SOAR

STATE-OF-THE-ART REPORT (SOAR)
SEPTEMBER 2023

CSIAC-BCO-2023-483

BLOCKCHAIN APPLICATIONS FOR FEDERAL GOVERNMENT

By Megan N. Lietha
Contract Number: FA8075-14-D-0001
Published By: CSIAC

This Page Intentionally Left Blank

SOAR

STATE-OF-THE-ART REPORT (SOAR)
SEPTEMBER 2023

BLOCKCHAIN APPLICATIONS FOR FEDERAL GOVERNMENT

MEGAN N. LIETHA

ABOUT CSIAC

The Cybersecurity & Information Systems Information Analysis Center (CSIAC) is a U.S. Department of Defense (DoD) IAC sponsored by the Defense Technical Information Center (DTIC). CSIAC is operated by SURVICE Engineering Company under contract FA8075-21-D-0001 and is one of the three next-generation IACs transforming the DoD IAC program: CSIAC, Defense Systems Information Analysis Center (DSIAC), and Homeland Defense & Security Information Analysis Center (HDIAC).

CSIAC serves as the U.S. national clearinghouse for worldwide scientific and technical information in four technical focus areas: cybersecurity; knowledge management and information sharing; modeling and simulation; and software data and analysis. As such, CSIAC collects, analyzes, synthesizes, and disseminates related technical information and data for each of these focus areas. These efforts facilitate a collaboration between scientists and engineers in the cybersecurity and information systems community while promoting improved productivity by fully leveraging this same community's respective knowledge base. CSIAC also uses information obtained to generate scientific and technical products, including databases, technology assessments, training materials, and various technical reports.

State-of-the-art reports (SOARs)—one of CSIAC's information products—provide in-depth analysis of current technologies, evaluate and synthesize the latest technical information available, and provide a comprehensive assessment of technologies related to CSIAC's technical focus areas. Specific topic areas are established from collaboration with the greater cybersecurity and information systems community and vetted with DTIC to ensure the value-added contributions to Warfighter needs.

CSIAC's mailing address:

CSIAC
4695 Millennium Drive
Belcamp, MD 21017-1505
Telephone: (443) 360-4600

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.
PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE September 2023	**2. REPORT TYPE** State-of-the-Art Report	**3. DATES COVERED**
4. TITLE AND SUBTITLE Blockchain Applications for Federal Government		**5a. CONTRACT NUMBER** FA8075-14-D-0001
		5b. GRANT NUMBER
		5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) Megan N. Lietha		**5d. PROJECT NUMBER**
		5e. TASK NUMBER
		5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Cybersecurity & Information Systems Information Analysis Center (CSIAC) SURVICE Engineering Company 4695 Millennium Drive Belcamp, MD 21017-1505		**8. PERFORMING ORGANIZATION REPORT NUMBER** CSIAC-BCO-2023-483
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) Defense Technical Information Center (DTIC) 8725 John J. Kingman Road Fort Belvoir, VA 22060		**10. SPONSOR/MONITOR'S ACRONYM(S)** DTIC
		11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT
Blockchain is an emerging technology with a growing number of applications across many industries. Understanding how blockchain technology can be implemented and utilized successfully requires understanding the fundamentals of the technology, its applications, its limitations, and what research and investment are still required to take it to its full potential. Some government organizations have already begun investing in this technology. Improvements to blockchain research and development, the datafication of available information, and the utilization of versatile and customizable solutions will help expand the technology's applications for more organizations and agencies.

15. SUBJECT TERMS
materials, electric propulsion, chemical propulsion, nuclear propulsion, nontraditional propulsion

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
U			UU	60	Vincent "Ted" Welsh
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(include area code)*
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED			443-360-4600

Standard Form 298 (Rev. 8/98)
Prescribed by ANSI Std. Z39.18

ON THE COVER:
(Source: iStock)

THE AUTHOR

MEGAN N. LIETHA

Megan N. Lietha is a writer and editor from Austin, TX, and is the publications manager at Texas Research Institute, Austin, Inc. She has written and edited for software companies, technology firms, independent authors, and small businesses. She has additional training in technical writing and editing and is a member of the Association for Proposal Management Professionals. Ms. Lietha holds a degree in professional writing from the University of Oklahoma's Gaylord College of Journalism and Mass Communication.

ABSTRACT

Blockchain is an emerging technology with a growing number of applications across many industries. Understanding how blockchain technology can be implemented and utilized successfully requires understanding the fundamentals of the technology, its applications, its limitations, and what research and investment are still required to take it to its full potential. Some government organizations have already begun investing in this technology. Improvements to blockchain research and development, the datafication of available information, and the utilization of versatile and customizable solutions will help expand the technology's applications for more organizations and agencies.

ACKNOWLEDGMENTS

The author would like to extend a special note of appreciation to John Noltensmeyer for his time spent answering questions and providing useful resources for the research of this report.

CONTENTS

CONTENTS, *continued*

CONTENTS, *continued*

TABLES

This Page Intentionally Left Blank

SECTION 01 INTRODUCTION

Blockchain has emerged as a popular technology, particularly in concert with the rise in cryptocurrencies ("a digital currency designed to work as a medium of exchange through a computer network that is not reliant on any central authority, such as a government or bank, to uphold or maintain it" [1]) such as Bitcoin and Ethereum. The term blockchain has been used interchangeably with other technology buzzwords such as distributed ledger, peer-to-peer (P2P) network, and decentralized networks in media. However, blockchain itself is an established technology that refers to a network system that utilizes certain protocols and encryption techniques to create secure data storage and a distributed computing system. Blockchain is the technology that underlies Bitcoin and makes it work, and the unique features of blockchain are what helped to propel Bitcoin to success. In turn, the successful execution of a blockchain concept led to continued innovation of blockchain-based applications across a variety of sectors, which are still evolving today.

Blockchain first gained public recognition when, in January 2009, Bitcoin (the first majorly successful cryptocurrency) was launched by an unidentified individual/group under the pseudonym Satoshi Nakamoto as a decentralized form of virtual currency [2]. Bitcoin initially grew slowly but eventually took off in the mid-to-late 2010s and skyrocketed to massive success in 2021, where it reached its peak value of $68,990/coin [2]. The key to its success was the technology that made it possible—blockchain. Nakamoto was the first to effectively combine cryptography and distributed computing in such a way, and blockchain technologies have continued evolving even after Bitcoin's rise and fall.

The next major blockchain application to follow Bitcoin was another highly successful cryptocurrency called Ethereum. Ethereum is distinct from Bitcoin in that it employs a different type of consensus mechanism [3], an element of blockchain construction that is described in Section 2.1. This change in blockchain construction meant that Ethereum was significantly less resource intensive to run than Bitcoin. As Ethereum's creators continued to update the technology, it was used for more diverse applications, including the launch of decentralized autonomous organizations, a sort of crowd-controlled entity making decisions with no centralized authority on the blockchain ecosystem. As more innovations on blockchain occurred, developers expanded the technology's applications to more business-focused goals.

While cryptocurrencies still operate, they have lost favor among the general public, as the model of unregulated currency has proven volatile and unreliable and they have been used to illegally finance criminal entities [4]. However, most people still only understand blockchain in relation to cryptocurrencies and do not recognize the broader applications it has in the modern age of digital information. This report provides an overview of the elements that form a complete blockchain technology, discusses the benefits

and limitations of blockchain technology, provides examples and use cases of blockchain applications for government organizations, and discusses the potential of the technology and what kinds of research and investments are needed to reach that potential.

1.1 WHAT ARE DISTRIBUTED LEDGERS AND BLOCKCHAINS

Blockchain is a term that means different things to different people depending upon the context. Blockchain is not a cryptocurrency, though it does support the operation of cryptocurrency networks. It is not synonymous with distributed ledger, though they do have a relationship. Rather, according to Daniel Drescher in *Blockchain Basics: A Non-Technical Introduction in 25 Steps*, blockchain can have three meanings. Blockchain is the data storage structure of linking blocks of data together in a chain; it is the algorithm or sets of protocols that instruct a network's operations; and it is the technology suite of data structure, algorithms, and applications that form a P2P distributed system [5]. When used generally, the term blockchain refers to the technology suite and not specific parts of a system.

1.1.1 Distributed-Ledger Technology (DLT)

DLT is a form of ledger or record that is not kept centrally in one location (see Figure 1-1). Rather, it is held by nodes on a decentralized network, also called a P2P network, where the ledger is replicated and kept by each node on the system. Nodes are "individual computers…which make their computational resources (e.g., processing power or storage capacity, data, or network bandwidth) directly available to all other members of the network without having any central point of coordination. The nodes in the network are equal concerning their rights and roles in the system" [5]. These nodes are any device connected to a shared network that collectively share information on the ledger.

A simplified way to visualize how P2P works is to imagine a group of 10 people who each have a copy of a book, and an 11th person asks to make a copy of the book (rather than each person checking a copy out from the library, aka the centralized ledger). The book is made up of individual chapters, representing the blocks of data in a chain. For representation purposes, pretend the chapters can be reviewed independently of each other.

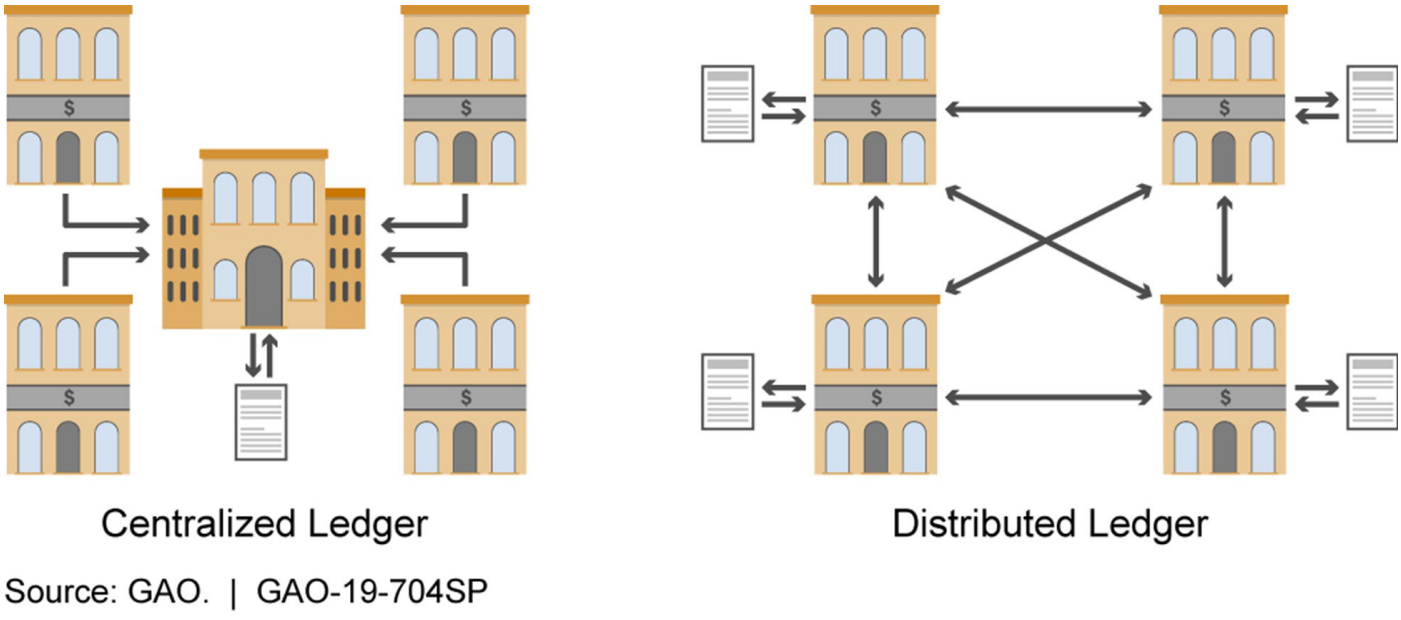

Figure 1-1. Government Accountability Office (GAO) Visualization of How DLT Differs From Traditional Centralized Ledgers *(Source: Persons [6])*.

It may be that some of those 10 people are unable to provide some chapters of the book at the time of the request, as the chapters are being viewed or copied by someone else. The new person wishing to gain a copy of the book must gather the different chapters from multiple people in the group to compile a full copy. Once the 11th person has compiled a copy of the book (the ledger), that person is part of the network, having a full copy of the book from which new users/members can gather copies of chapters as well. This is not unlike music and movie torrenting systems on the internet, where larger downloads are split apart into smaller packages and hosted across various user's computers from which the content can be downloaded by others. However, with a proper distributed ledger system, protocols and cybersecurity measures exist to prevent malicious attacks and protect the source data from manipulation.

Furthermore, in a distributed ledger, users can create new blocks and distribute them to others. In the case of the book example, users can all write additional chapters to the ledger and, through some predetermined method, chapters are verified by other members and added to the ledger. Distributed ledgers are built on this basic principle in that a commonly held record is shared in a "live" state by all participants.

The primary issue presented by simple DLTs and P2P networks is that they are vulnerable to bad actors who can inject incorrect information or otherwise disrupt the system and its collectively held record, even when security measures are taken. This issue is referred to as the Byzantine Generals Problem [7], and a rough diagram of how the problem affects a distributed ledger is shown in Figure 1-2.

The common example given to the Byzantine General's Problem is that of an army attacking a castle. The army is split into multiple camps surrounding the enemy fortress, with a commander

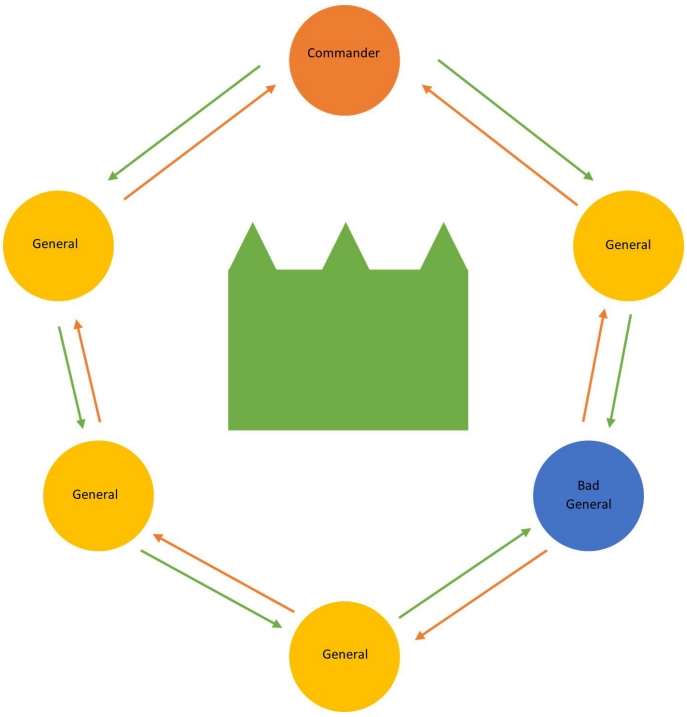

Figure 1-2. Byzantine General's Problem Diagram *(Source: M. N. Lietha)*.

and several generals commanding the different groups. When the commander of the army sends out the signal to attack (represented in Figure 1-2 by the green arrows moving away from the orange "Commander" circle), this message is propagated to the next general in the chain. If one of the generals changes the message, it will propagate further down the chain until it creates some form of conflict. This can be seen where the blue circle (labeled the "Bad General") changes the message from attack (represented by a green arrow) to retreat (represented by an orange arrow). This changes the message that is being sent between camps. In this example, rooting out the bad actor would simply require tracing the path of the message and noting where the change occurs, but, in a much larger network, this can be significantly more difficult, particularly if there are multiple malicious actors. This issue translates to distributed ledgers in computing systems. Overcoming this and related issues is where Satoshi Nakamoto's Bitcoin technology succeeded (at least to a certain

degree—there are further cybersecurity issues that are discussed later in this report).

The terms distributed ledger and blockchain tend to be used interchangeably in media, by experts, and sometimes in research, which can lead to confusion on the relationship of the words and their meanings. To simplify, DLT is the overarching technology concept and blockchain is a method of implementing the concept—distributed ledgers do not need to be composed of chains of linked blocks of data but can use other forms of data storage, sharing, and organization (one example of these alternative systems is called a directed acrylic graph [DAG]), as represented in Figure 1-3. Going a step further, Bitcoin and other cryptocurrencies such as Ethereum are the specific systems that use a unique blockchain architecture to accomplish a desired action. Each different blockchain system is defined by its own set of parameters and functions, each with its own particular strengths and weaknesses.

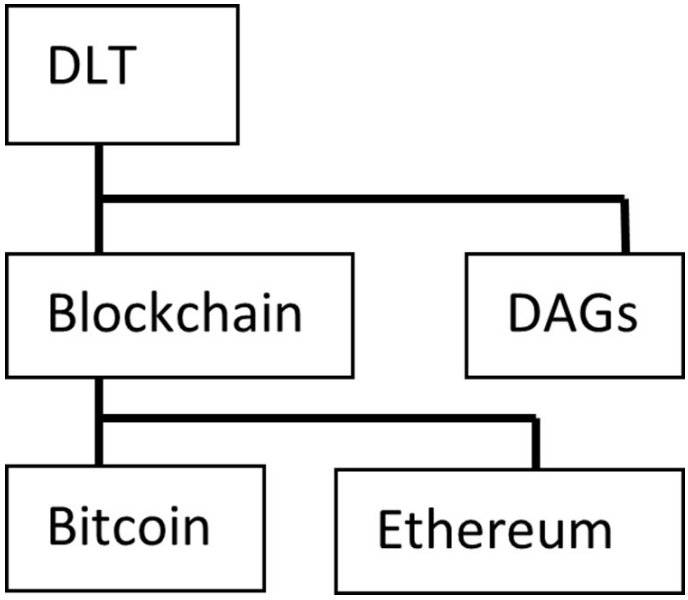

Figure 1-3. Diagram of the Relationship Between DLTs and Blockchains *(Source: M. N. Lietha)*.

1.1.2 Blockchain

In a blockchain, the ledger is composed of individual "blocks" of data that are "chained" together using encryption (see Figure 1-4). Each block consists of specific data points and is limited to a certain size, which is determined during the creation of the blockchain. In cryptocurrency, the data in the block would be the transaction record for the block. When a new block is generated, a majority of the network's nodes must verify the block (verifying involves confirming the source of the information and the integrity of the information/data) before it is cryptographically linked to the ledger. By requiring a majority consensus on the legitimacy of the block, the system ensures that no single bad actor can disrupt the record. Once consensus is reached, the block of data is added to the ledger by use of hashing and encryption techniques. This process makes the block immutable (unable to be edited or changed).

In extension of the book-copying metaphor, blockchain protects the network in that, if any new chapters are added to the book, at least half of the people in the group must view and approve the new chapters and confirm that they indeed come from an authorized owner of a book on the network before the chapters are added to the record. Additionally, pages are then sequentially numbered and superglued together so that they cannot be removed, rewritten, or rearranged.

Blockchain is not only useful for cryptocurrency. It is being employed across the financial sector for a variety of uses, such as in healthcare, energy management, supply chain management, real estate, and media, and as a tool for regulation, compliance, and auditing, in addition to a wide array of other uses. Employing blockchain effectively hinges on understanding its strengths and weaknesses and the best applications for the tool.

1.2 HOW ARE DISTRIBUTED LEDGERS AND BLOCKCHAINS USED

Blockchains and DLTs have the most application in environments where trust in and integrity of recorded data (the ledger) are highly necessary

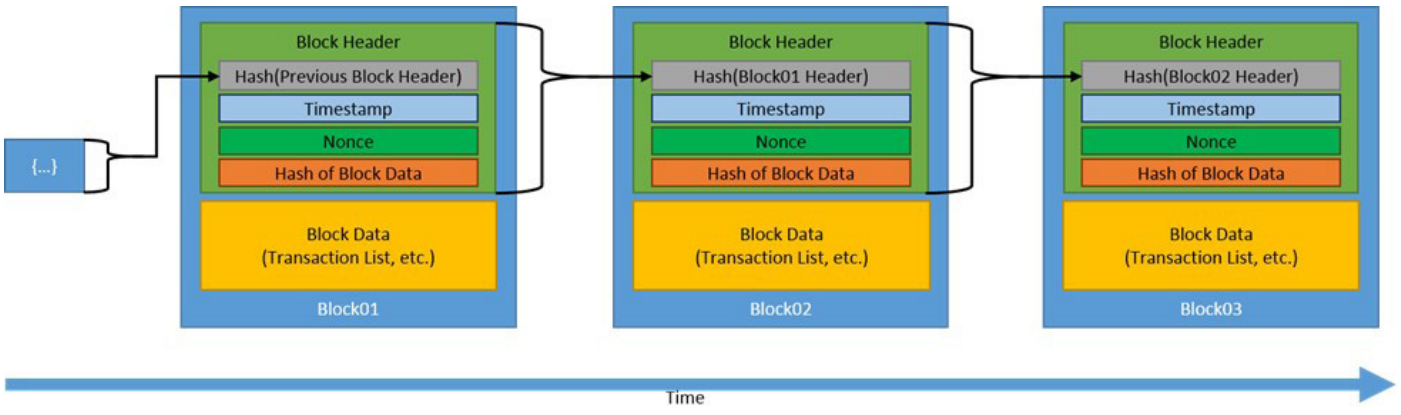

Figure 1-4. NIST Diagram on the Makeup of a Blockchain *(Source: National Institute of Standards and Technology [8])*.

functions in a system. Financial applications, for example, require a high level of trust in the data system to protect and accurately account for money and monetary transactions, hence, the strong relationship between the two. But blockchains work well for other instances where a strong historical record is important to business or organizational function. Another pertinent application of blockchain is in supply chains. Blockchain can provide an immutable record of the origins, processing, development, handling, and storage of goods and can collate this information from all of the multiple entities involved in the process. However, blockchain can also have drawbacks, including issues with scalability, resource use, implementation, and integration. Knowing how to implement a blockchain is one part of the challenge; knowing when and where to implement it is the other. Section 2 gives a deeper explanation of the technical aspects that make up blockchain technology and its specific capabilities and limitations, and Section 3 provides extensive examples of how the technology is being implemented, but this section provides an initial overview of the technology and how it is being used.

1.2.1 USE AND FUNCTION

In its most basic form, or the first iteration of blockchain technology, a blockchain is a set of protocols that direct a collection of nodes to operate a database that is used to securely transmit and store data in a decentralized network. This is how blockchain is used for Bitcoin. The different nodes that form the decentralized network make transactions of the currency, also called tokens, which are approved by the other nodes in the system and then linked by a hash, which is "a mathematical function that converts an input of arbitrary length into an encrypted output of a fixed length" [9]. In Bitcoin's blockchain structure, the hash in the header of Block01 is used in the data sequence recorded in Block02 (see Figure 1-4). Hashing is an irreversible process; because each block is linked to the hash in the previous block, the chain of data cannot be manipulated or changed without affecting the entire chain. Additionally, blockchains use cryptographic keys—strings of numbers used to represent a particular user on the network to track and identify who is making changes on the ledger. As stated, to prevent manipulation by bad actors, the nodes in the network work together to verify data accuracy through a process called consensus. Different blockchain systems use different consensus mechanisms, but all methods for consensus serve the system by providing trust, or the "assured reliance on the character, ability, strength, or truth of someone or something" [10].

Trust is an important element of blockchains and is a large part of what makes them a useful tool. The blockchain must keep correct and accurate records,

while also protecting privacy and preventing unauthorized changes to the ledger. Without trust, the ledger upon which the system relies would be undependable and users would abandon the system. In order to create trust, blockchains employ several tools, including ownership, transaction records, consensus mechanisms, hashes, and public and private keys. Keys are another element of the cryptographic aspect of blockchain technology, and they allow users to operate with privacy on an open network, while their transactions are still visible on the record. Keys are strings of characters (usually numbers) generated by the system to stand in place of identifying information such as a name or account information. Using Bitcoin as an example again, users of the Bitcoin blockchain have both a private key (represented by a certain string of numbers), which functions much like a password, and a public key (a different string of numbers), which is what other users on the system can use to send a transaction. The transaction with the public key is what is recorded on the blockchain, keeping the transactors' identities private. Only the private key is able to decode or access whatever data or digital commodity was transferred. This process is called asymmetric cryptography and is explained in more depth in Section 2.

Another development in blockchain technology is private, or permissioned, blockchains. While cryptocurrencies operate in the public sphere, not all blockchains need to be or should be public. The transparency of the ledger, which makes it a strength in public applications, is a hinderance to use in sectors where sensitive and private data need to be protected. This could mean private patient information in healthcare, sensitive government and military information, private entities wanting to protect intellectual property, etc. For example, if a company wants to keep an auditable record of a particular company activity, whether for compliance purposes or other internal use, it can set up a blockchain network with all employee devices connected as nodes but with no outside access to the system. Permissioned blockchains include some form of login or authorization process to access the system, and data are retained only by the permissioned devices on the network.

As blockchain technology has developed, further uses for blockchains have evolved. After Bitcoin's launch, the Ethereum blockchain was developed. Ethereum can be considered a second generation of blockchain, as it introduced the ability to execute applications on the blockchain, called smart contracts—"programs stored on a blockchain that run when predetermined conditions are met. They typically are used to automate the execution of an agreement so that all participants can be immediately certain of the outcome, without any intermediary's involvement or time loss" [11]. This pushed the application of the technology beyond simple transactional capabilities with tokens and allowed people to transfer goods and services and run applications while taking advantage of the immutable benefits of blockchains. Because of this advancement, more applications have been developed and demonstrated using blockchain technology.

1.2.2 Pros

Blockchains provide a host of benefits by virtue of their construction and operation and have led to new and innovative development of the technology. Blockchain is the first DLT to have successfully overcome the Byzantine Generals Problem, as previously explained. In computing, this problem is characterized by a situation where one of the decision-making actors in a system presents inconsistent and/or incorrect information to different observers (i.e., a server presenting as functioning to one observer and as nonfunctioning to another) [12]. Byzantine fault tolerance is the measure of a system's resiliency to such an issue [13]. Distributed systems are inherently susceptible to this problem, but the design of blockchains provide a solution to the issue with consensus mechanisms, which are explained in more detail in Section 2.1.

Blockchains also provide traceability and automation to eliminate human errors in data entry. Human error is a major hinderance to large database management and can occur from 1–4% of the time in data entry [14]. Data-entry errors can cost time and money to fix and lead to quality control issues and other harm. By allowing for thorough traceability of data using immutable blocks and automating data record-taking, blockchains can significantly reduce, if not eliminate, the chances for data-entry errors. When an error does occur, the blockchain can be audited to discover the inflection point.

Another benefit of DLT/blockchain systems is that they get rid of the "middleman" in transactional operations, also called disintermediation [5]. Increasingly, blockchains have the potential to cut out middleman entities from different sectors—this is most evident in the removal of banks (the centralized entity) from cryptocurrency systems. The blockchain removes the need for the central agency (bank) to hold a single master ledger and allows all participants in the system access to the ledger. This can allow people to transfer money or goods (i.e., eBay-like blockchain platforms) from P2P without the need to pay a transaction fee to a third party.

1.2.3 Cons

Counter to its many advantages and the success of the technology, blockchain does have drawbacks. Setting up and using a blockchain, or any DLT, requires a lot of computing power, and, in the case of blockchain, data size can only grow, as a blockchain ledger is "append-only," meaning that data can only be added, not removed or changed. Therefore, more data storage is required as time goes on and the ledger size grows. This is called a scalability issue [15]. As the stored data become too large, the system becomes more sluggish. This can happen at different rates depending on the system and how it is set up, but recent developments on blockchain have been addressing this issue and new solutions are now available to either eliminate or circumnavigate scalability problems. Depending upon the system in use, this may or may not still be an issue.

Blockchains are a great resource for storing, organizing, and tracking large amounts of data that need to be thoroughly logged and immutable. Blockchains excel in use cases where large amounts of data are being automatically generated by existing systems. Conversely, blockchain is not very effective where "datafication" is not already prevalent [16]. Trying to set up a blockchain in a sector where large quantities of data or automated data generation are not already a standard creates an additional barrier to adoption.

Blockchains deliver on the promise of being immutable and trustworthy, leading proponents of blockchain to laud it as "unhackable" [17]. However, cybersecurity is still very much an issue from multiple angles for blockchain and is one of the most fruitful areas for continued research on blockchain technology. While the blockchain itself is still considered to be "safe" in that its hashing-based construction would take massive amounts of computing power to decrypt, applications on the blockchain have proven to be susceptible to a variety of hacking attacks [18]. Blockchain cybersecurity is explored more in Section 4.

For all of these reasons, blockchain is not necessarily appropriate to use for every conceivable application but is instead best suited to any application where data must be recorded for audit or review/analysis purposes and/or when human data-entry error can interfere with quality of product or data output. Essentially, the best applications for DLT are in supply chain management, financial industry, and healthcare. Some lesser-known uses for blockchain include research (for data collection and retention) and security. Sections 2.4 and 3 elaborate further on the best use cases and examples of blockchain implementation across many sectors.

1.3 HOW CAN GOVERNMENT AGENCIES USE BLOCKCHAIN TECHNOLOGY

As blockchain changes the way users interact with the internet and each other, and as more applications for blockchain are discovered, governments are interacting with this technology more frequently. This can be as part of government administration to improve processes or address internal needs or also as a regulating authority in order to monitor potential mismanagement or abuse of or with the technology.

In the GAO report "Blockchain: Emerging Technology Offers Benefits for Some Applications but Faces Challenges," a myriad of possible opportunities for blockchain application are listed, from pharmaceutical supply chain management (Figure 1-5) to digital identifications and voting [19]. The GAO details benefits, as well as challenges, to each different application of blockchain. The report also goes in depth on how cryptocurrencies and transaction-based blockchains are affecting the financial sector. It is probable that decentralized finance, "financial services built using the decentralized foundations of blockchain technology," will play a significant role in shaping the future evolution of finance. Decentralized finance can provide benefits but also poses challenges and risks, especially to the global financial system. The GAO sets forth a formula for developing policy around the use and regulation of blockchain to mitigate risks posed by the technology, including setting standards, mandating oversight, developing educational materials, and defining appropriate uses for the technology.

Within the U.S. Department of Defense (DoD), several agencies have already begun to research and even implement blockchain technologies. One commonly considered application for blockchains is for logistics. Tracking and keeping tabs on military equipment and supplies, personnel, data, etc., is a monumental task that requires significant time and resources to manage. In 2019, the U.S. Army stated its case for developing blockchain technology to bring to bear the potential value "for developing digital tools to advance advantages in logistics planning within tactical, operational, and strategic environments" [20]. More applications and development of military blockchain projects are discussed in Section 3.1.

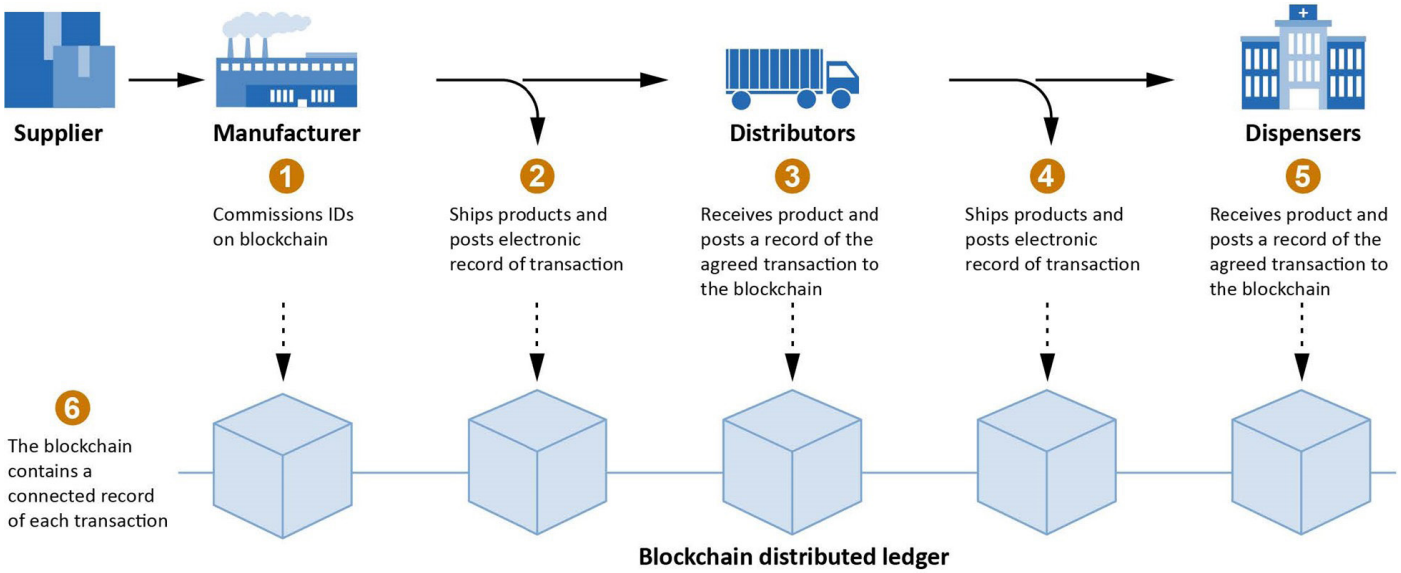

Figure 1-5. Potential Example of a Blockchain-Based Pharmaceutical Supply Chain Ledger *(Source: GAO [19])*.

One solution to the hurdles to adoptability is to utilize "ready-to-use" products or commercial-off-the-shelf blockchain technologies. Some government projects working on blockchain development have contracted companies to develop blockchain solutions for specific applications, but other projects are taking advantage of blockchains already developed in the commercial sector and adapting them to government needs [21]. This type of solution may prove to solve some of the barriers to entry that programs may face when wanting to implement a blockchain system.

This Page Intentionally Left Blank

SECTION 02 TECHNOLOGY

Blockchain in its basic function, as described in Section 1, is the first generation of blockchain technology. This technology is the original system designed by Nakamoto, which forms the backbone for Bitcoin and is the most well-known and understood iteration of blockchain technology. First-generation blockchain technology is well suited to recording transactions and storing data, hence its prominence in cryptocurrencies [22]. However, issues with scalability, slow speeds, and a lack of diverse applications led to the development of the next generation of blockchain.

Blockchain's second generation saw the advent of Ethereum, proof-of-stake consensus mechanisms, and smart contracts. The introduction of smart contracts made blockchain significantly more versatile. Now, "two users or organizations [could] do more than just simple cryptocurrency transactions" [22]. Smart contracts allowed users on blockchains to start performing significantly more complicated actions than simple monetary transactions. Decentralized finance and decentralized autonomous organizations also became feasible with the second generation of blockchain. These applications all sit above the blockchain, which acts as the sort of operating system for the applications and allows more freedom in activities available on the system. However, these applications involve writing new code to execute, and this has proven to create vulnerabilities in blockchain networks. Famously, Ethereum was forced into a hard fork, which split Ethereum into two separate blockchains after a vulnerability to a smart contract was exploited to siphon over 30 million dollars from a crowdfunding effort in 2016 [23, 24].

The third generation of blockchain technology refers to its use in enterprise applications. This level of application for blockchain requires significantly more resources, data, and maintenance. Enterprise blockchains suffer from a combination of weaknesses from the previous generations but provide the potential for significantly larger-scale use and application of the technology. Research into the application of large-scale blockchain technologies is ongoing.

2.1 THE FOUNDATION OF BLOCKCHAIN TECHNOLOGY

Different blockchain systems use a variety of different applications to execute their respective distributed networks. Blockchains begin at the node, and the basic data then block and build to include advanced applications and smart contracts. Many of the more basic elements of blockchains are elements that have existed for decades and are not in fact new to computing. A simple, basic blockchain can be developed with minimal work if the only need is for a system to record and store data in a date-stamped, continuous log [25]. Elements such as hashing, asymmetric cryptography, digital signatures, and even simple private/permissioned blockchain concepts have been around for a very long time. Advanced elements that have been developed in recent

years have used blockchain architecture as a sort of underlying layer upon which to build more complicated and useful applications. More work is required to incorporate elements for privacy, security, and immutability. It would be difficult to discuss an exhaustive list of each of these elements; therefore, an overview of the most common general tools and principles is given here.

2.1.1 Nodes

Nodes are added to a distributed network when the software/code for the blockchain system, called the client software, is downloaded and installed on a computing device (computers, servers, etc.) [26]. Nodes execute protocols written into the downloaded/installed client software and allow a user access to the distributed ledger or network. The protocols a node executes will depend upon its function within the network, and different client software may be needed for the different types of nodes in a network. Nodes are operated by the code they are given, not by human users; though, a human user can execute transactions or other actions on the blockchain by accessing the blockchain through a node [27]. While users can interact with applications on the blockchain, they should not be able to interface with other functions of the node, such as the consensus/validation mechanisms, or directly write onto the ledger (at least theoretically). See more on cybersecurity in Section 4. It is quite common, if not essential, for a blockchain to operate using multiple different types of nodes. There are several types of nodes that are typically used in blockchains, and each performs different functions.

The two main categories for nodes are full and light nodes. Full nodes retain a complete record of the recent ledger or transaction history to perform block verification functions [28]. Full nodes maintain the transaction or tracking data and can have voting rights (part of consensus mechanisms), meaning they partake in the validation of the blockchain [27]. Full nodes can be further subcategorized into pruned full nodes and archival full nodes. Pruned nodes serve the purpose of reviewing the blockchain and eliminating old transaction data to reduce file size. Pruning nodes keep only the metadata from transactions before a certain point in the blockchain (usually to maintain a record of a certain size [i.e., 500 MB or another set file size]). This allows full nodes to validate transactions from the most recent trusted block, without having to look back to the original, or genesis, block [28].

By contrast, archival nodes host the full blockchain record and maintain an archive or historical record of the blockchain and can take up a significant amount of space in the storage of the hardware hosting the node [29]. Archival nodes are subdivided again into authority, mining, and staking nodes. Authority nodes, as the name suggest, perform a moderating role on the blockchain. Authority nodes can perform different actions, including authorizing new nodes or regulating levels of access within the blockchain [30]. Mining nodes are somewhat of a misnomer—they are nodes that write new transactions to the block in proof-of-stake blockchains. The node itself is simply a node with the ability to write to the blockchain. For users to prove their stake and "win" a transaction, they must guess a randomly generated number or cryptographic puzzle. To do this, miners (the users operating the hardware running the node) must set up massive computing systems capable of running software to rapidly compute the correct number or answer within the fastest amount of time. This is where the debate about the resource and energy consumption of Bitcoin mining has propagated [31]. Staking nodes are another node used for proof-of-stake consensus mechanisms where, instead of cryptographic puzzles, users are rewarded randomly according to predetermined metrics [32]. Staking involves a certain amount of luck and rewards nodes with interest on transactions, and they do not require the computation resources that mining nodes do. Master nodes are also a type of archival node in that

they store ledger data and validate transactions but cannot write to the blockchain like other archival nodes [29].

Light nodes, in contrast to full nodes, do not store full records. These simple payment verifications communicate with full nodes to obtain the necessary data to process transactions and broadcast them for validation/consensus nodes [29]. There are two additional special nodes that do not fall under the full or light node categories. Lighting nodes allow for off-chain transactions to occur and then be broadcast onto the blockchain afterward to alleviate congestion in heavily active blockchains. This can be beneficial when two active participants, such as a customer and a café, agree to a transaction without needing consensus from the underlying network. Super nodes are specialty nodes that are typically used to perform specific tasks such as pushing updates to the blockchain, implementing protocol change, or maintaining reliable connections [27].

2.1.2 Blocks

Blocks on the blockchain are the data packages that are recorded and stored on the ledger. What data are stored, and how much data are stored in each block, is determined by the designer of the blockchain. In a supply chain application, the data recorded may include a timestamp, location tag, and temperature reading, along with the header of the block, hash of the previous block, and hash of the current block in the chain (Figure 1-4 illustrates the composition of a block of data). With digital signatures, the owner of the transaction can also be recorded. The block also contains a timestamp and a nonce, or "number only used once," in the header [33]. When a block is written, it is sent into a queue to be verified by the appropriate nodes [34]. Once a block is verified to have the correct information, it is broadcast to the other nodes in the network to be written into the blockchain or ledger. In a transactional blockchain, once this process is complete, the original transactor will receive the currency allocated to the transaction. In nontransactional blockchains, verified blocks are simply recorded as per the protocols of the system.

The first block in a blockchain system is called the genesis block. This block serves to synchronize the nodes on a network. "Synchronization is only feasible when [all] nodes' databases have the same genesis block" [35]. All blocks that have been validated and linked to the successive chain are considered valid blocks. As blocks are made, it is possible for two blocks to be generated at the same time, with both pushed to the network for validation at the same time. When this happens and both blocks are written to some of the nodes' ledgers, the system will eventually throw back errors in consensus on the state of the ledger. Depending on the blockchain, different solutions can be used to determine which block will be accepted and the unaccepted block is cast off and becomes an orphan block.

Block time is the measure for how long it takes a system to generate a new block and can range from seconds to minutes [36]. Early blockchains, especially Bitcoin, have very slow block times when considering the time as a representation of transaction speed compared to a modern centralized banking system. Modern credit-card transaction systems can support tens of thousands of transactions per second, whereas Bitcoin can process just seven [37]. Continuing development in blockchain has focused, in part, on improving block time for newer blockchain systems.

2.1.3 Validation and Consensus Mechanisms

Public distributed ledgers operate in an environment that lacks trust. If anyone can connect a node to the network anywhere around the world, there is no easy way to prove the credentials or good faith of that person or, more particularly, the node. Ensuring that nodes are operating in accordance with the rules of the DLT requires some method for validating the actions of nodes on the

network. This is where consensus mechanisms come in. By developing a method for nodes to supervise each other, a system of trust can be built. Not only are consensus mechanisms necessary for public blockchains, they also serve a purpose in private blockchains by continuing to prevent false acts (i.e., a faulty node or potential bad actor) and can create authority structures for approving block transactions.

Consensus mechanisms are composed of a few important elements. First, consensus mechanisms contain rules for validation [5]. These rules dictate how one node can confirm the truth of another node's actions. The correct information in the correct format must be present and describe the transaction correctly according to the validation rule. Additionally, the node performing the transaction must have completed any required actions or meet any requirements held by the validation rule. Second, most consensus mechanisms have some form of reward structure [5]. In cryptocurrency, the digital coin is the obvious reward for completing a transaction. However, even in nonmonetary blockchains, there can be rewards for nodes performing transactions. In a privately owned blockchain for a commercial company, the reward may simply be the ownership of the block or access granted for a node to information in a data-sharing application. Some consensus mechanisms have punishments for failing transactions, but these are not as common or necessary to the protocol. Third, consensus mechanisms can include elements of competition to drive quality of work performed on the blockchain. Competition may require speed, such as in puzzle-based consensus mechanisms, which reward the first node to solve the puzzle, or may require quality in the manner of high correctness of the data.

Finally, a consensus mechanism must have a set of rules dictating how to resolve dishonest or untrustworthy activities [5]. These rules will dictate how a node should select the "correct" history of the ledger when an untrustworthy action is presented or detected. When the necessary number or type of node(s) validate the transaction and ensure it is not an untrustworthy action, the block is officially pushed out to all nodes to be appended onto the ledger and the transaction (or action) is complete.

2.1.3.1 Proof of Work (PoW)

PoW is probably the most recognized consensus mechanism, as it is the protocol used by Bitcoin. The concept for PoW as a solution to the Byzantine General's Problem was first proposed by Leslie Lamport in 1982 [38]. "The solution states that to tolerate one arbitrary failure, the system requires at least four replicated nodes so that they can reach a consensus on a specific decision. A more generalized statement is that to tolerate f Byzantine failures, the system has to have $n \geq 3f + 1$ nodes." Two researchers proved the solution's application to a functioning algorithm in 1999, and then in 2008, Satoshi Nakamoto published the PoW protocols (based on the previous solution and proof).

PoW requires miners to solve a cryptographic puzzle to "mine" the next block on the chain [39]. Winning the race to solve the puzzle awards a Bitcoin. The puzzle and subsequent reward are classic examples of competition and rewards in consensus mechanisms. However, the heavy computing requirements for solving the puzzle means that more resources and, therefore, more energy are expended. The biggest drawback to PoW consensus mechanisms is that they involve high resource costs.

2.1.3.2 Proof of Stake (PoS)

PoS mechanisms are a popular and common alternative to PoW. PoS involves a level of randomness and protocols for selecting transaction validators based on given parameters [39]. In PoS, a node offers up a chosen number of coins as a stake. This essentially puts the node in a pool of other staked nodes, all waiting to be selected to validate

a new block. The node that is chosen is selected partially at random. The algorithm gives weight to the number of coins staked, the time since a node's last transaction, and any other number of factors as determined by the originator of the blockchain. PoS is popular because it does not require the resources for computing that PoW does. It can also have faster block times and transaction speeds. PoS mechanisms do have drawbacks, including requiring nodes to lock up a certain amount of currency in the staking process, and some nodes may be able to affect unequal influence on the algorithm for determining nodes for new transactions [39].

2.1.3.3 Delegated PoS

Delegated PoS modifies the original PoS concept by adding new roles for nodes [39]. These new roles are voters and delegates, where voters are the nodes staking coins and delegates are elected to validate transactions. Delegates who are elected to validate receive a portion of the transaction fee for the block, and voters split the block reward in accordance with the share they staked. Delegated PoS mechanisms do introduce a certain amount of centrality to the system with the designated node roles. Additionally, the delegated PoS can still be susceptible to power imbalances between nodes.

2.1.3.4 Proof of Authority (PoA)

PoA is a suitable consensus mechanism for private blockchains, which may not have a need to arbitrate transactions. In PoA, nodes stake their identity and reputation to become one of a selected group to validate transactions, build blocks, and maintain the network [39]. This method can allocate the administrative tasks of the blockchain to certain nodes, while allowing other nodes, perhaps employee computers, to retain computing resources. The system does create centralization, which counteracts some of the purpose of developing a decentralized network.

2.1.3.5 Others

Other forms of consensus mechanisms have been developed in recent years and utilize unique requirements for proving validity. "Proof of Capacity (PoC)...allow[s] sharing of memory space of the contributing nodes on the blockchain network. The more memory or hard disk space a node has, the more rights it is granted for maintaining the public ledger. Proof of Activity..., used on the Decred blockchain, is a hybrid that makes use of aspects of both PoW and PoS. Proof of Burn (PoB) requires transactors to send small amounts of cryptocurrency to inaccessible wallet addresses, in effect "burning" them out of existence" [40]. Further development of consensus mechanisms will focus on developing solutions to balance out weaknesses in existing mechanisms.

2.1.4 Hashing

Hashing is the process of transforming a string of characters into another value, typically of a shorter, fixed-length value that represents and makes it easier to find or employ the original string [41]. Generating a hash can be made one way with a one-way hash, and it generally cannot be undone or reversed without great computational burden [42]. Once a set of data, an input, has been passed through a one-way hashing algorithm, the resulting string of characters cannot be decoded into the original set of data in the input. The value of generating a hash in a blockchain is to output a completely unique value that cannot be replicated. This unique value becomes the unique identifier for a block in a blockchain, not unlike a human fingerprint being unique to an individual person. In writing a block to a blockchain and giving it a hash value, the block is uniquely identified. Additionally, as new blocks are added, they include the hash value of the block that came directly before. The hash from the previous block is included in the data value that is input to the hash algorithm for the new block and is written onto the data of the block, thereby creating an immutable

bond between the two blocks. Hashes are also used in blockchains as part of the public-key encryption process.

2.1.5 Asymmetric Encryption and Digital Signatures

Asymmetric encryption, also called public-key cryptography, is a cryptographic technique that uses a dual private- and public-key pair to encrypt and decrypt information. Asymmetric encryption uses two keys to encrypt and decrypt transaction data [5]. The public key is used like an address, sort of like a bank routing number, to which other users can send transactions. The public key encrypts the transaction onto the chain, like a key locking a door. The public key may be changed with each use so that it cannot be tracked to a single individual. The private key is a different key from the public one, and it acts like the key which can unlock the transaction (or decrypt it). In a public blockchain like Bitcoin, when a user's private key is written onto a block, while all other users can see that block on the ledger, only the user with the correct private key can decrypt the transaction. Private keys operate very much like passwords, but these passwords cannot be recovered if lost or stolen. Therefore, private keys need to be held carefully by users and not shared in any way.

As illustrated in Figure 2-1, if the person on the left wishes to transmit a message to the person on the right without anyone else on the distributed network being able to read the message, public key encryption can be employed [43]. For most public blockchains, encryption is required for all transactions on the blockchain. After the message is generated, a hashing algorithm is used with the recipient's public key to generate an encrypted output or data set to be transferred [44]. A digital signature is used to sign the data or message that is transmitted. Digital signatures can be generated through different cryptographic methods, but one method is to use a hash with the encrypted data and the sender's private key to create a unique signature or value. When the resulting information is sent to the recipient, the recipient may first use the sender's public key to decrypt the digital signature [44]. The decryption should result in a hash value that can be compared by the recipient with a new one-way hash of the same hash value. The resulting two values should match. After this, the encrypted data from the hash can be decrypted using the recipient's private key.

2.1.6 Smart Contracts

Smart contracts are not a required element to a blockchain, but they are one of the most useful functions that have been developed for blockchains. Smart contracts are coded contracts that operate and engage on the blockchain without the need for direct human input [45]. As an example, a lender may write a smart contract

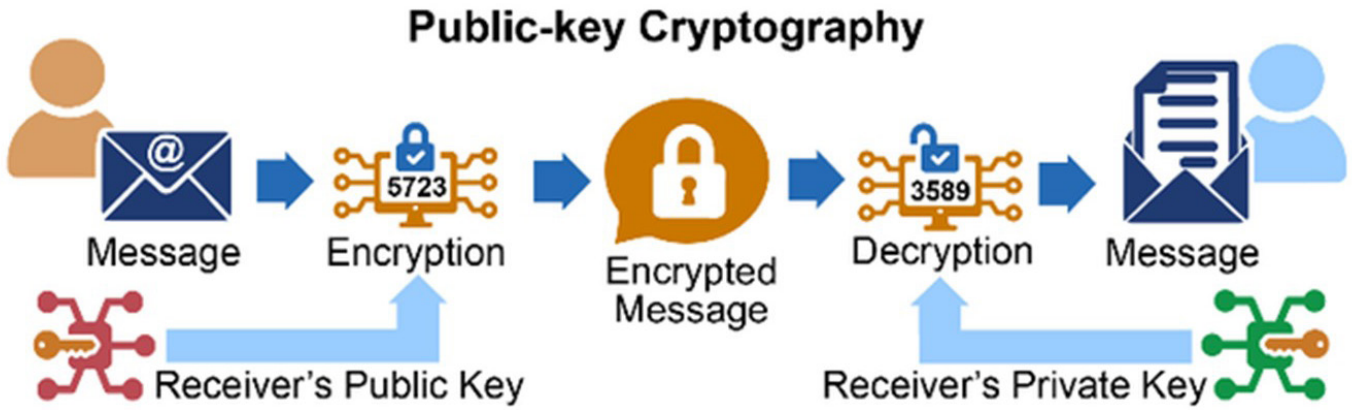

Figure 2-1. Illustration of Public-Key, or Asymmetric Encryption *(Source: GAO [43])*.

that keeps track of payments made on a car loan. When the loan has been paid off, the title for the vehicle would be digitally signed over to the loanee. Smart contracts can be written in a number of different codes and stored on the blockchain, and they are generally immutable. Smart contracts are best suited to enacting relatively simple or straightforward contracts, especially to lessen the possibility of crossing into legal grey areas. A post on the Harvard Law School Forum on Corporate Governance asks questions about the enforceability of smart contracts, their negotiation and adjudication, the ability to amend terms, the ability to incorporate ambiguity, and the validity of the final agreement [46]. Contracts written and adjudicated by humans are surprisingly flexible, but smart contracts, by nature of their construction, are not at all flexible. In straightforward contexts, smart contracts provide a robust tool to engage in contracting without necessitating human intervention, but any contract that requires ambiguity, flexible interpretation, or offline interaction should continue to be executed in traditional formats.

2.2 IMPLEMENTATIONS OF BLOCKCHAIN TECHNOLOGY

Blockchains can be deployed to very different kinds of networks, and network needs should be considered against blockchain capabilities in order to maximize the function of the system. If a system is public and requires anonymity, then logins should not be used and a public/private key system should be employed. If the network needs to allow certain nodes or users access to certain parts of the blockchain, a permissioned blockchain should be enabled. If the network needs to combine multiple user bases with independent blockchains, an alternative blockchain, such as the Hyperledger Fabric, should be considered for use. When setting up a blockchain, one of the most important steps is to consider all the needs of the network and identify which blockchain tools can be used to fill those needs.

2.2.1 Public vs. Private

Public and private blockchains have already been mentioned in this report, but, to reiterate, public blockchains are open to anyone who can download the node software onto a computing device. Public blockchains are highly decentralized and generally unregulated, the ledger is transparent to all users, user identities are protected with anonymity, and the ledger is highly immutable [47]. Private blockchains are typically less concerned with privacy (despite the name), as the system is closed, and only approved nodes should be able to join the network. The network may tend toward being more centralized, which can expose private blockchains to higher risk from cybersecurity threats. Private blockchains tend not to scale as large as public blockchains, making them less resource intensive, though this measure depends upon the computing power of the network [48].

2.2.2 Permissioned vs. Permissionless

Permissioned and permissionless may coincide with private and public blockchains, respectively, for most applications, but they are not necessarily exclusive. Permissioned blockchains use some form of restriction on access, and this lends permissioned structures to private blockchains very well. Permissionless blockchains do not place restrictions on access in any way to the system. In this way, the two are closely interrelated with public and private networks. However, if necessary, the two could be swapped. A public permissioned blockchain would require permission be granted for a node to access the system, which might be gained with a fee payment [49]. Once on the network, the node would behave as it would in a public blockchain. By contrast, a private permissionless blockchain would require nodes to be given permission to access the system during the network's deployment but nodes would operate with anonymity inside of the network [50]. Both situations are pretty rare though, and most blockchains follow the traditional public, permissionless/private, permissioned structure.

2.2.3 Consortium

A blockchain consortium is a group of organizations that collaborate to administer, maintain, and operate a blockchain network [51]. Consortium blockchains work to promote interorganizational collaboration for the benefit of all involved. Consortium blockchains may contain a single network shared by all involved parties, or, more realistically, a blockchain consortium may integrate multiple blockchains together to achieve data sharing while still maintaining organizational structure. Additionally, the network will maintain data privacy and the network may also be mutable in the case of needing to remove data from the shared ledger. Blockchain consortiums are powerful tools and have a wide range of relevance, especially for large organizations and across multiple agencies or organizations within an industry.

2.2.4 Hybrid and More

Hybrid blockchains combine elements of public and private blockchains to maximize benefits from both [52]. When designing a blockchain, if two needs of the network compete with each other, developing a hybrid system to incorporate the individual needs may be the best solution. This could mean allowing full transparency of the ledger, while also having permissioned access, or some other variation.

Sidechains are another way to implement blockchains, which allows for blockchains to be connected [53]. Sidechains can be extremely useful for transferring information from one blockchain to another without needing to somehow combine the two. A sidechain can be set up temporarily for the express purpose of a single transfer or can be used for a length of time to transfer information repeatedly, though it does add complexity to the system. Multiple sidechains can be opened and connected to a blockchain, and information can be transferred both ways through the sidechain [54]. Because sidechains are their own entities operating alongside the system, they can expose the blockchain to security risks, so care should be taken when implementing them.

2.3 OTHER TYPES OF DLTS

Sections 2.3.1–2.3.3 discuss other DLT types that are not blockchain or that were evolved from blockchain.

2.3.1 Hyperledger Fabric

Hyperledger Fabric is an open-source, private blockchain framework developed by the Linux Foundation [55]. It is an enterprise blockchain solution that helps organizations to interact in a shared environment [56]. On a Hyperledger Fabric system, each organization has its own certificate authority and network of peer nodes. These minor constructions are essentially channels, within which members who belong to that organization can operate. The overarching network employs an ordering service that helps to process transactions. By organizing independent entities into channels, privacy of data can be maintained to protect sensitive or proprietary data but still allow for transfer of information between organizations with a close relationship. The Hyperledger Fabric system is highly modular and customizable, and several organizations have already employed it for their particular needs (see Section 3 for use cases).

2.3.2 Hashgraph

Hashgraphs are closely related to blockchains and employ much the same structure. However, hashgraphs allow transactions with matching timestamps to be recorded [57]. Hashgraphs treat all ledger entries as their own "event" [50]. "All network transactions are provable in this type of distributed ledger implementation. As soon as a transaction occurs on the network, everyone on the network will know where the transaction will be recorded in the ledger within a few minutes" [50]. This process is known as a gossip protocol, where every node is made aware that a transaction has

taken place. Hashgraphs take the gossip protocol a step further to gossip about gossip. Essentially, the hash chain process is added to the message chain and messages become chained together so that they cannot be changed [58]. Additionally, on a hashgraph, data do not need to be stored on blocks indefinitely. Instead, data are stored in a graph as events, making them significantly smaller and easier to manage [59].

2.3.3 DAG

DAGs are a type of data structure system that has been compared to decentralized networks due to the nature of the composition of the vertices and edges [60]. DAGs do not require nodes to all be directly connected to each other; rather, nodes branch out from parent roots to create a graph structure [61]. Transactions are stacked in a DAG, and multiple transactions can be recorded in the same place and at the same time, meaning they can be referenced all at the same time. DAG structures are highly decentralized and are very beneficial to initiating new networks [61].

2.3.4 Holochain

The Holochain platform differs from blockchains and related structures in that it does not require consensus mechanisms [57]. Instead, individual nodes operate with a set of rules that serve as a forking system. Holochains do not rely on global agreement from the system but instead provide agency to the individual. Without global consensus, Holochains provide lower trust in a network and should not be used to store sensitive data [62].

2.4 DETERMINING THE NEED FOR BLOCKCHAIN TECHNOLOGY

This section discusses how to determine blockchain need and how to choose a blockchain system. Making decisions on when and where to use a blockchain approach can be difficult. After reviewing the components, tools, and technologies that comprise blockchain systems, it is important to review the benefits and tradeoffs to blockchains and blockchain tools to inform decisions about how and when to use blockchains. A research study was conducted by a group from Germany that empirically studied the attributes of blockchain systems and their tradeoffs in 2020 [63]. The research conducted is thorough. The researchers assigned 40 DLT characteristics to 6 DLT properties and analyzed how the tradeoffs between characteristics and properties affected the viability of DLT applications. The report by Niclas Kannengießer et al. is worth reviewing to understand how blockchain characteristics can dictate the selection and development of a system.

When trying to determine whether blockchains are the correct solution for a need, the National Institute of Standards and Technology (NIST) and the U.S. Department of Homeland Security (DHS) have developed resources to break down the decision-making process and guide potential adopters to the solution best suited to them. NIST, in a report titled "Blockchain Technology Overview," provides the following list of considerations to make when determining if a blockchain solution is applicable [64].

"Blockchain technology solutions may be suitable if the activities or systems require features such as:

- Many participants
- Distributed participants
- Want or need for lack of trusted third party
- Workflow is transactional in nature (e.g., transfer of digital assets/information between parties)
- A need for a globally scarce digital identifier (i.e., digital art, digital land, digital property)
- A need for a decentralized naming service or ordered registry
- A need for a cryptographically secure system of ownership
- A need to reduce or eliminate manual efforts of reconciliation and dispute resolutions

- A need to enable real-time monitoring of activity between regulators and regulated entities
- A need for full provenance of digital assets and a full transactional history to be shared amongst participants"

According to the same NIST report, the DHS has created a flowchart to help potential adopters determine if blockchain will be useful for their application (Figure 2-2).

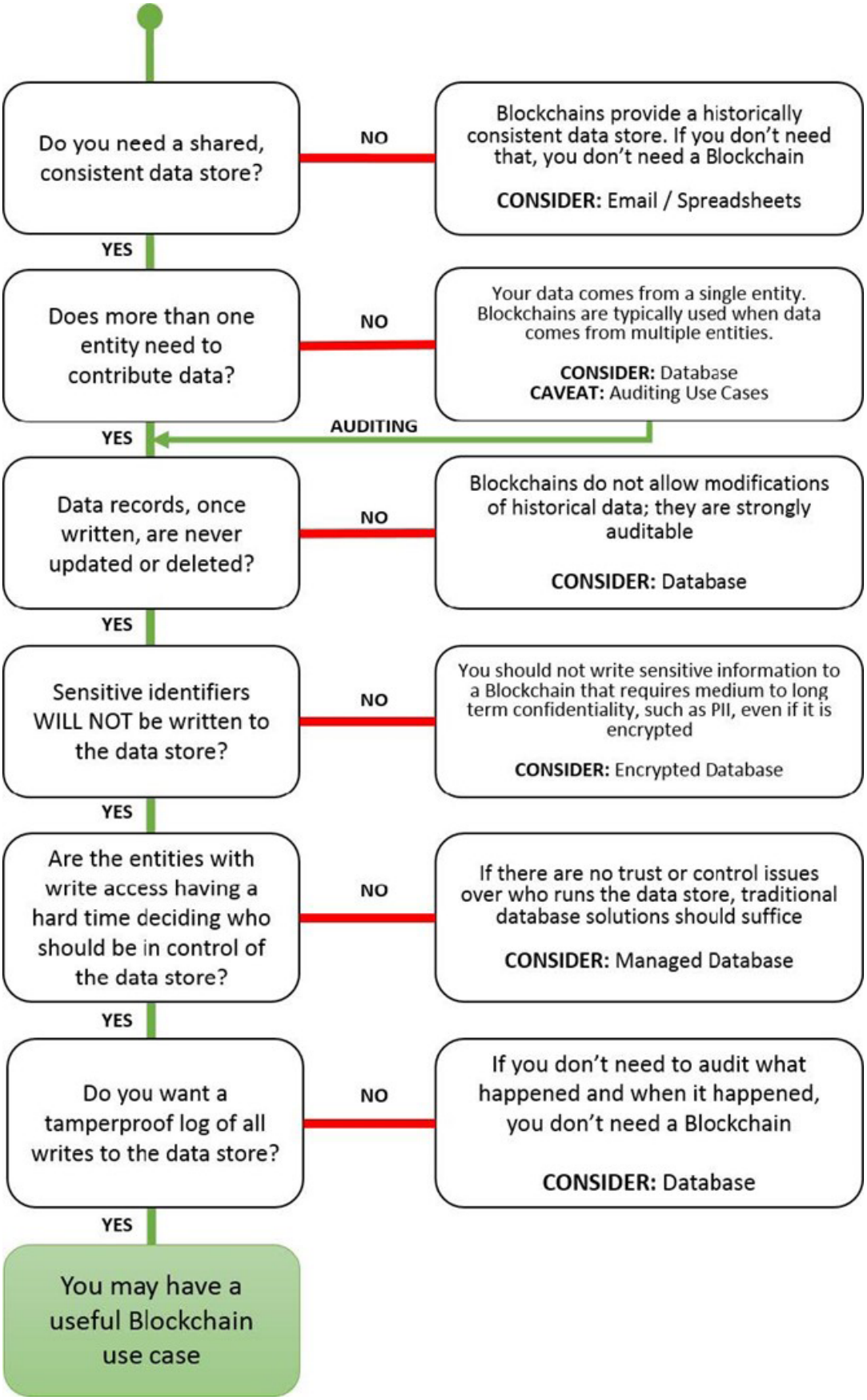

Figure 2-2. DHS Science and Technology Directorate Flowchart *(Source: Yaga et al. [64])*.

This Page Intentionally Left Blank

SECTION 03 IMPLEMENTATION AND USE CASES FOR BLOCKCHAIN

Understanding how blockchains in their current evolution are being used by government agencies and around the world provides information on how the technology can and will need to grow in the future. This section looks at blockchain projects within the U.S. government within recent years, as well as how governing agencies around the globe have been applying the technology to tackle their own needs and issues.

A large portion of these example cases utilize existing and primarily commercial solutions. One of the biggest hinderances to blockchain adoption can be the amount of time and resources needed to stand up a blockchain system. By taking advantage of the platforms already available, these organizations can jump-start their projects. This approach can allow flexibility in that existing platforms can be tailored as necessary to the needs of the application and therefore provide a "bespoke" solution. This approach also eliminates the redundant aspects of standing up a blockchain—the reinvention of code bases that already exist, the architecture for distributed networks, etc.

Several of the blockchain projects used in the examples here are either research focused or proofs of concept for blockchain applications. Due to the relative infancy of this technology, the extent of its applications is still being explored and not every possible use case will result in a "successful" application of the technology. It is important that decision-makers looking into potential blockchain applications understand its capabilities and where and how it is best applied. According to Aileen Scott of TechTarget, several common mistakes made in blockchain implementation include replacing paper-based (or centralized) records too quickly, not adequately investing in the setup and required resources (i.e., implementing datafication where needed, setting up new or additional nodes, etc.), and assuming the technology is already able to be applied exactly as the operator intends [65]. Another issue in blockchain adoption is interoperability and the ability to move data across different platforms.

Continued development and research will ameliorate the limitations and weaknesses of the current blockchain technologies and guide more informed decisions about the technology in the future.

3.1 U.S. AND STATE GOVERNMENT BLOCKCHAIN USE CASES/EXAMPLES

The U.S. government has taken notice of blockchain and the technology's potential, both positive and negative [19, 31]. Several organizations, including NIST and the DHS have put forth guides for establishing blockchain needs, and both organizations have invested in projects developing the technology for government use. Blockchain applications are now being proven across a variety of industries, including the military, healthcare, supply chains, and energy sector, as detailed next.

3.1.1 Military

The DoD has been looking at implementing blockchain solutions for a variety of purposes, including supply chain management and asset tracking. The scale of domestic and global military operations makes keeping track of even a single asset group or the supply chain for a single product a monumental challenge. Blockchain can help alleviate the burden of paperwork and the man hours involved in producing the paperwork by creating a cohesive tracking system that is always up to date and reflects the real-time status of assets and procurement.

3.1.1.1 Authenticity Ledger for Auditable Military Enclaved Data Access (ALAMEDA) Project— U.S. Navy and Defense Logistics Agency (DLA)

In 2020, the U.S. Navy awarded a Small Business Innovation Research (SBIR) program contract to SIMBA Chain Inc., to begin developing blockchain-based supply chain management solutions for the DLA [66]. The project, titled "Authenticity Ledger for Auditable Military Enclaved Data Access (ALAMEDA)," worked with the U.S. Marine Corps and used the M2A1 .50-caliber machine gun [67] "to define a use case for a blockchain-based prototype to monitor the inventory and movement of physical assets at its Albany, GA, depot. This effort resulted in a proof of concept for a single source of truth ledger to support monitoring the inventory and movement of physical assets" [68]. "Single source of truth (SSOT) is a concept that an organization can apply as part of its information architecture to ensure that everyone in the organization uses the same data when making business decisions" [69].

A follow-on Phase II contract was awarded in 2021 to advance the solution [70]. The project aimed to create a "demand sensing" system to anticipate and manage weaponry parts needs and reduce "disruption issues and threats to engineering and maintenance operations" [70]. The goal of the end product was to cut down on long lead times in the supply chain and allow for faster repair timelines on critical weapons systems. The project focused on the F/A-18 Hornet supply chain at the Fleet Readiness Center Southeast in Jacksonville, FL.

SIMBA Chain has also been working with the U.S. Air Force on several blockchain-based solutions. Another series of SBIR awards by the Air Force tasked SIMBA Chain with setting up a risk management system at Tinker Air Force Base. SIMBA's chief executive officer (CEO) Joel Neidig said the system would run Hyperledger Fabric (an open-source DLT "for developing applications or solutions with a modular architecture" provided by Hyperledger Foundation [71]) to track parts in cooperation with Boeing [72]. Earlier this year, the Air Force invested another $30M into SIMBA Chain for general supply chain management blockchain solution developments [73].

In addition to supply chain solutions, the military has also been investing in data management and cybersecurity. Using various tools centered around the security aspects of blockchain technology can help ensure safety in transmitting data or communicating sensitive information. Blockchain solutions can be used to guarantee the authenticity of data or information by preventing unauthorized access to or manipulation of documents and data stored on blockchain networks and provide an auditable record of information. Private blockchains provide added layers of security for sensitive military data and reduce chances of a cybersecurity attack from adversaries.

3.1.1.2 Constellation's Hypergraph Network— U.S. Air Force, U.S. Transportation Command

In 2021, Constellation Network was awarded a Direct to Phase II SBIR award by the Air Force's AFWERX office to develop a data security solution for the Air Force's Transportation Command and a civilian reserve partner [74]. The intention of the project was to develop a way to transfer confidential data securely and more efficiently from government agencies to commercial partners [75]. The resulting system was built on

what Constellation calls the Hypergraph Transfer Protocol, a blockchain replacement for Hypertext Transfer Protocol. Constellation partnered with Kinnami Software to integrate its data software with its DLT solution. The project was a success and is now offered as a service for federal agencies [76]. Constellation states that by "organizing information into encrypted objects owned by end users (both people and systems) and storing them across a network of devices, Kinnami cryptographically guarantees that an object is secured before it is stored or transmitted anywhere else" [76]. Additionally, because of the system's data classification features and auditing metadata, it can be used at different classification levels. Potential expanded uses of this, or similarly constructed blockchain/DLT solutions, include being able to securely provide classified or otherwise sensitive information to foreign adversaries (such as exchange of intelligence information), safely and securely send sensitive information to forward deployments in hostile environments, and share classified or sensitive information to government-contracted commercial partners while ensuring the protection of the data.

3.1.1.3 Defense Advanced Research Projects Agency (DARPA)

In a July 2019, publication from the DoD, the "DoD Digital Modernization Strategy," blockchain is stated as an important technology for development, particularly for secure data storage and transmission [77]. DARPA is cited as "starting to experiment with blockchain to create a more efficient, robust, and secure platform using a blockchain protocol that will allow personnel from anywhere to transmit secure messages or process transactions that can be traced through numerous channels of a decentralized ledger" [77]. Evidence of this development is given by a 2017 DARPA award to ITAMCO, a privacy app developer, to "develop the cybersecurity architecture for a secure messaging application based on the company's existing Crypto-Chat application with added blockchain technology" [78]. Furthermore, the report states that DARPA is attempting to develop an "unhackable code," which could be made possible with blockchain.

DARPA is also working on other blockchain initiatives with diverse focuses, including researching the potential effects of and threats posed by blockchain-based cryptocurrencies. In an SBIR project called "Mapping the Impact of Digital Financial Assets" awarded to Inca Digital's government contracting division, Inca Digital Federal, DARPA is attempting to gain insight into how digital currencies might be used for money laundering and to finance terrorist organizations and activities [79]. Inca Digital will aim to develop a cryptocurrency mapping tool to better understand how cryptocurrency is being used, transferred, and exchanged. This will provide insight into how money is moved both digitally and physically and how and where assets can be exchanged or used in real-world transactions. According to the firm's CEO Adam Zarazinski, part of the system is already in operation and available to government and financial institutions—"two pieces, including an analytics tool that tracks scammers and hackers in 'near real-time' as well as a 'cross-market surveillance tool,' were already developed in partnership with DARPA" [80].

3.1.2 Healthcare

Blockchain technology has a lot of potential applications in healthcare, but there has been resistance in the healthcare sector toward adopting the technology. Part of this resistance stems from the rules and regulations surrounding patient privacy and the sensitivity of medical records and also from the number of resources required to stand up a blockchain solution [81]. More research programs on blockchain for healthcare applications, like these examples, will help to inform future adopters and better aid decision-makers on selecting the best applications for blockchain technologies in healthcare.

3.1.2.1 Centers for Disease Control and Prevention (CDC) and IBM

In 2017, the CDC and IBM announced a partnership to develop a blockchain technology to track public health issues. According to a Forbes news article, "the new system, which IBM and the CDC's National Center for Health Statistics have tested using simulated data, could make it easier for the CDC to survey medical providers about data like the reasons patients visit and the symptoms they display. The CDC already collects much of that data through surveys like the National Ambulatory Medical Care Survey and National Hospital Ambulatory Medical Care Survey, which collect patient visit information from doctors and hospitals around the country" [82]. The platform will not store personal health information but rather track and grant access to users to view the data, taking advantage of encryption keys to manage access [83]. There have been no official announcements on the development of the project since 2018, but the CDC did dip back into blockchain development with IBM in 2020 during the height of the COVID-19 crisis.

The 2020 project brought together multiple partners to work on aggregating data from several organizations, including the World Health Organization, CDC, and John Hopkins University, to study COVID-19-related data [84]. The project took advantage of startup HACERA's MiPasa platform and tasked IBM and Oracle with data aggregation.

3.1.2.2 Food and Drug Administration's (FDA's) Drug Supply Chain Security Act (DSCSA) Pilot Project Program

In 2019, the FDA began a pilot program called the DSCSA Pilot Project Program to develop capabilities for identifying and tracing certain drugs in the prescription supply chain [85]. The project involved a long list of U.S. and global agencies and commercial partners conducting different pilot programs to address different needs. The project as a whole was not designed to analyze blockchain, but, due to the nature of the research goal, several of the pilot programs did employ or evaluate blockchain as a solution. The final report for the program, including lessons learned, is available publicly as of May 2023 [86]. Pharmaceutical supply chain is one commonly cited potential use case for blockchain in healthcare, and this project researched the applicability of the technology as a solution. Using the lessons learned from this program will give future adopters useful knowledge for implementing and adapting new solutions.

3.1.2.3 MedRec

MedRec is a thesis project by student Ariel C. Ekblaw at the Massachusetts Institute of Technology (MIT), which "accomplishes record management without creating any centralized data repositories; a modular system design integrates with providers' existing, local data storage solutions, facilitating interoperable data exchange between data sources and the patients" [87]. The project included running a pilot program with Beth Israel Deaconess Medical Center, a teaching hospital at Harvard. Ekblaw's thesis provides insight into the challenges faced with implementing the pilot and details the specific features of the blockchain technology with regard to security, privacy, interoperability, and scalability [87].

3.1.3 Supply Chain

Supply chains are one of the most cited examples for the impact that blockchain implementation can have. This is in part due to the fact that supply chains already employ extensive tracking and data-management technologies, and having ready-to-use sources for data makes implementing a blockchain more effective. Supply chains also take advantage of one of the inherent features in blockchain—establishing traceability and immutable records. What blockchains have to offer in terms of tracing information and storing data

automatically and immutably is what supply chains need for auditing and managing their operations.

3.1.3.1 National Oceanic and Atmospheric Administration (NOAA)

NOAA's Fisheries department held a workshop in 2021 to address supply chain traceability issues for the global seafood industry [88]. The fishing industry faces many issues, including illegal fishing activities, environmental waste and habitat destruction, and safety and sustainability of supply chain practices. The workshop brought together over 35 different fisheries-based agencies to discuss potential solutions to mitigate the myriad issues within the industry, including how blockchain technologies can be applied. The workshop summary report cites a few instances of blockchain research for fisheries applications, including a program between NOAA and Texas A&M University and a program in the Philippines with each focusing on traceability of tuna [89]. The Seafood Alliance for Legality and Traceability is also referenced with regard to its work on traceability and blockchain use [90]. As more organizations engage with blockchain technologies, workshops like this may develop into consortiums where blockchain data can more readily be shared and more can be gained from the collective participation of the member agencies.

3.1.3.2 DHS

The DHS has shown a significant interest in blockchain, both as a tool and from a regulatory standpoint, and has issued awards for several blockchain-based projects specifically addressing supply chain issues [91]. These projects address a wide range of industries from oil and gas industries to food supply chains, and even tracking of biological threats. All but one of the awards is a Phase I award, meaning that they will all be developing proof-of-concept solutions for potential future application.

The DHS awarded Neoflow, formerly Mavennet, a Phase 4 award "to digitally trace natural gas and crude oil transiting from Canada to the United States" [92]. This project is an extension of a 2019 Phase 1 award, and this phase of the project includes demonstrating the platform for use. The company states that its solution "doesn't just prove the origin of the oil and gas but also the environmental compliance with a record of emissions throughout the supply chain" [92]. Another award was made to Mesur.io to develop a blockchain-based solution for visibility of food supply chains [93]. Mesur.io used its existing Earthstream platform, which monitors agricultural risks such as pathogens and toxins [94], as a foundation for the solution. A second award was made to Mesur.io to adapt its Earthstream platform to focus on outbreaks, such as COVID-19 [95]. A final award was made to Spherity GmbH to develop traceability for "direct-to-consumer e-commerce shipments" [96]. The solution aims to create a digital-twin technology and adds customs data to securely link e-commerce shipments and information. The DHS states that the goal of this project is to help reduce and deter trade in illicit and dangerous goods.

3.1.4 Energy

Blockchains have been employed in many other sectors, with one of them being the energy sector. Elements of the energy sector, such as energy trading, regulation and compliance, and grid management, already share overlap with available blockchain features. As with many other sectors, datafication is needed across the energy system to fully realize the potential for blockchain applications. Additionally, security requirements, investment cost, and manageability at scale are all potential barriers to adoption for organizations in the energy sector [97]. The Department of Energy (DOE) has begun conducting research into potential blockchain solutions for the energy sector.

3.1.4.1 Keyless Infrastructure Security System (KISS)—DOE

KISS [98] was a project led by the Pacific Northwest National Laboratory (PNNL) in partnership with Guardtime, a company specializing in the research and development of blockchain protocols and application [99]. The project had three objectives, the first of which was to develop blockchain-based cybersecurity the PNNL platform could use to execute energy exchanges. The other two objectives were to build a solution that would autonomously monitor and verify the integrity of critical systems and identify opportunities to use blockchain for preventing cybersecurity threats to the energy sector. Testing and demonstration of the developed technology was performed after the project [100].

3.1.4.2 Grid Guard—DOE

The Grid Research Integration and Deployment Center at Oak Ridge National Laboratory (ORNL) demonstrated how blockchain technology can help secure the power grid in a project titled Grid Guard [101]. The product developed was built on the Hyperledger Fabric, an open-source blockchain framework, and employs a variety of additional features for security, operation, and maintenance of the system. The goal of the research and development was to produce a tool that could help identify anomalies or faults in the energy grid, whether cybersecurity related or due to natural events. The resulting report for the project goes into thorough details on the development and testing of the system [102]. Overall, the demonstrations of the system were largely successful and ORNL is continuing to conduct research on the applications and usefulness of the technology.

3.2 FOREIGN GOVERNMENT BLOCKCHAIN USE CASES

Governments around the globe have also been developing blockchain applications and solutions to address important issues and needs. Some countries have been significantly more involved in developing blockchain applications, and some of those developments might even be considered high risk and/or highly experimental, such as China's development of a centralized digital currency. Other projects can provide great insight into additional applications for blockchain technology, such as Singapore's development of COVID-19 health credentials.

3.2.1 China

China is working diligently to develop blockchain technologies for a variety of applications. Last year, China selected 164 different entities to participate in a wide variety of pilot programs that range from "manufacturing, energy, [and] government and tax services, [to] law, education, health, trade and finance, and cross border finance" [103].

One of China's focuses with blockchain-based technology is on creating a central bank digital currency (CBDC) [104]. CBDCs are "a form of digital currency issued by a country's central bank. They are similar to cryptocurrencies, except that their value is fixed by the central bank and equivalent to the country's fiat currency" [105]. Because these types of currencies are issued and controlled by a central entity, they are not true blockchain technologies but do operate using principles of blockchain technologies. There are significant potential benefits to developing digital currencies, including reduced costs and increased speed of transactions, but there are also concerns surrounding CBDCs [106]. These concerns include barriers to adoption for certain users, decreased market value, and an inability to match predicted benefits [106]. CNN has in fact reported that China is struggling to launch its digital yen and has given away millions of dollars in incentives to generate adoption of the currency [107].

Another project to boost CBDC development that has been announced in China is attempting to implement CBDCs in cross-border payments [108].

The platform will be called the Universal Digital Payments Network and is in development with Red Date Technology, a Hong Kong based company. The project will develop a proof of concept and demonstrate it with the assistance of several global participants.

Red Date Technology is the designer of the government's Blockchain-based Service Network (BSN). "BSN bills itself as a 'one-stop shop' to deploy...blockchain applications in the cloud," and is intended to solve problems of interoperability among different blockchain platforms [109]. The company's CEO cited low demand for this solution but predicted a delay of roughly 10 years to more widespread adoption across industries. The benefit to developing this technology is that, as new blockchain systems are developed and deployed, they will already be prepared to tackle any challenges to interoperability.

3.2.2 Europe and European Union

Guardtime, the company that worked with the DOE on their KISS project, has been involved in a significant number of DLT and blockchain projects for different European governments and agencies. Two dozen research projects are featured on its website, and the company claims over 50 patents on solutions resulting from their research [110]. Rather than summarize each project individually, a selected list of representative projects is given in Table 3-1, with a short synopsis for each.

3.2.3 Canada

The Canadian government has recognized that blockchain technology may become a useful tool for economic growth and has invested in developing different capabilities with the technology [111].

3.2.3.1 National Digital Trust Service (NDTS)

Last year, the Canadian government launched a collaboration with ATB Ventures, the research and innovation arm of Alberta-based financial institution ATB Financial, called NDTS [112]. NDTS is a proof of concept for the development of digital credentials that are easier to issue and verify. "ATB Venture's blockchain-identity management solution, Oliu and digital credential wallet Proof, allow businesses and regulators to develop use cases and issue, use, and verify digital credentials in a sandbox environment." The program has over 20 participating organizations and is still in development.

3.2.3.2 Talent Cloud

An older project by the Canadian government experimented with using blockchains to provide a digital CV for certification of skills, experience, and credentials of civil employees [113]. The experiment, called Talent Cloud, had an overarching goal of exploring "digital age concepts for modernizing the government's approach to talent and recruitment" [114]. The digital CV solution was intended to create a permanent and employee-owned record of job experience based on the projects in which an employee was involved. The overarching project was successful in recruiting new talent, and the government does intend to use the knowledge gained from the effort to develop a talent platform in the future.

3.2.4 Singapore

Singapore also looked to blockchain technologies as a potential aid in the fight against COVID-19. In 2020, the Singapore government teamed up with a commercial partner to develop the Digital Health Passport, a solution for tracking the vaccination status of people moving across the country's borders [115]. The resulting system allowed for medical documents, including COVID-19 test results and treatment documentation, to be stored in a digital wallet. This made verifying a citizen's medical status fast and seamless and also eliminated the risk of lost, damaged, or even falsified records. The program created by Accredify

Table 3-1. Research Projects Performed by Guardtime in the European Union

Project (Agency)	Synopsis
CHESS (Estonia and Czech Republic)	Cyber-Security Excellence Hub in Estonia and South Moravia (CHESS) "will conduct a thorough analysis of needs and capabilities of the two regions and develop a joint cross-border [research and innovation] R&I strategy for cybersecurity."
STCM (European Space Agency [ESA])	Space traffic coordination monitoring (STCM) aims to address global needs for coordination among actors in space and make "the space traffic data available to the market in a secure and trusted way." The project involves collaboration with GMV and Advice GEO to build a complete solution.
DGS/DLT for Space Situational Awareness (ESA)	"The Decentralised Ground Segment (DGS) Authentication Using Blockchain Technology project focused on the entire operations ground segment for a space mission." Guardtime's role was to identify how blockchain could provide greater security and operational efficiency for space industry partners.
BC4Space (ESA)	The BC4Space project used the previously developed KSI blockchain technology to develop an application for verifying "the integrity and provenance of Earth Observation (EO) data," to ensure integrity of data for processing with other applications.
EOGuard (ESA)	The EOGuard (EO) project "focused on providing security for ESA EO data archives in order to facilitate the availability and usability of these datasets and reduce the costs of archiving EO products."
R2D2 (European Union [EU])	Reliability, resilience, and defence technologies for the grid (R2D2) is a project aimed at improving Europe's energy system. The goal of the effort is to "facilitate the creation of the EU's reliable, resilient, secure, and cyber-aware energy system" and will be demonstrated across four countries.
i3-MARKET (EU)	The i3-MARKET project aims to address the need for a centralized European data market economy and create "interoperable and secure marketplaces with decentralised economy-driven and scalable data repositories."
Gravitate-Health (EU)	Gravitate-Health is intended to be a healthcare information solution that ensures trusted sources for medical information. The platform, intended for both patients and providers, will provide trusted information on digital medical services to inform users and reduce risk.

runs on the Singapore government's HealthCert platform, and the system was rolled out in a matter of months to allow safe return to travel. The HealthCert program continues to be used by the government, and in conjunction with other commercial partners, to issue certifications for medical records [116].

3.2.5 Australia

Australia, much like NOAA, held a forum in 2020 to address supply chain issues faced by the country [117]. Australia faces "$1.7 billion worth of food fraud annually" [117], and experts were gathered to discuss the potential for blockchain technology to be employed in counteracting this problem.

Rob Allen, the event's moderator, "set the scene by stating that verifying the authenticity of produce claiming to be Australian-made in local and overseas markets is one of the largest challenges facing the country's agricultural industry" [117]. The forum discussed uses for blockchain systems and examples of their use in other supply chain applications. Ultimately, the panel's takeaway was that a lack of "technological literacy" presented the largest barrier to blockchain adoption and advocated for educational initiatives.

3.2.6 Africa

A project in Ghana is using blockchain to "help Ghanaians attain property rights and secure more financially stable futures" [118]. The project, run by startup Bitland, aims to provide land registry and title services to local residents in order to boost autonomy. Bitland's CEO, Naringamba Mwinssubo, says the project operates in three parts: (1) land survey, (2) preparation of titles and land registry, and (3) land tokenization. The service helps secure property rights for poor residents who would not have access to such services otherwise. Forbes states that the benefits from projects like this "often fail to resonate due to the markets targeted and the way in which they are communicated" [119]. However, these projects do provide needed services for those who cannot access them and promote transparency and fairness for governments and their citizens.

This Page Intentionally Left Blank

SECTION 04 CONTINUING RESEARCH

Blockchains are hampered by certain limitations and are susceptible to certain vulnerabilities; therefore, more research and development are needed, not only to develop the applications of the technology, but also to ensure blockchains are properly maintained and security vulnerabilities are addressed. The limitations of the technology include resource use and a lack of available data, as well as poor public understanding and awareness of blockchain technologies and their capabilities that lead to low adoption. Addressing these limitations will boost adoption of the technology, which is crucial to its growth.

Research into the security vulnerabilities of blockchains is also of paramount importance, as the technology is relatively new, and public "hype" has deemed the technology foolproof. This is a dangerous misconception that, if not addressed and debunked, could lead to significant security issues in the future. Researchers are already making headway on analyzing blockchain weaknesses and vulnerabilities, and continued support for government, academic, and public research will provide pathways to creating the tools and solutions needed to address blockchain limitations and vulnerabilities and push the technology in new directions.

4.1 PHYSICAL LIMITATIONS

Physical limitations on blockchains include issues that are bounded by the resources available for computing. These issues can include computing power, data storage, the amount of data, or the availability of or access to necessary data. Ideally, blockchains can make dealing with a large amount of data more efficient and effective. However, without the proper resources, blockchains either become unmanageable or simply unnecessary.

4.1.1 Resource Use

Blockchain technology, depending on how it is set up, can be heavily resource intensive. This is especially true of early blockchain designs, as seen with Bitcoin. Because Bitcoin requires nodes to complete complex cryptographic equations, more computing power allows nodes to complete the puzzles faster. Realizing this, many Bitcoin miners started chaining together graphical processing units to boost the computing power of the node being run. Not only did this lead to massive shortages in computer parts [120], but it also generated an estimated energy consumption "of 127 terawatt-hours (TWh). That usage exceeds the entire annual electricity consumption of Norway" [121]. Excessive resource use and global climate impact became an important discussion in the wake of the rise of Bitcoin and spin-off cryptocurrencies.

Resource use is still a concern to some degree, as cryptocurrencies are still popular, but newer blockchain technologies have reduced their resource use footprint considerably. Ethereum, in contrast to Bitcoin, uses just 2,601 MWh (0.0026 TWh) of energy annually [122]. Many new blockchain technologies

do not require large amounts of computing power, particularly if they are not cryptocurrency focused, such as private blockchains. However, blockchains, including private blockchains, do face other resource issues, including a still relatively high computing-power requirement, physical hardware to run networks, and data-storage availability. These issues tie into the scalability issue of blockchains, and any organization employing blockchain will need to reconcile the hardware, space, and data-storage requirements for large scale blockchain applications [64]. Developers of blockchains need to consider how data will be managed and stored on networks and how those data will be facilitated over time.

4.1.2 Datafication

Another limitation of blockchain is its dependency upon data. Blockchain is a data-management structure, and without data to manage, it does not serve its intended purpose. With further data-driven technologies becoming available, more industries are adapting to capture and record additional data. For example, supply chains rely heavily on data tracking in the management of supply chains and blockchain technologies have already seen some adoption in supply chains (see Section 3). In other sectors that do not rely as heavily on data analysis, blockchain adoption will be hampered by a lack of useful applications.

To drive blockchain adoption into new sectors, more data will need to be generated. This process—the development of data generation and analysis—is called datafication [16]. Upscaling data generation and analysis adds another level of investment to the adoption process for blockchains and comes with added issues. One issue with datafication is individual's resistance toward personal data being recorded, stored, and used by others. Privacy concerns are well founded in today's technology landscape, when, in 2022, 1,802 data breaches affected 422 million people in the United States, according to Statista [123]. Keeping private data in a permanent record could cause more susceptibility to attack, if not handled properly. Improved security for blockchains, as well as public perception campaigns and education may be required to drive further blockchain adoption in some sectors.

4.2 CYBERSECURITY ISSUES

One of the biggest misunderstandings of blockchains is their vulnerability to attacks. Blockchains have been billed as "unhackable" due to the nature of their construction, and, while immutability is a core feature of blockchain construction, this does not mean they are not susceptible to different kinds of attacks. A study conducted by a group of researchers in Germany titled "Attacking the Trust Machine: Developing an Information Systems Research Agenda for Blockchain Cybersecurity," surveyed literature for examples of attacks made on blockchains [124]. The researchers identified a total of 87 recorded blockchain attacks that had been reported. They categorized the attacks by the vectors of attack. These vectors included P2P networks, consensus mechanisms, virtual machine/programming language, application logic, and client application wallet. These vectors had 15, 27, 11, 28, and 10 attacks, respectively. Attacks on the P2P network included distributed denial of service attacks and domain name system attacks. These attacks take advantage of the network itself. Attacks on the consensus mechanism take advantage of limitations with the protocols, such as the 51% attack and related Goldfinger attack. The 51% attack, which involves a malicious actor or group of actors to gain control over 50% of the nodes or hashing power of the blockchain, has been leveled at several major cryptocurrencies, including Bitcoin SV and Ethereum Classic [125]. The paper divides application logic into both on-chain and off-chain attacks. On-chain attacks include attacks on applications deployed on the blockchain. The Hard Fork attack on the smart contract run by the investing group The DOA on the Ethereum blockchain is an example of an on-chain attack. Other on-chain attacks accounted for 17 of

the application logic category's 28 combined recorded attacks. Attacks at the client application/wallet level consist of classic social engineering and phishing attacks. These attacks might also include malicious "man-in-the-middle" attacks that intercept data in transit across public wireless networks [124]. Schlatt et al. go on to provide a series of recommendations for how to research these vulnerabilities, listing a total of six research propositions.

An MIT article from 2019 states that "hackers have stolen nearly $2 billion worth of cryptocurrency since the beginning of 2017" [17], and these attacks also pose a threat to information privacy and data security for blockchains. It is therefore imperative that security of blockchains remains a priority for researchers and developers.

4.3 FUTURE BLOCKCHAIN DEVELOPMENT

Research to develop solutions to the issues presented here, as well as develop new blockchain applications, is happening across universities, technology consortia, the technology industry, and government organizations. Several universities have established centers for blockchain research, including Stanford [126], Carnegie Mellon [127], MIT [128], and Arizona State University [129], to name a few. Additionally, consortia such as the Blockchain Research Institute [130] have been formed to promote and facilitate research on the technology. Meanwhile, DARPA, the DHS, and NIST have also been conducting research efforts on blockchain technologies to understand their applicability to government. These collective concerted efforts are pushing blockchain into its 3.0 stage, as defined in Section 2. Where the technology development will go is still not entirely clear, but some of the common areas of research include: enterprise solutions, privacy, enhanced security, improved blockchain design, integrating blockchain with other technologies, and building industry solutions.

The major motivators in blockchain research consist primarily of private commercial software developers, colleges and universities, and blockchain consortia. Private companies and research groups include software and finance giants like IBM and Deloitte, as well as blockchain service providers such as OpenLedger, Hyperledger Foundation, and Ethereum. Blockchain platform developers and private organizations are developing blockchain through their own research, as well as providing research services to outside organizations [131, 132]. Bespoke research services allow blockchain developers to identify and grow new applications for blockchain technologies and implement the solutions into real-world environments, where they can be further developed and refined.

Universities are boosting blockchain research through dedicated programs, as well as putting on symposia and conferences. The University of Texas at Austin put on a symposium in April 2023 with Byte Trade Lab, a blockchain research group [133]. Carnegie Mellon University hosted its Secure Blockchain Summit less than a month later in May 2023, bringing together "experts from academia and industry to discuss the future of blockchain research, technology, and applications, focusing on a variety of topics, including crypto-economics, applied cryptography, programming languages, security and privacy, policy and usability, ethics, and equity" [134]. Stanford hosted a three-day conference in August 2023, covering the latest technological innovations in blockchain [135]. These academic technology symposia provide a resource for foundational research on blockchain technology and develop a talent base for future developers and researchers to continue advancing the technology.

Government research has included research by DARPA on potential vulnerabilities in blockchains. In a report titled "Are Blockchains Decentralized? Unintended Centralities in Distributed Ledgers," the contracted research group, Trail of Bits, goes into depth on how unintentional centralization on

blockchain networks can create weak or vulnerable areas susceptible to attack via different methods [136]. NIST has also researched blockchain's ability to address traceability in supply chains [137]. This research addressed how blockchains could provide capabilities to store and share data across supply chain systems.

Blockchain research has taken a dip in recent years, especially with the advent of artificial intelligence technologies, but many organizations and individuals are still exploring the benefits and capabilities of this technology. Continuing to grow blockchain development will require more investment in studying the vulnerabilities, limitations, and potential applications of the technology, as well as increasing education for adopters and the public about the capabilities and potential benefits and risks of using blockchains [6].

SECTION 05 CONCLUSION

Blockchain technology possesses the potential to improve many aspects of information management and potentially revolutionize the foundations of computing. In order to realize this potential, however, careful consideration of the technology's capabilities and significant investment into the necessary resources for its growth are needed. As it stands today, blockchain technology provides a viable and useful means for storing, organizing, protecting, and auditing large quantities of data in a manner that is significantly safer and more effective than traditional means. In the future, with the proper growth of datafication and continued improvements of the capabilities of the technology, blockchains could be used as the basis for entire internet ecosystems and provide a new, more secure internet of things. Even if this potential is not realized, the technology has significant potential as a highly useful tool in several industries and government sectors.

For decision-makers looking to determine how blockchain can be applied within their organization, it is important to know where to start. NIST, the DHS, and other organizations have produced a variety of useful guides to help determine how and when blockchain can be utilized successfully, and numerous blockchain systems already exist. Blockchain, in its simplest form, is an easy technology to replicate, but to be effective, it must include all of the additional security features and applications that have made commercial solutions viable. Rather than attempt to stand up entire new blockchain solutions, organizations implementing the technology should look to existing solutions that offer customization to fit their needs and invest in resources and practices that will maximize the datafication of the organization or system utilizing blockchain technology. More research and development on blockchain technology applications, and especially on the integrity of different blockchain solutions, are also needed to further prove how the technology can best be used and implemented in the future.

This Page Intentionally Left Blank

REFERENCES

1. Wikimedia Foundation, Inc. "Cryptocurrency." *Wikipedia, the Free Encyclopedia*, https://en.wikipedia.org/wiki/Cryptocurrency, accessed 11 August 2023.
2. Pinkerton, J. "The History of Bitcoin, the First Cryptocurrency." *U.S. News*, https://money.usnews.com/investing/articles/the-history-of-bitcoin, accessed 26 June 2023.
3. Cointelegraph. "History of ETH: The Rise of the Ethereum Blockchain." *Cointelegraph: The Future of Money*, https://cointelegraph.com/learn/history-of-ethereum-blockchain, accessed 11 August 2023.
4. Europol. "Cryptocurrencies: Tracing the Evolution of Criminal Finances." *Europol Spotlight*, Publications Office of the European Union, Luxembourg, December 2021.
5. Drescher, D. *Blockchain Basics: A Non-Technical Introduction in 25 Steps*. DOI: 10.1007/978-1-4842-2604-9, New York, NY: Apress, 16 March 2017.
6. Persons, T. M. "Blockchain and Distributed Ledger Technologies." *GAO*, https://www.gao.gov/products/gao-19-704sp, accessed 12 July 2023.
7. Medium. "Before Blockchain, There Was Distributed Ledger Technology." https://medium.com/blockstreethq/before-blockchain-there-was-distributed-ledger-technology-319d0295f011, accessed 13 July 2023.
8. National Institute of Standards and Technology. "Blockchain." *NIST*, https://www.nist.gov/blockchain, accessed 25 May 2023.
9. Frankenfield, J. "What Is a Hash? Hash Functions and Cryptocurrency Mining." *Investopedia*, https://www.investopedia.com/terms/h/hash.asp, accessed 4 June 2023.
10. Cisco. "Trusted Computing. Trustworthy Computing. Zero-Trust Computing." https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/what-is-trust.pdf, accessed 20 June 2023.
11. IBM. "What Are Smart Contracts on Blockchain?" *IBM*, https://www.ibm.com/topics/smart-contracts#:~:text=Next%20Steps-,Smart%20contracts%20defined,intermediary's%20involvement%20or%20time%20loss, accessed 8 August 2023.
12. Wikimedia Foundation, Inc. "Byzantine Fault." *Wikipedia, the Free Encyclopedia*, https://en.wikipedia.org/wiki/Byzantine_fault, accessed 24 June 2023.
13. Cointelegraph. "How Does Blockchain Solve the Byzantine Generals Problem?" *Cointelegraph: The Future of Money*, https://cointelegraph.com/learn/how-does-blockchain-solve-the-byzantine-generals-problem, accessed 6 July 2023.
14. Tilleli, F. "How Manual Data Entry and Human Error Are Costing You Money." *ConnectPointz*, https://www.connectpointz.com/blog/manual-data-entry-costing-you-money#:~:text=Fatigue%2C%20stress%2C%20distractions%2C%20boredom,rates%20usually%20hover%20around%201%25, accessed 7 July 2023.
15. Wikimedia Foundation, Inc. "Bitcoin Scalability Problem." *Wikipedia, the Free Encyclopedia*, https://en.wikipedia.org/wiki/Bitcoin_scalability_problem, accessed 4 June 2023.
16. Wikimedia Foundation, Inc. "Datafication." *Wikipedia, the Free Encyclopedia*, https://en.wikipedia.org/wiki/Datafication, accessed 22 June 2023.
17. Orcutt, M. "Once Hailed as Unhackable, Blockchains Are Now Getting Hacked." *MIT Technology Review*, https://www.technologyreview.com/2019/02/19/239592/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/, accessed 7 July 2023.
18. Stoltzfus, J. "Can the Blockchain Be Hacked?" *Techopedia*, https://www.techopedia.com/can-the-blockchain-be-hacked/2/33623#:~:text=The%20short%20answer%2C%20from%20a,Blockchain%20assets%20can%20be%20stolen, accessed 7 July 2023.
19. U.S. Government Accountability Office. "Blockchain: Emerging Technology Offers Benefits for Some Applications but Faces Challenges." GAO-22-104625, https://www.gao.gov/assets/gao-22-104625.pdf, accessed 28 June 2023.
20. Simerly, M. T., and D. J. Keenaghan. "Blockchain for Military Logistics." *U.S. Army*, https://www.army.mil/article/227943/blockchain_for_military_logistics, accessed 7 June 2023.
21. PixelPlex. "Blockchain in Government: Use Cases, Challenges, and Real-Life Projects." *PixelPlex*, https://pixelplex.io/blog/blockchain-in-government-processes/, accessed 1 August 2023.
22. OriginStamp AG. "Blockchain 1.0 vs. 2.0 vs. 3.0—What's the Difference?" *OriginStamp*, https://originstamp.com/blog/blockchain-1-vs-2-vs-3-whats-the-difference/, accessed 12 July 2023.
23. Gemini Trust Company, LLC. "What Was the DAO?" *Cryptopedia: Your Trusted Source for All Things Crypto*, https://www.gemini.com/cryptopedia/the-dao-hack-makerdao, accessed 24 July 2023.
24. Siegel, D. "Understanding the DAO Attack." *CoinDesk*, https://www.coindesk.com/learn/understanding-the-dao-attack/, accessed 24 July 2023.

REFERENCES, *continued*

25. Nueshul, J. D. Personal communication. Neushal Solutions, Carlsbad, CA, 5 August 2023.
26. Web3 Labs Ltd. "Blockchain Explained: What Are Blockchain Nodes?" *Web3 Labs*, https://www.web3labs.com/blockchain-explained-what-are-blockchain-nodes, accessed 8 August 2023.
27. Geroni, D. "Blockchain Nodes: An In-Depth Guide." *101 Blockchains*, https://101blockchains.com/blockchain-nodes/, accessed 30 June 2023.
28. Ethereum. "Nodes and Clients." *Ethereum.org*, https://ethereum.org/en/developers/docs/nodes-and-clients/, accessed 7 August 2023.
29. Evans, J. "Blockchain Nodes: An In-Depth Guide." *Nodes.com*, https://nodes.com/, accessed 30 June 2023.
30. Acharya, D. P. "An In-Depth Guide on the Types of Blockchain Nodes." *Geekflare*, https://geekflare.com/blockchain-nodes-guide/, accessed 7 August 2023.
31. The White House. "Fact Sheet: Climate and Energy Implications of Crypto-Assets in the United States." *The White House*, https://www.whitehouse.gov/ostp/news-updates/2022/09/08/fact-sheet-climate-and-energy-implications-of-crypto-assets-in-the-united-states/, accessed 24 June 2023.
32. Becher, B. "What Are Blockchain Nodes and How Do They Work?" *Builtin*, https://builtin.com/blockchain/blockchain-node, accessed 1 July 2023.
33. Techskill Brew. "What Is a Block in a Blockchain? (Part 2—Blockchain Series)." *TBS: Techskill Brew*, https://techskillbrew.com/what-is-a-block-in-the-blockchain-part-2-blockchain-series/, accessed 3 August 2023.
34. Soares, X. "How Blocks Are Added to a Blockchain, Explained Simply." *CoinDesk*, https://www.coindesk.com/learn/how-blocks-are-added-to-a-blockchain-explained-simply/, accessed 4 August 2023.
35. Dutta, B. "3 Types of Block in a Blockchain Network." *Analytic Steps*, https://www.analyticssteps.com/blogs/3-types-block-blockchain-network, accessed 17 July 2023.
36. Wikimedia Foundation, Inc. "Blockchain." *Wikipedia, the Free Encyclopedia*, https://en.wikipedia.org/wiki/Blockchain, accessed 27 May 2023.
37. Crypto.com. "A Deep Dive Into Blockchain Scalability." *Crypto.com*, https://crypto.com/university/blockchain-scalability, accessed 14 July 2023.
38. Clavin, J. S. Duan, H. Zhang, V. P. Janeja, K. P. Joshi, Y. Yesha, L. C. Erickson, and J. D. Li. "Blockchains for Government: Use Cases and Challenges." *Digital Government: Research and Practice*, vol. 1, issue 3, article no. 22, pp. 1–21, https://doi.org/10.1145/3427097, accessed 11 July 2023.
39. PixelPlex. "What Is the Difference Between Blockchain Consensus Algorithms?" *PixelPlex*, https://pixelplex.io/blog/best-blockchain-consensus-algorithms/, accessed 14 July 2023.
40. Frankenfield, J. "What Are Consensus Mechanisms in Blockchain and Cryptocurrency?" *Investopedia*, https://www.investopedia.com/terms/c/consensus-mechanism-cryptocurrency.asp, accessed 15 July 2023.
41. Zola, A. "Hashing." *Tech Target*, https://www.techtarget.com/searchdatamanagement/definition/hashing, accessed 8 August 2023.
42. Okta. "One-Way Hash Function: Dynamic Algorithms." *Okta*, https://www.okta.com/identity-101/one-way-hash-function-dynamic-algorithms/, accessed 8 August 2023.
43. U.S. Government Accountability Office. "Securing Data for a Post-Quantum World." *GAO*, https://www.gao.gov/assets/gao-23-106559.pdf, accessed 9 August 2023.
44. IBM. "Digital Signatures." *IBM*, https://www.ibm.com/docs/en/ztpf/1.1.0.15?topic=concepts-digital-signatures, accessed 9 August 2023.
45. Coinbase. "What Is a Smart Contract?" *Coinbase*, https://www.coinbase.com/learn/crypto-basics/what-is-a-smart-contract, accessed 5 July 2023.
46. Levi, S. D., and A. B. Lipton. "An Introduction to Smart Contracts and Their Potential and Inherent Limitations." *Harvard Law School Forum on Corporate Governance*, https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/, accessed 5 July 2023.
47. GeeksforGeeks. "Difference Between Public and Private Blockchain." *GeeksforGeeks*, https://www.geeksforgeeks.org/difference-between-public-and-private-blockchain/, accessed 8 July 2023.
48. GeeksforGeeks. "Private Blockchain." *GeeksforGeeks*, https://www.geeksforgeeks.org/private-blockchain/?ref=lbp, accessed 8 July 2023.
49. R3. "How 'Pubic-Permissioned' Blockchains Are Not an Oxymoron." *R3*, https://r3.com/blog/how-public-permissioned-blockchains-are-not-an-oxymoron-2/, accessed 9 July 2023.
50. Dutta, B. "5 Types of Distributed Ledger Technology (DLT)." *Analytic Steps*, https://www.analyticssteps.com/blogs/5-types-distributed-ledger-technologies-dlt, accessed 5 July 2023.

REFERENCES, *continued*

51. OriginStamp AG. "What Is a Consortium Blockchain?" *Originstamp*, https://originstamp.com/blog/what-is-a-consortium-blockchain/, accessed 9 July 2023.
52. Kamil, S. "Hybrid Blockchain Explained." *Coinmetro*, https://coinmetro.com/learning-lab/hybrid-blockchain-explained, accessed 9 July 2023.
53. Roth, S. "An Introduction to Sidechains." *CoinDesk*, https://www.coindesk.com/learn/an-introduction-to-sidechains/, 10 July 2023.
54. Crypto.com. "What Are Sidechains? Scaling Blockchain on the Side." *Crypto.com*, https://crypto.com/university/what-are-sidechains-scaling-blockchain, accessed 30 June 2023.
55. Oak-Tree Technologies. "Hyperledger Fabric: How it Works, Made Easy." *Oak-Tree*, https://www.oak-tree.tech/blog/hyperledger-overview, accessed 2 July 2023.
56. GeeksforGeeks. "Hyperledger Fabric in Blockchain." *GeeksforGeeks*, https://www.geeksforgeeks.org/hyperledger-fabric-in-blockchain/, accessed 6 July 2023.
57. Geroni, D. "Distributed Ledger Technology: Simply Explained." *101 Blockchains*, https://101blockchains.com/distributed-ledger-technology/, accessed 22 June 2023.
58. Stein, S. "Hashgraph Wants to Give You the Benefits of Blockchain Without the Limitations." *TechCrunch*, https://techcrunch.com/2018/03/13/hashgraph-wants-to-give-you-the-benefits-of-blockchain-without-the-limitations/, accessed 9 July 2023.
59. Haritonova, A. "Blochchain vs. Hedera Hashgraph: Which DLT Is Better?" *PixelPlex*, https://pixelplex.io/blog/blockchain-vs-hedera-hashgraph/, accessed 11 July 2023.
60. Wikimedia Foundation, Inc. "Directed Acrylic Graph." *Wikipedia, the Free Encyclopedia*, https://en.wikipedia.org/wiki/Directed_acyclic_graph, accessed 28 June 2023.
61. Deer, M. "What Is a Directed Acrylic Graph in Cryptocurrency? How Does DAG Work?" *Cointelegraph*, https://cointelegraph.com/explained/what-is-a-directed-acyclic-graph-in-cryptocurrency-how-does-dag-work, accessed 11 July 2023.
62. 101 Blockchains. "Holochain Ultimate Guide: Better Technology Than Blockchain?" *101 Blockchains*, https://101blockchains.com/holochain-blockchain-guide/, accessed 11 July 2023.
63. Kannengießer, N., S. Lins, T. Dehling, and A. Sunyaev. "Trade-Offs Between Distributed Ledger Technology Characteristics." *ACM Computing Surveys*, vol. 53, no. 2, article 42, https://dl.acm.org/doi/fullHtml/10.1145/3379463, May 2020.
64. Yaga, D., P. Mell, N. Roby, and K. Scarfone. "Blockchain Technology Overview." NISTRIR 8202, National Institute of Standards and Technology, Gaithersburg, MD, https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf, accessed 27 June 2023.
65. Scott, A. "5 Common Mistakes Blockchain Professionals Should Avoid." *TechTarget*, https://www.datasciencecentral.com/5-common-mistakes-blockchain-professionals-should-avoid/#:~:text=Not%20Using%20Blockchain%20Protocols,are%20rarely%20used%20in%20projects, accessed 17 June 2023.
66. SBIR.gov. "Master Command and Control for Multiple Activity Visibility: 2020." *SBIR • STTR*, https://www.sbir.gov/sbirsearch/detail/1925051, accessed 20 June 2023.
67. SIMBA Chain Inc. "SIMBA Chain Receives a $1.5 Million SBIR Phase II Contract From the U.S. Office of Naval Research." *Global Newswire*, https://www.globenewswire.com/news-release/2021/01/13/2157839/0/en/SIMBA-Chain-Receives-a-1-5-Million-SBIR-Phase-II-Contract-From-the-U-S-Office-of-Naval-Research.html, accessed 20 June 2023.
68. Akhtar, T. "US Navy Commissions $1.5M Blockchain System for Tracking Critical Weaponry." *CoinDesk*, https://www.coindesk.com/tech/2021/01/13/us-navy-commissions-15m-blockchain-system-for-tracking-critical-weaponry/, accessed 24 June 2023.
69. TechTarget. "Single Source of Truth (SSOT)." *TechTarget*, https://www.techtarget.com/whatis/definition/single-source-of-truth-SSOT, accessed 12 July 2023.
70. SBIR.gov. "Master Command and Control for Multiple Activity Visibility: 2021." *SBIR • STTR*, https://www.sbir.gov/node/2178827, accessed 20 June 2023.
71. Hyperledger Foundation. "Type: Distributed Ledger Software." *Hyperledger Foundation*, https://www.hyperledger.org/use/fabric, accessed 21 June 2023.
72. Nelson, D. "U.S. Air Force Gives Blockchain Firm $1.5M to Build Supply Chain Network." *CoinDesk*, https://www.coindesk.com/markets/2020/06/15/us-air-force-gives-blockchain-firm-15m-to-build-supply-chain-network/, accessed 21 June 2023.
73. Nagarajan, S. "U.S. Air Force Pumps $30M Into Blockchain for Supply Chains." *Blockworks*, https://blockworks.co/news/us-air-force-simba-blockchain-supply-chains, accessed 22 June 2023.
74. Wright, T. "U.S. Air Force Prioritizes Blockchain Security With New Constellation Network Contract."

REFERENCES, *continued*

Cointelegraph, https://cointelegraph.com/news/us-air-force-prioritizes-blockchain-security-with-new-constellation-network-contract, accessed 21 June 2023.

75. Constellation Network, Inc. "Constellation Network Achieves Scalability, Security and Defense Approval in Executing U.S. Air Force Phase II Blockchain Contract." *Cision: PR Newswire*, https://www.prnewswire.com/news-releases/constellation-network-achieves-scalability-security-and-defense-approval-in-executing-us-air-force-phase-ii-blockchain-contract-301821462.html, accessed 23 June 2023.
76. Constellation Network, Inc. "The Standard for Government." *Constellation*, https://constellationnetwork.io/federal/, accessed 22 June 2023.
77. U.S. Department of Defense. "DoD Digital Modernization Strategy." Office of Prepublicaton and Security Review, Arlington, VA, https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF, accessed 24 June 2023.
78. ITAMCO. "ITAMCO to Develop Blockchain-Based Secure Messaging App for U.S. Military." *Cision: PR Newswire*, https://www.prnewswire.com/news-releases/itamco-to-develop-blockchain-based-secure-messaging-app-for-us-military-300464063.html, accessed 24 June 2023.
79. Inca Digital. "DARPA Launches Crypto Project With Inca Digital." *Cision: PR Newswire*, https://www.prnewswire.com/news-releases/darpa-launches-crypto-project-with-inca-digital-301632136.html, accessed 24 June 2023.
80. Kelly, L. J. "DARPA Is Bankrolling Research Into Crypto and National Security." *Decrypt*, https://decrypt.co/110401/us-military-agency-bankrolls-research-crypto-national-security, accessed 24 June 2023.
81. Siwicki, B. "Healthcare Blockchain Leader Talks Challenges and Trends in DLT." *HealthcareITNews*, https://www.healthcareitnews.com/news/healthcare-blockchain-leader-talks-challenges-and-trends-dlt, accessed 25 June 2023.
82. Melendez, S. "How IBM and the CDC Are Testing Blockchain to Track Health Issues Like the Opioid Crisis." *Fast Company*, https://www.fastcompany.com/90231255/how-ibm-and-the-cdc-are-testing-blockchain-to-track-health-issues-like-the-opioid-crisis, accessed 25 June 2023.
83. ETHNews. "IBM Doubles Down on Blockchain to Improve Security of Personal Health Records." *Bitnewsbot*, https://bitnewsbot.com/ibm-doubles-down-on-blockchain-to-improve-security-of-personal-health-records/, accessed 25 June 2023.
84. Ledger Insights. "IBM, Oracle Launch Blockchain to Integrate COVID-19 Data From World Health Organization, CDC." *Ledger Insights*, https://www.ledgerinsights.com/ibm-oracle-launch-blockchain-to-integrate-covid-19-data-from-world-health-organization-cdc/, accessed 25 June 2023.
85. U.S. Food and Drug Administration. "DSCSA Pilot Project Program." *FDA*, https://www.fda.gov/drugs/drug-supply-chain-security-act-dscsa/dscsa-pilot-project-program, accessed 25 June 2023.
86. U.S. Food and Drug Administration. "Drug Supply Chain Security Act Pilot Project Program: Final Program Report." *FDA*, https://www.fda.gov/media/168307/download, accessed 25 June 2023.
87. Ekblaw, A. C. "MedRec: Blockchain for Medical Data Access, Permission Management and Trend Analysis." Massachusetts Institute of Technology, Cambridge, MA, https://www.media.mit.edu/publications/medrec-blockchain-for-medical-data-access-permission-management-and-trend-analysis/#:~:text=MedRec%20accomplishes%20record%20management%20without,data%20sources%20and%20the%20patients, accessed 26 June 2023.
88. National Oceanic and Atmospheric Administration Fisheries. "Tackling Challenges of Global Seafood Traceability Programs." *NOAA Fishiereis*, https://www.fisheries.noaa.gov/feature-story/tackling-challenges-global-seafood-traceability-programs, accessed 25 June 2023.
89. National Oceanic and Atmospheric Administration Fisheries, STIMSON, World Wildlife Fund. "Seafood Traceability Practitioner's Workshop: Exploring Programs From Design to Implementation—Summary Report." https://media.fisheries.noaa.gov/2022-03/NOAAStimsonWWFWorkshopReportMarch2022.pdf, accessed 25 June 2023.
90. Seafood Alliance for Legality and Traceability. "Unpacking the Blockchain: A Seafood Perspective on Blockchain Technology." *SALT*, https://www.salttraceability.org/story-hub/unpacking-the-blockchain-a-seafood-perspective-on-blockchain-technology/, accessed 25 June 2023.
91. U.S. Department of Homeland Security. "News Release: DHS S&T Silicon Valley Innovation Program Makes New Phase 1 Awards to a Global Cohort of Five Blockchain Companies." *DHS Science and Technology*, https://www.dhs.gov/science-and-technology/news/2020/10/09/news-release-dhs-st-svip-makes-new-phase-1-awards-five-blockchain-companies, accessed 26 June 2023.

REFERENCES, *continued*

92. Ledger Insights. "Homeland Security Makes an Award for Blockchain Oil Traceability." *Ledger Insights*, https://www.ledgerinsights.com/homeland-security-makes-an-award-for-blockchain-oil-traceability/, accessed 26 June 2023.

93. U.S. Department of Homeland Security. "News Release: DHS Awards $193K for Standards Based Technology to Enhance the Visibility of Food Supply Chains." *DHS Science and Technology*, https://www.dhs.gov/science-and-technology/news/2020/10/09/news-release-dhs-awards-193k-enhance-visibility-food-supply-chains, accessed 26 June 2023.

94. Measur.io. "Earthstream." *Measur.io. The Intelligence Standard*, https://www.mesur.io/earthstream, accessed 26 June 2023.

95. U.S. Department of Homeland Security. "News Release: DHS S&T SVIP Awards Funding to Monitor Current and Future Biological Threats." *DHS Science and Technology*, https://www.dhs.gov/science-and-technology/news/2021/04/05/news-release-dhs-st-svip-awards-funding-monitor-current-and-future-biological-threats, accessed 26 June 2023.

96. U.S. Department of Homeland Security. "News Release: DHS Awards $145K for Standards Based Digital Twin Solution for E-Commerce Shipment Traceability." *DHS Science and Technology*, https://www.dhs.gov/science-and-technology/news/2020/10/09/news-release-dhs-awards-twin-solution-e-commerce-shipment-traceability, accessed 26 June 2023.

97. AppInventiv. "How Is Blockchain Disrupting the Energy Sector? Benefits and Use Cases." *Appinventiv*, https://appinventiv.com/blog/blockchain-in-energy-sector/, accessed 17 June 2023.

98. Pacific Northwest National Laboratory. "Building Trust in Blockchain for the Electric Grid." *Pacific Northwest National Laboratory*, https://www.pnnl.gov/news-media/building-trust-blockchain-electric-grid, accessed 27 June 2023.

99. Guardtime. "About." *Guardtime*, https://guardtime.com/about, accessed 27 June 2023.

100. Johnson, B., and M. Mylrea. "Keyless Infrastructure Security Solution (KISS) Pacific Northwest National Laboratory (PNNL)." U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response, Wasington, DC, https://www.energy.gov/sites/default/files/2018/12/f58/PNNL%20-%20KISS.PDF, accessed 27 June 2023.

101. Walton, R. "DOE Tests Blockchain Technology to Ensure Grid Security, Resilience in First-of-Its-Kind Demonstration." *UtilityDive*, https://www.utilitydive.com/news/doe-tests-blockchain-technology-to-ensure-grid-security-resilience/637364/, accessed 27 June 2023.

102. Hink, R. B., G. Hahn, A. Werth, E. C. Piesciorovsky, A. Lee, W. Monday, and Y. Polsky. "Oak Ridge National Laboratory Pilot Demonstration of an Attestation and Anomaly Detection Framework Using Distributed Ledger Technology for Power Grid Infrastructure." ORNL/TM-2022/2527, Oak Ridge National Laboratory, Oak Ridge, TN, https://info.ornl.gov/sites/publications/Files/Pub180482.pdf, accessed 27 June 2023.

103. Chow, E. "China Selects Pilot Zones, Application Areas for Blockchain Project." *Reuters*, https://www.reuters.com/world/china/china-selects-pilot-zones-application-areas-blockchain-project-2022-01-30/, accessed 30 June 2023.

104. Elston, T.-B. "China Is Doubling Down on its Digital Currency." *Foreign Policy Research Institute*, https://www.fpri.org/article/2023/06/china-is-doubling-down-on-its-digital-currency/#:~:text=What%20Is%20the%20Digital%20Yuan,digitized%20version%20of%20physical%20RMB, accessed 30 June 2023.

105. Seth, S. "What Is a Central Bank Digital Currency (CBDC)?" *Investopedia*, https://www.investopedia.com/terms/c/central-bank-digital-currency-cbdc.asp, accessed 30 June 2023.

106. McKinsey & Company. "What Is Central Bank Digital Currency (CBDC)?" *McKinsey & Company*, https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-central-bank-digital-currency-cbdc, accessed 30 June 2023.

107. He, L. "China Makes Major Push in its Ambitious Digital Yuan Project." *CNN Business*, https://www.cnn.com/2023/04/24/economy/china-digital-yuan-government-salary-intl-hnk/index.html, accessed 30 June 2023.

108. Tassev, L. "China-Backed Blockchain Project Proposes SWIFT Alternative for Stablecoins and CBDCs." *Bitcoin.com*, https://news.bitcoin.com/china-backed-blockchain-project-proposes-swift-alternative-for-stablecoins-and-cbdcs/, accessed 30 June 2023.

109. Kharpal, A. "China Has Been Quietly Building a Blockchain Platform. Here's What We Know." *CNBC*, https://www.cnbc.com/2022/05/16/china-blockchain-explainer-what-is-bsn-.html, accessed 30 June 2023.

110. Guardtime. "Research." *Guardtime*, https://guardtime.com/research, accessed 30 June 2023.

REFERENCES, *continued*

111. Canadian Broadcasting Corporation. "Blockchain Could Boost Economic Growth in Canada—But Is Canada Ready?" *CBC*, https://www.cbc.ca/news/politics/blockchain-canada-report-1.6898656, accessed 18 September 2023.

112. Sehgal, P. "ATB Ventures to Help Canadian Government With Its Digital ID Efforts." *IT World Canada*, https://www.itworldcanada.com/article/atb-ventures-to-help-canadian-government-with-its-digital-id-efforts/473393, accessed 30 June 2023.

113. Leal, N. "Canada Pilots Blockchain Staff Records." *Global Government Forum*, https://www.globalgovernmentforum.com/canada-pilots-blockchain-staff-records/, accessed 30 June 2023.

114. Government of Canada. "Talent Cloud." *Government of Canada*, https://talent.canada.ca/en/talent-cloud, accessed 30 June 2023.

115. Government Technology Agency. "Digital Health Passport Joins the Fight Against COVID-19." *GovTech Singapore*, https://www.tech.gov.sg/media/technews/digital-health-passport-joins-the-fight-against-covid-19, accessed 30 June 2023.

116. Government of Singapore. "HealthCerts—Digital Standards and Schema." *Singapore Government Developer Portal*, https://www.developer.tech.gov.sg/products/categories/digital-solutions-to-address-covid-19/healthcerts/overview.html#what-is-healthcert, accessed 30 June 2023.

117. Mapperson, J. "Blockchain Can Combat Australia's $1.7B Food and Wine Fraud Problem." *Cointelegraph*, https://cointelegraph.com/news/blockchain-can-combat-australia-s-1-7b-food-and-wine-fraud-problem, accessed 30 June 2023.

118. Miller, M. "Bitland: Property Rights for the World's Poor." *The Borgen Project*, https://borgenproject.org/property-rights-for-the-worlds-poor/, accessed 30 June 2023.

119. Aitken, R. "Bitland's African Blockchain Initiative Putting Land on the Ledger." *Forbes*, https://www.forbes.com/sites/rogeraitken/2016/04/05/bitlands-african-blockchain-initiative-putting-land-on-the-ledger/?sh=12fb6e3c7537, accessed 30 June 2023.

120. Gordon, N. "The Crash in Crypto Prices May Be Good News for at Least One Interest Group: Gamers." *Fortune*, https://fortune.com/2022/06/17/crypto-crash-graphics-card-price-nvidia-amd-bitcoin-ether-mining/, accessed 14 July 2023.

121. Schmidt, J. "Why Does Bitcoin Use So Much Energy?" *Forbes Advisor*, https://www.forbes.com/advisor/investing/cryptocurrency/bitcoins-energy-usage-explained/, accessed 14 July 2023.

122. Ethereum. "Ethereum's Energy Expenditure." *Ethereum.org*, https://ethereum.org/en/energy-consumption/, accessed 14 July 2023.

123. Petrosyan, A. "Annual Number of Data Compromises and Individuals Impacted in the United States From 2005 to 2022." *Statista*, https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/, accessed 14 July 2023.

124. Schlatt, V., T. Guggenberger, J. Schmid, and N. Urbach. "Attacking the Trust Machine: Developing an Information Systems Research Agenda for Blockchain Cybersecurity." International Journal of Information Management, vol. 68, https://www.sciencedirect.com/science/article/pii/S0268401222000019#bib36, accessed 15 July 2023.

125. McShane, G. "What Is a 51% Attack?" *CoinDesk*, https://www.coindesk.com/learn/what-is-a-51-attack/, accessed 15 July 2023.

126. Stanford University. "The Stanford Center for Blockchain Research." *Stanford*, https://cbr.stanford.edu/, accessed 15 July 2023.

127. Carnegie Mellon University. "Blockchain Research." *CyLab*, https://www.cylab.cmu.edu/research/blockchain/research.html, accessed 15 July 2023.

128. Massachusetts Institute of Technology. "Blockchain." *MIT Media Lab Research*, https://www.media.mit.edu/research/?filter=everything&tag=blockchain, accessed 15 July 2023.

129. Arizona State University. "Arizona State University's Blockchain Research Lab." *ASU*, https://blockchain.asu.edu/, accessed 15 July 2023.

130. Blockchain Research Institute. Homepage. *Blockchain Research Institute*, https://www.blockchainresearchinstitute.org/, accessed 16 July 2023.

131. OpenLedger Lab ApS. "Blockchain R&D Services." *OpenLedger*, https://openledger.info/services/research-and-development/, accessed 16 July, 2023.

132. Ethereum. "Active Areas of Ethereum Research." *Ethereum.org*, https://ethereum.org/en/community/research/, accessed 16 July 2023.

133. Business Wire. "Business and Academia Leaders Join to Host Inaugural Blockchain Research Symposium" *BW*, https://www.businesswire.com/news/home/20230420005042/en/Business-and-Academia-

REFERENCES, *continued*

Leaders-Join-to-Host-Inaugural-Blockchain-Research-Symposium, accessed 16 July 2023.

134. Carnegie Mellon University. "CMU Secure Blockchain Summit." *CyLab*, https://www.cylab.cmu.edu/research/blockchain/secure-blockchain-summit.html, accessed 16 July 2023.
135. Stanford University. "The Science of Blockchain Conference 2023 (SBC'23)." *Stanford*, https://cbr.stanford.edu/sbc23/, accessed 16 July 2023.
136. Sultanik, E., T. Brunson, M. Myers, A. Remie, S. Moelius, T. Amir, F. Manzano, E. Kilmer, and S. Schriner. "Are Blockchains Decentralized? Unintended Centralities in Distributed Ledgers." *Trail of Bits*, https://www.trailofbits.com/documents/Unintended_Centralities_in_Distributed_Ledgers.pdf, accessed 16 July 2023.
137. Stouffer, K. A. "NIST Releases Study on Blockchain and Related Technologies for Manufacturing Supply Chain Traceability." *NIST*, https://www.nist.gov/news-events/news/2022/04/nist-releases-study-blockchain-and-related-technologies-manufacturing, accessed 16 July 2023.

This Page Intentionally Left Blank

This Page Intentionally Left Blank

BLOCKCHAIN APPLICATIONS FOR FEDERAL GOVERNMENT

Megan N. Lietha

CSIAC-BCO-2023-483