Information Services & Use 38 (2018) 173–185
DOI 10.3233/ISU-180021
IOS Press



# Blocks as digital entities: A standards perspective

Patrice A. Lyons[*] and Robert E. Kahn
*Corporation for National Research Initiatives (CNRI), 1895 Preston White Drive, Suite 100 Reston, VA 20191, USA*

**Abstract.** The notion of thoughts, ideas and other information fixed in a tangible medium of expression for purposes of reproducing, displaying or communicating the information to others has its origins in antiquity. Both the information itself and its symbolic expression are purely conceptual entities until fixed in a material object. When an intangible means of expression, in which symbolic logic is represented as or converted to machine-independent data structures in digital form, and structured as digital objects (i.e., digital entities), this implementation may be viewed as the logical equivalent of fixation in a material object; and, in this context, we are viewing a block as a particular way of structuring a digital object, and a blockchain in itself as a digital object that incorporates one or more objects.
In considering the development of commerce based on the Digital Object (DO) Architecture, an interesting area for exploration and development has been introduced around the concept of mobile computer programs configured as digital objects. This technology may play an important role in the management of software embedded in new Internet of Things (IoT) devices such as microcontrollers, where issues have arisen with respect to the interoperability of such software with other resources in the developing IoT. There have been many efforts over the years to evolve the Internet to embrace new technology, such as the DO Architecture, and we hope this trend continues unabated.

Keywords: Internet, CNRI, blockchain, digital object architecture, packet switching, ARPANET, mobile program technology, DARPA, knowbot, digital object, DOA

## 1. From circuits to packets

With the introduction of telegraphy and later telephony, communications technology was created and evolved on the basis of circuits being established between parties A and B that wished to communicate with each other. Whether these circuits were physical wires or other electronic pathways made little conceptual difference. These pathways enabled analog signals (i.e., waveforms) to be communicated between A and B. Telegraph operators (i.e., individuals) mapped information into simple signals (e.g., using Morse code) that could be sent from one operator to another and interpreted by each operator upon reception. This process typically involved keying in the dots and dashes by hand for relay from one operator to another. Thus was born the original digital communications revolution. Note that we purposely start well beyond the use of smoke signals and naval signaling which were arguably even earlier forms of digital communication, but did not really represent a technological revolution in their own right.

[*]Corresponding author: E-mail: palyons@cnri.reston.va.us.

Telephony was all about communicating sounds as analog signals in a move away from the earlier digital world of telegraphy. Microphones embedded in telephones converted voice into waveforms for transmission and, upon reception, the sound was reproduced by devices called speakers (unfortunately along with any noise introduced along the way). Many years later, it was recognized once again, that such signals could also represent more general forms of information in digital form, if it was embedded or mapped into the transmitted waveforms. It was then up to the two parties to interpret or otherwise process the received waveforms properly to manifest the information. Eventually modems were developed that enabled digital information to be modulated into waveforms for transmission; they also enabled the received waveforms to be demodulated into received data, albeit with some probability of error. Thus was enabled a new era of digital communications where eventually, digital devices such as computers, could also be attached at one or both ends to enable computer communication.

The role of operators was inherent in early telegraph systems to handle keying; and operators were used to establish connections or circuits between A and B in the early telephone systems. Eventually it became clear for both technical and economic reasons that the role of operators needed to be automated. Switches were developed to create connections, so that circuits could be established without operator intervention; and thus was introduced the need for an early technical notion of identifiers (rather than just the names of the parties) for use in communications. Once acquired, party A's phone would communicate the identifier to a nearby telephone switch that would establish the connection.

In addition to identifying party B's phone, the combination of the identifier for party A's phone and party B's phone would constitute an implicit identifier for the connection. Of course, this identifier would not be unique for that particular connection since every succeeding connection between those two parties would have exactly the same identifier. A date-timestamp could also be added to distinguish them, but, typically, this was only done in billing records and not, generally, for purposes of accessing information sent over any particular connection. Nevertheless, it did associate the identifier with the circuit and, by indirection, the information sent over the circuit.

The early telephone switches were mainly mechanical, and thus took many seconds to activate, but subsequently switches were built with electronic components and thus operated faster. At first, this approach was used for making local connections, but establishing connections over longer distances took more time, if for no other reason than the speed of light dictated a limit to how fast a long-distance circuit could be established. Computer communication requirements dramatically changed the landscape, as they called for more efficient use of the communication resources for handling short bursts of computer data, faster setup times than circuit switching provided, and error-free communication.

## 2. Introduction of packet switching

Packet switching technology, developed in the 1960s, enabled that more efficient system; however, this approach was not without some controversy and resistance. The main concern was its potential to negatively impact the steady revenue streams that resulted from the use of existing circuit switching systems. Nevertheless, with impetus from government funding and the research community, progress was steadily made. Initially, this occurred without the direct involvement of the existing telecommunications industry – other than in the provision of leased lines. Ultimately, though, the value of this new switching approach became apparent throughout the industry and was adopted by most of the telecommunication service providers.

The basis of this new approach was no longer the circuit, but rather the packet. Generally, a packet was viewed as an elemental container for carrying data in a distributed network; and it typically included addressing information used for routing. A packet consisted of a finite set of bits with a known, but relatively small limit (such as 1,000 bits), and a unique identifier for the destination party B, which, in this case, would likely be a computer. Thus, in principle, packets communicated between party A and party B could be identified by the concatenation of the two identifiers of A and B; but, as before, this identification would not be unique to any specific packet, as all packets between A and B would have the same identifier. Duplicate transmissions were anticipated to occur in these new packet switching systems, perhaps due to errors incurred enroute, which could easily have confused the receiver. Packets could also arrive out-of-order. However, if the computers relied on protocols that numbered the packets in some appropriate fashion, the packets could be re-ordered at the destination and any duplicate packets rejected upon reception. Limits were placed on how large such numbers could be and, after a long while, and with enough traffic, the numbers would be recycled.

In the Advanced Research Projects Agency Network (ARPANET), the first packet-switched net, packets were routed though minicomputers that acted as small packet switches. Each computer in the net was connected by wire to one of the packet switches. Then, after one or more hops, and no errors along the way, the packets sent by party A would presumably be delivered accurately to party B along the appropriate wire. In the early Internet, whose protocols enabled different networks and computers to intercommunicate, the packets were routed between networks through gateways. The identifiers used by the gateways were globally unique machine addresses called Internet Protocol (IP) addresses. The gateways (now called routers) interacted with each other to determine how best to route the IP packets [1].

In these cases, for a very brief period, the packets were a specifically-identified set of bits; but very soon after their delivery, the ability of a network to map these identifiers to those specific bits became lost as the packets were not retained within the network. One simply did not ask for the packet with identifier X after the fact since such a request could not be fulfilled. If desired, the computers could store the packets themselves and give them a new identifier known only to party B's computer - such as a file name. No other party would know that unique identifier, unless party B made it available; nor would party B necessarily want any other party to know it in each instance, if at all. But, even if it did, it would have to support a way for others to learn about these unique identifiers. Typically, they would advertise them with directory listings on specific computers known by their network addresses or strings that resolved to them.

As a program manager of a packet radio project at the Defense Advanced Research Projects Agency (DARPA) in the mid-1970s, one of the authors (Kahn) explored the idea of moving information represented in digital form over a new kind of packet- switched network involving wireless communication and switches and terminals that could be mobile. This approach became the paradigm for many of today's cellular networks. The idea was based on the movement of digital information, including computer programs, from one computer to another over a multi-hop wireless network; and issues such as authentication and privacy were addressed in that context [2].

Managing information represented in digital form in a distributed computer network is another matter entirely. Whether the specific information is private and of interest only to party B, or may be made available only to a defined group of users (based upon a system that enables users to be authenticated and information to be identified) one needs to be able to identify the information for access or for dissemination. This is technically straightforward on most time-sharing systems, which typically provide this capability using access control mechanisms based on information stored in specific files, and user authentication based on unique (to that system) names and passwords. Any two users on the same system could, in principal, share information on that system. The spread of the Internet made this approach of

centralized sharing either impractical or infeasible for many applications. In the distributed world that the Internet enabled, information represented in digital form could be stored at multiple places, in different systems, and with a variety of access controls; and what had been a simple sharing option on a single computer no longer worked as straightforwardly as before.

## 3. Development of mobile program technology

Early experiments with pairs of computers sometimes involved the movement of programs from one computer to another over telephone lines. These can be understood in a general sense as mobile programs, although such communications, even with the advent of computer networks, were basically pairwise between the two parties. The receiving machine was set up manually to expect a specific type of program, which it stored and then ran at some later time. Various network-based defense system capabilities were deployed in the early days (circa late 1950s–1970s). File transfer protocols were developed to move files between computers on a network; and the Web was later introduced to simplify access to remote files.

The first public capability to manage mobile programs was arguably the use of Remote Job Entry (RJE) in the ARPANET. RJE was a protocol for remote submission of a program, then called a "job", from one machine to another for purposes of having the program executed remotely and the results made available by some means to the sender. In this case, while the program might have been created on one machine for sending to the other, the program did not necessarily have to run on both machines; and if it could be run on both machines, one might not need to have it executed remotely. This RJE capability typically involved the use of a file transfer protocol over the network; and the results could have been stored at the remote computer for subsequent retrieval rather than being automatically returned to the user.

In the mid-1980s, Robert E. Kahn and Vinton G. Cerf, working together at Corporation for National Research Initiatives (CNRI), continued the efforts they had started earlier to evolve the Internet architecture by introducing new methods of identifying, securing, and otherwise managing information in digital form. Their basic approach was to develop the notion of mobile programs that could be tasked by humans or computers, and to describe a network-based system for managing mobile programs so that a human did not need to participate in the processing and communications loop, until perhaps after the designated task was completed. Prior to this work, communicating a program from one location to another, and performing operations on a computational facility to carry out a given task, would typically have required a separate step by a human – perhaps to run the program, collect the results, and cause those results to be sent back to the program's origin. Such processes and communications would not have qualified as mobile programs in today's sense of the term.

## 4. Architecture for Managing Mobile Programs

The creation of a systems approach for managing mobile programs, involved developing an overall architecture and a corresponding set of protocols. Use of standard protocols was pioneered in the ARPANET and enabled computers on a given network to communicate with each other without the need to first learn how to communicate via proprietary protocols possibly unique to each computer. The Internet protocols extended this concept to a multiple network environment, and thus made the Internet possible. A systems approach was also needed for mobile programs to be managed as network-based entities. Such an approach was outlined in the seminal paper "Digital Library System – The World of Knowbots",

(1988) [3]. While the paper was marked DRAFT, it was widely-circulated in the late 1980s, and, in particular, was distributed at a meeting on "Collaboratories" held at Rockefeller University in 1989 [4], and at a Workshop held at CNRI that same year [5]. The "World of Knowbots" document provided the first conceptual discussion of a network approach to mobile programs as they might be understood today [6].

"The World of Knowbots" described a system comprised of multiple Service Stations that cooperated to collectively form an Operating Environment. A Service Station would take responsibility for creating a mobile program and managing its existence, with security, in this environment during the lifetime of the mobile program. Mobile programs could be moved from Service Station to Service Station in the environment, be executed in the Service Station's computational environment, and the results incorporated into, or attached to, the mobile program for communication to another Service Station (or to another mobile program at that location) within the operating environment [7].

An early example of the use of this mobile program technology was developed by CNRI (starting in 1989) for the National Library of Medicine (NLM). Known as the ABIDE Gateway System, the service enabled a user of the NLM's systems to communicate in the Internet using mobile programs [8]. The various NLM databases, such as Medline and Toxnet, were connected to a local area network (LAN) at NLM for fast interactive Internet access. Previously, only dial-up access via the landline telephone system was available there. A user's query would be formatted by the user's system into a mobile program and sent to NLM via the Internet for processing. The Service Station at NLM would interpret the arriving program, determine which of the NLM databases to query, format the query into a command language request that was unique to the appropriate database (or format multiple requests to multiple databases, if applicable), send the request(s) via the LAN and, upon receipt of the results over the LAN, return them interactively to the user's system for presentation to the user. Subsequent research in this project focused on the use of multiple Service Stations working cooperatively to provide enhanced processing capabilities.

## 5. Digital objects in a mobile environment

Based on the earlier work described in the "World of Knowbots" paper, in the late 1980s, CNRI focused more specifically on the information management portions of its mobile program technology and embarked on efforts to establish an architecture for managing digital information in a distributed network environment such as the Internet. As a defensive matter, CNRI filed a U.S. patent application for this idea in 1993 [9], and highlighted the use of digital object identifiers (informally called handles), a resolution mechanism, repositories for information management, and related techniques such as authentication. While now expired, this patent provides a benchmark in the public domain for those seeking to provide services based on the DO Architecture going forward.

As a digital object, a mobile program has a structure of parts, one or more of which may also be digital objects with separate identifiers. This would allow, for example, such identifiers to be used to refer to specific processing steps, or previous results obtained by the mobile program and perhaps incorporated therein or stored elsewhere. Other information about the mobile program may be accessed by resolving its identifier, such as its provenance, its authenticity (using separate fingerprints of the digital object), public keys and terms and conditions for its use.

With funding from DARPA, CNRI organized the Computer Science Technical Reports (CSTR) project in 1992, as a multi-participant testbed to demonstrate and evaluate the potential of the above-mentioned digital object framework [10]. What later became known as the Digital Object Architecture was introduced by CNRI to the participants in the CSTR project soon thereafter for consideration.

As part of the CSTR project, and based on the CNRI inputs, Robert Wilensky and Robert E. Kahn prepared a paper entitled "A Framework for Distributed Digital Object Services". Drafts of the paper were first circulated to the CSTR participants early in 1994, and made publicly available in the Internet in 1995 [11]. This framework differed from the basic approach taken in object-oriented (O-O) programming by addressing instead the management of each object's internal data structures (i.e., those parts that are normally not directly accessible in an O-O environment), as well as the parts of the architecture that were required to support its use in a distributed system. CNRI called these data structures (as well as the programs in which they may have been incorporated) "digital objects".

The notion of a digital object (DO) may be viewed as a *logical extension of a packet in a network context* [12], with the exception that (unlike most packets) digital objects are normally intended to be stored for subsequent access by authorized parties; and each DO has an associated unique persistent identifier. A "digital object" is defined as a sequence of bits, or a set of such sequences, that incorporates a work or other information in which a party has rights or interests, or in which there is value. A DO's associated unique persistent identifier can be resolved to "state information" about the DO, such as its location(s), access controls, time of creation, public keys (if any), and verification information. A trustworthy resolution system is critical to the overall management of digital objects, much as a trustworthy routing system is critical to the use of IP addresses.

During the early development of the DO Architecture (or DOA), CNRI presented the architectural ideas to a group of about fifty companies meeting as part of CNRI's Cross-Industry Working Team (XIWT), where it was noted that the DO Architecture could play an important role in the developing Internet. The group was supportive of implementing and testing the DO Architecture as part of the growing Internet. In its May 1997 report, the group addressed business, technical, and legal aspects of what they called containers [13], cryptolopes, packages, or, more generally, digital objects. The importance of chaining of operations and value management was also recognized in the report [14].

Today, the development of microcontroller (MCU) technology and microservices in the developing Internet of Things (IoT) provides new challenges from an information management perspective. The interaction of computer processes involving sensor technology raises interesting questions about how to structure the digital representation of programs to produce desired results [15]. The implementation of the DO Architecture in this context may be quite useful, particularly where the program code in digital form uses encryption or is otherwise protected to help secure operations and to enable interoperability with other resources.

## 6. Representing value in digital form

Historically, a block, also called a data structure, was viewed essentially, as a sequence of bits, usually with a defined beginning and end, but may or may not have been uniquely identified other than, perhaps, by its arrival sequence in time. Also, use of blocks often involved encryption. The terms block and block coding are well known in the communications field, and the term "block cipher" is well known in the security arena [16].

In general, a "block" may be considered a digital object that is configured using specific methods; and there are many issued or pending patents on various ways to accomplish this. Commentators often attribute the notion of a block and blockchain as having originated with an unknown person or persons (called Satochi Nakamoto) who authored the original bitcoin white paper, and the first reference implementation became available soon thereafter [17]. Earlier efforts to develop digital cash systems had existed, but this

is generally understood to be the start of the current blockchain and digital ledger technology activities. The authors would like to note, however, an article they wrote on the general subject of representing value as digital objects (discussed below) was made available earlier that decade.

Their article, titled "Representing Value as Digital Objects: A Discussion of Transferability and Anonymity", introduced the idea that value could be represented in digital form and structured as a digital object [18]. The article described the important role of unique persistent identifiers associated with digital objects and a resolution mechanism to enable a capability for anonymity and transferability. The representation of "value" based on an implementation of the DO Architecture was introduced as a logical equivalent to various paper-based entities such as bills of lading, wills, and contracts, and the chaining of one digital object to another, was described. A use case was presented in the patent application below where, for example, the Federal Reserve represents a ten-dollar value in digital form, structures this information as a digital object having an associated unique persistent identifier, and then a hash of this identifying information is incorporated in the digital object when it is issued to a bank. While the dollar value may be called a block, a better approach would be to view it simply as a one-dollar bill even though it is in digital form, since tying the representation of value and chaining of operations to the latest jargon may lead to confusion in practice.

A patent application, titled "Authenticating and using digital objects", was filed by CNRI in 2003 based on the approach described in the representing value paper, in which it was specified that the technology may be applied in managing, *inter alia*, the issuance and authentication of financial instruments, documents, articles, medical records, contracts, bills of lading, and other information in digital form [19]. CNRI later decided to abandon this application when the claims were rejected by the U.S. Patent & Trademark Office as being already covered by the now expired CNRI Patent No. 6,135,646, "System for Uniquely and Persistently Identifying, Managing, and Tracking Digital Objects [20]". CNRI's rationale for this decision was to avoid having to argue against interest in the application process. The patent application on "Authenticating and Using Digital Objects" was also about engendering trust in digital objects having value. As a matter of public record, this application may represent a useful starting point from a prior art perspective.

## 7. Standardization of digital entities

The DO Architecture represents a coherent approach to managing digital information that may be distributed in a network environment. It provides a general way to manage information for multiple purposes, over both the short and/or long-term, based on the concept of the digital object. The information in the form of a digital object can be managed based on its identifier while in transit, while stationary (as in a storage system), and while being processed.

In the 2007, CNRI was invited to introduce the DO Architecture at a meeting of International Telecommunication Union (ITU) Focus Group on Identity Management [21]; and later CNRI submitted a formal contribution to ITU-T, Study Group 17 (Security) that provided a summary of the then existing components of the DO Architecture [22]. The three basic components of the DO Architecture were introduced: the identifier/resolution system, the DO Registry, and the DO Repository [23]. Work proceeded on the CNRI contribution, and Dr. Kahn served as Editor. In September 2013, the member states approved ITU-T Recommendation X.1255: "Framework for discovery of identity management information [24]". While based substantially on the Digital Object Architecture, for purposes of X.1255, a "digital object" was defined as a "digital entity".

The National Institute of Standards and Technology (NIST), in its "Framework for Cyber-Physical Systems", expressed support for ITU-T Recommendation X.1255. In its Release 1.0, it observed that X.1255 "adopts a fundamental approach toward defining core concepts for purposes of interoperability across heterogeneous information systems. It describes a digital entity data model that provides a uniform means to represent metadata records as digital entities, and can also be used to represent other types of information as digital entities (whether also referred to as data, data item, data fusion, or other terminology). It is a logical model that allows for multiple forms of encoding and storage, and enables a single point of reference (i.e., the identifier) for many types of information that may be available in the Internet [25]".

There has also been discussion recently about whether a "digital entity" may be considered a "block" in the context of an ITU-T Focus Group on Application of Distributed Ledger Technology (FG-DLT). To clarify matters, CNRI submitted a Contribution to a meeting of the FG-DLT (Bern, Switzerland; Feb. 2018) where it addressed the definition of "blocks" as "digital entities [26]". In the "Base document for terms and definitions for DLT" agreed to by the meeting, the following note was added to the definition of block: "A block may be mutable and considered as the digital entity described in clause 3.2.2 in [b-X.1255], however, it can be applied to other networks or other computational facilities [27]". It should be recalled, however, that, while a block may be considered a digital entity for distributed ledger technology applications, this is but one of a wide-variety of ways to implement the information management technology described in ITU-T Recommendation X.1255.

## 8. Security considerations

In the past few decades, cybersecurity threats have increased significantly. The possible role of the DO Architecture in protecting the Internet was discussed in an article written by Dr. Kahn, titled "The Role of Architecture in Internet Defense [28]". The efficient and secure management of information in digital form structured as digital objects was also addressed by Dr. Kahn at a full committee hearing on "*Energy Efficiency of Blockchain and Similar Technologies*", in the U.S. Senate Committee on Energy and Natural Resources [29].

In his prepared testimony, he stated that, in his view, blockchain technology represents one specific way of structuring digital objects, and that a blockchain is, in reality, a digital object that consists of other linked digital objects. He observed that the DO Architecture could be implemented in a wide variety of ways and was not just limited to the specific approaches being taken by the emerging bitcoin and blockchain industries. From a security perspective, he noted that: "Ultimate trust in a digital object, no matter how you obtain it, would be based on the application of strong cryptography, whether just for authentication or to hide the contents. One size fits all is unlikely to be what is required for all applications in either the short- or the long-term. And the overall efficiency of the choices made will be an important part of the decision-making process".

From a security perspective, a DO can be signed and validated using PKI (Public Key Infrastructure) or other cryptographic methods that are intrinsic to the overall DO Architecture. Each digital object, or parts of an object, may be encrypted or otherwise protected, apart from the transmission pathway. Unlike many other applications, where an end-to-end philosophy may apply, this concern does not directly arise in the DO Architecture. In this respect, what is sometimes called virtual circuit technology was not a requirement for the early Internet, and its use was only intended as an expedient to get started [30]; however, it is still the basis of how the Transmission Control Protocol (TCP) is used today. Other protocols, such as User

Datagram Protocol (UDP) were introduced a few years later to support applications for which such a packet-based virtual circuit technique was not appropriate.

## 9. Use of DOA in commerce

Digital objects are being widely used today, although such use is not necessarily described in those words; nor does such use exhibit all the attributes one would normally associate with a digital object. For example, while virtually every item of information represented in digital form must be identified for it to be accessed, often the identification methods are not persistent in the sense that they cannot be used effectively over time. While several specific well-known use cases are mentioned below, other implementations may not be as prominent, even though they have been in widespread use for many years.

An early set of adopters came from the library and publishing communities, where persistent reference was critical. The identifier/resolution component of the DO Architecture was deemed to be an excellent choice for this purpose, and has been in widespread use for almost two decades in the science, technology, and medical communities. This led to the establishment of the DOI System by a joint initiative of three trade associations in the publishing industry (International Publishers Association; International Association of Scientific, Technical and Medical Publishers; and the Association of American Publishers) [31]. The DOI System was announced at the Frankfurt Book Fair 1997; and the International DOI® Foundation (IDF) was created soon thereafter to develop and manage the System that is now an ISO standard [32]. In recent years, new industry groups have been working with the IDF to develop applications using the DOI System; e.g., an interesting project in the construction industry for the managing a building's lifecycle (including plans, approvals, applicable codes, and everything in the building itself).

The implementation of the DOA for supply-chain management was demonstrated by a research group in China in 2015 in connection with the management of the infant formula industry (i.e., powdered milk) that had recently been exposed to counterfeiting [33]. By inserting digital object identifiers directly into each such milk container (inside and out), as well as printing it on the label, one could reliably access the metadata about the product, which would typically include the manufacturer of the product and where the product had been originally delivered by the manufacturer for sale to the public. Changing this information would have required obtaining the private key of the manufacturer. If a bogus product were supplied to the market, it would have to have an identifier not created by the manufacturer (and thus immediately be detectable by the purchaser).

Combating counterfeiting of information in digital form involving mobile devices has also been the subject of interest in other areas. Such devices may be as simple as a mobile terminal or as complex as an autonomous vehicle (whether a car, airplane or ship). Implementation of the identifier/resolution component of the DOA has been a focus of discussion, as well as the interoperability of DO identifiers with device identifiers, particularly from a legal perspective [34]. Experiments to apply this technology to chaining of digital objects are being explored.

The entertainment industry applied the technology to the management of certain important entertainment industry assets - in particular movies, television programs, and related activities. During the supply-chain process, each asset is generally made available in multiple stages of release to multiple parties, in multiple formats and in accordance with multiple technical standards. A registry for the Entertainment Identifier Registry Association, based on the DO Architecture was developed for managing this set of assets and has been in use within that industry for close to a decade [35].

Another use case is in the financial industry and concerns the management and visibility of derivative trading records. A system was developed to acquire information from brokerage houses about such trades and to create digital objects that can be globally accessed by authorized parties on a near real-time basis. A demonstration version was first released in 2016 [36]; and a production version was later released in 2017 [37]. The relevant regulatory bodies in the European Union have stipulated that this system be used by the brokerage firms doing business there. Such digital objects are stored in one or more repositories for future access, including many years in the future, even if the underlying technology changes.

The European scientific community leverages the identifier/resolution component of the Digital Object Architecture for persistently identifying scientific datasets and related scientific resources. Efforts are currently underway in Europe to make use of the other components of the DOA to enable scientific workflows and cross-discipline activities. A non-profit organization, the European Identifier Consortium (ePIC), is centrally involved in these efforts [38].

Since its early work in the 1980s, CNRI has continued to develop and deploy reference software implementations of the DO Architecture [39], and, on January 20, 2014, CNRI founded a non-profit organization in Geneva, Switzerland, called the DONA Foundation, to administer a capability for maintaining unique identifiers created by other organizations (first established by CNRI in the early 1990s), and to assume responsibility for evolution of the Digital Object Architecture in the public interest [40].

## 10. Conclusion

Information represented as, or converted to, digital form may be structured as a digital object. For example, a service provided in the Internet can be represented as a digital object, which might consist of metadata about the service, including access and validation information. Once allotted a unique persistent identifier and otherwise structured as a digital object, the service can be managed in the Internet or other computational environments as a digital object now or in the future. The role of software in the provision of services, or as intermediaries, for access or security, will become increasingly important.

Mobile computer programs may soon play a more significant role in either carrying out tasks or efficiently combatting emerging threats as the Internet confronts increased complexity. While techniques like layering and end/end interactions will continue to be used, a more integrated approach seems appropriate when autonomous vehicles and devices are widely deployed and are capable of acting on behalf of users or programs to produce desired results. These devices, whether fixed or mobile, need to have the ability to interoperate with each other and with other information systems, as appropriate. The mobile devices will deploy very unique kinds of mobile programs for which we need to be prepared. The complexities and sheer volume and mobility of information in digital form that will be available require a new paradigm for information management, and the Digital Object Architecture can provide a sound basis for moving forward.

## About the Authors

Ms. Patrice A. Lyons: As General Counsel, Corporation for National Research Initiatives (CNRI), Ms. Lyons has been involved in the analysis of a wide-range of legal and regulatory issues relating to the development of the Internet and the use of new technology in society. Some highlights of her efforts at CNRI include participation in the establishment of ISOC, ensuring that the name INTERNET is available

for use by the public at large, helping to establish the Internet Engineering Task Force (IETF) Secretariat, and later conceiving of an IETF Trust as an integral part of the transition process. She has also provided advice and guidance to CNRI on other legal matters, in particular, the MEMS and Nanotechnology Exchange (MNX®) effort, development of the Digital Object Architecture, and software releases such as Python, Handle.Net, and Cordra.

Ms. Lyons' interest in the application of the law to new technical developments began upon graduation from Georgetown University Law Center (J.D.1969), and later at Columbia University Law School (1969–70) as the Burton Memorial Fellow in copyright and communications studies. While serving as a legal officer at UNESCO (Paris, France; 1971–76), she participated in the drafting of the *Convention Relating to the Distribution of Programme-Carrying Signals Transmitted by Satellite* (1974), and provided advice on an early computer networking project. As a Senior Attorney, Library of Congress (1976–87), she participated in the drafting of regulations on the cable compulsory licensing system, played a lead role in the preparation of the Semiconductor Chip Protection Act of 1984, provided advice on design protection issues, and the status of computer programs from a legal perspective. Phone: 703-620-8990; E-mail: palyons@cnri.reston.va.us

Dr. Robert E. Kahn: Robert E. Kahn is President & CEO of Corporation for National Research Initiatives (CNRI), which he founded in 1986. He received a B.E.E. from the City College of New York in 1960, and M.A. and Ph.D. degrees from Princeton University in 1962 and 1964 respectively. He worked on the Technical Staff at Bell Laboratories and then became an Assistant Professor of Electrical Engineering at MIT. In 1966, he took a leave of absence from MIT to join Bolt Beranek & Newman (BBN), where he was responsible for the system design of ARPANET, the pioneering packet-switched computer network. In 1972, he moved to DARPA and subsequently became Director of DARPA's Information Processing Techniques Office (IPTO). While Director of IPTO, among other things, he initiated Strategic Computing Program, the largest computer research and development program that had ever been undertaken by the federal government up to that point. Dr. Kahn conceived the idea of open-architecture networking. He is a co-inventor of the TCP/IP protocols and was responsible for originating DARPA's Internet Program. More recently, he has been involved in the development and deployment of the Digital Object Architecture, an open architecture for managing information in the Internet. Dr. Kahn has numerous publications and has received many honorary degrees and fellowships. Among his many awards, he is a recipient of the 1997 National Medal of Technology, the 2001 Charles Stark Draper Prize from the National Academy of Engineering, the 2002 Prince of Asturias Award, and the 2004 A. M. Turing Award from the Association for Computing Machinery, the 2004 Presidential Medal of Freedom. He was the recipient of the Japan Prize in 2008 and was one of the inaugural winners of the Queen Elizabeth Prize for Engineering in 2013. He is a member of the National Academy of Engineering and the National Academy of Sciences.

## References

[1] V.G. Cerf and R.E. Kahn, A Protocol for Packet Network Intercommunication, available at https://www.cs.princeton.edu/courses/archive/fall06/cos561/papers/cerf74.pdf; for a brief history of the Internet, see "A Brief History of the Internet", available at https://www.internetsociety.org/wp-content/uploads/2017/09/ISOC-History-of-the-Internet_1997.pdf, accessed 2 September 2018.

[2] R.E. Kahn, The organization of computer resources into a packet radio network, *Managing Requirements Knowledge, International Workshop* (1975), available at https://www.computer.org/csdl/proceedings/afips/1975/5083/00/50830177.pdf, accessed 2 September 2018.

[3] "The Digital Library Project Volumne 1 – The World of Knowbots (DRAFT)", (1988), available at: http://www.cnri.reston.va.us/kahn-cerf-88.pdf, accessed 2 September 2018.

[4] For a group photo of participants at the meeting on "Collaboratories", see http://ai.eecs.umich.edu/people/conway/CSE/CollabTech/CollabTechWorkshop.html, accessed 2 September 2018.
[5] The Workshop Report, "Knowbots in the Real World", is available at http://www.cnri.reston.va.us/wkshp_intel_prop_knowbots_may1989.pdf, accessed 2 September 2018.
[6] Knowbot is a registered trademark of CNRI and has been used in commerce by CNRI for software information services since September 26, 1989.
[7] For additional information and reference software, written in Python, see https://www.cnri.reston.va.us/home/koe/index.html, accessed 2 September 2018; see also U.S. Patent No. US 6,574,628, now expired, covering the mobile program technology, entitled "System for Distributed Task Execution", granted to CNRI by the USPTO on June 3, 2003.
[8] For reference to ABIDE Gateway System, see Long, K., Fowler, J., and Barber, S., "VNS Retriever: Querying MEDLINE over the Internet", Baylor College of Medicine (1992); see also Application Gateway System, Annual Reports (1995-1997), available at https://www.usenix.org/legacy/publications/library/proceedings/sa92/long.pdf, accessed 2 September 2018.
[9] The DO patent, now expired, titled "System for uniquely and persistently identifying, managing and tracking digital objects", U.S. Patent No. 6,135,646, was granted to CNRI by the USPTO in 2000.
[10] CSTR Project, information available at http://www.cnri.reston.va.us/tmp_hp/cstr/cnri-cstr.html, accessed 2 September 2018.
[11] R.E. Kahn and R. Wilensky, A Framework for Distributed Digital Object Services, *International Journal on Digital Libraries* (2006), available at https://www.doi.org/topics/2006_05_02_Kahn_Framework.pdf (First published by the authors May 1995, "A Framework for Distributed Digital Object Services"), http://hdl.handle.net/4263537/5001.
[12] See R.E. Kahn, CNRI Response to draft NIST Blockchain Technology Overview (2018) available at https://csrc.nist.gov/publications/detail/nistir/8202/draft, accessed 2 September 2018.
[13] The notion of a "container" is still quite popular today, see, e.g., Marvin, R., "Containers, Explained (2018), available at https://www.pcmag.com/article/349238/containers-explained.
[14] Managing Access to Digital Information, Cross-Industry Working Team, p. 23 (May 1997), available at http://www.xiwt.org/documents/ManagAccess-1.pdf; see also Lyons, P. A., "Managing Access to Digital Information: Some Basic Terminology Issues", Bulletin of the American Society of Information Science, p. 12 (Dec.-Jan. Issue 1998), available at https://www.cnri.reston.va.us/papers/Managing-Access-to-Digital-Information-Monaco.pdf, accessed 2 September 2018.
[15] As defined in the U.S. Copyright Law, a "computer program" is a set of statements or instructions to be used directly or indirectly in a computer in order to bring about a certain result, 17 U.S.C. sec. 101, available at https://www.copyright.gov/title17/92chap1.html102, accessed September 2, 2018; see also Copyright Office Compendium of Office Practices. Ch. 700, available at https://www.copyright.gov/comp3/chap700/ch700-literary-works.pdf, accessed 2 September 2018.
[16] See, e.g., M. Dworkin, "Recommendation for Block Cipher Modes of Operation", NIST Special Publication 800-38A (2001 ed.), available at https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf, accessed 2 September 2018.
[17] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, (October 2008) available at https://bitcoin.org/bitcoin.pdf, accessed 2 September 2018.
[18] P.A. Lyons and R.E. Kahn, Representing value as digital objects, *Journal on Telecommunications High Technology Law* **5** (2006), 189, available at http://www.jthtl.org/content/articles/V5I1/JTHTLv5i1_KahnLyons.PDF, accessed 2 September 2018.
[19] Authenticating and using Digital Objects, patent application available at http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PG01&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.html&r=1&f=G&l=50&s1=%2220030233570%22.PGNR.&OS=DN/20030233570&RS=DN/20030233570, accessed 2 September 2018.
[20] DO patent, *supra* note 9.
[21] N. Paskin, The Handle System and Identity Management (Geneva, Switzerland; 2007), available at https://www.doi.org/doi_presentations/070207-ITU-Handle.ppt, accessed 2 September 2018.
[22] *Overview of the Digital Object Architecture* (2012), available at http://www.cnri.reston.va.us/papers/OverviewDigitalObjectArchitecture.pdf, accessed 2 September 2018.
[23] Today the DO Registry and DO Repository have been integrated by CNRI in a reference software implementation called **Cordra** https://cordra.org, accessed 2 September 2018.
[24] ITU-T Recommendation X.1255, "Framework for discovery of identity management information", approved on September 4, 2013, available at http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=11951&lang=en, accessed 2 September 2018.

[25] NIST, "Framework for Cyber-Physical Systems", Section B.5.2.1.1, page 100 (see also page 108), Release 1.0 (May 2016), Cyber Physical Systems Public Working Group, available at https://s3.amazonaws.com/nist-sgcps/cpspwg/files/pwgglobal/CPS_PWG_Framework_for_Cyber_Physical_Systems_Release_1_0Final.pdf, accessed 2 September 2018.
[26] Contribution of Corporation for National Research Initiatives, FG-DLT (2018), DLT-I-048, *Definition of "block" as a "digital entity,"* available at http://www.cnri.reston.va.us/documents/DLT-I-048_CNRI_Contribution_FG_DLT.pdf, accessed 2 September 2018.
[27] Outcome Document, FG-DLT (2018), DLT-O-013, *Base document for terms and definitions for DLT*.
[28] R. E. Kahn, The Role of Architecture in Internet Defense, America's Cyber Future: Security and prosperity in the Information Age, Center for a New American Security (CNAS), Volume II, Chapter XII (May 2011), available at http://www.cnri.reston.va.us/papers/CNAS_CyberSecurity_Kahn.pdf, accessed 2 September 2018.
[29] Testimony of Robert E. Kahn, Full Committee Hearing: *Energy Efficiency of Blockchain Similar Technologies*, U.S. Senate Committee on Energy and Natural Resources (8-21-18), available at https://www.energy.senate.gov/public/index.cfm/hearings-and-business-meetings?Id=61CD5B55-EA3E-41F2-BB4B-3EEB7879131F&Statement_id=8805E2F1-D106-49E2-B675-7EDF6227AE4B, accessed 2 September 2018.
[30] P. A. Lyons, End-to-End Principle and the Definition of Internet, Working Group on Internet Governance (Nov. 10, 2004), available at https://www.cnri.reston.va.us/papers/Internet-definition-WGIG.pdf, accessed September 2, 2018; see also "Comments of Corporation for National Research Initiatives (CNRI)", In the Matter of Preserving the Open Internet, FCC GN Docket No. 09-191 (2010), available at https://prodnet.www.neca.org/publicationsdocs/wwpdf/0114cnri.pdf, accessed 2 September 2018.
[31] For description of DOI System, see *DOI Handbook*, available at http://www.doi.org/hb.html.
[32] Information and Documentation—Digital Object Identifier System, ISO 26324:2012, available at https://www.iso.org/standard/43506.html, accessed September 2, 2018.
[33] Dr. Zhou, Jian, *Digital Object Architecture-based Product Quality Safety Information Traceability System in Infant Formula Industry: Architecture, Advantages and* Impacts, Combating Counterfeit and Substandard ICT Devices, ITU (Geneva; November 2014), presentation available at https://www.itu.int/en/ITU-T/C-I/Documents/WSHP/S3-2P1-Zhou-Jian.ppt, accessed 2 September 2018.
[34] P.A. Lyons, Managing information in digital form, Exhibit A, *Information Security Privacy News*, Information Security Committee, ABA Section of Science & Technology Law (2014), available at http://www.cnri.reston.va.us/papers/Info_Sec_and_Privacy_2014.pdf, accessed 2 September 2018.
[35] Entertainment Identifier Registry Association (EIDR), https://eidr.org/about-us/, accessed 2 September 2018.
[36] *ANNA Presents Demo Version of the Derivatives Service Bureau,* https://www.anna-web.org/anna-presents-demo-version-derivatives-service-bureau/, accessed 2 September 2018.
[37] Information on the service is now available at https://www.anna-dsb.com/, accessed 2 September 2018.
[38] For information on the work of ePIC, visit https://www.pidconsortium.eu/, accessed 2 September 2018.
[39] See, e.g., Handle.Net Registry, http://www.handle.net, accessed 2 September 2018.
[40] For information about the DONA Foundation, visit https://www.dona.net, accessed 2 September 2018.