful to have met you along the way. To the 2105/2106 CHDS cohort, you are an incredible group of devout public safety specialists. I enjoyed our time together and the ideas we shared inside and outside the classroom. I wish you all the best of luck in whatever comes next for you.

Finally, and most significantly, to my wife, Teresa, thank you for your incredible support during this program and our last 20 years together. I would not be anywhere, personally or professionally, if not for your unconditional love and commitment to our family and me. You are the most incredible person I have ever met. I consider spending our life together my greatest accomplishment. To our children, Andrew and Evelyn, should you ever read this one day, your mother and I often express to you the importance of education if you want to make a difference in the world. I hope you will one day find someone as special as your mother and a place as special as the Naval Postgraduate School. Both have truly changed my life.

I. INTRODUCTION

Many state and local law enforcement agencies in the United States lack the necessary knowledge to investigate cryptocurrency that has been employed in crimes.¹ According to Chainalysis in its *2022 Crypto Crime Report*, crimes involving cryptocurrency hit an all-time high of \$14 billion in 2022, and cryptocurrency transactions increased 567 percent to \$15.8 trillion.² Although cryptocurrency appears to be a key element of many cybercrimes, criminals also increasingly use it in traditional crimes because they can convert it into conventional money. State and local law enforcement experts first identified the law enforcement education gap in 2018 when approximately 200 law enforcement professionals from around the nation gathered to discuss technology-enabled crimes, including those involving cryptocurrency.³ They concluded that addressing rising rates of technology-enabled crime requires law enforcement to adapt to evolving technologies.⁴ In this way, law enforcement training needs to address the gaps identified.

Not surprisingly, cybercriminals use cryptocurrency more often than fiat currency to commit crimes. According to the Federal Bureau of Investigation's Internet Crime Complaint Center (IC3), Americans reported over 350,000 cybercrimes in 2018.⁵ In addition, IC3's 2016 annual report estimated that 85 percent of victims failed to report crimes.⁶ In 2020, the center received a staggering 791,790 complaints from American

¹ Police Executive Research Forum, *New National Commitment Required: The Changing Nature of Crime and Criminal Investigations* (Washington, DC: Police Executive Research Forum, 2018), <https://www.policeforum.org/assets/ChangingNatureofCrime.pdf>.

² Chainalysis, *The 2022 Crypto Crime Report* (Chainalysis, 2022), <https://www.chainalysis.com/>; Mengqi Sun and David Smagalla, "Cryptocurrency-Based Crime Hit a Record \$14 Billion in 2021," *Wall Street Journal*, January 6, 2022, <https://www.wsj.com/articles/cryptocurrency-based-crime-hit-a-record-14-billion-in-2021-11641500073>.

³ Police Executive Research Forum, *New National Commitment Required*.

⁴ Police Executive Research Forum.

⁵ Federal Bureau of Investigation, *2018 Internet Crime Report* (Washington, DC: Federal Bureau of Investigation, 2019), 3, https://www.ic3.gov/Media/PDF/AnnualReport/2018_IC3Report.pdf.

⁶ Federal Bureau of Investigation, *2016 Internet Crime Report* (Washington, DC: Federal Bureau of Investigation, 2017), 3, https://www.ic3.gov/Media/PDF/AnnualReport/2016_IC3Report.pdf.

consumers, representing a 69 percent increase over the previous year and more than \$4.1 billion in losses.⁷ Notably, 2020 also saw an uptick in complaints related to the conversion of funds to cryptocurrency.⁸ For example, due to cryptocurrency's ability to move funds swiftly across borders, criminals use it in romance scams, ransomware attacks, and various fraud schemes. Thus, cryptocurrency has become inextricably linked to cybercrimes of many types.

The proliferation of Bitcoin ATMs also increases opportunities to commit cryptocurrency crimes.⁹ The New Jersey State Commission of Investigation identified over 11,000 Bitcoin ATMs operating within the United States.¹⁰ Their placement and operation help to fuel the cryptocurrency phenomenon for investors and can contribute to some of the crimes reported to state and local law enforcement. For example, the New Jersey State Commission of Investigation found that in 2017, a New Jersey resident defrauded victims of over \$600,000 nationally through the website eBay using only one Bitcoin ATM in northern New Jersey.¹¹ In this way, the prevalence of ATMs creates a major vulnerability for cryptocurrency crimes.

Likewise, the absence of specific police training on cryptocurrency creates an unprepared police force. Despite professionals' recognition that law enforcement must adapt to evolving technologies, police training nationally focuses on the initial training required to become a police officer rather than continuing education to meet a changing technology landscape.¹² According to Blumberg et al. in their article for the *International*

⁷ Federal Bureau of Investigation, *2020 Internet Crime Report* (Washington, DC: Federal Bureau of Investigation, 2021), 3, https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf.

⁸ Federal Bureau of Investigation, 10.

⁹ A Bitcoin ATM is a machine placed in a physical location that exchanges fiat currency for virtual currency.

¹⁰ New Jersey State Commission of Investigation, *Bitcoin ATMs: Scams, Suspicious Transactions and Questionable Practices at Cryptocurrency Kiosks* (Trenton, NJ: New Jersey Commission of Investigation, 2021), 2, <https://www.state.nj.us/sci/pdf/Bitcoin%20Report.pdf>.

¹¹ New Jersey State Commission of Investigation, 10.

¹² Police Executive Research Forum, *New National Commitment Required*; Alana Semuels, "Society Is Paying the Price for America's Outdated Police Training Methods," *Time*, November 20, 2020, <https://time.com/5901726/police-training-academies/>.

Journal of Environmental Research and Public Health, most police training fits into the following categories: operations, firearms, self-defense, use of force, self-improvement, legal education, and mental illness.¹³ No training or education addresses technology or cryptocurrency to prepare officers to investigate such crimes, leaving police without the tools to combat these crimes.

Nonetheless, law enforcement can successfully investigate cryptocurrency-related crimes. For example, on November 5, 2020, the Department of Justice seized and applied for forfeiture of over \$1 billion in Bitcoin following its dark web investigation into the Silk Road on the Tor network.¹⁴ This seizure represented the largest seizure of cryptocurrency in world history.¹⁵ The Silk Road investigation was the most significant investigation into illegal activities on the dark web, and the website's founder, Ross Ulbricht—a now 37-year-old American—received a 40-year sentence. Acknowledging the changing nature of these crimes, the Motorola Solutions Foundation has concluded that state and local law enforcement should understand the severity of the issue and endeavor to reduce rising crimes involving cryptocurrency.¹⁶ More extensive knowledge of how cryptocurrency connects to crime might motivate police officers to devote more attention to such activities.

Cryptocurrency and associated crimes are increasing, but law enforcement's efforts do not match the threat. As Eric Rosner identified in his Naval Postgraduate School thesis, the federal government can no longer be solely responsible for investigating all technology-enabled crimes.¹⁷ For its part, state and local governments need to engage and create new policies where they do not exist.¹⁸ They must also equip their organizations with the

¹³ Daniel M. Blumberg et al., "New Directions in Police Academy Training: A Call to Action," *International Journal of Environmental Research and Public Health* 16, no. 24 (2019): 2, <https://doi.org/10.3390/ijerph16244941>.

¹⁴ "United States Files a Civil Action to Forfeit Cryptocurrency Valued at Over One Billion U.S. Dollars," U.S. Attorney's Office, Northern District of California, November 5, 2020, <https://www.justice.gov/usao-ndca/pr/united-states-files-civil-action-forfeit-cryptocurrency-valued-over-one-billion-us>.

¹⁵ U.S. Attorney's Office, Northern District of California.

¹⁶ Police Executive Research Forum, *New National Commitment Required*.

¹⁷ Eric Rosner, "Cyber Federalism: Defining Cyber's Jurisdictional Boundaries" (master's thesis, Naval Postgraduate School, 2017), <https://calhoun.nps.edu/handle/10945/56794>.

¹⁸ Rosner.

knowledge to respond to and investigate crimes involving emerging technologies such as cryptocurrency.¹⁹ This effort will require a complete understanding of how cryptocurrency connects to crime.

A. RESEARCH QUESTION

This thesis advances state and local law enforcement's understanding of cryptocurrency by identifying and closing the current knowledge gap. It addresses the following overarching and ancillary questions:

1. What are cryptocurrency's key characteristics or affordances, and how do criminals exploit them?
2. What policies and procedures would help prepare state and local law enforcement agencies to respond to and investigate cryptocurrency crimes?
3. What drivers to organizational change would better prepare state and local law enforcement agencies to respond to and investigate cryptocurrency? What barriers would need to be overcome?

B. LITERATURE REVIEW

Research on cryptocurrency concludes that it is a rapidly evolving technology that has become a significant part of the financial landscape.²⁰ Cryptocurrency is becoming more popular among criminals, and nefarious use is increasing.²¹ This increase in cryptocurrency crime places a demand on law enforcement to identify and understand how to solve these crimes. Scholars and practitioners overwhelmingly agree that evolving technologies can be important drivers of trends in crime and suggest that solutions need to

¹⁹ Police Executive Research Forum, *New National Commitment Required*.

²⁰ Eva Su, *Digital Assets and SEC Regulation*, CRS Report No. R46208 (Washington, DC: Congressional Research Service, 2021), <https://www.hsdl.org/?abstract&did=855875>.

²¹ Financial Crimes Enforcement Network, *Anti-Money Laundering and Countering the Financing of Terrorism National Priorities* (Washington, DC: Department of the Treasury, 2021), <https://www.hsdl.org/?abstract&did=856103>.

be responsive to technology.²² Research suggests that adapting to evolving technologies requires understanding the technology and, often, implementing organizational change, which is difficult for law enforcement.²³ Existing research, however, provides little guidance regarding cryptocurrency for law enforcement. Research has not explored how law enforcement organizations can adapt to cryptocurrency crime or what policies and procedures would be required to support change.

1. Technology, Crime, and Law Enforcement

The dominant view recognizes the importance of knowledge for investigators tasked with solving evolving crimes that employ newer technologies like cryptocurrency. For example, understanding cryptocurrency is vital in crimes like computer network intrusions because these crimes remain among the top threats to the U.S. homeland security enterprise.²⁴ Exemplifying this importance, in May 2021, law enforcement was called to investigate ransomware on the Colonial Pipeline’s computer network, which led to fuel shortages on the East Coast of the United States for several days. Both criminal groups and nation-state actors perpetrated the cyberattack. As a result of the Colonial Pipeline attack, the Department of Justice seized \$2.3 million in Bitcoin from proceeds belonging to the individuals responsible for the cyberattack.²⁵ The literature indicates that cryptocurrency crimes are significant, complicated to comprehend, and challenging for police to become adept at managing.²⁶

The literature recognizes that the federal government has made considerable efforts in responding to cryptocurrency’s cyber threat by assigning responsibility to several federal agencies. One agency proactive in identifying cryptocurrency users is the U.S. Treasury’s

²² Attorney General’s Cyber Digital Task Force, *Cryptocurrency Enforcement Framework* (Washington, DC: Department of Justice, 2020), <https://www.justice.gov/cryptoreport>.

²³ Attorney General’s Cyber Digital Task Force.

²⁴ Attorney General’s Cyber Digital Task Force.

²⁵ “Department of Justice Seizes \$2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside,” Department of Justice, June 7, 2021, <https://www.justice.gov/opa/pr/departments-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside>.

²⁶ Attorney General’s Cyber Digital Task Force, *Cryptocurrency Enforcement Framework*.

Financial Crimes Enforcement Network (FinCEN), equipped with a team of cryptocurrency analysts and investigators. These skilled representatives capture cryptocurrency trading trends and investigate cryptocurrency transactions. Agencies like FinCEN provide a vital service to protect American interests. FinCEN has verified in publications that cryptocurrency is the preferred payment method in various illicit online activities.²⁷ According to research, cryptocurrency enables criminals to buy online goods, illegal drugs, child sexual abuse material, and ransomware applications and services. In conjunction with law enforcement partners, identifying and apprehending individuals responsible for using ransomware represent a top priority for the federal government.²⁸ Federal law enforcement agencies have identified cryptocurrency's potential threats and shifted some investigative efforts to increase knowledge.

Increasingly, scholars have indicated that state and local law enforcement need to do more to protect the homeland security environment and communities from technology-enabled crimes. At the state and local levels, the Police Executive Research Forum (PERF) has been a national leader in police organizational research since 1976. In 2018, the Motorola Solutions Foundation and PERF published *The Changing Nature of Crime and Criminal Investigations* after 200 state and local law enforcement experts from around the United States discussed the proliferation of technology in crimes, including those involving cryptocurrency.²⁹ The law enforcement experts involved in the 2018 study concluded that addressing rising rates of technology crime requires state and local law enforcement to radically adapt to evolving technologies.

Ryan Monaghan of the Naval Postgraduate School similarly assesses the knowledge gap between state and local law enforcement and emerging technologies in his 2020 thesis.³⁰ In addition to analyzing quantifiable data and providing extensive references

²⁷ Financial Crimes Enforcement Network, *Anti-Money Laundering*.

²⁸ Financial Crimes Enforcement Network.

²⁹ Police Executive Research Forum, *New National Commitment Required*.

³⁰ Ryan M. Monaghan, "Cybercrime Response Capabilities and Capacity: An Evaluation of Local Law Enforcement's Response to a Complex Problem" (master's thesis, Naval Postgraduate School, 2020), <https://calhoun.nps.edu/handle/10945/66690>.

from national law enforcement literature on state and local law enforcement's responses to specific crimes, the author surveyed 32 California police departments and assessed their reactions to cybercrimes. The author focused on California because data indicate it is home to the most cybercrime victims. Monaghan evaluates the potential of a state and local task force concept to combat cybercrimes effectively, finding that a hybrid task force rated as the most popular way among survey respondents to increase response capabilities. Although Monaghan's thesis set out to understand whether a task force approach could reduce cybercrimes, the material is relevant because cryptocurrency is often intimately involved in the commission of cybercrimes. The author concludes that state and local law enforcement must develop the ability to address how criminals use technology. However, the research does not offer decision-makers guidelines for preparing state and local law enforcement or developing fundamental strategies to reduce cybercrimes.

Significant literature investigates how evolving technologies like cryptocurrency threaten the homeland security environment.³¹ A subset of this literature explores whether the responsibility to investigate these types of crimes when they occur lies at the state or federal level.³² Limited research addresses how state and local law enforcement agencies should prepare police to respond to and investigate cryptocurrency crimes.

2. Technology Adoption and Organizational Change in Law Enforcement

Organizational change usually occurs in response to driving factors, awareness of a deficiency, a motivation to change, research into the issue, and next steps, such as recommendations for a new policy or procedure. Considerable research supports the conclusion that people generally resist change within their organizations. According to Pierce and Delbecq, research finds that organizational change usually occurs when things

³¹ Attorney General's Cyber Digital Task Force, *Cryptocurrency Enforcement Framework*.

³² Rosner, "Cyber Federalism."

go wrong, and an organization must create new ways of doing things.³³ However, research consistently shows that change challenges individuals and organizations.

The literature recognizes a need to adopt technology in law enforcement organizations. In her thesis on cybersecurity from Utica College, Chelsea Montgomery finds three main reasons law enforcement fails to implement organizational change to adopt technologies: a lack of awareness, a low prioritization, or an absence of technically savvy personnel.³⁴ She argues that many cybercrimes and investigations involve cryptocurrency, and law enforcement organizations themselves are often left vulnerable to cybercrimes.³⁵ Although her research focuses on the risk of police departments' becoming the target of cybercrimes, Montgomery argues that one of the top challenges facing law enforcement is the need to adapt to evolving technology.

Scholars have used the concept of organizational change in studying policing, despite some gaps. In her dissertation from Rutgers University in New Jersey, Michele-Lynne Muni argues police departments prioritize street gangs, gun violence, drugs, and violent crime prevention because these crimes are visible and a top priority in public safety when high crime rates exist.³⁶ She argues that prioritizing such crime prevention distracts organizational leaders from influencing other areas like policy creation, training, and long-term strategy.³⁷ She identifies in her research the success of Bill Bratton's introduction of CompStat meetings to the New York City Police Department in 1994. CompStat was an organizational change model that created monthly meetings for police executives to measure crime statistics and apply real-time crime trends so that decision-makers could

³³ Jon L. Pierce and André L. Delbecq, "Organization Structure, Individual Attitudes and Innovation," *Academy of Management Review* 2, no. 1 (January 1977): 27–37, <https://doi.org/10.5465/AMR.1977.4409154>.

³⁴ Chelsea Montgomery, "New Security for a New Era: An Investigation into Law Enforcement Cybersecurity Threats, Obstacles, and Community Applications" (master's thesis, Utica College, 2017), ProQuest.

³⁵ Montgomery.

³⁶ Michele-Lynne Muni, "Policing Domestic Violence: Case Study of Organizational Change in the Trenton Police Department, Trenton, New Jersey" (PhD diss., Rutgers University, 2012), <https://doi.org/10.7282/T36H4GCC>.

³⁷ Muni.

allocate resources appropriately. Police departments nationally viewed CompStat meetings as widely successful, and other police departments have modeled it in their operating procedures.³⁸ The literature shows that prioritizing organizational change to identify gaps makes law enforcement officers more effective in their jobs.

Scholars concur that current police training fails to prepare officers for emerging crimes, including cryptocurrency, because of the dominance of paramilitary training over adult learning. The literature pinpoints the current gap in knowledge of emerging technologies, including cryptocurrency, particularly in police training, which could prepare officers to respond to and investigate technology-related crimes.³⁹ In their article for the *International Journal of Environmental Research and Public Health*, Blumberg et al. indicate most police training fits into the following categories: operations, firearms, self-defense, use of force, self-improvement, legal education, and mental illness.⁴⁰ This study draws on data about police training from the Department of Justice to inform the reader of the current broader curriculum of police training from 664 state and local law enforcement academies. The scholars argue that skills taught in police academies, such as firearms, driving, and arrest procedures, decrease over time and require periodic retraining throughout a law enforcement officer's career. They also criticize the knowledge taught at police academies and the curricula prepared by police instructors nationally in that they ought to shift from a paramilitary to an adult-based learning concept.⁴¹ Although this study does not explicitly focus on technology adoption, it provides a helpful framework for what is currently being taught to police officers at the state and local levels nationally. One might conclude that current police training demonstrates a failure of imagination in preparing law enforcement investigators to respond to and investigate crimes that involve emerging technologies like cryptocurrency.

³⁸ Muni.

³⁹ Blumberg et al., "New Directions in Police Academy Training."

⁴⁰ Blumberg et al.

⁴¹ Blumberg et al.

Finally, according to Anne Kohnke, Greg Laidlaw, and Charles Wilson in their 2021 conference paper, technology-enabled crimes change constantly, and state and local law enforcement organizations have not kept pace.⁴² These scholars agree with PERF's assessment that law enforcement's ability to investigate cybercrimes at the state and local level has lagged technological advancements in crime.⁴³ They recommend performing a gap analysis in addition to creating partnerships and task forces to remedy the situation.

3. Gap Analysis

According to Langford et al. in their report for the Naval Postgraduate School,

Gap Analysis is an assessment tool that compares a system's actual performance with its potential. What you desire versus what you have is, in essence, a Gap. The gap is as much the relationship between what is perceived to be important and the derived difference between performance and expectations.⁴⁴

Richard E. Clark and Fred Estes find that organizations experience three fundamental performance gaps: knowledge, motivation, and organizational barriers.⁴⁵ Clark and Estes argue that motivation and the belief in an organization's goals can successfully change performance. In addition, they underscore the significant role organizational culture plays in increasing organizational performance. This literature provides a framework for conducting a gap analysis, which guides this research.

4. Conclusion

The existing literature shows that addressing cryptocurrency-enabled crimes will require law enforcement to adopt new technologies. This transition will require state and local law enforcement to prioritize organizational change, but such change is hard.

⁴² Anne Kohnke, Greg Laidlaw, and Charles Wilson, "Challenges in Bridging the Law Enforcement Capability Gap," in *International Conference on Cyber Warfare and Security* (Reading, UK: Academic Conferences International, 2021), 521–26, <https://doi.org/10.34190/IWS.21.013>.

⁴³ Kohnke, Laidlaw, and Wilson.

⁴⁴ Gary Langford et al., *Gap Analysis: Rethinking the Conceptual Foundations*, NPS-AM-07-051 (Monterey, CA: Naval Postgraduate School, 2007), 1, <https://dair.nps.edu/handle/123456789/2815>.

⁴⁵ Richard E. Clark, *Turning Research into Results: A Guide to Selecting the Right Performance Solutions* (Charlotte, NC: Information Age Publishing, 2008).

Although the literature suggests that such a transition requires knowledge, motivation, and policy changes, it remains unclear how state and local law enforcement agencies can prepare and organize to respond to and investigate cryptocurrency crimes. The possible solution to these issues may require organizational change at the state and local levels. Much scholarly literature confirms this problem exists, but none of it addresses the root causes nor the next steps for addressing it. This thesis represents further research into the literature, focusing on key characteristics of cryptocurrency, cases involving cryptocurrency, and DNA analysis to synthesize and assess how law enforcement previously responded to another emerging technology to solve crimes. It also offers an analytical review and case analysis to support the policy changes recommended in prescriptive research.

C. RESEARCH DESIGN

This prescriptive thesis encompassed three phases to answer the three research questions and provide solutions. The first phase of the research integrated existing literature on cryptocurrency. This systematic review characterized cryptocurrency and analyzed how cryptocurrency links to crimes.

The second phase of the research analyzed how law enforcement responded and adapted to another emerging technology, DNA analysis, by creating policies and procedures, increasing knowledge, and acknowledging legal precedents. DNA analysis technology has moved from its infancy just 35 years ago to an integral role in securing convictions and exonerations in major crimes today.⁴⁶ A case exploration is a qualitative research method focusing on a particular event or topic.⁴⁷ Such an exploration could be most helpful in comparing DNA analysis to cryptocurrency, as it assists in supporting

⁴⁶ Celia Henry Arnaud, “Thirty Years of DNA Forensics: How DNA Has Revolutionized Criminal Investigations,” *Chemical & Engineering News*, September 18, 2017, <https://cen.acs.org/analytical-chemistry/Thirty-years-DNA-forensics-DNA/95/i37>.

⁴⁷ John Gerring, “What Is a Case Study and What Is It Good For?,” *American Political Science Review* 98, no. 2 (May 2004): 341–54, <https://doi.org/10.1017/S0003055404001182>.

policy changes recommended in prescriptive research.⁴⁸ I identified the approaches law enforcement used to adapt to DNA technology, the outcomes of the approaches, and the driving and resisting forces that influenced law enforcement's response to the technology. Analyzing how law enforcement adapted to an evolving technology informed recommendations for its adapting to and investigating crimes involving cryptocurrency.

The final phase of this research integrated the analytical review and case analysis. I distilled policy and procedural recommendations regarding cryptocurrency for state and local law enforcement and identified barriers and levers to change. This study aimed to inspire and provide tools for policy change at leadership levels and lead to an increased awareness and motivation among front-line investigators. Organizational changes, cultural shifts, and training and practical tools will be necessary for state and local law enforcement to become adequate investigators of cryptocurrency crimes.

D. CONTRIBUTION

This thesis contributes significant knowledge to state and local law enforcement on the nature of cryptocurrency and its links to crime by identifying and closing the knowledge gap. This thesis also aims to prepare law enforcement to investigate cryptocurrency-related crimes. The ultimate contribution of this research is to provide tips and tools to state and local law enforcement to build agencies' capabilities in making citizens safer. Augmenting their capabilities enables agencies to identify criminals, exonerate the innocent, protect communities, and increase the competencies of the U.S. homeland security environment. Finally, if state and local law enforcement can become more proficient in cryptocurrency management during investigations, information- and intelligence-sharing with federal partners will naturally improve.

⁴⁸ Pamela Baxter and Susan Jack, "Qualitative Case Study Methodology: Study Design and Implementation for Novice Researchers," *Qualitative Report* 13, no. 4 (December 2008): 544–58, <https://doi.org/10.46743/2160-3715/2008.1573>.

II. KEY CHARACTERISTICS OF CRYPTOCURRENCY

This chapter discusses the key characteristics or affordances of cryptocurrency and describes how cybercriminals employ them in crimes. This exploration of cryptocurrency aims to highlight the characteristics that make it attractive to criminals, including its anonymity, its ease in crossing nation's borders, its defense against hacking, and its concealability. This chapter also discusses cryptocurrency's origins and legitimate uses to provide the reader with a thorough understanding of its mainstream application, thereby illustrating the implications of these traits.

A. NATURE OF CRYPTOCURRENCY

State and local law enforcement should understand the fundamentals of cryptocurrency. With this decentralized digital product, consumers may purchase items where fiat currency (i.e., government-issued paper money and coinage) is traditionally accepted as payment for goods and services.⁴⁹ As a digital alternative to the traditional banking structure, it cannot be physically handled and is valuable only to the extent its community of users determines its worth.⁵⁰ The value of any cryptocurrency can change radically in a day, given the thousands of different variations in circulation.⁵¹ In short, it is a peer-to-peer electronic and cashless payment transaction system. Cryptocurrency depends on blockchain technology, but that was not the original purpose of the latter.

1. Blockchain Technology

Understanding blockchain technology is vital to building the knowledge of cryptocurrency for law enforcement. This section shows the need to grasp the criminality associated with its creation. It could be challenging to understand the bigger picture until someone understands how blockchain technology works.

⁴⁹ Attorney General's Cyber Digital Task Force, *Cryptocurrency Enforcement Framework*.

⁵⁰ Ryan L. Frebowitz, "Cryptocurrency and State Sovereignty" (master's thesis, Naval Postgraduate School, 2018), <https://calhoun.nps.edu/handle/10945/59663>.

⁵¹ Attorney General's Cyber Digital Task Force, *Cryptocurrency Enforcement Framework*.

Security concerns over the vulnerability of digital records to hacking inspired the creation of blockchain technology. Rudimentary blockchain technology attempted to address the vulnerabilities of digital records, specifically the accuracy and modifiability of those records from outside sources, as record-keeping shifted from physical documents (e.g., paper files) to a digital platform.⁵² The cryptocurrency Bitcoin’s public launch in 2008 was the first widely recognized use of blockchain technology.⁵³ When a transaction is requested, all participants in the network (nodes) receive the block. The participants and nodes—individual computers in a network—independently validate the transaction and transmit an update to all the other nodes and add a block to the chain. This update is distributed to the nodes, creating a “ledger” that no one can modify. The nodes receive an authorization notice for processing the transaction (see Figure 1).

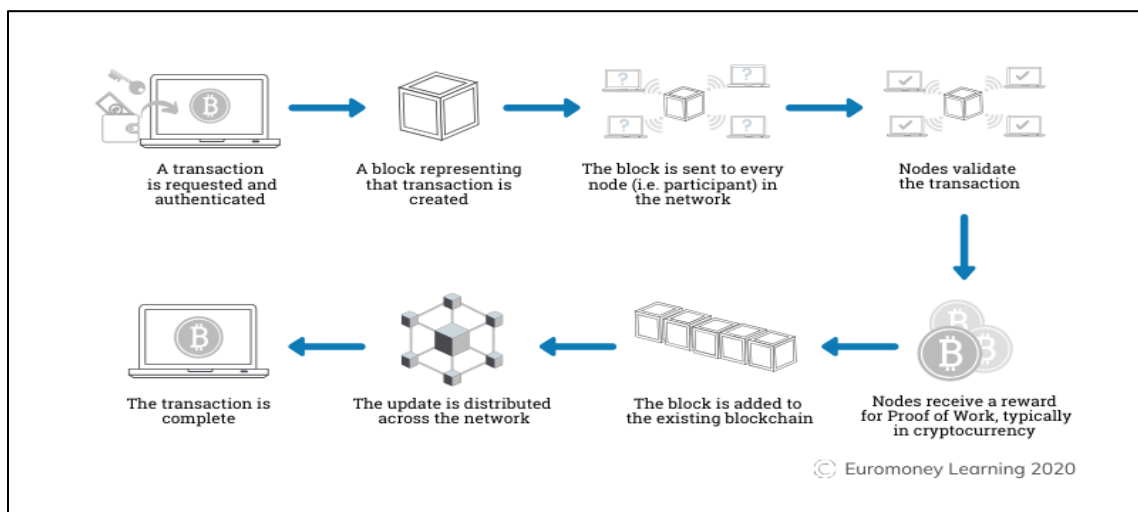


Figure 1. How a Transaction Gets into the Blockchain.⁵⁴

⁵² Buck Endemann et al., *Blockchain*, ed. Amritha Jayanti and Bogdan Bele (Cambridge, MA: Harvard Kennedy School, Belfer Center for Science and International Affairs, 2020), <https://www.belfercenter.org/sites/default/files/files/publication/Blockchain.pdf>.

⁵³ Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” Bitcoin Project, 2009, <https://bitcoin.org/bitcoin.pdf>.

⁵⁴ Source: “How Does a Transaction Get into the Blockchain?,” Euromoney Learning, accessed October 5, 2021, <https://www.euromoney.com/learning/blockchain-explained/how-transactions-get-into-the-blockchain>.

Blockchains offer advantages over traditional database storage that can be useful in developing certain emerging technologies.⁵⁵ Blockchains come in wide varieties and generally share similar features. Two of these features appeal particularly to blockchain users: decentralized data storage, which contains a public ledger of all associated transaction records, and data encryption, which is ever-present.⁵⁶ Decentralized data storage means that information is stored across many different computers instead of in one place. Blockchains store encrypted data across peer-to-peer networks (i.e., many different computers as opposed to a single computer server), linking sequential “blocks” of information into “chains.”⁵⁷ The data are available to all the network participants on a shared ledger, capturing all transactions within the blockchain, and the individual user is unknown. Computer algorithms ensure that the information is consistent and accurate across all the devices on a peer-to-peer network. Individual users cannot add to the blockchain ledger without authorization from the network. This process makes “hacking” the blockchain very difficult because verification from other computers on the peer-to-peer network must also match. An impressive benefit of blockchain technology is that changing or removing any information compromises the integrity of the decentralized ledger.⁵⁸ Figure 2 compares the characteristics of blockchain technology to traditional databases.

⁵⁵ Endemann et al., *Blockchain*.

⁵⁶ Endemann et al.

⁵⁷ Endemann et al.

⁵⁸ Endemann et al.

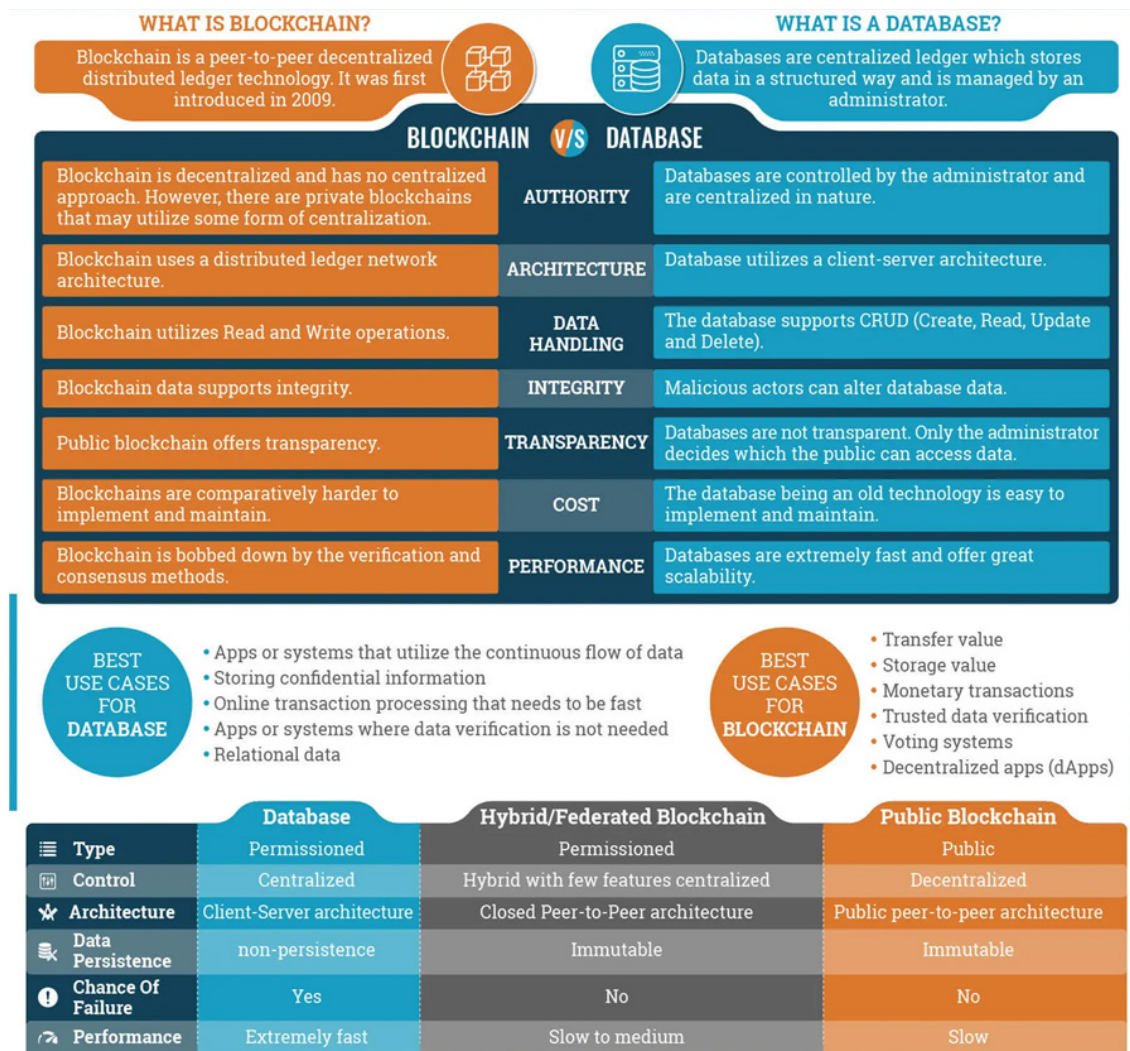


Figure 2. Blockchain versus Database.⁵⁹

In summary, several key features of blockchain technology appeal to criminals. Its encryption makes it nearly impossible for law enforcement to track crimes in process. Likewise, it is also virtually unhackable, allowing individuals to conceal and store funds obtained illegally. Although blockchain was intended to solve issues with digital records, it easily lends itself to nefarious purposes.

⁵⁹ Source: Gwyneth Iredale, "Blockchain vs. Database: Understanding the Difference," 101 Blockchains, July 30, 2021, <https://101blockchains.com/blockchain-vs-database-the-difference/>.

Someone interested in trading cryptocurrency may use the associated software to become a user on a blockchain. Cryptocurrency software generates the necessary data to include someone in a blockchain, so once users create blocks and are effectively in the chain, they can remain anonymous until they exchange the virtual currency for fiat currency.⁶⁰ This distinction is important because users can repeatedly deposit cryptocurrency units into their respective blocks; however, identification remains nearly impossible if the users do not exchange crypto for fiat currency. The ability to stay anonymous while dealing with money attached to crime is another feature of cryptocurrency that appeals to those using it for nefarious purposes.

2. Cryptocurrency Wallets

Law enforcement must understand what a cryptocurrency wallet is, where it may find one, and how to analyze the information because it may affect an investigation. As discussed in this subsection, cryptocurrency information may be stored and accessed in different ways, and untrained investigators might not know what they are looking at. This subsection provides an overview of cryptocurrency wallets, including a visual representation, to recognize them during investigations.

To access, store, and buy or sell cryptocurrency, users have both a public and a private key to decrypt their block in the chain. Computer algorithms create public–private key pairs that cannot be reverse-engineered, meaning that one cannot derive the private key by knowing the public key.⁶¹ The private key is always kept confidential, and only the public key is shared with others. The public key is the only portion of data publicly identified and accessible to other users within the blockchain. Only when blockchain users own both the public and private keys can their respective blocks have value added or subtracted. Following a transaction, the blockchain ledger records the trade and publicizes

⁶⁰ Euromoney Learning, “How Does a Transaction Get into the Blockchain?”

⁶¹ Bailey Reutzell, “What Is Cryptocurrency? Here’s What You Need to Know about Blockchain, Coins and More,” CNBC, September 22, 2021, <https://www.cnbc.com/select/what-is-cryptocurrency/>.

it to everyone in the blockchain community.⁶² Possessing both the public and private keys means having complete control of the account.

In Bitcoin, a private key is a 256-bit number in hexadecimal numbering (i.e., 64 characters in the range 0–9 and A–F) that resembles the following:

```
A0FD23B457A0FD23B457A0FD23B457A0FD23B457A0FD23B457A0
FD23B4571234
```

A public key in Bitcoin usually comprises 26–35 characters and resembles the following:

```
1CQdEut2E4YmXm53Qt614NbrhBvuCoyxQc
```

Once someone identifies a public key, the public address can be verified on the blockchain. Public addresses can also be researched to determine the account’s value and identify transactions. Websites such as <https://www.blockchain.com/> are an excellent place to start exploring a particular blockchain.

If a cryptocurrency owner loses his private key, he cannot access his cryptocurrency shares. Such systems lack an “I forgot my password” button. Several anecdotes have circulated on the internet about individuals who have lost their private keys to their cryptocurrency fortunes. In January 2021, for example,

Stefan Thomas, a German-born programmer living in San Francisco, [had] two guesses left to figure out a password that is worth . . . about \$220 million. The password will let him unlock a small hard drive, known as an IronKey, which contains the private keys to a digital wallet that holds 7,002 Bitcoin. . . . The problem is that Mr. Thomas years ago lost the paper where he wrote down the password for his IronKey, which gives users 10 guesses before it seizes up and encrypts its contents forever. He has since tried eight of his most commonly used password formulations—to no avail.⁶³

Interestingly, if senders enter a public key incorrectly, they also could transmit cryptocurrency accidentally to an unintended receiver. The senders will lose their money

⁶² Endemann et al., *Blockchain*.

⁶³ Nathaniel Popper, “Lost Passwords Lock Millionaires Out of Their Bitcoin Fortunes,” *New York Times*, January 14, 2021, <https://www.nytimes.com/2021/01/12/technology/bitcoin-passwords-wallets-fortunes.html>.

if it is not voluntarily returned.⁶⁴ Thus, the accuracy of the system demands proper input from its users.

Private keys demonstrate ownership in cryptocurrency and can be stored in several forms, referred to as crypto wallets, as shown in Figure 3. The first is a paper wallet, an actual piece of paper containing the cryptocurrency user's private key information. Also, someone could create and write down a passphrase called a seed, which translates into a private key. Second, software, such as an application on a smartphone, could house private keys and link them with visible QR codes for easy transactions.⁶⁵ Third, a dedicated USB drive or other storage device might form a hardware wallet for a private key. Fourth, users could memorize their private keys if they are smart enough to retain the vast information. Fifth, a web program could be used to store a private key for a user within its servers.

⁶⁴ "I Sent Funds to the Wrong Address. How Do I Get Them Back?," Coinbase, November 12, 2021, <https://help.coinbase.com/en/coinbase/trading-and-funding/sending-or-receiving-cryptocurrency/i-sent-funds-to-the-wrong-address-how-do-i-get-them-back.html>.

⁶⁵ A QR code is a visible label whose data can be read and interpreted by a computer or device.

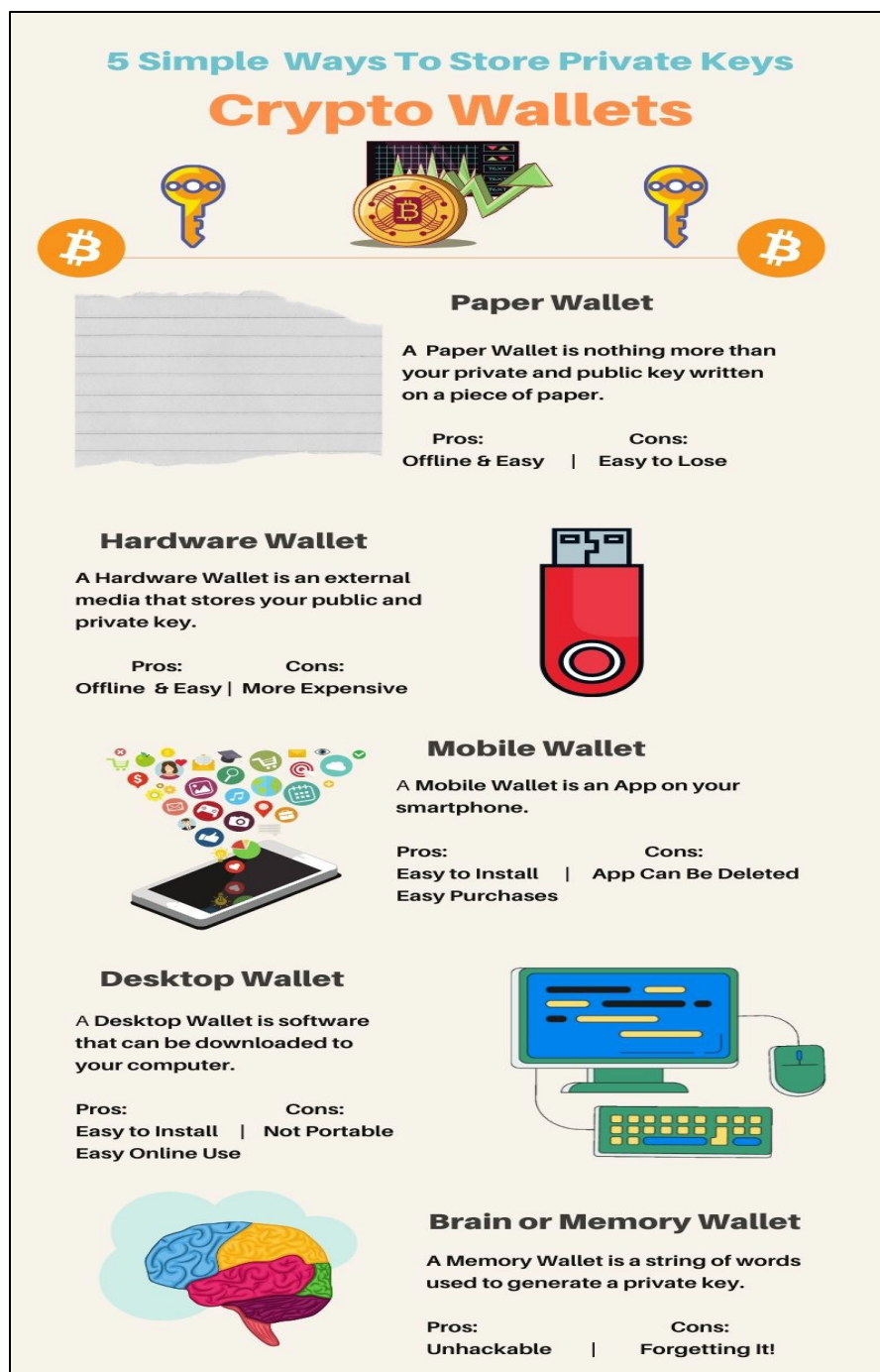


Figure 3. Five Simple Ways to Store Private Keys

In summary, understanding cryptocurrency wallets is important because if an investigator identifies a piece of paper with the aforementioned letters and numbers during an investigation, he could recognize it as a key. Similarly, knowing that a cryptocurrency

peripheral could be identified as digital evidence is significant if a mobile device or computer is seized during an investigation.

3. Creation of Cryptocurrency

Toward answering the research question of cryptocurrency's key characteristics or affordances, this subsection explores why it is attractive to certain people. Cryptocurrency purposefully eliminates and decreases the influence of centralized banks, saves the consumer banking fees associated with financial transactions generally, and eliminates foreign exchange fees.⁶⁶ When an individual in one part of the world sells something to an individual elsewhere, the acknowledged terms of the deal do not adjust to the valuation of the respective countries' domestic centralized currency. This unchanging value makes its application ideal on the internet.⁶⁷

Following the financial crisis in 2008, which some have described as the most significant economic recession since the Great Depression in 1929, the first cryptocurrency, Bitcoin, emerged as an alternative to the banking system because of a lack of confidence in banks.⁶⁸ Bitcoin was the first cryptocurrency and remains the most popular. The basic premise is that it can be traded from individual to individual without using a banking institution or "middle man." Any person involved in the blockchain of the cryptocurrency can identify any transaction. Thus, every transaction is stored indefinitely in the cryptocurrency's ledger and is available for identification within the entire blockchain community.⁶⁹

Certain privacy advocates are interested in using cryptocurrency as an alternative to the traditional banking structure.⁷⁰ As described in a 2020 *Cryptogeek* article,

⁶⁶ Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System."

⁶⁷ Nakamoto.

⁶⁸ Nakamoto.

⁶⁹ Nakamoto.

⁷⁰ Jonathan, "Why We Need Anonymous Exchanges—Pros and Cons in 2022," *Cryptogeek* (blog), July 1, 2020, <https://cryptogeek.info/en/blog/exchanging-cryptocurrencies-anonymously>.

individuals have voiced many beliefs about remaining anonymous while making online payments. According to Jonathan, motivations vary—from the criminal to the skeptical:

Some people want to conceal purchases that conflict with laws or the community norms. . . . Others simply don't want to waste time and energy on making copies of all the documents required for KYC [know your customer] procedures that can last for days or even longer depending on the diligence of the support team. More than that, many people just don't like to be an object of surveillance. They don't consent to share their private data with corporations and authorities even though they are law-abiding citizens.⁷¹

A 2008 article posted under the pseudonym Satoshi Nakamoto on Bitcoin.org identifies other motivations for adopting cryptocurrency.⁷² As Nakamoto indicates,

A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed but proof that it came from the largest pool of CPU [central processing unit] power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers.⁷³

The creation of Bitcoin was well planned. One of Bitcoin's most noteworthy features is its maximum quantity available, or fixed supply. Bitcoin can create only 21 million units—to prevent Bitcoin from ever being subject to massive inflation.⁷⁴ Halving events, whereby the amount of Bitcoin earned per block divides in half, occurs at fixed intervals when Bitcoin is created and keeps the inflation rate steady, with the current

⁷¹ Jonathan, para. 1.

⁷² The authors' identities were never verified and remain a mystery today. It is possible the pseudonym Satoshi Nakamoto represents a group of individuals who refer to themselves as "we."

⁷³ Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 1. *Double-spending* refers to the possibility of the same Bitcoin being spent on more than one occasion, a potential flaw in cryptocurrency.

⁷⁴ Nakamoto.

inflation rate at 1.7 percent. When the last Bitcoin is created, in approximately 2140, the inflation rate will be 0 percent.⁷⁵ Every cryptocurrency is designed differently, hence its moniker as the “wild west” of technology and finance.⁷⁶ Understanding the creation of the first cryptocurrency helps to develop an understanding of its key characteristics.

4. Cryptocurrency Mining

Law enforcement’s understanding of cryptocurrency’s key characteristics and affordances requires knowledge of the mining process. Cryptocurrencies like Bitcoin are created through a process called “mining.”⁷⁷ During this process, computers compile a series of algorithms to solve complex mathematical problems.⁷⁸ In exchange for participating in the mathematical process, miners receive cryptocurrency until the blockchain’s intended number of cryptocurrency units is satisfied. The digital currency is then added to the public ledger, and the process continues.⁷⁹ The only resources needed to mine cryptocurrency are a computer and electricity. Sophisticated computer equipment was developed to mine cryptocurrency faster, and electricity is bid on in certain places to save on the cost of mining decentralized digital currencies.⁸⁰ Any individual can choose to mine cryptocurrency as an alternative to purchasing it, and Bitcoin miners connect their computers anywhere they can find free electricity—or they may even steal electricity to create cryptocurrency without the overhead. Figure 4 simplifies the Bitcoin mining process.⁸¹

⁷⁵ Crypto Casey, “What Blockchain Is & How Blockchain Works (Simple Overview),” May 25, 2020, in *Cryptocurrency for Beginners*, podcast, MP3 audio, 37:00, <https://cryptocasey.com/podcasts/what-bitcoin-is-how-bitcoin-works-a-simple-explanation/>.

⁷⁶ Crypto Casey.

⁷⁷ Attorney General’s Cyber Digital Task Force, *Cryptocurrency Enforcement Framework*.

⁷⁸ Subhan Nadeem, “How Bitcoin Mining Really Works,” Free Code Camp, May 31, 2018, <https://www.freecodecamp.org/news/how-bitcoin-mining-really-works-38563ec38c87/>.

⁷⁹ BitcoinMiningCom, “What Is Bitcoin Mining?,” April 9, 2013, YouTube, video, 1:55, <https://www.youtube.com/watch?v=GmOzh6I1zs>.

⁸⁰ Nadeem, “How Bitcoin Mining Really Works.”

⁸¹ James Morris, “How Mining and Blockchain Fit Together,” Kit Guru, February 16, 2018, <https://www.kitguru.net/components/james-morris/bitcoin-ethereum-and-cryptocurrency-ultimate-beginners-guide-to-mining/4/>.

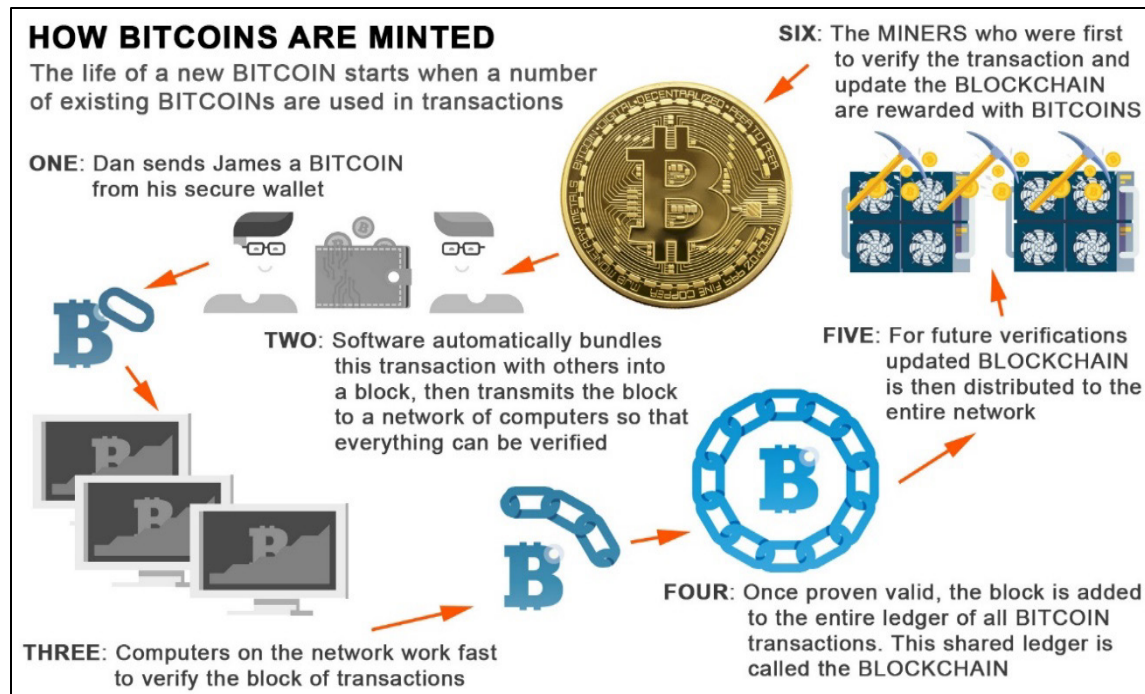


Figure 4. How Bitcoin Is Minted.⁸²

Cryptocurrency mining has become an industry in itself and created a slew of environmental concerns. Companies that mine Bitcoin build extensive, industrialized infrastructure and consume vast amounts of resources and electricity.⁸³ As indicated by CBS News in 2021, a Bitcoin mining operation was constructed in Seneca Lake, New York, near one of the famous Finger Lakes, known for private home wineries and serenity. Critics and some residents in the region are concerned about cryptocurrency mining’s environmental impact on their community because lake water is used to cool the massive power generators, and natural gas is used to generate electricity.⁸⁴ In an interview with CBS News, Tony Ingraffea, a former Cornell University professor and natural gas expert, warned of the environmental consequences of cryptocurrency mining:

⁸² Source: Morris.

⁸³ MacKenzie Sigalos, “Two of the Biggest Bitcoin Mining Companies in the World Are Battling It Out in a Texas Town of 5,600 People,” CNBC, October 31, 2021, <https://www.cnbc.com/2021/10/31/bitcoin-mining-giants-bitdeer-riot-blockchain-in-rockdale-texas.html>.

⁸⁴ “Will Industrial-Scale Bitcoin Mining Impact the Environment?,” CBS News, October 9, 2021, <https://www.cbsnews.com/news/will-industrial-scale-bitcoin-mining-impact-the-environment/>.

Outside the state of New York there are hundreds more plants. In New York state, two plants are targeted to quickly open up. . . . He said using power plants to mine bitcoin raises an ethical concern, because of emissions of carbon dioxide, and methane leakage, which is common along the supply chain leading to the plant. “Methane is, over the short term, a hundred times more potent than CO2.”⁸⁵

Law enforcement must understand that the placement of cryptocurrency mining equipment can also lead to residual crimes simply because of its existence in a community. The mining equipment comes at a high price and with the risk of being stolen. For example, on October 20, 2021, a hail of gunfire erupted in the Republic of Abkhazia near the Russian border during a robbery of cryptocurrency mining equipment. Unfortunately, according to police, while fending off the attackers, one man mistakenly shot and killed his friend.⁸⁶ Due to the expense of both owning and using cryptocurrency mining, residual property crimes such as theft and even violent crimes can occur.

B. LEGITIMATE USES OF CRYPTOCURRENCIES

Cryptocurrency’s many valid transactions illustrate further characteristics and affordances. Notably, if law enforcement identifies a cryptocurrency wallet during an investigation, it does not necessarily mean that the crime involved cryptocurrency.

Many notable online articles describe the use of cryptocurrency in purchasing big-ticket items. For example, in Middletown, New Jersey, a home for sale in 2008 drew considerable media attention following the creation of Bitcoin: “The Portland Road House, which also boasts eight baths and sits on two-and-a-half acres, is available for \$2.3 million in Bitcoin and a little less, \$2.1 million, in good old-fashioned cash.”⁸⁷ In 2021, a Miami

⁸⁵ CBS News.

⁸⁶ Matthew Gault, “Man Shot Dead in Hail of Gunfire over Crypto Mining Rigs, Police Say,” Vice News, October 28, 2021, <https://www.vice.com/en/article/n7nwwq/man-shot-dead-in-hail-of-gunfire-over-crypto-mining-rigs-police-say>.

⁸⁷ Paul Milo, “Seller of This Pricey N.J. Home Wants \$2.1M. Or You Can Pay in Bitcoin,” New Jersey Advance Local Media, February 2, 2018, https://www.nj.com/monmouth/2018/02/seller_of_this_pricy_nj_home_wants_21m_or_you_can_pay_in_bitcoin.html.

mansion sold for \$22.5 million in Bitcoin units, one of the most significant real estate transactions using cryptocurrency to date.⁸⁸

Other examples of people using cryptocurrency are relatively common and appear in current events and news publications. Videos and newsworthy articles have documented individuals' purchasing yachts, airplanes, and exotic cars with cryptocurrency. CNBC's Jim Cramer even publicized on his television show *Mad Money* that he had used his profits from Bitcoin to pay off his mortgage.⁸⁹ On January 22, 2022, New York City Mayor Eric Adams even converted his first paycheck from the City of New York into Bitcoin and Ethereum to increase awareness of his intent to bring the city to the cutting edge of cryptocurrency use.⁹⁰ In these ways, current news publications are adding to the normalization of cryptocurrency use in American markets.

On September 30, 2021, the *Washington Post* published an article indicating that the City of Miami had begun a pilot program to use cryptocurrency in its local government. The city is exploring mining its own cryptocurrency called MiamiCoin, and advocates speculate its success could eliminate local taxes in the future. City employees could soon have the option to be paid in Bitcoin, and residents could quickly pay local taxes in the cryptocurrency, too. MiamiCoin is currently available for purchase or can be mined by individuals who choose to support the endeavor. The mayor of Miami estimates that implementing cryptocurrency in the local economy could increase revenue by \$60 million annually.⁹¹ Thousands of cryptocurrencies are currently in use, and all are created similarly. According to Bailey Reutzel with CNBC, since its application in 2009,

⁸⁸ Peter Lane Taylor, "Miami Beach's Most Expensive Penthouse Just Sold in America's Largest-Known Cryptocurrency Real Estate Deal," *Forbes*, June 7, 2021, <https://www.forbes.com/sites/petertaylor/2021/06/07/miami-beachs-most-expensive-penthouse-just-sold-in-americas-largest-known-cryptocurrency-real-estate-deal-that-could-change-housing-forever/?sh=379718fc64a6>.

⁸⁹ Kevin Stankiewicz, "Cramer Sells Some Bitcoin and Pays Off a Home Mortgage," CNBC, April 15, 2021, <https://www.cnbc.com/2021/04/15/jim-cramer-says-he-sold-some-of-his-bitcoin-and-paid-off-a-mortgage.html>.

⁹⁰ Sam Raskin, "Eric Adams Converting First Paycheck as NYC Mayor to Bitcoin, Ethereum," *New York Post*, January 20, 2022, <https://nypost.com/2022/01/20/eric-adams-converting-first-paycheck-as-nyc-mayor-to-bitcoin-ethereum/>.

⁹¹ Dalvin Brown, "Crypto Tax: 'MiamiCoin' Has Made the City \$7 Million So Far, a Potential Game-Changer for Revenue Collection," *Washington Post*, September 30, 2021, <https://www.washingtonpost.com/technology/2021/09/30/crypto-miamicoin/>.

“cryptocurrency and blockchain technology has ballooned into a billion-dollar industry, while cryptocurrencies have a total market cap over \$1 trillion.”⁹² Thus, cryptocurrency is becoming a driver in diversifying financial portfolios.

Some financial planners are beginning to advise clients to place a portion of their retirement savings into cryptocurrency to diversify their retirement portfolios and capitalize on potentially significant returns.⁹³ The idea of using an alternate currency outside the power of government appeals to some individuals.⁹⁴ Cryptocurrency such as Bitcoin is less susceptible to inflation and crashes like the U.S. economy experienced in 2008, but it is subject to wild swings in value for reasons unrelated to the economy. Cryptocurrency transactions are also irreversible, so a charge-back or third-party reversal is impossible. Finally, transactions can be completed without the recipient or sender attaching an identity to the transaction, which is like dealing in cash.⁹⁵ By incorporating cryptocurrency into mainstream use, the user benefits from a borderless, easy-to-use, relatively low-cost money system.

Bitcoin ATMs are also legitimate and can be found in many places traditional ATMs are commonly located. The New Jersey Commission of Investigation identified over 11,000 Bitcoin ATMs operating in the United States.⁹⁶ The machines look very similar to traditional ATMs, but they convert fiat currency into cryptocurrency for a transaction fee. However, Bitcoin ATMs are not regulated by the State of New Jersey, unlike traditional ATMs. Therefore, such Bitcoin ATMs provide risk-free crime opportunities because of the gap in regulations.

Cryptocurrency ATMs have been subject to investigations, so state officials could understand their use. The New Jersey State Commission of Investigation served legislative

⁹² Reutzel, “What Is Cryptocurrency?”

⁹³ Carmen Reinicke, “Some Investors Are Putting More Money into Cryptocurrencies than Stocks,” October 20, 2021, <https://www.cnbc.com/2021/10/20/some-investors-putting-more-money-into-cryptocurrencies-than-stocks.html>.

⁹⁴ Reutzel, “What Is Cryptocurrency?”

⁹⁵ Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System.”

⁹⁶ New Jersey State Commission of Investigation, *Bitcoin ATMs*.

subpoenas requesting records for approximately 300 Bitcoin ATMs in New Jersey for research purposes.⁹⁷ In its research, the commission learned that individuals using most Bitcoin ATMs need only submit a cell phone number to convert fiat currency to Bitcoin. The commission's report indicates that specific Bitcoin ATMs require no personal identifying information for a transaction and emphasizes the appeal of these ATMs to people wanting privacy and those who are unbanked or underserved:

Unlike transactions made directly through online exchanges—a common way to purchase cryptocurrency—kiosk customers do not need to provide a credit card or link to a bank account. Some machines do not even require users to create an account to conduct a transaction. Whereas transactions on an online exchange may take days to complete, those conducted on the machines are immediate. Industry operators maintain the [kiosks'] appeal not only to customers who want to keep their personal information private but also to those with no bank account, the underbanked or those who operate mainly with cash, such as service industry workers.⁹⁸

State and local law enforcement should be aware that while Bitcoin ATMs are legitimate and legal, they can also be used for criminal activity. Currency transactions whereby fiat currency is transferred to cryptocurrency can support transnational organized crime groups that carry out cybercrimes against U.S. citizens. It is important for investigators to be discerning with cryptocurrency, as it has become more common and mainstream.

C. CRYPTOCURRENCY ON THE DARK WEB AND THE TOR NETWORK

Cryptocurrency is neutral—both a free market for oppressed nations and a regulation-free zone for criminals, much like the “dark web.” The dark web represents a non-indexed portion of the internet where specialized web browsers are necessary to access websites. The most common way to access the dark web is with the Tor browser. However, the Tor network can be used for both good and nefarious purposes like anything else. As noted by William Allen in the *Small Wars Journal*, the dark web creates an interesting dilemma: so much criminal activity flourishes due to Tor technology, but the anonymity it

⁹⁷ New Jersey State Commission of Investigation.

⁹⁸ New Jersey State Commission of Investigation, 3.

can provide is vital to individuals who reside under oppression.⁹⁹ Users of Tor who live in these troubled areas of the globe require its anonymizing protections to surf the web, access censored content, and otherwise exercise a right to free expression. In other words, Tor is a neutral tool that can be used for either good or ill.¹⁰⁰ The Tor network is perhaps the easiest, most common way for cybercriminals, terrorists, and nation-state actors to flourish on the web.¹⁰¹ By simply downloading and installing a Tor browser on any ordinary computer, someone can navigate instantly to illegal websites accessible only on Tor. Law enforcement should be concerned with how easy it is to purchase illegal street drugs, prescription medications, illegal guns, weapons, ammunition, and stolen goods. Also, it offers murder for hire, child pornography, and even people actively offering sex with their children in exchange for money.

The dark web is universally known among law enforcement as an online marketplace for criminal activity.¹⁰² It is also well known that cryptocurrency is the preferred payment method on the dark web.¹⁰³ Understanding how traditional internet browsing works illuminates why criminals use Tor to facilitate crimes. With conventional internet use, two interconnected devices communicate via internet protocol (IP) addressing. Each device on a computer network is assigned an IP address, allowing it to communicate, in either an IP version 4 (IPv4) or IP version 6 (IPv6) format. An IPv4 address is a series of numbers from 0 to 255 separated by a decimal (e.g., 192.155.2.201). IPv6, created after the world ran out of IPv4 addresses, comprises eight groups of four hexadecimal digits, separated by colons (e.g., 2001:0db8:1234:0042:0000:7a2e:0443:6757).

⁹⁹ William Allen, "Cryptocurrency in Threat Finance: The Manipulation of Non-fiat Digital Currencies to Finance Nefarious Actors," *Small Wars Journal*, April 4, 2018, <http://smallwarsjournal.com/jrnl/art/cryptocurrency-threat-finance-manipulation-non-fiat-digital-currencies-finance-nefarious>.

¹⁰⁰ Allen.

¹⁰¹ Eric Jardine, *The Dark Web Dilemma: Tor, Anonymity and Online Policing* (Waterloo, Ontario: Centre for International Governance Innovation and Chatham House, 2015), <https://www.cigionline.org/sites/default/files/no.21.pdf>.

¹⁰² Jardine.

¹⁰³ Jardine.

Like a residential address, which describes the locality of a house in the real world, an IP address describes the physical location of a computer on the internet. IP addresses are maintained by internet service providers, which keep records of their subscribers' connections to the internet for some time. Law enforcement can usually identify a user on a computer network by determining where a device was communicating. Serving standard legal orders such as grand jury subpoenas and search warrants to internet service providers can establish a location, eventually leading to a residential search warrant for the seizure of computers and other digital evidence.

Like cryptocurrency's design, the decentralized and encrypted TOR system hides transactions from law enforcement. Its use of onion routing makes it impossible for law enforcement to track criminal use.¹⁰⁴ The inventors of Tor developed onion routing to decentralize and encrypt communications—which closely resemble the design of cryptocurrency.¹⁰⁵ Figure 5 depicts an attacker's and a user's progress on the TOR network.¹⁰⁶

¹⁰⁴ "Home Page," Tor Project, accessed September 28, 2021, <https://www.torproject.org/>.

¹⁰⁵ Tor Project.

¹⁰⁶ Juin Chiu, "Privacy, Blockchain and Onion Routing," *Medium* (blog), October 7, 2019, <https://medium.com/unitychain/privacy-blockchain-and-onion-routing-d5609c611841>.

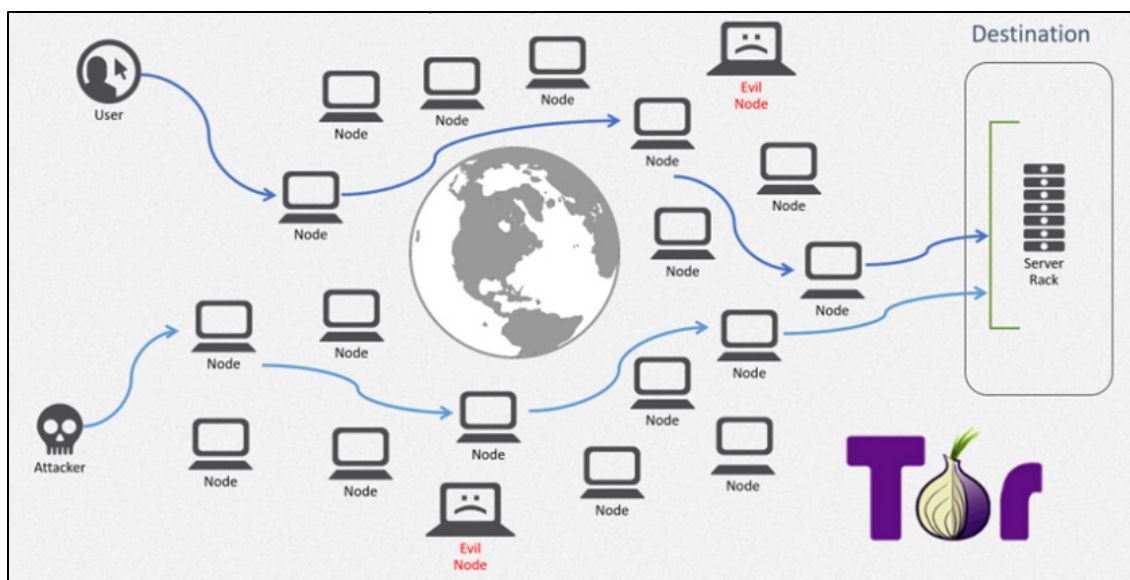


Figure 5. Depiction of the Tor Network.¹⁰⁷

With onion routing, communication between the user and the destination server is indirect. The messages and data are peeled apart—like an onion—and re-assembled at the destination to enable communication. In addition, the message transmission is encrypted. If a criminal uses the Tor network to commit crimes, cryptocurrency can facilitate payment for those crimes. In that case, understanding cryptocurrency is essential in contributing meaningful intelligence and developing investigative leads. Due to the complexity of Tor and its onion routing capabilities, it is nearly impossible to identify the persons offering these items for sale.¹⁰⁸ State and local law enforcement must be proficient in cryptocurrency to have any chance of conducting an investigation on the dark web. Unfortunately, state and local law enforcement can do little to identify someone on the Tor network because the technology differs vastly from traditional computer networking. Therefore, law enforcement’s best option in such investigations is following the cryptocurrency associated with financial transactions.

¹⁰⁷ Source: David Holmes, “Snooping on Tor from Your Load Balancer,” F5 Labs, July 3, 2018, <https://www.f5.com/labs/articles/threat-intelligence/snooping-on-tor-from-your-load-balancer>.

¹⁰⁸ Jardine, *The Dark Web Dilemma*.

D. CRYPTOCURRENCY COUPLED WITH ENCRYPTED MESSAGING SOFTWARE AND APPLICATIONS

State and local investigators must understand that criminals already use encrypted messaging software and applications to conduct their illegal activities, making it difficult for them to do their job. “Going dark” is a term law enforcement uses when encryption prevents law enforcement from obtaining legally warranted information, affecting law enforcement at all levels. The term applies when a legal authority mandates the electronic interception and access to data or communications under court orders but lacks the technical ability to carry out further investigation because of encryption’s fundamental communication shift.¹⁰⁹ This encryption issue was highlighted in San Bernardino, California, in 2015 when the FBI could not gain access to a terrorist’s cell phone to further an investigation.¹¹⁰

Encrypted messaging applications play a significant role in hindering law enforcement investigations. Law enforcement should know that operating anonymously on the dark web and using cryptocurrency to finance illegal activity are enhanced by encrypted messaging applications—a nearly impenetrable trifecta of anonymity for anyone trying to identify individuals hiding behind their computers.¹¹¹ Encrypted messaging applications allow users to communicate without someone from the outside intercepting the data. Because the Tor network provides anonymity on the internet, cryptocurrency may be the only possible investigative lead in cases where encrypted messaging and the dark web coexist.

Law enforcement faces two challenges in the world of encryption. The first challenge is the real-time interception of data in motion approved by a judiciary official, sometimes referred to as wiretaps, for example, recorded phone calls, emails, text

¹⁰⁹ James B. Comey, “Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?” (remarks, Brookings Institution, Washington, DC, October 16, 2014), <https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course>.

¹¹⁰ “Apple v. FBI,” Electronic Privacy Information Center, accessed October 6, 2022, <https://epic.org/documents/apple-v-fbi-2/>.

¹¹¹ Police Executive Research Forum, *New National Commitment Required*.

messages, and chat sessions.¹¹² The second challenge concerns data digitally stored on devices, referred to as “data at rest,” for instance, stored emails, text messages, photos, and videos on a computer server.¹¹³ Data in motion and electronically stored data are important records for law enforcement, but some methods of encryption prevent law enforcement from obtaining digital evidence that may be used to identify and save victims, expose evidence of criminal conduct, or exonerate the innocent.¹¹⁴ The current level of encryption available offers an advantage for criminals.

E. CONCLUSION

This chapter has drawn from existing literature on cryptocurrency and analyzed how its key characteristics are favorable for criminality. It has described blockchain technology, bitcoin mining, cryptocurrency wallets, and the history of cryptocurrency; assessed the proliferation of cryptocurrency, including its legitimate uses; and identified current events pertinent to this analysis. A basic understanding of cryptocurrency reveals the implications of these traits. Among these factors, its anonymity, the ease with which it flows across national borders, its impenetrability, and its concealability make it especially attractive to criminals.

¹¹² Comey, “Going Dark.”

¹¹³ Comey.

¹¹⁴ Comey.

THIS PAGE INTENTIONALLY LEFT BLANK

III. CRYPTOCURRENCY CRIMES AND POLICY RESPONSES

This chapter presents some significant newsworthy cases involving cryptocurrency. These current events demonstrate that cryptocurrency has links to crime, that the technology is not going away, and that the federal government is doing its part to secure its use.

A. CRIMES AND POLICY RESPONSES

The U.S. government's statement on cryptocurrency suggests the technology will be a vulnerability in the years to come. On October 5, 2021, the Securities and Exchange Committee (SEC) indicated it would not seek to ban the use of cryptocurrency in America. The SEC noted that current efforts would "focus . . . on ensuring that the industry adheres to investor and consumer protection rules, anti-money laundering regulations and tax laws."¹¹⁵ The SEC advised, however, that the U.S. Congress could still implement a complete ban. President Biden coordinated efforts to audit the nation's cryptocurrency capabilities related to crimes and terrorism.¹¹⁶ State and local law enforcement should look to this information as an indicator of its permanence in America and begin to plan accordingly.

On October 6, 2021, the United States announced the creation of a National Cryptocurrency Enforcement Team.¹¹⁷ The exponential increase in criminal and terrorist activity associated with cryptocurrency necessitated the creation of this body.¹¹⁸ This new task force falls under the umbrella of the Department of Justice and will exclusively

¹¹⁵ Benjamin Bain, "SEC Chief Says the U.S. Won't Ban Cryptocurrencies," Bloomberg, October 5, 2021, <https://www.bloomberg.com/news/articles/2021-10-05/sec-chief-signals-crypto-ban-like-china-s-won-t-happen-in-u-s>.

¹¹⁶ Benjamin Bain and Jennifer Epstein, "White House Weighs Wide-Ranging Push for Crypto Oversight," Bloomberg, October 8, 2021, <https://www.bloomberg.com/news/articles/2021-10-08/white-house-weighs-wide-ranging-push-for-crypto-oversight>.

¹¹⁷ Will Feuer, "Biden Administration Unveils 'National Cryptocurrency Enforcement Team,'" *New York Post*, October 7, 2021, <https://nypost.com/2021/10/07/biden-administration-unveils-national-cryptocurrency-enforcement-team/>.

¹¹⁸ Feuer.

investigate the illegal use of cryptocurrency to protect U.S. interests. Its goals are to identify and prosecute individuals laundering money through cryptocurrency and investigate individuals using digital currencies for nefarious purposes and terrorism. The creation of this new entity suggests that the United States is responding appropriately to these threats at the federal level.

Some interesting national and international headlines surrounding cryptocurrency have recently appeared in the news. On October 10, 2021, national news developed after the Department of Justice arrested and charged a husband and wife for treason and espionage in the United States.¹¹⁹ According to the Department of Justice, the pair attempted to trade \$10,000 in Bitcoin for information from top-secret encrypted messaging aboard U.S. nuclear submarines. The suspects were introduced to an undercover FBI agent, and they allegedly hid a microSD card containing the national secrets inside a peanut butter sandwich. According to the media, the couple specifically requested cryptocurrency because of its anonymous nature. Such news reports may represent the tip of the iceberg for crimes involving cryptocurrency.

On October 26, 2021, the Federal Deposit Insurance Corporation (FDIC) indicated it would seek options for banks and their clients to have cryptocurrency protection. The FDIC could provide some clear direction on the trading and deposits of cryptocurrency and its use as an asset to secure loans in the future. According to Jelena McWilliams, who chairs the FDIC, “If we don’t bring this activity inside the banks, it is going to develop outside of the banks. . . . The federal regulators won’t be able to regulate it.”¹²⁰ Thus, at the highest levels, policymakers recognize the potential long-term relevance of cryptocurrency in American culture.

On October 27, 2021, the Department of Justice recognized publicly that the dark web is still active among transnational criminal groups. International law enforcement

¹¹⁹ “Maryland Nuclear Engineer and Spouse Arrested on Espionage-Related Charges,” Department of Justice, October 10, 2021, <https://www.justice.gov/opa/pr/maryland-nuclear-engineer-and-spouse-arrested-espionage-related-charges>.

¹²⁰ Echo Wang, “U.S. Regulators Exploring How Banks Could Hold Crypto Assets—FDIC Chairman,” Reuters, October 26, 2021, <https://www.reuters.com/business/finance/us-regulators-exploring-how-banks-could-hold-crypto-assets-fdic-chairman-2021-10-26/>.

arrested and charged 150 people for drug trafficking on the dark web. Through a mission dubbed Operation Dark Hun, the United States and international partners recovered a cache of the following:

over \$31.6 million in both cash and virtual currencies; approximately 234 kilograms (kg) of drugs worldwide including 152.1 kg of amphetamine, 21.6 kg of cocaine, 26.9 kg of opioids, 32.5 kg of MDMA, in addition to more than 200,000 ecstasy, fentanyl, oxycodone, hydrocodone, and methamphetamine pills, and counterfeit medicine; and 45 firearms.¹²¹

In contrast to the United States, some countries acknowledge the potential drawbacks associated with cryptocurrency. In 2021, China wholly banned all cryptocurrencies.¹²² This ban includes the creation or “mining” of cryptocurrencies, and China blocked all social media accounts associated with virtual currency. China cited the threat of money laundering and criminal activity related to cryptocurrency and many cybercrimes, among other reasons.¹²³

Recognizing the threat of cryptocurrency by other nations, American corporations like Starbucks and McDonalds began to encourage its use and accept Bitcoin as legal currency in El Salvador.¹²⁴ In addition, on January 16, 2022, Walmart began preparations to create its own cryptocurrency for use in the United States.¹²⁵ As outlined in this section, cryptocurrency has been discussed significantly in America. As the Police Executive Research Forum cautions in its report on evolving criminal activities, law enforcement

¹²¹ “International Law Enforcement Operation Targeting Opioid Traffickers on the Darknet Results in 150 Arrests Worldwide and the Seizure of Weapons, Drugs, and Over \$31 Million,” Drug Enforcement Administration, October 26, 2021, para. 3, <https://www.dea.gov/press-releases/2021/10/26/departments-justice-announces-results-operation-dark-hunter>.

¹²² Gian M. Volpicelli, “China’s Sweeping Cryptocurrency Ban Was Inevitable,” *Wired*, September 30, 2021, <https://www.wired.com/story/chinas-sweeping-cryptocurrency-ban-inevitable/>.

¹²³ Volpicelli.

¹²⁴ Nelson Renteria and Anthony Esposito, “El Salvador’s World-First Adoption of Bitcoin Endures Bumpy First Day,” Reuters, September 8, 2021, <https://www.reuters.com/business/finance/el-salvador-leads-world-into-cryptocurrency-bitcoin-legal-tender-2021-09-07/>.

¹²⁵ Lauren Thomas, “Walmart Is Quietly Preparing to Enter the Metaverse,” CNBC, January 16, 2022, <https://www.cnbc.com/2022/01/16/walmart-is-quietly-preparing-to-enter-the-metaverse.html>.

needs to recognize these changing technologies and prepare for the crimes resulting from cryptocurrency's proliferation.¹²⁶

B. CRYPTOCURRENCY'S USE IN TRADITIONAL CRIMES

As indicated by the Police Executive Research Forum, cryptocurrency has emerged in traditional drug and gun cases, human-trafficking investigations, and financial fraud crimes committed by local gang members and other criminals.¹²⁷ Law enforcement should be aware of cryptocurrency's presence as it gains national momentum, and police and prosecutors must understand its use. Also, the Police Executive Research Forum has pointed out that "local gang members and other criminals have noticed that they can make more money, with less risk of getting caught, and smaller penalties if they do get caught, by using technology."¹²⁸ In addition, as cryptocurrency is becoming such a popular commodity, law enforcement will have to learn how to use it to increase efforts in combatting local criminals' selling illegal items. In addition, they will need the knowledge to change policies while conducting undercover operations. New guidelines can only be developed once decision-makers fully grasp the nature of cryptocurrency and its importance to the overall criminal environment, including its application to traditional crime.

C. DARK WEB AND TOR BROWSING CRIMES

Cryptocurrency is extremely attractive to criminals because of its anonymity, relative impenetrability to hacking, concealability, and ease of international exchange. On November 5, 2020, the Department of Justice seized and applied for forfeiture of over \$1 billion in Bitcoin because of the dark web investigation into the Silk Road on the Tor network, representing the largest seizure of cryptocurrency in world history.¹²⁹ According to the civil forfeiture complaint, "from 2011 until October 2013 when it was seized by law

¹²⁶ Police Executive Research Forum, *New National Commitment Required*.

¹²⁷ Police Executive Research Forum.

¹²⁸ Police Executive Research Forum, 5.

¹²⁹ U.S. Attorney's Office, Northern District of California, "Civil Action to Forfeit Cryptocurrency."

enforcement, Silk Road was the most sophisticated and extensive transnational criminal marketplace on the Internet.”¹³⁰ The Silk Road investigation has been the most significant investigation into illegal activities on the dark web to date. The website’s founder, Ross Ulbricht—a now 37-year-old American—was sentenced to 40 years in prison.

The investigation into the Silk Road began in 2011 after the Federal Bureau of Investigation learned of a website on the dark web that offered the sale of illegal drugs, guns, poisons, murder for hire, and other items and services.¹³¹ Former FBI Special Agent Milan Patel referred to the Silk Road as the “Amazon of drug sites.”¹³² The investigation lasted approximately two years before the most significant lead in the case was developed by accident.¹³³ While this investigation is an example of the extreme criminality associated with cryptocurrency and the dark web, many other kinds of investigations follow in subsequent sections.

D. DENIAL OF SERVICE, RANSOMWARE, AND CRIMES COMMITTED WITH CRYPTOCURRENCY

Computer network intrusions remain among the top threats to the U.S. homeland security enterprise.¹³⁴ A recent example shows why law enforcement should be aware of such activities. In May 2021, a ransomware attack on the Colonial Pipeline’s computer network led to fuel shortages on the East Coast of the United States for several days. Criminal groups and nation-state actors perpetrated the cyberattack. As a result of the investigation, the Department of Justice seized 63.7 Bitcoins valued at \$2.3 million from proceeds belonging to the individuals responsible for the Colonial Pipeline cyberattack.¹³⁵

¹³⁰ U.S. Attorney’s Office, Northern District of California.

¹³¹ Emily Bernstein and Caroline Sommers, “Inside the FBI Takedown of the Mastermind behind website Offering Drugs, Guns and Murders for Hire,” CBS News, November 10, 2020, <https://www.cbsnews.com/news/ross-ulbricht-dread-pirate-roberts-silk-road-fbi/>.

¹³² Bernstein and Sommers.

¹³³ Joshua Bearman and Tomer Hanuka, “The Rise & Fall of Silk Road,” *Wired*, April 2015, <https://www.wired.com/2015/04/silk-road-1/>.

¹³⁴ Attorney General’s Cyber Digital Task Force, *Cryptocurrency Enforcement Framework*.

¹³⁵ Department of Justice, “Department of Justice Seizes \$2.3 Million.”

Cryptocurrency was the payment requested in the ransom and a critical investigative lead for law enforcement.

Also significant to law enforcement are denial of service (DoS) attacks on computer networks emanating from ransomware, malware, or DoS services sold by criminals on the dark web. These are all commonly referred to as computer network intrusions. A DoS attack floods a computer network with messages that bog down the network's bandwidth, rendering it useless.¹³⁶ Computer scientists call such an attack a *user datagram protocol flood*. Ransomware is malicious software that encrypts a computer system until a ransom is paid while malware is any type of destructive software to a computer or network. Before the ransomware or malware is executed, a data breach commonly occurs, the proceeds of which are usually sold on the dark web.¹³⁷ Cryptocurrency is the most common payment source for purchasing ransomware, malware, and network disruption tools.¹³⁸ It is also the preferred form of payment for the services to deploy these nefarious tools on sensitive and unprotected computer systems.¹³⁹ The nexus between cryptocurrency and these crimes is essential for law enforcement to recognize. Figure 6 explains the relationship between Bitcoin, ransomware, and system vulnerabilities.

¹³⁶ Zak Islam, "The Dark Web Has Become Darker and Busier, Cybercrime Services Cost Less than \$500," *Techspot Magazine*, October 19, 2021, <https://www.techspot.com/news/91830-dark-web-has-become-darker-busier-cybercrime-services.html>.

¹³⁷ Jardine, *The Dark Web Dilemma*.

¹³⁸ Justin Muzinich, "America's Crypto Conundrum," *Foreign Affairs*, November/December 2021, <https://www.foreignaffairs.com/articles/united-states/americas-crypto-currency-conundrum>.

¹³⁹ Islam, "The Dark Web Has Become Darker and Busier."



Figure 6. Ransomware Infographic.¹⁴⁰

The New Jersey State Police (NJSP) Cyber Crimes Unit (CCU) is the premier New Jersey agency responsible for investigating and reviewing computer network intrusions when a data breach is reported to state officials. In 2020, the NJSP CCU, in collaboration with the New Jersey Cybersecurity and Communications Integration Cell, cataloged 1,385 network intrusions affecting 1,946,563 state residents.¹⁴¹ This number suggests the scale and scope of network intrusions and should certainly concern state and local law enforcement.

Cryptocurrency is inextricably tied to all ransomware attacks—it is the standard payment used to negotiate the return of stolen data or to regain control of a system encrypted with ransomware.¹⁴² Despite these staggering numbers, the Internet Crime Complaint Center indicates a delayed and underreported aspect to these types of investigations. Due to brand reputation management, companies hesitate to report unauthorized access to their computer systems.¹⁴³ The potential impact computer network

¹⁴⁰ Source: “Ransomware,” University of Florida, accessed November 12, 2021, <https://security.ufl.edu/resources/protect-your-computer/ransomware/>.

¹⁴¹ “Public Data Breaches,” New Jersey Cybersecurity and Communications Integration Cell, November 19, 2021, <https://www.cyber.nj.gov/threat-center/public-data-breaches/>.

¹⁴² Attorney General’s Cyber Digital Task Force, *Cryptocurrency Enforcement Framework*.

¹⁴³ Dan Swinhoe, “Why Businesses Don’t Report Cybercrimes to Law Enforcement,” CSO Online, May 30, 2019, <https://www.csoonline.com/article/3398700/why-businesses-don-t-report-cybercrimes-to-law-enforcement.html>.

intrusions can have on victims is massive and expensive. According to Angelena Bradfield and Stephanie Wake, writing for the Bank Policy Institute, a member bank “reported a 334 percent rise in attacks on its clients [in 2021]. . . . The one constant in all these ransomware attacks appears to be the demand that the ransom be paid in cryptocurrency.”¹⁴⁴ In this way, the implications for law enforcement will certainly continue to grow.

Global banking means attackers can be located anywhere in the world. As Bradfield and Wake highlight,

Ransomware attacks can be spread globally to computers and operating systems without regard to borders. . . . Cryptocurrency laundering methods can be used to obfuscate funds’ origins, making it difficult for law enforcement to track the source of funds derived from a ransom upon their inevitable reentry to the global banking system. Recently, ransomware actors have been seen switching their demands for payments from Bitcoin to more anonymous and privacy-oriented digital currency, such as Monero, making it even more difficult to trace.¹⁴⁵

Unfortunately, a computer novice, not a “hacker,” may purchase a ransomware variant and execute it on a computer system. “Script-kitties,” those who use computer programs but have neither the ability nor education to create a program themselves, can wreak havoc on computer systems around the globe—even with their limited knowledge—by shutting down critical systems from the comfort of their homes.¹⁴⁶ They can purchase network disruption tools on Tor using any cryptocurrency as the preferred payment source. Although people commonly believe cybercriminals reside abroad, they also live within U.S. borders. The effects of their actions can be long-lasting and devastating.

Demonstrating how common and easy it is for local script-kitties and hackers to create chaos, Microsoft has warned that

Dark Web denizens can acquire most cybercrime services for less than \$500. Atlas VPN [virtual private network] discovered that underground marketplaces offer a single ransomware kit for as low as \$66, while hackers

¹⁴⁴ Angelena Bradfield and Stephanie Wake, “Top 7 Things to Know about Ransomware and Why Criminals Prefer Crypto Payments,” *Bank Policy Institute* (blog), May 12, 2021, <https://bpi.com/top-7-things-to-know-about-ransomware-and-why-criminals-prefer-crypto-payments/>.

¹⁴⁵ Bradfield and Wake.

¹⁴⁶ This anecdote is from many years of professional experience as a cybercrime detective.

only charge about \$311 to deliver a sustained DDoS attack against a target for as long as a month. Data breaches are commonplace nowadays, so it's not surprising that stolen usernames and passwords are offered for as little as 97 cents per 1,000 accounts. Additionally, hackers perform custom jobs such as credit card scams or identity theft for as little as \$250.¹⁴⁷

Even if an individual is not a skilled computer user, one can be hired to commit these types of crimes for a small sum. Figure 7 illustrates the price of these disruptive services.

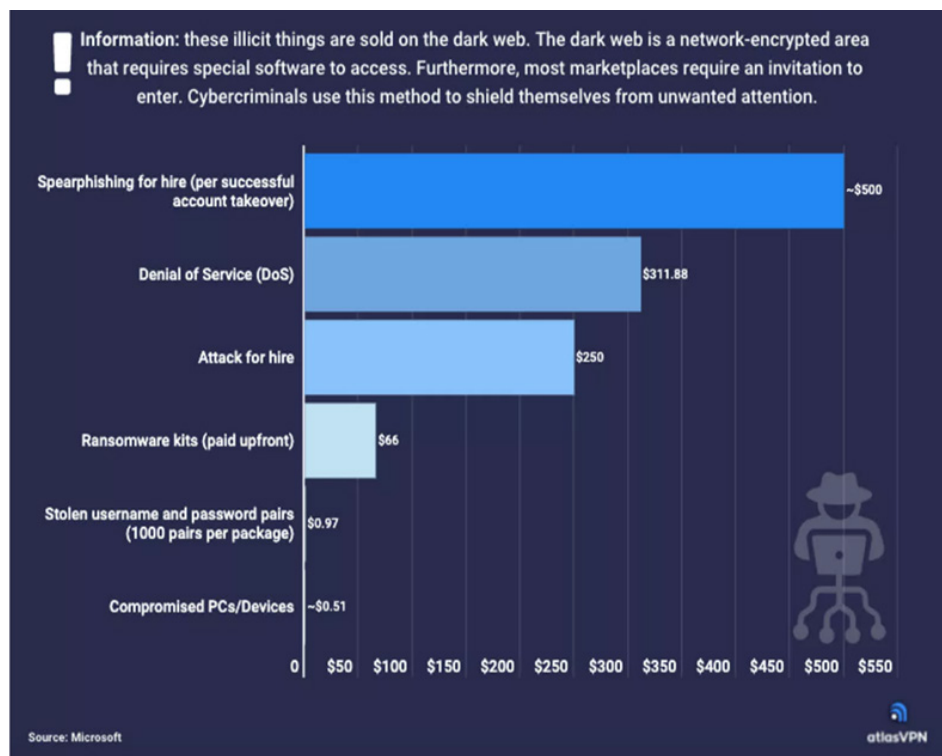


Figure 7. Average Prices of Cybercrime Services for Sale in 2021.¹⁴⁸

¹⁴⁷ Islam, "The Dark Web Has Become Darker and Busier."

¹⁴⁸ Source: Islam.

E. NATION-STATE HACKING, TERRORISM AND APPLICATION TO CRYPTOCURRENCY

Cryptocurrency use in terrorism financing concerns national security, and it is essential for law enforcement to understand its application.¹⁴⁹ Law enforcement must also be aware of the overall national security environment where cryptocurrency applies. Unfortunately, state and local government officials generally lack the training and experience to contribute meaningful intelligence and help with criminal prosecutions whenever cryptocurrency is involved.¹⁵⁰ If state and local law enforcement had a better understanding of cryptocurrency, it could solve more crimes and disseminate better intelligence among federal, state, local, and tribal governments. The following FBI cases of terrorism illustrate the threat to the nation. Hopefully, they spur policies that enable local and state law enforcement to better contribute intelligence to such cases.

In August 2020, the Department of Justice announced the U.S. government's disruption of three cyber-enabled terrorist financing campaigns involving the Al-Qassam Brigades, Hamas, al-Qaeda, and the Islamic State of Iraq and Syria. These actions represent the largest U.S. cryptocurrency seizure related to terrorism. The Department of Justice outlined the integral nature of cryptocurrency in these campaigns:

These three terror finance campaigns all relied on sophisticated cyber-tools, including the solicitation of cryptocurrency donations from around the world. The action demonstrates how different terrorist groups have similarly adapted their terror finance activities to the cyber age. Each group used cryptocurrency and social media to garner attention and raise funds for their terror campaigns.¹⁵¹

Figure 8 depicts an example of the Federal Bureau of Investigation's efforts to combat cyber terrorism. In many cases, cryptocurrency finances terrorist activities.

¹⁴⁹ Attorney General's Cyber Digital Task Force, *Cryptocurrency Enforcement Framework*.

¹⁵⁰ Police Executive Research Forum, *New National Commitment Required*.

¹⁵¹ "Global Disruption of Three Terror Finance Cyber-Enabled Campaigns: Largest Ever Seizure of Terrorist Organizations' Cryptocurrency Accounts," Department of Justice, August 13, 2020, para. 2, <https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns>.



Figure 8. GRU Hackers Wanted by the FBI.¹⁵²

Cryptocurrency has also played a role in attacking infrastructure. Nation-state hackers exploit critical American infrastructure daily and use cryptocurrency to extort American citizens' tax dollars to further their agendas.¹⁵³ While U.S. adversaries live

¹⁵² Source: "GRU Hackers' Destructive Malware and International Cyber Attacks," Federal Bureau of Investigation, accessed February 6, 2023, <https://www.fbi.gov/wanted/cyber/gru-hackers-destructive-malware-and-international-cyber-attacks>.

¹⁵³ Attorney General's Cyber Digital Task Force, *Cryptocurrency Enforcement Framework*.

thousands of miles away physically, they are much closer virtually than many Americans realize. On October 25, 2021, Microsoft revealed that the Russian hacker group responsible for SolarWinds cyberattacks across the United States had made numerous attempts to disrupt American infrastructure.¹⁵⁴ In its statement, Microsoft warned, “This recent activity is another indicator that Russia is trying to gain long-term, systematic access to a variety of points in the technology supply chain and establish a mechanism for surveilling—now or in the future—targets of interest to the Russian government.”¹⁵⁵ Over the past decade, criminals and terrorists have begun diversifying their funding sources to include cryptocurrency.¹⁵⁶ Cryptocurrency’s ability to cross borders freely and easily lends to its popularity among adversaries of the United States.

Both cybercriminals and nation-state hackers are motivated predominantly by money.¹⁵⁷ Since these entities operate anonymously on a portion of the internet designed to protect their identities, an obvious choice is to accept anonymous payments for goods and services. Cryptocurrency is a cashless, peer-to-peer transaction system that fits the needs of the nefarious customer.

F. DOMESTIC INSIDER-THREAT HACKING CASES INVOLVING CRYPTOCURRENCY AND THE DARK WEB

Although law enforcement attributes many hacking events to terrorism, countless domestic criminals and nefarious computer professionals in the United States commit cybercrimes. The Department of Homeland Security considers such individuals *insider threats*—for example, those who separate from employment can use their computer skills and personal knowledge of a business’s computer network to extort a company after they

¹⁵⁴ “Latest Russian Cyberattack Targeting Hundreds of U.S. Networks—Microsoft,” Reuters, October 25, 2021, <https://www.reuters.com/technology/microsoft-says-russian-group-has-targeted-hundreds-us-networks-2021-10-25/#:~:text=Latest%20Russian%20cyberattack%20targeting%20hundreds%20of%20U.S.%20networks%20%2DMicrosoft,-Reuters&text=Microsoft%2C%20in%20a%20blog%20post,service%20providers%22%20of%20cloud%20services>.

¹⁵⁵ Reuters.

¹⁵⁶ Department of Justice, “Global Disruption of Three Terror Finance Cyber-Enabled Campaigns.”

¹⁵⁷ This anecdote is from many years of professional experience as a cybercrime detective.

quit.¹⁵⁸ Insider-threat cases occur for many reasons. Former employees might feel the computer system's design and architecture are their personal intellectual property, even though they were hired to perform a service for a corporation.¹⁵⁹ Along this line, the Federal Bureau of Investigation has identified 10 examples of employees from within corporations who stole information during cyber network intrusions: Wen Chyu Liu, Kexue Huang, Yuan Li, Elliot Doxer, Sergey Aleynikov, Michael Mitchell, Shalin Jhaveri, Hanjuan Jin, Greg Chung, and Chi Mak. Most of these high-profile insider threats were convicted of theft or espionage.¹⁶⁰ For readers in state and local law enforcement, the following paragraphs present a hypothetical scenario to illustrate the importance of cryptocurrency in cybercrimes relating to insider threats.

A contracted information-technology worker named John Doe is employed for a local business named Car Industries, Inc., and has worked there for almost a year designing and updating its computer systems. Due to budgetary constraints, John Doe finds out that his contracted position is unavailable next year. On his last day, John Doe arrives at work, turns in his access card to the building, gathers his personal belongings, and leaves without incident.

The computer system for Car Industries, Inc., stores local data used for daily operations and current projects. It also includes a point-of-sale computer server used to process credit card purchases. Customers' personally identifiable information for car loans is also processed through the computer system, which integrates with online banks. John Doe had been instrumental in enabling employees to work from home on their laptops during the height of the COVID-19 pandemic.

Approximately one month after John Doe leaves Car Industries, Inc., its computer network becomes encrypted with a known variant of ransomware. Along with the

¹⁵⁸ "Insider Threat," Department of Homeland Security Science and Technology, January 12, 2023, <https://www.dhs.gov/science-and-technology/cybersecurity-insider-threat#>.

¹⁵⁹ Department of Homeland Security Science and Technology.

¹⁶⁰ Source: "The Insider Threat: An Introduction to Detecting and Deterring an Insider Spy," Federal Bureau of Investigation, accessed January 17, 2022, https://www.fbi.gov/file-repository/insider_threat_brochure.pdf/view.

ransomware, a message requests that the recipient send five Bitcoins to a public address to regain access to the company's devices. Car Industries, Inc., does not pay the ransom but hires a private information-technology vendor, 123 Computer Solutions, to investigate the incident and restore its system. 123 Computer Solutions identifies a known ransomware variant and uses a publicly available decryption key to restore access to the system.¹⁶¹ The files are recovered, and the system is updated. All the servers and workstations are re-imaged, and the data are restored.¹⁶² Car Industries' computer system is operating better than before the incident.

During 123 Computer Solutions' investigation into the ransomware attack, it identifies that an IP address emanating from another country entered the computer network through a vulnerability in the computer network's remote desktop application installed on employee machines to allow them to work from home during the global pandemic. The IP address identified within the system and used to deploy the ransomware was assigned to a mainstream VPN company.¹⁶³ The VPN company does not record IP address connections because it firmly believes in the privacy of its customers on the internet—and the U.S. government does not require it.

One month after the ransomware attack, Car Industries is contacted by a friendly business owner who advises the company that its customers' data are for sale on the dark web in multiple forums for small amounts of Bitcoin. The data were likely stolen from Car Industries during a hacking event. Car Industries, Inc., contacts 123 Computer Solutions immediately, as company executives believe they have just been hacked. 123 Computer Solutions identifies no computer network vulnerabilities within the network and no signs of unauthorized computer access. Meanwhile, local law enforcement responds and unknowingly attributes the event to foreign hacking. At this point, one might ask, What happened?

¹⁶¹ "Decryption Tools," No More Ransom, accessed January 12, 2023, <https://www.nomoreransom.org/en/decryption-tools.html>.

¹⁶² Re-imaging involves the installation of a new operating system on a computer.

¹⁶³ A VPN is a protected, encrypted network connection used to disguise one's identity on a public computer network.

The answer: John Doe's computer access had not been revoked before he was notified of his termination from Car Industries, Inc., and there was no computer use policy for transitioning employees. The upset and unemployed John Doe used his VPN service to change his IP address manually and virtually transfer his digital footprint to another country. Once he changed his digital location, John Doe used Car Industries' remote desktop protocol, implemented during the pandemic, to enter the computer network somewhere offsite. John Doe exfiltrated the company's sensitive data and executed ransomware before logging off the system. John Doe's ransomware included a message for Car Industries to send the Bitcoin to his account in exchange for restored access to its files.

123 Computer Solutions had been hired to repair the computer network and did just that. It identified a foreign IP address that entered Car Industries' computer system remotely and attributed it to hackers from a foreign nation trying to extort the business. 123 Computer Solutions re-imaged the servers and workstations without thoroughly investigating the network intrusion. In doing so, it destroyed any evidence of John Doe's exfiltration. Due to the lack of U.S. regulation, the VPN company was not required to possess IP address connection information to assist law enforcement in potentially identifying a suspect. Due to an incomplete investigation, the investigators missed crucial evidence. When the business did not pay the cryptocurrency ransom, John Doe—who was looking for a way to earn some extra money and believed the computer system was his intellectual property—surreptitiously released all the data on the dark web. John Doe sold the data to unknown individuals for Bitcoin. The suspect had never been to another country but remained unidentified.

An alternate ending: Car Industries, Inc., pays the ransom in Bitcoin to John Doe without ever identifying him, and John Doe might choose to release the data on the dark web. No one ever fully understands what happened. Hackers often exfiltrate sensitive and personally identifiable data before executing ransomware to disguise the data breach.

In either ending to this scenario, law enforcement could have identified John Doe if somebody had trained them in locating the public Bitcoin address associated with the

initial ransomware attack or the sale of data on the dark web. Investigators would have discovered that John Doe resided in their local jurisdiction and solved the crime.

G. CONCLUSION

In summary, to plan and implement any modern-day crime anonymously, one may use cryptocurrency, conduct illegal business on anonymous computer networks such as Tor, or communicate with other criminals on encrypted messaging applications.¹⁶⁴ Cybercriminals are armed with every advantage to outwit their victims. State and local enforcement must comprehend the involvement of cryptocurrency in criminal investigations to have a better chance of solving crimes. Cryptocurrency is the Alamo. State and local law enforcement must rally against the criminals using these technologies to perpetrate crimes. If the battle against the unlawful use of cryptocurrency is lost, law enforcement may never competently investigate such crimes for the public.

¹⁶⁴ Police Executive Research Forum, *New National Commitment Required*.

IV. DNA CASE ANALYSIS

This chapter examines another technological revelation from the past—DNA analysis—offering a timeline of events surrounding this exciting technology and its use in investigations, from its infancy to projections for the future. The legal precedents, policy and procedural development, and certifications for DNA analysis can guide policies and procedures for cryptocurrency.

A. INTRODUCTION TO DNA

First identified by scientists in the 1800s, deoxyribonucleic acid (DNA) defines the genetic makeup of all living things.¹⁶⁵ DNA is an essential tool for investigators because, aside from identical siblings, everyone’s DNA is different.¹⁶⁶ It comprises three crucial “building blocks”: a phosphate group; a sugar group; and one of four types of nitrogen bases, adenine (A), thymine (T), guanine (G), or cytosine (C).¹⁶⁷ Simply, the phosphate and sugar groups form alternate sides of the DNA ladder, and the base pairs (A–T or G–C) connect to the sugar groups like rungs on the ladder. This structure twists into what is famously described as a double helix (see Figure 9).¹⁶⁸

¹⁶⁵ “Deoxyribonucleic Acid (DNA) Fact Sheet,” National Human Genome Research Institute, accessed August 8, 2022, <https://www.genome.gov/about-genomics/fact-sheets/Deoxyribonucleic-Acid-Fact-Sheet>; Emily J. Hanson, *The Use of DNA by the Criminal Justice System and the Federal Role: Background, Current Law, and Grants* (Washington, DC: Congressional Research Service, 2022), ProQuest.

¹⁶⁶ Hanson, *The Use of DNA by the Criminal Justice System*.

¹⁶⁷ National Human Genome Research Institute, “Deoxyribonucleic Acid.”

¹⁶⁸ National Human Genome Research Institute.

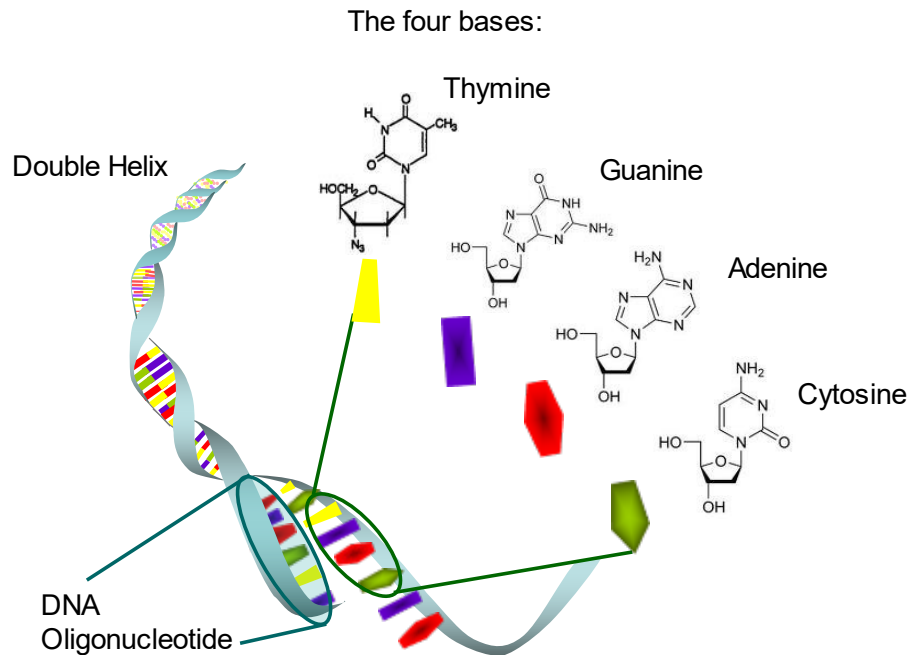


Figure 9. DNA Structure

DNA makes up the structure of a chromosome inside a cell's nucleus, and chromosomes exist within the nucleus of every cell.¹⁶⁹ As described by Medline Plus, "Chromosomes are not visible in the cell's nucleus—not even under a microscope—when the cell is not dividing. However, the DNA that makes up chromosomes becomes more tightly packed during cell division and is then visible under a microscope."¹⁷⁰ Celia Henry Arnaud details the relationship between chromosomes and DNA: "Chromosomes contain markers where short DNA sequences are repeated multiple times. The number of repeats at each marker varies from person to person, and each person has two copies, or alleles, of each marker, one inherited from their mother and one from their father."¹⁷¹

¹⁶⁹ "What Is a Chromosome?," Medline Plus, accessed August 11, 2022, <https://medlineplus.gov/genetics/understanding/basics/chromosome/>.

¹⁷⁰ Medline Plus.

¹⁷¹ Arnaud, "Thirty Years of DNA Forensics."

B. DNA ANALYSIS

DNA can be obtained in myriad ways, including from hair, bones, saliva, blood, semen, or other bodily fluids.¹⁷² More than three decades of technological development have seen DNA's use in identifying missing individuals, apprehending criminals, and exonerating the innocent.

For years, potential DNA evidence was obtained during criminal investigations, but the evidentiary sample collected from the crime scene was too small for existing technology to analyze it. Investigators would have needed a larger specimen to test and analyze the genetic material.¹⁷³ Investigators can now analyze criminal DNA evidence where they once could not. The invention of polymerase chain reaction (PCR) made it possible to replicate or extend DNA to create a suitable sample for analysis. The inventor of PCR, Kary Mullis, won a Nobel Prize in Chemistry for his work in DNA development. Without his efforts, the law enforcement community would not have the investigative tools that it does today.

Forensic scientists break down cells to extract DNA from blood, other fluids, or tissues; copy the DNA using PCR, and separate the copied markers using electrophoresis. Electrophoresis occurs by separating DNA by size using an electropherogram.¹⁷⁴ Scientists then use either gel or capillary electrophoresis. In the former, both an unknown DNA sample and a known control sample are injected into gel to compare the results. A color dye added to the DNA samples makes them visible.¹⁷⁵ The process employs a power supply, a prepared agarose gel sheet, and positively and negatively charged electrodes placed at either end of the gel.¹⁷⁶ Because DNA is negatively charged, DNA samples are

¹⁷² Hanson, *The Use of DNA by the Criminal Justice System*.

¹⁷³ "Polymerase Chain Reaction (PCR) Fact Sheet," National Human Genome Research Institute, August 17, 2020, <https://www.genome.gov/about-genomics/fact-sheets/Polymerase-Chain-Reaction-Fact-Sheet>.

¹⁷⁴ "Gel Electrophoresis," Scitable, accessed August 8, 2022, <https://www.nature.com/scitable/definition/gel-electrophoresis-286/>.

¹⁷⁵ "What Is Gel Electrophoresis?," Your Genome, July 21, 2021, <https://www.yourgenome.org/facts/what-is-gel-electrophoresis/>.

¹⁷⁶ Your Genome.

naturally pulled toward the positive charge on the gel sheet. Capillary electrophoresis works similarly; however, tubes and liquid move the positively charged DNA sample more rapidly and efficiently than with gel.¹⁷⁷ Once forensic scientists complete the electrophoresis procedure, they can create a readable DNA profile for analysis.¹⁷⁸ Results from the electropherogram link each marker's number of repeats, revealing the separation of markers, including repetitions in both alleles.¹⁷⁹ The DNA profile is stored and compared against other known samples in law enforcement DNA databases—the Combined DNA Index System (more commonly known as CODIS) or the National DNA Index System (NDIS)—which are explored in the next section of this chapter.

In dealing with evolving technologies like DNA analysis in the past, the creation of PCR was the real game-changer for law enforcement, and partnering with scientists from the private sector and the academic community was the lynchpin. Because of technological developments in DNA profiling from the discovery of PCR, investigators can now submit decades-old evidence for DNA analysis in criminal investigations known as cold cases. Through further analysis, not long after the invention of PCR whereby the use of DNA evidence analysis proliferated, law enforcement created new policies, re-examined old criminal cases, and changed how it responded to crime scenes and conducted investigations.

C. TIMELINE

One of the first notable investigations in which DNA analysis helped to solve a crime was in Leicestershire, England, in 1986. Law enforcement requested the assistance of Alec Jeffreys, a professor at the University of Leicester, who discovered that DNA could be used to identify perpetrators in cold cases.¹⁸⁰ Jeffreys, who had published his research on DNA profiling, had been regularly approached by attorneys requesting his analysis for paternity and immigration testing. Law enforcement contacted him to develop a profile of

¹⁷⁷ Arnaud, “Thirty Years of DNA Forensics.”

¹⁷⁸ Arnaud.

¹⁷⁹ Arnaud.

¹⁸⁰ Arnaud.

the perpetrator of the murder of a 15-year-old girl. A suspect had already confessed to the crime—an exciting development—but when Jeffreys identified and compared the DNA of this suspect with the DNA from the crime scene, the samples did not match. After a lengthy investigation that involved collecting thousands of individuals' DNA, the real suspect, Colin Pitchfork, was identified and linked to the crime, as well as the murder of another girl several years prior. The original suspect was eliminated from the investigation.¹⁸¹ This investigation was a landmark case in law enforcement's use of DNA analysis.

Also in 1986, police used DNA analysis in Orlando, Florida, to identify and arrest a perpetrator of the rape of a 27-year-old woman.¹⁸² Tommy Lee Andrews was convicted of breaking into the woman's home and raping and stabbing her. The victim positively identified Andrews during his trial, wherein a research biologist at the Massachusetts Institute of Technology, David Houseman, "testified that the DNA in the semen and in Mr. Andrews' blood matched."¹⁸³ DNA was the key to a successful investigation and prosecution in this case.

By 1987, the validity and acceptability of DNA evidence in criminal investigations were put to the test. In *People v. Castro*, the New York Supreme Court heard a 12-week argument about using DNA evidence in a criminal investigation where the defendant, Jose Castro, was accused of a gruesome double murder of a two-year-old and her mother.¹⁸⁴ In the investigation, detectives identified and analyzed a bloodstain on Jose Castro's watch, and scientists confirmed the blood sample belonged to one of the victims. The court decision began a movement among law enforcement to create a policy for training, certification, accreditation, standardization, and quality-control guidelines for DNA laboratories in America. The court determined that experts who offer opinions and present facts on DNA must be "qualified by knowledge, skill, experience, training or

¹⁸¹ Arnaud.

¹⁸² Associated Press, "Rapist Convicted on DNA Match," *New York Times*, February 6, 1988, <https://www.nytimes.com/1988/02/06/us/rapist-convicted-on-dna-match.html>.

¹⁸³ Associated Press.

¹⁸⁴ "The DNA 'Wars' Are Over," Frontline, accessed August 10, 2022, <https://www.pbs.org/wgbh/pages/frontline/shows/case/revolution/wars.html>.

education.”¹⁸⁵ The expert should be able to speak about the collection and testing procedures, including the PCR process, and offer insight into the results of DNA comparisons. Moreover, education, training, and experience must be provided to the court to determine the admissibility of the expert.¹⁸⁶

Following that landmark court decision, policies on responding to crime scenes to acquire DNA for analysis also had to be created. In 1992, the first report by the National Research Council, *DNA Technology in Forensic Science*, was released to the public to assist in matching suspects to DNA evidence at crime scenes.¹⁸⁷ In addition, the U.S. Congress passed the DNA Identification Act in 1994 to create an advisory committee for best practices in handling DNA in criminal investigations.¹⁸⁸ In addition, since the proliferation of DNA evidence in criminal prosecutions almost 40 years ago, law enforcement agencies have had to adapt in other ways to the expansion of DNA as an evolving technology. Websites like the National Criminal Justice Reference Service guide law enforcement in identifying, collecting, transporting, and storing DNA samples.¹⁸⁹

During the years of implementing and adopting DNA analysis into standard practice by law enforcement, the Federal Bureau of Investigation developed the NDIS in 1998 as a federal DNA repository.¹⁹⁰ The creation of NDIS followed the implementation of state laws that required law enforcement to collect DNA samples. These samples were obtained from offenders convicted of certain sexual and violent crimes.¹⁹¹ The idea behind NDIS was to share DNA information so that forensic intelligence could be disseminated, and both interstate and intrastate crimes could be solved more easily.

¹⁸⁵ National Research Council, Committee on DNA Forensic Science, “DNA Evidence in the Legal System,” in *The Evaluation of Forensic DNA Evidence* (Washington, DC: National Academies Press, 1996), 169, <https://www.ncbi.nlm.nih.gov/books/NBK232607/>.

¹⁸⁶ National Research Council, Committee on DNA Forensic Science.

¹⁸⁷ Stuart H. James and Jon J. Nordby, eds., *Forensic Science: An Introduction to Scientific and Investigative Techniques*, 2nd ed. (Boca Raton, FL: CRC Press, 2005), 667.

¹⁸⁸ James and Nordby, 668.

¹⁸⁹ “What Every Law Enforcement Officer Should Know about DNA Evidence,” National Criminal Justice Reference Service, accessed August 11, 2022, <https://www.ncjrs.gov/nij/DNAbro/evi.html>.

¹⁹⁰ Hanson, *The Use of DNA by the Criminal Justice System*.

¹⁹¹ Hanson.

The discovery of latent DNA at crime scenes caused law enforcement to examine its response procedures. In 2000, the United States Institute of Justice created a Technical Working Group on Crime Scene Investigation, comprising 44 scientific, academic, legal, and law enforcement experts, to standardize best practices for responding to crime scenes and handling, transporting, and analyzing physical evidence, including that which contains DNA.¹⁹² The working group drafted and published its results for state and local governments to establish a baseline for law enforcement agencies responding to crime scenes.

DNA analysis has also been employed by Canadian law enforcement in humanitarian missions. In 2018, the Royal Canadian Mounted Police (RCMP) created a National Missing Persons' DNA Program to aid in locating missing persons and identifying human remains.¹⁹³ The program allows investigators to use discretion in deciding when to enter a Canadian resident's DNA into its database, which was created as a voluntary humanitarian effort to identify missing loved ones.¹⁹⁴ Residents of Canada are under no obligation to participate in the program. The RCMP created the DNA database in response to over 62,000 missing persons complaints and 40 unidentified human remains each year.¹⁹⁵ Once written consent is provided, investigators use a blood sample or cheek swab as a control to enter family members' DNA into the database. Missing persons' DNA submission forms are available on a public website for residents to download and view.¹⁹⁶ Should a DNA analysis identify comparisons that conflict with information provided by family members, the information is not shared by the police, with few exceptions. This

¹⁹² National Institute of Justice, *Crime Scene Investigation: A Guide for Law Enforcement* (Washington, DC: Department of Justice, 2000).

¹⁹³ "National Missing Persons DNA Program Hits Milestone: 50th Case Solved with the Help of DNA," Royal Canadian Mounted Police, May 26, 2022, <https://www.rcmp-grc.gc.ca/en/news/2022/national-missing-persons-dna-program-hits-milestone-50th-case-solved-the-help-dna>.

¹⁹⁴ "A Family's Guide to the National Missing Persons DNA Program," Royal Canadian Mounted Police, October 29, 2020, <https://www.rcmp-grc.gc.ca/en/a-familys-guide-the-national-missing-persons-dna-program>.

¹⁹⁵ Royal Canadian Mounted Police, "DNA Program Hits Milestone."

¹⁹⁶ "Forms for the National DNA Data Bank," Royal Canadian Mounted Police, accessed February 6, 2023, <https://www.rcmp-grc.gc.ca/en/forensics/forms-the-national-dna-data-bank>.

practice prevents, for instance, past extramarital affairs from embarrassing or breaking up families.

In addition, the RCMP authored a guide to explain what happens to an individual's DNA and how it could be used to identify a missing loved one.¹⁹⁷ Canada's three public forensic laboratories support the National Missing DNA Program by appropriately processing DNA submissions and archiving the results. Having DNA samples from the voluntary database enhances forensic intelligence and enables law enforcement's mission of keeping its residents safe. While the RCMP's missing persons DNA database was created in response to a humanitarian mission, the voluntary forensic intelligence obtained from its residents is invaluable. According to Canada's National DNA Data Bank in 2021, the more than 500,000 DNA profiles stored have produced in excess of 73,000 matches used in law enforcement criminal investigations.¹⁹⁸ As a result of this initiative, in 2021 alone, 3,971 DNA offender hits and 356 forensic intelligence reports were generated.¹⁹⁹ In 2021, the RCMP's missing persons DNA database was responsible for over 1,200 voluntary submissions of the 23,136 law enforcement entries.²⁰⁰ Once a DNA entry is archived, it can produce forensic intelligence in investigations forever. Law enforcement could consider such archiving of cryptocurrency data to create future intelligence.

As of this writing, most large, modern law enforcement agencies and prominent local and city police departments have designated crime scene investigation units to collect DNA evidence. These units work with forensic scientists to analyze the DNA evidence recovered from crime scenes for evidentiary value. Analyzed DNA samples are routinely archived in state and federal DNA repositories for comparisons in the future. Many police departments in America have increased their agencies' capability to adapt this technology

¹⁹⁷ "Guide to the Victims Index and Voluntary Donors Index of the National DNA Data Bank of Canada," Royal Canadian Mounted Police, February 17, 2021, <https://www.rcmp-grc.gc.ca/en/forensics/guide-the-victims-index-and-voluntary-donors-index-the-national-dna-data-bank-canada>.

¹⁹⁸ "The National DNA Data Bank of Canada—Annual Report 2020–2021," Royal Canadian Mounted Police, March 7, 2022, <https://www.rcmp-grc.gc.ca/en/the-national-dna-data-bank-canada-annual-report-20202021>.

¹⁹⁹ Royal Canadian Mounted Police.

²⁰⁰ Royal Canadian Mounted Police.

by having dedicated crime scene investigation units collect DNA from crime scenes and trained forensic scientists analyze the evidence. State and local agencies have created policies and procedures for best practices in accordance with federal standards.

In 2019, the Golden State Killer was identified and brought to justice through genetic genealogy—a search for a biological family member to gain an investigative lead—enabled by DNA analysis. Law enforcement served a warrant for data from the private DNA repository GEDmatch and searched its entire database for the suspect’s familial DNA.²⁰¹ While the courts agreed with the actions of law enforcement, privacy advocates deemed the use of such data an overstep. The court decision allows state and local law enforcement to search other recognized DNA databases like 23andMe and Ancestry.com.²⁰² Privacy advocates are likely to argue the government is overreaching and creating mass surveillance of its citizens’ DNA.

Since the proliferation of DNA analysis, private advocacy groups have assisted in exonerating wrongful convictions using the same DNA technology. Known as the Innocence Project, the organization has used DNA to exonerate 375 people wrongfully convicted of crimes including more than 100 murders.²⁰³ See Figure 10 for a detailed timeline of evolving DNA technologies in criminal investigations.

²⁰¹ Jocelyn Kaiser, “A Judge Said Police Can Search the DNA of 1 Million Americans without Their Consent. What’s Next?,” *Science*, November 7, 2019, <https://www.science.org/content/article/judge-said-police-can-search-dna-millions-americans-without-their-consent-what-s-next>.

²⁰² Kaiser.

²⁰³ “DNA Exonerations in the United States,” Innocence Project, accessed August 11, 2022, <https://innocenceproject.org/dna-exonerations-in-the-united-states/>.

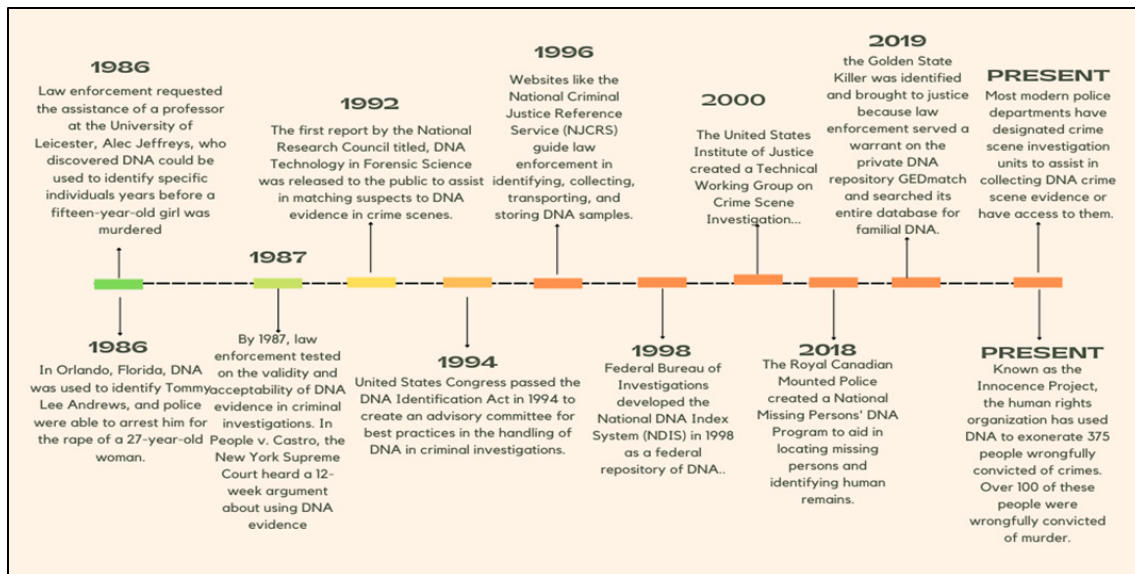


Figure 10. DNA Timeline

Law enforcement has shown it can embrace private partnerships to implement technology to solve crimes. ANDE Corporation is currently changing the game for law enforcement by developing and implementing rapid DNA technology to produce results from crime scenes without delay.²⁰⁴ The technology will enable law enforcement to solve investigations faster and exonerate the innocent quickly, so resources may be allocated differently when investigative leads are incorrect.

D. CONCLUSION

Law enforcement agencies have adapted to new and evolving technologies over time. Analyzing how DNA collection and analysis occurred can aid law enforcement in understanding cryptocurrency. It is an excellent way to equip state and local law enforcement with the impetus for organizational change. Law enforcement has created specialty units, developed policies, created working groups, and routinely collaborated with federal partners. State and local law enforcement will likely follow a similar historical

²⁰⁴ “Breaking the Cycle of Crime: ANDE Is Changing the Paradigm in Law Enforcement,” ANDE, accessed January 12, 2023, <https://www.ande.com/law-enforcement/>.

path to develop cryptocurrency guidelines successfully. See Table 1 for a summary of DNA analysis in this chapter.

Table 1. DNA Analysis

		Example	Key Effort/Block
Barriers	Legal	Legal frameworks and court decisions	No federal or state laws guided the use of DNA in criminal investigations.
	Knowledge	Law enforcement trained and educated in DNA analysis	Private sector and academia were the only partners with knowledge of DNA.
	Policy	Existence of law enforcement policies and best practices	No standardized or uniform policies for DNA analysis guided criminal investigations.
Drivers/Responses	Legal	1987 <i>People vs. Castro</i> , New York Supreme Court decision	Court decision established rules for court testimony and mandated the qualifications of knowledge, skill, experience, training, or education.
	Knowledge	National Criminal Justice Reference Service	A website was used to guide law enforcement in identifying, collecting, transporting, and storing DNA samples.
	Policy	U.S. Institute of Justice's Technical Working Group on Crime Scene Investigation	A group of 44 scientific, academic, legal, and law enforcement experts came together to standardize best practices for responding to crime scenes and handling, transporting, and analyzing physical evidence, including that which contains DNA, for state and local law enforcement.

THIS PAGE INTENTIONALLY LEFT BLANK

V. GAP ANALYSIS

The previous chapters have shown the increasing use of cryptocurrency by nation-state actors, terrorists, and criminals to commit crimes mostly anonymously and law enforcement's inability to recognize, understand, and combat it. In this context, this chapter applies a gap analysis, a formal process commonly used to identify steps to close the gap between the desired state and the current state of law enforcement knowledge to make it more effective at investigating crimes involving cryptocurrency. As defined by Langford et al., professors at the Naval Postgraduate School,

Gap Analysis is an assessment tool that compares a system's actual performance with its potential. What you desire versus what you have is, in essence, a Gap. The gap is as much the relationship between what is perceived to be important and the derived difference between performance and expectations.²⁰⁵

Clark and Estes find that organizations experience three fundamental performance gaps: knowledge, motivation, and organizational barriers.²⁰⁶ In addition, they underscore the significant role organizational culture plays in increasing organizational performance. These sources provide a framework for conducting a gap analysis, which has guided this thesis.

Existing literature shows that addressing cryptocurrency-enabled crimes requires adopting new technologies and policies. This transition requires state and local law enforcement to prioritize organizational change. Change is hard. Although the literature suggests that motivation, knowledge, and policy changes are necessary, it remains unclear how state and local law enforcement agencies can prepare and organize to respond to and investigate cryptocurrency crimes. The possible solution to these issues necessitates organizational change at the state and local levels. Much scholarly literature has confirmed that this problem exists, but none of it addresses the root causes. The main purpose of this chapter is to use gap analysis to identify areas of improvement and make logical

²⁰⁵ Langford et al., *Gap Analysis*, 1.

²⁰⁶ Clark, *Turning Research into Results*.

recommendations. The table at the conclusion of this chapter identifies four gaps, illustrating a significant disparity in standardizing practices between DNA analysis and cryptocurrency.

A. DESIRED STATE

This section discusses the best possible outcome for state and local law enforcement when dealing with cryptocurrency. Whenever digital currency emerges in investigations, each agency should implement best practices and know how to identify cryptocurrency wallets, understand cryptocurrency transactions, and share cryptocurrency intelligence with other agencies, including the federal government. Solving criminal investigations and sharing cryptocurrency intelligence remain the key objective. Numerous scholars have concluded that intelligence-sharing reduces crime and contributes to a safer homeland security environment.²⁰⁷ Finally, as stated by Stuart James and Jon Nordby in their book on forensic science, the criminal justice system aims both to identify the truth for the courts and to protect the innocent from false accusations.²⁰⁸ To contribute to the overall mission of the criminal justice system in understanding the truth behind certain cryptocurrency-related crimes, state and local law enforcement must prepare to incorporate this technology into their organizations. State and local governments have identified and applied best practices in collecting and archiving traditional digital evidence, such as computer or mobile device evidence. The method also applies to evidence on the internet and social media. Sridhar, Bhaskari, and Avadhani have organized best practices for cataloging digital evidence into four phases: identification, acquisition, analysis, and reporting (see Figure 11).²⁰⁹

²⁰⁷ Diego Esparza and Thomas C. Bruneau, “Closing the Gap between Law Enforcement and National Security Intelligence: Comparative Approaches,” *International Journal of Intelligence and Counterintelligence* 32, no. 2 (2019): 322–53, <https://doi.org/10.1080/08850607.2018.1522219>.

²⁰⁸ James and Nordby, *Forensic Science*, 4.

²⁰⁹ N. Sridhar, D. Lalitha Bhaskari, and P. S. Avadhani, “18: Plethora of Cyber Forensics,” *International Journal of Advanced Computer Science and Applications* 2, no. 11 (2011), <https://doi.org/10.14569/IJACSA.2011.021118>.

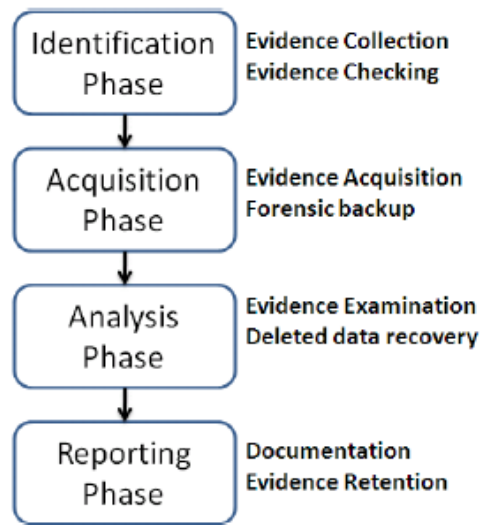


Figure 11. Process for Cataloging Digital Evidence.²¹⁰

In the best of circumstances, state and local governments should follow similar guidelines in identifying, acquiring, analyzing, and reporting cryptocurrency evidence.

1. Knowledge Needed

As noted in Chapter I of this thesis, the literature recognizes that investigators tasked with solving crimes that employ newer technologies like cryptocurrency must understand them. For example, investigating crimes like computer network intrusions requires knowledge of cryptocurrency because ransomware may be at the heart of the crime. These crimes remain among the top threats to the U.S. homeland security enterprise.²¹¹ The literature indicates that cryptocurrency crimes are significant, complicated to comprehend, and challenging for police to become adept at managing. As demonstrated previously, cryptocurrency has been increasingly linked to traditional crimes.

Beyond the desire to solve more investigations, increased knowledge would facilitate cryptocurrency intelligence-sharing. Whether an actual crime can be solved by

²¹⁰ Source: Sridhar, Bhaskari, and Avadhani, 111.

²¹¹ Attorney General's Cyber Digital Task Force, *Cryptocurrency Enforcement Framework*.

state and local law enforcement is irrelevant when it comes to intelligence-sharing. Many criminal investigations contain vital information that can be shared between law enforcement agencies, even if the original crime remains unsolved. Crimes involving cryptocurrency are not different. Mark Lowenthal defines *intelligence* as known secret information collected, processed, and narrowed to meet a specific need.²¹² He maintains, “All intelligence is information; not all information is intelligence.”²¹³ Intelligence is critical in keeping America safe and protecting its homeland security environment. According to Lowenthal, the “United States intelligence system remains the largest and most influential in the world—as model, rival, or target.”²¹⁴ National security intelligence can be derived from many sources, but state and local law enforcement is a crucial source because it regularly collaborates with federal partners in intelligence regarding gun crimes, human source development, cyber threats, and open-source social media, to name a few. Federal, state, and local law enforcement would like intelligence-sharing at the same level for cryptocurrency intelligence-sharing.

Cryptocurrency intelligence cannot be analyzed if it is not collected and dots are not connected. Erik Dahl, a subject-matter expert on intelligence and distinguished professor at the Naval Postgraduate School since 2008, details the concept of signals versus noise in his book *Intelligence and Surprise Attack*.²¹⁵ Dahl explains that intelligence failures can be partly attributed to losing essential signals among the noise and analysts’ failing to “connect the dots.”²¹⁶ He believes that strategic intelligence remains critical to the fight against terrorism, arguing that it needs to be precise and timely to be successful. State and local law enforcement agencies can provide meaningful and strategic cryptocurrency intelligence once they fully understand the process of identifying, cataloging, and disseminating meaningful information to the federal government. It bears

²¹² Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, 8th ed. (Thousand Oaks, CA: CQ Press, 2020).

²¹³ Lowenthal, 1.

²¹⁴ Lowenthal, 11.

²¹⁵ Erik J. Dahl, *Intelligence and Surprise Attack: Failure and Success from Pearl Harbor to 9/11 and Beyond* (Washington, DC: Georgetown University Press, 2013).

²¹⁶ Dahl, 175.

repeating that to connect the dots requires collecting the dots, and state and local officials play a role in separating the signals from the noise.

A uniform intelligence- and information-sharing policy adopted by a state and local law enforcement agency—including the use of suspicious activity reporting when illegal cryptocurrency is identified—would help identify nefarious and illicit cryptocurrency wallets used by terrorists, transnational organized crime groups, and ordinary criminals. The shared information could lead to more substantial prosecutions for all agencies and make the overall homeland security environment safer when digital currencies are involved. Sharing intelligence can also yield investigative leads and provide decision-makers with an overall view of threats so that mitigation efforts can be developed and implemented.

Fusion centers can play a significant role in cryptocurrency intelligence-sharing. As Sam McGhee notes in *Police Chief Magazine*, fusion centers are one of the most significant information-sharing developments since the 9/11 attacks.²¹⁷ In his article, he indicates, “State and local law enforcement agencies are at the forefront of this evolution, yet they may not fully recognize how crucial their role is.”²¹⁸ Most state and local law enforcement agencies are briefed daily on actionable intelligence from federal agencies. For this reason, fusion centers should be at the center of cryptocurrency intelligence analysis and dissemination.

The literature also recognizes that state and local law enforcement needs to join efforts with colleges and universities to reduce cryptocurrency-related crimes. After all, as identified in Chapter IV of this thesis, academia was instrumental in shaping DNA analysis into one of the essential tools for solving many violent crimes.

²¹⁷ Sam McGhee, “Impacting the Evolution of Information Sharing in the Post-9/11 United States,” *Police Chief Magazine*, February 1, 2015, <https://www.policechiefmagazine.org/impacting-the-evolution-of-information-sharing-in-the-post-911-united-states/>.

²¹⁸ McGhee.

2. Organizational Policies

Law enforcement should seek organizational policies and procedures to identify and acquire cryptocurrency when it is used in crimes, just as it developed policies and procedures in DNA analysis. Likewise, law enforcement also needs administrative policies for training and continued education in technological areas, including cryptocurrency. A well-educated, trained team of investigators at the state and local levels will solve more crimes and be more cognizant of the tools available to protect the public. A better-educated and trained team of investigators at the state and local level will make fewer mistakes in the field, be more efficient in managing investigations, and share more meaningful intelligence with federal partners. Creating organizational policies and procedures in cryptocurrency could reduce risks to the organization and serve the citizen better. The probability of solving criminal investigations also increases.

Understanding a simple risk management cycle can provide state and local law enforcement decision-makers with comfort in technologies like cryptocurrency to drive organizational change. Douglas Hubbard's simplified risk management cycle applies to creating positive organizational change by requiring technology-based training for state and local law enforcement:

- Identify Risks (e.g., Nefarious Use of Cryptocurrency)
- Assess Risks
- Identify Risk Mitigation Approaches
- Assess Expected Risk Reduction and Costs of Mitigation Methods
- Select and Implement Mitigation Methods²¹⁹

If the risk to the citizen is cryptocurrency's nefarious use, Hubbard's risk management cycle could prove valuable in minimizing it. In this case, the risk does not spur organizational change, and with rising cyber-related crimes, overall crime grows. Law enforcement is seemingly struggling to investigate crimes related to cryptocurrency, which contrasts with its fundamental benchmark—to solve crimes for its citizens.

²¹⁹ Douglas W. Hubbard, *The Failure of Risk Management: Why It's Broken and How to Fix It*, 2nd ed. (Hoboken, NJ: Wiley, 2020), 290.

Eugene Bardach and Eric Patashnik's *Practical Guide for Policy Analysis* outlines an eight-step roadmap for decision-making and analysis of policy.²²⁰ They outline the following steps, which need not adhere to this order:

- Define the Problem
- Assemble Some Evidence
- Construct the Alternatives
- Select the Criteria
- Project the Outcomes
- Confront the Trade-Offs
- Stop, Focus, Narrow, Deepen, and Decide!
- Tell Your Story²²¹

Bardach and Patashnik's method for analyzing policy is similar to that for risk management.

The takeaway from the risk management and policy analysis research is that state and local law enforcement should recognize that cryptocurrency is a risk to citizens, and unprepared organizations increase that risk. Incorporating a policy for education and seizing illegal cryptocurrency in criminal investigations seem logical and appropriate considering the proliferation of such crimes.

B. CURRENT STATE

This section briefly discusses state and local law enforcement's current response to proliferating technologies like cryptocurrency. A basic understanding of current knowledge, training, and education is beneficial in analysis, and in understanding the current state, logical recommendations can be drawn from the research.

1. Law Enforcement's Current Knowledge, Training, and Education

As mentioned in the previous chapters, many state and local law enforcement agencies lack the knowledge to investigate cryptocurrency employed in crimes in

²²⁰ Eugene Bardach and Eric M. Patashnik, *A Practical Guide for Policy Analysis: The Eightfold Path to More Effective Problem Solving*, 6th ed. (Washington, DC: CQ Press, 2020), xvi.

²²¹ Bardach and Patashnik, xvi.

America.²²² Although cryptocurrency appears to be a key element of many cybercrimes, criminals increasingly use it in traditional crimes because they can convert it into conventional money.

In their article for the *International Journal of Intelligence and Counterintelligence*, Diego Esparza and Thomas Bruneau point to the numerous scholars who have concluded that intelligence-sharing reduces crime and contributes to a safer homeland security environment.²²³ However, they also suggest that most police agencies have no formal strategies for collecting and disseminating intelligence.²²⁴ The authors argue that intelligence differs by type, e.g., national security versus criminal intelligence. Esparza and Bruneau define *intelligence-led policing*, which originated in criminal intelligence, as “the gathering of data and statistical analysis to predict criminal activities and possible locations, and thereby help deploy patrols to dissuade crime in those regions.”²²⁵ Many investigative agencies have adopted a portion of the intelligence-led policing model, but few have focused their efforts on cyber-related crimes or crimes involving cryptocurrency. According to Esparza and Bruneau, “Without relevant training police forces can have no practical role in intelligence work. In the U.S., police officers, whether members of large forces or small town units, are minimally trained in intelligence gathering.”²²⁶ In this way, police need training not only on cryptocurrency but also within the context of intelligence-led policing.

State and local police departments are not supporting the use of suspicious activity reports. Interestingly, according to Esparza and Bruneau, “Although some sporadic support exists for the National Suspicious Activity Reports [SAR] Initiative, and larger city police departments frequently support collection of national security intelligence, smaller departments rarely know what SAR is, what it means, or how to enhance it.”²²⁷ A SAR is

²²² Police Executive Research Forum, *New National Commitment Required*.

²²³ Esparza and Bruneau, “Closing the Gap between Law Enforcement and National Security.”

²²⁴ Esparza and Bruneau.

²²⁵ Esparza and Bruneau, 325.

²²⁶ Esparza and Bruneau, 332.

²²⁷ Esparza and Bruneau, 333.

a mechanism for state and local law enforcement to report a suspicious event and provide the information to federal agencies for analysis to determine whether it requires additional investigation. If state and local law enforcement agencies are not completing SARs, the intelligence may not be disseminated properly.

An insufficient focus on intelligence-sharing in police academy training further complicates the issue. As indicated by Esperanza and Bruneau,

Most officers train for six months in police academies, with two months of field training, little of which is related to intelligence. Although 95 percent of the academies provide basic training on terrorism-related topics, only 53 percent of those surveyed were preparing personnel for intelligence gathering. On average, officers receive 1,364 hours of training, of which only nine are dedicated to counterterrorism and intelligence.²²⁸

Annual law enforcement training on conducting searches and seizures, interacting with people in crisis, and adapting to new social norms is regularly mandated, helping reduce the risk or likelihood of violating a citizen's civil rights or using deadly force instead of de-escalating a situation. This risk-reduction training can decrease complaints and enhance community relationships, proven worthy endeavors and crucial training in modern-day policing. American police training also generally focuses on preliminary education to prepare new police officers for their careers in law enforcement.²²⁹ Nevertheless, federal agencies such as the National White Collar Crime Center provide free online training on cryptocurrency.²³⁰ Anecdotally, these training courses are robust and beneficial to students in law enforcement. In this way, gaps in police training could be addressed no matter where policer officers are in their careers.

2. Law Enforcement Organization

Law enforcement does not typically publish the existing training and educational levels of its investigators. For this reason, each agency's organizational policies are

²²⁸ Esparza and Bruneau, 332.

²²⁹ Semuels, "Society Is Paying the Price."

²³⁰ "Classroom Training," NW3C, accessed January 12, 2023, <https://www.nw3c.org/classroom-training>.

unknown for technology-related education in cryptocurrency. It is also unknown whether agencies possess procedures for identifying and seizing unlawful cryptocurrency. However, many policies and guidelines, as well as standardized training and education, outline how to respond to physical crime scenes and recover DNA evidence. Although DNA evidence is subject to the Frye standard in most jurisdictions, the recovery of digital evidence follows different protocols.²³¹

C. RESULTS AND FINDINGS

Based on the literature, there is a gap in police training nationally for continuing education and mandatory training in technological areas like cryptocurrency. The literature identifies the considerable focus on initial training to become a police officer and nothing on incorporating a technology-related curriculum like cryptocurrency into early training and education. No literature could be found to confirm whether state and local law enforcement has created or adopted new policies and standard operating procedures for identifying and seizing cryptocurrency. Despite law enforcement executives' agreeing that "crime has been changing, and law enforcement needs to catch up," the literature does not recognize that this significant change is the result of crimes increasingly involving cryptocurrency.²³² Scholars indicate that improvements are needed to report intelligence of illegal cryptocurrency use to Fusion Centers, so it can be disseminated. In analyzing how DNA changed the way law enforcement responded to crimes, local law enforcement can draw from the past to make logical recommendations to streamline the response to crimes involving cryptocurrency (see Table 2).

²³¹ Robert A. Fiatal, "DNA Testing and the Frye Standard," *FBI Law Enforcement Bulletin* 59, no. 6 (June 1990), <https://www.ojp.gov/ncjrs/virtual-library/abstracts/dna-testing-and-frye-standard>.

²³² Police Executive Research Forum, *New National Commitment Required*, 4.

Table 2. Comparative Analysis: DNA versus Cryptocurrency

	DNA	Outcome	Cryptocurrency	Recommendation
Technical training and education requirements	Present	The 1987 <i>People vs. Castro</i> New York Supreme Court decision mandates requirements.	Absent	Create technical and training requirements.
Legal requirements	Present	The 1987 <i>People vs. Castro</i> New York Supreme Court decision mandates requirements (Frye Standard).	Absent	Follow guidelines like those of Sridhar, Bhaskari, and Avadhani: identification, acquisition, analysis, and reporting.
Policy requirements	Present	In 1996, the United States DNA Identification Act created an advisory committee for developing uniform standards and policies.	Absent	Develop uniform policy requirements for cryptocurrency identification and collection.
Intelligence shared with partnering agencies for collaboration	Present	In 1998, the FBI created NDIS as a repository for DNA profiles for information-sharing.	Absent	Consider creating a repository for cryptocurrency profiles, and share intelligence with partnering agencies.

As illustrated in Table 2, there is a significant disparity in standard practices between DNA analysis and cryptocurrency. This gap analysis shows four unique deficiencies that can be addressed moving forward. Using DNA analysis as a guide for other evolving technologies like cryptocurrency, the final chapter provides useful recommendations for law enforcement agencies.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CHANGING LAW ENFORCEMENT ORGANIZATIONS TO COUNTER CRYPTOCURRENCY CRIME

This final chapter aims to answer the research questions by integrating current knowledge about cryptocurrency to make logical recommendations for state and local law enforcement. Law enforcement agencies have already applied some of these principles to other areas of concern in the past, and cryptocurrency issues and crimes are closely related. First, this chapter examines the instrumental concepts of issue selling and social identity theory—regarding the research question about barriers and drivers to organizational change—in responding to and investigating cryptocurrency. Then, this chapter summarizes the major findings of the thesis.

A. ISSUE SELLING

Issue selling could assist law enforcement policymakers in addressing the rise in cryptocurrency-related crimes. In short, an individual who successfully sells cryptocurrency's crime role to executive leadership in law enforcement could bring about successful organizational change. According to Lauren Keller Johnson in an article for the *MIT Sloan Management Review*, issue selling is “the process by which individuals within an organization bring ideas or concerns, solutions, and opportunities together in ways that focus others’ attention and invite action. The process represents the earliest stage of change—that of focusing attention on an issue.”²³³ The general idea is that mid-level managers can propose change within an organization to top-level management by having a clear plan to identify an issue and offer a solution.²³⁴ According to Johnson, the desired outcome can be accomplished in myriad ways, from sending a survey to stakeholders, to identifying a policy change issue, to breaking a significant problem into more minor issues

²³³ Lauren Keller Johnson, “Issue Selling in the Organization,” *MIT Sloan Management Review*, April 15, 2002, <https://sloanreview.mit.edu/article/strategy-issue-selling-in-the-organization/>.

²³⁴ Johnson.

that can be resolved independently.²³⁵ This theory inspires top-level organizational leaders to embody ideas from mid-level managers to implement change successfully.

In further research, Jennifer A. Howard-Grenville concludes that issue selling can positively affect an organization.²³⁶ She conducted extensive research into the organizational practices of Chipco, one of the largest manufacturers of microchips, before producing findings for top-level management.²³⁷ The conclusion of her study emphasizes issue sellers' value as insiders:

The value that issue sellers bring to their organizations lies in their knowledge of, and often a passion for, a new issue that has potential strategic consequences. The dilemma for issue sellers is how to advance such issues in an organizational context in which the dominant meanings and norms may blind others to the issues, their consequences, and the value in addressing them.²³⁸

The theory supports state and local law enforcement's identifying those in its respective agencies best suited to drive organizational change to respond to and investigate cryptocurrency.

In this thesis, the organizational field comprises state and local law enforcement agencies. Issue selling may have an apparent positive influence as a building block to create organizational change for state and local law enforcement to adapt to evolving technologies, including cryptocurrency, when used in criminal investigations. The theory suggests law enforcement agencies should identify the most qualified mid-level managers within their organizations and empower them to assist in creating positive change by institutionalizing policies, education, training, and partnerships. In order for an issue seller to be successful in the proliferation of cryptocurrency, one possibility is to create a bigger

²³⁵ Johnson.

²³⁶ Jennifer A. Howard-Grenville, "Developing Issue-Selling Effectiveness over Time: Issue Selling as Resourcing," *Organization Science* 18, no. 4 (August 2007): 560–77, <https://doi.org/10.1287/orsc.1070.0266>.

²³⁷ Howard-Grenville.

²³⁸ Howard-Grenville, 574.

group of people to drive organizational change. Driving organizational change might mean creating a working group of stakeholders with the most intimate knowledge on the subject.

In practical terms, this group might represent issue selling for cryptocurrency in a law enforcement setting. To illustrate, in the event of repeated cyber incidents involving ransomware that encrypts computer systems, the malicious actors typically request cryptocurrency to decrypt the systems. On-scene investigators cannot effectively investigate the incidents because they are unfamiliar with cryptocurrency. First, they advise their supervisors of the ongoing issue. Then, the supervisors notify their officer-in-charge, who needs to brief executive management. In this case, the officer-in-charge is the issue seller driving organizational change to correct the problem by briefing agency heads with resources and decision-making power. That person could create a working group and collaborate on the needs of the agency before requesting a briefing with executive leadership.

Whatever the agency's hierarchy, an issue seller is a person in the middle who can provide the most assistance in driving organizational change to better prepare the organization. Executives should listen to these individuals if they present an issue because they are most likely to interact with front-line and executive-level people.

B. SOCIAL IDENTITY THEORY

Social identity theory (SIT) offers additional solutions in the face of cryptocurrency crimes. According to David Brannan, Kristin Darken, and Anders Strindberg, the SIT framework can assist with understanding organizational culture—in this case, police culture—by exploring group dynamics and relationships between groups.²³⁹ As Brannan, Darken, and Strindberg indicate, belonging to a group is part of a person's identity.²⁴⁰ People join law enforcement to make a difference and keep communities safe, so group dynamics in police culture could be crucial in making progress toward handling

²³⁹ David Brannan, Anders Strindberg, and Kristin Darken, *A Practitioner's Way Forward: Terrorism Analysis* (Salinas, CA: Agile Press, 2014), 45–46.

²⁴⁰ Brannan, Strindberg, and Darken.

cryptocurrency cases knowledgeably for the public. As demonstrated in this thesis, the public pressures police executives and decision-makers to reduce violent crime.

SIT would suggest that because efforts among police executives usually fixate on reducing violent crime, the group dynamics within the organization translate into focusing only on that one thing. As defined by SIT, a group comprises “some people who are united around a common interest, purpose, or practice, and who think of themselves as connected in some way.”²⁴¹ Group dynamics can naturally fashion an ingroup–outgroup relationship.²⁴² For example, members of a homicide unit may form an ingroup within an organization and believe only homicide investigations are essential. The rest of the organization could become an outgroup from their perspective. The homicide unit ingroup could begin competing with other groups inside the organization for resources. The same group dynamics can be applied to intelligence-sharing among law enforcement agencies. The group with the best intelligence might not share its resources because it wants to be the best agency in the area.

Law enforcement executives should be aware of group dynamics and understand concepts like SIT to understand the balance necessary to lead an organization successfully. Cryptocurrency could be the motive behind a violent crime and may well be connected to traditional crime. Understanding SIT could motivate decision-makers to prioritize technology-related training for such things as cryptocurrency. Essentially, SIT could assist law enforcement executives in understanding their organizations better.

C. DISCUSSION, RECOMMENDATIONS, AND CONCLUSION

Bringing state and local law enforcement up to speed on cryptocurrency used in criminal investigations requires substantial work so that U.S. citizens are safer and that fewer cryptocurrency crimes take place. Some practical solutions might begin to reduce the number of crimes reported to the Internet Crimes Complaint Center—simultaneously

²⁴¹ Brannan, Strindberg, and Darken, 51.

²⁴² Brannan, Strindberg, and Darken.

aiding state and local law enforcement with crime reduction and contributing to the overall homeland security environment when cryptocurrency is involved.

1. Agency Investment in New Cryptocurrency Identification Technologies

State and local law enforcement should consider a policy and procedure on the use of private-sector cryptocurrency software to enhance agencies' capabilities. The development of PCR in DNA analysis helped law enforcement turn the corner in solving many criminal cases. The advent of DNA technology can be attributed to the hard work and dedication of scientists, investigators, and law professionals who quickly recognized the value of an evolving technology. The same could be said for cryptocurrency identification technologies.

Tremendous developments in cryptocurrency identification software programs can help the government identify users on a blockchain. Some authorities use third-party private software programs like Chainalysis to investigate cryptocurrency transactions and bring resolution to criminal and terrorist investigations.²⁴³ Chainalysis allows analysts to “flag” and monitor certain cryptocurrency blocks to identify users and generate investigative leads.²⁴⁴ These software products enable state and local law enforcement to track illegal cryptocurrency transactions linked to crimes. They also assist in identifying intelligence associated with unlawful cryptocurrency that can be analyzed and shared.

However, these programs have downsides as well benefits. For one, these cryptocurrency tracking programs cover only mainstream cryptocurrencies like Bitcoin, so they are not a perfect solution. Also, despite the availability of powerful identification tools, blockchain technology is so advanced that users can still avoid detection. To illustrate, cybercriminals on the dark web offer illicit computer network intrusion tools and services for sale. These criminals might negotiate a 20 percent cryptocurrency commission added to their blocks for customized software and services. Nevertheless, if the funds'

²⁴³ “Government Agencies,” Chainalysis, accessed January 12, 2023, <https://www.chainalysis.com/government-agencies/>.

²⁴⁴ Chainalysis.

recipients do not exchange this cryptocurrency for fiat currency, the criminally suspected blocks can collect cryptocurrency units in 20 percent commission-based increments without the possibility of identification. Analysts could use Chainalysis to flag and monitor the blocks that repeatedly receive a 20 percent cryptocurrency commission associated with dozens of ransom-paying victims. If any changes to the flagged blocks occur, Chainalysis will alert analysts, who can investigate the transactions further.

To avoid detection, illegal recipients could transfer the cryptocurrency to other forms of cryptocurrency. If a perpetrator repeats this step enough times, he can launder any amount of illegal cryptocurrency into something legitimate. In addition, someone could also use a tumbler, which mixes one cryptocurrency with other cryptocurrencies for a small fee to make it untraceable. A tumbler is probably best described as unregulated money laundering in cryptocurrency. After enough time and laundering/tumbling, illegal cryptocurrency can be transferred into its final currency, exchanged into fiat currency, or used for purchases. It might become so complicated that no one ever identifies the original owner. Law enforcement should know these software products' limitations and their incredible strengths.

Despite these limitations, partnering with enterprise software corporations like Chainalysis is a tremendous force multiplier in building agencies' capabilities. As with the creation of PCR, which enabled forensic scientists to collect and analyze DNA, the invention of cryptocurrency tracking programs like Chainalysis represents leaps in innovation and assists in bridging the knowledge gap. It could be challenging to investigate modern-day crimes involving cryptocurrency without the assistance of software products like Chainalysis.

2. Training Law Enforcement on U.S. Regulations for Traditional Financial Crimes

State and local law enforcement should consider a policy and procedure on the use of standardized training in traditional financial crimes as a prerequisite for cryptocurrency training to enhance agencies' capabilities. Law enforcement must become aware of traditional banking regulations to understand their application to cryptocurrency.

Cryptocurrency firms operating within the United States must follow anti-money laundering rules and requirements.²⁴⁵ These rules include the need to “know your customer,” whereby the proper identification of a customer is necessary to create and use an account. The institution must also report suspicious activity and transactions exceeding certain classified financial limits. By understanding traditional banking regulations, a more seamless transition to understanding cryptocurrency will occur.

Once an agency understands traditional banking regulations, it can apply them to cryptocurrency. One of the biggest cryptocurrency exchange companies in the United States is Coinbase, based in Wilmington, Delaware.²⁴⁶ It exchanges fiat currency for Bitcoin and Ethereum, meaning anyone can join this service and begin trading cryptocurrency for a small fee.²⁴⁷ Coinbase is not the only company through which someone can purchase Bitcoin. Other exchanges like Kracken and Gemini exchange crypto and offer similar services. Any Apple iPhone user can download and install Coinbase’s App on one’s device, as shown in Figure 12.²⁴⁸

²⁴⁵ Mark P. Keightley and Andrew P. Scott, *Cryptocurrency Transfers and Data Collection*, IF11910 (Washington, DC: Congressional Research Service, 2021).

²⁴⁶ Jeff Kauflin, “Coinbase’s Public Stock Listing Creates a Multibillion Dollar Windfall for Founders—Now It Faces Five Big Threats,” *Forbes*, April 14, 2021, <https://www.forbes.com/sites/jeffkauflin/2021/04/14/coinbases-ipo-creates-a-multibillion-dollar-windfall-for-founders-now-it-faces-five-big-threats/?sh=5362938261ff>.

²⁴⁷ “Explore the Cryptoeconomy,” Coinbase, accessed November 6, 2021, <https://www.coinbase.com/price>.

²⁴⁸ “Coinbase: Buy Bitcoin & Ether,” Apple App Store, accessed November 16, 2021, <https://apps.apple.com/us/app/coinbase-trade-btc-eth-shib/id886427730>.

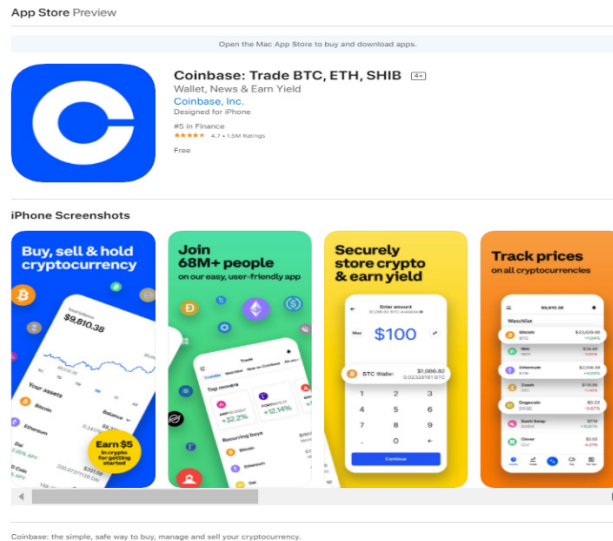


Figure 12. Coinbase on the Apple App Store.²⁴⁹

Since Coinbase’s headquarters is in the United States, it must adhere to know-your-customer rules and identify a user to cooperate with banking regulations—if the user resides in the United States.²⁵⁰ Whenever cryptocurrency is exchanged for U.S. currency, Coinbase must generate a bank record.

Although identification on such exchanges would assist homeland security professionals, more savvy cryptocurrency users might use a non-U.S. exchange. Notably, the largest cryptocurrency exchange globally, Binance, is headquartered outside the United States.²⁵¹ It remains under investigation by the Department of Justice and other nations for criminal activity, including insider trading and money laundering.²⁵² Coinbase has different regulations for international clients, and verifying foreign documents often proves

²⁴⁹ Source: Apple App Store.

²⁵⁰ Muzinich, “America’s Crypto Conundrum.”

²⁵¹ Emily Flitter, “The World’s Biggest Crypto Exchange Still Lacks U.S. Footing,” *New York Times*, August 19, 2021, <https://www.nytimes.com/2021/08/19/business/binance-cryptocurrency-exchange-ipo.html>.

²⁵² Tom Schoenberg, “Binance Faces Probe by U.S. Money-Laundering and Tax Sleuths,” *Bloomberg*, May 13, 2021, <https://www.bloomberg.com/news/articles/2021-05-13/binance-probed-by-u-s-as-money-laundering-tax-sleuths-bore-in>.

difficult.²⁵³ Criminals might use fraudulent foreign documents to obtain a legitimate Coinbase account and launder illegally obtained cryptocurrency. Anecdotal, fraudulent foreign documents are available for purchase on the dark web and could be used to bypass these security measures. As mentioned in the example, savvy users can quickly transfer between multiple varieties of cryptocurrency to avoid identification or use a tumbler. Thus, no perfect solution counters all illegal cryptocurrency efforts.

In their report, Pascal Sprenger and Franziska Balsiger offer several reasonable solutions for handling the evolution of cryptocurrency:

- Strengthening [anti–money laundering] procedures at financial institutions . . .
- Transaction monitoring . . .
- Improving regulation . . .
- Regulating cryptocurrency exchanges, especially advanced digital exchanges and exchanges offering to purchase primary cryptocurrencies . . . [and]
- Using blockchain as a solution.²⁵⁴

3. Leveraging Federal Partnerships and the Educational Sector in Law Enforcement Training

State and local law enforcement should consider a policy and procedure on creating federal partnerships to enhance agencies’ capabilities. Training and partnerships for law enforcement are critical in learning about and identifying cryptocurrency. The U.S. government has progressively offered local and state law enforcement training to disrupt and identify crypto criminals.²⁵⁵ The following federal agencies provide free training on cryptocurrency, but others may exist:

- National White Collar Crime Center, available at <https://www.nw3c.org>

²⁵³ Coinbase, “Explore the Cryptoeconomy.”

²⁵⁴ Pascal Sprenger and Franziska Balsiger, *Anti–Money Laundering in Times of Cryptocurrencies* (Zurich: KPMG, 2018).

²⁵⁵ “Online Training,” NW3C, accessed January 12, 2023, <https://www.nw3c.org/online-training>.

- Federal Virtual Training Environment, available at <https://niccs.cisa.gov/training>
- Northeast Counterdrug Training Center, available at <https://nctc.counterdrug.org>
- National Computer Forensics Institute, available at <https://www.ncfi.usss.gov>

Partnerships with federal agencies are also essential for information information-sharing and dissemination. The Federal Bureau of Investigation, the Secret Service, the Customs and Border Patrol's Homeland Security Investigations, and FinCEN all have reputable task forces with state and local law enforcement and have been progressive in incorporating cryptocurrency into investigations in the New York/New Jersey region. The use and application of task forces are not new. They have been successfully implemented to combat all criminal behaviors, including gun violence, crime, narcotics, and human trafficking. For example, the Federal Bureau of Investigation's Regional Computer Forensic Laboratories use the task force concept for computer forensics.

Intelligence-sharing in cryptocurrency needs to be prioritized. Ideally, the cryptocurrency response effort should be intelligence driven, using state and local fusion centers to prioritize intelligence collection, analysis, and dissemination. The Internet Crime Complaint Center could also consider supplying real-time crime information, including cryptocurrency intelligence, directly to fusion centers for trends and intelligence used in local criminal investigations. By combining these resources with other mechanisms already in place for crime reporting, organizational change may occur and help to reduce crime where illegal cryptocurrency is involved.

State and local law enforcement should also consider partnering with the educational sector, such as local colleges and universities, to gain the advice of academics on cryptocurrency and empower law enforcement with more knowledge. Reciprocally, academia may leverage law enforcement data to adjust the curricula for criminal justice programs if they do not already include evolving technologies like cryptocurrency. If

cryptocurrency education begins earlier, the problem could drastically diminish in four to five years when criminal justice graduates enter the police force.

For all new investigators, state and local law enforcement should consider creating mandated training on evolving technologies, including cryptocurrency. Seasoned investigators could also attend the same curriculum. The New Jersey Police Training Act identifies the need to improve training and education for law enforcement in New Jersey.²⁵⁶

The Legislature of New Jersey hereby finds and declares that a serious need for improvement in the administration of local and county law enforcement exists in order to better protect the health, safety and welfare of its citizens; that police work, a basic adjunct of law enforcement administration, is professional in nature, and requires proper educational and clinical training in a State whose population is increasing in relation to its physical area, and in a society where greater reliance on better law enforcement through higher standards of efficiency is of paramount need; that the present need for improvement can be substantially met by the creation of a compulsory educational and training program for persons who seek to become permanent law enforcement officers wherein such persons will be required, while serving in a probationary capacity prior to permanent appointment, to receive efficient training in this profession provided at facilities selected, approved and inspected by a commission created for such purpose; and that by qualifying and becoming proficient in the field of law enforcement such persons shall individually and collectively better insure the health, safety and welfare of the citizens of this state in their respective communities.²⁵⁷

Also, as recognized by the New Jersey Legislature,

The amount and quality of a policeman's education often determines the value of his contribution to the community, and the degree of proficiency with which he performs his duties. An educated policeman is a better public employee since his viewpoint, understanding, and awareness have been broadened beyond the narrow confines of police work.²⁵⁸

The best possible outcome would be to encourage a high technology crimes investigations course, including training on cryptocurrencies for all new investigators and

²⁵⁶ New Jersey Police Training Act, N.J. Stat. Ann. § 52:17B-66 (1965), https://www.state.nj.us/lps/dcj/njptc/pdf/njsa52_17b-69-2.pdf.

²⁵⁷ New Jersey Police Training Act, § 52:17B-66.

²⁵⁸ New Jersey Police Training Act, § 52:17B-71.2

detectives. Also, all existing investigators and detectives should be strongly encouraged to receive the same education, if possible. Since technology and its application to the criminal environment are forever evolving, the curriculum would also grow with these ever-changing technologies. This training would have a positive value in reducing crimes and sharing intelligence, in addition to preparing investigators for the proliferation and implementation of cryptocurrency in American commerce. Policies for each state and local law enforcement agency should also be developed to share cryptocurrency intelligence from criminal investigations with state and local fusion centers.

Law enforcement should become proficient in identifying cryptocurrency wallets, including mobile wallets (when legally permitted to search a device). Figure 13 illustrates several examples of cryptocurrency icons commonly found on mobile devices.



Figure 13. Mobile Wallet Examples

Ideally, once a criminal's cryptocurrency account is known, the information should be disseminated to federal partners if there is reason to believe the intelligence could benefit the homeland security environment. State and local law enforcement can accomplish this goal by using existing suspicious activity reporting mechanisms between federal, state, and local law enforcement agencies.

4. Developing a Standard Policy and Procedure for Encountering and Seizing Illegal Cryptocurrency

State and local law enforcement agencies should develop and implement a standard policy and procedure to identify and seize cryptocurrency in an investigation linked to criminal activity. A generic example of a policy and procedure for seizing cryptocurrency appears in Table 3 for guidance; however, each agency should develop a plan following its standard operating procedures.

Table 3. Policy Example: Seizure of Cryptocurrency

SEIZURE OF CRYPTOCURRENCY
Appropriate language should be included in a judicial or legal order if an agency expects a seizure of unlawful cryptocurrency. Personnel should work with prosecutors and their legal team to determine the appropriate direction. When the seizure of unlawful cryptocurrency is unexpected, a government official can seize it if there is probable cause that the cryptocurrency is criminal evidence of unlawful activity or criminal proceeds of unlawful activity. NOTE: Not all cryptocurrency exchanges cooperate with government agencies due to no existing regulations. In addition, not every cryptocurrency exchange requires proper legal documentation for customers to obtain and create a cryptocurrency account. Finally, records are not guaranteed to exist because they are unregulated. When seizing cryptocurrency managed by a cryptocurrency exchange that does not cooperate with government agencies, or when the cryptocurrency exchange does not comply with the U.S.-based legal process, the seizing government agency may use the following procedure. Explanation of Storage Wallets: a “cold” offline wallet is a wallet for storing cryptocurrency. This digital wallet is not connected to the internet, and it offers additional data protections from computer network vulnerabilities that exist while connected to the internet. The opposite is a “hot” online wallet, whereby the cryptocurrency assets are held within a company and linked to a software application on a computer or phone. 1. Use an authorized agency’s digital device to create a government-controlled cryptocurrency cold wallet. A new cold wallet should be created for each suspect’s wallet subject to seizure.

2. Document the amount of seized cryptocurrency. Cryptocurrency's numerical values can be measured from small portions such as .00000001 to 1.00 and up.
3. Conduct a test transfer of the minimal amount to a government-controlled wallet and confirm it was processed on the blockchain. Be sure to document the successful cryptocurrency transfer test.
4. Transfer and document the remaining balance of the seized cryptocurrency to the government-controlled wallet and confirm it was transferred on the blockchain.
5. Transfer the government-controlled cryptocurrency wallet and the private key to external digital media and print the private key on paper. The external digital media and paper copy will be placed into evidence following routine standard operating procedures of evidence management. All remaining computer data relating to the cryptocurrency seizure on the computer or device used for the seizure should be removed.
6. At least two people, including a witness, will observe all of the steps included in this process. The witness will sign as documentation the evidence container.
7. All documentation of this process will be recorded and placed along with the investigation reports.
8. Any cryptocurrency seizure should be memorialized with other forfeitures for record-keeping. A specialist should be contacted for further technical assistance if necessary.
9. Intelligence about the illegal cryptocurrency should be disseminated to relevant partnering agencies involved in the homeland security environment if it might assist collaborating partnering agencies, including federal agencies.

5. Community Outreach on Cryptocurrency and Crimes

State and local law enforcement should consider a policy and procedure to perform community outreach on cryptocurrency and crimes to enhance agencies' capabilities and increase protection for the public. As with many other crime-reduction strategies, community outreach remains a best practice for any plan. If the public understands how cryptocurrency links to crimes, people can make more informed decisions to avoid becoming victims of crimes involving cryptocurrency. A more informed citizen through community outreach will lead to an overall safer community. Once state and local law

enforcement agencies comprehend cryptocurrency, the information should be shared with citizens in their communities through public outreach.

6. Re-examining Historical Investigations for Cryptocurrency Intelligence and Information-Sharing

State and local law enforcement should create a policy to identify and re-examine historical investigations in which cryptocurrency perpetuated crime. Law enforcement can collaborate with partners to use cryptocurrency identification software to help the government identify users on a blockchain. If investigators discover new investigative leads, a supplemental investigation into these cold cases may continue. Criminal investigations have been re-examined for potential DNA evidence since PCR changed the ability to analyze DNA; so too may cryptocurrency identification software allow for a re-evaluation of older investigations that involved illegal cryptocurrency. Additionally, cryptocurrency intelligence from historical investigations can be shared with fusion centers and disseminated efficiently as it may assist a collaborating agency in its investigations.

D. CONCLUSION AND FUTURE RESEARCH

As of this writing, the cryptocurrency market is in turmoil following a drastic reduction in value in 2022. However, it still seems likely that bad actors will use cryptocurrency, and law enforcement will need to know how to address the problem now that the infrastructure exists. The world is still trying to figure out the best way to handle cryptocurrency, and law enforcement is no exception. American law enforcement must become versed in identifying and applying cryptocurrency in criminal investigations at the state and local levels. This thesis has shown that cryptocurrency is growing in popularity, and the government is not inhibiting its use in American commerce.

This thesis set out to guide state and local law enforcement in identifying cryptocurrency. It highlighted common network intrusions that local or foreign actors could perpetrate and recognized that enemies of the United States, terrorists, transnational criminal groups, nation-state hackers, and domestic criminals commonly use cryptocurrency. State and local law enforcement agencies must be prepared for its regular

use in America, and the resources and examples in this thesis should aid them in developing solutions.

Training and education in cryptocurrency for state and local governments are critical. Identifying cryptocurrency information in criminal investigations and entering the data into intelligence-sharing databases are an urgent need.²⁵⁹ A more extensive intelligence dataset could be crucial in identifying both legitimate and nefarious cryptocurrency users. Moreover, partnering with local colleges and universities accelerated law enforcement's efforts in solving violent crimes involving DNA and should be replicated in strategic planning for attacking the cryptocurrency used in crimes. Only with the cooperation and efforts of state and local officials can mass identification of cryptocurrency users improve, and all law enforcement can solve more crimes. These challenges will likely require even more advanced technologies. As with all evolving technologies, future research will need to continue to assess cryptocurrency as a threat to the homeland security environment and generate new ideas that might aid in creating a safer place for residents of our nation.

²⁵⁹ Police Executive Research Forum, *New National Commitment Required*.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

- Allen, William. "Cryptocurrency in Threat Finance: The Manipulation of Non-fiat Digital Currencies to Finance Nefarious Actors." *Small Wars Journal*, April 4, 2018. <http://smallwarsjournal.com/jrnl/art/cryptocurrency-threat-finance-manipulation-non-fiat-digital-currencies-finance-nefarious>.
- ANDE. "Breaking the Cycle of Crime: ANDE Is Changing the Paradigm in Law Enforcement." Accessed January 12, 2023. <https://www.ande.com/law-enforcement/>.
- Apple App Store. "Coinbase: Buy Bitcoin & Ether." Accessed November 16, 2021. <https://apps.apple.com/us/app/coinbase-trade-btc-eth-shib/id886427730>.
- Arnaud, Celia Henry. "Thirty Years of DNA Forensics: How DNA Has Revolutionized Criminal Investigations." *Chemical & Engineering News*, September 18, 2017. <https://cen.acs.org/analytical-chemistry/Thirty-years-DNA-forensics-DNA/95/i37>.
- Associated Press. "Rapist Convicted on DNA Match." *New York Times*, February 6, 1988. <https://www.nytimes.com/1988/02/06/us/rapist-convicted-on-dna-match.html>.
- Attorney General's Cyber Digital Task Force. *Cryptocurrency Enforcement Framework*. Washington, DC: Department of Justice, 2020. <https://www.justice.gov/cryptoreport>.
- Bain, Benjamin. "SEC Chief Says the U.S. Won't Ban Cryptocurrencies." *Bloomberg*, October 5, 2021. <https://www.bloomberg.com/news/articles/2021-10-05/sec-chief-signals-crypto-ban-like-china-s-won-t-happen-in-u-s>.
- Bain, Benjamin, and Jennifer Epstein. "White House Weighs Wide-Ranging Push for Crypto Oversight." *Bloomberg*, October 8, 2021. <https://www.bloomberg.com/news/articles/2021-10-08/white-house-weighs-wide-ranging-push-for-crypto-oversight>.
- Bardach, Eugene, and Eric M. Patashnik. *A Practical Guide for Policy Analysis: The Eightfold Path to More Effective Problem Solving*. 6th ed. Washington, DC: CQ Press, 2020.
- Baxter, Pamela, and Susan Jack. "Qualitative Case Study Methodology: Study Design and Implementation for Novice Researchers." *Qualitative Report* 13, no. 4 (December 2008): 544–58. <https://doi.org/10.46743/2160-3715/2008.1573>.
- Bearman, Joshua, and Tomer Hanuka. "The Rise & Fall of Silk Road." *Wired*, April 2015. <https://www.wired.com/2015/04/silk-road-1/>.

- Bernstein, Emily, and Caroline Sommers. "Inside the FBI Takedown of the Mastermind behind website Offering Drugs, Guns and Murders for Hire." CBS News, November 10, 2020. <https://www.cbsnews.com/news/ross-ulbricht-dread-pirate-roberts-silk-road-fbi/>.
- BitcoinMiningCom. "What Is Bitcoin Mining?" YouTube, April 9, 2013. Video, 1:55. <https://www.youtube.com/watch?v=GmOzih6I1zs>.
- Blumberg, Daniel M., Michael D. Schlosser, Konstantinos Papazoglou, Sarah Creighton, and Chuck Kaye. "New Directions in Police Academy Training: A Call to Action." *International Journal of Environmental Research and Public Health* 16, no. 24 (2019): 1–14. <https://doi.org/10.3390/ijerph16244941>.
- Bradfield, Angelena, and Stephanie Wake. "Top 7 Things to Know about Ransomware and Why Criminals Prefer Crypto Payments." *Bank Policy Institute* (blog), May 12, 2021. <https://bpi.com/top-7-things-to-know-about-ransomware-and-why-criminals-prefer-crypto-payments/>.
- Brannan, David, Anders Strindberg, and Kristin Darken. *A Practitioner's Way Forward: Terrorism Analysis*. Salinas, CA: Agile Press, 2014.
- Brown, Dalvin. "Crypto Tax: 'MiamiCoin' Has Made the City \$7 Million So Far, a Potential Game-Changer for Revenue Collection." *Washington Post*, September 30, 2021. <https://www.washingtonpost.com/technology/2021/09/30/crypto-miamicoin/>.
- CBS News. "Will Industrial-Scale Bitcoin Mining Impact the Environment?" October 9, 2021. <https://www.cbsnews.com/news/will-industrial-scale-bitcoin-mining-impact-the-environment/>.
- Chainalysis. "Government Agencies." Accessed January 12, 2023. <https://www.chainalysis.com/government-agencies/>.
- . *The 2022 Crypto Crime Report*. Chainalysis, 2022. <https://www.chainalysis.com/>.
- Chiu, Juin. "Privacy, Blockchain and Onion Routing." *Medium* (blog), October 7, 2019. <https://medium.com/unitychain/privacy-blockchain-and-onion-routing-d5609c611841>.
- Clark, Richard E. *Turning Research into Results: A Guide to Selecting the Right Performance Solutions*. Charlotte, NC: Information Age Publishing, 2008.
- Coinbase. "Explore the Cryptoeconomy." Accessed November 6, 2021. <https://www.coinbase.com/price>.

- . “I Sent Funds to the Wrong Address. How Do I Get Them Back?” November 12, 2021. <https://help.coinbase.com/en/coinbase/trading-and-funding/sending-or-receiving-cryptocurrency/i-sent-funds-to-the-wrong-address-how-do-i-get-them-back.html>.
- Comey, James B. “Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?” Remarks at Brookings Institution, Washington, DC, October 16, 2014. <https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course>.
- Crypto Casey. “What Blockchain Is & How Blockchain Works (Simple Overview).” In *Cryptocurrency for Beginners*, May 25, 2020. Podcast, MP3 audio, 37:00. <https://cryptocasey.com/podcasts/what-bitcoin-is-how-bitcoin-works-a-simple-explanation/>.
- Dahl, Erik J. *Intelligence and Surprise Attack: Failure and Success from Pearl Harbor to 9/11 and Beyond*. Washington, DC: Georgetown University Press, 2013.
- Department of Homeland Security Science and Technology. “Insider Threat.” January 12, 2023. <https://www.dhs.gov/science-and-technology/cybersecurity-insider-threat#>.
- Department of Justice. “Department of Justice Seizes \$2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside.” June 7, 2021. <https://www.justice.gov/opa/pr/departments-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside>.
- . “Global Disruption of Three Terror Finance Cyber-Enabled Campaigns: Largest Ever Seizure of Terrorist Organizations’ Cryptocurrency Accounts.” August 13, 2020. <https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns>.
- . “Maryland Nuclear Engineer and Spouse Arrested on Espionage-Related Charges.” October 10, 2021. <https://www.justice.gov/opa/pr/maryland-nuclear-engineer-and-spouse-arrested-espionage-related-charges>.
- Drug Enforcement Administration. “International Law Enforcement Operation Targeting Opioid Traffickers on the Darknet Results in 150 Arrests Worldwide and the Seizure of Weapons, Drugs, and Over \$31 Million.” October 26, 2021. <https://www.dea.gov/press-releases/2021/10/26/departments-justice-announces-results-operation-dark-hunter>.
- Electronic Privacy Information Center. “Apple v. FBI.” Accessed October 6, 2022. <https://epic.org/documents/apple-v-fbi-2/>.

- Endemann, Buck, Irving Wladawsky-Berger, Cara LaPointe, and Hugo Yen. *Blockchain*, edited by Amritha Jayanti and Bogdan Bele. Cambridge, MA: Harvard Kennedy School, Belfer Center for Science and International Affairs, 2020. <https://www.belfercenter.org/sites/default/files/files/publication/Blockchain.pdf>.
- Esparza, Diego, and Thomas C. Bruneau. "Closing the Gap between Law Enforcement and National Security Intelligence: Comparative Approaches." *International Journal of Intelligence and Counterintelligence* 32, no. 2 (2019): 322–53. <https://doi.org/10.1080/08850607.2018.1522219>.
- Euromoney Learning. "How Does a Transaction Get into the Blockchain?" Accessed October 5, 2021. <https://www.euromoney.com/learning/blockchain-explained/how-transactions-get-into-the-blockchain>.
- Federal Bureau of Investigation. "GRU Hackers' Destructive Malware and International Cyber Attacks." Accessed February 6, 2023. <https://www.fbi.gov/wanted/cyber/gru-hackers-destructive-malware-and-international-cyber-attacks>.
- . "The Insider Threat: An Introduction to Detecting and Deterring an Insider Spy." Accessed January 17, 2022. https://www.fbi.gov/file-repository/insider_threat_brochure.pdf/view.
- . *2018 Internet Crime Report*. Washington, DC: Federal Bureau of Investigation, 2019. https://www.ic3.gov/Media/PDF/AnnualReport/2018_IC3Report.pdf.
- . *2016 Internet Crime Report*. Washington, DC: Federal Bureau of Investigation, 2017. https://www.ic3.gov/Media/PDF/AnnualReport/2016_IC3Report.pdf.
- . *2020 Internet Crime Report*. Washington, DC: Federal Bureau of Investigation, 2021. https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf.
- Feuer, Will. "Biden Administration Unveils 'National Cryptocurrency Enforcement Team.'" *New York Post*, October 7, 2021. <https://nypost.com/2021/10/07/biden-administration-unveils-national-cryptocurrency-enforcement-team/>.
- Fiatal, Robert A. "DNA Testing and the Frye Standard." *FBI Law Enforcement Bulletin* 59, no. 6 (June 1990): 26–31. <https://www.ojp.gov/ncjrs/virtual-library/abstracts/dna-testing-and-frye-standard>.
- Financial Crimes Enforcement Network. *Anti-Money Laundering and Countering the Financing of Terrorism National Priorities*. Washington, DC: Department of the Treasury, 2021. <https://www.hsd.org/?abstract&did=856103>.
- Flitter, Emily. "The World's Biggest Crypto Exchange Still Lacks U.S. Footing." *New York Times*, August 19, 2021. <https://www.nytimes.com/2021/08/19/business/binance-cryptocurrency-exchange-ipo.html>.

- Frebowitz, Ryan L. "Cryptocurrency and State Sovereignty." Master's thesis, Naval Postgraduate School, 2018. <https://calhoun.nps.edu/handle/10945/59663>.
- Frontline. "The DNA 'Wars' Are Over." Accessed August 10, 2022. <https://www.pbs.org/wgbh/pages/frontline/shows/case/revolution/wars.html>.
- Gault, Matthew. "Man Shot Dead in Hail of Gunfire over Crypto Mining Rigs, Police Say." Vice News, October 28, 2021. <https://www.vice.com/en/article/n7nwwq/man-shot-dead-in-hail-of-gunfire-over-crypto-mining-rigs-police-say>.
- Gerring, John. "What Is a Case Study and What Is It Good For?" *American Political Science Review* 98, no. 2 (May 2004): 341–54. <https://doi.org/10.1017/S0003055404001182>.
- Hanson, Emily J. *The Use of DNA by the Criminal Justice System and the Federal Role: Background, Current Law, and Grants*. Washington, DC: Congressional Research Service, 2022. ProQuest.
- Holmes, David. "Snooping on Tor from Your Load Balancer." F5 Labs, July 3, 2018. <https://www.f5.com/labs/articles/threat-intelligence/snooping-on-tor-from-your-load-balancer>.
- Howard-Grenville, Jennifer A. "Developing Issue-Selling Effectiveness over Time: Issue Selling as Resourcing." *Organization Science* 18, no. 4 (August 2007): 560–77. <https://doi.org/10.1287/orsc.1070.0266>.
- Hubbard, Douglas W. *The Failure of Risk Management: Why It's Broken and How to Fix It*. 2nd ed. Hoboken, NJ: Wiley, 2020.
- Innocence Project. "DNA Exonerations in the United States." Accessed August 11, 2022. <https://innocenceproject.org/dna-exonerations-in-the-united-states/>.
- Iredale, Gwyneth. "Blockchain vs. Database: Understanding the Difference." 101 Blockchains, July 30, 2021. <https://101blockchains.com/blockchain-vs-database-the-difference/>.
- Islam, Zak. "The Dark Web Has Become Darker and Busier, Cybercrime Services Cost Less than \$500." *Techspot Magazine*, October 19, 2021. <https://www.techspot.com/news/91830-dark-web-has-become-darker-busier-cybercrime-services.html>.
- James, Stuart H., and Jon J. Nordby, eds. *Forensic Science: An Introduction to Scientific and Investigative Techniques*. 2nd ed. Boca Raton, FL: CRC Press, 2005.
- Jardine, Eric. *The Dark Web Dilemma: Tor, Anonymity and Online Policing*. Waterloo, Ontario: Centre for International Governance Innovation and Chatham House, 2015. <https://www.cigionline.org/sites/default/files/no.21.pdf>.

- Johnson, Lauren Keller. “Issue Selling in the Organization.” *MIT Sloan Management Review*, April 15, 2002. <https://sloanreview.mit.edu/article/strategy-issue-selling-in-the-organization/>.
- Jonathan. “Why We Need Anonymous Exchanges—Pros and Cons in 2022.” *Cryptogeek* (blog), July 1, 2020. <https://cryptogeek.info/en/blog/exchanging-cryptocurrencies-anonymously>.
- Kaiser, Jocelyn. “A Judge Said Police Can Search the DNA of 1 Million Americans without Their Consent. What’s Next?” *Science*, November 7, 2019. <https://www.science.org/content/article/judge-said-police-can-search-dna-millions-americans-without-their-consent-what-s-next>.
- Kauflin, Jeff. “Coinbase’s Public Stock Listing Creates a Multibillion Dollar Windfall for Founders—Now It Faces Five Big Threats.” *Forbes*, April 14, 2021. <https://www.forbes.com/sites/jeffkauflin/2021/04/14/coinbases-ipo-creates-a-multibillion-dollar-windfall-for-founders-now-it-faces-five-big-threats/?sh=5362938261ff>.
- Keightley, Mark P., and Andrew P. Scott. *Cryptocurrency Transfers and Data Collection*. IF11910. Washington, DC: Congressional Research Service, 2021.
- Kohnke, Anne, Greg Laidlaw, and Charles Wilson. “Challenges in Bridging the Law Enforcement Capability Gap.” In *International Conference on Cyber Warfare and Security*, 521–26. Reading, UK: Academic Conferences International, 2021. <https://doi.org/10.34190/IWS.21.013>.
- Langford, Gary, Raymond Franck, Tom Huynh, and Ira Lewis. *Gap Analysis: Rethinking the Conceptual Foundations*. NPS-AM-07-051. Monterey, CA: Naval Postgraduate School, 2007. <https://dair.nps.edu/handle/123456789/2815>.
- Lowenthal, Mark M. *Intelligence: From Secrets to Policy*. 8th ed. Thousand Oaks, CA: CQ Press, 2020.
- McGhee, Sam. “Impacting the Evolution of Information Sharing in the Post-9/11 United States.” *Police Chief Magazine*, February 1, 2015. <https://www.policechiefmagazine.org/impacting-the-evolution-of-information-sharing-in-the-post-911-united-states/>.
- Medline Plus. “What Is a Chromosome?” Accessed August 11, 2022. <https://medlineplus.gov/genetics/understanding/basics/chromosome/>.
- Milo, Paul. “Seller of This Pricey N.J. Home Wants \$2.1M. Or You Can Pay in Bitcoin.” *New Jersey Advance Local Media*, February 2, 2018. https://www.nj.com/monmouth/2018/02/seller_of_this_pricey_nj_home_wants_21m_or_you_can_pay_in_bitcoin.html.

- Monaghan, Ryan M. "Cybercrime Response Capabilities and Capacity: An Evaluation of Local Law Enforcement's Response to a Complex Problem." Master's thesis, Naval Postgraduate School, 2020. <https://calhoun.nps.edu/handle/10945/66690>.
- Montgomery, Chelsea. "New Security for a New Era: An Investigation into Law Enforcement Cybersecurity Threats, Obstacles, and Community Applications." Master's thesis, Utica College, 2017. ProQuest.
- Morris, James. "How Mining and Blockchain Fit Together." Kit Guru, February 16, 2018. <https://www.kitguru.net/components/james-morris/bitcoin-ethereum-and-cryptocurrency-ultimate-beginners-guide-to-mining/4/>.
- Muni, Michele-Lynne. "Policing Domestic Violence: Case Study of Organizational Change in the Trenton Police Department, Trenton, New Jersey." PhD diss., Rutgers University, 2012. <https://doi.org/10.7282/T36H4GCC>.
- Muzinich, Justin. "America's Crypto Conundrum." *Foreign Affairs*, November/December 2021. <https://www.foreignaffairs.com/articles/united-states/americas-crypto-currency-conundrum>.
- Nadeem, Subhan. "How Bitcoin Mining Really Works." Free Code Camp, May 31, 2018. <https://www.freecodecamp.org/news/how-bitcoin-mining-really-works-38563ec38c87/>.
- Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." Bitcoin Project, 2009. <https://bitcoin.org/bitcoin.pdf>.
- National Criminal Justice Reference Service. "What Every Law Enforcement Officer Should Know about DNA Evidence." Accessed August 11, 2022. <https://www.ncjrs.gov/nij/DNAbro/evi.html>.
- National Human Genome Research Institute. "Deoxyribonucleic Acid (DNA) Fact Sheet." Accessed August 8, 2022. <https://www.genome.gov/about-genomics/fact-sheets/Deoxyribonucleic-Acid-Fact-Sheet>.
- . "Polymerase Chain Reaction (PCR) Fact Sheet." August 17, 2020. <https://www.genome.gov/about-genomics/fact-sheets/Polymerase-Chain-Reaction-Fact-Sheet>.
- National Institute of Justice. *Crime Scene Investigation: A Guide for Law Enforcement*. Washington, DC: Department of Justice, 2000.
- National Research Council, Committee on DNA Forensic Science. "DNA Evidence in the Legal System." In *The Evaluation of Forensic DNA Evidence*. Washington, DC: National Academies Press, 1996. <https://www.ncbi.nlm.nih.gov/books/NBK232607/>.

- New Jersey Cybersecurity and Communications Integration Cell. “Public Data Breaches.” November 19, 2021. <https://www.cyber.nj.gov/threat-center/public-data-breaches/>.
- New Jersey State Commission of Investigation. *Bitcoin ATMs: Scams, Suspicious Transactions and Questionable Practices at Cryptocurrency Kiosks*. Trenton, NJ: New Jersey Commission of Investigation, 2021. <https://www.state.nj.us/sci/pdf/Bitcoin%20Report.pdf>.
- No More Ransom. “Decryption Tools.” Accessed January 12, 2023. <https://www.nomoreransom.org/en/decryption-tools.html>.
- NW3C. “Classroom Training.” Accessed January 12, 2023. <https://www.nw3c.org/classroom-training>.
- . “Online Training.” Accessed January 12, 2023. <https://www.nw3c.org/online-training>.
- Pierce, Jon L., and André L. Delbecq. “Organization Structure, Individual Attitudes and Innovation.” *Academy of Management Review* 2, no. 1 (January 1977): 27–37. <https://doi.org/10.5465/AMR.1977.4409154>.
- Police Executive Research Forum. *New National Commitment Required: The Changing Nature of Crime and Criminal Investigations*. Washington, DC: Police Executive Research Forum, 2018. <https://www.policeforum.org/assets/ChangingNatureofCrime.pdf>.
- Popper, Nathaniel. “Lost Passwords Lock Millionaires Out of Their Bitcoin Fortunes.” *New York Times*, January 14, 2021. <https://www.nytimes.com/2021/01/12/technology/bitcoin-passwords-wallets-fortunes.html>.
- Raskin, Sam. “Eric Adams Converting First Paycheck as NYC Mayor to Bitcoin, Ethereum.” *New York Post*, January 20, 2022. <https://nypost.com/2022/01/20/eric-adams-converting-first-paycheck-as-nyc-mayor-to-bitcoin-ethereum/>.
- Reinicke, Carmen. “Some Investors Are Putting More Money into Cryptocurrencies than Stocks,” October 20, 2021. <https://www.cnbc.com/2021/10/20/some-investors-putting-more-money-into-cryptocurrencies-than-stocks.html>.
- Renteria, Nelson, and Anthony Esposito. “El Salvador’s World-First Adoption of Bitcoin Endures Bumpy First Day.” Reuters, September 8, 2021. <https://www.reuters.com/business/finance/el-salvador-leads-world-into-cryptocurrency-bitcoin-legal-tender-2021-09-07/>.

- Reuters. “Latest Russian Cyberattack Targeting Hundreds of U.S. Networks—Microsoft.” October 25, 2021. <https://www.reuters.com/technology/microsoft-says-russian-group-has-targeted-hundreds-us-networks-2021-10-25/#:~:text=Latest%20Russian%20cyberattack%20targeting%20hundreds%20of%20U.S.%20networks%20%2DMicrosoft,-Reuters&text=Microsoft%2C%20in%20a%20blog%20post,service%20providers%22%20of%20cloud%20services>.
- Reutzel, Bailey. “What Is Cryptocurrency? Here’s What You Need to Know about Blockchain, Coins and More.” CNBC, September 22, 2021. <https://www.cnbc.com/select/what-is-cryptocurrency/>.
- Rosner, Eric. “Cyber Federalism: Defining Cyber’s Jurisdictional Boundaries.” Master’s thesis, Naval Postgraduate School, 2017. <https://calhoun.nps.edu/handle/10945/56794>.
- Royal Canadian Mounted Police. “A Family’s Guide to the National Missing Persons DNA Program.” October 29, 2020. <https://www.rcmp-grc.gc.ca/en/a-familys-guide-the-national-missing-persons-dna-program>.
- . “Forms for the National DNA Data Bank.” Accessed February 6, 2023. <https://www.rcmp-grc.gc.ca/en/forensics/forms-the-national-dna-data-bank>.
- . “Guide to the Victims Index and Voluntary Donors Index of the National DNA Data Bank of Canada.” February 17, 2021. <https://www.rcmp-grc.gc.ca/en/forensics/guide-the-victims-index-and-voluntary-donors-index-the-national-dna-data-bank-canada>.
- . “The National DNA Data Bank of Canada—Annual Report 2020–2021.” March 7, 2022. <https://www.rcmp-grc.gc.ca/en/the-national-dna-data-bank-canada-annual-report-20202021>.
- . “National Missing Persons DNA Program Hits Milestone: 50th Case Solved with the Help of DNA.” May 26, 2022. <https://www.rcmp-grc.gc.ca/en/news/2022/national-missing-persons-dna-program-hits-milestone-50th-case-solved-the-help-dna>.
- Schoenberg, Tom. “Binance Faces Probe by U.S. Money-Laundering and Tax Sleuths.” Bloomberg, May 13, 2021. <https://www.bloomberg.com/news/articles/2021-05-13/binance-probed-by-u-s-as-money-laundering-tax-sleuths-bore-in>.
- Scitable. “Gel Electrophoresis.” Accessed August 8, 2022. <https://www.nature.com/scitable/definition/gel-electrophoresis-286/>.
- Samuels, Alana. “Society Is Paying the Price for America’s Outdated Police Training Methods.” *Time*, November 20, 2020. <https://time.com/5901726/police-training-academies/>.

- Sigalos, MacKenzie. “Two of the Biggest Bitcoin Mining Companies in the World Are Battling It Out in a Texas Town of 5,600 People.” CNBC, October 31, 2021. <https://www.cnbc.com/2021/10/31/bitcoin-mining-giants-bitdeer-riot-blockchain-in-rockdale-texas.html>.
- Sprenger, Pascal, and Franziska Balsiger. *Anti–Money Laundering in Times of Cryptocurrencies*. Zurich: KPMG, 2018.
- Sridhar, N., D. Lalitha Bhaskari, and P. S. Avadhani. “18: Plethora of Cyber Forensics.” *International Journal of Advanced Computer Science and Applications* 2, no. 11 (2011): 110–14. <https://doi.org/10.14569/IJACSA.2011.021118>.
- Stankiewicz, Kevin. “Cramer Sells Some Bitcoin and Pays Off a Home Mortgage.” CNBC, April 15, 2021. <https://www.cnbc.com/2021/04/15/jim-cramer-says-he-sold-some-of-his-bitcoin-and-paid-off-a-mortgage.html>.
- Su, Eva. *Digital Assets and SEC Regulation*. CRS Report No. R46208. Washington, DC: Congressional Research Service, 2021. <https://www.hsdl.org/?abstract&did=855875>.
- Sun, Mengqi, and David Smagalla. “Cryptocurrency-Based Crime Hit a Record \$14 Billion in 2021.” *Wall Street Journal*, January 6, 2022. <https://www.wsj.com/articles/cryptocurrency-based-crime-hit-a-record-14-billion-in-2021-11641500073>.
- Swinhoe, Dan. “Why Businesses Don’t Report Cybercrimes to Law Enforcement.” CSO Online, May 30, 2019. <https://www.csoonline.com/article/3398700/why-businesses-don-t-report-cybercrimes-to-law-enforcement.html>.
- Taylor, Peter Lane. “Miami Beach’s Most Expensive Penthouse Just Sold in America’s Largest-Known Cryptocurrency Real Estate Deal.” *Forbes*, June 7, 2021. <https://www.forbes.com/sites/petertaylor/2021/06/07/miami-beachs-most-expensive-penthouse-just-sold-in-americas-largest-known-cryptocurrency-real-estate-deal-that-could-change-housing-forever/?sh=379718fc64a6>.
- Thomas, Lauren. “Walmart Is Quietly Preparing to Enter the Metaverse.” CNBC, January 16, 2022. <https://www.cnbc.com/2022/01/16/walmart-is-quietly-preparing-to-enter-the-metaverse.html>.
- Tor Project. “Home Page.” Accessed September 28, 2021. <https://www.torproject.org/>.
- University of Florida. “Ransomware.” Accessed November 12, 2021. <https://security.ufl.edu/resources/protect-your-computer/ransomware/>.

U.S. Attorney's Office, Northern District of California. "United States Files a Civil Action to Forfeit Cryptocurrency Valued at Over One Billion U.S. Dollars." November 5, 2020. <https://www.justice.gov/usao-ndca/pr/united-states-files-civil-action-forfeit-cryptocurrency-valued-over-one-billion-us>.

Volpicelli, Gian M. "China's Sweeping Cryptocurrency Ban Was Inevitable." *Wired*, September 30, 2021. <https://www.wired.com/story/chinas-sweeping-cryptocurrency-ban-inevitable/>.

Wang, Echo. "U.S. Regulators Exploring How Banks Could Hold Crypto Assets—FDIC Chairman." Reuters, October 26, 2021. <https://www.reuters.com/business/finance/us-regulators-exploring-how-banks-could-hold-crypto-assets-fdic-chairman-2021-10-26/>.

Your Genome. "What Is Gel Electrophoresis?" July 21, 2021. <https://www.yourgenome.org/facts/what-is-gel-electrophoresis/>.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, Virginia
2. Dudley Knox Library
Naval Postgraduate School
Monterey, California



DUDLEY KNOX LIBRARY

NAVAL POSTGRADUATE SCHOOL

WWW.NPS.EDU

WHERE SCIENCE MEETS THE ART OF WARFARE