PRIORITY
Criminal Justice
NEEDS INITIATIVE

A project of the **RAND Corporation**, the **Police Executive Research Forum**, **RTI International**, and the **University of Denver**

Cryptocurrency and Blockchain Needs for Law Enforcement

Dulani Woods, John S. Hollywood, Jeremy D. Barnum, Danielle Fenimore, Michael J. D. Vermeer, Brian A. Jackson

EXECUTIVE SUMMARY

As society's relationship to technology has changed, criminal justice systems have often struggled to keep pace. The development and increasing use of blockchain technologies within society has created new challenges for the criminal justice system, especially for law enforcement. Blockchain technology can be leveraged for a variety of purposes but is perhaps best known as the foundation for a certain type of digital currency that is often called *cryptocurrency*, the most famous examples of which are Bitcoin, Ethereum, and Dogecoin. The technology itself is often described as a ledger, which is often publicly available on the internet (although nonpublic versions also exist). Essentially, it allows a group of individuals, who might not know each other, to collectively manage a shared and growing record of data elements. For a cryptocurrency ledger, that is typically a record of transactions. Cryptocurrency's footprint within society has grown, and cryptocurrency is increasingly an accepted form of payment in many legitimate business transactions. It has become a popular investment vehicle as well. However, it is also used to facilitate many illegal activities, even catalyzing new crimes, in large part because of its capacity to facilitate mostly anonymous transactions remotely via the internet. There is a need to better understand the problems and opportunities that cryptocurrencies, and blockchain technology more generally, will create for law enforcement in the short term and plan to address them.

On behalf of the National Institute of Justice, the RAND Corporation and the Police Executive Research Forum convened a workshop to identify law enforcement needs related to blockchain and cryptocurrency. The workshop was held virtually on August 24 and 26, 2021. Workshop participants were invited based on our review of the research literature and consultation with federal partners and known law enforcement practitioners who have experience working with cryptocurrencies.

SELECTED PRIORITY NEEDS

RESULTS

Policies and procedures

- Identify best-practice policies and procedures for rapidly securing cryptocurrency assets during investigations.
- Develop best-practice policies and procedures (e.g., two-person systems) to minimize opportunities for mishandling cryptocurrency.
- Identify best-practice policies and procedures for handling, storing, transferring, and redacting digital cryptocurrency keys within record-management systems.
- Catalog and publicize the training resources that are already available, including training that is not tailored for justice practitioners.

Training

- Develop regional or national sharing systems that facilitate sharing of training materials and actionable intelligence for ongoing cases (e.g., digital or cyber fusion centers).
- Develop model materials that can be easily adapted for training recruits, investigators, forensics experts, prosecutors, judges, and others.
- Conduct research to examine the balance of skills and expertise that law enforcement agencies look for when hiring and assess whether those are likely to meet current and future needs.

Research needs assessment

- Convene a standing group of practitioners and experts who can examine the "state of the possible" and generate requirements for research and development organizations.

SELECTED PRIORITY NEEDS

Tools for investigations

- Work with federal, state, local, and private entities (e.g., the Regional Computer Forensics Laboratory, Lawyers Without Borders) to make available appropriate cryptocurrency-tracking resources so that costs can be more easily shared.
- Assess the costs and benefits of developing a private-sector clearinghouse that will allow the public sector and vetted private-sector entities to coordinate (similar to how the National Center for Missing and Exploited Children screens potentially abusive materials).

The workshop explored the following specific law enforcement concerns related to blockchain and cryptocurrency: (1) the use of blockchain technologies to support the criminal justice system, (2) officer training associated with understanding how blockchain technologies are used to facilitate crimes, (3) conducting crime and investigations with blockchain technologies, and (4) other issues. Participants were led in a semi-structured discussion of each topic. Following the discussions, the experts participated in a ranking exercise to identify the most-important needs. (In this report, we use the term *need* to describe a combination of a problem or opportunity and an accompanying solution.)

WHAT WE FOUND

The unique features of blockchain-based cryptocurrencies have facilitated and motivated the rise of a variety of crime types, including ransomware, extortion, fraud, theft of electricity and computing resources, money laundering, human trafficking, and illicit trade. The workshop was focused on law enforcement needs pertaining to such criminal uses of blockchain, and the workshop participants identified and prioritized a series of research and development needs. Of the 24 needs identified by the group, ten were categorized as high priority.

Most needs were associated with multi-jurisdictional cooperation, but the high-priority needs also pertained to training, tools for investigations, public education, policies and procedures, operational applications of blockchain, and research. The needs that rose to the top of the list during the prioritization exercise focused on policies, procedures, and training because participants deemed those the easiest to produce, adopt, and implement as a part of a research and development process. This report details the ten high-priority needs that emerged through this exercise and provides additional context based on the participants' discussions.

The needs that rose to the top of the list during the prioritization exercise focused on policies, procedures, and training because participants deemed those the easiest to produce, adopt, and implement as a part of a research and development process.

INTRODUCTION

The criminal justice system in the United States is intended to deter, punish, and reform individuals who violate the norms of good order and mutual respect that are enshrined in law. The associated legal structures were developed, for the most part, before the development of such information technologies as the postal service, telegraph, and telephone systems. With the development of personal computers connected by the internet, much larger portions of economic and interpersonal interactions have moved online, as has criminal activity. This shift of activity into digital spaces has presented a multitude of difficulties, as well as opportunities, for criminal justice practitioners (Goodison, Davis, and Jackson, 2015; Tanneeru, 2009; Vermeer, Woods, and Jackson, 2018).

A traditional assumption, built into the structure of the U.S. criminal justice system, is that individuals who are committing crimes are physically within a geographical jurisdiction, their victims are physically present within that jurisdiction, and any necessary evidence that exists could also be obtained within that jurisdiction. The shift to digital and online interactions has meant that the "same jurisdiction" conditions are being met less and less frequently for many types of crimes (Caldwell, 2016; Hill, 2015; Vermeer, Woods, and Jackson, 2018). Furthermore, at the time a crime is committed, the jurisdiction that the participants are in might be completely unknown to law enforcement. This presents new challenges for law enforcement agencies in carrying out criminal justice system processes efficiently and effectively (Goodison et al., 2019; Tanneeru, 2009; Vermeer, Woods, and Jackson, 2018).

Emerging digital technologies that are rendering jurisdictional boundaries less meaningful include blockchain technologies and associated cryptocurrencies. (Details of blockchain, cryptocurrency, digital wallets, and other related technologies are provided in Appendix A.) The rise of blockchain and associated technologies is the latest example of an emerging technology posing both challenges and potential opportunities for law enforcement. Blockchain technologies are distributed digital ledgers for financial and other transactions, similar to traditional accounting ledgers. For a public blockchain, these ledgers are available to anyone with access to the internet; are very hard to alter and corrupt; and can obscure the identities of parties to a transaction (Katkar, 2021). (For example, one knows that two parties with specified identifiers exchanged funds, but one does not know whom the identifiers represent.) Blockchain-based cryptocurrencies have features similar to the way cash is used, but the individuals who are conducting transactions do not need to physically exchange anything; in fact, they might not even know each other. These cryptocurrencies also have features similar to how funds can be exchanged in popular money-sharing apps, such as PayPal or Venmo, but those systems tie back to banks with "Know Your Customer" identification requirements, whereas the average blockchain-based system does not.

Blockchain-based technologies can be used for a variety of purposes, both legitimate and illegitimate. For this report, we focus on both the legitimate opportunities to improve criminal justice processes that depend on exchanging data and the forms of illegal behavior that have been catalyzed by the existence of blockchain-based technologies. Blockchain's most common application is as the backbone for digital assets called *cryptocurrencies*, which are intended to function like money, as mediums of exchange, while adding the immutability and anonymity protections afforded by the blockchain. Arguably, the most well-known cryptocurrencies are Bitcoin, Ethereum, and Dogecoin. However, there are thousands of different cryptocurrency implementations (CoinMarketCap, undated), each with a unique set of features.

Cryptocurrencies are digital assets that allow users to remotely and semiautonomously conduct transactions. There is not an entrusted third-party organization managing cryptocurrency transactions, and the "currencies" are typically not issued by a government. Instead, transactions are managed by decentralized networks of individuals and organizations voluntarily operating computer servers that are working transparently and cooperatively using a shared governance protocol (i.e., a software algorithm). The software algorithm is designed to prevent any one group or individual from asserting control over the entire system. As a result, there is no centralized authority with which law enforcement can interact. Individuals looking to conduct transactions need access to compatible software called a *wallet* and a password-like set of numbers and letters called a *private key* (Nakamoto, undated). (We explore the vari-

ABBREVIATIONS

MLAT	mutual legal assistance treaties
NIJ	National Institute of Justice
NW3C	National White Collar Crime Center
PCJNI	Priority Criminal Justice Needs Initiative
PERF	Police Executive Research Forum
QR	quick response
WIF	wallet import format

ous permutations of wallets and keys in more detail below.) For many users, the wallet can take the form of a smartphone app that manages the private keys and wallet addresses. According to participants of a workshop we held to identify law enforcement needs related to blockchain, the wallet is the source of many of the challenges that blockchain technologies present to the criminal justice system.[1]

Criminal Justice System Uses for Blockchain

Often, there are opportunities for elements of the justice system to adopt the same technologies that are being adopted by the rest of society to improve efficiency and effectiveness. Examples of historical new technologies to which various sectors of the justice system have had to adapt include radios; automobiles; telephones; surveillance cameras; mobile phones; and various internet technologies, such as email, social media, DNA forensics, and video teleconferencing. When this happens, the justice system needs to adapt its tactics and techniques to avoid falling behind and becoming less effective at upholding the ideal of justice for all (Goodison, Davis, and Jackson, 2015; Gourdet et al., 2020; Hollywood et al., 2015; Hollywood et al., 2018b).

Within the criminal justice system, several potential uses for blockchain have been considered, but these are largely still in development. In June 2019, the Integrated Justice Information Systems Institute considered several potential applications for improving certain justice system functions by using blockchain technologies (Integrated Justice Information Systems Institute, 2019; Integrated Justice Information Systems Institute and Microsoft, 2019). These included decentralized identification systems (e.g., badges) that could be used for verifying officer credentials during multiagency responses and digital protective orders (Kita et al., 2020; McAdoo, 2020).[2] Other proposed applications of blockchain include improving record-management systems, evidence chain of custody, interagency data sharing, and management and authentication of body-worn camera footage (Coins Capture, 2020; Dave, 2019; Williams and Murat, 2019).

> Technologies with societally desirable uses often also have undesirable applications, and blockchain technologies are often criticized for their role in facilitating and obscuring criminal activity.

Criminal Uses of Blockchain

Philosophers often cite the *double power principle*, which states that something that has a certain power for good also has equal power for bad (Postman, 1993). Similarly, technologies with societally desirable uses often also have undesirable applications, and blockchain technologies (specifically cryptocurrencies) are often criticized for their role in facilitating and obscuring criminal activity (Clark, Kreps, and Rao, 2022; Stroukal and Nedvědová, 2016).

Ransomware and Extortion

Some of the most notable crimes that cryptocurrencies have facilitated are ransomware-based schemes. In such schemes, criminals manage to install malicious software onto a victim's computer. This software encrypts the stored contents of the user's computer, rendering it unusable. The criminal then requests payment to provide the decryption codes. The criminal might also threaten to publicly release the individual's data. These types of schemes certainly existed prior to the advent of cryptocurrencies (Giri and Jyoti, 2006), but the relative anonymity, speed, and irreversibility of cryptocurrency transactions makes them ideal for ransomware schemes (Braaten and Vaughn, 2021).

Cryptocurrency-related crimes are rapidly growing in type and frequency (Federal Bureau of Investigation National Press Office, 2021; Internet Crime Complaint Center, 2020; Jeffery and Ramachandran, 2021). One workshop participant observed that a high percentage of people using Bitcoin ATMs installed in local convenience stores were being walked through the process of obtaining Bitcoin while on the phone with criminal entities that held the keys to their data. However, although the advent of ubiquitous cryptocurrencies is facilitating these crimes, only a small portion of the overall use of these technologies is tied to crime. According to Chainalysis, "Transactions involving illicit addresses represented just 0.15% of cryptocur-

When an improper transfer is discovered in traditional banking, there are procedures between banks to reverse the transaction and retrieve the funds. However, when criminals receive funds in the form of cryptocurrency, it can become difficult or impossible to recover them.

rency transaction volume in 2021" (Grauer, Kueshner, and Updegrave, 2022, p. 4).

Fraud and Theft

Theft and hacking schemes that have previously relied on "traditional" banking, such as wire transfers, are being enabled by cryptocurrencies. When an improper transfer is discovered in traditional banking, there are procedures between banks to reverse the transaction and retrieve the funds. However, when criminals receive funds in the form of cryptocurrency, it can become difficult or impossible to recover them. In one recent example, a suspect allegedly stole $154 million from the Sony Life Insurance Company and then quickly transferred the stolen funds into cryptocurrency to maintain control of them (U.S. District Court, Southern District of California, 2021).

A crime that is increasingly associated with cryptocurrency is a unique form of identity theft and fraud called *SIM swapping*. SIM swapping allows hackers to take over an individual's phone number so that they receive the two-factor authentication password codes that are often sent by SMS to improve login security (Johansen, 2019). When SIM swapping is done to an individual or person who is allowing an online cryptocurrency exchange to manage their cryptocurrency assets (e.g., Coinbase, Binance.us), this kind of fraud can allow the attacker to send cryptocurrency assets to a wallet that is under the control of the thief and not under the control of the exchange. Because of the irreversibility of blockchain transactions, these funds are often lost (Gromek, 2020; Nakamoto, undated; Zaytoun, 2019).

As discussed in Appendix A, participants who dedicate computing resources to the record-keeping validation of a blockchain network are called *miners*, and the algorithms behind the blockchain are designed to reward miners with additional cryptocurrency. These proof-of-work–based systems are well known for requiring significant amounts of computing power and electricity to perform the block validation step, and it can be quite expensive to maintain a reasonable return on the investment in electricity and hardware (Cambridge Bitcoin Electricity Consumption Index, undated). This trade-off has motivated criminals in the United Kingdom and Ukraine to steal electricity to improve the economic prospects of their operations (Antoniuk, 2021; Jolly, 2021; Shalvey, 2021). Some criminals have also compromised individual cloud computing accounts to use those servers for cryptocurrency mining (Mechler and Rosenblatt, 2021; Wright, 2021).

While blockchain remains a relatively secure mechanism, humans are often the weakest element and are being duped into various kinds of scams, fraud, or phishing schemes. Many of these crimes are not new but have simply transitioned to cryptocurrencies because they are anonymous and make fraudulently obtained funds nearly impossible to recover.

Criminal Content

Blockchain-based technologies may also be used to create distributed, persistent storage of illicit content (e.g., child sexual abuse material). The LBRY protocol, for example, was intended to be a censorship-resistant publishing mechanism (LBRY, undated-b). Although LBRY's parent organization has protocols that make it difficult for users to come across illegal content, as long as the content is being hosted somewhere, the link to it will continue to function and will be available to users (LBRY, undated-a). Criminal content has also reportedly been stored in the metadata of the blocks in at least one of the varieties of the Bitcoin-type blockchains, although a Bitcoin advocacy group disputes that this has occurred ("Child Abuse Images Hidden in Crypto-Currency Blockchain," 2019; Gibbs, 2018; Sedgwick, 2018; Schneier, 2021).

Existing Solutions Associated with Criminal Uses of Blockchain

Despite new difficulties, law enforcement has had some recent high-profile successes in addressing criminal uses of blockchain technologies. During May 2021, the servers of an important portion of the Colonial Pipeline's oil and gasoline infrastructure in the eastern United States were attacked by ransomware, making the pipeline inoperable and driving short-term fears of gas shortages. The hackers demanded a ransom payment of 75 Bitcoins, which were worth $4.3 million at the time (Northern District of California, 2021). The Colonial Pipeline company ultimately paid the ransom and resumed operations. Then, in June 2021, the Federal Bureau of Investigation was able to recover nearly 64 of those Bitcoins because they managed to obtain the private key to the hackers' Bitcoin wallet (Office of Public Affairs, U.S. Department of Justice, 2021). Also during 2021, law enforcement managed to catch a corporate employee who had embezzled funds through a wire-transfer scheme and then transferred those funds to the cryptocurrency exchange Coinbase. Investigators were able to work with Coinbase to identify the individual and seize the stolen funds.

Several tools exist that law enforcement can lean on to help resolve the identities of individuals using cryptocurrency in connection with criminal activity. For cryptocurrency assets to be useful in the real world, the owner of those assets needs to be able to spend or transfer them to obtain something else of value. Because transactions on a blockchain are typically public transactions, this process typically leaves a trail that can help investigators resolve the identity of the suspects. In addition, many cryptocurrency exchanges, especially U.S.-based ones, such as Coinbase and Binance.us, are required to follow the same Know Your Customer laws that U.S. banks must follow. This reduces the potential for anonymity in some cryptocurrency transactions. The identity of the accused individual in the recent case involving theft from the Sony Life Insurance Company was proven through the cooperation of Coinbase (U.S. District Court, Southern District of California, 2021). However, when law enforcement needs the cooperation of exchanges that are operated overseas, or is attempting to trace transactions that are initiated without the use of an exchange subject to the jurisdiction of the United States, it can be much harder to identify the individuals involved.

Several tools exist that law enforcement can lean on to help resolve the identities of individuals using cryptocurrency in connection with criminal activity.

Ownership of cryptocurrency is typically associated with the possession of a private key that can grant access to the account, or wallet, where those assets are held. There are open-source tools, such as BlockSci and GraphSense, that law enforcement can employ to get additional clues about the identity of the custodian of the private key (Kalodner et al., 2020; GraphSense, undated). However, these may require significant amounts of technical skill and computing power to operate. Most medium-sized and smaller law enforcement agencies might not have the appropriate skills or computing resources to leverage these open-source tools.

As with many other highly technical aspects of the justice system, especially digital evidence and the dark web, there are commercial providers who are increasingly bringing their resources to bear to assist law enforcement. Chainalysis, CipherTrace, and Elliptic are examples of commercial providers who run sophisticated tracking algorithms to follow the money and use clues in the data to identify and monitor problematic transactions and ultimately help law enforcement establish the identities of investigation suspects who are using cryptocurrency (Brown, 2021). One particularly notable example of this was in 2017, when U.S. Homeland Security Investigations used Chainalysis to track, identify, and build a case against individuals trafficking in child pornography (Greenberg, 2022).

In terms of training, there are some law enforcement–related resources currently available through such organizations as the National White Collar Crime Center (NW3C, undated). For example, NW3C released a "Bitcoin Investigative Field Guide" to provide basic training around cryptocurrency and best practices for collecting and preserving digital evidence (NW3C, 2017). In addition, professional-development events, such as Europol's global conference on digital currencies and crime, are available to share knowledge and best practices.

Report Organization

In the remainder of this report, we describe the Priority Criminal Justice Needs Initiative (PCJNI) workshop that we convened with the Police Executive Research Forum in August 2021, on behalf of the National Institute of Justice (NIJ), to identify and prioritize law enforcement needs related to blockchain and cryptocurrency. We then present a prioritized list of research and development needs identified by a group of subject-matter experts at the workshop. Finally, we explain the mechanics of blockchain technologies (Appendix A) and how we conducted the workshop (Appendix B).

WORKSHOP ON LAW ENFORCEMENT NEEDS RELATED TO BLOCKCHAIN AND CRYPTOCURRENCY

To identify and prioritize opportunities that are ripe for additional research investment, we and the Police Executive Research Forum convened a workshop of law enforcement practitioners and other experts with experience in blockchain technologies and their nexus with the criminal justice system. To recruit participants, we identified knowledgeable individuals through existing professional and social networks (e.g., LinkedIn) and literature published on the topic. We then extended invitations to those individuals to participate in the workshop and to participate in a series of group interviews in advance of the workshop.

During these interviews, which we conducted with all 14 workshop participants, we walked the group through different topics, including how the new blockchain technologies are likely to present new opportunities and affect law enforcement, both in the present and in five to ten years. Initially, our goal was to examine a variety of blockchain-related opportunities and potential pain points over a broad time horizon. However, as we began talking with participants, it quickly became apparent that one of the primary uses of blockchain technologies, cryptocurrency, is rapidly becoming something that police, prosecutors, and courts are having to deal with more and more every day. So, we narrowed the scope of our discussion to focus primarily on cryptocurrency, along with a few blockchain-related problems and opportunities with more–future-oriented timelines.

Following our interviews, we compiled a list of needs that were identified through the group interviews. We categorized the needs into four topic themes: (1) the use of blockchain technologies to support the criminal justice system, (2) officer training associated with understanding how blockchain technologies are used to facilitate crimes, (3) conducting crime and investigations with blockchain technologies, and (4) other issues. Then, we invited participants to attend three virtual focus groups using the teleconferencing platform Zoom. During these sessions, we walked the participants through the needs. As we worked through each topic area, we asked the participants to refine and improve the wording of the needs so that it reflected their collective perspective. In some cases,

PARTICIPANTS

John Bates
Attestiv

Pamela Clegg
CipherTrace

Alan Cohn
Blockchain Alliance

Michael Davidson
National Institute of Standards and Technology

Rahul Gupta
Orange County District Attorney (California)

Frederic Lemieux
Georgetown University

Maureen Murat
University of New Hampshire School of Law

Ergin Orman
New Jersey State Police

Jonathan Reifer
New York Police Department

Jeremy Rosenberg
New York District Attorney's Office

Pete Teigen
IBM

Erin West
Santa Clara County District Attorney (California)

Samson Williams
University of New Hampshire School of Law

Michael Yu
Montgomery County Police Department (Maryland)

new needs were added as a result of this process. In other cases, some needs were removed because, as a group, the participants decided that they were no longer worth prioritizing. For each category, we also showed the participants a list of miscellaneous "grab bag" topics that were mentioned during the interviews but not discussed thoroughly enough to define a need or an opportunity. At this stage of the workshop, the participants were free to identify anything in the grab bag that should be refined and fleshed out as a need. They were also free to suggest the addition of new needs, and, if the group concurred, these needs were added.

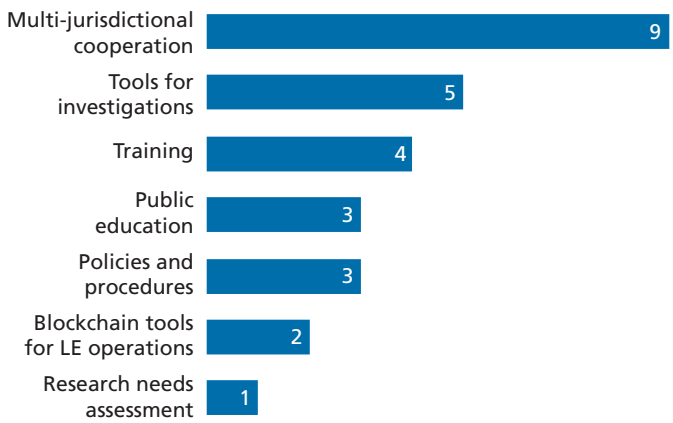
At the end of each topic area discussion, the participants took part in an exercise to prioritize each of the identified needs. The results from this prioritization activity are presented in the next section as a three-tiered list of 24 needs. More details about this process can be found in Appendix B.

RESULTS AND DISCUSSION

During the workshop, the participants identified and prioritized 24 needs, which we divided into three tiers. In this section, we explore those needs and present selected perspectives from the participants' discussion about the needs and the topic areas more generally.

To better understand the needs at a high level, we assigned them to categories. Depending on the issues they addressed, some needs were assigned to multiple categories. These are shown in Figure 1. As can be seen in the figure, multi-jurisdictional cooperation was the category most frequently associated with the needs identified by the participants. This was followed by tools for investigations. Emphasis was also placed on training, public education, and policies and procedures. During the prioritization process, the participants provided two votes for each need, one for the importance of the need and one for the need's probability of success when implemented.

Figure 1. Categories Associated with the Needs Identified by Workshop Participants



NOTE: LE = law enforcement. The numbers in the figure add up to 27 (instead of 24) because three needs were associated with two categories.

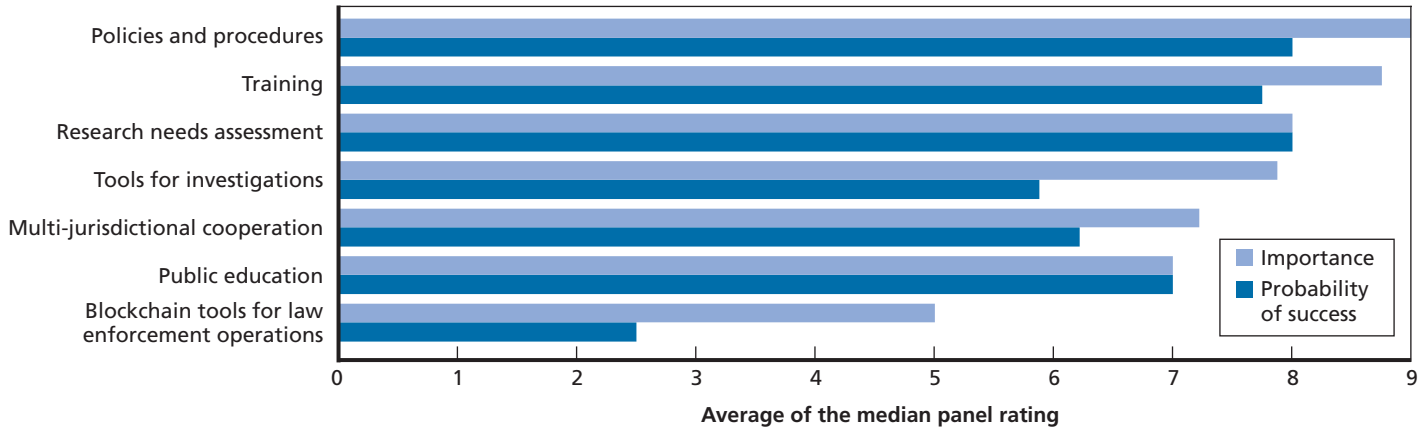
Figure 2 shows that the participants ranked needs associated with policies and procedures and training as both important and having a high probability of success. This is likely because law enforcement agencies already heavily rely on both of these approaches to provide guidance in difficult and unique situations; thus, they are viewed as useful and well proven. In Figure 1, we saw that the category most frequently associated with needs was multi-jurisdictional cooperation. In Figure 2, we see that the participants viewed needs relating to multi-jurisdictional cooperation as somewhat important but also much harder to implement. This is likely owing to the difficulty of cross-jurisdictional cooperation in general. There were two needs that involved developing tools that could be used within departments to improve operations or administration (i.e., the category of blockchain tools for law enforcement operations), which were collectively given the lowest level of importance and an even lower probability of success. This is likely because new information technology development in any organization can be difficult, especially if that organization does not already have personnel with the requisite skill sets.

Highest-Priority Needs

As described in Appendix B, the prioritized needs were split into three tiers. Of the 24 needs considered, ten rose to the top tier during the prioritization process. These needs are shown in Table 1. Most of the highest-priority, or Tier 1, needs are related to a need to develop additional policies, procedures, and training. As shown in Figure 2, this is because participants indicated that those needs were both very important and likely to be successful when implemented. Participants favored efforts that would make it easier for agencies to share training materials because this would reduce the level of time and effort to locate or develop training materials.

Participants observed that there are significant barriers to using commercial tools (e.g., cost) and open-source tools (e.g., computing resources and technical ability) for many agencies. As a result, they prioritized solutions in which larger coordinating entities (such as states and regions) could acquire those tools

Figure 2. Ratings of Importance and Probability of Success of Needs, by Category



NOTE: We used the median rating for importance and probability of success for each need. This had the effect of discounting extreme values on individual needs, but it likely had no significant effect when comparing topic areas.

and make them available to agencies on a more cost-effective basis. The last need in the top tier involves ways to make connections across jurisdictions. There are a number of commercial and nonprofit organizations that already perform this function (i.e., CopLink, CrimeDex, and NW3C), and participants said that at least one of them is already working in this space and would be best suited to take on the additional role of making these connections (Forensic Logic Coplink, undated; CrimeDex, 2019; NW3C, undated).

Second-Tier Needs

Table 2 contains Tier 2 needs. This is where many of the multi-jurisdictional cooperation needs landed. Collectively, the multi-jurisdictional cooperation needs address issues that agencies have with correlating and sharing relevant case information with other agencies that might be conducting investigations associated with the same criminals, the same types of criminal schemes, the same wallet addresses, or the same exchanges.

There is also a need for ways to explain blockchain's extremely technical and complex technologies and the investigation methods associated with them to other elements of the criminal justice system, such as judges and juries. The last need in Tier 2 involves public education. Often, law enforcement agencies deem it useful to provide notices or bulletins to the public about ways to improve their safety (Vermeer et al., 2022). These notices may involve flyers incentivizing people to lock their cars, or they might be shared via social media (such as on agency Facebook and Twitter accounts). Participants said that they could use help crafting these types of messages to educate the public about blockchain and cryptocurrency.

Third-Tier Needs

Table 3 contains the needs that landed in the lowest-priority tier (Tier 3). These needs are associated with multi-jurisdictional cooperation, tools for investigations (specifically, evidence handling), and blockchain for law enforcement operations. As illustrated in Figure 2, the participants collectively indicated that these needs are both not as important as and much harder to implement than the other needs.

Internationally, there is an interlocking system of bilateral treaties called *mutual legal assistance treaties* (MLAT). In the United States, these treaties are managed at the federal level, and the demand for working within their processes is high (Hill, 2015). The workshop participants found MLAT processes to be particularly difficult to navigate, especially for some smaller-value crimes, such as a demand for $300 in ransom via ransomware on a single individual's computer.

Participants discussed the possibility of using blockchain-based smart contracts (described in more detail in Appendix A) to govern information sharing between law enforcement agencies. If this was accomplished with a private blockchain system, then authorized agencies and investigators could request information via a smart contract, and the system could be used to provide notifications of changes. The primary advantage of such an approach is that there would not need to be a central organization operating the service. However, there would still need to be a consortium of some type that would manage access to the private blockchain and changes to the system over time. (See Appendix A for a more detailed discussion of smart contracts.) One participant also suggested using blockchain systems to store information about the public that requires destruction

Table 1. Tier 1 Needs

Category	Problem or Opportunity	Potential Solution
Training	There are not enough law enforcement–specific blockchain and cryptocurrency training and experts to meet the demand for educating justice practitioners.	Develop regional or national sharing systems that facilitate sharing of training materials and actionable intelligence for ongoing cases (e.g., digital or cyber fusion centers).
Policies and procedures	Cryptocurrency can be transferred by anyone in possession of an easy-to-copy digital key. Individuals with copies of the keys may move assets before an agency can take possession.	When seizing cryptocurrency assets, officers need to swiftly move the assets to a wallet controlled by the agency. Identify best-practice policies and procedures for rapidly securing cryptocurrency assets during investigations. (Exemplars include the U.S. Marshals Service, New Jersey State Police, and NW3C.)
Policies and procedures	Seized cryptocurrency assets can be transferred by anyone in possession of a digital key to a digital wallet of unknown ownership. This presents opportunities for officer misconduct.	Develop best-practice policies and procedures (e.g., two-person systems) to minimize opportunities for mishandling cryptocurrency.
Policies and procedures	Cryptocurrency assets can be transferred by anyone in possession of a digital key that is merely a unique set of letters and/or numbers (i.e., text). This text allows the bearer to control digital assets of high value and should not be treated like other text-based information within a case file.	Identify best-practice policies and procedures for handling, storing, transferring, and redacting digital cryptocurrency keys within record-management systems.
Training	There are not enough law enforcement–specific blockchain and cryptocurrency training or experts to meet the demand for educating justice practitioners.	Catalog and publicize the training resources that are already available, including training that is not tailored for justice practitioners.
Research needs assessment	Blockchain and cryptocurrency are fast-moving, rapidly evolving technologies. Justice practitioners are having difficulty keeping up with the changes.	Convene a standing group of practitioners and experts who can examine the "state of the possible" and generate requirements for research and development organizations.
Training	There are not enough law enforcement–specific blockchain and cryptocurrency training or experts to meet the demand for educating justice practitioners.	Develop model materials that can be easily adapted for training recruits, investigators, forensics experts, prosecutors, judges, and others.
Training	There is a lack of expertise in all aspects of blockchain and cryptocurrency technologies across the justice system.	Conduct research to examine the balance of skills and expertise that law enforcement agencies look for when hiring and assess whether those are likely to meet current and future needs.
Tools for investigations	Commercial cryptocurrency-tracking tools can be more expensive than an agency can afford. Open-source tools can require significant computing power.	Work with federal, state, local, and private entities (e.g., the Regional Computer Forensics Laboratory, Lawyers Without Borders) to make available appropriate cryptocurrency-tracking resources so that costs can be more easily shared.
Tools for investigations, multi-jurisdictional cooperation	Once a problematic cryptocurrency wallet is identified by law enforcement (via subpoena or another method), there is no good way to notify other interested investigators in other jurisdictions.	Assess the costs and benefits of developing a private-sector clearinghouse that will allow the public sector and vetted private-sector entities to coordinate (similar to how the National Center for Missing and Exploited Children screens potentially abusive materials).

Table 2. Tier 2 Needs

Category	Problem or Opportunity	Potential Solution
Multi-jurisdictional cooperation	Law enforcement agencies often face problems with cross-jurisdictional and cross-agency information sharing.	Develop and socialize prototype concepts for case information sharing on a permissioned,[a] private blockchain, potentially with automated connection notifications.[b]
Multi-jurisdictional cooperation	It is difficult to verify remote inquiries from individuals identifying themselves as law enforcement officers. (This includes civilian-to-officer or agency-to-agency verification.)	Develop a cross-jurisdictional distributed data system containing verifiable authentication information (i.e., digital signatures, quick response [QR] codes, or other verifiable information).
Multi-jurisdictional cooperation	Some cryptocurrency exchanges (including foreign exchanges) are voluntarily more compliant with the legal process (e.g., subpoenas) than others.	Develop a system for law enforcement to share contact information on blockchain exchanges and more (similar to what search.org operates for the mobile phone ecosystem).
Multi-jurisdictional cooperation	Crimes enabled by cryptocurrency technologies are not violent crimes and are frequently associated with smaller dollar values that are extremely difficult to recover. As a result, they often do not compete well for investigation and prosecution resources.	Develop tools for identifying and aggregating cryptocurrency-based crimes to raise their profile among the public and among justice system practitioners.
Tools for investigations	The lack of transparency within cryptocurrency tools results in difficulties for auditing cryptocurrency transactions.	Identify scientifically sound and valid best practices (using current practice, case law, independent validations, etc.) that are likely to be acceptable to judges, juries, and others.
Public education	Digital finance is rapidly evolving; as a result, there is additional potential for victims to lose large sums of money.	Conduct research to identify the scope of the problem, and disseminate educational information to appropriate law enforcement entities.

[a] A permissioned blockchain is one that is not publicly available and requires permission to access.
[b] Automated connection notifications would likely take the form of an email or a mobile device notification. They would occur when another law enforcement agency adds wallet addresses or other metadata of interest to the system and when the system is able to establish a connection between cases based on the metadata.

if it is not needed within a certain period (e.g., video analytic products, license plate reader data, some social media collections). The primary advantage for this use case is that destruction would happen automatically and potentially transparently. However, the participants did not add either of these selections to the full list of needs.

Workshop Discussion of Criminal Justice Concerns Related to Cryptocurrencies

In this section, we describe some higher-level themes from the interviews and the workshop discussions that were not directly associated with a single issue or need that was part of the prioritization.

Challenge of Anonymity

Some of the characteristics that make cryptocurrencies unique are also the sources of new challenges facing law enforcement agencies. As one participant noted, "cryptocurrency is a system designed for criminals because of its anonymity." However, even some prominent politicians have pushed back on that concept, suggesting that cryptocurrencies are no more anonymous than cash transactions (Hill, 2014). In truth, they are generally less anonymous because of the nature of the public ledger. Historically, law enforcement could rely on intermediaries, such as banks, to function as gatekeepers and identify who uses value-transfer systems. However, these intermediaries do not exist within the decentralized environment enabled by cryptocurrencies. Challenges continue to grow with enhancements to privacy-preserving features in some newer cryptocurrencies. For example, certain cryptocurrency services, such as Monero, offer users greater levels of anonymity. Such tools as mixers and tumblers, services that blend together several cryptocurrency transactions to enhance the chance of remaining anonymous

Table 3. Tier 3 Needs

Category	Problem or Opportunity	Potential Solution
Tools for investigations	Lack of transparency about cryptocurrency wallet ownership presents problems for investigations and court proceedings.	Identify attribution best practices (using current practice, case law, independent validations, etc.) that are acceptable to judges, juries, and others.
Multi-jurisdictional cooperation	Most cryptocurrency crimes are cross-jurisdictional.	Identify best practices for efficient cross-jurisdictional investigations.
Multi-jurisdictional cooperation	Many domestic and international justice agency collaboration processes (e.g., MLAT processing) are cumbersome and slow.	Develop and release a prototype federated (not centrally managed) and user-friendly legal cooperation tool designed around law enforcement's needs (which would likely rely on blockchain technologies, such as smart contracts).
Tools for investigations	It is difficult for law enforcement to identify clusters of wallet addresses that are likely to be connected with illicit activity. Current heuristics are imperfect and could inadvertently affect innocent individuals.	Conduct research to assess the accuracy of existing heuristics, appropriate uses for investigation and prosecution, and potential civil liberties implications.
Public education	Individual and organizational victims of fraud or scams are often unwilling to report the crime (because of potential stigma). Also, individuals and agencies are unaware of their reporting or response options.	Identify best practices for individuals, organizations, and agencies and disseminate them widely. (This should take into consideration potential long-term privacy issues from disclosing wallet addresses.)
Multi-jurisdictional cooperation, public education	Some cryptocurrency exchanges (including foreign exchanges) are voluntarily more compliant with the legal process (e.g., subpoenas) than others.	Conduct research to identify the reasons for compliance and, thus, ways to improve levels of compliance among other exchanges.
Multi-jurisdictional cooperation, blockchain tools for law enforcement operations	From time to time, there are errors in cross-jurisdictional and correctional recordkeeping, which can result in mistakes associated with the early or late release of an individual from jail or prison.	Explore the potential benefits of shared multi-jurisdictional data systems based on blockchain technologies.
Blockchain tools for law enforcement operations	It is difficult for law enforcement to prevent and investigate crimes associated with large supply chains.	Explore the benefits of how blockchain-based data systems could allow law enforcement practitioners to be more helpful to supply chain managers when property goes missing.

(U.S. Treasury Financial Crimes Enforcement Network, 2019), as well as zero-knowledge proofs that enable verification of information (Newman, 2019), can be used to make it even more difficult to track assets. Even when wallets associated with illegal behavior can be identified, they cannot always be readily associated with a particular person. Sometimes that person may be in an entirely different country. Also, when assets are successfully seized by law enforcement, it can be difficult or impossible to determine to whom they belong.

Because the sole source of ownership or control of a typical cryptocurrency is the private key (i.e., a long string of random text characters that serves as a password), there are additional considerations that affect agency investigations. When agencies seize funds in connection with an arrest or a criminal investigation, they need to move those funds into a wallet that is controlled by the agency alone. Because there can be more than one copy of a private key, agencies need to move swiftly to take custody of the funds controlled by that key. Some of the workshop participants reported that funds they were preparing to seize upon the arrest of a suspect were subsequently moved to a new address before they could seize them. This was likely because there was an accomplice with a copy of the private key who could move the funds.

The kind of anonymity that can be achieved when handling cryptocurrency funds can also be exploited by corrupt officials. In 2015, there was a notable case in which two federal agents were convicted of money laundering for transferring Bitcoin, Bitcoin Cash, Bitcoin Gold, and Bitcoin SV assets

worth nearly $60 million to wallets they personally controlled (Roberts, 2021). There are still thousands of Bitcoins (now worth hundreds of millions of dollars) associated with that case that remain unaccounted for. This speaks to the need for agencies to have adequate procedures and controls in place to minimize the risk of this kind of theft.

Handling of Private Keys to Access Cryptocurrency

Other issues arise when it comes to recognizing and handling private keys (and backups of private keys). As noted above, these are merely long strings of characters, and they can be handled in a variety of formats. With Bitcoin, a private key is basically a series of 44 to 64 characters; the length depends on the format. (See Appendix A for a more detailed description.)

This same string of characters can be converted into a QR code (see Figure 3), which allows it to be easily scanned by mobile phone cameras or other scan-capable technology.

Private keys can also be stored on paper. Paper-based wallets can merely be printouts or handwritten documents with strings of characters or QR codes. The information in Figure 3 can also be given a more professional-looking appearance through online and offline wallet-generation services. Figure 4 is an example of a paper wallet.

In addition, because the private key can be as valuable as the digital assets it protects, there are several methods to make backups or reconstitute them if needed. One form of backup is a set of human-readable seed words. If specific words are provided in a specific order to a key-generation algorithm, the private key can be reconstituted. The following is an example of a set of seed words (randomly selected from admin-slush, 2014):

> *crop delay biology dove blur inspire town mom pistol original ozone limb.*

Other, more-secure backups include a hardware wallet, which often looks like a USB thumb drive (see Figure 5).

Each of these methods for storing a private key represents an important artifact that arresting and investigating officers need to be aware of when attempting to secure evidence or digital assets associated with a crime (or crime scene). If officers do not recognize the value of such artifacts, valuable evidence (or leads) could be lost.

In general, seizing private keys and cryptocurrency assets requires the development of a legal framework or standard procedures for law enforcement. One participant explained that their jurisdiction requires two persons to be involved in any seizure of cryptocurrency, which can mitigate both mistakes and misconduct.

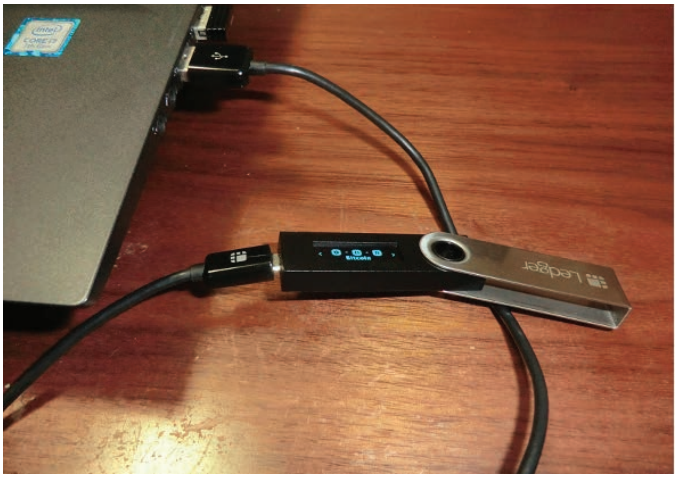
Figure 3. QR Code

SOURCE: Author-generated QR code reproduced from bitaddress.org.

Figure 4. Paper Wallet with Public Address and Private Key

SOURCE: Author-generated Bitcoin wallet reproduced from bitaddress.org.

Figure 5. Hardware Wallet



SOURCE: Reproduced from Wikimedia Commons, 2019.

Need for Training Across the Field

A major challenge related to the issues raised by participants is training. Participants agreed that there is a fundamental lack of training in the criminal justice system around blockchain- and cryptocurrency-related issues—not only for police,

who conduct cryptocurrency investigations, but also for other criminal justice actors, such as attorneys and judges, who must understand these technologies to properly adjudicate cases. However, such training is expensive and time intensive. Finding resources for investigators to get "keyboard time" is a critical need, according to some participants. One participant explained that the barrier to entry for investigators is extremely high, and complex technical knowledge is required to be effective. Participants stressed the importance of future-proofing and keeping trainings updated given the rapid pace of development in technologies.

With the growing salience of cryptocurrency-related crimes, participants suggested that training must be introduced during preservice training for all officers to begin building familiarity and understanding. Currently, training is typically limited to specialized units or individuals who serve on task forces. Alternatively, participants noted that law enforcement agencies can fill immediate gaps and build long-term foundations of knowledge by deploying targeted recruitment strategies to hire individuals with the requisite technological skills. Participants also noted the need for law enforcement agencies to protect their talent. Often, agencies lose highly skilled personnel to the private sector, where salary and benefits are more generous.

Need to Provide Resources to Small and Disadvantaged Agencies

Beyond the costs of training, there are also resource issues for law enforcement, particularly for local or smaller law enforcement agencies. Although there are many products to facilitate investigations involving cryptocurrency and tracking on a blockchain, they are typically very expensive and thus unavailable to law enforcement. Although there are some open-source tools available, they typically require technical knowledge to use and other agency resources to operate (e.g., dedicated server space). Participants identified possible solutions for smaller law enforcement agencies to have better access to these tools: federal grants, regional software-sharing agreements, management at the state level, and creation of a single entity that holds multiple licenses that can be shared with local law enforcement agencies on a case-by-case basis.

> Once cryptocurrency assets have been seized, agencies need to treat them similarly to other assets that can change in value.

Risks of Holding Cryptocurrency and Digital Assets

Once cryptocurrency assets have been seized, agencies need to treat them similarly to other assets that can change in value (e.g., stocks, collectible artwork). The U.S. Internal Revenue Service has declared that cryptocurrency assets should be treated similarly to property and other physical assets, such as gold (Aqui, 2014). Participants explained the difficulties of handling seized cryptocurrency assets because of their instability, referring to one case where cryptocurrency was seized and then converted to fiat currency, which lost value relative to the cryptocurrency, which climbed in value. The agency was sued and lost in court. Participants noted that it helps to consider cryptocurrency "high-risk" property, like expensive cars.

Coordination and Collaboration Challenges

As covered in prior PCJNI workshops (Hollywood et al., 2018a; Vermeer, Woods, and Jackson, 2018), systems for interjurisdictional cooperation exist both domestically and internationally. Domestically, often just a simple phone call or email between agencies can be sufficient to initiate cooperation, but even that step can be cumbersome if neither agency has the full picture of data and evidence needed to pursue a case. Workshop participants reported significant barriers when attempting to coordinate with agencies and officers who had little to no understanding of what blockchain technologies were and how cryptocurrencies were used.

Participants also noted the difficulty of working through MLAT processes. Some reported virtually closing an investigation when the word *MLAT* entered the discussion because negotiating the process would have required more investigatory resources than were available and appropriate to the case. Other participants reported that foreign law enforcement and commercial entities with useful information (e.g., exchanges) are sometimes willing to cooperate outside the MLAT process, which can streamline investigations.

The items at the top of the agenda are primarily focused on raising the level of knowledge for the average officer and investigator, training or hiring experts who can assist with investigations, and adapting existing policies and procedures to ensure that blockchain-based cryptocurrencies are handled responsibly.

CONCLUSION

As society's systems for transacting and interacting evolve, its systems for ensuring and enforcing individual and collective rights must keep pace in order to ensure justice for all. Blockchain-based technologies offer a lot of promise for facilitating much more efficient transactions and interactions in many areas that might not have benefited from the information technology revolution over the past 30 to 40 years. Unfortunately, new processes and new technologies often create or expand opportunities for criminals to take advantage of the differences, leaving law enforcement and the rest of the justice system struggling to catch up. To help elements of the justice system catch up, and potentially get in front of the problem, we have developed a prioritized research and development agenda to help inform potential public- and private-sector funders about where investment is needed most. The items at the top of this agenda are primarily focused on raising the level of knowledge for the average officer and investigator, training or hiring experts who can assist with investigations, and adapting existing policies and procedures to ensure that blockchain-based cryptocurrencies are handled responsibly. There are many needs that focus on the international and domestic cross-jurisdictional nature of cryptocurrency-based crimes, but these did not rise to the top of the list, in part because participants saw them as less important than improving individual agency and officer competencies and in part because they were viewed as too hard to implement (i.e., not likely to succeed).

The participants also explored some opportunities to develop blockchain-based information systems to improve agency efficiency. Needs were included that would facilitate data sharing across jurisdictions or help law enforcement investigate crimes occurring within large supply chains. Ultimately, these needs were given relatively low priority by the participants in favor of first investing time and effort in officer- and agency-level improvements in training and procedures. As mentioned earlier, the workshop was originally intended to focus on blockchain opportunities across law enforcement both today and in the future. However, the participants made it clear that there is an urgent and increasing need to start catching up today in cryptocurrency forensics and cryptocurrency investigation skills. If the justice system is unable to keep up or catch up in this domain, it will be the public who will suffer when their rights are violated and the systems that have been developed to detect and deter are not sufficiently effective.

APPENDIX A. BLOCKCHAIN TECHNICAL OVERVIEW

How Do Blockchain Technologies Work?

Blockchain, or distributed ledger technology, provides a way for a decentralized network of computers to agree on and manage a growing set of shared data records. Collectively managing data records can be applied to many other purposes in addition to cryptocurrencies, such as storing or sharing data; independently and autonomously executing agreements, such as contracts; or even voting (Nakamoto, undated).

Individuals, through their computers, interact with a blockchain network by sending (broadcasting) a data element (e.g., a block[3]) that they would like to add to the list. Other computers participating in the network then receive and process the new data element, following a procedure (algorithm) that the participants in the network have previously agreed upon. In some cases, this requires computers to solve a diffi-

cult math puzzle (known as *proof of work*). In others, it merely requires enough shares of the network's digital assets to be able to contribute (known as *proof of stake*). The process of adding new blocks to the shared list, or the blockchain, is called *mining*, and participants can earn digital assets by supporting the process (Buterin, 2017; Nakamoto, undated; Stockinger, 2022).

The algorithm that governs the addition of new blocks combines some information about the previous blocks with the new block that is being added using a kind of mathematical fingerprint, such as a hash function (Schneier, 2004). In this way, each new block of data is connected to the blocks that came before it, thus creating a chain. Because of the nature of this chain-linked fingerprinting process, the contents of a blockchain are typically not changeable by a single participating individual or organization (which is why blockchain is often said to be immutable). In many cases, there is no agreed-upon mechanism within a network for adjusting the contents of a blockchain (Condliffe, 2016; Nakamoto, undated).

For transparency, the contents of past blocks and their "fingerprints" are typically made publicly available (the shared ledger). One primary difference from most prior or existing data-management systems is that the only thing new individuals or computers need to do to interact with a blockchain system is to turn on a computer and install the cooperative software algorithm that the rest of the network is already running. For public blockchains, there is typically no central authority or permission-granting system that manages who participates, which computers connect, or what is contained within the blocks going into the blockchain (and, importantly, there is typically no central authority that can dictate alteration or removal of past blocks of data).[4] The software algorithm that governs how new pieces of data (blocks) are added to the existing collection of blocks (the blockchain) is called a *consensus mechanism* (Nofer et al., 2017).

Blockchain and Cryptocurrencies

The most well-known applications of blockchain technologies are for interacting with digital assets, such as cryptocurrencies. Everyday users typically interact with cryptocurrencies using a piece of software called a *wallet*. This software allows the user to communicate with the network of blockchain servers that are keeping track of transactions.[5] (From the user's perspective, this has some parallels with how a credit card works, in terms of presenting a "code" for payment.)

The wallet software helps the user keeps track of long strings of random text that are known as *keys* (like passwords). Keys are usually created in sets in which one key is intended to be kept secret and secure and the others are intended to be publicly shared. Keys are also used by the wallet to generate a wallet address, which is the functional equivalent of a bank account number. To send cryptocurrency assets to other users, the sender's wallet software assembles the data needed for the transaction (i.e., the "from" address, the "to" address, and the amount) and then mathematically "signs" that transaction with the sender's private key and broadcasts the transaction to the blockchain network for addition to the chain. Every transaction is verified by miners before being added to the blockchain to ensure that the sender has sufficient cryptocurrency and has not already spent that cryptocurrency. Figure A.1 summarizes the process of sending cryptocurrency funds over a blockchain.

The complex math (cryptography) behind these systems allows the computers participating in a blockchain network to validate that the transaction details, such as the sending address, signature, and associated public key, were generated from the secret private key. In this manner, the private key is the only means to certify ownership and authorize the transfer of assets in a blockchain-based cryptocurrency system. Because the only thing needed to control the movement of assets from a wallet address on a blockchain network is the private key, these systems are effectively anonymous. Even though the list of transactions (the ledger) is public, it can be difficult or impossible for anyone, including law enforcement, to determine who is in possession of a key or who "owns" a wallet address for any given transaction.

Not everyone participating in the cryptocurrency ecosystem directly manages their public and private keys. Because of the complexity of this process, some individuals have recognized a commercial opportunity and created businesses known as *cryptocurrency exchanges* (e.g., Coinbase, Binance). These exchanges function like online banks. To interact with an exchange, users will typically log into a website, or use a mobile phone app, with a simple username and password (and potentially an additional validation mechanism). Then, they can use the interface provided by the exchange to interact with cryptocurrency networks. These exchanges often accept credit card payments or bank transactions to convert traditional national currencies, known as *fiat currencies*, into cryptocurrencies, and vice versa. Importantly, as organizations similar to banks, exchanges often are legally required to know the identities of their customers and have some ability to hold or reverse transactions under their control (i.e., within their networks).

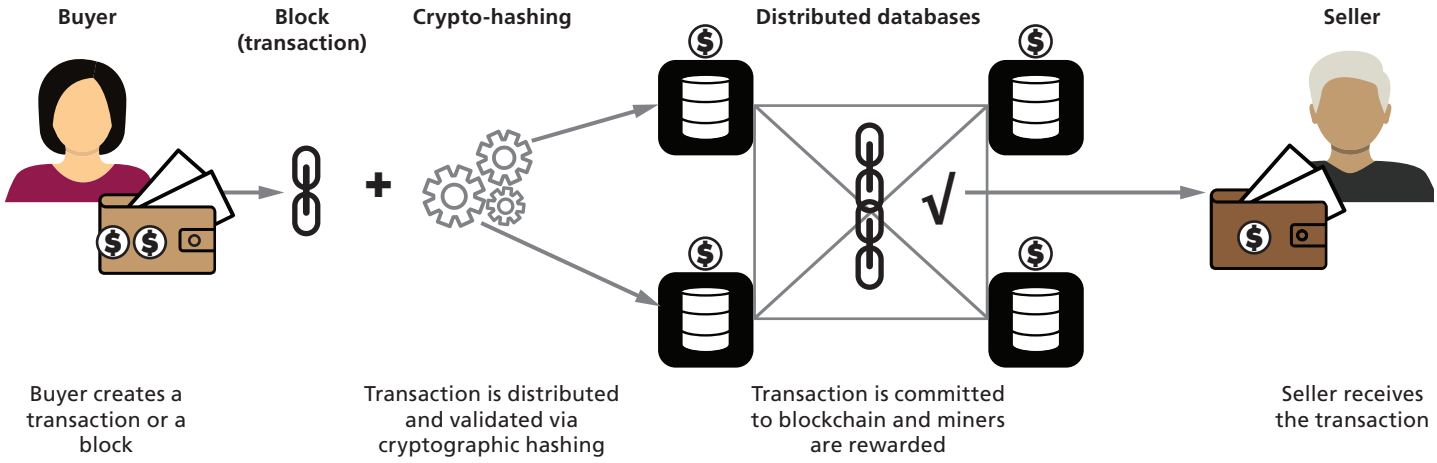
What a private key is and what it looks like are important for law enforcement officers at all levels to recognize. During contact with the public or while law enforcement is conducting an investigation, recognizing that a random string of numbers and letters could be used to manage cryptocurrency or facilitate a transaction could be an important detail. To help the reader understand this, several variations of a single Bitcoin private key are shown in Figure A.2. The first two variations use a version of wallet import format (WIF), which is shorter than the hexadecimal format and contains some embedded error-checking codes to help prevent typographical errors (Bitcoin Wiki, 2021).

Other Uses for Blockchain Technologies

As mentioned earlier, in addition to providing the complex algorithms needed to support cryptocurrencies, blockchain technologies can be used for many other purposes. For example, Ethereum, the second-largest blockchain network, is now used to power a variety of online blockchain applications that are not merely exchanges of digital assets. At the time of its creation, its primary innovation was the inclusion of a robust computer language called Solidity[6] that would facilitate a variety of automation and computation on the blockchain. Ethereum's computer language is often used to create what are known as *smart contracts*, which allow the computers on the network to automatically execute exchanges between participants on the network when certain conditions are met. Smart contracts can execute exchanges of cryptocurrency, but other sorts of data exchanges and instructions are permitted.

A nonfungible token (NFT) is an example of a smart contract that has received a significant amount of press attention recently (Dormehl, 2021). It is a digital certificate (an entry on a blockchain) that indicates that a certain wallet address is the "owner" of an asset (typically a digital asset, such as files,

Figure A.1. Process of Sending and Receiving Cryptocurrency on a Blockchain



SOURCE: Adapted from Wikimedia Commons, 2017.

Figure A.2. Various Text Representations of the Same Private Key

`5HuayatEW7ErhazKjbhadHsFX2bUmdgeKVE4axLeCMgU99Gzohx`
(Base58 WIF format)

`Kwd6xkZ8bUWG2921h2A7RBSo5Y3BzzuyibaepsFhB8HcnYyo9Ffa`
(Base58 compressed WIF format)

`0C08BAAF6840463E01B66BCAFA17C7DEC728E679AC8B66866FE72BB9805257D5`
(Hexadecimal format)

`544317741330751281267546806569282470253675024675354472304966338209723936558 9`
(Decimal format)

SOURCE: Author-generated text representations reproduced from bitaddress.org.

photos, or music, but it can also be a physical asset, such as certificates of authenticity). An NFT does not typically grant copyright or actual ownership of the asset or ensure the asset's permanence. Most often, the data stored on the blockchain are simply a hash function to a peer-to-peer file-sharing network or a hypertext transfer protocol (HTTP) URL where the digital asset is stored. The blockchain itself facilitates the sale and exchange of the asset and permits fractional ownership.

Other applications include distributed applications, or dApps, which provide similar functionality to what is found in more-traditional web applications (webpages) but without the centralized servers that most web applications rely on. The STORJ network (Kraken, undated-b; STORJ, undated) is an example of a system that relies upon the Ethereum network and allows people and organizations to store and share data in a decentralized way, using a "freemium" pricing model, similar to how people and organizations store data on Dropbox or Google Drive. Ethereum and other distributed functionality applications allow individuals or organizations to rent the computing power of hundreds or thousands of other computers—a service similar to those offered by Amazon Web Services or Google Cloud. Examples of networks that offer this functionality are Golem and iExec (Golem, undated; iExec, undated). Blockchain technologies are also being discussed as having the potential to improve or replace some of the systems that are relied on for loans and loan repayment, equity and ownership instruments, and derivatives (Clayton, 2021; Jena and Chauhan, 2021).

Another trend emerging from the blockchain and cryptocurrency space is called *decentralized finance* (DeFi). With DeFi, individuals can engage in more-traditional finance activities, such as lending or borrowing money or trading on the value of traditional financial assets, through a form of derivatives that is based on blockchain technologies (Schär, 2021); (Vlachos, 2022). It is likely that as adoption increases and money flows in, criminal activity will follow.

Blockchain technologies also have potential uses for efficiently managing democratically managed organizations. One common organizational scheme is called a *decentralized autonomous organization*. This is an organization that allows a group of people (or their computers) to make decisions by "voting" with the cryptocurrency or other tokens of ownership (Kraken, undated-a; Marr, 2022). There are situations where this could be used within the decentralized justice system in the United States. One current area is in the collection of crime statistics and other system-wide data.

The promise of blockchain-based applications has prompted major organizations, such as Mastercard, that use traditional electronic payment networks to begin exploring blockchain-based payment systems, "which promise . . . to deliver instant payments to merchants, fast-tracking for customers and secure verification of payments" (MintDice, 2019; see also Dhamodharan, 2021). The U.S. Federal Reserve is exploring a "digital dollar," which could make it "faster and cheaper to move money around the financial system"; however, only some of these explorations rely on blockchain technologies (Ackerman, 2021; see also Board of Governors of the Federal Reserve System, 2022). El Salvador has made Bitcoin a national currency alongside the U.S. dollar in hopes that it will reduce the high fees paid by those receiving remittances sent via traditional systems (Barber, 2022). Regulatory agencies, such as the Internal Revenue Service, have declared that cryptocurrencies are to be treated as property for the purposes of taxation (Aqui, 2014), while the Securities and Exchange Commission warned the creators of cryptocurrency assets to be careful that they do not also create securities that might then be subject to regulation (Anello, 2021).

APPENDIX B. WORKSHOP TECHNICAL APPENDIX

This appendix presents additional details on the workshop and our process for identifying and prioritizing research and technology needs and turning them into the research agenda that is presented in the main report. The descriptions in this appendix are drawn and adapted from previous PCJNI publications and reflect adjustments to the needs identification and prioritization process implemented at this workshop.

Workshop Scope and Participant Selection

The topics for PCJNI workshops are selected by reaching a consensus among the action officers and subject-matter experts at NIJ and research staff at the organizations that will be facilitating the workshop. Multiple topic areas, accompanied by brief scoping descriptions, are typically suggested months before the workshop by one or more of the parties involved, and staff engage in group deliberations with NIJ to reach consensus on the topic. We then engage in further scoping of the workshop to craft a discussion agenda through literature review, informal discussions with other practitioners and subject-matter experts, or both. Once the topic and scope have been determined, we

recruit participants by identifying knowledgeable individuals through existing professional and social networks (e.g., LinkedIn) and by reviewing literature published on the topic. We then extend an invitation to those individuals and provide a brief description of the workshop's focus areas.

The process of expert elicitation was designed to gather unbiased, representative results from experts and practitioners in the field. However, several limitations could affect the findings. The process typically elicits opinions from a relatively small group of experts. To limit the effect of group size on the representativeness of the results, we strive to make the group as representative as possible of different disciplines, perspectives, and geographic regions. However, the final output of the workshop likely is significantly influenced by the specific group of experts invited to participate. It is possible that the findings from the workshop would vary were a different group of experts selected. Moreover, although the discussion moderators make every effort to act as neutral parties when eliciting opinions from the collected experts, the background and experience of the moderators has the potential to influence which questions they pose to the group and how they phrase those questions. This could also introduce bias that could influence the findings.

Identification and Prioritization of Needs

To develop and prioritize a list of technology and policy issues that are likely to benefit from research and investment, we followed a process similar to processes we used in previous PCJNI workshops (see, for examples, Jackson et al., 2015; Jackson et al., 2016; and references therein). Participants discussed and refined needs that could address each problem. In addition, needs could be framed in response to opportunities to improve performance by adopting or adapting a new approach or practice (e.g., applying a new technology or tool in the sector that had not been used before). After identifying and refining the needs, we used a voting process based on the Delphi method, a technique developed at RAND, to elicit prioritization information from the group about the identified needs (RAND Corporation, undated).

Prior to the coronavirus disease 2019 pandemic, PCJNI workshops were conducted in person in a group setting. However, under the restrictions and mitigations implemented in response to the pandemic, our participants and staff were unable to travel. Our typical in-person format involves a two-day, 14-hour in-person meeting (eight hours the first day, six hours the second day). However, drawing on several organizations' and individuals' experiences in running and participating in high-intensity virtual events, we determined that it would not be advisable to try to directly replicate this meeting format using virtual conferencing tools. Instead, we prepared a multistage process:

1. interviews with each participant, either individually or in small groups, for approximately an hour to build an initial picture of their views and ideas
2. a set of shorter, more focused virtual sessions to provide the group with the opportunity to react to and shape the consolidated picture that came from our synthesis of the individual interview input
3. a final voting stage, after the last interactive session, in which participants provided their final assessment of the rankings of the different needs.

Interviews

During the interviews, we asked practitioner participants to discuss the challenges that they or their colleagues have experienced. We asked participants who were not practitioners (e.g., academics) to speak from their experiences working with practitioners. We also asked them to identify areas in which additional investment in research and development could help alleviate the challenges. During these discussions, participants suggested additional areas that were potentially worthy of research or investment. We consolidated and integrated the problems, opportunities, and potential solutions described by the participants in the separate interviews into a single summarized list. In advance of the first meeting of the virtual workshop, participants were provided with the list of issues and needs.

Virtual Sessions

Once each participant had been interviewed and the needs were consolidated, we held three two-hour virtual meetings using Zoom. These meetings were configured such that the participants could see each other's video feeds and collaborate to refine and edit the consolidated needs, which were shared from a moderator's desktop.

At the end of the discussion of each group of needs, participants were given an opportunity to review and revise the list of problems, opportunities, and potential solutions that they had identified. The participants' combined lists for each topic were displayed one by one on the screenshare portion of Zoom using Microsoft PowerPoint slides that were edited in real time to incorporate participants' revisions and comments.

Once the group reached consensus on a group of needs, we conducted a real-time voting prioritization exercise using Delphi techniques. We asked the participants to anonymously vote using a web-based polling system (the Anywhere Polling feature from Turning Technologies). Each participant was asked to score each need and the associated strategies to address those needs using a 1–9 scale for two dimensions: importance and probability of success.

For the *importance* dimension, participants were instructed that 1 was a low score and 9 was a high score. Participants were told to score a need's importance with a 1 if it would have little or no impact on the problem and with a 9 if it would reduce the impact of the problem by 20 percent or more. Anchoring the scale with percentage improvements in the need's performance is intended to help make rating values comparable from participant to participant.

For the *probability of success* dimension, participants were instructed to treat the 1–9 scale as a percentage chance that the need could be met and broadly implemented successfully. That is, they could assign the need's chance of success between 10 percent (i.e., a rating of 1) and 90 percent (i.e., a rating of 9). This dimension was intended to include not only technical concerns (i.e., whether the need would be hard to meet) but also the effect of factors that might cause practitioners to not adopt the new technology, policy, or practice even if it were developed. Such factors could include, for example, cost, effect on practitioner workloads, other staffing concerns, and societal concerns.

After the participants provided their individual ratings using the web-based polling system (i.e., for importance or probability of success), we displayed a histogram-style summary of participant responses within the polling system's interface. If there was significant disagreement among the participants, then they were asked to verbally discuss or explain their votes at one end of the spectrum or the other. (The degree of disagreement was determined by our visual inspection of the histogram.) If a second round of discussion occurred, participants were given an opportunity to adjust their rating on the same question. This process was repeated for each question and dimension at the end of each topic area.

Post-Session Prioritization

Once the participants had completed this rating process for all of the topic areas, we put the needs into a single prioritized list. We ordered the list by calculating a median expected value using the method outlined in Jackson et al., 2016. For each need, we multiplied the final (second-round) ratings for importance and probability of success to produce an expected value. We then calculated the median of that product across all of the respondents and used that as the group's collective expected value score for the need.

Next, we used a minimum variance method to hierarchically cluster the median expected value scores into three tiers. (We used the "ward.D" method in the "hclust" routine of the R statistical package, version 4.0.2.) We chose this algorithm to minimize within-cluster variance when determining the breaks between tiers. We chose to use three tiers in part to keep the methodology consistent across the set of technology workshops we have conducted for NIJ. Also, the choice of three tiers provides a manageable system for policymakers. Specifically, the Tier 1 needs are the priorities that should be the primary policymaking focus, the Tier 2 needs should be examined closely, and the Tier 3 needs are probably not worth much attention in the short term (unless, for example, they can be addressed with existing technology or approaches that can be readily and cheaply adapted to the identified need).

Because the participants initially rated the needs one topic area at a time, we gave them an opportunity at the end of the workshop to review and weigh in on the tiered list of all identified needs. The intention of this step was to let participants see the needs in the context of the other tiered needs and allow them to consider whether there were some that appeared too high or low relative to the others. Participants were able to see all of the ranked needs collected across all of the sessions; this provided a top-level view that was complementary to the rankings provided session by session. To collect the participants' assessments, we emailed the entire tiered list to them in a Microsoft Word document. The participants were then asked to examine where each of the needs landed on the overall tiered list and whether this ordering was appropriate or needed fine-tuning. Participants had the option to indicate whether each problem and need pairing should be voted up or down on the list. Table B.1 provides an example of this form.

We then tallied the participants' responses and applied those votes to produce a final list of prioritized and tiered needs. To adjust the expected values using the up and down votes from the third round of prioritization, we implemented a method equivalent to the one we used in previous work (Hollywood et al., 2016). Specifically, if every participant voted "up" for a need that was at the bottom of the list, then the collective effect of those votes should be to move the need to the top. (The opposite would happen if every participant voted

Table B.1. Example of the Delphi Third-Round Voting Form

Question	Tier	Vote Up	Vote Down
Tier 1			
Issue: Seized cryptocurrency assets can be transferred by anyone in possession of a digital key to a digital wallet of unknown ownership. This presents opportunities for officer misconduct. **Need:** Develop best-practice policies and procedures (e.g., two-person systems) to minimize opportunities for mishandling cryptocurrency.	1		
Issue: There are not enough law enforcement–specific blockchain and cryptocurrency training or experts to meet the demand for educating justice practitioners. **Need:** Catalog and publicize the training resources that are already available, including training that is not tailored for justice practitioners.	1		
Tier 2			
Issue: The lack of transparency within cryptocurrency tools results in difficulties for auditing cryptocurrency transactions. **Need:** Identify scientifically sound and valid best practices (using current practice, case law, independent validations, etc.) that are likely to be acceptable to judges, juries, and others.	2		
Issue: Digital finance is rapidly evolving; as a result, there is additional potential for victims to lose large sums of money. **Need:** Conduct research to identify the scope of the problem, and disseminate educational information to appropriate law enforcement entities.	2		
Tier 3			
Issue: Lack of transparency about cryptocurrency wallet ownership presents problems for investigations and court proceedings. **Need:** Identify attribution best practices (using current practice, case law, independent validations, etc.) that are acceptable to judges, juries, and others.	3		
Issue: From time to time, there are errors in cross-jurisdictional and correctional recordkeeping, which can result in mistakes associated with the early or late release of an individual from jail or prison. **Need:** Explore the potential benefits of shared multi-jurisdictional data systems based on blockchain technologies.	3		

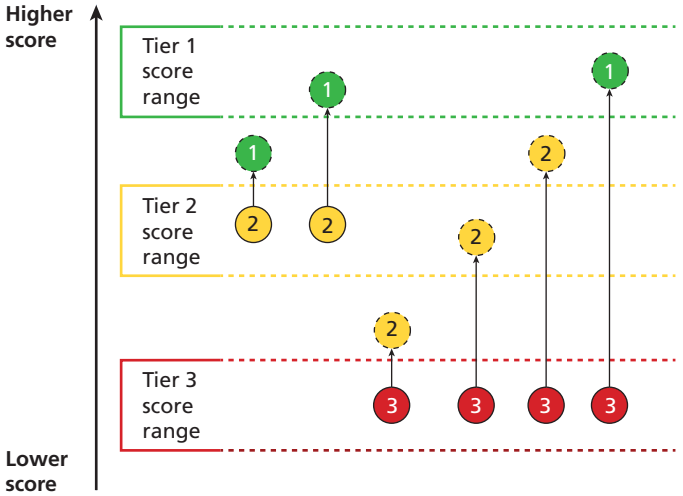
"down" for a need that was at the top of the list.) To determine the point value of a single vote, we divided the full range of expected values by the number of participants voting.

To prevent the (somewhat rare) situation in which small numbers of votes have an unintended outsized impact—for example, when some or all of the needs in one tier have the same or very similar expected values—we also set a threshold that at least 25 percent of the workshop participants must have voted on that need (and then rounded to the nearest full participant). For this workshop, there were 14 participants, so, for any votes to have an effect on changing a need's tier, at least three participants would have had to vote to move the need up or down.

After applying the up and down vote points to the second-round expected values, we compared the modified scores with the boundary values for the tiers to see whether the change was enough to move any needs up or down in the prioritization. (Note that there were gaps between these boundaries, so some of the modified expected values could fall in between tiers. See Figure B.1.) As with prior work, we set a higher bar for a need to move up or down two tiers (from Tier 1 to Tier 3, or vice versa) than for a need to move to the tier immediately above or below. Specifically, a need could *increase by one tier* if its modified expected value was higher than the highest expected value score in its initial tier. And a need could *decrease by one tier* if its modified expected value was lower than the lowest expected

value in its initial tier. However, to *increase or decrease by two tiers* (which was possible only for needs that started in Tier 1 or Tier 3), the score had to increase or decrease by an amount that fully placed the need into the range two tiers away. For example, for a Tier 3 need to jump to Tier 1, its expected value score had to fall within the boundaries of Tier 1, not just within the gap between Tier 1 and Tier 2. See Figure B.1, which illustrates the greater score change required for a need to move two tiers (one need on the far right of the figure) compared with one tier (all other examples shown).

Figure B.1. How a Need's Increase in Expected Value Might Result in Its Movement Across Tier Boundaries



NOTE: Each example need's original tier is shown by a circle with a solid border (the two needs starting in Tier 2 and the four needs starting in Tier 3). Each need's new tier after the third-round score adjustment is shown by the connected circle with a dotted border.

Applying these decision rules to integrate the participants' third-round inputs into the final tiering of needs resulted in numerical separations between tiers that were less clear than the separations that resulted when we used the clustering algorithm in the initial tiering. This can occur because, for example, when the final expected value score for a need that was originally in Tier 3 falls just below the boundary value for Tier 1, that need's final score could be higher than that of some other needs in the item's new tier (Tier 2). See Figure B.2, which shows the distribution of the needs by expected value score after the third-round voting process.

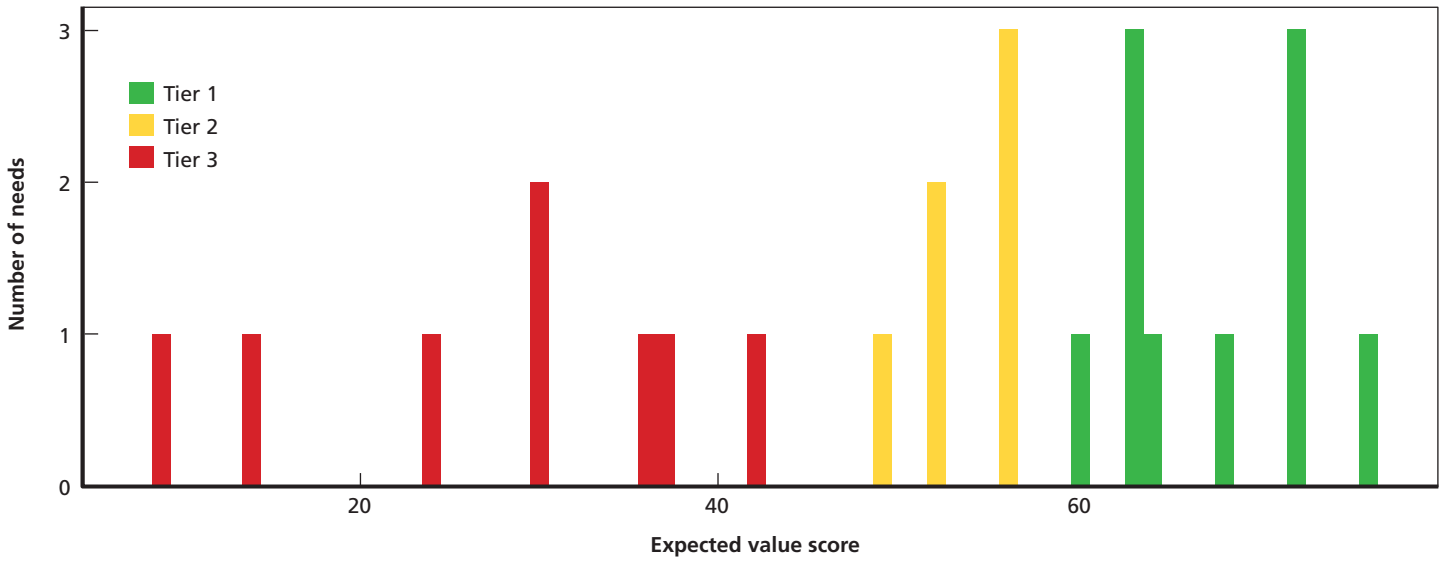
For the third round of voting, we received only a few changes from one participant. As a result, no needs changed position during the third round. The output from this process became the final ranking of the participants' prioritized results.

ENDNOTES

[1] It has become popular to refer to this new and innovative collection of blockchain technologies as *Web3*, or the third major version of the World Wide Web (Livni, 2021). This term is intended to refer to the decentralized and "democratized" web-based systems that are rapidly emerging and have the potential to become mainstream in the future. However, this is different from what was called *Web 3.0*, or the *Semantic Web*, which was previously examined by many of the authors of this report (Hollywood et al., 2015; Shannon, 2006).

[2] The handling of protective orders is plagued by challenges given paper-based processes that are handled by multiple independent organizations.

Figure B.2. Final Distribution of the Tiered Needs



[3] In practice, a block contains multiple data elements or transactions, but, for the purpose of explanation, we prefer this oversimplified version.

[4] There are other types of blockchain structures that include private and permissioned blockchains. However, because these blockchains have a governing body of one form or another, they are out of scope for the criminal investigation aspect of this report (but not for use as a tool to facilitate law enforcement operations and sharing).

[5] A wallet may contain multiple types of keys for multiple networks. Also, in many implementations, it is possible to generate more than one address (e.g., account number) per set of keys.

[6] Vitalik Buterin, the inventor of Ethereum, has emphasized that one of the key innovations of the computer language supporting Ethereum blockchain computation is the flexibility of the implementation of the language (i.e., that it is Turing complete so that it can be used to implement nearly any computer algorithm) and that it is *stateful*—i.e., it can store and carry information from one computation to the next (Buterin, 2016; Wang, 2017).

REFERENCES

Ackerman, Andrew, "Fed Prepares to Launch Review of Possible Central Bank Digital Currency," *Wall Street Journal*, October 4, 2021.

admin-slush, "bip39 english wordlist," GitHub post, February 7, 2014.

Anello, Robert, "Digital Art May Be Next in the SEC's Crosshairs," *Forbes*, July 15, 2021.

Antoniuk, Daryna, "Security Service Uncovers Crypto Mining Farm in Vinnytsia Allegedly Stealing Electricity (Updated)," *Kyiv Post*, July 12, 2021.

Aqui, Keith A., Notice 2014-21, Internal Revenue Service, 2014.

Barber, Gregory, "In El Salvador, Bitcoin's Libertarian Streak Meets an Autocratic Regime," Wired, January 2, 2022.

Bitcoin Wiki, "Wallet Import Format," webpage, last edited October 28, 2021. As of January 20, 2022: https://en.bitcoin.it/wiki/Wallet_import_format

Board of Governors of the Federal Reserve System, *Money and Payments: The U.S. Dollar in the Age of Digital Transformation*, Washington, D.C., January 2022.

Braaten, Claire Nolasco, and Michael S. Vaughn, "Convenience Theory of Cryptocurrency Crime: A Content Analysis of U.S. Federal Court Decisions," *Deviant Behavior*, Vol. 42, No. 8, August 2021.

Brown, Dalvin, "Tracking Stolen Crypto Is a Booming Business: How Blockchain Sleuths Recover Digital Loot," *Washington Post*, September 22, 2021.

Buterin, Vitalik [vbuterin], "This argument that 'computation' is something that is *oh so much harder* than 'verification', and that one is acceptably fast for a blockchain . . . ," comment on u/go1111111, "Greg Maxwell's critique of Ethereum: blockchains should do verification, not computation," Reddit post, 2016.

Buterin, Vitalik, "Proof of Stake FAQ," webpage, December 31, 2017. As of March 21, 2022: https://vitalik.ca/general/2017/12/31/pos_faq.html

Caldwell, Leslie R., "Assistant Attorney General Leslie R. Caldwell Delivers Remarks at the Securities Enforcement Forum West Conference," U.S. Department of Justice, May 12, 2016.

Cambridge Bitcoin Electricity Consumption Index, "Methodology," webpage, undated. As of March 9, 2022: https://ccaf.io/cbeci/index/methodology

"Child Abuse Images Hidden in Crypto-Currency Blockchain," BBC News, February 6, 2019.

Clark, Richard, Sarah Kreps, and Adi Rao, "Shifting Crypto Landscape Threatens Crime Investigations and Sanctions," *TechStream*, Brookings, March 7, 2022.

Clayton, Jay, "America's Future Depends on the Blockchain," *Wall Street Journal*, December 16, 2021.

CoinMarketCap, homepage, undated. As of November 15, 2022: https://coinmarketcap.com/

Coins Capture, "10 Use Cases for Blockchain Technology and Law Enforcement," Medium, August 4, 2020.

Condliffe, Jamie, "Is an Editable Blockchain the Future of Finance?" *MIT Technology Review*, September 20, 2016.

CrimeDex, homepage, 2019. As of November 15, 2022: https://www.crimedex.com/

Dave, Paresh, "Axon Boosts Encryption, Weighs Blockchain to Tackle Body-Cam 'Deepfakes,'" Reuters, October 3, 2019.

Dhamodharan, Raj, "Why Mastercard Is Bringing Crypto onto Its Network," Mastercard, February 10, 2021.

Dormehl, Luke, "A Brief History of NFTs," Digital Trends, March 10, 2021.

Federal Bureau of Investigation National Press Office, "FBI Statement on Recent Ransomware Attacks," press release, June 4, 2021.

Forensic Logic Coplink, "Coplink: Advanced Crime Analytics Platform," webpage, undated. As of January 19, 2022: https://forensiclogic.com/coplink/

Gibbs, Samuel, "Child Abuse Imagery Found Within Bitcoin's Blockchain," *The Guardian*, March 20, 2018.

Giri, Babu Nath, and Nitin Jyoti, "The Emergence of Ransomware," Pennsylvania State University, 2006.

Golem, homepage, undated. As of November 17, 2022: https://www.golem.network/

Goodison, Sean E., Jeremy D. Barnum, Michael J. D. Vermeer, Dulani Woods, Tatiana Lloyd-Dotta, and Brian A. Jackson, *Autonomous Road Vehicles and Law Enforcement: Identifying High-Priority Needs for Law Enforcement Interactions with Autonomous Vehicles Within the Next Five Years*, Santa Monica, Calif.: RAND Corporation, RR-A108-4, 2020. As of November 16, 2022: https://www.rand.org/pubs/research_reports/RRA108-4.html

Goodison, Sean E., Jeremy D. Barnum, Michael J. D. Vermeer, Dulani Woods, Siara I. Sitar, Shoshana R. Shelton, and Brian A. Jackson, *Wearable Sensor Technology and Potential Uses Within Law Enforcement: Identifying High-Priority Needs to Improve Officer Safety, Health, and Wellness Using Wearable Sensor Technology*, Santa Monica, Calif.: RAND Corporation, RR-A108-7, 2020. As of November 16, 2022: https://www.rand.org/pubs/research_reports/RRA108-7.html

Goodison, Sean E., Robert C. Davis, and Brian A. Jackson, *Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence*, Santa Monica, Calif.: RAND Corporation, RR-890-NIJ, 2015. As of November 15, 2022: https://www.rand.org/pubs/research_reports/RR890.html

Goodison, Sean E., Dulani Woods, Jeremy D. Barnum, Adam R. Kemerer, and Brian A. Jackson, *Identifying Law Enforcement Needs for Conducting Criminal Investigations Involving Evidence on the Dark Web*, Santa Monica, Calif.: RAND Corporation, RR-2704-NIJ, 2019. As of November 15, 2022: https://www.rand.org/pubs/research_reports/RR2704.html

Gourdet, Camille, Amanda R. Witwer, Lynn Langton, Duren Banks, Michael G. Planty, Dulani Woods, and Brian A. Jackson, *Court Appearances in Criminal Proceedings Through Telepresence: Identifying Research and Practice Needs to Preserve Fairness While Leveraging New Technology*, Santa Monica, Calif.: RAND Corporation, RR-3222-NIJ, 2020. As of November 15, 2022: https://www.rand.org/pubs/research_reports/RR3222.html

GraphSense, homepage, undated. As of January 19, 2022: https://graphsense.info/

Grauer, Kim, Will Kueshner, and Henry Updegrave, *The 2022 Crypto Crime Report*, Chainalysis, February 2022.

Greenberg, Andy, "Inside the Bitcoin Bust That Took Down the Web's Biggest Child Abuse Site," Wired, April 7, 2022.

Gromek, Michal, "Reclaiming Your Stolen Crypto—An Original but Blurry Service of Coinfirm," *Forbes*, January 31, 2020.

Hill, Jonah Force, "Problematic Alternatives: MLAT Reform for the Digital Age," *Harvard Law School National Security Journal*, January 28, 2015.

Hill, Kashmir, "Pro-Bitcoin Congressman Calls for Ban on U.S. Dollar Bills," *Forbes*, March 5, 2014.

Hollywood, John S., Michael J. D. Vermeer, Dulani Woods, Sean E. Goodison, and Brian A. Jackson, *Using Social Media and Social Network Analysis in Law Enforcement: Creating a Research Agenda, Including Business Cases, Protections, and Technology Needs*, Santa Monica, Calif.: RAND Corporation, RR-2301-NIJ, 2018a. As of November 15, 2022: https://www.rand.org/pubs/research_reports/RR2301.html

Hollywood, John S., Michael J. D. Vermeer, Dulani Woods, Sean E. Goodison, and Brian A. Jackson, *Using Video Analytics and Sensor Fusion in Law Enforcement: Building a Research Agenda That Includes Business Cases, Privacy and Civil Rights Protections, and Needs for Innovation*, Santa Monica, Calif.: RAND Corporation, RR-2619-NIJ, 2018b. As of November 15, 2022: https://www.rand.org/pubs/research_reports/RR2619.html

Hollywood, John S., Dulani Woods, Andrew Lauland, Sean E. Goodison, Thomas J. Wilson, and Brian A. Jackson, *Using Future Broadband Communications Technologies to Strengthen Law Enforcement*, Santa Monica, Calif.: RAND Corporation, RR-1462-NIJ, 2016. As of November 15, 2022: https://www.rand.org/pubs/research_reports/RR1462.html

Hollywood, John S., Dulani Woods, Richard Silberglitt, and Brian A. Jackson, *Using Future Internet Technologies to Strengthen Criminal Justice*, Santa Monica, Calif.: RAND Corporation, RR-928-NIJ, 2015. As of November 15, 2022: https://www.rand.org/pubs/research_reports/RR928.html

iExec, homepage, undated. As of November 17, 2022: https://iex.ec/

Integrated Justice Information Systems Institute, "Blockchain Technology Summit," 2019. As of January 5, 2022: https://www.ijis.org/page/blockchainsummit

Integrated Justice Information Systems Institute and Microsoft, "Agenda," Blockchain Technology Summit, 2019. As of January 5, 2022: https://cdn.ymaws.com/www.ijis.org/resource/resmgr/events/19blockchain_summit/blockchainsummit_agenda_0618.pdf

Internet Crime Complaint Center, *Internet Crime Report 2020*, Federal Bureau of Investigation, 2020.

Jackson, Brian A., Duren Banks, John S. Hollywood, Dulani Woods, Amanda Royal, Patrick W. Woodson, and Nicole J. Johnson, *Fostering Innovation in the U.S. Court System: Identifying High-Priority Technology and Other Needs for Improving Court Operations and Outcomes*, Santa Monica, Calif.: RAND Corporation, RR-1255-NIJ, 2016. As of November 15, 2022: https://www.rand.org/pubs/research_reports/RR1255.html

Jackson, Brian A., Joe Russo, John S. Hollywood, Dulani Woods, Richard Silberglitt, George B. Drake, John S. Shaffer, Mikhail Zaydman, and Brian G. Chow, *Fostering Innovation in Community and Institutional Corrections: Identifying High-Priority Technology and Other Needs for the U.S. Corrections Sector*, Santa Monica, Calif.: RAND Corporation, RR-820-NIJ, 2015. As of November 15, 2022: https://www.rand.org/pubs/research_reports/RR820.html

Jackson, Brian A., Michael J. D. Vermeer, Dulani Woods, Duren Banks, Sean E. Goodison, Joe Russo, Jeremy D. Barnum, Camille Gourdet, Lynn Langton, Michael G. Planty, Shoshana R. Shelton, Siara I. Sitar, and Amanda R. Witwer, *Promising Practices from Law Enforcement's COVID-19 Response: Protecting the Public*, Santa Monica, Calif.: RAND Corporation, RB-A108-1, 2021. As of November 16, 2022: https://www.rand.org/pubs/research_briefs/RBA108-1.html

Jeffery, Lynsey, and Vignesh Ramachandran, "Why Ransomware Attacks Are on the Rise—and What Can Be Done to Stop Them," PBS, July 8, 2021.

Jena, Jagjeet, and Harsh Singh Chauhan, "Decentralized Finance: On Blockchain and Smart Contract-Based Financial Markets," *International Journal of Trend in Scientific Research and Development*, May 2021.

Johansen, Alison Grace, "SIM Swap Fraud Explained and How to Help Protect Yourself," Norton, 2019.

Jolly, Jasper, "Police Find Bitcoin Mine Using Stolen Electricity in West Midlands," *The Guardian*, May 28, 2021.

Kalodner, Harry, Malte Möser, Kevin Lee, Steven Goldfeder, Martin Plattner, Alishah Chator, and Arvind Narayanan, "BlockSci," web tool, November 13, 2020. As of January 31, 2022: https://github.com/citp/BlockSci

Katkar, Pavan, *How I Learned to Stop Worrying and Love Blockchain: Implications and Applications of Blockchain*, dissertation, Pardee RAND Graduate School, Santa Monica, Calif.: RAND Corporation, RGSD-A1084-1, 2021. As of November 15, 2022: https://www.rand.org/pubs/rgs_dissertations/RGSDA1084-1.html

Kita, Jim, Tom Messerges, Anil Sharma, Anne Thompson, and Steven White, *Protective Orders Use Case Assessment*, Ashburn, Va.: Integrated Justice Information Systems Institute, 2020.

Kraken, "What Is a DAO? (Decentralized Autonomous Organization): The Beginner's Guide," webpage, undated-a. As of January 20, 2022: https://www.kraken.com/en-us/learn/what-is-decentralized-autonomous-organization-dao

Kraken, "What Is Storj? (STORJ): The Beginner's Guide," webpage, undated-b. As of January 20, 2022: https://www.kraken.com/en-us/learn/what-is-storj

LBRY, "Frequently Asked Questions," webpage, undated-a. As of January 19, 2022: https://lbry.com/faq

LBRY, "What Is LBRY Exactly? Is It a Protocol, an App, a Website, or a Company?" webpage, undated-b. As of January 19, 2022: https://lbry.com/faq/what-is-lbry

Livni, Ephrat, "Welcome to 'Web3.' What's That?" *New York Times*, December 5, 2021.

Marr, Bernard, "The Best Examples of DAOs Everyone Should Know About," *Forbes*, May 25, 2022.

McAdoo, Alex, "IJIS Blockchain Task Force Publishes Protective Order Use Case Assessment," press release, Integrated Justice Information Systems Institute, April 1, 2020.

Mechler, Bob, and Seth Rosenblatt, "Illicit Coin Mining, Ransomware, APTs Target Cloud Users in First Google Cybersecurity Action Team Threat Horizons Report," blog post, Google Cloud, November 23, 2021.

MintDice, "Mastercard vs. Visa: Blockchain Projects," blog post, February 10, 2019.

Nakamoto, Satoshi, "Bitcoin: A Peer-to-Peer Electronic Cash System," Bitcoin.org, undated.

National White Collar Crime Center, "About Us," webpage, undated. As of November 15, 2022: https://www.nw3c.org/about

National White Collar Crime Center, "Bitcoin Investigative Field Guide," 2017.

Newman, Lily Hay, "Hacker Lexicon: What Are Zero-Knowledge Proofs?" Wired, September 14, 2019.

Nofer, Michael, Peter Gomber, Oliver Hinz, and Dirk Schiereck, "Blockchain," *Business & Information Systems Engineering*, Vol. 59, No. 3, 2017.

Northern District of California, Affidavit in Support of an Application for a Seizure Warrant, San Francisco, Calif.: U.S. District Court, June 7, 2021. As of November 15, 2022: https://www.justice.gov/opa/press-release/file/1402056/download

NW3C—*See* National White Collar Crime Center.

Office of Public Affairs, U.S. Department of Justice, "Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside," press release, June 7, 2021.

Postman, Neil, *Technopoly: The Surrender of Culture to Technology*, Vintage Books, 1993.

RAND Corporation, "Delphi Method," webpage, undated. As of November 18, 2022:
https://www.rand.org/topics/delphi-method.html

Roberts, Jeff John, "Feds' $3 Billion Bitcoin Seizure Tied to Corrupt Federal Agents," Fortune, February 8, 2021.

Schär, Fabian, "Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets," *Federal Reserve Bank of St. Louis Review*, Vol. 103, No. 2, Second Quarter 2021.

Schneier, Bruce, "Cryptanalysis of MD5 and SHA: Time for a New Standard," Schneier on Security, August 19, 2004.

Schneier, Bruce, "Illegal Content and the Blockchain," blog post, Schneier on Security, March 17, 2021. As of January 19, 2022:
https://www.schneier.com/blog/archives/2021/03/illegal-content-and-the-blockchain.html

Sedgwick, Kai, "No, There Isn't Child Porn on the Bitcoin Blockchain," Bitcoin.com, March 21, 2018.

Shalvey, Kevin, "Take a Look Inside This Underground Crypto Mining Farm in Ukraine with Its 3,800 PlayStations and 5,000 Computers," *Insider*, July 11, 2021.

Shannon, Victoria, "A 'More Revolutionary' Web," *New York Times*, May 23, 2006.

Stockinger, Alwin [@Arnor1711], @tentodev, Ryan Cordell [@ryancreatescopy], Alex Ismodes [@qe], Victor Luna [@vluna], @selfwithin, Sam Richards [@samajammin], Julius Degesys [@JuliusDegesys], Mário Havel [@taxmeifyoucan], Seth Ariel Green [@setgree], et al., "Proof-of-Stake (POS)," webpage, Ethereum, last updated January 26, 2022. As of January 20, 2022:
https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/

STORJ, "How It Works," webpage, undated. As of November 15, 2022:
https://www.storj.io/how-it-works

Stroukal, Dominik, and Barbora Nedvědová, "Bitcoin and Other Cryptocurrency as an Instrument of Crime in Cyberspace," *Proceedings of the Business & Management Conferences*, International Institute of Social and Economic Sciences, 2016.

Tanneeru, Manav, "Can the Law Keep Up with Technology?" CNN, November 17, 2009.

U.S. District Court, Southern District of California, *United States of America v. Defendant BTC*, hearing, San Diego, December 20, 2021. As of November 16, 2022:
https://www.courthousenews.com/wp-content/uploads/2021/12/usa-ishii-forfeiture.pdf

U.S. Treasury Financial Crimes Enforcement Network, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies*, FIN-2019-G001, May 9, 2019.

Vermeer, Michael J. D., Jeremy D. Barnum, Siara I. Sitar, Dulani Woods, and Brian A. Jackson, *Amplifying the Speakers: Identifying High-Priority Needs for Law Enforcement Public Information Officers*, Santa Monica, Calif.: RAND Corporation, RR-A108-15, 2022. As of November 16, 2022:
https://www.rand.org/pubs/research_reports/RRA108-15.html

Vermeer, Michael J. D., Dulani Woods, and Brian A. Jackson, *Identifying Law Enforcement Needs for Access to Digital Evidence in Remote Data Centers*, Santa Monica, Calif.: RAND Corporation, RR-2240-NIJ, 2018. As of November 16, 2022:
https://www.rand.org/pubs/research_reports/RR2240.html

Vlachos, Andreas, "What Are DeFi Derivatives?" blog post, The Crypto App, January 11, 2022.

Wang, Kyle [@kyletwang], "Ethereum: Turing-Completeness and Rich Statefulness Explained," HackerNoon, July 6, 2017.

Wikimedia Commons, "Blockchain—Process," image file, December 4, 2017. As of November 17, 2022:
https://commons.wikimedia.org/wiki/File:Blockchain-Process.png

Wikimedia Commons, "Ledger Nano S—Hard Wallet—Cold Storage for Cryptocurrency 05," image file, July 26, 2019. As of November 17, 2022:
https://commons.wikimedia.org/wiki/File:Ledger_Nano_S_-_Hard_Wallet_-_Cold_Storage_for_Cryptocurrency_05.jpg

Williams, Samson, and Maureen Murat, "What Blockchain Means to the Justice and Public Safety Sectors," *IBM Supply Chain and Blockchain Blog*, March 12, 2019.

Wright, Turner, "Hackers Can Use Compromised Google Cloud Accounts to Install Mining Software in Under 30 Seconds: Report," Cointelegraph, November 26, 2021.

Zaytoun, Henry S., "Cyber Pickpockets: Blockchain, Cryptocurrency, and the Law of Theft," *North Carolina Law Review*, Vol. 97, No. 2, 2019.

Acknowledgments

The authors would like to acknowledge the contributions of the workshop participants identified near the front of the report. Without their willingness to participate in one-on-one interviews, three workshop engagements, and multiple rounds of voting on the priority and feasibility of different needs related to cryptocurrency and blockchain in law enforcement, this report would not have been possible. The authors also would like to acknowledge the contributions of Steve Schuetz, Joel Hunt, and other colleagues from the National Institute of Justice, who assisted with the development of the workshop and identification of participants. Finally, the authors acknowledge the valuable contributions of the peer reviewers of this report and the anonymous reviewers from the U.S. Department of Justice.

About the Authors

Dulani Woods is a data scientist at the RAND Corporation. He is adept at data acquisition, transformation, visualization, and analysis, and his research typically focuses on justice and homeland security policy. Woods specializes in maintaining and operating simulation models and has developed or maintained models designed to estimate potential policy impacts on justice outcomes and defense logistics, among other topics. He holds an M.S. in agricultural economics.

John S. Hollywood is a senior operations researcher at the RAND Corporation, where he conducts decision science and systems engineering research in the areas of criminal justice, homeland security, and information technology. His recent projects include leading development of a web resource on promising policing strategies and developing tools to predict areas at risk of increased crime. He holds a Ph.D. in operations research.

Jeremy D. Barnum is a research associate at the Police Executive Research Forum (PERF). He specializes in geographic information science, spatial data analysis, policing, and crime prevention. Prior to joining PERF, he was a project manager for the Rutgers Center on Public Security. He holds an M.A. in criminal justice.

Danielle Fenimore is a research associate at PERF, where she oversees a variety of federally funded projects, including a procedural justice experiment in Tucson, a test of an evidence-based investigative model in Topeka, and a national survey of police response to civil disturbances. Prior to joining PERF, she held a postdoctoral researcher position at the University of Memphis's Public Safety Institute. Fenimore holds a Ph.D. in criminal justice.

Michael J. D. Vermeer is a physical scientist at the RAND Corporation. His interests and expertise include science and technology policy, criminal justice, national security, cybersecurity, and emerging technologies, and his research portfolio includes work related to technology foresight and analysis guiding decisionmaking for homeland security, defense, the intelligence community, and government agencies. He holds a Ph.D. in inorganic chemistry.

Brian A. Jackson is a senior physical scientist at the RAND. His research focuses on criminal justice, homeland security, and terrorism preparedness, and his areas of examination have included safety management in large-scale emergency response operations, the equipment and technology needs of criminal justice agencies and emergency responders, and the design of preparedness exercises. He has a Ph.D. in bioinorganic chemistry.

Justice Policy Program

RAND Social and Economic Well-Being is a division of the RAND Corporation that seeks to actively improve the health and social and economic well-being of populations and communities throughout the world. This research was conducted in the Justice Policy Program within RAND Social and Economic Well-Being. The program focuses on such topics as access to justice, policing, corrections, drug policy, and court system reform, as well as other policy concerns pertaining to public safety and criminal and civil justice. For more information, email justicepolicy@rand.org.

About This Report

On behalf of the U.S. Department of Justice, National Institute of Justice (NIJ), the RAND Corporation, in partnership with the Police Executive Research Forum, RTI International, and the University of Denver, is carrying out a research effort to assess and prioritize technology and related needs across the criminal justice community. This research effort, called the Priority Criminal Justice Needs Initiative (PCJNI), is a component of the Criminal Justice Requirements and Resources Consortium (RRC) and is intended to support innovation within the criminal justice enterprise. For more information about the RRC and the PCJNI, please see www.rand.org/well-being/justice-policy/projects/priority-criminal-justice-needs.

This report is one product of that effort. In August 2021, RAND conducted an expert workshop on cryptocurrency and blockchain research needs for law enforcement. This report presents the proceedings of that workshop, topics considered, needs that the workshop participants developed, and overarching themes that emerged from the participants' discussions. This report should be of interest to criminal justice practitioners, administrators, and researchers who directly and indirectly interact with blockchain-based technologies in criminal justice contexts. Other RAND research reports from the PCJNI that might be of interest are

- Brian A. Jackson, Michael J. D. Vermeer, Dulani Woods, Duren Banks, Sean E. Goodison, Joe Russo, Jeremy D. Barnum, Camille Gourdet, Lynn Langton, Michael G. Planty, Shoshana R. Shelton, Siara I. Sitar, and Amanda R. Witwer, *Promising Practices from Law Enforcement's COVID-19 Response: Protecting the Public*, Santa Monica, Calif.: RAND Corporation, RB-A108-1, 2021.
- Sean E. Goodison, Jeremy D. Barnum, Michael J. D. Vermeer, Dulani Woods, Siara I. Sitar, Shoshana R. Shelton, and Brian A. Jackson, *Wearable Sensor Technology and Potential Uses Within Law Enforcement: Identifying High-Priority Needs to Improve Officer Safety, Health, and Wellness Using Wearable Sensor Technology*, Santa Monica, Calif.: RAND Corporation, RR-A108-7, 2020.
- Sean E. Goodison, Jeremy D. Barnum, Michael J. D. Vermeer, Dulani Woods, Tatiana Lloyd-Dotta, and Brian A. Jackson, *Autonomous Road Vehicles and Law Enforcement: Identifying High-Priority Needs for Law Enforcement Interactions with Autonomous Vehicles Within the Next Five Years*, Santa Monica, Calif.: RAND Corporation, RR-A108-4, 2020.

Mention of products or companies do not represent endorsement by NIJ or the RAND Corporation.

NIJ | National Institute of Justice
STRENGTHEN SCIENCE. ADVANCE JUSTICE.

This publication was made possible by Award Number 2018-75-CX-K006, awarded by the National Institute of Justice, Office of Justice Programs, U.S. Department of Justice. The opinions, findings, conclusions, and recommendations expressed in this publication are those of the author(s) and do not necessarily reflect those of the Department of Justice, the RAND Corporation, or the organizations represented by any of the workshop participants.

Research Integrity

Our mission to help improve policy and decisionmaking through research and analysis is enabled through our core values of quality and objectivity and our unwavering commitment to the highest level of integrity and ethical behavior. To help ensure our research and analysis are rigorous, objective, and nonpartisan, we subject our research publications to a robust and exacting quality-assurance process; avoid both the appearance and reality of financial and other conflicts of interest through staff training, project screening, and a policy of mandatory disclosure; and pursue transparency in our research engagements through our commitment to the open publication of our research findings and recommendations, disclosure of the source of funding of published research, and policies to ensure intellectual independence. For more information, visit www.rand.org/about/principles.

Limited Print and Electronic Distribution Rights

This document and trademark(s) contained herein are protected by law. This representation of RAND intellectual property is provided for noncommercial use only. Unauthorized posting of this publication online is prohibited. Permission is given to duplicate this document for personal use only, as long as it is unaltered and complete. Permission is required from RAND to reproduce, or reuse in another form, any of our research documents for commercial use.

For information on reprint and linking permissions, please visit www.rand.org/pubs/permissions.html. For more information on this publication, visit www.rand.org/t/RRA108-17.

© 2023 RAND Corporation

www.rand.org

RAND CORPORATION

The RAND Corporation is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest.

RAND's publications do not necessarily reflect the opinions of its research clients and sponsors. RAND® is a registered trademark.

RR-A108-17