REPRESENTING VALUE AS DIGITAL OBJECTS: A DISCUSSION OF TRANSFERABILITY AND ANONYMITY*

ROBERT E. KAHN & PATRICE A. LYONS**

This article discusses the use of "digital objects" to represent "value" in the network environment. Deeds of trust, mortgages, bills of lading and digital cash can all be represented as digital objects. The notion of "transferable records" structured as digital objects is introduced, along with references to its application in real financial situations. Even in a formal information system, anonymity reflects the desire of a holder of value to remain incognito, except as he or she wishes to be made known. The use of unique, persistent identifiers and a resolution mechanism to fashion such a capability for anonymity and transferability is presented.

I. BACKGROUND

A basic element in commerce is the representation of "value" by a writing, or more generally, a "data structure," fixed in a tangible form such as paper. The use of such instruments is so ubiquitous that they are often taken for granted in daily life. A business will take delivery of a new computer, desk, photocopy machine or some other good and sign a

---

* An earlier version of this article was published in DLib Magazine (May 2001), at http://www.dlib.org/dlib/may01/kahn/05kahn.html.

** Dr. Robert E. Kahn is Chairman, CEO and President of the Corporation for National Research Initiatives (CNRI), which he founded in 1986 after a thirteen year term at the U.S. Defense Advanced Research Projects Agency (DARPA). 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, which he led for the first three years.

Patrice A. Lyons serves as Senior Legal Counsel to CNRI. While serving as a legal officer in the Copyright Division of Unesco (Paris, France; 1971-76), she participated in the preparation of the Convention relating to the distribution of programme-carrying signals transmitted by space satellite; as a Senior Attorney in the Office of General Counsel of the U.S. Copyright Office, Library of Congress (1976-87), she was called upon to assist in the drafting of regulations to implement the cable compulsory licensing system adopted by the U.S. Congress in 1976, and played a lead role in the preparation of the Semiconductor Chip Protection Act of 1984. Ms. Lyons later served as a Partner in the communications law firm of Haley, Bader & Potts (1987-90), and is currently in practice in Washington, D.C. at Law Offices of Patrice Lyons, Chartered.

document acknowledging receipt without a second thought about the validity of the process being used. This is not a recent development. For example, data structures such as "bills of lading" were used in the thirteenth century.[1]

A promise to carry loads of produce to a country fair centuries ago may differ from a promise to perform "operations" on material in digital form to produce a required informational result. Additionally, promises of centuries ago may also differ from a promise to deliver a digital object, embodying a literary or musical work. Even so, the instruments evidencing the contract of carriage, the right to possession of the goods, or the receipt by a customer of the product or service, have basic elements in common. The issue addressed in this paper is whether and how such elements may be appropriately represented in a way that frees the transaction from the need for a physical manifestation, while allowing for both anonymity and transferability.

Representing a transaction in the form of a digital object does not preclude the production of a corresponding physical artifact upon demand. However, whether such artifacts are in fact necessary at all would depend more on the perceived needs of the participants than on the validity and reliability of the underlying mechanisms that can produce it. Transferability is achieved if the data structure may be transferred with authenticity from the party in possession to another party using verifiable techniques. While transferability would require a third-party trusted system to facilitate the transaction, the third-party system would only serve as an intermediary in a technical sense, but would not need to know who the current holder of the object is or maintain any information about the transaction. Anonymity is achieved where the party currently deemed the "holder" of a data structure is not generally known, or cannot be known, without the consent of that party. With such a third-party system in place, each party to a transaction can demonstrate a legitimate claim to the data structure before and then after the transaction has taken place. If an adequate confirmation of legitimate possession after the transaction cannot be made, the second party would normally reject the transaction.

Although a tangible fixation of an object provides a relatively easy means of displaying the data structure representing the intangible "value" being provided, we consider here only the case where the need for such a physical artifact is no longer present. As discussed in a report prepared

1. *See, e.g.*, PAUL HALSALL, MEDIEVAL SOURCEBOOK: BILL OF LADING 1248 (1998), http://www.fordham.edu/halsall/source/1248billoflading.html; SPYROS M. POLEMIS, THE HISTORY OF GREEK SHIPPING, http://www.greece.org/poseidon/work/articles/ polemis_one.html (last visited Oct. 1, 2006) (noting similar mechanisms employed in ancient Greek and Roman times); RULES FOR ELECTRONIC BILLS OF LADING (Comite Mar. Int'l [CMI]), http://www.comitemaritime.org/cmidocs/rulesebla.html (last visited Oct. 1, 2006) (recent effort by the Comité Maritime International to develop Rules for Electronic Bills of Lading).

for the United Nations Commission on International Trade Law (UNCITRAL) Working Group on Electronic Commerce,[2] there have been many attempts over the last few years to replace traditional paper-based bills of lading by electronic messages, and more generally, what was termed the "dematerialization of documents of title," particularly in the transportation industry.[3] It was thought useful to expand such efforts beyond maritime bills of lading to encompass other modes of transportation, as well as issues involving "dematerialized securities."

In the United States, efforts to develop alternatives to paper-based documents have given rise to the concept of a "transferable record." Initially, this work was carried out under the umbrella of the National Conference of Commissioners on Uniform State Laws ("NCCUSL"). Section 16 of the Uniform Electronic Transactions Act ("UETA") was approved and recommended for enactment by NCCUSL in all States in 1999, and sets forth the general parameters of the "transferable record." In essence, this section provides for the creation of "a record created, generated, sent, communicated, received, or stored by electronic means,"[4] i.e., an "electronic record" as defined for purposes of UETA, "which may be controlled by the holder, who in turn may obtain the benefits of holder in due course and good faith purchaser status."[5]

A more restricted definition of a "transferable record" was enacted into law by the U.S. Congress.[6] Title II, sec. 201(a) of what has become known as the ESIGN Act provides that the term "transferable record" is limited to specific types of "electronic records" such as loans secured by real property. As experience is gained in this area, and technical systems and processes are developed to support electronic equivalents of paper-based loan documents, steps may be taken to expand the scope of the law to encompass other representations of "value" in commerce.

The digital object architecture has been under development by Corporation for National Research Initiatives ("CNRI") for a number of years and is currently being implemented in several commercial contexts. This architecture may be of relevance to the evolution of the notion of a transferable record for purposes of the ESIGN Act, as well as the ongoing discussions in the United Nations relating to the transfer of rights in

2. U.N. Comm'n on Int'l Trade Law [UNCITRAL], Working Group on Elec. Commerce, Note by the Secretariat, *Legal Aspects of Electronic Commerce* 2, U.N. Doc. A/CN.9/WG.IV/WP.93 (March 2001), *available at* http://daccessdds.un.org/doc/UNDOC/LTD/V01/812/31/PDF/V0181231.pdf.

3. U.N. Comm'n on Int'l Trade Law [UNCITRAL], *Report of the United Nations Commission on International Trade Law on its Thirty-Fourth Session*, ¶ 288, U.N. Doc. A/56/17 (June 25, 2001).

4. UNIF. ELEC. TRANSACTIONS ACT § 2(7) (1999).

5. *Id.* at § 16.

6. Electronic Signatures in Global and National Commerce Act, Pub. L. No. 106-229, 114 Stat. 464 (codified as amended in scattered sections of 15 U.S.C. and 47 U.S.C.).

tangible goods and other rights.

II. PHYSICAL ARTIFACTS

Many applications involving physical artifacts, such as health records fixed on paper, often raise the notion of an original or authentic copy. In fact, in many cases there may be multiple originals of the same document like a contract that is signed in duplicate originals. In other cases, only one original record may exist, as in bearer bonds or in deeds to real property. For some applications there is no requirement of anonymity. The holder of the original record may be known by any of several means. In other cases, the holder may be completely unknown unless and until he or she produces the physical artifact. This is the case for issued paper money such as a dollar bill. Although the issuer of the official record or document is generally known to the holder and to anyone else who is permitted to inspect it, there can, but need not be, any record of the actual holders in due course of the record over time. Furthermore, it is generally understood that physical artifacts such as paper or other material objects are not required to maintain certain official records. For example, the issuer of an official document may retain a computer record of the issuance. This might be known by any of several terms such as a book entry, or journal entry and the official record is kept by the issuer or a known designated agent of the issuer. The issuer may also maintain a record of the "chain of title" to the entry. Various registries maintain this kind of information, such as a typical Recorder of Deeds, although the actual deed may be retained by others. Still, the prevailing mode of operation is to issue paper for many, if not most, of these applications.

In each of the above cases where only computer records are used, there is usually a trusted party that maintains the records, as well as the linkages between each record and the party to whom the record is currently "attached." Absent the maintenance of accurate records by the trusted party, proof of ownership may be compromised, perhaps fatally. Even though an official computer-based record may be kept by a trusted party, normally the issuing party or its agent, a copy of the record may be available in digital form at other locations. In order for the record to be negotiable, the bearer may be required to provide the record in digital form, but the authenticity of the holder as well as the record can be separately validated if the appropriate records are available.

The discussion below focuses generally on the case where a record of linkages is not kept, and thus, no equivalent "chain of title" is maintained by the trusted party. It also assumes that a generalized record-keeping capability need not be in existence, but that a trusted means of authentication is available. The digital object architecture described generally below can play a key role in facilitating the authentication process.

III. DIGITAL OBJECTS AND THEIR IDENTIFIERS

The term "digital object" is used to denote an identifiable item of structured information in digital form within a network-based computer environment. Generally speaking, a digital object is a set of sequences of bits or elements, each of which constitutes structured data interpretable by a computational facility, at least one of the sequences denoting a unique, persistent identifier for that object. Information of virtually any kind that is represented in digital form may be structured as a digital object. The identifier of a digital object may be of any form, as long as it may unequivocally be de-referenced to the digital object. The Handle System® is an example of such an identifier system.[7] Some known part of the identifier could contain a cryptographic hash or fingerprint of the identified object, which could be used to help to authenticate the object.

The Handle System being developed by CNRI, serves as a "resolution system" and would typically contain "resolution information" sufficient to resolve an identifier to the "location" of the computational facility containing the object. However, the resolution information, nominally state information about the digital object, may not necessarily be publicly available in its entirety. Indeed, portions of the state information may be available only to the party that is the current owner or "holder" of the object. The resolution system is also assumed to be secure from tampering. This is achieved through a combination of mechanisms including the use of public key infrastructure, backup procedures, and protected physical equipment. It need be no less secure than, for example, other parts of an on-line banking system.

The location, if designated in the state information, may be merely the service point for obtaining the digital object. In fact, there may be multiple locations that can produce the digital object, and for informational purposes, any of these will suffice. However, it is assumed that only one of these objects is the official version, and the rest merely replicas. This leads to an important consideration: given the ease by which information can be replicated by computer and on a network, how can the official version be distinguished from the other identical versions?

IV. TRANSFERABILITY OF DIGITAL OBJECTS

In this section, the focus is on the transfer of an authentic version of a record or document in the form of a digital object. We begin by considering how a given digital object accessible on the network can be authenticated as having the proper information from the original issuer and possibly contain additional chain of title information where appropriate. The

7. The Handle System, http://www.handle.net (last visited Sept. 17, 2006).

possibility of encrypting each digital object may indeed be desirable for all of or parts of a digital object, especially where classified information comes into play. However, this capability is not essential to the basic system in which it is only assumed that the digital object is signed by its issuer using a strong encryption mechanism such as the U.S. federal digital signature standard. The authenticity of the digital object can then be verified directly from the digital object and its signature, if the signature can be assured. The use of a trusted public key infrastructure is one, but not the only way to achieve this result.

The Handle System can store digital object signatures to be used for authentication, and even bind the signatures tightly to the identifiers. The digital object will generally contain other information that can be used to show authenticity, but this is not necessarily required. For example, the inclusion of a sequence number, date-time stamp and/or the length in bytes would inhibit attempts to tamper with even weak signatures, or strong signatures made weak over time with increased computer power.

The question of determining which of N authentic digital objects is the original is, in some sense, an epistemological question since there is no way for a computer to know where a party providing bits to it "obtained them." If all instances of a digital object are identical and since bits are themselves fundamentally incorporeal there is really no notion of original bits. For purposes of illustration, four transferability mechanisms are identified below. The first two are equivalent to physical artifacts embodying data structures. The third is a hybrid situation. Only the fourth will be discussed in any detail.

Mechanism one is a tamper-proof device provided by the original issuer that contains the original information. It is assumed that the issuer only issues one such device, that others cannot replicate the device without destroying some critical part of it, and that no means exist to change the original information (although it may be possible to incorporate additional signatures to reflect chain of title). The device thus assumes the role of paper and ink and, for most purposes, can be viewed as equivalent to paper and ink. One transfers the data structure by transferring the physical device. Mechanism two is like mechanism one, in that the above assumptions apply except that the internal information may be read out of the original device and into another device. Assuming a means by which there is no possibility for corrupting the information in the transfer process (e.g., the receiving device will reject corrupted information), this leads to the issue of whether the receiving or sending device can insure that only one such transfer can occur. There may be cases where, in fact multiple transfers might be appropriate, but this possibility is not addressed here. Mechanism three is like mechanism two, except that one of the devices is not tamper proof. This would have to be assumed if one of the devices were a general-purpose computer. The techniques for ad-

dressing mechanism three are essentially the same as those that would be used if all the devices were general-purpose computers; and so we go directly to the fourth case.

V. DISTINGUISHING ORIGINAL INFORMATION ON THE NET

Mechanism four assumes that the original information is structured as a digital object and stored in a general-purpose computer or other computational facility on the net. The notion of "holder" is tied to the notion of unambiguously designating the computational facility that purports to hold the original digital object. For example, a transferable record such as a deed of trust could be the original digital object held at a particular moment in time in such a computational facility (referred to in this paper as the "holder facility"). While recognizing that this is a logical construct, the holder facility may be deemed generally equivalent to the evidentiary role played by a physical object. The evidentiary showing could entail demonstrating how the system works. For example, the showing could identify the particular holder facility as the authorized holder at a particular moment in time and producing the relevant digital object using the system. The identifier uniquely identifies the data structure stored within the designated holder facility. For an individual to claim to be the holder in due course of an electronic record structured as a digital object, the holder facility must be able to present the record to the appropriate party or parties for inspection on demand. It is asserted that only the authorized holder of the original digital object will be able to cause the desired object to be produced by the holder facility (unless, of course, it was trusted for safekeeping with untrustworthy associates). For example, if the holder was untrustworthy, it could present the material to a third party and claim it was holding the digital object on behalf of someone other than the party who is the authorized possessor.

The holder facility must be known to the resolution system, or a means of determining the holder facility must be uniquely derivable from the resolution system. While information about the holder of a transferable record need not be made available to others, the actual holder facility containing the object may also not be known publicly. However, it is mandatory that each holder facility only provide the original digital object to the bearer or his agent and in a form that allows the authenticity of the information to be verified. This can be achieved without the resolution system knowing the identity of the holder. In this case, the agent of the bearer might be a trusted computer system or its operator. A compromise of this trusted system would be equivalent to a loss of say a bearer document. A compromise of the resolution system could also result in a loss of such a document, but the latter compromise must be addressed on a system-wide basis. The former compromise (of a specific

trusted system) would be the responsibility of the bearer that selected it.

Each digital object can be validated by use of its fingerprint or signature, which is maintained by the issuer or its agent. The issuer may also elect to retain a replica of the original object, or only certain archival information about it such as its digital signature, length, date-time stamp of original issue, and possibly other non-personal identification information, such as sequence numbers. A transferable record itself consists of the original digital object and its signature, possibly along with additional information such as chain of title information added each time the object is transferred to another party. Certain elements of the additional information would be necessary for some objects and not for others. For example, bearer bonds would not usually have chain of title information, nor would digital cash. At the time of transfer, an instance of the digital object would be formed in a new holder facility corresponding to the new holder and the system would require that a change in the state information indicating the then valid holder facility be entered into the resolution system.

The Handle System has all the attributes necessary to provide the functionality of a trusted third party system. Specifically, system responses may be "signed" by the system upon request and each signature may be authenticated by a built-in certificate authority, if desired. The built-in certificate authority may itself be certified on a system-wide basis, and the cryptographic strength of the certificate authority increases as its purview widens. For example, the system-wide authority has the longest and strongest key. Each entry into the Handle System requires the use of a private key known only to the owner or its authorized agent. Further, various cross-checks carried out regularly within the system are designed to detect anomalies with respect to replication and mirroring of data. The top level of the Handle System is known as the Global Handle Registry and consists of a number of servers and services managed by a single trusted authority.

Entries in the Handle System for a newly designated holder facility would be made by the authorized holder at the time of transfer; the identifier for the data structure need not change, but the corresponding information in the Handle System would be changed to indicate that the data structure is now accessible from the new holder facility. It is not required that the entire Handle System be trustworthy in order to implement this capability. It is only required that a subset of the system be trusted, namely, a subset separately cordoned off to manage objects of value in which transferability and/or anonymity are needed.

VI. DIGITAL OBJECTS SENT VIA E-MAIL AND/OR AGENTS

Digital objects structured as mobile programs or software "agents"

may serve as their own transport mechanism or be used to transport other digital objects with appropriate access procedures to effect the authorized disseminations. Existing mechanisms such as email may also be used for the same purpose. Specifically, both email and agents may be viewed as ways to move the separately identifiable information contained within them, but these would not be an integral part of the Handle System per se. While in transit, the information may or may not have any status of value until and unless it arrives at its proper destination and is validated. Alternatively, the use of identifiers, such as handles, can obviate the need for an actual data structure to be communicated as the data structure can be retrieved independently if the ability to access it at a remote holder facility is enabled. If desired, a synchronization mechanism, familiar in distributed data base technology, may then be invoked to insure the designated object is moved from one holder facility to another and that only one such facility is the newly designated one. The Handle System can also provide the equivalent of this function. At that point, an email reply could go back to the sender confirming the transaction. For audit purposes, the reply itself could be structured as a digital object with its own unique identifier.

The case of network-based agents is in many ways the more interesting and also more complex topic. In this case, the value represented by a digital object may be present entirely in a mobile context, with the object never stopping at any computational facility for more than a transitory period of time. Interactions involving value transactions may thus take place in arranged meetings and rendezvous situations. Validation of the agents as well as their contained data structures and/or identifiers would be necessary. This could be carried out using the same techniques as for any other type of digital object, whether stationary in a repository or in transit on the net.

This paper does not purport to fully describe, much less specify, an entire system for representing value. There are many other issues remaining to be worked out on the way toward creating a viable system for identifying value based on the notion of a digital object. A starting point down this road would be the development of a general "type framework" for transferable records. The capability for such a mechanism exists in the current implementation of the Handle System. The notion of typed data, inherent in a digital object, is deliberately intended to be an open and extensible attribute of the system. If the digital object architecture were introduced in various areas of commerce, it would be possible to agree on specific "types" that are meaningful for specific subjects or industries. There may be multiple types for representing "value," such as a category called "bill of lading" or "deed of trust." A data structure would be assigned a "type" for purposes of resolution of digital objects that are designated by an issuer as conforming to the particular type. Types may

also be defined dynamically and resolved by the resolution system. Once agreement is reached on the use of "types" in such a system, consideration may be given to identifying possible standard operations allowed to be performed on a given type. For example, where dealing with the type: "transfer of copyright ownership," there may be a permitted operation: deposit for recordation in the Copyright Office.

While various notions concerning "value" and "typed data" require additional study in the network environment, the basic underlying resolution system, already in operation in Internet commerce, may be used directly to resolve typed data and to manifest value. The flexibility of a system based on the notion of a digital object may serve to open new avenues of commerce in a networked environment and contribute efficiencies and cost savings to existing methods of doing business.