Securing Uniqueness of Rights e-Documents: A Deontic Process Perspective

Ronald M. Lee[1,] Vu Nguyen[2] and Anastasia Pagnoni[3]

[1] Florida International University, Department of Decision Sciences, r.lee@fiu.edu
[2] Florida International University, Department of Decision Sciences, vu.nguyen@fiu.edu
[3] Università degli Studi di Milano, Dipartimento di Informatica e Comunicazione
anastasia.pagnoni@unimi.it

Abstract

We typically think of documents as carrying information. However, certain kinds of documents do more than that: they are not only informative but also performative in that they represent rights. When these documents are in paper form or some other physical medium, holding the document indicates holding the right. Since the document represents a right, a hazard is that by duplicating the document, one may fraudulently claim a new right. For this reason, physical documents that represent rights are both tamper resistant and copy resistant. However, problems arise when such performative documents are converted to electronic form: duplicates are bit for bit perfect and undetectable. Thus, the normal heuristic of uniqueness of the document token as representing the uniqueness of the right no longer holds for performative electronic documents. This is especially challenging when the rights are transferable, as with various financial instruments such as stocks and bonds. This paper presents an analysis, based on deontic logic, about the necessary requirements for electronic documents and their corresponding electronic procedures in order to guarantee the uniqueness of rights and prevention of fraud. A design is sketched, based on a notion we call digital parchment, which offers improved flexibility.

Key words: e-Business, Electronic documents, Electronic transactions, Performative, Deontic, Negotiable documents, Bill of lading, International trade procedures, Inter-organizational workflows

1   Introduction

Consider the following situations:

1.   Alex booked online for his travel to a conference. However, his university will not reimburse him unless he provides original receipts.

2.   Barbara has a ticket to the concert on Friday, but cannot go. She gives the ticket to a friend. The friend goes to the concert.

3.   Clive is taking an online course. The exam is also online. He has a friend do the exam for him.

4.   Debra finds a $20 bill on the street. She keeps it.

5.   Edward wants to transfer $10 from his digital wallet to his friend Frank. He cannot.

6.   Grace broke her leg in a ski accident. She has emergency treatment and gets a receipt. She files a claim with her health insurance company. Since she is also covered by her husband's policy, she also files a claim with that insurance company.

All of these examples have aspects involving the transferability of rights and obligations. While certain physical media have evolved to evidence transferability of rights, this continues to be a fundamental challenge for digital media.

This paper examines the basic modeling requirements for transferability of rights, and specific issues for e-business.

A word about what this paper is NOT about. This paper is not about digital rights management (DRM). Digital rights management is concerned with engineered constraints on user functionality to protect digital content from piracy, e.g. via peer to peer (P2P) exchange networks [67]. Thus DRM is about the enforcement of digital content producers' intellectual property (IP) rights. By contrast, this paper is about documentary digital evidence of rights of any kind. These might include IP rights, but we are mainly concerned with other kinds of contractual rights.

This paper is also not attempt to make a contribution about digital security (e.g. [17], [57]). Indeed, we will generally presume that secure digital communications are already in place. Our concerns focus on a subset of communications that are not only informative but also performative. Thus we shall not specifically address aspects such as attribute certifications, or security assertions (e.g. [51]).

1.1   What is a Right?

Like many everyday concepts, the concept of right seems to have a variety of overlapping meanings [73], [22]. When we drive on the freeway, for instance, we have the right of way over merging traffic. Buying a ticket gives us the right to ride the bus. We have the right to vote, the right of free speech, etc. The notion of right is of course central to theories of law, where there is an extensive literature about rights, especially in the philosophy of law. For the present discussion, we will use the definition of right due originally to Hohfeld [27], who described it as the 'correlative' of an obligation. That is, to have a certain right to a certain benefit means that some other party is obligated to realize that benefit for you. This is illustrated in Figure 1.
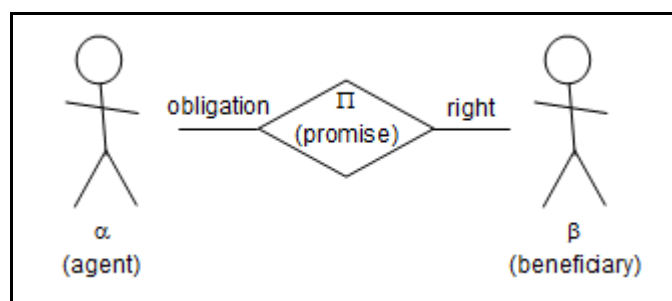

Figure 1: Right as Correlative of Obligation

Thus we are here talking about right to a specific performance. This is different than for instance human rights, which do not entail obligations from specific parties, but rather are more like general protections or liberties. A contract may be characterized as two opposing promises, where the agent of the first promise is the beneficiary of the second,

and vice versa for the second promise [38], [40]. Each of these promises includes an obligation of one party and a right of the other party. For simplicity here, we focus only on single promises, and primarily from the perspective of the beneficiary, as a right.

1.2   Transferability of Rights

An important feature of right is whether or not it permits transferability. Transferability of rights is a fundamental feature of capitalist economies [12]. Here, we are concerned with the mechanisms of how rights are transferred, and how to safeguard against fraud. As we shall elaborate later, the fundamental challenge is that since the right itself is not directly observable, the transfer of rights is accomplished by transferring some kind of physical symbol or indicator that represents the right. For instance, a common kind of indicator of a right is a paper ticket. Paper tickets are used in many kinds of ordinary activities like riding the bus or train, attending a sports event, or even waiting in line at the meat counter. In most cases, the right associated with a ticket is also transferable. That is, I can give my movie ticket to someone else, and that person will gain the right to see the movie. (It is this transferability that enables scalping of tickets before a major sporting event.)

The transferability of rights is typically concerned with changes in the beneficiary role of the promise, since this is the role that receives benefit or value. However, rights may be designed to permit changes in the other roles as well. For instance, when trading in commodities futures, both the agent role and the beneficiary role may change. This is the difference between buying short and buying long.

1.3   Rights as Social Reality

As mentioned earlier, a fundamental challenge of managing rights is that no one can see a right. Thus the content of a right, who owns it, etc, must somehow be made observable to the parties concerned. To elaborate the issues of observability, we find the 'social reality' ontology developed by Searle [59], [61] useful. Searle distinguishes between those aspects of the world that are natural ('brute facts') versus those that are based on human social conventions, which he calls 'institutional facts'. Thus, the sun, the moon, stars, rivers, mountains, even houses, cars (as physical objects) are brute facts. By contrast, governments, corporations, marriages, citizenships, ownerships, licenses, contracts, rights, privileges, duties, obligations, promises, etc. are 'institutional facts'. Such institutional facts are the principal kinds of 'social reality'. (Other kinds of social reality are more informal social norms, such as respect for elders, forms of dress, food preferences, etc.) Unlike physical facts, which can be verified by observation, institutional facts do not have any empirical verification: one cannot 'see' a promise or a right or a privilege. Instead we know about these things by certain kinds of observable indicators or documentary evidence.

Searle characterizes the relationship between observable reality and institutional facts using the formula 'X counts as Y in C', where X is an observable indicator, Y is a (non-observable) institutional fact, and C is a certain conventional context (C). For instance, a certain piece of paper (X) counts as a Euro, official currency (Y) in the European Union (C), or a piece of wood counts as a queen (Y) in a chess game (C). A Euro has the function of 'a legal tender for all debts' that a normal piece of paper does not have. A queen can move horizontally, vertically, or diagonally in chess while other pieces cannot. Institutional facts exist because we collectively agree they exist. In this regard, they are rather like magic or superstition. Like magic, they are brought about by special incantations or rituals. We have all participated in such events like baptisms or weddings. On a grander scale, these include the inaugurations of presidents, or the crowning of royalty. On a more mundane level, these include the signing of contracts or the assignment of student grades.

The kind of event that brings about an institutional fact is called a performative. Because the point is to incorporate social consensus, performatives are communications, addressed to the public whose collective consensus brings them about. Thus, the audience of a wedding is the family and friends who will collectively recognize the marriage. Similarly, the crowning of a king is performed before the aristocracy, nobility, etc. whose collective recognition grants kingship. In all of these performative events, there is one particular moment when the institutional fact is created. This is often done as a spoken declaration called a 'speech act'. For instance, in the wedding ceremony the priest may declare: 'I now pronounce you husband and wife.'

An institutional fact thus is created simply by declaring it, subject to the satisfaction of the contextual conditions, which Searle calls 'constitutive rules'. These are rules that "create the very possibility of certain activities" ([59] p.27), in contrast with 'regulative rules', rules that regulate existing activities. In other words, the creation, existence and cessation of institutional facts are determined by constitutive rules. Examples of constitutive rules are those that define moves in chess or those that determine the formation of a contract.

1.4   Three Realities of Doing Business

The common view of an organizational database is that it represents facts. That is, the entries in the database denote some aspect of the environment. This correspondence is illustrated in Figure 2 as between the 'documentary reality' of the database, and the 'physical reality' of the environment [31]. The correspondence between documentary reality and physical reality is truth functional. For instance, if there is a database entry "Male(John)" – this will be true

Ronald M. Lee
Vu Nguyen
Anastasia Pagnoni

if and only if the entity denoted by "John" is a member of the set of things denoted by "Male". Thus, if there is any doubt, one can go out and check the physical reality to verify if the database entry is true. This is the typical assumption made in the formal denotational semantics for logic [19], [15], which in turn serves as the basis for semantic theories of databases [5].
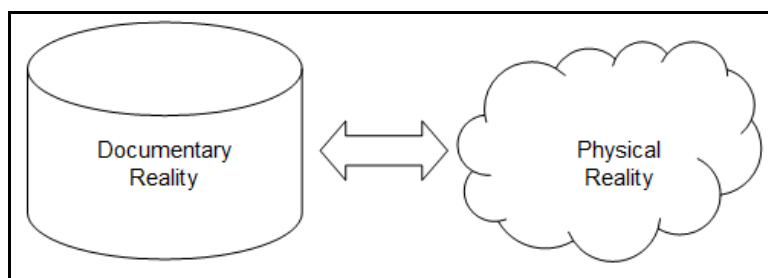

Figure 2: Documentary Reality versus Physical Reality

Our concern here is that many of the facts in a typical business database do not follow this simple logical model. This is because there is no corresponding physical reality to check. Consider these typical entries:

```
Student(John).
Professor(Bill).
Married(John, Sally).
Owns(John, Car123).
```

In each of these cases there are no physical properties to verify. For instance, one cannot do a physical examination of the biological entity named John and determine whether he is a student. The same is true for being a professor, being married, owning a certain thing, and many other kinds of attributes and relationships that represent not physical facts, but rather 'institutional facts' in the sense that they are created by the institution, rather than observations of physical properties [59]. Thus, in these cases, one does not examine physical properties, but rather evidence. But evidence of what? In this paper we will argue that the semantics of many kinds of business data involves a different kind of ontology, which we will call 'deontic reality'. This correspondence is sketched in Figure 3.
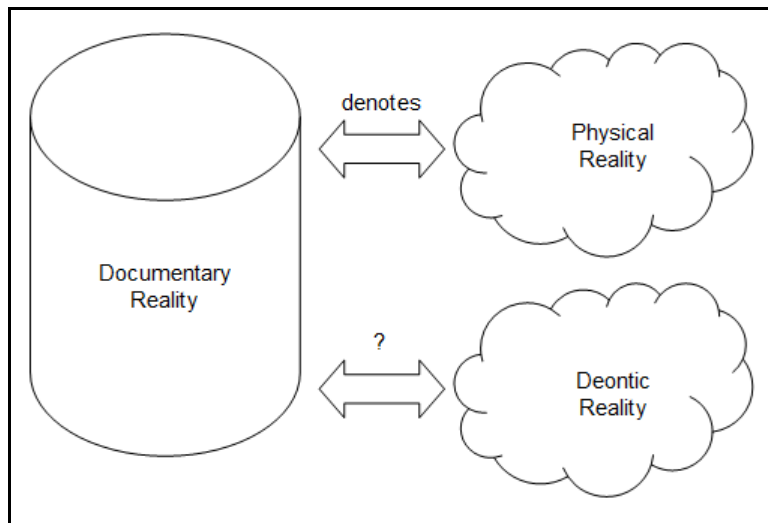

Figure 3: Many Business Facts Refer to Deontic Reality

2   Comparison to Other Work

As will be elaborated below, the focus of this paper is on issues of managing what we call performative documents, specifically those that evidence unique, transferable rights. This focus seems to fall between several established research areas, which we characterize as logic/philosophy; artificial intelligence (AI); and practical / implementational.

2.1   Related Issues in Philosophy and Logic

There are three sub-areas here: deontology and deontic logic; philosophy of law; speech act theory and social reality.

Ronald M. Lee
Vu Nguyen
Anastasia Pagnoni

Deontology and Deontic Logic.
Deontology is broadly concerned with the structure and principles underlying normative systems [2], including morality and ethics. Deontic logic is concerned with deductive reasoning about norms. (Additional background about deontics is provided in the appendix.)

Philosophy of Law.
There is a large amount of literature in the philosophy of law that is potentially relevant. The deontic aspects of law were elaborated in detail by Hohfeld [27], which has become the starting point for much later work. For instance, Hart [22], [23] extends the work of Hohfeld in the philosophy of law.

Speech Act Theory and Social Reality.
Speech act theory encompasses not only speech acts but performatives, illocutionary logic, and theories of social action. A key starting point for this research is the little book by John Austin, How to Do Things With Words [3]. Austin's student, John Searle, refined this into a more elaborate theory of speech acts [58]. This has had wide-ranging impact, including the series of conferences on Language-Action Perspective (LAP) [69]. Searle and Vanderveken formalized the theory of speech acts into what they called illocutionary logic [62].

Later, Searle expanded these theories to a broader theory of social cognition in his book, The Construction of Social Reality [59]. In a later paper [61], he touches on the relevance of deontology to his theory of social/institutional reality, and suggests that it is of central importance. However, he does not elaborate this potential relevance in any detail. In a way, this paper is concerned with this gap. To avoid getting caught up in the ambiguities of what 'Searle really said' – we have chosen to introduce our own term, deontic reality, which is specifically concerned with the deontic aspects of social reality.

Searle would refer to evidentiary documents as 'status indicators'. Also, his colleague Barry Smith has begun to consider an ontology of documents in a presentation [63], which resembles our notion of documentary reality. However, neither Searle nor Smith considers the possibility of inconsistency between deontic reality and documentary reality. For instance, a status indicator might incorrectly represent a right, perhaps with intentions of fraud or deception. Our concern here is with the necessary controls needed in complex societies to manage status indicators of rights.

2.2   AI / E-Business

Deontics has become of increasing interest in computer science research, as suggested by the many papers in the series of annual DEON conferences since 1999 [14]. Deontics is also a prominent theme in the ICAIL Conferences of the International Association for Artificial Intelligence and Law [28]. In this paper, our interest is more the relevance of these themes to business. One particular area where the deontic aspects of law overlap with business is contracting. Lee's dissertation in 1980 was an early effort here [38]. Subsequent research in this area has been called electronic contracting [39], [66]. Steven Kimbrough and colleagues have expanded this scope to what he calls a 'formal language for business communications' (FLBC) [32]. This resulted in the PhD dissertation of Scott Moore [47]. This also includes notions of speech act theory and illocutionary logic [34]. Also, a formal ontology of deontic actions and entities is presented in [40].

This paper is also concerned with formal, business communications, but more from an evidentiary standpoint, rather than a deductive one. That is, here we are not specifically concerned with the propositional content of a particular right (such as the conduct permitted by attending a baseball game). Rather, we are more concerned with the falsification of evidence of rights (e.g. forging baseball tickets). In this paper, we emphasize the mapping from what we call documentary reality to deontic reality. As noted above, this notion is suggested in the writings of Searle about social / institutional reality.

The paper by Jones and Sergot [30] also deals with how rights may be created using institutional performatives. However, they address the institutional pre-conditions for a performative to have effect. Here we are more concerned with the post-conditions, the persistent evidence of a deontic change.

2.3   Practical Applications

This paper is mainly directed towards applications of inter-organizational e-business. This reaches greatest complexity and challenge in applications of international trade.

An international trade transaction can easily involve some 20 different parties and as many as a hundred different documents [74]. Some kinds of document such as bank drafts or negotiable bills of lading embody rights to receive payment or to claim for goods. Such rights are linked to the possession of the documents, and transfer of the rights can be accomplished simply by transferring the possession of the documents [37]. While converting data to electronic form is not problematic, capturing this notion of possession of the physical document is. In this respect, the bill of lading belongs to a special class of commercial documents called negotiable documents. The "law of negotiability permits a piece of paper to embody rights in a separate commercial asset, such as right to receive

payment or to claim for goods in the possession of a bailee" [72]. The negotiability function of a document is indispensable for conducting business between parties located at a distance from each other. It helps traders to liquidate their capital and increase credit circulation by trading the documents of goods while the goods are still in transit. It also help banks to secure the credits and loans provided to traders by holding the documents as valuable collateral. Keeping the documents of goods as collateral is much more convenient and economical than keeping the goods.

A paper document can be designed in a way to make its duplication or alteration detectable. This can be done by traditional measures like signature, stamp and seal, or by more advanced techniques such as hologram, watermark, micro printing, intaglio ink, and color changing inks. In a paper document, securing of the rights against frauds by duplicated or altered evidence is afforded based on the physical attributes of the document itself. Electronic data, on the other hand, can be duplicated identically. When a party transfers an electronic document to another party, he may retain an identical copy that could be used to exercise the right. This makes the application of electronic data to concepts such as possession and transferability more challenging, and the control of holding and transferring of rights can not be done in the same way as in paper-based procedures.

This highlights the practical relevance of the issues addressed in this paper. Particularly in the case of documents that evidence unique rights, the transformation from physical documents to electronic documents also requires a re-design of the associated procedures [8], [49].

3   Fraud Risks

As we have discussed it so far, issues of rights are reducible to the notion of obligation: to have a right is to be the beneficiary of an obligation. Rights in this sense are valuable. Indeed, considering that most kinds of property are actually rights (to land, to home, bank accounts, investments, stocks, bonds), rights are the very essence of economic value. As such, rights require careful protection. But, since rights are ephemeral, what to they need to be protected from? For instance, a physical asset like a car can be stolen. But what would it mean to steal a right? The theft of a right is more commonly known as a fraud. This occurs when some other party falsely assumes the role of beneficiary, and exploits the benefits afforded to that role. Thus, a fraud is a deception that enables illegal economic gain.

3.1   Frauds as Impersonation of Beneficiary

If you look in your wallet you will find numerous performative documents – for instance credit cards, driver's license, insurance card, that serve as indicators (evidence) that you are the beneficiary of certain rights, e.g. to purchase goods on credit, to drive on the road, to make an insurance claim if you are in an accident. A common kind of fraud is that someone obtains one or more of these performative documents and impersonates the beneficiary to illegally exploit their right – for instance, using another's credit card to make purchases.

3.2   Frauds Based on Transferability

Other kinds of frauds exploit the transferability of rights. As noted earlier, rights are normally for a single beneficiary. When the right is transferred, the second party acquires the right, while the first party gives it up. One kind of fraud based on transferability is that the first party somehow manages to retain evidence of the right. A similar form of fraud is that the evidence of the right that is transferred is actually forged.

3.3   Forgeries

A common mechanism to achieve a fraud is based on the simple duplication of a (performative) document, namely forgeries. With the advance of photocopier technologies, now available in color, this kind of fraud has become more popular. For this reason, in the paper world, performative documents are nearly always printed on media that is difficult to modify and duplicate. These typically have special paper and/or raised seals that cannot be easily reproduced. Thus, paper tickets usually have various markings or tactile aspects (raised lettering), to make it easy to distinguish photocopied fakes. Other kinds of performative documents include titles of ownership (land, vehicles), academic diplomas, etc., all of which have special paper, watermarks, embossing, or special seals.

There is rough correspondence between the difficulty of reproduction and the value represented by the ticket: for instance, a paper airline ticket is more difficult to duplicate than a bus ticket. Resistance to duplication has become a fine art in the production of paper currency – to make it as difficult as possible to produce forgeries. The goal of this is to make the indicator of the right unique, so that only one party may possess it at a given time.

Ronald M. Lee
Vu Nguyen
Anastasia Pagnoni

3.4 Detecting Forgeries

The normal condition of a right is that it is exclusive for a single beneficiary. The notion of 'individual' here refers to a legal person rather than being limited to a biological person. Thus, an individual legal person could be a corporation, church, or governmental agency or any other legally recognized agent. In the case of certain contracts such as credit cards, the individual might also include family members.

When one party transfers a right to another by changing the possession of the physical indicator, the second party obtains evidence as the beneficiary of the right, whereas the first party automatically ceases to be the beneficiary. The way the transfer of rights is evidenced also needs to reflect this characteristic. Thus if a successful forgery has occurred, more than one party holds an indicator (sufficient evidence) that they are the beneficiary to the right. Said otherwise, the constraint we would like to enforce is that no two distinct parties can hold indicators as the beneficiaries of the same right:

$$\forall \alpha \forall \beta \forall \Phi \; Right(\Phi) \; \& \; HasEvidence(\alpha, \Phi) \; \& \; HasEvidence(\beta, \Phi) \rightarrow \alpha = \beta$$

This says that if two individuals, α and β have evidence of the same right, they must be the same individual. Paraphrased a bit more intuitively, it cannot be the case that two different individuals have evidence of the same right. Thus, if the right is represented by a unique physical paper document, giving it to someone else means you no longer have it. However, when the right is represented by an e-document, sending the document to someone else does not automatically remove the first party's evidence of the right.

For instance, imagine that tickets to the movies would be sold online. You are sent the ticket via email and print it out. The problem, of course, is that you could print it out multiple times, and take a friend for free. Now, suppose you and your friend go together to the movie theatre and present your two copies of the ticket. Is there a way that the movie theatre could detect the duplication? The key here is being able to identify the uniqueness of the right itself. Since movie theatres tend to have open seating, the right is not uniquely identified by a seat number. Instead, the right might be artificially identified by for instance assigning it a unique identification number. This might simply be a sequence number for a given showing of the movie, up to the capacity of the movie theatre. Thus, two movie tickets with the same sequence number for certain showing of the movie would be a violation of evidence constraint K.

3.5 Frauds Based on Overlapping Rights

Another situation is where the same party is beneficiary to multiple obligations, whose benefits may overlap. This is the case for instance when a person has multiple health insurance policies. A potential fraud is where they may claim reimbursement for the same illness with multiple insurance companies.

Another variation is where one might duplicate a performative document (such as receipt) to make claims on multiple agents. This is why universities, for instance, may require original receipts. They want to avoid the possibility that a faculty member might get reimbursed multiple times from different funds.

4 Dynamics of Rights

4.1 Rights Created by Speech Acts

Rights, at least the specific kinds of rights discussed here, are formed as the result of a certain kind of symbolic action known as a 'linguistic performative' [3] or a 'speech act' [58]. The relevance of performative communications to information systems and e-business is discussed in [33], [34], [41]. The typical example is the proclamation "I now pronounce you husband and wife" when spoken by a priest during a special kind of ceremony. Such performative statements differ from informative ones in that the latter are either true or false, whereas performatives, if successful, actually *make* their statement true. Performatives succeed based on the satisfaction of pre-conditions. In the marriage example, pre-conditions include the priest being ordained, the bride and groom each being unmarried, willing, of sufficient age, etc.

4.2 Persistent Evidence of Deontic States

A key issue for the digital management of rights is this: deontic states -- institutional facts, including rights, obligations, prohibitions, etc. -- are brought about by (successful) speech acts, which are momentary events. But the relevance of the deontic state is its persistence. (This is what distinguishes a marriage from a one night stand, for instance.)

Ronald M. Lee
Vu Nguyen
Anastasia Pagnoni

4.2.1 Persistent Evidence of Spoken Performatives

When performatives are merely spoken utterances, evidence of the persistence of the new deontic status resides in the memories of the witnesses of the utterance. Thus, in pre-literate societies, it is important to make changes in social status memorable to the entire group by means of an elaborate ceremony. Thus, for instance, rites of passage, such as the transition to adulthood, involve elaborate rituals and festivities in nearly all cultures [35].

The importance of ceremonies tends to diminish as the society becomes literate and social status is recorded in public records. For instance, modern students often skip their university graduation ceremonies. Indeed, as education drifts more towards fully online e-learning, we might expect the physical ceremony to disappear altogether. Nonetheless, even in modern societies, we still like to celebrate changes in social status that directly affects the family, such as baptisms, marriages, and funerals. Also, it might be noted, that the more socially important the change, the bigger the audience and the bigger the ceremony. Examples are the crowning of royalty and the inauguration of presidents.

Pre-literate societies also used ceremonies to record other kinds of social changes, such as transfers of land ownership. Ronald Stamper (personal conversation) relates a graphic example of achieving persistent social memory of a performative event, as the procedure for land transfer known as 'foeffment' in parts of England in medieval times, when most villagers were illiterate. All the villagers, including children, were called to witness the event. The seller took some soil from the land and placed it in the hands of the buyer. Meanwhile, the parents took sticks and brutally beat their children. The purpose of this is apparently to indelibly record the land transfer event in the memories of the children, as a kind of persistent social memory [64].

4.2.2 Persistent Evidence of Written Performatives

Despite the term 'speech acts', most performatives in business are not actually spoken, but are rather communicated in some kind of written medium. A commonplace example is the signing of a contract. The signed contract document actually serves a dual function of performative communication and performative record. Whereas a spoken utterance is momentary, and preserved only in the memories of the parties and witnesses, a written performative serves as recorded evidence, even to other parties that were not actually present at the performative event.

4.2.3 Persistent Evidence of Digital Performatives

Unlike communications on a paper medium, digital communications do not automatically create a persistent record. While it is true that both sender and receiver may keep copies of the communication, this is an optional step on each of their parts. However, using various kinds of digital security protocols, certain features of the paper communication can be achieved, and even improved. The main feature that concerns us here is the linking of a performative digital communication (C) and its persistent digital record (R). Assuming that X is the sender and Y is the recipient, security protocols can assure the following:

- Authenticity – that X sent the message, C.

- Non-repudiation – that X cannot deny having sent the message, C.

- Integrity – that the message C that Y received is the same that X sent.

- Confidentiality – that no one else except X and Y could read the content of message C.

Furthermore, the same security protocols can be used to ensure that record R is an accurate recording of communication C. However, the security protocols do not provide any controls on exclusivity – for instance to control against X making the same performative communication to another party.

4.3 Transferability as Chain of Role Assignments

As noted earlier, whether or not a particular right is transferable, depends on the terms and conditions of the right. Typically, if the right is transferable, this may be done at the discretion of the beneficiary. However, again depending on the terms of the right, other conditions may apply. Indeed, a third party may have discretion to re-assign the beneficiary role of a right. (This is the case for wills for example)

Also as noted earlier, other roles of the right may change, depending on the terms of the right. Whatever the situation, the change in role in a right is a kind of deontic change. As such, it is accomplished by some sort of speech act, conforming to certain specified conditions. Considered more abstractly, the transferability of a right requires that its terms include a procedure to determine the beneficiary (or whatever other role) at a given time, particularly at the time when the right is exercised. This procedure would identify the end result of a chain of (successful) speech acts of rights transfers.

4.3.1 Coat Check Example

Bringing this discussion down to earth a bit, consider the familiar case of a coat check, for instance in a museum. You leave off your coat at the coat-check counter, and receive a numbered plastic token or 'chit'. The number on the chit corresponds to the number on the hanger where the clerk hangs your coat. When you later wish to retrieve your coat, you present the chit and receive your coat. This is a simple example of a transferable right. You may for instance give the chit to a friend, and the friend can then retrieve your coat. If your friend gives the chit to another friend, then that person can also retrieve your coat. Indeed, if you lose the chit, whoever finds it can also retrieve the coat. The procedure of the right to retrieve the coat is that who ever possesses the chit, gets the coat. The chit is the indicator of the right of coat retrieval.

The fact that a lost or stolen chit is sufficient to retrieve the coat is a control weakness of this procedure. Ideally, it should only be retrievable via a sequence of authorized transfers (successful performatives) of the right. However, the overhead of such added controls is usually not worth the effort. There is not a great incentive to fraudulently obtain coats from coat checks.

4.3.2 How Physical Tokens Model Exclusivity

Simple as it is, the coat check procedure is a model of exclusivity. This is a property of possession of physical objects – only one person can possess it at a time. (Witness children fighting over a toy) Thus in transferring the chit from one person to another, the first party no longer has the chit. Since the chit is indicator of right to retrieve the coat, the first party also no longer has the right to retrieve the coat. Assuming it is a big museum and the clerks have no memory of who left which coat, how is a clerk to ascertain if the chit has been obtained legally? One approach is to invoke a certain kind of defeasible reasoning. The chit is considered sufficient evidence of the right to the coat if no one has reported the chit lost or stolen. In that case, a dispute is reported between the person reporting the chit lost and the person now in possession of the chit. A separate procedure of dispute resolution is then applied (e.g. does the coat fit, etc.)

While disputes over checked coats may seem rather trivial, it is easy to scale up the example. For instance, valet parking is a close analogue – one can steal a car using a stolen valet ticket. Another example might be an anonymous Swiss bank account.

5 Controlling Frauds of Rights

5.1 Closed World Requirement

Earlier it was observed that a fraud can be achieved by a non-destructive transfer of documentary evidence for a right. For instance, party A may have a certain obligation to party B to bring about some state of affairs, call it Φ.
Party B transfers their right to the benefits of Φ to party C by sending a digital document to Party C. However, sending a document digitally is normally not a destructive transfer, so that Party B continues to have evidence of the right. The constraint we would like to enforce is the following:

$$\forall \Phi\, \iota x HasEvidence(x, \Phi)$$

Or, equivalently, expanding the definition of the iota quantifier [43], ι :

$$\forall \Phi \forall x \forall y HasEvidence(x, \Phi)\, \&\, HasEvidence(y, \Phi) \rightarrow x = y$$

Basically, this is saying that for a given right, there may not be any duplication of evidence for holding that right. However, checking for duplicates entails an assumption that the entire collection of evidence for a certain class of rights can be identified. This is analogous to the so-called 'closed world assumption' common in AI applications [53]. This assumption is essentially the difference between 'not knowing' and 'knowing not'. In the open world case, if a certain fact is not provable, then one can only conclude "I don't know". On the other hand, in the closed world case, if a fact is not provable, then one infers it is false.

Note: the right, Φ, is represented here as if it were a first order individual. Depending on the intended application, representation of the internal deontic structure of the right might involve deontic and intensional operators, as discussed in [40]. For a readable introduction to intensional logic, see [21].

5.2 Prima Facie versus Conclusive Documentary Evidence

Closely related to the closed world assumption is the notion of conclusive versus prima facie evidence. Legal texts distinguish between prima facie evidence and conclusive evidence [10]. Prima facie evidence is evidence that establishes the truth of fact if it is uncontested. An example of prima facie evidence in trade is a quotation that evidences an offer, or a carrier receipt that evidences goods were received by the carrier. Conclusive evidence, on

Ronald M. Lee
Vu Nguyen
Anastasia Pagnoni

the other hand, is evidence that establishes the truth of fact which cannot be contradicted by any other evidence. In other words, any proof of the contrary is not permissible. A typical example of conclusive evidence in trade is the negotiable bill of lading. International conventions recognize the bill of lading as conclusive evidence of rights to take possession of the transported goods. When a bill of lading is transferred to a third party in good faith, this third party has the right to take possession of the goods and any proof of the contrary is not admissible [16].

For instance, a negotiable right to possession of goods in transit defines the functionality of a negotiable bill of lading, and a privilege to export a certain commodity defines the functionality of an exporting license.

In paper-based procedures, when the exporter delivers the goods to the carrier, the carrier issues a document namely the bill of lading. According to international conventions, the bill of lading is conclusive evidence of rights. Any person who legally possesses the bill of lading is the person who owns the goods, and a transfer of the right to goods is done simply by transferring the possession of the bill of lading. As mentioned earlier, the uniqueness of a paper document can be afforded by its physical attributes. By handling over the bill of lading to another, one no longer holds the document.

Moving to an electronic environment, the problem is that a digital document can be duplicated bit for bit, so that copies are indistinguishable from the original. After transferring the electronic bill of lading to another party, the transferring party may still retain an identical copy which could be used to claim possession of the goods.

5.3 Registry Models

5.3.1 Registries for Institutional Facts

A registry is a repository for a certain kind of institutional fact. Examples include registries of land ownership; ownership of vehicles; residence in a city or locale; voting privileges; social welfare benefits ('social security' in the USA). A key feature of a registry is that it is 'conclusive' or determinative of the institutional facts that it records. That is to say, the registry entry is sufficient evidence – what the registry record says, is the case. Since it records institutional facts, such as ownership, there is no externally verifiable physical reality. Thus the registry determines the fact – it cannot be wrong.

Registries are defined by a file of records, which may be either paper or electronic, and a rigorous procedure that controls how updates to these records are made.

Consider the example of a land registry, which determines who owns what land in a certain region. Land ownership is a kind of institutional fact, determined by the legal system of the country. Thus, if the legal system for some reason collapses, as is the case in some revolutions, the rules of ownership may change.

However, some other kinds of registries may record physical facts. An example is a birth registry. Consider, what does a registry of births actually do? The general procedure is that the doctor (perhaps midwife) in charge of the delivery signs a document that a child has been born to a certain mother at a certain date and time in a certain location. The birth mother (and father) also sign the form and provide a name for the baby. This form is filed with the governmental department that maintains the birth records. This procedure may vary from one country to the next, but this is its essential logic. Conceivably, such a registry could be wrong – perhaps no baby was born at all. Or, more likely, perhaps a baby was born, and it was not recorded in the registry.

In what sense does a birth registry determine an institutional fact? The birth certificate only certifies that a birth occurred at certain time, date, and place [48]. As such, it is not reliable evidence of identity, even though it is often mis-used for that purpose, especially in identity fraud scams [24]. So, if a person's identity is not the purpose of a birth certificate, what is? The answer is that the fact determined by the birth registry is not the existence of the physical person, but the *legal person*. Consider the case of a baby born but not recorded in the birth registry. In most countries, the birth record evidences citizenship. Without this baby is effectively 'stateless'. All the other affordances of the country's legal system, e.g. voting, welfare, taxation – would also not be available to this baby.

Imagine the reverse – that a birth record was somehow created, with no physical birth. This is the ideal circumstance for an identity fraud – a false legal person, who can accumulate debts, etc, with no risk of liability or punishment.

As the registry of births reflects the creation of legal person, the registry of deaths determines the termination of that legal person. However, in certain places, the registry of births is not directly linked with the registry of deaths. This gap is in fact exploited as a means of identity fraud. The crook searches for a baby born about the same time who died early in life. If that crook is able to obtain the birth certificate for that baby, he/she may obtain various other identity documents, credit cards, etc for that fictional legal person, which can be exploited to various illegal purposes.

5.3.2 Registries for Rights

Our interest here is registries of unique rights between two parties, agent and beneficiary. The special challenge for such a registry is to enable transferability of rights.

Ronald M. Lee
Vu Nguyen
Anastasia Pagnoni

A familiar kind of registry for rights is a land registry, also called a cadastre. This is a comprehensive registration of all real property within a country or region within a country such as a state, county, or municipality. It specifies the location of the property and the extent of its boundaries, established by survey. It also specifies the current owner(s), and usually all prior owners as well. Typically, the land registry is determinative of the institutional fact of land ownership. That is, whoever the land registry says is the owner, is in fact the owner, despite alternative evidence to the contrary.

5.4   Centralized versus Distributed Registries

The typical notion of a registry concentrates all the relevant records in a single place. We call this a centralized registry. For instance, land registries are typically centralized. However, in large countries like the USA, there may be separate land registries for various regions within the country. Thus the registry would be hierarchical in organization.

By contrast, a distributed registry would allow parts of the registry to be distributed across various repositories – some of which may in fact be portable, as with smart cards.

A challenge for all kinds of registries, but especially for distributed registries, is to enforce the aforementioned closed world assumption. Thus, it must be possible to exhaustively search the registry. If a certain entry is not found, the closed world assumption permits the conclusion that it is NOT TRUE.

To illustrate the differences between central versus distributed registries, we now present two example registry models, one central, the other distributed. These two cases are designs for the management of electronic bills of lading.

5.4.1   Background: Bill of Lading

As everyone knows, the term EDI abbreviates 'electronic data interchange'. We believe it ought to abbreviate 'electronic document interchange'. As we have argued throughout this paper, a document is more than the data it contains -- it also has performative effect. This is what gives the bits in certain documents value.

A persuasive example of this is the negotiable bill of lading (BOL). The data in a bill of lading is similar to a sales order, or a packing receipt. However, the significance of a bill of lading is quite different. The bill of lading is issued by the carrier to the shipper (party sending the goods) as evidence of dispatch of the goods. The bill of lading may be non-negotiable, indicating that the named party is the one and only recipient for the goods. Alternatively, the bill of lading may be negotiable, indicating that the recipient ('consignee') may change during transit. It is this negotiable version of the bill of lading that provides an interesting challenge for electronic documents [16], [29].

The law of international trade recognizes the negotiable bill of lading as the document evidencing the right to take possession of the goods -- thus functioning very much like document of title -- and transfer of the bill of lading operates as a transfer of the right to receive the goods. By holding the bill of lading, a party also has the right of control over the goods, including right to instruct the carrier to stop the goods in transit or to re-route the shipment. However, the carrier may refuse to comply with these instructions if they interfere with the carrier's operations.

5.4.2   Example: BOLERO

"Bolero is a smooth, sophisticated, sentimental love dance"
[http://www.salsasite.com/dances/bolero.htm]

"Bolero is a neutral secure platform enabling paperless trading between buyers, sellers, and their logistics service and bank partners."
[www.bolero.net]

The business model for Bolero, Inc. is based on providing a reliable and trustworthy version of the negotiable electronic bill of lading (BOL), using a central registry. The company was formed in 1998, as an outgrowth of a project originally sponsored by the European Union called TEDIS. With Bolero, bills of lading are stored in an electronic registry that is accessible online via the Internet as a web-based facility. Bolero is thus a prime example of the centralized registry model for managing electronic documents of rights. According to the Bolero website [7], the advantages they claim over paper bills of lading include:

- speed -- much faster than paper bills of lading

- cost -- eliminates paper-related costs of couriers, etc.

- efficiency -- electronic bills of lading are logged and tracked automatically; since BOL data is updated to a database, transcription and other data errors are avoided.

Ronald M. Lee
Vu Nguyen
Anastasia Pagnoni

As might be expected, Bolero incorporates elaborate precautions to ensure that all transfers of bills of lading are done strictly via established, legally-recognized procedures [6]. Indeed, Bolero's principal asset is its set of business rules, called the Bolero Rulebook, which all Bolero members must agree to obey, as part of their user agreement. The Bolero website describes their Rulebook as follows:

> "The Rulebook is a multi-lateral contract that binds each User to every other user in relation to their use of the Bolero service. The purpose of this contract, which is at the core of the Trusted Trade Platform (TTP) structure, is to ensure that every User agrees to be governed by a common set of rules enshrining the key elements of the Bolero service. For example, that Users agree, as between each other, that electronic communications will be treated as valid, that no User will deny that it sent a message bearing its digital signature and that messages so signed will bind the User (the company).

> In addition, the Rulebook provides the legal rules that underpin the system for the ability to transact electronic Bills of Lading (Bolero Bills of Lading) through an application that mirrors the rights and obligations of those Users in relation to the international carriage of goods (Importers and Exporters, banks, carriers, forwarders and other intermediaries).

> The Rulebook also includes detailed Operating Procedures and a few Operational Rules involving precise and technical points of user-to-user operations."

5.4.3   Example: EDIBOL

EDIBOL was a project sponsored by the European Union in the late 1990's. This project also investigated solutions for an electronic version of the negotiable bill of lading. One of the authors (Lee) participated in this project [9]. Indeed, EDIBOL was a competitor project to the aforementioned BOLERO, though in end did not achieve practical success. We present it here as an alternative architecture for managing rights documents via a distributed registry.

The solution proposed in EDIBOL was essentially a distributed registry solution. The idea was that a bill of lading would be digitally stored on a special kind of 'BOL-smartcard'. To transfer the bill of lading to someone else, they would also have such a BOL-smartcard. By means of a special encryption protocol, the digital bill of lading could be transferred over the Internet to the other smart card. The critical functionality of the system was the following point: at the end of the transfer, the digital record of the bill of lading of the sending smartcard would be automatically erased.

A somewhat more robust variation was that the BOL smartcard would have a write once read many (WORM) memory. With such a WORM memory, records can be written onto the smartcard memory, but not altered or erased. Thus, instead of the digitized bill of lading being erased, it would be cancelled by a subsequent cancellation record appended to it. In principle, this model seemed to satisfy the closure conditions mentioned previously. In essence, the set of all BOL-smartcards constituted a distributed repository. On the other hand, whereas in single, centralized repository, it is possible to check the entire repository to see that there are no duplications. In the case of smartcards which are not always online -- in fact, not usually online -- it was not possible to check for duplicates.

Nonetheless, the proposing manufacturer insisted that the automatic erasure after sending would be completely reliable, so that duplicates could not arise. Indeed, smartcards are in common use as digital coin purses, which work on exactly this principle. However, there was a further objection that finally killed the idea for a BOL-smartcard. The amount of money carried in a digital coin purse is fairly small. By contrast, the value of a single bill of lading may be millions of dollars or euros.

Why should this make a difference? Because, for that amount of money, it becomes worthwhile for a fraudster to manufacture a cloned BOL-smartcard that did _not_ automatically erase on sending the bill of lading. In that case, the fraudster could sell the bill of lading multiple times to various parties. Of course this would eventually be detected on delivery of the goods, but by then the fraudster would presumably have vanished.

5.5   Application to Frauds Based on Duplication

5.5.1   E-Tickets

An electronic ticket, or e-ticket, is the paradigm example of a unique right evidenced electronically. An e-ticket is usually for attendance at some social or entertainment event, or some other personalized service such as a train or air travel. Indeed, it was the airline industry that was the first to innovate the notion of an e-ticket. The first e-ticket was issued by Northwest airlines on 1 February 1996 for flights between Minneapolis and Chicago. In the remainder of this section we will use airline e-tickets as our primary source of examples.

An e-ticket has numerous advantages. A major advantage is that e-tickets permit purchases online, without the need to issue a performative paper ticket, on official ticket paper. This is a tremendous simplification of customer logistics – customers no longer need to physically go to the travel agent or airline office to purchase their ticket.

Ronald M. Lee
Vu Nguyen
Anastasia Pagnoni

Another significant advantage is to avoid the complications of lost tickets. With performative paper tickets, when the official paper version is lost, so is the right it evidences. The recovery process in these cases can be quite complicated. The service providing company needs to verify that no one else has claimed the right in question.
In the case of a lost airline ticket, the procedure typically requires that the client purchase a new ticket, and then claim reimbursement for the lost ticket after the flight has been made. In the case of an e-ticket, there is no physical token to be lost, thus the entire issue of lost tickets is avoided. One merely needs to present identification in order to exercise the right evidenced by the ticket. Indeed, use of e-tickets by airlines is sometimes called "ticketless travel".

On the other hand, there are certain situations where the old paper version of the ticket has advantages over the e-ticket. As mentioned earlier, a physical token used to represent a right is especially useful for negotiability. This also applies in the case of e-tickets for airlines. However, even paper-based airline tickets airline tickets have the traveler's name on them, and so are not readily transferrable to another person. Nevertheless, paper-based airline tickets may be transferable to another airline. This is especially useful when the original airline has a mechanical problem or some other airline-specific problem. (In the case of weather problems, all the airlines will be equally delayed.) As noted by About.com Air Travel [1],

> "If you have a paper ticket on a major airline and are flying out of an airport where another major airline also flies to your destination, having a paper ticket can serve to your advantage. If your flight is canceled, you can ask an agent at another airline whether they will accept your ticket… Often the other airline will, and you are now ahead of those on electronic tickets. You see, with an electronic ticket, because you do not have a physical ticket, you are more at the mercy of the airline you are booked on. And in the case of a non- weather related cancellation, you will be put on the next available flight on that same airline, even if it is hours later."

This article goes on to point out that transferring tickets to another airline is more easily done with domestic flights than with international flights. In the domestic case, the airlines have very similar rules, which make substitutability easier.

One description (Site 2) of an e-ticket says that electronic ticket is an "airline ticket in the form of a computer entry. An electronic ticket, or e-ticket, is supposed to function like an actual paper ticket by reserving you a space on a flight; all you need to do is give an identification number and show an ID at the airport. But you should also bring the written receipt sent by the airline in the event the airline's computer system has crashed or the airline has lost your reservation."

This quote raises the issue of the fallibility of e-ticket databases. Beyond technical failure, one might also consider the possibility of fraudulent abuse. In the case of air travel, airline companies are typically regarded as stable and reliable. Most clients do not consider that the airline might try to cheat them by denying the existence of their e-ticket. However, as the quote above indicates, computer failures do sometimes occur, and data may even be lost. There may also be cases of the airline databases being hacked and e-ticket data destroyed or altered. In the case of airlines, the probability of this happening is considered low compared to the convenience of the e-ticket. In fact, in the airline industry, e-tickets are now nearly universal. Indeed, the International Air Transport Association (IATA) Electronic Ticketing project (Site 1) has as its stated goal, "100% implementation of e-ticketing worldwide by May 31, 2008."

But what is of applicability of e-tickets to other forms of business? As noted earlier, e-tickets are also becoming more common for entertainment and sporting events. Yet – these seem to be mainly in use by large scale enterprises. But how about for small businesses, who may not have the resources to support their own e-ticket databases reliably? One might expect a third party industry to emerge to provide e-ticket capabilities for client firms. As yet, this market niche appears to be empty.

In the earlier discussion of the EDIBOL project, the idea was entertained about transferring bills of lading, which function as evidence of rights, among smart-cards. This idea was not adopted, partly because of the high value amounts represented by bills of lading, could produce sufficient incentives for the complete fabrication of phony smart cards. But how about using smart cards for the exchange of rights documents which represent smaller value amounts? This idea has indeed been proposed by Kuramitsu et al [36] in what they call a "Ticket Transfer Protocol (TTP)". The purpose of this protocol is to enable transfer of e-tickets among personal tamper-proof devices.

5.5.2   E-Receipts

In market economies, it is commonplace to give a paper receipt in return for the payment of a purchase. This is especially true if the purchase is in cash. In the USA, when paying with a personal check, the returned check can also function as a receipt that evidences the payment.

Why should receipts matter? The original purpose of a receipt was as payment evidence in case there was a dispute. However, another important function of receipts is in situations of reimbursement. In these contexts, the receipt has value as the right to be reimbursed in the indicated amount. Likewise, receipts may also have value as rights for certain tax deductions, e.g. as business expenses.

Since they can evidence rights, it becomes important to control that receipts are not faked or duplicated in multiple claims. Thus, reimbursement procedures typically verify if the receipts are original. But what happens when the purchase was made online? We typically get a receipt, but it is digital. We can print it out, but that does not qualify it as an 'original'.

A common practice in these cases is to require a printout of the credit card statement or bank statement that indicates the payment. A current shortcoming of this procedure is that, unlike the paper receipt, the credit card statement may not provide full detail about what the purchase was for. As online purchases become more common, it is likely that receipt function will become a more important aspect of credit card services and other online payment services like Paypal.

5.5.3 Duplicate Insurance Claims

The other kind of fraud we mentioned is where the beneficiary duplicates a receipt to make multiple claims, each to a different insurance company where he/she has a policy. (Another variant is where each spouse has coverage for the other under their respective health insurance policies, with different companies.)

Obviously, no single insurance company can solve this problem on their own. Somehow, the scope of potential insurance claims needs to be brought under a unified purview (closed world requirement). One way would be to have all insurance claims reported to a single trusted third party for the industry.

Another way, at least for health insurance claims, is to enlist the various clinics and hospitals as a kind of distributed trusted third party. They send claims directly to the insurance company, and enforce the rule of claiming only to a single insurance company.

6 Proposal for a New Performative Medium

6.1 Why Invent a New Medium?

We want to illustrate that other technological alternatives might become available, hence motivating continuing use of the deontic and security validation methodology proposed here. In this section we sketch a possible new alternative, which we call 'digital parchment'.

During our discussions in the earlier EDIBOL project, we eventually asked ourselves the question: suppose we develop a smart-card solution for the electronic bill of lading that is 100% secure. Would traders actually use it? The answer was not obvious. For instance, we were troubled by the outcome of another e-bol solution known as SeaDocs developed in the 1980's by the Association of Tanker Owners (INTERTANKO) and the Chase Manhattan Bank [13], [74]. SeaDocs was efficient and technically sound, yet it failed for lack of acceptance by the traders and banks. A reason given was that traders did not trust Chase Manhattan Bank having control (hence access) of their confidential trade documents. Another reason given was that banks did not have sufficient confidence in 'dematerialized' negotiable bills of lading as evidencing ownership, and resorted to verifying communications with both the carrier and the endorsee [13].

True, in our smart-card solution, the trader could print out the BOL at any time and see and hold it. But what he/she would hold in their hands would not be the performative version of the BOL, only a copy. The performative version would be what is recorded in the smart card. If there would be a difference between the paper version and the internal version on the smart card, it would be the latter version that would count legally. In this important sense, traders could feel a loss of control they might consider unacceptable.

This is what led us to entertain the notion we came to call 'digital parchment'. The requirements of this new medium would be combine the communication efficiencies of electronic media with the intuitive trust that traders had in physical paper documents. We enumerated the requirements as follows:

- operates over distance (digital, programmed)

- individual control (like paper, smart card)

- intuitive, verifiable by user (not a black box)

- presentable to court (readable by judge)

Addressing these criteria, we propose the notion we call *digital parchment*.

In ancient times, parchment was made of thin, flattened animal skins, typically calf, sheep or goat. Indeed, it was quite expensive but also durable, so it was often erased and reused for different recording purposes. In modern

Ronald M. Lee
Vu Nguyen
Anastasia Pagnoni

times, the word 'parchment' has taken on certain performative associations. For instance, a university diploma is sometimes referred to as a parchment. It is these latter associations that we build on here.

Like real parchment, our notion of digital parchment is durable, portable, and readable to the holder. Also like real parchment, it has a uniqueness to it that would be difficult to photo-duplicate. Whereas real parchment was sometimes erased, digital parchment would not permit erasures. (In this respect, comparison to stone or clay tablets might have been more apt.) Additional features of digital parchment include the following:

- it looks like plastic covered paper -- e.g. like a coated driver's license;

- it is written with MICR (magnetic ink character recognition) or OCR (optical character recognition) font;

- any party holding the digital parchment can read the text directly, without any mechanical aids, but cannot write on it (because of the plastic covering, for ordinary ink; and because of encrypted hash code checks, for electronic inscriptions);

- it can be written using a special computer-device (like a heat-sensitive fax), but it cannot be erased (archival, write-once memory);

- the lines of the digital parchment may have bar codes (as hash check).

As noted, a special read/write device will be needed, to write and verify (detect fraudulent changes) of digital parchment; this device will work something like a fax machine (?) with computer interface that can:

- read an existing parchment

- write new lines

- be transmitted digitally, e.g. over Internet, using digital signatures (for authentication), and maybe encryption (for privacy), with a smart-card like handshake protocol, to ensure the integrity of the transfer (including that a cancellation record is placed on the sending parchment).

Summarizing, traders cannot directly modify the digital parchment BOL document by writing on it. The BOL can only be modified by adding to its log, not erasing, and this may only be done via an electronic device that writes the specialized (MICR or OCR) text. Nonetheless, the printed version that traders hold in their hands is performative: this printed form is the official version.

6.2   Negotiability Using Digital Parchment

Trading using digital parchment involves a logic similar to that for smart cards, except that the BOL record is not erased, but rather *canceled*. Thus, digital parchment is a private registry solution that uses "archive" or "write-once" memory. (Write-once memory might also be used by smart-cards as well.) However, it is an essential assumption of the digital parchment solution that each local registry uses an archive memory that cannot be deleted or altered once written. The added feature of digital parchment is that what is written is not only readable by computer, but also directly by a person. Thus, these will have the same structure as for smart-card, except that databases are write-once only.

Each trading party requests a "DOC carrier" digital parchment, e.g. from registration authority. The DOC Carrier digital parchment is stamped with the trader's public key (either at top, or on each line). To transfer a (BOL) document, seller and buyer make a synchronous, digital connection; using some secure hand-shake protocol, which simultaneously:

- writes an arrival record to the receiving (buyer's) doc-carrier digital parchment, e.g. a message like "Received BOL #XXX"

- writes a cancellation record to the sending (seller's) doc-carrier digital parchment, e.g. a message like "Canceled BOL #XXX

Thus, a party owns the BOL if there is an arrival record but no cancellation record on his/her DOC-Carrier digital parchment.

6.3   Digital Parchment Pros and Cons

Advantages of digital parchment as a BOL doc-carrier include:

Ronald M. Lee
Vu Nguyen
Anastasia Pagnoni

- ▪ intuitively similar to paper, only that it must be written by a special device;

- ▪ it can also be read directly by judge;

- ▪ only need Functional TTP (as with smart card)

Disadvantages of digital parchment for this purpose are:

- • MICR, OCR have higher error rate than other magnetic media. However, since digital parchment is always written by computer, writing can be coupled with hash sum as control check.

Note -- there are numerous analogues to the "parchment" notion of a document that carries (evidence of) rights that are subsequently cancelled by application of a cancellation stamp. An example found in certain countries is paper strip ticket for public transportation. This is a long thin card with a series of numbered slots. A mechanical device is available at each bus or metro stop, which allows the user to cancel a slot with a date stamp, permitting a single ride.

6.4   Functional Comparison of Media

Features of media relevant to the digital transfer of rights are shown in Table 1. These are compared to the media discussed in the above solutions.

Table 1: Comparison of Media Features Relevant to the Digital Transfer of Rights

	Paper	Magnetic Media	Smart Card	Digital Parchment
Human readable	yes	no	no	yes
Machine readable	no (?)	yes	yes	yes
Non-reproducible	yes	no	yes	yes
Machine writable	yes	yes	yes	yes
Person writable	yes	no	no	no

7   Concluding Remarks

Understanding business, we claim, involves the interplay of three realities: physical reality, documentary reality, and deontic reality. Of these, the deontic reality is arguably the most important for business, because it provides the basic mechanisms for managing the future.

The critical element, as any business person knows intuitively, is commitment: of closing the deal; of signing the contract; to shake hands on it. But, how do the parties know just what they agreed about? Each has their own individual understanding, but what matters is their joint understanding. Thus, they need some way to objectively evidence their agreement; if later they find they misunderstood one another, the evidence serves as the basis of arbitration by a third party. For situations like this, we have focused on ways of evidencing rights, specifically the contractual rights, where one party is obliged to deliver or perform some service to another.

The driving concern in this article has been fraud -- when the evidence is somehow altered to obtain resources that were not part of the agreement. Centuries of commerce and trade have tuned the forms and uses of physical documentary evidence (mainly paper) to be sufficiently reliable for business purposes, albeit often rather cumbersome. Innovations in business uses of digital documentary communications (e.g. EDI) have offered tremendous efficiency and accuracy improvements over paper documents. But, some of the features of paper documents, in particular the recognizable uniqueness of an original document, are not sufficiently represented in digital form. A key challenge is the secure digital transferability of unique rights. The main result of this paper has been to explicate this challenge in detail; to point to some existing solution strategies; and to propose some possible improvements.

Websites List

Site 1: The International Air Transport Association (IATA)
http://www.iata.org.

Site 2: NOLO Glossary, "electronic ticket".
http://www.nolo.com.

References

[1] A. Fleming (2002). Paper versus Electronic Tickets. [Online] Available: http://airtravel.about.com/cs/bookitonline/a/paperelectronic.htm.

[2] L. Alexander (2007). Deontological Ethics. Stanford Encyclopedia of Philosophy. [Online]. Available: http://plato.stanford.edu/entries/ethics-deontological/.

[3] J. L. Austin, How to Do Things with Words. Cambridge (MA): Harvard University Press, 1962.

[4] N. Belnap and M. Perloff, Seeing To It That: A Canonical Form for Agentives. Theoria. vol. 54, pp. 175-199,1988.

[5] L. Bertossi, G. O. H. Katona, K. D. Schewe and B. Thalheim (Eds.), Semantics in Databases: Second International Workshop, Lecture Notes in Computer Science, Springer, 2003.

[6] Bolero, Legal Aspects Bolero Bill of Lading. [Online]. Available: http://bolero.codecircus.co.uk/assets/31/legal%20aspects%20of%20a%20bill%20of%20lading1092161487.pdf.

[7] Bolero. Rule Book. [Online]. Available: http://bolero.codecircus.co.uk/solutions/trade_platform/rulebook.html.

[8] R.W.H. Bons, Designing Trustworthy Trade Procedures for Open Electronic Commerce. Ph.D. thesis, Erasmus University, Rotterdam, 1997.

[9] R. W. H. Bons, R. M. Lee and R. W. Wagenaar, Obstacles for the Development of Open Electronic Commerce. Proceedings of the Ninth International Conference on EDI: Electronic Commerce for Trade Efficiency, Bled, Slovenia, June, 1996, pp. 191-202.

[10] C.E. Chadman, Chadman's Cyclopedia of Law. Chicago: American Correspondence School of Law, 1912.

[11] G. F. Chandler, It's the Information That's Important, Not the Paper, L/C MONITOR, Apr. 2000. [Online]. Available: http://www.globaltradecorp.com/archives/lcminfo.htm.

[12] H. De Soto, The Mystery of Capital: Why Capitalism Triumphs in the West and Fails Everywhere Else. Basic Books, New York, 2000.

[13] A. Delmedico, EDI Bills of Lading: Beyond Negotiability. Hertfordshire Law Journal. [Online]. vol. 1, no. 1, pp. 95-100, 2003. Available: http://perseus.herts.ac.uk/uhinfo/library/w45525_3.pdf.

[14] DEON'08 Ninth International Conference on Deontic Logic in Computer Science, Luxembourg, 15-18 July, 2008. [Online]. Available: http://deon2008.uni.lu/.

[15] D. R. Dowty, R. W. Wall S. Peters, Introduction to Montague Semantics. Boston: Reidel, 1981.

[16] M. Dubovec, The Problems and Possibilities for Using Electronic Bills of Lading as Collateral, Arizona Journal of International and Comparative Law. [Online]. vol. 23, no. 2, pp. 437-466, 2006. Available: http://www.law.arizona.edu/journals/ajicl/AJICL2006/vol232/Dubovec note.pdf.

[17] N. Ferguson and B. Schneier, Practical Cryptography. Wiley Publishing, 2003.

[18] S. Firozabadi, Y. H. Tan and R. M. Lee, Formal Definitions of Fraud, In P. McNamara and H. Prakken (Eds.) Norms, Logics and Information Systems - New Studies in Deontic Logic and Computer Science, IOS Press, Amsterdam, The Netherlands. pp. 275–288, 1999.

[19] B. C. van Fraasen, Formal Semantics and Logic. New York: Macmillan, l971.

[20] C. Fried, Contract as Promise: A Theory of Contractual Obligation, Harvard University Press, 1981.

[21] L. T. F. Gamut, Logic, Language, and Meaning: Volume 2 Intensional Logic and Logical Grammar, University of Chicago Press, 1991.

[22] H. L. A. Hart, The Concept of Law. Oxford University Press, 1961.

[23] H. L. A. Hart, Essays on Bentham – Studies on Jurisprudence and Political Theory. Clarendon Press, Oxford, 1982.

[24] K. Henry, Document Credibility as a Metric for Potential Identity Fraud, Ph. D Dissertation, School of Business, Florida International University, March, 2008.

[25] H. Herrestad and C. Krogh, Obligations directed from bearers to counterparties. Proceedings of the 5th International Conference on Artificial Intelligence and Law (ICAIL'95), New York: ACM, 1995.

[26] R. Hilpinen, Deontic Logic: Introductory and Systematic Readings. D. Reidel, Dordrecht, the Netherlands, 1971.

[27] W. H. Hohfeld, Fundamental Legal Conceptions as Applied in Judicial Reasoning. Yale Law Journal. vol. 26, no. 8, pp. 710-770, 1917.

[28] ICAIL, International Association for Artificial Intelligence and Law. [Online]. Available: http://idt.uab.cat/icail2009/index.php?option=com_frontpage&Itemid=1.

[29] International Chamber of Commerce (ICC) Uniform Customs and Practice for Documentary Credits (UCP 600), 2007. [Online]. Available www.chelinvest.ru/corp/currency/UCP_600_2007_208751_v1.pdf.

[30] A. J. I. Jones, and M. Sergot, A Formal Characterisation of Institutionalised Power. Journal of the Interest Group in Pure and Applied Logics (IGPL). vol. 4, no. 3, pp. 429-445, 1996.

[31] Kent, W. Data and Reality. North-Holland, 1978.

[32] S. O. Kimbrough, Sketch of a Basic Theory for a Formal Language for Business Communication. Proceedings of the Thirty-First Hawaii International Conference on System Sciences, January 1998.

[33] S. O. Kimbrough, R. M. Lee and D. N. Ness, Performative, Informative and Emotive Systems: The First Piece of the PIE, Proceedings of the Fifth International Conference on Information Systems, pp.141-148, 1984.

[34] S. O. Kimbrough and R. M. Lee, On Illocutionary Logic as a Telecommunications Language", Proceedings of the International Conference on Information Systems (ICIS), 1986.

[35] C. P. Kottak, Cultural Anthropology, McGraw Hill, 2004.

[36] K. Kuramitsu, T. Murakami, H. Matsuda and K. Sakamura, TTP: Secure ACID Transfer Protocol for Electronic Ticket between Personal Tamper-Proof Devices, 24th International Computer Software and Applications Conference (COMPSAC), pp. 87-92, 2000.

Ronald M. Lee
Vu Nguyen
Anastasia Pagnoni

[37] E. T. Laryea, Paperless Trade: Opportunities, Challenges, and Solutions. London: Kluwer Law International. 2002.
[38] R. M. Lee, CANDID: A Logical Calculus for Describing Financial Contracts. Ph.D. dissertation, available as WP-80-06-02. Philadelphia, PA: Department of Decision Sciences, The Wharton School, University of Pennsylvania, 1980.
[39] R. M. Lee, A Logic Model for Electronic Contracting. Decision Support Systems. vol. 4, no. 1, pp.27-44, 1988.
[40] R. M. Lee, Candid Description of Commercial and Financial Concepts: A Formal Semantics Approach to Knowledge Representation, in Formal Modeling in Electronic Commerce, eds. S. O. Kimbrough and D.J. Wu, Springer Verlag, 2004.
[41] R. M. Lee, Performatives, Performatives Everywhere But Not a Drop of Ink, in Formal Modeling in Electronic Commerce, eds. S. O. Kimbrough and D.J. Wu, Springer-Verlag, pp. 177-200, 2004.
[42] R. M. Lee, K. Dutta, K. Henry and V. Nguyen, Controls as a Sharable Knowledge Commodity: An Architecture for Open Exchange, Journal of Group Decision and Negotiation. vol. 16, no. 2, pp. 143-167, 2007.
[43] B. Linsky, The Notation in Principia Mathematica. Stanford Encyclopedia of Philosophy (SEP), 2005. [Online]. Available: http://plato.stanford.edu/entries/pm-notation.
[44] D. N. MacCormick and O. Weinberger, An Institutional Theory of Law. D. Reidel, Dordrecht, the Netherlands, 1986.
[45] D. Makinson, On the formal representation of rights relations. Journal of Philosophical Logic, vol. 15, pp. 403-425, 1986.
[46] J. J. Meyer and R. J. Wieringa, Deontic logic: a concise overview, in J. J.Ch Meyer and R. Wieringa (eds.) Deontic Logic in Computer Science, London: John Wiley & Sons, 1993.
[47] S. Moore, Saying and Doing: Uses of Formal Languages in the Conduct of Business. Ph. D Dissertation, Department of Operations and Information Management, University of Pennsylvania, 1993.
[48] National Center for Health Statistics, Revisions of the U.S. Standard Certificates of Live Birth and Death and the Fetal Death Report, 2003. [Online]. Available: http://www.cdc.gov/nchs/vital_certs_rev.htm.
[49] V. Nguyen, A Deontic Analysis of Inter-organizational Control Requirements. Ph. D Dissertation, School of Business, Florida International University, May, 2008.
[50] V. Nguyen, R. M. Lee and K. Dutta, An Aspect Architecture for Modeling Organizational Controls in Workflow System. Information Technology Journal. vol. 5, no. 3, pp. 460-470, 2006.
[51] OASIS. Security Assertion Markup Language (SAML). [Online]. Available: http://xml.coverpages.org/saml.html.
[52] A. Pagnoni, Project Engineering: Computer-Oriented Planning and Operational Decision Making. Springer-Verlag, 1990.
[53] R. Reiter, On Closed World Data Bases. In H. Gallaire and J. Minker, editors, Logic and Data Bases, pages 119-140. Plenum., New York, 1978.
[54] F. Santos and J. Carmo, Indirect action, Influence and Responsibility. Deontic Logic, Agency and Normative Systems, Proceedings of the 3th International Workshop on Applications of Deontic Logic in Computer Science (DEON'96), Berlin: Springer Verlag, 1996.
[55] F. Santos, A. J. I. Jones J. Carmo, Action Concepts for Describing Organised Interaction. Proceedings of the 30th Annual Hawaii International Conference on System Sciences (HICSS'9), IEEE Computer Society, 1997.
[56] A. Schmidt, TEDIS Phase II Task F4 Final Report: Legal Aspects, EDI Law Review 4: 5-49, Kluwer Academic Publishers, 1997. [Online]. Available: https://openaccess.leidenuniv.nl/dspace/bitstream/1887/3260/1/166_024.pdf.
[57] B. Schneier, Secrets and Lies: Digital Security in a Networked World, Wiley, 2004.
[58] J. R. Searle, Speech Acts: An Essay in the Philosophy of Language. Cambridge University Press, London, 1969.
[59] J. R. Searle, The Construction of Social Reality. The Free Press, 1995.
[60] J. R. Searle, What is an Institution? Journal of Institutional Economics. vol. 1, no. 1, pp. 1-22, 2005.
[61] J. R. Searle, Social Ontology: Some Basic Principles. Anthropological Theory. vol. 6, no. 1, pp. 12-29, 2006.
[62] J. R. Searle and D. Vanderveken. (2005, October) Foundations of Illocutionary Logic. Cambridge University Press, London, 1985.
[63] Smith, Barry. The Ontology of Documents. Presentation Ontolog Forum. [Online]. Available: http://ontolog.cim3.net/cgi-bin/wiki.pl?ConferenceCall_2005_10_13
[64] R. Stamper, Keynote Address, ICEIS 1999. [Online]. Available: http://www.iceis.org/iceis99/stamper/bio.htm.
[65] R. Stamper, K. Liu, M. Hafkamp and Y. Ades, Understanding the Roles of Signs and Norms in Organizations -- A Semiotic Approach to Information Systems Design. Behaviour and Information Technology. vol. 19, no. 1, pp. 15-27, 2000.
[66] Y. H. Tan, and W. Thoen, A Logical Model of Directed Obligations and Permission to Support Electronic Contracting. International Journal of Electronic Commerce. vol. 3, no. 2, pp. 87-104, 1998.
[67] J. van Tassel, Digital Rights Management, Focal Press, 2006.
[68] G. B. Thompson, Ethereal Goods, The Economic Atom of the Information Society, Paper prepared for the EEC Conference on the Information Society, Ottawa: Bell Northern-Research, Dublin, Ireland, November 18-20, 1981.
[69] K. Umapathy, The Language Action Perspective (LAP), Theories Used in Information Systems Research, 2007. [Online]. Available: http://www.istheory.yorku.ca/languageactionperspective.htm.
[70] G. H. von Wright, An Essay on Deontic Logic and the General Theory of Action. North-Holland Publishing Company, 1968.
[71] H. Weigand and W. Hasselbring, An Extensible Business Communication Language, International Journal of Cooperative Information Systems, 2001.

[72] J. K. Winn, Electronic Chattel Paper under Revised Article 9: Updating the Concept of Embodied Rights for Electronic Commerce. Chicago-Kent Law Review Symposium on Revised Article 9. 1999.

[73] L. Wittgenstein, Philosophical Investigations. Translated by G.E.M. Anscombe. Third Edition. New York: Macmillan, 1953.

[74] A. N. Yiannopoulos (Ed.) Ocean Bills of Lading: Traditional Forms, Substitutes, and EDI Systems. 14th International Congress of Comparative Law. Kluwer Law International. 1995.

Appendix I

Deontic Foundation

Basic Deontic Concepts

Deontic logic has its origin in the classical philosophy of ethics. The modern development of deontic logic was initiated in the early 1950's by G.H. von Wright who coined the term, based on the Greek $\delta\varepsilon o\nu$ meaning 'as it should be' or 'duly'. Deontic logic is a logic of normative concepts. Its major application, outside of ethics, has been to the philosophy of law. It is here that the connections to contract law, and eventually to bureaucratic regulation, might be made. The first axiomatization for deontic logic was proposed by Von Wright [70]. As a basic concept, he introduced the operator:

$$O\,\phi$$

read that state ϕ is obligatory. Based on this, a notion of permission can be defined as its logical dual:

$$P\;\phi \equiv\; \sim O \sim \phi$$

That is, ϕ is permitted if and only if $\sim\phi$ is not obligatory. A related concept of prohibition was defined as:

$$F\phi \equiv O \sim \phi$$

That is, ϕ is forbidden if and only if $\sim\phi$ is obligatory. For completeness, we also add a notation for waiver (of an obligation):

$$W\;\phi \equiv\; \sim O\;\phi$$

That is, ϕ is waived if and only if ϕ is not obligatory.

It should be emphasized here that ϕ represents a *state* (technically, a proposition that is true in a state). This state-based interpretation allowed Von Wright to formalize deontic logic as a variant of modal logic. With minor adaptations, the modal logic form has come to be called Standard Deontic Logic [26].

Deontics for Actions

In contrast to this state-oriented formulation of deontic concepts, normative rules are more commonly used to apply to actions. For instance, the purpose of a "No Smoking" sign is to forbid people from engaging in the action of smoking, rather than to prohibit a state where smoke is present. However, a formulation of deontic logic based on actions has presented various logical challenges, and there is no solid consensus. One approach utilizes a representation of action due to Belnap and Perloff [4], where actions are typically represented by the so-called 'see to it that' (STIT) operator:

$$E_x\phi$$

read that agent x 'sees to it that' ϕ is brought about. There is ongoing debate whether this is sufficient to represent all kinds of action: e.g. smoking, which does not seem to have a separate goal other than the pleasure of the activity itself.

Deontic Changes

While deontic relationships define the static structure of a deontic process, deontic changes reflect the dynamic aspect of the process. For any deontic change, there is a 'scope of effect' defined by the deontic relationships. For instance, in a documentary credit, by delivering goods to the carrier, the seller completes his obligation of shipment, and according to the correlative relationship between obligation and right, the buyer has no right to claim for shipment. At the same time, according to the unilateral contract with the issuing bank, the seller entitles to get payment.

Deontic changes are due to certain 'deontic events', whose occurrence, by satisfying prescribed rules and conventions, changes the deontic positions of the involved parties. A deontic change might be a temporal event like the passing of a deadline of a contract, or a natural event like an earthquake that releases a contracting party from a duty. Most commonly, deontic events are agents' actions, which could be physical acts like sending goods and making a cash payment, or performative actions like sending a purchase order and signing a contract.

Securing Uniqueness of Rights e-Documents: A Deontic Process Perspective

Ronald M. Lee
Vu Nguyen
Anastasia Pagnoni