First Monday, Volume 1, Number 2 - 5 August 1996

first monday

PEER-REVIEWED JOURNAL ON THE INTERNET

TRUST IN ELECTRONIC MARKETS

The Convergence of Cryptographers and Economists

By JOSEPH M. REAGLE JR.

Special Issue Update

This paper is included in the First Monday *Special Issue #3: Internet banking, e-money, and Internet gift economies, published in December 2005. Special Issue editor Mark A. Fox asked authors to submit additional comments regarding their articles.*

This paper was certainly a creature of its time. A decade ago the Internet bubble was receiving its first puffs of exaggerated exuberance. For me, this time was also informed by Barlow's A Declaration of the Independence of Cyberspace and more importantly, May's Crypto Anarchist Manifesto. The Internet and the anonymous cryptographic markets that would evolve upon it were immensely exciting. Or, at least their potential was exciting; the vision has yet to be.

This text was based on my Master's thesis, which in addition to material found in First Monday also included a protocol for managing trust in information asymmetric relationships via a cryptographic security deposit. The protocol was accepted for presentation at a USENIX conference, but I, nor anyone else to my knowledge, have ever used such an instrument. I continue to buy things over the Internet with a simple credit card; thoughts of digital cash and micro payments are distant memories.

However, the themes of this article are still relevant -- even if some of its inspirations are not. If one is interested in the question of trust, what it is, and how it relates to expected values or financial instruments, I hope the work is still of use. And trust is but one aspect of a theme that continues to be much discussed: social relationships. From digital reputation, to social protocols, social networks, and now social computing -- though this label too seems to be fading -- a prevalent question continues to be how do we replicate and augment social relations in this technologically mediated space? The expectation that this could be done with cryptographic systems may now, 10 years later, seem overly ambitious. Indeed in their 2000 book *The Social Life of Information* John Seely Brown and Paul Duguid cite this paper when they asked: "Can it really be useful, after all, to address people as information processors or to redefine complex human issues such as trust as 'simply information?'"

Perhaps, in the next decade we will see widespread computerized reputation markets. Or, maybe they are already here, with things like Amazon's book ratings, rankings in the blogosphere, and collaborative filters. First Monday continues to provide analysis of this compelling space, but, in considering this article, it also reflects how we have changed in our ways of thinking about it.

Abstract

Relative to information security and electronic commerce, trust is a necessary component. Trust itself represents an evaluation of information, an analysis that requires decisions about the value of specific information in terms of several factors. Methodologies are being constructed to evaluate information more systematically, to generate decisions about increasingly complex and sophisticated relationships. In turn, these methodologies about information and trust will determine the growth of the Internet as a medium for commerce.

Contents

Introduction

The richness and complexity of actions an Internet user may perform may soon match, or exceed, the capabilities of that person's interactions in the physical world. Transactions involving information retrieval and processing for medical, financial, professional, or entertainment purposes will exist upon a - hopefully - secure infrastructure. However, even if all underlying protocols are sound, this does not ensure that transactions in this environment are free of risk. Methods for managing the amount of risk one takes, and the amount of trust one extends to others, are still required. These methods are being created on two fronts. Cryptographers have begun expanding their understanding of market requirements and are creating the tools necessary for meeting those requirements. Economists are awakening to the immense possibilities of fast, inexpensive, ubiquitous digital networks and the potentials for the new cryptographic instruments.

Historically, formal trust relationships are represented by financial and legal instruments. A contractual obligation contingent on the recovery of a security deposit demonstrates both the "encoding" of the relationship, and the incentives for compliance with (or the lack of betrayal of) that relationship. In this paper I argue that many of the contemporary instruments for dealing with trust can be implemented in digital form - with perhaps greater efficacy. To make this argument, I first focus on the concept of trust: what is trust, and how is trust represented and evaluated in the real world. I then examine a few financial instruments with respect to trust - how they either increase the trust between principals of a transaction, or simple lessen the need for trust between the principals. I then briefly discuss some of the cryptographic protocols that mimic, or extend the capabilities of traditional instruments.

Elsewhere, I have shown how these instruments may become an integral part of a "cryptographic economy [1]." By this, I meant how will people establish trust relationships in a market that is created from agents (customers, merchants, computers, and value added services) using information, digital media, and strong cryptographic applications to conduct commerce. In this paper, I attempt to briefly present a general understanding nature of trust, and how both cryptography and economics shall contribute to creating an environment where trust relationships are created and used on a daily basis.

I conclude by briefly focusing on the third group of constituents - not mentioned in the subtitle: policy makers. There is a danger of policy makers' confusing the historical instance of a financial or trust management instrument (tool) with the operational qualities of such tools [2]. I address how this can affect the development of efficient tools - and consequently the electronic markets which would be dependent upon them.

What is trust?

The term "trust" is increasingly used by those concerned with information security and electronic commerce. The most popular domain for its usage has been research regarding authentication and the infrastructure for public key technology in a networked environment [3]. The issue of how to exchange public keys and their certifications over the Internet has been important to the creators and users of public key applications such as PGP. However, the broader, more traditional usage of the word - beyond the specifications of certification formats for public keys - has increased with the rise of electronic commerce.

Even though the term trust is used, it is rarely defined. Trust is defined, in part, by the Oxford English Dictionary as:

1. Confidence in or reliance on some quality or attribute of a person or thing, or the truth of a statement;
2. Confident expectation of something; hope;
3. Confidence in the ability and intention of a buyer to pay at a future time for goods supplied without present

payment.

Each one of these definitions applies towards an understanding of trust that I shall present in this paper. The first definition speaks to the common sense understanding of trust. If I trust you, I am relying upon a quality or attribute of something, or the truth of a statement. It also hints at a logical treatment that could apply towards understanding trust. The second definition includes the word "expectation" which reflects the strong mapping between the common sense understanding of trust and concepts from decision analysis. The third definition speaks to the driving force behind interest in trust: commerce. The language of markets, credit, risk, and the law may be successfully extended to the digital realm.

Trust as truth and belief

In the relatively small but quickly growing amount of technical literature regarding trust, a few references are made to the significant amount of philosophical literature on the topic of trust and belief. Zurko and Hallam-Baker refer to modern hermeneutics (the study of knowledge descending from Heidegger's philosophies) as an insightful philosophy into the nature of trust [4]. May suggested that artificial intelligence (AI) research on belief systems is also relevant to the study of trust [5].

There are also a number of more formal, logical systems that attempt to capture the nature of trust, and how it is used to evaluate one's environment. Rangan developed an approach for formalizing trust by constructing a theory based on a modal logic in which "first-order predicate logics are enhanced by modal operators such as belief [6]." The approach developed a model in which agents maintain a database of beliefs regarding the real world. Associated with each agent is a set of states corresponding to the real world, or his belief of the real world. A series of papers related to the analysis of authentication and beliefs about a system further advances the understanding of trust and introduces a number of more sophisticated concepts relating to trust [7]. For instance, an agent should not have to hold a universal and exclusive evaluation of the world about him. One should be able to evaluate contradictory statements from a number of differently trust agents.

In Yahalom, Klein, and Beth's 1993 paper, they "distinguish between directly trusting some entity in some respect, and directly trusting an entity in some respect due to some other entity's trust [8]." Given this new distinction, the obvious concern is how does one traverse the network or web of trust (called a trust recommendation path) that develops in an environment in which one trusts an agent, who also can express beliefs about the trustworthiness of others, and the others may do the same? They accomplish this by presenting a trust derivation algorithm which, "generates, from a given set of [trust] expressions, a set of all entities in which a corresponding entity, say A, indirectly trusts in respect to x," where x is a function that one may trust another to perform properly, such as authentication or introduction [9].

In Beth, Borcherding, and Klein's paper "Valuations of Trust in Open Networks," the analysis of derived trust is further extended for cases in which, "different entities offer different allegedly authentic data ... [10]." A method of resolving these differing opinions is required. A number of interesting concepts are introduced, one of which is the recording of both positive and negative experiences with other agents. I call this record a history. The concept of direct trust (trust about a direct interaction with another) and recommendation trust (one's level of trust in another, especially introducing strangers) are also defined in the following manner. A direct trust relationship exists if:

"all experiences with Q with regard to trust class x which P knows about are positive experiences ... V is the value of the trust relationship which is an estimation of the probability that Q behaves well when being trusted. It is based on the number of positive experiences with Q which P knows about [11]."

A recommendation trust relationship exists "if P is willing to accept reports from Q about experiences with third parties with respect to trust class x [12]." As the positive experiences grow with a particular agent, v will approach 1. If the negative experiences exceed the positive over time, v will approach 0. Given a non-cyclic network with v representing the value of the trust relationships (vertices) between the agents (nodes) a derived trust value can be calculated which includes the strength of the recommendation, and how much one trusts the actual source of the recommendation.

Also, an interesting result of this analysis is that trust valuation is considered in light of economic value. As mentioned earlier, we assume that the value of each task can be measured in units, e.g. in ECU which are lost when the task is performed incorrectly. Our estimations about the reliability of entities were made relative to tasks consisting of a single unit. If we wish to entrust a task consisting of T units, the trust entity has to fulfill T "atomic" tasks in order to complete the whole task. Bearing in mind, we can estimate the risk when entrusting a task to an entity.

Given the above progression of formal models which become increasingly sophisticated, my intent is not to replicate the formal methods, but to provide a general understanding of trust in the most comprehensive manner and to show how that understanding can be used to represent complex interactions on digital networks - and the interactions of trust with economic value.

A Theory of trust

In keeping with Rangan's treatment, I posit that there is in fact a real world. However, each agent can consider potentially contrary beliefs about that real world, each which is expected to be true with some probability. In Beth, Borcherding, and Klein's abstraction of direct trust and recommended trust, I only consider one form of trust which is the trust one extends about various assertions [13]. An assertion is a statement which asserts an attribute of the real world.

The abstraction here is that one can place a variable amount of trust on both first and second hand perceptions and stimuli. Trust is the degree to which an agent considers an assertion to be valid for the real world. There is an associated risk of the assertions being wrong [14].

Experience is the creation of a history that contains mappings between various assertions about the real world. For instance, someone may predict (assert) that the sun will rise tomorrow, and when my eyes have told me (assert) that it does, I have gained experience. A belief or assumption is a strong assertion that is innate to an agent's intelligence, or perhaps common to many agents (similar to Beth, Borcherding, and Klein's concept of direct trust.) Assumptions are rarely challenged and are considered to be (1) a seed for the evaluation of all other assertions, (2) a common basis for the creation of histories between agents. For instance, the assertion:

- "I exist" is considered to be a very strong assumption. (~99.999%)

- "I believe what my eyes tell me about the real world" is considered to be a relatively strong assumption. (~99%)

- "I believe what other agents tell me the real world" is not an assumption. (~75%)

For instance, an agent may tell me that I may find $5 under the blue stone. If $5 is found under the blue stone, an experience relative to the assumption that I indeed saw it for my own eyes becomes part of my history - experience is created. In this case:

- assertion of $5 under blue stone

- assumption of I may believe my eyes that $5 was found under the blue stone

So as to not to always have to question an agent's first hand knowledge, I define an event to be the eventual result or determination of an assertion based on first hand knowledge or an equally strong assumption. The mapping between two assertions (one often being an assumption) is similar to Rangan's belief acquisitions.

Unlike Rangan, I assume agents may accept new assertions which are contrary to previous assertions. Also, I differ with Rangan by allowing an agent to hold a wide range of possible beliefs, including p, ~p, and p probabilistically.

In place of Rangan's belief-database (in which only assertions consistent with previous assertions in the database are accepted), I consider a more complex trust algorithm akin to the Beth, Borcherding, and Klein's derivation algorithms which generates the probability with which an agent feels an assertion is likely to pertain to the real world. As an example, an agent may see a ball drop 100 times after being released and have a lot of trust (a high expectation) in the assertion that the ball will drop again if released in the future. Trust algorithms can be considered to be function which describe personal behavior, or a deterministic algorithm of an agent, both of which will have some of the following characteristics:

Characteristics of Trust Evaluations

C1. Closeness - given an experience of the form A1A2, if A2 is an assumption, the strength of the mapping between A1 and A2 will be greater. Hence, seeing five dollars under the blue rock is closer (and in this case more likely to be believed) than reading about it. This strong mapping may then be used as a basis for believing other assertions about the world. Also, if no money is found under the blue rock this negative experience is closer than having read about the money not being found under the blue rock.

C2. Accuracy - the degree to which an assertion matches another. Finding $5 under the blue rock, rather than $4, $3, or no money under the rock leads to a stronger experience.

There are also a number of variables which take into account multiple actions from agents over time.

C3. Sample size - the number of times (or samples) an assertion about the real world is taken (seen). (The amount of experience, similar to the relationship between the number of p and n in Beth, Borcherding, and Klein's paper.)

C4. Variance - the degree to which an assertion varies from aggregated experience. (For instance, an assertion may be "too good to be true.")

And amongst the above variables are the demographic categories with which they are compared to or correlated with:

C5. Expertise - Proclamations by an agent that is known to be a doctor (with perhaps a digital certificate from an organization such as American Medical Association (AMA) to prove it) is trusted with regards to assertions on medical information, but not with regards to automotive information.

C6. Deferral (Accreditation) - The example above of the AMA asserting that a doctor is a good doctor is an example of an agent trusting an assertion about another agent.

C7. Threshold (Group) - One many not trust the individual assertion of Bill, Al, or Joe; but, if all three assert the same thing, one may have a higher opinion of that assertion.

Furthermore, one may examine the above components with respect to a specific individual or demographic group:

C8. Individual History - The history of that particular individual (or threshold group).

C9. Category History - The history of similar individuals (or threshold groups).

Finally, there could be any number of initial conditions and assumptions for the algorithm itself.

C10. An agent is generally (dis)trusting in believing assertions.

C11. An agent does (not) give people the benefit of the doubt initially.

For some, this algorithm is most likely not monotonic, and may be non-deterministic (seeming irrational). For instance, a favorite saying of some parents relative to C7 is, "if everyone jumped off the cliff, would you do it too?" This ambiguity with respect to the rationality and expectations of the agents leads one to consider the realms of risk perception and decision analysis.

Decision analysis

A field other than philosophy and logic which may provide a means for understanding trust in the digital realm is decision analysis. Such a mapping seems particularly appropriate since there is a wide body of literature on preference functions, expected values, and risk assessment. All of these are concepts we are attempting to understand in relation to a networked environment and apply to the second definition of trust as provided earlier by the Oxford English Dictionary. For the following discussion, I will repeatedly referred to an example of two users attempting to decide if or how to conduct transactions in a hypothetical for.sale newsgroup.

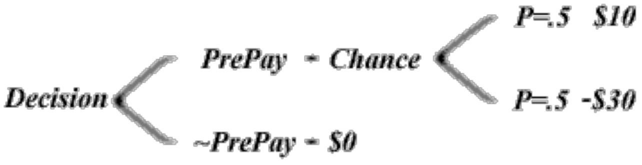
The Value of credit information

A common-place occurrence on the Internet is that of a user wishing to buy a product from another. There is risk for both the seller and buyer in such a scenario depending on a selected arrangement. A buyer needs to be concerned about receiving the product in working order in return for the money spent for the product. The seller in turn, needs to be concerned with the quality of payment for his product: will it be the right amount and on time? The concerns of the buyer and seller often take the form of negotiation regarding whether the product is paid for by check, cash, or credit card; whether the transaction is cash on delivery (COD), or prepaid. This negotiation shifts the amount of risk between the parties and the level and direction of trust required in the transaction. It is dependent on the economic properties of the supply and demand for the product [15]. For instance, tenancy places the land-owner at risk since the tenant may ruin the property, but because the owner often has a stronger position in the market (a take-it-or- leave-it deal), the owner can force the transference of risk to the tenant with a security deposit.

Often, buyers and sellers in such a situation are faced with a decision: to purchase the item, or forgo the purchase. In a more sophisticated case, a user also has an option to purchase information concerning the expected result. This is likened to buying credit or rating information regarding the trust worthiness of the other principal. Decision analysis provides one a way to analyze such a scenario. While it probably would not be a plausible nor efficient exercise for conducting transactions over the Internet, it does provide an understanding of the concepts involved [16]. Consider the following example from a buyer's point of view.

Expectation with no information

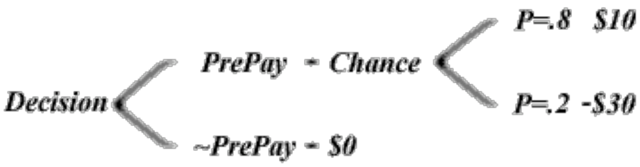
The buyer has been offered 1 megabyte of computer RAM for $30, prepaid. One megabyte of RAM is worth approximately $40. The buyer has never done business with the seller before and is not very trusting. He expects the seller will cheat him with a 50% probability. The decision the buyer is then presented with is as follows (see Figure 1):



The expected value for the PrePay decision is $(.5)10 + (.5)(-30) = -10$. The expected value of the ~PrePay (and as such no transaction) is 0. Since, $-10 < 0$ the buyer would not proceed with the transaction. A useful extension to this scenario is the expected value of information (EPVI). EPVI corresponds to the information about a market, the credit history of a user, or the certification a third party could provide to vouch for the level trustworthiness of another user. Assuming that the third party (referred to as a credit agency) is trustworthy, what service and increased benefits could be provided?

Expectation with extended information

deNeufville defines the value of information in decision analysis as, "The increase in expected value to be obtained from a situation due to the information, without regard for the cost of obtaining it [17]." In this example, assume that the credit agency has aggregate market information that shows that prepaid transactions for RAM are honestly completed 80% of the time (see Figure 2).



The revised expected value for the decision is (.8)10 + (.2)(-30) = 2. As such, over a significant number of transactions, on average this information provided the buyer with a benefit of $2 - some of which can be collected by the credit agency.

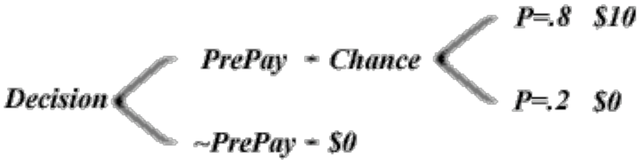
Expectation with perfect information

The credit agency would be remiss if it was not able to provide specific information about the seller. In such a case, the buyer could attain information about the character of that seller. Or it could procure the results of a test in which the credit agency would either "approve" or "disapprove" the transaction on a basis of its own models. Perhaps the agency has a "better," more sophisticated trust algorithm; with specific information on agents, it is able to make recommendations regarding a transaction.

In this case, the credit agency's service provides specific information which the user can than apply towards his own preferences, or the agency can give a simple recommendation for conducting the transaction [18]. Take a similar example over the acceptance of a credit card; every store cannot process all the trust information regarding every transaction, hence they defer such decisions to credit card agencies. Since this recommendation is an assertion (even if it is an assertion about the assertion of another), it too is subject to the exercise of trust. In other words, it has a probability of being an accurate assertion. The credit agency may be able to assert that it's predictions are accurate 85% at the time. Or perhaps one has enough experience with the credit agency to come to this conclusion on one's own. To avoid any confusion, the buyer will continue to trust the assertions of the credit agency, and as such will not worry that the agency may be misrepresenting its accuracy rate. In this situation, the user could calculate the expected value of perfect information and assume the credit agency is always accurate. In such a case, the new calculations would be correspond to the following:

"First, every test result, Trk, from the perfect test will tell us exactly what will happen subsequently, and its associated outcome, Oik, will have probability one in the revised decision tree following the test result [19]."

In our case, we would conduct the calculation taking the branch of each decision with the best outcome. Since we have perfect information and know exactly when to conduct a transaction, the decision tree and expect value is simple: (.8)10 + (.2)0 = 8 (see Figure 3).



The expected value of perfect information is then our new result less the old: 8 - 2 = 6.

Expectation with sample information

Calculations for the expected value of sample information are more complex and require one to consider the fact that predictions are incorrect 15% of the time. Such errors will decrease our benefit because of valuable business lost, and the bad risks that were needlessly assumed. The calculations for this case are shown elsewhere, but the resulting value of the expected value of sample information is 5.9008 [20]. Hence, the value of the sample information in this case was (5.9008 - 2) 3.9.

However, there are a number of contentious theoretical questions with regards to using this type of analysis with respect to statistically independent events. Regardless of these, we have come to an understanding of trust which is reflected in the following definitions:

trust: the expectation of an assertion being true [21];

trust algorithm: an algorithm that determines/explains the creation of the expectations.

Trust as commerce

The third definition of trust from the Oxford English Dictionary was simply stated: "Confidence in the ability and intention of a buyer to pay at a future time for goods supplied without present payment." This definition allows one to consider aspects of trust not given in the previous analysis. For while it may seem intuitive to consider trust in light of decision analysis, the expected value and probabilities in such an analysis are considered to be phenomena of the real world and not interactions with competitive agents.

For instance, consider the case where agent (B) - who plans to cheat - offers agent (A) $20 for a 1M of RAM. Agent (A) may be suspicious and not accept the offer based on his expectations (level of trust) of agent (B). Knowing this beforehand, perhaps agent (B) would offer \$100 for 1M of RAM. If this were a very simple expected value calculation, in which the probability of the \$20 and \$100 deals were the same, a cheating agent could inflate the outcome so as to turn the decision to his favor. However, one of the variables considered in the treatment of the trust algorithm was the consideration for outcomes which seemed "too good to be true." This section will deal with such topics more specifically and will refer to concepts from microeconomics and game theory.

Hal Finney and Wei Dai discuss a concept related to trust, that of reputation [22]. Reputation is the amount of trust an agent has created for himself through interactions with other agents [23]. Hence, if one's assertions consistently meet the expectations of other agents, they will have higher expectations of later assertions being valid.

Reputation is valuable for three main reasons. A user may prefer to conduct transactions with trusted users. The costs of transactions between trusting users may be smaller because third party reputation services need not be consulted. Finally, if the conditions are right, one can betray one's reputation for a very large gain.

The exact economic nature of reputation and trust is not often addressed with regards to transactions over information networks aside from discussions on the cypherpunks list. Dai, for example, wrote [24]:

"In a reputation based market, each entity's reputation has three values. First is the present value of expected future profits, given the reputation (let's call it the operating value). Note that the entity's reputation allows him to make positive economic profits, because it makes him a price-maker to some extent. Second is the profit he could make if he threw away his reputation by cheating all of his customers (throw-away value). Third is the expected cost of recreating an equivalent reputation if he threw away his current one (replacement cost)."

In more traditional economic terms, reputation could be viewed as an asset: "something that provides a monetary flow to its owner. For example, an apartment can be rented, proving a flow of rental income to the owner of the building [25]." It probably cannot be considered a product in that concepts of supply, demand, marginal cost and other costs associated with production do not generally hold. For instance, consider how trust can be created:

a) Trust is created through the development of experience with other agents. Hence, it is a relation rather than a product. For instance, if agent (B) successfully completes a transaction with agent (A), agent (B)'s reputation is still a product of the "arbitrary" trust algorithm agent (A) employs. However, agent(A) may be distrustful no matter how many satisfactory transactions occur;

b) The only relevant cost in the creation of trust seems to be the opportunity cost of betraying that cost. Any costs pertaining to the transaction itself (i.e. the cost of being on the network) would be accounted for in the cost of the transactions;

c) There is a boundary on both how much (100%) and how little (0%) trust can be generated;

d) Agents can transfer trust by certifying another agent; and,

e) The creation or destruction of trust is not a zero sum game. The net sum of trust may increase or decrease.

However, perhaps these two general rules could be applied in decision making regarding reputation creation as asset creation:

1. An agent should maximize profit over its planning horizon, where profit is defined in the economic sense as revenue less costs, including opportunity cost. The opportunity cost of reputation is the excess revenue that could be generated from the exchange of the reputation (and its revenue over the planning horizon) for immediate revenue (by cheating) over ones planning horizon.
2. The decision as to whether to invest in building reputation is subject to the NPV Criterion which states: "Invest if the present value of the expected future cash flows from an investment is larger than the cost of the investment" or if the following equation is positive for cost C, discount rate R, and time horizon n [26]:

$$NPV = -C + \frac{\pi_1}{(1+R)} + \frac{\pi_2}{(1+R)^2} + \ldots + \frac{\pi_n}{(1+R)^2}$$

The important consideration here is that C is a function of an agents reputation algorithm and the trust algorithms of agents with which he will interact.

Clearly, the defining and characterization of trust and reputation in such a scenario soon becomes very complex. By considering trust from an economic perspective, there are a number of economic sub-disciplines by which trust can be considered. Examine, for example, markets with asymmetric information [27]. The most common example is that of the used car market where the buyer has very little knowledge regarding the quality of an object being purchased [28]. Such a market is characterized as failing because of asymmetric information, or the lack of trust. The example of the used car often fails because the market is perceived as being one of low quality cars, which exacerbates the removal of high quality cars from the market, which in turn exacerbates the perception of their being a disproportionate amount of "lemons."

There is a fair amount of economic literature dedicated to product quality and asymmetric information, particularly in the field of insurance and credit. Temporary goods and services are another field where this sort of information is an issue;.

as an example, think about a highway motel or restaurant that is not likely to have repeat customers and cannot build, at first blush, a personal reputation. The solution may have an interesting application in the network world and consists of creating a reputation - market brand - through standardization. For instance, all McDonald's restaurants have relatively the same color schemes, foods and prices and attract customers that may have never eaten in that particular restaurant [29]. Hence, brand identifications, in the form of logos, seals, or labels, on the World Wide Web may be of great importance; already, there are a number of digital equivalents of these identifications that are appearing on different sites. Other common economic concepts are that of market signaling, particularly guarantees and warranties [30].

The second field of economics which is of interest is competitive strategy and game theory. Dai mentions a reputation algorithm (the counterpart of the trust algorithm) which determines the optimum conditions for increasing utility, by creating a strong reputation or exchanging it for some other value [31]. Dai posits that a good reputation algorithm (1) need be efficient (I assume this ranges from optimal efficiency to at least a "competitive" efficiency), (2) not too costly to evaluate, (3) and relatively stable in an evolutionary system. Such characteristics apply towards trust algorithm as well. In fact, trust algorithms and reputation algorithms can be thought of as competitors in a networked market where information and one's algorithms determine one's success over time.

Already we have seen that agents are employing both their trust and reputation algorithms so as to make the best choice against potential competitors. Finney refers to the Prisoner's Dilemma (PD) game as an example of a simulation of agents concerned with reputation [32]. Such games can be played multiple times, over which the agents playing have a fixed amount of memory with which to hold a grudge or to preen their reputations. Axelrod, for example, conducted a tournament in which algorithms programmed by humans competed against each other in an iterated PD game [33]. Interestingly, such games also lend themselves to the employment of "genetic algorithms" in which competitive algorithms evolve by promulgating the "fit" strategies through the lifetime of the game by the reproduction of winners, the crossing of two different winning strategies, or through random mutation [34]. Genetic algorithms have been used to simulate the creation of brands by marketing managers in simulated regional coffee markets. They gave proven "that in the limited tests we can feasibly conduct these agents outperform the historical actions of brand managers in this regional market [35]."

Consequently, the fascinating realms of competitive strategy and game-theory [36]; emergent behavior/institutions [37]; electronic [38] and information [39] markets and complexity [40] are relevant to the study of trust.

Trust Management and Financial Instruments

"Trust management instruments" and "financial instruments" in this section represent the broad range of tools used to exchange value in a marketplace. Each tool (instrument) has a quality or attribute that makes it more suitable for aiding certain transactions than others. When anonymity is required, cash is an instrument of choice. In the real world, a whole range of financial instruments exist to satisfy the needs of market participants. Each varies with respect to operational qualities such as anonymity, immediacy, and cost. They also differ with respect to the strength and direction of trust that is inherent to the use of that instrument. Some instruments may require a great deal of trust between the participants (but may facilitate very fast transactions). Others are specifically intended to allow transactions to occur in a low trust environment. The low trust environment is similar to the motivating problem of how to buy and sell things over the Internet as described earlier under the heading "Decision analysis."

Unfortunately, the term "instrument" may be misleading because it connotes a sense of physical substance, as if the real world object necessarily embodies the functionality of the instrument (for instance, a piece of paper or token). This is not necessarily true, and is becoming less true as finance becomes further digitized. A piece of paper or token has little intrinsic value. Rather it is a representation of a capability or service. Hence, it is useful to think of an instrument as both the underlying service and its physical or digital representation. With the above discussion in mind, I will make the following distinctions for the digital world:

instrument - a service that is provided to facilitate the exchange of value and its representation or certificate; similar to "3. that with or by which something is effected; means; agency [41]"

service - "13. ∞ the performance of any duties or work for another; helpful or professional activity [42]"

certificate - the representation of a service; this may be in the form of a token, legal agreement, security, digitally signed assertion, etc. Similar to "1. a document serving as evidence or as written testimony, as of status, qualifications, privileges, the truth of something, etc. [43]"

Hence, United States currency is an instrument. It is the representation of a service provided by the government that allows users to exchange value. Note that physical bills, stock and bond certificates and legal contracts are the representations of a service, even if that service is not related to the immediate transaction. These instruments are not commodities with intrinsic value. Rather, they are a representation of a complex web of trust relationships and services, just as digital certificates are representations of trust in the digital world.

Digital instruments are very young. The number of services provided are few, and the technical representations are still being standardized. One description of instruments, other than direct payment, distinguishes three types of certification instruments:

a) license - a credential that indicates a service provider is legally authorized to provide a service [which] ... has been found to meet certain minimal qualifications required by the law ... [This is a form of a credential.]

b) endorsement - provides assurance that a service provider meets more rigorous requirements determined by the endorser ... [Another form of a credential.]

c) liability insurance policy or surety bond - provides a client with a means to recover damages in the event of a loss that is the fault of the service provider. [Where] liability insurance policy represents an agreement between two parties, and a surety bond represents an agreement between three parties: the surety, the obligee, and the principal [44].

However, as exciting as these possibilities are, the relative number of instruments available to Internet users is small. Tim May stated, " ... the 'ontology' of digital money, the instruments and forms it can take, are impoverished compared to the real world." May challenged readers for the cryptographic equivalents of options, warrants, bearer bonds, promissory notes, zero coupon bonds, checks, receipts, lock boxes, coupons, time deposits, money orders, escrow, and IOUs.

Finally, before proceeding on to examples of such instruments, I must qualify my aggregation of trust instruments with financial instruments. I have already stated that financial instruments provide services. A significant service is the provision of trust (introduction, reputation, certification, etc.) Financial instruments are a means of transferring or creating value. Trust services, as discussed elsewhere in this paper, increase the efficiency or likelihood of the transference of value by acting as a "market making" or at least "market honing" force that brings otherwise recalcitrant buyers and sellers together. Many hope that digital "intermediary" services will increase the efficiency of a market, decrease the costs in a market, and act as a "market maker" where a market would otherwise fail - leading to "friction free capitalism [45]

In the digital world, bits will be bits. One string of bits may certify that a user should have access to a service. This string of bits could be exchanged for bits that represent an equivalent value in electronic cash. Just as stocks, bonds, and certificates have a market value, so will digital instruments. As discussed earlier in this paper, reputation itself has value and can be both purchased (by enduring the cost of staying honest), sold (by betraying trust) and transferred (credit agencies). Due to the nature of digital technology and an ubiquitous network, the liquidity of value as represented in various instruments will be very high. However, certain digital instruments will still be valued more than others (or more cost effective) for the appropriate transaction. While one may be able to simulate one instrument using another, the added costs of such transformation may be counter-productive.

As such, an understanding of the concepts regarding value and how they relate to trust instruments shall have a direct bearing on how trust develops in an electronic market.

Incorporating risk into the cost

If one has a predictable model of customer untrustworthiness, a simple way to handle the lack of trust is to simply incorporate the cost of the defaults into the charges levied for those services. For instance, if 5% of credit card users default, the companies can increase the fees associated with having a credit card. Of course, credit card companies also compete on the basis of fees (such as the annual fees) hence it benefits them to keep the default rate as low as possible using various selection methods.

Credit

One of the most ubiquitous and profitable trust brokers of the real world are banks. Banks extend both personal and corporate credit through charge accounts or loans. These services provide the "lubrication" for much of the activity of our economy. With respect to personal credit, every merchant cannot know the trustworthiness of every customer. Banks and credit card companies alleviate this problem by exposing themselves to risk - for a price - while allowing most transactions to proceed without inhibition. However, banks and credit agencies also wish to minimize their risk with respect to the price in order to maximize profit. To accomplish this, they have developed sophisticated systems, known as credit scoring, to measure the trustworthiness of potential customers. Credit scoring has been described as the "scientific approach to determining which applicants are granted credit" and has existed for many years [46]. but only became serious when scoring tables become widely used in the 1970s. The credit management profession and its accompanying literature reduce the risk and increase the profits inherent to such operations [47].

Money

The most familiar economic instrument throughout the world is money. I have already mentioned that intermediary trust services allow one to exchange services in a market that would have otherwise failed. Money accomplishes the same except that there is an extra step of indirection. With money, there is not trust in an immediate third party but in the stability of the currency. Just as there may be attempts to find a certification path in privacy enhancing technologies, there are efforts to find a path in a market through which one may trust that the transaction can occur in a fair and valid manner. This path needs to be cost effective as well.

This history of money is fascinating, and the future capabilities of digital money are very exciting [48]. Economic investigations on different kinds of models for electronic forms of money is proving quite intriguing, such as the efforts by Marimon, McGrattan, and Sargent [49]. Marimon, McGrattan, and Sargent extend a model of Kiyotaki and Wright [50]. This effort describe economies "in which particularly commodities emerge as media of exchange .∞ or in which a good from which no agent derives utility emerges as fiat money" using agents employing Holland's classifier systems [51].

However, with the truly daunting amount of literature on the nature of money, and a quickly growing series of treatises and articles on electronic cash, I cannot address all aspects of digital money in depth [52]. However, I will briefly touch upon those aspects with respect to trust.

A definition would be useful. Peter Huber defined money in the following way:

Money ... is just another network, our oldest medium of systematic communication. And new communications technologies are fast surpassing the old. The paperless bank, unlike the paperless office, is at hand [53]."

To underscore the importance of trust in this "systematic communication", the stability of fiat money - money that is required to be accepted by government fiat - is dependent on the economy of the government backing the money or the capability of the government to enforce its acceptance. In an examination of efforts to support the Russian ruble, Huber wrote of the importance of trust:

"But new governments of young nations, especially nations with turbulent histories, can't make money, either. Nobody quite trusts them, and without trust the paper lovingly engraved at the government mint is valueless [54]."

An interesting characteristic of trust and money supplies is that neither are, necessarily, zero sum games. The use of some instruments, and the increase in the faith of a money or its backing institution can lead to an overall greater money supply and trust in the economy. As a consequence, it is much easier to exchange value at a lower cost.

Trust and securities

To further support the argument that trust and financial instruments are tightly coupled, consider the nature of trust and the markets for securities. Futures, options, stocks, and bond markets are all creatures of trust. In a futures market, you create an obligation to sell or purchase a commodity at a set price sometime in the future. With an option, you acquire the right to sell or purchase a commodity at a certain price. Each is an expectation of the future and an attempt to profit by or hedge one's risks against uncertainty. In the stock market, you make assertions about the expected performance of a company or the market itself. A bond is a loan to a company, government, or other institution. The market depends on the buyers' confidence in or reliance upon the ability of the issuer to meet interest payments and to redeem the full value of the bond upon its maturity. Each market, and particularly the bond market, has certification and reputation agents that provide information services, the innumerable number of indexes, portfolios and rating services. For instance, the reputation of a bond is extremely important and rated according to the risk of the loan. Rating services such as Standard and Poor's or Moody's ratings dramatically influence the attractiveness and the rates of bonds offered. Lower rated bonds must offer higher rates to compete against higher rated bonds.

Primitive markets are forming on the Internet which may come to resemble the more sophisticated traditional markets. The Security Exchange Commission (SEC) recently gave permission to Spring Street Brewing Co. to continue offering information services to buyers to sellers of its stocks [55].World Wide Web-based stock reporting and index services are becoming widely available and popular to online investors.

Older institutions are not standing idly by, as seen in the SEC's own offering of EDGAR and mutual filings database to the Internet with its SEC-LIVE service [56]. These sorts of activities on the Internet will increase the efficiency of normal market institutions, replacing or extending the capabilities of current indexes and services. It will give birth to new and hybrid services such as distributed ecash-based trading. One example is the Electronic Cash Market where various ecash instruments are sold and traded [57].

Letters of credit

Letters of credit are perhaps the most striking example of an instrument that is suitable for electronic markets [58]. They are commonly used in international commerce when a buyer does not trust the seller nor the foreign (legal) institutions involved in the transaction. The same concern is felt by the supplier. Note, that it is not merely a lack of trust in each other that may hinder an international transaction, but also an inability of each party to rely upon an infrastructure (collection agencies and legal systems) to collect money even when one party cheats.

What can bridge the gap of trust to allow the transaction to occur? Letters of credit structure payments through trusted intermediaries and credible commitments so that each party is confident of payment. For instance, a supplier of sprockets in the United States wants to sell his merchandise to a customer in Japan. Each party and his representative bank make certain commitments for payment. The customer's bank in Japan makes promises to pay the supplier's bank in the United States, if the sprockets are delivered according to the contract. Likewise, the supplier is not paid until he has supplied the purchaser in compliance with the contract. While each country has its own sets of law and regulations regarding banking and collecting debts - which explains why international transactions are difficult in the first place - terms for defining and documenting letters of credit and the resulting transaction are fairly uniform. They are defined in Uniform Customs and Practices for Documentary Credits [59]. Any problems within each jurisdiction (for instance, if the customer doesn't pay for the sprockets) can be resolved within that jurisdiction (the Japanese banks sues the purchaser according to local regulations) but the supplier still receives his payment.

An obvious digital counterpart to the letter of credit is not financially oriented, but it is the exclusive focus of public key certificates. Such certificates enable two users who may be a world apart to mutually exchange keys by relying upon a hierarchical system of intermediary trust services. Just as I may not be able to trust a bank in Japan, I may not trust his key server. I do, however, trust an American server, which in turn trusts the United Nations server, which eventually trusts the Japan server.

Digital bearer bonds

Digital bearer certificates are another trust instrument which provides strong anonymity. Robert Hettinga has argued that digital bearer certificates may return the method of securities exchange to its relatively anonymous state when a bond could be transferred between parties [60]. Before 1970, bonds were anonymous bearer instruments. Every bond certificate had a number of detachable coupons which could be sent in to the issuer for redemption. This meant that the bond could be exchanged anonymously and out of sight of various government agencies such as the United States Internal Revenue Service [61]. However, after legislation requiring that such transactions be reported and a 1983 SEC ruling, many bond holders do not even receive a certificate. All payments and transactions are conducted (and reported) electronically. They are called book-entry bonds and are easily traceable.

Hettinga argued that the low cost and hierarchical structure of the communications networks on which trading services occurs makes it easy for government to regulate these securities. Regulation will be all but impossible with the even cheaper and distributed nature of Internet style communications:

"So, with a digital bearer bond, you would have in effect a bundle of digital certificates. One would be for the principal and would be good for the repayment of that principal on the date the bond was called or the redemption date, however the bond offering is written. The other certificates would represent coupons, one for each interest period for the life of the bond.

These digital certificates, in combination [with] increasingly geodesic networks enabled by exponentially falling microprocessor prices and strong cryptography, theoretically allow secure, point-to-point trading of any security of any amount with instantaneous clearing and cash settlement [62]."

Land owners (security deposits)

Another mechanism for bridging the gap between buyers (renters) and sellers (land owners) of leases for apartments is the security deposit. In such a situation, the security deposit can be thought of as coercion of the renter's behavior. In a microeconomic framework, this market is characterized by asymmetric information: the land owner does not know if the renter will be able to pay for any excess damage to the property. In this case, a security deposit acts as a signaling mechanism. It tells a land owner that the renter is a trustworthy person, and has made a credible commitment to demonstrate the fact, much like warranties, and insurance enables parties to signal in other types of markets.

The Efficacy of digital instruments

There is currently no conclusive evidence that many of the instruments mentioned in this paper will enjoy widespread support because of ease of use and efficiency. Rather, this is the expectation driving the research and development of electronic payment systems. Some of the mechanisms proposed so far include Netbill, the OMI Payment Switch, CyberCash, DigiCash, First Virtual's Green Commerce Protocol, Netcheque/Cash, and MasterCard's and VISA's Secure Electronic Transaction protocol [63]. The market for digital instruments is still immature. Many are trying to find the proper business model or even the right pricing strategy.

While there is no conclusive evidence for the success of these services - many are just at the demonstration stage - I feel there are strong arguments for their success. Consider an Internet bank, the Security First Network Bank (SFNB). How does SFNB make money? From SFNB's FAQ:

"We make money because our business model is far more efficient than traditional banking models. We have a "footprint" that spans the entire U. S. through the Internet. Yet all our Internet operations are located in Atlanta along with our banking office in Pineville, Kentucky. A traditional bank would need to have fully staffed branches all over the country to achieve the same reach. As a result, our operating costs are far lower than a traditional bank and we can pass the savings onto our customers.

Subject to regulatory approval, we plan to offer brokerage, insurance, loans, and other financial services. Although we intend to generate fee revenue for these services, we anticipate the fees will still be lower than what is competitively available to you. Because our costs are lower, everyone benefits [64]."

Much of this paper has concentrated on the competitive nature of commerce in a cryptographic economy. The success of digital instruments will consequently be dependent on improvements that they can offer over other instruments in terms of quality of service, efficiency, and security. However, since most real world services are planning to employ digital networks as part of their underlying infrastructure, I assert that purely digital services will be at least as competitive. If the infrastructure proves to be more efficient in digital form, the user interface should be doubly so. For instance, a traditional bank may offer ATM or tele-banking services. SFNB uses the same banking infrastructure, and in addition to the costs saving at the infrastructure and user interface level, the user has the added capability to check bank statements on the World Wide Web, conduct electronic payments and transfers, schedule automatic payments, and dynamically generate financial reports.

Protocols for financial and trust instruments

Previous parts of this paper discussed the relevance of financial instruments and the economic characteristics of trust relationships. Let me now briefly review some of the cryptographic protocols that allow the use of these financial instruments. These protocols also obviate the need for trust, or shift the amount or direction of trust required in a transaction. The class of protocols discussed can be subdivided into three levels. These levels have been defined as:

"Arbitrated protocols, in which a trusted third party participates in each transaction to ensure that both sides act fairly;

Adjudicated protocols, in which a third party judges - after the fact - whether both parties acted fairly and if not, which party had not; and,

Self-enforcing protocols, in which an attempt to cheat become immediately obvious to the other party and the protocol is safely terminated [65]."

Many of the schemes that I have discussed elsewhere in this paper are in fact one of the first two types of protocols. Arbitrated protocols, as has been noted by others, have several disadvantages, the main being:

"The two sides may not be able to find a neutral third party that both sides trust. Suspicious users are rightfully suspicious of an unknown arbiter in a network [66]."

With protocols, adjudication only comes after damage or cheating has already occurred. Many electronic payment or trust schemes are a combination of self-enforcing protocols, and protocols which rely upon financially arbitrated or adjudicated schemes. For instance, two untrusting principals may rely indirectly upon their trust in ecash to exchange value over the Internet. These protocols are not strictly self-enforcing because they rely upon the trust of a bank to redeem electronic tokens. Nor are they strictly arbitrated or adjudicated because a bank - the trusted third party - may not even realize that its services are used for arbitration or adjudication.

With respect to personal privacy, a bank should not be aware of the details of any transaction beyond the fact that it validly creates, exchanges, or processes forms of payment in an efficient manner. Hence, the class of protocols is defined as a indirectly arbitrated or indirectly adjudicated (collectively abbreviated as IAA) in the sense that they are often not acting actively to arbitrate or adjudicate the protocol which is employing their service. Banks and governments do well in the real world by providing a basis for others' transactions. There is no reason why they would fail to be equally successful in the digital world.

Examples of trust instrument protocols

Let me provide a general description of some of the rather surprising protocols which can be implemented over networks. The protocols are painted with a rather broad brush, complete with technical weaknesses or considerations. However, this list represents characteristics of self-enforcing protocols, or at least IAA protocols. For instance, there is a certified mail protocol that allows Teresa to require a signed receipt from Justin if he reads the message. Other schemes include:

- bit commitment - a stockbroker may wish to show that he knows whether a stock will fall (0) or rise (1) so a customer will contract with him. However, the stockbroker does not wish to disclose information prematurely. Bit commitment protocols allow a stockbroker to commit to a bit beforehand, without revealing it;
- contract signing - two untrusting users on a network may fairly sign a contract over the network by using a protocol which mutually commits each to the contract with ever increasing probability;
- zero-knowledge proofs (ZKP) - proves one knows something without releasing what one knows;
- threshold schemes (m,n) - allow for (m) people out of a total (n) to reconstruct an escrowed key or digitally sign a message. The capabilities of the protocols can be quite sophisticated. For instance, one can require specific thresholds from specific groups, such as (3,5) from group A, and (2,5) from group B. Schemes for negative votes in which, "any qualified minority can prohibit the intended action" exist as well [67].
- fair coin flips - between two persons allow for the generations of a random bit - or string of bits - of information that each feels the other party did not coerce;
- mental poker - two mutually untrusting players can play poker against each other, and at the end of each round check to see if the round was played fairly;
- digital (e)cash - digital cash allows one to anonymously create and spend something akin to cash. In the most popular form today, Chaum's DigiCash, users submit a money order to a bank. The bank signs the money order without being able to see who submitted it. The user can then give this money to a merchant in exchange for services, the merchant returns it to the bank. This scheme allows for anonymity unless the customer attempts to cheat, and spend the DigiCash twice;
- coin ripping - Imagine an untrusting person using an untrusting taxi driver to pick up some goods. The taxi driver does not wish to make a trip without payment, and the person does not wish to pay the taxi who may take the money and never return. His solution is to rip ecash so that the value is completely useless to both participants until the protocol has be satisfactorily completed by both sides [68]; and,
- digital security deposits - Envision a scheme in which a Web service provider can sell access tokens to his service

and be assured that those tokens will not be redistributed or illegally sold to other users. It requires a security deposit, established in a public place. However, the security deposit is blinded and encrypted using the access token. Hence, only the owner of the access token can claim the security deposit. If a user gives away or sells the access token, the security deposit will be lost [69].

Technology policy:
Implications for trust in electroic markets

Can complex trust instruments be implemented in a digital market? Earlier sections of this paper addressed the technical and economic aspects of this question. This part focuses on the broader - but no less important - policy issues. I use the term "policy" as the conditions and guidelines under which an institution legislates, regulates, or acts. Often technologists refuse to acknowledge the importance of anything other than technical superiority or market forces in shaping technology. However, policy is often tightly coupled with, or biased by, the technology it applies to, and vice versa.

The digital world presents a number of challenges to typical policy processes. First, technology often changes faster than policy. Second, networking technologies are capable of affecting the policy process itself. The network can be used to communicate and organize. Third, networking technologies, while similar in many ways to other communication technologies, could exceed the effects of any previous technology in the depth and breadth of their impact on society. The ability to develop sophisticated markets that employ a variety of trust and financial instruments - as well as provide communication, entertainment, and civil functionality - is dependent on the underlying technology, which can be shaped by government policy.

Currently, a debate is taking place around the world about the roles governments relative to this technology. The debate is partly the result of the phenomena I define as precedent dependency [70]. Regulatory structures become dependent on technological and political precedents (accidents) rather than general principles. For instance, in the United States a number of general principles (rights) were non-exclusively enumerated in the amended Constitution. An oft cited right is that of free speech. However, this rather simple principle has evolved into a complex policy structure wherein the right of free speech is different with respect to the communications media it employs: person-to-person, broadcast, common carrier, or print. Digital network technologies, which make those distinctions moot, confuse policy makers [71]. The unfortunate result of this dependency is promulgation of regulations that are no longer relevant to the current environment or technology.

An example of precedent dependency is the controversial United States wiretap legislation [72]. Wiretaps, which obligate a communications carrier to assist in the monitoring of a communication, are generally approved as a limited exception to the right of privacy. Law enforcement agencies have since become dependent on this mechanism, and - to their alarm - this capability may be threatened by new digital technologies. Consequently, law enforcement agencies promoted new legislation that required telecommunications carriers to build automatic wiretapping capabilities into their networks [73]. Hence, a judicial exception to the right of privacy and the technological "accident" - of being able to put a clip on a wire - has become an unusual technological requirement of communications infrastructure.

Certainly, not all government involvement is folly. Yet, the issues at hand are truly difficult and will require a great deal of thought on the part of policy makers. The situation has been described in one way:

"As U. S.. lawyers we are most accustomed to thinking about the problems of data creation, dissemination, and access in certain delimited categories such as the First Amendment, intellectual property rules, the torts of invasion of privacy and defamation, and perhaps in the ambit of a few narrowly defined statutes such as the Privacy Act or the Fair Credit Reporting Act. The categories are valuable, but are collective inadequate to the regulatory and social challenges posed by the information production, collection, and processing booms now under way [74]."

Policy and rule making

In the real world, expectations are partially a social construct. Assumptions are made in order to conduct business, or to just get through the day. It could be argued that social institutions are motivated by the dissatisfaction of members with a chaotic and untrusting society. Regulatory institutions develop to limit this dissatisfaction and increase stability. A world without traffic lights would be intolerable. Laws exist so that a green light means that one can safely proceed through the intersection. Society has encoded a number of useful default expectations about the world and attempts to enforce them [75].

Hence, governments mint money, regulate markets, and legislate. The digital realm is quickly becoming an area that is ripe for the emergence of trust intermediaries, brokers, and third party services. Consequently, governments around the globe are becoming increasingly interested in extending their regulatory powers into this new realm. However, are governments the proper institution to fill this void? This question is complex because underlying it are a number of equally difficult questions.

In terms of political theory, what abilities are granted and restrictions placed upon governments? This question is often confused by precedent dependency.

Do those abilities and restrictions upon governments change when they enter into this new realm? Examples of free speech and wiretapping have already been mentioned.

Are aspects of the digital realm so unlike the real world that many government services are no longer needed? For example, need they be the sole "creator" of currency in the future?

How does one deal with the international aspects of regulating networks?

David Post examined these questions on cyberspace governance by relying upon Robert Ellickson's framework of behavioral controls, and the role various entities play in regulating an environment. He argues - as I did earlier - for the capability of policy to dramatically affect technology:

"Networks - electronic or otherwise - are particular kinds of "organizations" that are not merely capable of promulgating substantive rules of conduct; their very essence is define by such rules - in this case, the "network protocols". Accordingly, the person or entity in a position to dictate the content of these network protocols is, in the first instance at least, a primary "rule maker" in regard to behavior on the network [76]."

The Internet, of course, is not immune from government coercion.

Cryptography

Some degree of trust will exist between the participants of any electronic communications. For example, I have purchased computer RAM over the Internet without requiring anything beyond electronic mail. However, encryption technologies - as should be evident from this paper - are essential to the development of sophisticated and efficient trust and financial instruments. I, and the seller of the RAM, were each at significant risk which would have been reduced by encryption technologies. Unfortunately, governments across the world have hampered the development of widely usable encryption in a number of ways. Countries like France and Russia have made the general use of cryptography illegal [77]. The United States government has attempted to hamper cryptographic deployment in several ways [78]:

- by attempting to restrict cryptographic research; it has in the past "requested" that the dissemination and publication of research results be postponed [79];
- by regulating the export of encryption technologies as a munitions under the United States' International Traffic in Arms Regulations (ITAR). Hence, only very weak technologies can be exported or sold on the world market. Many have argued this hampers American competitiveness in the world market for communications and transaction technologies [80];
- by offering a number of substitute technologies that are weaker or limited such as EES, a standard for escrowing keys for government access, or Clipper, a chip for voice communications that is part of the EES. Another example of offering an alternative technology is the DSS scheme which unlike RSA can only be use for authentication and not confidentiality.

There have also been attempts to create weak, or restricted, encryption policies at the international level.

In the recent Bernstein v. United States Department of State case, Judge Marilyn Patel in the Northern District of California denied the request to dismiss the case which has implications on cryptographic export controls and communications. According to the Electronic Frontier Foundation, Judge Patel's acknowledgment that source code enjoys Constitutional protection has implications that reach far beyond cases involving the export of cryptography. The decision holds importance to the future of secure electronic commerce and lays the groundwork needed to expand First Amendment protection to electronic communication [81].

It is unclear how this issue will be resolved, but it is clear that what is at stake is of both a global and personal significance. This technology is important to the development of a global information economy and to the rights of the individual participants.

Commerce

Encryption technologies can enable a number of instruments or tools that are strongly related to trust. However, even if electronic cash, security deposits, digital signatures, contracts, intermediary agents and notaries are technically possible, the legal standing of these instruments will have an immense impact on their acceptance. Many instruments such as digital signatures will be used by real world companies for real world commerce. Hence, a legal understanding will have to be reached before these instruments are used for even a small portion of the many transactions that occur across the globe. Of course, the legal and regulatory system is often far behind the cutting edge of technology, but it is sometimes in step or even ahead of daily business practice - at least in terms of the topics being addressed and not necessarily the quality of the decisions.

Digital signatures and contracts

Digital signatures are perhaps the most widely legislated upon topics in this section and they enable the encoding and authentication of contracts, purchase orders, and the like in digital form [82]. Currently, ten states (including Utah, Washington, and Wyoming) are considering digital signature legislation [83].

California passed the California Digital Signature on October 4, 1995. The Legal Counsel's Notes for the legislation are relatively are straightforward [84]:

"This bill would provide that, in any written communication with a public entity, a signature may be affixed using a digital signature and that in those communications, the use of a digital signature would have the same force and effect as the use of a manual signature if it complies with the bill's requirements∞ ."

And the definition of the signature is informative.

"...
(**1**) It is unique to the person using it.
(**2**) It is capable of verification.
(**3**) It is under the sole control of the person using it.
(**4**) It is linked to data in such a manner that if the data are changed, the digital signature is invalidated.
(**5**) It conforms to regulations adopted by the Secretary of State... .
(**b**) The use or acceptance of a digital signature shall be at the option of the parties. Nothing in this section shall require a public entity to use or permit the use of a digital signature.
(**c**) Digital signatures employed pursuant to Section 71066 of the Public Resources Code are exempted from this section.
(**d**) "Digital signature" means an electronic identifier, created by computer, intended by the party using it to have the same force and effect as the use of a manual signature."

To guide policy makers, the American Bar Association's Section of Science and Technology has written Digital Signature Guidelines to help inform legal processes with regards to this topic [85]. The acceptance of digital signatures will be one of the first indicators of the ability of legal and corporate cultures to adapt to the digital world.

Electronic Cash, Banking, Tax Evasion, Money Laundering, and Fraud

The United States government began minting money because of the incompatibility of independent currencies from different banks or states, making interstate commerce extremely difficult [86]. With electronic cash systems, this incompatibility may no longer be a problem. If the incompatibility of digital instruments were to be a problem, it may not be one best solved by a central entity issuing fiat currency. Standards bodies could attempt to mediate interoperability or third party intermediaries would no doubt extend services for the exchange of electronic currencies.

Speculation about the impact of electronic currencies outside of the control of governments is imaginative and wide ranging [87]. Australian and Swiss banks have been pressured from the international community to remove anonymous accounts and services [88]. Bonded offshore services that employ PGP are easily reachable on the Internet [89]. Companies are using the Internet to exchange IPO information and plan to employ the Web as the vehicle for actual trading.

A major worry for governments, beyond terrorists taking advantage of ecash, is that a significant portion of the tax base would erode with the use of electronic finance instruments. To quote:

"The Clinton administration's reluctance to ease up on export controls for encryption software stems in part from pressure from U. S.. law enforcement agencies, and the owner of a New York-based software company sees heavy lobbying behind the government's desire to regulate content on the Internet: "I think the Internal Revenue Service and the FBI are watching this one very carefully. They wouldn't mind seeing the government set a precedent for deciding what can and cannot go on the Internet." The IRS fears that easy access to cheap and sophisticated encryption software will make income- and sales-tax evasion too easy, and the FBI worries about criminal and terrorist plots hatched in cyberspace, but some observers say government control tactics are too little, too late. A Hudson Institute economist says, "Electronic money gets really interesting when you realize how impossible it is to put national walls around it, mandate the use of national currencies, or require that transactions go through banks... The country will have no practical choice but to rely more than ever on voluntary tax compliance. That means tax rates will have to be kept as low as possible on people and on businesses." [90]"

Some, however, have argued that governmental intervention has driven the capital out of the United States, long before digital instruments were ever considered. For example, Hawley notes:

"State intervention to form, structure, and regulate markets, unintentionally but inevitable produces financial and market innovations circumventing state barriers, as individual units of capital pursue profits and unimpeded growth. Each instance of U. S.. capital controls, along with other national restrictions on the free movement of international capital, only intensified the pace of the internationalization of finance, thereby further limiting the ability of the U. S.. and other states to conduct monetary system and fiscal policy as they had previously [91]."

New digital financial and trust instruments may not prove to be a crushing financial blow to governments around the world. Instead, they indicate the importance of the underlying network infrastructure. Digital instruments are icons of the ever increasing velocity, liquidity, and lack of control of even "normal" currencies, instruments, and ideas that happen to use digital networks.

Conclusion

The evaluation of trust is a necessary component in making any decision. How will trust be decided on the Internet? In this paper, I have argued that trust is simply information. Even with limited information, information of poor quality, or improperly used information, information is employed to make decisions and assign trust. There are tools that are engaged electronically and otherwise to evaluate, manipulate, and communicate information. Cryptographers, economists, policy makers, and participants in the global financial markets are slowly building methods to take advantage of the vast quantity of electronic information. With evaluated sources, including those that manage trust relationships, the market will grow with increasingly sophisticated transactions. In this current phase of research and development, it is unclear to which degree technology, the market itself, or governmental policy will push the actual growth of the market and its tools.

Abstract

Joseph M. Reagle Jr.

Joseph Reagle is a Doctoral Fellow at NYU's Culture and Communication Department where he studies collaborative cultures, including the Wikipedia. For seven years, he was a Research Engineer at the MIT Lab for Computer Science where he served as a W3C public policy analyst and working group author and chair. He worked within the Technology & Society domain and focused on Web policy, security, privacy, and intellectual rights. He has served as a Working Group Chair and Author within the joint IETF/W3C XML Signature, XML Encryption and Platform for Privacy Preferences (P3P) activities. Additionally, Mr. Reagle helped develop and maintain the W3C's privacy and intellectual rights policies (i.e., copyright and trademark licenses and patent analysis).

In 1998, Mr. Reagle took a sabbatical from his responsibilities at MIT as a Resident Fellow at the Berkman Center for Internet & Society at the Harvard Law School; there he worked with the faculty and students of two Harvard/MIT courses and furthered his examination of social protocols (technologies that enable the expression of sophisticated social relationships) by writing and lecturing about Web-data schema design and contract law, computer agents and legal agency, and Internet culture and democratic/anarchist principles.

Mr. Reagle has a Computer Science degree from UMBC and a Masters from MIT's Technology and Policy Program, where he was a Research Assistant at the Research Program on Communication Policy. Mr. Reagle has done short consulting projects at Open Market (electronic commerce protocols), McCann-Erickson (Internet and interactive media) and go-Digital (Internet gambling).

Web: http://reagle.org/joseph/

E-mail: reagle [at] mit [dot] edu

Notes

1. Joseph M. Reagle Jr., 1996. "Trust in a cryptographic economy and digital security deposits: Protocols and policies," Master of Science in Technology and Policy Thesis, Massachusetts Institute of Technology, http://rpcp.mit.edu/~reagle/commerce/commerce.html

2. I borrow the term "trust management" from M. Blaze, J. Feigenbaum, J. and Lacy, 1996. "Decentralized trust management," Proceedings of the IEEE Symposium on Security and Privacy, May 6-8, 1996, Oakland, Calif.

3. A. D. Birrell, B. W. Lampson, R. M. Needham, and M. D. Schoreder, 1986. "A Global authentication service without global trust," Proceedings of the IEEE Symposium on Security and Privacy; R. Yahalom, B. Klein, and T. Beth, 1993. "Trust relationships in secure systems - A Distributed authentication perspective," Proceedings of the 1993 IEEE Symposium on Research in Security and Privacy, pp. 150-164; T. Beth, M. Borcherding, and B. Klein, 1994. "Valuation of trust in open networks," Proceedings of the European Symposium on Research in Computer Security (ESORICS), vol. LNCS 875, pp. 3-18; M. E. Zurko and P. M. Hallam-Baker, 1995. "Secure authorization issues on the Web," half-day workshop at the Third International World Wide Web Conference; M. Branstad, W. C. Barker, and P. Cochrane, 1990. "The Role of trust in protected mail," Proceedings of the IEEE Symposium on Security and Privacy, pp. 210-215.

4. M. E. Zurko and P. M. Hallam-Baker, 1995. "Secure authorization issues on the Web," half-day workshop at the Third International World Wide Web Conference.

5. T. C. May, 1995. "Crypto + Economics + AI = Digital Money Economies," Cypherpunks. The Cypherpunks list is archives at http://www.hks.net/cpunks/index.html

6. P. V. Rangan, 1988. "An Axiomatic basis of trust in distributed systems," Proceedings of the IEEE Symposium on Security and Privacy, p. 205. http://dx.doi.org/10.1109/SECPRI.1988.8112

7. M. Abadi, M. Burrows, and R. Needham, 1990. "A Logic of authentication," ACM Transactions on Computer Systems, vol. 8, no. 1, pp. 18-36; L. Gong, R. Needham, and R. Yahalom, 1990. "Reasoning about belief in cryptographic protocols," Proceedings of the 1990 IEEE Symposium on Research in Security and Privacy, pp. 234-248. http://dx.doi.org/10.1145/77648.77649

8. R. Yahalom, B. Klein, and T. Beth, 1993. "Trust relationships in secure systems - A Distributed authentication perspective," Proceedings of the 1993 IEEE Symposium on Research in Security and Privacy, p. 152. In this paper, the authors provide an interesting table of functions for which principles are often trusted to do: identification, key generation, escrow, non-interference, clock synchronization, protocol compliance, and providing information about others' trustworthiness or reputation. http://dx.doi.org/10.1109/RISP.1993.287635

9. R. Yahalom, B. Klein, and T. Beth, 1993. "Trust relationships in secure systems - A Distributed authentication perspective," Proceedings of the 1993 IEEE Symposium on Research in Security and Privacy, p. 156.

10. T. Beth, M. Borcherding, and B. Klein, 1994. "Valuation of trust in open networks," Proceedings of the European Symposium on Research in Computer Security (ESORICS), vol. LNCS 875, p. 3. http://dx.doi.org/10.1007/3-540-58618-0_53

11. T. Beth, M. Borcherding, and B. Klein, 1994. "Valuation of trust in open networks," Proceedings of the European Symposium on Research in Computer Security (ESORICS), vol. LNCS 875, p. 5. The interesting constraint of this analysis is that any negative experience destroys any direct trust relationship.

12. Op. cit.

13. T. Beth, M. Borcherding, and B. Klein, 1994. "Valuation of trust in open networks," Proceedings of the European Symposium on Research in Computer Security (ESORICS), vol. LNCS 875, pp. 3-18.

14. The term trust is often used in two contrary ways which can be confusing. On one hand, "I don't trust that person," means one has a low expectation of individual assertions being true, and the consequent risk is higher. Risk is the inverse of trust. There is also the concept of, "the less risk there is, the less I need to trust the person." Trust and risk are related linearly. However, the second statement is speaking about the need of trust to overcome some amount of risk. Rather than this being the expectation of an assertion being true, one is expressing the existence of risk (or variance in one's expectation) but that one will act upon the assertion regardless. For most of this paper, I will use "trust" in the first sense.

15. Chapter 5 of R. S. Pindyck and D. L. Rubinfeld, 1995. Microeconomics. Englewood Cliffs, N. J.: Prentice-Hall, entitled "Choice under uncertainty," provides an economic treatment of uncertainty. R. De Neufville, 1990. Applied systems analysis: engineering planningand technology management. New York: McGraw-Hill, provides a much more extensive and practical treatment. For a more theoretical treatment, see P. C. Fishburn, 1982. The Foundations of expected utility. Dordrecht, Holland; Boston: D. Reidel, and P. C. Fishburn, 1972. Mathematics of decision theory. The Hague: Mouton. http://dx.doi.org/10.1002/0470018860.s00707

16. There is a significant amount to be gained by establishing stable long standing trust relationships or certification agencies so as to avoid such calculations for the most part.

17. R. De Neufville, 1990. Applied systems analysis: engineering planning and technology management. New York: McGraw-Hill, p. 330.

18. I must caution that the case in this part of the paper is an example of a perfect information problem. The nature of information is much more general (the whole market). As such, I found it useful to break up the two cases to demonstrate that credit agencies could provide a wide range of information in depth, breadth, and detail regardless of whether the information was theoretically perfect or imperfect.

19. R. De Neufville, 1990. Applied systems analysis: engineering planning and technology management. New York: McGraw-Hill, p. 337.

20. See Joseph M. Reagle Jr., 1996. "Trust in a cryptographic economy and digital security deposits: Protocols and policies," Master of Science in Technology and Policy Thesis, Massachusetts Institute of Technology, http://rpcp.mit.edu/~reagle/commerce/commerce.html

21. Within the confines of the philosophical issue of "in as far as we can know what is true."

22. H. Finney and W. Dai, 1995. "Re: Towards a Theory of Reputation," cypherpunks@toad.com: Tuesday, 21 Nov 1995 15:32:08 -0800. Cypherpunks' archives can be found at http://www.hks.net/cpunks/index.html

23. Certainly, reputation already plays a key part of many Internet communities including Internet Relay Chat (IRC), backgammon servers, chess servers, Netrek, and MUDS. For more details on some these environments, see Joe Pantusoi, Will Moss, Rawn Shah, and Jim Romine, 1996. The Complete Internet gamer. New York: Wiley.

24. In H. Finney and W. Dai, 1995. "Re: Towards a Theory of Reputation," cypherpunks@toad.com: Tuesday, 21 Nov 1995 15:32:08 -0800; cypherpunks' archives at http://www.hks.net/cpunks/index.html

25. R. S. Pindyck and D. L. Rubinfeld, 1995. Microeconomics. Englewood Cliffs, N. J.: Prentice-Hall, p. 157.

26. Op. cit., p. 532.

27. For work on information economics, see R. E. Babe, 1993. "The Place of information in economics," In: R. E. Babe (ed.), Information and communications in economics, Boston: Kluwer, and, J. Eatwell, M. Milgate, and P. Newman, eds., 1989. The New Palgrave: Allocation, information and markets. London: Macmillan Reference.

28. R. S. Pindyck and D. L. Rubinfeld, 1995. Microeconomics. Englewood Cliffs, N. J.: Prentice-Hall, p. 594.

29. Op. cit., p. 598.

30. C. Lai, G. Medvinsky, and B. C. Neuman, 1994. "Endorsements, licensing, and insurance for distributed system services," Proceedings of the Second ACM Conference on Computer and Communications Security, Nov. 94.

31. H. Finney and W. Dai, 1995. "Re: Towards a Theory of Reputation," cypherpunks@toad.com: Tuesday, 21 Nov 1995 15:32:08 -0800; archives at http://www.hks.net/cpunks/index.html

32. Op. cit.

33. R. Axelrod, 1987. "The Evolution of strategies in the iterated prisoner's dilemma," in L. Davis, ed. Genetic algorithms & simulated annealing. London: Pittman; and, R. Axelrod, 1984. The Evolution of cooperation. New York: Basic Books.

34. J. H. Holland, 1975. Adaptation in natural and artificial systems: an introductory analysis with applications to biology, control, and artificial intelligence. Ann Arbor, Mich.: University of Michigan Press.

35. D. F. Midgley, R. E. Marks, and L. G. Cooper, 1995. "Breeding competitive strategies," Working Paper for the Santa Fe Institute Economics Research Program, no. 95-06-052, p. 3; abstract at http://www.santafe.edu/sfi/publications/Abstracts/95-06-052abs.html http://dx.doi.org/10.1287/mnsc.43.3.257

36. L. K. Eisenberg, 1995. "Connectivity and financial network shutdown," Working Paper for the Santa Fe Institute Economics Research Program, no. 95-04-041, abstract at http://www.santafe.edu/sfi/publications/Abstracts/95-04-041abs.html; R. Marimon, E. McGrattan, and T. J. Sargent, 1990. "Money as a medium of exchange in an economy with artificially intelligent agents," Journal of Economic Dynamics and Control, vol. 14, pp. 329-373; D. F. Midgley, R. E. Marks, and L. G. Cooper, 1995. "Breeding competitive strategies," Working Paper for the Santa Fe Institute Economics Research Program, no. 95-06-052, abstract at http://www.santafe.edu/sfi/publications/Abstracts/95-06-052abs.html; I. Karatzas, M. Shubik, and W. D. Sudderth, 1995. "A Strategic market game with secured lending," Working Paper for the Santa Fe Institute Economics Research Program, no. 95-03-037, PostScript version available at http://www.santafe.edu/sfi/publications/Working-Papers/95-03-037.ps; D. Lane, F. Malerba, R. Maxfield, and L. Orsenigo, 1995. "Choice and action," Working Paper for the Santa Fe Institute Economics Research Program, no. 95-01-004, PostScript version available at http://www.santafe.edu/sfi/publications/Working-Papers/95-01-004.ps; and, S. H. Paskov and J. F. Traub, 1995. "Faster valuation of financial derivatives," Working Paper for the Santa Fe Institute Economics Research Program, no. 95-03-034, abstract at http://www.santafe.edu/sfi/publications/Abstracts/95-03-034abs.html

37. K. Kelly 1995. Out of control: The New biology of machines, social systems and the economic world. Reading, Mass.: Addison-Wesley, and, N. J. Vriend, 1994, "Self-Organized markets in a decentralized economy," Working Paper for the Santa Fe Institute Economics Research Program, no. 94-03-013, abstract at http://www.santafe.edu/sfi/publications/Abstracts/94-03-013abs.html

38. J. P. Barlow, 1994. "The Economy of ideas," Wired, vol. 2, no. 3, p. 84; B. Don and D. Frelinger, 1995. "Can the conventional models apply? The Microeconomics of the information revolution," First USENIX Workshop on electronic commerce, New York, New York (July 11-12, 1995), abstract at http://www.usenix.org/publications/library/proceedings/ec95/don.html; and, H. R. Varian, 1995. "Economic mechanism design for computerized agents," First USENIX Workshop on electronic commerce, New York, New York (July 11-12, 1995), abstract at http://www.usenix.org/publications/library/proceedings/ec95/varian.html

39. E. Dyson, 1995. "Intellectual Value," Wired, vol. 3, no. 7, p. 137, and at http://www.hotwired.com/wired/3.07/features/dyson.html; J. Eatwell, M. Milgate, and P. Newman, eds., 1989. The New Palgrave: Allocation, information and markets. London: Macmillan Reference; and, U. Witt, 1989. "The Evolution of economic institutions as a propaganda process," Public Choice, vol. 62, pp. 155-172.

40. M. M. Waldrop, 1992. Complexity: The Emerging science at the edge of order and chaos. New York: Simon & Schuster.

41. Webster's unabridged dictionary of the English language. New York: Portland House, 1989, p. 737.

42. Op. cit., p. 1304.

43. Op. cit., p. 242.

44. C. Lai, G. Medvinsky, and B. C. Neuman, 1994. "Endorsements, licensing, and insurance for distributed system services," Proceedings of the Second ACM Conference on Computer and Communications Security, Nov. 94, p. 170.

http://dx.doi.org/10.3998/3336451.0001.114

45. S. Bendiek, K. Laws, and C. Woehler, 1996. "Brokers and intermediaries," a student group project for class 15.967: Electronic commerce and marketing, Sloan School of Management, Massachusetts Institute of Technology, at http://www-sloan.mit.edu/15.967/GROUP23/group%20project%232.html

46. Credit scoring and credit control : based on the proceedings of a conference on credit scoring and credit control, organized by the Institute of Mathematics and Its Applications and held at the University of Edinburgh in August 1989, L. C. Thomas, ed. Oxford: Clarendon Press, 1992, p. v.

47. For example, C. J. Bond, 1993. Credit management handbook: A Complete guide to credit and accounts receivable operations. New York: McGraw Hill; G. O. Bancroft, 1989. A Practical guide to credit and collection. New York: American Management Association; and, G. Clemenz, 1986. "Credit markets with asymmetric information," In: B. Beckmann and W. Krelle, eds. Lecture Notes in Economics and Mathematical Systems, Berlin: Springer-Verlag.

48. Roy Davies, "Money - History present & future" at http://www.ex.ac.uk/~RDavies/arian/money.html

49. R. Marimon, E. McGrattan, E., and T. J. Sargent, 1990. "Money as a medium of exchange in an economy with artificially intelligent agents," Journal of Economic Dynamics and Control, vol. 14, pp. 329-373.

50. N. Kiyotai and R. Wright, 1989. "On money as a medium of exchange," Journal of Political Economy, vol. 97, pp. 927-954.

51. Holland's classifier system is a form of an evolutionary modeling system; see J. H. Holland, 1975. Adaptation in natural and artificial systems: an introductory analysis with applications to biology, control, and artificial intelligence. Ann Arbor, Mich.: University of Michigan Press.

52. For instance, see P. Panurach, 1995. "The Economics of digital commerce: An Analysis of digital cash, electronic fund transfers, and ecash," ecash@digicash.com: Tuesday, 19 Dec 1995 12:42:23 +0700. In this paper, Patiwat Panurach (e-mail: pati@ipied.tu.ac.th), of the Faculty of Economics at Thammasat University in Bangkok, describes the characteristics of various digital instruments with respect to anonymity, liquidity, velocity, and money-supply.

53. P. Huber, 1992. "On Money," Forbes, vol. 16, p. 144.

54. Op.cit.

55. Originally it was actually processing trades and transactions itself but the SEC warned that it was not a licensed broker and the transactions should be carried out through a legitimate bank or escrow agent. See J. Taylor, 1996. "SEC says brewery may use Internet to offer its stock," Wall Street Journal (March 26), p. B4.

56. SEC-LIVE can be found at http://www.seclive.com/

57. http://www.ai.mit.edu/people/lethin/ecm.html

58. Cambridge Trading Services Corp., "Letters of credit," http://www.cambtrade.com/Letters.html

59. Article 5 of the Uniform Commercial Code deals with letters of credit and can be found at http://www.law.cornell.edu/ucc/5/overview.html

60. R. Hettinga, 1995. "e$: What's a digital bearer bond?," cypherpunks@toad.com: Tuesday, 19 Nov 1995 17:43:15; http://thumper.vmeng.com/pub/rah/dbb.html

61. Dimitri Vulis opined that "The fact that bearer bonds were outlawed suggests that if and when new ways are invented to conduct financial transactions that are conductive to tax evasion (e.g., using anonymous electronic payments), they too may become outlawed." See D. Vulis, 1995. "RE: Anonymity and intellectual capital," http://infinity.nus.sg/cypherpunks/dir.archive-95.11.15-95.11.21/0267.html

62. R. Hettinga, 1995. "e$: What's a digital bearer bond?," cypherpunks@toad.com: Tuesday, 19 Nov 1995 17:43:15; http://thumper.vmeng.com/pub/rah/dbb.html

63. Some mechanisms that are not being used or have been incorporated into other proposals include iKP, Secure Transaction Technology, Secure Electronic Payment Protocol, Netscape's Secure Courier, the Simple Network Payment Protocol, the Hewlett Packard Payment Method, and Anonymous Internet Mercantile Protocol.

64. This information was formerly part of the Frequently Asked Questions file for the Security First Network Bank. This site has been reorganized and this information has been dispersed. Visit the Bank's site at http://www.sfnb.com/infodesk/infodesk.html for more information.

65. C. P. Pfleeger, 1989. Security in computing. Englewood Cliffs, N. J.: Prentice-Hall, p. 132.

66. Op.cit., p. 131.

67. A. Beutelspacher, 1990. "How to say "no"," In: J.-J. Quisquater and J. Vandewalle, eds. Advances in Cryptology - EUROCRYPT '89, Lecture Notes in Computer Science vol. 434, p. 491. http://dx.doi.org/10.1007/3-540-46885-4_47

68. M. Jakobsson, 1995. "Ripping coins for a fair exchange," In: L. C. Guillou and J.-J. Quisquater, eds. Advances in Cryptology - EUROCRYPT '95, Lecture Notes in Computer Science, vol. 921, p. 220. http://dx.doi.org/10.1007/3-540-49264-X_18

69. Joseph M. Reagle Jr., 1996. "Trust in a cryptographic economy and digital security deposits: Protocols and policies," Master of Science in Technology and Policy Thesis, Massachusetts Institute of Technology, http://rpcp.mit.edu/~reagle/commerce/commerce.html

70. The concept of precedent dependency is related to "path-dependence" as discussed by P. Kavassalis, 1995. "Technical change in the televisionindust ry: Between "path-dependence" and new flexibilities," Communications & Strategies, vol. 17, p. 77.

71. See I. de Sola Pool, 1983. Technologies of freedom. Cambridge, Mass.: Belknap Press.

72. See http://www.cpsr.org/dox/wiretap.html

73. These wiretaps would be very convenient. Law enforcement agency could request that all pertinent calls be routed to their own facilities for monitoring.

74. A. M. Froomkin, 1996. "The Internet as a source of regulatory arbitrage," In: Information, national policies, and international infrastructure. Forthcoming, Cambridge, Mass.: MIT Press, p. 331.

75. The significant civil issue is to whom are the default rules useful for? Democratic societies generally strive to make legislation fair and useful to all.

76. D. Post, 1995. "Anarchy, state, and the Internet: An Essay on law-making in cyberspace," 1995 Journal of Online Law, article 3, at http://fatty.law.cornell.edu/jol/jol.table.html

77. See Bert-Jaap Koops' extensive Crypto-Law Survey at http://cwis.kub.nl/~frw/people/koops/lawsurvy.htm

78. Information on all of these points can be found in the Electronic Frontier Foundation "Privacy, Security, Crypto, Surveillance" archive at http://www.eff.org/pub/Privacy/

79. "In 1984, the President had issued a National Security Decision Directive, NSDD-145, which gave the intelligence agencies broad authority to peruse computer databases, for so-called 'sensitive but unclassified information.' A subsequent memorandum from John Poindexter, expanded this authority still further to include 'all computer and communications security for the Federal Government and private industry.' As the government's authority to control access to computerized information for the purpose of protecting national security expanded, the free of flow of information diminished. Stories of agents visiting private information vendors and public libraries soon followed. At the same time, a wide range of other activities by the government further threatened to restrict access to information." Marc Rotenberg's prepared testimony on The Computer Security Act Of 1987 (P. L. 100-235) and The Memorandum Of Understanding Between The National Institute Of Standards Technology (NIST) And The National Security Agency (NSA) Before The Subcommittee on Legislation and National Security, Committee on Government Operations U. S. House of Representatives. May 4, 1989. See http://www.epic.org/crypto/csa/rotenberg_testimony.txt

80. See Electronic Frontier Foundation "Privacy - Crypto - ITAR Export Restrictions" Archive at: http://www.eff.org/pub/Privacy/Key_escrow/ITAR_export/

81. See Electronic Frontier Foundation "Legal Cases - Crypto - Bernstein v. US Dept. of State: Legal Docs" Archive at: http://www.eff.org/pub/Legal/Cases/Bernstein_v_DoS/Legal/

82. Legislation and reports on digital signature may be found at http://web.aimnet.com/~software/industry_issues/1digsig.htm

83. See the Utah Digital Signature Legislation Base at http://www.gvnfo.state.ut.us/ccjj/digsig/

84. California Legislative Counsel's Digest, 1995. AB 1577 Digital Signatures.

85. The guideline is no longer freely available to the public. Information on the guidelines can be found at: http://www.intermarket.com/ecl/

86. See The United States Mint, A Brief History 1792 - 1995 at http://www.ustreas.gov/treasury/bureaus/mint/sub1.html

87. R. J. Anderson, 1995. "Crypto in Europe - Markets, law and policy," Conference on cryptographic policy and algorithms; M. Bernkopf, 1996. "Electronic cash and monetary policy," First Monday, vol. 1, no. 1, http://www.firstmonday.org/?journal=fm&page=article&op=view&path[]=465; A. M. Froomkin, 1996. "Flood control on the information ocean: Living with anonymity, digital cash, and distributed databases," Conference for the second century of the University of Pittsburgh School of Law Symposium; A. M. Froomkin, 1996. "The Internet as a source of regulatory arbitrage," In: Information, national policies, and international infrastructure. Forthcoming, Cambridge, Mass.: MIT Press; Building in big brother: the cryptographic policy debate. L. J. Hoffman, ed. New York: Springer-Verlag, 1995; D. R. Johnson and D. Post, 1996. "Law and borders: The Rise of law in cyberspace," First Monday, vol. 1, no. 1, http://www.firstmonday.org/?journal=fm&page=article&op=view&path[]=468; D. Post, 1995. "Anarchy, state, and the Internet: An Essay on law-making in cyberspace," 1995 Journal of Online Law, article 3, http://fatty.law.cornell.edu/jol/jol.table.html; D. Post, 1995, "Pooling intellectual capital: Anonymity, pseudonymity, and contingent identity in cyberspace," Draft; P. Panurach, 1995. "The Economics of digital commerce: An Analysis of digital cash, electronic fund transfers, and ecash," ecash@digicash.com: Tuesday, 19 Dec 1995 12:42:23 +0700; and J. Shearer and P. Gutmann, 1996. "Government, cryptography, and the right to privacy," Journal of Universal Computer

Science, http://hyperg.iicm.tu-graz.ac.at/government_cryptography_and_the_right_to_privacy_htf;sk=2F074060

88. Reuters (Vienna), 1996. "Pressure on Austrian bank laws," Financial Times (London), (April 12).

89. Quoting from an electronic mail message addressed to the author, "We can execute your financial transactions, move cash from bank to bank, from brokerage accounts to bank, attorney, escrow account, etc. You instruct us by PGP as to what you need accomplished."

90. Investor's Business Daily (1996), "IRS, FBI eye Internet with suspicion," vol. 9 (January), p. B1; summary can be found on Edupage for 9 January 1996 at http://educom.edu/edupage.old/edupage.96/edupage-01.10.96

91. J. P. Hawley, 1987. Dollars & borders: U. S. government attempts to restrict capital flows, 1960 - 1980. Armonk, N. Y.: M. E. Sharpe, p. 170.

Trust in electronic markets: the convergence of cryptographers and economists by Joseph M. Reagle Jr.
First Monday, volume 1, number 2 (August 1996),
URL: http://www.firstmonday.org/?journal=fm&page=article&op=view&path[]=475