A LONG-TERM PERSPECTIVE ON ELECTRONIC COMMERCE
by Eric Hughes

Payment systems and currencies emerge slowly. Successful systems are the result of tremendous energy and investment, which creates high barriers to exit. The investment goes far beyond the technical infrastructure -- the system's networks, payment handling mechanisms and processors as well as the distribution of devices (e.g., POS authorization terminals) and media (cards, bills and coins). It also includes new kinds of transactions, fresh legislation and court cases, and occasional (catastrophic, but not terminal) system crises. Long term, new systems usually lead to behavioral changes, such as lower savings rates and higher levels of indebtedness. They also make room for businesses that weren't possible before.

It takes a long time for financial institutions and ordinary folks to trust and use new payment systems and currencies. The process works on a nearly evolutionary time scale. In the move between major financial epochs, short-term solutions that harness the current infrastructure in new and useful ways act as stepping stones toward long-term evolution.

In January, we described a framework for electronic commerce and examined many of the companies that aspire to create the next platform for such activities. Many of those efforts are likely to be stepping stones. This month, Eric Hughes adds historic, structural and legal perspectives, all of which help frame the larger shifts underway. Hughes, co-founder of the cypherpunks group, has focused his interests in logic and cryptography on the evolution of the financial system to explore its future in the new medium. Now he helps design payment systems through his consulting firm, Open Financial Networks. He spoke on the electronic commerce panel at the PC Forum (see Release 1.0, 2-95).

To Hughes, current attempts at electronic commerce don't offer compelling general solutions over time. Some may work well over the short term and in specific markets, but most of them aren't designed for the new medium, which has strange characteristics. For

BUY PHYSICALLY, PAY VIRTUALLY

INSIDE
ELECTRONIC COMMERCE 1
Intro -- Jerry Michalski 2
APPROACHES 4
The credit-card model.
MONEY 7
Clearing and settlement.
Stores of value.
CLUBS 10
Vetting.
Extending settlement.
FAILURE 14
Keep it small.
Security maxims.
CONFLICT 16
Adjudication; explicitness.
IDENTITY 19
Anonymity.
Digital signatures.
INDUSTRY 23
Multiparty compatibility.
FUTURE 28
Open financial networks.
Unbundling & separability.
RESOURCES & CALENDAR
Names, phones, dates.
example, someone who cracks an electronic-commerce system could, in principle, create counterfeit money that not only would look identical to the real item (after all, it's just a string of bits), but would also be difficult for merchants to refuse. Not so with counterfeit physical currency, which companies can usually identify and refuse to accept.

Hughes offers some general principles for designing future net-based commerce systems. These include: make things explicit, keep things on a minimal need-to-know basis, keep things local, design systems that distribute vulnerability, and separate functions that don't need to be offered together. These principles may lead to a more flexible and functional transaction infrastructure. Companies may be able to unbundle features that currently happen within single systems.

Long run, Hughes foresees many opportunities for new entrants, new market configurations that unbundle and repackage current services. Perhaps most remarkable of all, he describes how the nature of the medium and the technologies such as cryptography it promotes may lead to new kinds of monetary-system stability and cooperation.

ENTRANTS AND APPROACHES

*Sauve qui peut.* Everyone in the computer industry seems to want to get into payment systems. There is broad consensus that money is important to implement right now. Some companies have announced their projects, some have started their projects and a few even understand their projects. If this is a race, it doesn’t look like one yet: Some participants have headed off in random directions, and the rest are milling around near the starting line.

*The glorious future.* I see no current effort among the network payment schemes that has the right properties for long-term success -- none, at least, with enough public detail to judge. The arena is still wide open. This is not to say that all the current efforts will fail, but rather that they won't compete well against better offerings.

*The credit-card model.* Let's get one matter out of the way first. Although makers and users of such systems may or may not realize it, any system that sends credit-card numbers around in the electronic environment is doing this as a stopgap measure until a robust networked payment system comes along. For example, Netscape has developed a protocol called the Secure Sockets Layer (SSL) to allow people to send credit-card information over the Internet in encrypted form.

Credit-card numbers are trivially replicable. Possession of the number is nine-tenths of the ability to use it. Credit-card numbers, therefore, don't have the right information model for the network.

*Not quite the credit-card model.* In a separate project with MasterCard to offer secure transaction services, Netscape will likely take a different approach that avoids exposing the credit-card number at all, though neither party will say much yet. Three other current electronic-commerce projects leverage the credit-card system without shipping around credit-card numbers:
the First Virtual Holdings system, the first CyberCash product and whatever Microsoft and Visa are up to (for descriptions, see Release 1.0, 1-95). Of these, only First Virtual's is in commercial use and moving real value.

Each of these four projects puts itself in the middle of the transaction as a trusted center to prevent the dissemination of credit-card numbers. This intermediation is technical as well as financial: The payment processors must verify each transaction. Visa and MasterCard's existing switch networks may be usable for this function; other entrants have to build verification, clearing and settlement systems.

A single, large intermediary is less stable than a trusted club of intermediaries (for more on clubs, see page 7). A club distributes transaction failure and limits the consequences of those failures. Stability involves risk at a systemic scale, not at the individual transaction. Vendors who wish to succeed long term should closely examine licensing models rather than models with themselves as the single intermediary.

I expect credit-card-based models to enjoy a certain amount of medium-term success for medium-ticket items. The per-transaction fees that seem to be typical of these systems compete favorably with snail-mail postage stamps.

---

**Some credit-card history**

Credit-card use has grown enormously as issuers broadened the cards' scope. The original credit cards, from the 1920s, were two-party cards for gas stations and department stores. These cards, which represented a bilateral credit relationship between the customer and the merchant, were usable only at the issuer's place of business. The first widely used multiparty cards were travel and entertainment cards: American Express, Diners Club, Carte Blanche. These cards, as their name suggests, were good for the needs of business travelers, but they were not originally general-purpose. The first such multi-purpose credit card to achieve wide success, BankAmericard, later Visa, began in 1958. Credit cards are now percolating through some of the last holdouts: low-margin businesses such as supermarkets.

Not as obvious is another clear trend toward decreasing intermediation costs. Initially, redemption of credit-card slips was at about 7 percent discount. Bank card discounts now average about 2.5 percent. We may certainly expect a continued drop in these discount rates. Any new payments venture planning a credit-card billing model that requires more than 2 percent discounts for profitability won't be able to compete for the long term.

Small transactions won't work well in this model. Even aggregating small transactions into larger ones will only very slightly help the situation, because the aggregation must occur between a single buyer and a single seller. The relatively high fees don't support many-to-many interaction at the low level; the transaction fees involved in all those relationships completely swamp the total volume of payments. A purchaser of five cents of service occasionally from a particular vendor is not going to spend thirty-two cents just to make a payment. The vendor is not going to offer even a dollar's worth of credit to his customer if most customers take a
year to accumulate enough due to make settlement worthwhile. A vendor with this profile could have 90 percent of receivables continuously outstanding. Not many enterprises can finance this float, and certainly not the smallest enterprises that are the ones who most need small transaction sizes.

MONEY: DYNAMICS AND DEFINITIONS

Clearing and settlement. Clearing is the process of authorizing a transaction; settlement is the process of completing it. Clearing and settlement are flip sides of a coin. They are sometimes difficult to distinguish, but the actual distinction is useful to remember. Clearing is the undertaking of a legal liability and settlement is the discharge of that liability. Clearing never comes after settlement but may occur before it or simultaneously with it.

The static confusion. One common misunderstanding about technologies broadly known as digital cash or digital money concerns their basic function. Digital cash is a means for transferring value and not a means for storing value. The store of value is with its definer, ultimately. Digital cash is a way of rearranging the ownership of assets, not a way of defining those assets or establishing their worth. Digital cash is entirely a clearing process; it has nothing itself to do with settlement.

The confusion is a linguistic one. Cash, as in paper bank notes, can act as a store of value. The old cash-stuffed-in-the-mattress saving method still resonates, likewise piggybanks. Digital cash is only a store of value when stuffed in a virtual mattress. A piggybanker of this type is not storing money indefinitely but rather delaying the completion of the digital cash withdraw-spend-deposit cycle. Delaying final deposit uses the float as a storage mechanism. Cycling a portfolio of digital cash does store value, even if it doesn’t define a source of value such as the dollar or yen.

Stable stores of value. The oldest stores of value are commodities whose value as storage rests with the human body: a harvest of grain, a herd of cattle. One kind of commodity, specie (gold and silver), is the transition into the second oldest store, namely money. Gold-based fractional reserve paper money used the circulational fact of economic activity to create a new store of value. It kept the old mode, coin transfer, for fallback.

Fiat currency is the ultimate extension of specie-backed paper. The specie backing has completely disappeared. Paper money was the first system to rely upon continued economic activity for validity. Fiat money relies not only upon continued economic activity but also upon the issuing government’s ability to collect taxes. This historical process illustrates an increasingly interconnected trust of humans for each other. The wealth of a modern economy depends profoundly upon specialization and trade. It is only fitting that the money of such an economy should reflect this necessary interconnection.

Just as paper money arose from specie as a transition to fiat currency, so too future forms of money will grow out of the current fiat money system. An analogy: paper currency is to gold as a fluid market in liquidity is to fiat money. In both systems, the quantity of the foundational store of
value (gold, fiat money) decreases as contingent relationships (bank notes, explicit failure agreements) build upon the foundation. That is, promises, linkages and other relationships expand the amount of money in circulation, while the underlying store of value remains relatively constant.

The conclusion of this process is the elimination of fiat currency as money, just as gold has passed away as money. The form that the replacement may take is still uncertain, but it will certainly contain both explicit representations of financial relationships and a sophisticated valuation system.

The composition of money. Money itself is not a technology. Various technologies implement money and thus become a form of money, but these are not themselves money. Specie (gold and silver), coins, book entries, paper bank notes, digital automation and smart cards all act as money, but no single one can lay claim to being money itself.

Even gold is not money itself, but rather its preeminent example. Gold is not currently money in the US, for example. You can't take a Krugerrand to your local Sears and buy a washing machine with it. Gold is also useful for jewelry, dental work and circuit boards. Gold has value as money only when people agree that it is money.

Money itself is a social fiction, like property, political parties, governments, gender and marriage. As a specific example, a corporation is a legal fiction. The socially fictive nature of money is key to understanding its transfer. Social fictions are real, even though they exist only in people's heads. When money moves across electronic networks, no substance called money is in motion. What is in motion is knowledge about rearrangements of money.

Money is ultimately a communications process. Any technology that implements a conserved and transferable quantity is usable as money. The physical properties of gold satisfy these two sufficient properties of money; therefore, gold works as money. These sufficient properties are also design criteria. Creating new forms of money involves two steps: inventing a suitable technology, then persuading society to use it as money.

Where did I get this beautiful car? Payment systems are a necessary epiphenomenon of an underlying economy. Payments themselves always arise from some exchange or transfer. Each payment, therefore, necessarily refers to some relationship outside itself. (Note that the payment vehicle need not carry a reference to the primary economic activity with it.) Representations of this linkage always lie somewhere and last for a certain time. The location and duration of the linking information determine important properties of scale, dispute and privacy.

Every discussion of electronic money inevitably touches upon the whole of economic activity. Trends in the automation of money movement presage those in the rest of the economy. Many of the issues that arise in payment systems arise also in systems for negotiation, delivery, billing and protest. The same principles for making payment systems more effective apply to commerce as a whole.

Synthetic currencies. The transition out of fiat currencies will be much easier with the presence of commodities that act like currencies but which
are not, strictly speaking, currencies. Two developments in the securities industry, derivatives and securitization, point the way.

Derivatives are items of value that are not themselves tangible but are mediated through some agent. An example of an aggregate derivative is an indexed security based upon the Standard & Poors 500. Conceptually, one trade of an S&P 500 index equity makes 500 different trades. The issuer of an index derivative does all these individual trades, but on net flow, not on each index trade.

Contingent derivatives are contracts for purchase or sale under some conditions other than here and now. The simplest derivative is a forward contract, which is an agreement to buy something tomorrow with a price set today. Other such derivatives include options, futures, futures options, interest swaps, strips and all sorts of more exotic arrangements. A corporate financier may use derivatives to stabilize price fluctuation or minimize exchange-rate risk. The same tools can be used to create what are essentially amplified bets on price motion; involvement of this kind led to trouble for Orange County, Procter & Gamble and Metallgesellschaft.

The second trend, securitization, is a general way to turn non-fungible property like home mortgages, business loans and real estate into fungible securities. A securitized asset is essentially a derivative asset based on an underlying basket of similar goods. Securitization allows more of the world’s wealth to exchange in financial markets, which have efficient price discovery mechanisms. It leads to more efficient capital allocation as well as more information about the economy.

A synthetic currency is a stabilized derivative asset based over as broadly a secured base as possible. The ideal synthetic currency's goal is not speculation but value maintenance. It should seek to minimize price fluctuation by targeting a broad market average. No single enterprise will be able to pull this off. The issuer of a broad synthetic currency will doubtless rely upon many other issuers. Derivative assets may derive from other derivative assets, and so on.

Synthetic currencies truly thrive with small value transactions. The cost of negotiating and processing a foreign exchange trade for each small transaction would be overwhelming. Commerce denominated in synthetic currencies avoids this issue by parceling out this trading function to the issuer of the synthetic currency. In addition, denomination in a synthetic currency avoids some of the fluctuation risk, particularly if present on both sides of the balance sheet. This application provides a potential initial market, namely, low-level trading where the exchange risk and transaction costs currently prevent commerce.

Non-inflationary currencies. The word "inflation" has different meanings in the phrases "price inflation" and "currency inflation". The two meanings are historically related but not identical. Price inflation is just a synonym for price increases. News reports are usually of this kind of inflation. Currency inflation, however, is an increase in the total number of nominal units of the currency.

The real value of any currency is unrelated to the total number of available accounting units. This variability of nominal value is a source of
great mischief. Under the current fiat money regime, the issuing government can decide at any point simply to print more money and assign it all to itself. (It’s not always this blatant, of course.) In the long term, an inflation of the money supply by 100 percent is a 50 percent tax on the real value of currency holdings. In the short term, the illusion of freer money stimulates economic activity. The transient effects of a credit relaxation are much more significant now than in a more highly networked future where the money illusion dissipates faster.

Inflationary currencies were at the center of last year’s Brazilian presidential elections. The new president, Cardoso, is the former finance minister who was responsible for bringing the inflation rate down from three digits to two digits. The poor overwhelmingly voted for him over even a strong leftist labor candidate, who nominally had their interests more at heart. In truth, Cardoso broke the crushing effective tax on cash which is the means of savings of the poor, assuring his election.

Here’s how to create a non-inflationary currency: A currency issuer announces in advance the total number of nominal units of value and makes an initial disbursement to currency holders. From then on, all transactions in the currency are zero-sum. The public can continuously verify that the number of nominal units is constant, either by legal assurance or by a function called remote auditing (see page 25). Unlike government currencies, the issuer does not simply create more money.

If the non-inflationary currency is a synthetic currency, the real value of one unit of currency increases at the same rate that productivity rises in the economy. Technological progress increases real wealth. One unit of non-inflationary currency pays real interest (not nominal interest) just by sitting around.

Power shift. The rapid expansion of the foreign exchange market has usurped a long-held power of governments to control exchange rates. Inexpensive and reliable long-distance telephony available in the 1960s allowed New York-to-London currency trading in real time rather than with periodic price fixings. The market responded more quickly to disparities in real economies and to various governments’ fiscal misbehavior, two trends that should continue. Automation further increased the size of these capital flows. As technologies accelerated international capital flows, governments lost the ability to set exchange rates between their currencies.

Another such transfer of power is imminent. Financial institutions will soon be able to create a store of value that can outcompete government-issued currencies in retention of value and in swiftness of transaction. The real issue then at hand is whether the governments of the world will allow for a smooth transition.

CLUBS: DISTRIBUTED EFFICIENCY

Respect for the past. I have always marveled at how strident improvers of both technology and politics consistently ignore the past. This ignorance is not primarily a lack of facts: Both reformers and the purveyors of new software have knowledge of the events of history. The ignorance is rather of the motivations and the underlying logic of the various social relation-
ships of the past. Are we really to believe that our forebears were incapable of competent effort, that they did not do the best they could in the situations they faced? Dismissal of the past belies a basic disrespect for people who had passions for excellence equal to our own.

The shiny brightness of the new obscures the old; the new seems triumphant over the old. The new is always, however, an overlay on the old and never a complete replacement. In particular, the bedazzlement of the new aborts a question of tremendous importance: "In what way is the past still relevant, and in what way is it not?"

A moment of perspective. Commercial banking has been around over 600 years. Computers are less than 60 years old. Microcomputer software companies are 20 years old and still reinvent the wheel. Assuming a convergence, who do you think will learn the other's business first? A hint: Don't bet on the arrogant.

Join the club. One defining characteristic of payment systems is the extent to which club membership determines participation. A transaction club is not merely a web of bilateral or correspondent relationships; rather, members of the club are peers in a single group. For example, a bank demonstrates sufficient capitalization and robustness to join the Federal funds-transfer system. Similarly, high-value systems such as CHIPS, SWIFT all have rules governing their members' stability, as do stock exchanges.

Membership in a club correlates with identity. All club systems use accounts -- records of the system's relationship with various identities. Club members' intrinsic properties matter: nostro and vostro balances, credit lines, payment history and capitalization.

Users of paper currency and coins, on the contrary, do not form a club. Similarly, promissory notes, unregistered bond certificates and other bearer instruments are freely exchangeable without prior arrangement. Possession of an instrument correlates with proxy, that is, with someone else's identity. The value of a dollar bill, for example, does not rest with the identity of its holder; it derives from the stability of the United States government. Likewise, a bearer bond gets its value from the solvency of the issuer. Every use of proxy eventually resolves to some direct relationship. Proxy is an indirectness of identity.

Extending settlement. Every transaction club must have some means for doing clearing and settlement. These do not, however, have to be the same means. While clearing may be local to the club, settlement frequently occurs externally in another club. Parties undertake obligations in the local clearing club but may discharge those obligations by moving value in a different club. For example, CHIPS settles its dollar trades at the Federal Reserve.

Settlement arrangements do not infinitely regress, however, because the transaction clubs operated by the definers of value do their own settlement. For the US dollar this terminus of reference is the Federal Reserve System. Money on account with the Fed is money by definition. The Fed doesn't need to offload its settlement to another organization. In some sense it simply couldn't, because that would change the point of origin. Foreign currencies each end at their respective central banks or currency
boards. Other definers of value exist such as the Fed (again) for government securities and the Depository Trust Company for equities.

The structure of settlement divides cleanly along the distinction of definitional assets and derivative assets. Nevertheless, money on account at the Fed is not the same as money on account at, say, J.P. Morgan. There's no contingency at the Fed -- none, at least, that wouldn't give you bigger problems to worry about. Funds at J.P. Morgan, though, are contingent upon the solvency of J.P. Morgan. Yes, the likelihood of a J.P. Morgan bankruptcy is extremely low, but the contingency is still there, as Citibank's recent close call indicates. Chains of contingency grow as settlement arrangements stack on top of each other; not all of these links are as strong as J.P. Morgan's would be. The risk is larger toward the periphery, so transactions' characteristic size will dwindle toward the edges.

Properties of payment systems

The financial structure of payment systems can be confusing. Each of the following axes is mostly independent from the others. The array of actual systems becomes easier to understand by examining these few basic properties.

The debit/credit axis refers to the order in which the intermediary receives and remits payment from the two parties to a transaction. In a debit system, the intermediary receives funds before remitting them; these are also called pre-paid systems. A credit system remits payment before receiving it.

The immediate/delayed axis is the time lag between clearing and settlement. There are two characteristic times here, one for payer/intermediary and one for payee/intermediary. Float and credit cost matter here. Also, long settlement times increase risk.

The gross/net axis is a relationship between clearing and settlement. In a gross payment system, each transaction cleared generates its own settlement action. A net system batches together multiple transactions (payments, receipts or both) for a single settlement. Net systems have lower operational costs because they perform less settlement but are riskier because of an unavoidable settlement lag during the accumulation period. This interval is a potential failure point.

The anonymous/identified axis is the degree of identity substitution present. Anonymous systems work well for low-value transactions. High-value transactions are riskier, so they require more robust (and expensive) proxy services, possibly involving identity.

The fixed/fraction axis is the fee structure of a transaction. Fixed fees are appropriate for paying for the infrastructure; fractional transaction amounts are appropriate for risk and short-term credit fees. As transaction systems become more technically efficient and technology reduces failure risk, the fee percentage will drop.
The resulting structure is a hierarchy of payment systems, each settling one level higher and the top settling itself. This structure is inherent in the nature of fiat money and will endure for some time. The parameters of this structure can change, however -- for example, the depth of the tree and the ratio of principals to proxies. A big advantage of nested clearing arrangements is encapsulation of failure, which eases the creation of local clearing arrangements.

Efficiency. Payment systems compete against each other for transactions. The costs of setup and entry are extremely high, so the market for payment systems is not fluid. Every new system must exhibit great benefits to succeed, either by offering entirely new capability or by charging significantly less than existing services. Competition between entirely new services, however, will be fierce. Direct system efficiency is much more likely to carry the day in a new environment. New enterprises may seek advantage in both routine and exception processing.

Two of the tools for future efficiency, host computers and wide-area data communications, have not yet fully realized their complete effects. Furthermore, we have only seen hints of other new technologies' potential effects, including smart cards, PDAs and wireless networks. Modern cryptography is one such tool that may make payment systems substantially cheaper to operate. Cryptography generally does not itself create efficiency; it establishes a foundation for other techniques and new ways of business.

Scale of the club. Transaction clubs exist because they’re more efficient than direct bilateral arrangements. Club members benefit from common and shared rules for exception processing, as well as more efficient vetting. The club’s center, however constructed, vets potential participants, which reduces or eliminates participants’ counterparty vetting requirements.

The club itself is an intermediary for ascertaining salient properties of potential counterparties. The essential subjectivity of this process is important. A party’s solvency is useless if a potential counterparty doesn’t have an assurance of it. By communicating knowledge of solvency, clubs allow larger scales of interaction than direct arrangements.

Yet no club can scale past its idiosyncratic maximum size. The vetting process, which includes club-specific assumptions and requirements, excludes potential members for cause. The ability to presume something is the reason-for-being of the club. Other unqualified parties who might want to join the club, even those who would benefit, can’t. The reasons for exclusion are fundamental; without them, the club is not of value.

FAILURE: SCALE, SECURITY AND IGNORANCE

The price of success. The hardest part of creating new payment systems is handling failure well. Payment systems that don’t will themselves fail, even if the service is free. Every new system must be at least as robust as the system it replaces.

Failures happen both accidentally and fraudulently; some kinds are expected, some are not. One common failure is simple non-payment of debt. Handling expected failures should be simple, but unexpected failures are always expensive.

Release 1.0

31 March 1995
The upper bound on aggregate transaction fees is in practice a small percentage of the transaction amount.\(^1\) The cost of a failed transaction, however, can be enormous. First at risk is the entire amount of the transaction. Next is arguing over fault and blame, which involves staff and often lawyers; for small transactions, this cost is always larger than the transaction amount. Cascading transaction failure may lead to credit cost, loss of business, bankruptcy or even court-ordered damages worth more than the enterprise itself.

People are skittish about unreliable money systems. Too many breakdowns, which is likely not very many, reduce customer confidence in the system to unsustainably low levels. An unsellable system is a lost investment.

**Scale variance.** In a working and deployed payment system, accidental failure is more common than purposive failure. In a badly designed payment system, however, purposive failure quickly leads to massive fraud, system failure and acrimonious lawsuits.

The dilemma of every new payment mechanism is that a small trial deployment cannot accurately demonstrate the security of a full-scale system, and that a large deployment is not a trial but a product. A potential defrauder has negative incentive to point out flaws during a trial. Should a bank deploy a flawed system, the defrauder's income stream from fraud would be much larger and longer lasting. Thus payment systems are not testable in advance but only after implementation. The importance of understanding the systems thoroughly up front is difficult to overstate.

Any payment system, no matter how unwieldy or expensive, is better than no payment system for certain people and certain types of transactions. The initial success of a payment system says nothing about its long-term viability or its growth potential. Rapid initial growth is no proof of a concept's excellence but rather evidence of pent-up demand.

**Optimist for a day.** Any idiot can design a payment system that works when nothing goes wrong. Here's one: I'll write down how much money I have and you write down how much money you have. When we do a transaction, I subtract the amount of money I'm paying you from my balance and you add it to yours. When nothing goes wrong, this system works just fine.

I immediately hear complaints: What if I just change my balance? Well, something went wrong.

**That pin-striped look.** Bankers are notoriously conservative. Rather than taking this comment as an opportunity for stereotyping, we might rather view it as a starting place for understanding. Banks are intermediaries. They get in the middle of interactions. These intermediaries do not arise for specific transactions but persist through time. One does not instantiate a bank to perform a set of transactions as one might a corporation to make a movie or to build an office high-rise. Banks are a shared resource.

---

1 The three most common transaction-fee structures are a fixed fee per transaction, a fixed fee per year or month, and a fixed percentage of the transaction amount.

*Release 1.0* 31 March 1995
The result of shared mediation is that banks become centers. As long as everything works normally, there is no particular concern with centrality. Nevertheless, things go wrong. A failure in the center is much larger than a failure in the periphery. The notion of adequate responsibility has much greater consequences for banking than for other endeavors.

In the same way, banks as a group form a trustworthy network. Not only is individual reliability important, but also the robustness of the banking system as another center. Hence stem periodic concerns over various kinds of systemic risk.

Credit-card security. Credit-card use at the point of sale has changed little since inception. The customer presents a card; the clerk hands back a bill; the customer signs it. Electronic capture of the transaction information has changed the efficiency of the point of sale but not the basic interaction of the card with the customer. Possession of the card is still the basic security mechanism at the point of sale. At the outset, this was a perfectly reasonable process, but it has not scaled gracefully.

Credit cards have seen a steady increase in generality and use. As a result, the utility of fraud has increased as it became easier to use pilfered card information to defraud for goods. A veritable technological arms race is afoot: Cheap reproductions of fake cards have led to the use of holograms (now themselves pirated in southern China) and cardholder photographs. The card companies currently have the upper hand. Credit-card fraud, which peaked in 1992, has decreased for the last two years. Two recent changes led to the bulk of the decrease. The first was requiring the customer to activate the card after it has arrived. The second is pattern-recognition to detect unusual spending.

A plastic credit card is still, however, information in a special carrier. The underlying information offers no toehold for any durable security. Fraud countermeasures thus rely entirely upon physicality, as card countermeasures illustrate. Spending-pattern analysis depends upon geographic knowledge of business locations. Even changing the card number invokes a physical action; the customer must receive a new card in the mail at the very least.

All this physicality completely disappears in commerce on electronic networks. Card numbers retain a long-term vulnerability precisely because they are bare data. Surely these numbers will be ciphertext during transit, but eavesdropping is only one of several modes of unauthorized copying. Kevin Mitnick, for example, had obtained Netcom's entire credit card database. Mitnick, however, could just as easily have been a disgruntled employee or a corrupt business owner or an unethical security contractor. The basic malfunction, shared with passwords, is that authorized users must completely reveal their access information at each session.

Willful ignorance. One rule of optimization is that an enterprise should know only the information it needs to conduct its business. Keeping any other data is simply a cost sink. The principle of willful ignorance is a great clarifier of potential designs. It continually forces the question of the real nature of a relationship and of the minimum information required to represent it. Much data in enterprises exists only for handling failure. This data for failure can take several forms, each with different efficiencies.
Security maxim

Security Maxim A. Security is subjective. Security is not just a state of invulnerability. Security is a knowledge of the fact of invulnerability. Different people will experience different levels of security at a given site. For example, an online-service operator has direct knowledge about security measures; its customers do not have such access and hence have a reduced assurance in the security of the system. Note that users generally keep their more valuable data on their own machines.

Security Maxim B. Security is invisible. When it's working perfectly, nothing unusual happens. Security, however, is indistinguishable from undiscovered vulnerability. This principle has some disquieting consequences for the funding of security measures; after all, if it's not broken.... As my friend Matt Blaze is always saying, security is not a feature. People buy computers to gain productivity, not to have a bit of impregnability on their desktops.

Software, like the proverbial iceberg, is already mostly invisible. Customers require a personal, subjective assurance of security, but invisibility interferes. The big obvious vault in the lobby is a standard bank technique for making the security of the enterprise visible. Making apparent the security present in personal financial software is going to take some doing. After all, anyone can put cute little icons of locks on the screen.

Security Maxim C. Security is predictability. Security is knowledge about properties of a system; knowledge not about specific futures but rather about the characteristics of all possible futures. There are many kinds of unapproved outside access (e.g., Trojan horses, password cracking). Denial of service, however, is when authorized users cannot use the system. The phrase "denial of service", for its part, camouflages that not only can intruders crash your system, but so can your operating system vendor.

Verbum sapienti. And Microsoft wants to be my banker?

By far the most common extra data is a real-life identity for an account. Recourse to a bodily or corporate identity becomes a default mechanism for failure handling. Enterprises that require identity to handle failures try to get the courts to subsidize much of their cost of enforcement. Yet the court system is far more expensive for everyone than explicit procedures to handle the contingencies for failure directly. Also, the costs of using a court system increase rapidly in an international context. The relative cost is especially prohibitive as transaction sizes decrease.

Explicit representation of failure contingencies yields greater effectiveness than leaving failure modes unexamined and letting the legal department sort things out. Consider a relationship that transfers failure modes automatically to a different context. A guarantor, for example, would pay immediately if something went wrong. The shift from a high-speed transaction system to a lower-speed resolution system itself adds value by splitting regular action from exceptional action.
Willful ignorance in the context of planning failure modes means ignorance of everything except exactly what will happen in case of failure. The result is a local system specified as completely as possible. Each exception generates failure notification for treatment elsewhere. Exception passing must end somewhere, but when a system can detach exceptions, exception management can then become a shared service and an intermediary in its own right. The aggregate economic gains from reducing the total cost of handling failures may be quite large.

The effects of willful ignorance vary with transaction size. For small retail transactions, the cost of failure handling far outweighs the transaction fee. Complete transfer of error handling may be more efficient here. For large wholesale transactions, failure handling might well involve identity, since large sums are at stake.

_Dwelling on failure_. Why concentrate so much on failure? Isn't it so... or, depressing?

**CONFLICT: COSTS AND STRATEGIES**

_Adjudication_. The cost of conflict resolution can quickly overwhelm a payment system. All else equal, a system with a more efficient adjudication mechanism will out-compete a lesser one. The major cost of adjudication is people's time. Eliminating conflict _a priori_ and making resolution mechanizable will reduce conflict costs. Increasing the determinism of resolution also reduces the occasions for conflict. Solving problems in advance is better than untangling a mess later.

The rhetoric of court argument is the same as the rhetoric of bickering except a judge watches to filter invalid statements. Questions of fact pertain to what did happen; questions of law pertain to what shall happen. Two parties in dispute may stipulate\(^2\) that certain events happened; this agreement narrows the range of contestable issues. An increase in stipulation is a decrease in conflict cost.

The best way to get more stipulation is for the parties to make them during the natural course of their interactions, within a defined protocol. At each step in an interaction, each party acknowledges all that has gone before. Digital signatures convert these acknowledgments into stipulations, and the protocol can advance. The only factual matter under dispute is the most recent message, which the sender can repeat if need be.

By the end of a protocol, each party will have completely released the other from any obligation arising during their interaction, obviating the need to store entire transcripts. In multiparty transactions where one party has a claim against more than one other party, stipulations limit the explosion of claim possibilities.

Questions of law are almost all subordinate to an underlying contractual relationship, which specifies what happens under various circumstances.

\(^2\) A stipulation is a statement that says "I acknowledge that X happened and I give up any right to contest the issue of fact X."

_Release 1.0_ 31 March 1995
The relationship may be explicit or derive from a legal default. Issues of law, regardless of their origin, are pragmatic; they address the question of what happens next. When particular contractual relationships become widespread and constant, they often pass into the law of the land, as did the Uniform Commercial Code. Members of a transaction club agree to use their own rule book to decide what happens once issues of fact are not at issue. These rule books are much more specific than statutory law.

The link between a contract and a transaction under it always has some representation. A payment on account, for example, has the account number, which refers to a particular customer and -- implicitly -- to the standard customer contract. To optimize adjudication, contracts will need an exact representation that mates closely with the transactions under it. The contractual relationship must ensure the validity of digital signatures and must provide an anchoring antecedent to the various promises, warrants and guarantees in the protocol itself.

The principle here is explicitness in representation, first in agreement and then in acknowledgment. Each expectation left implicit is one matter more for dispute.

**Encoding and scale.** Invariability in any commerce standard will become a problem as business practice changes. Companies will wish to change the way they do business with each other and, further, will wish to change outside the standard scope of variability. Transaction clubs centralize but do not eliminate this issue by setting rules. A fixed standard would be not only of encoding but also of specific interpretation. New interpretations require non-standard usage. The very fixity that makes standards useful will become a confinement.

Standards at the level of encoding are clearly necessary, as are those at the level of generating an interpretation. The risk, though, is to standardize the nature of the relationship itself. Certainly much benefit accrues from having the availability of standardized relationships, but the difference between availability and requirement is enormous. A level of indirection produces the ability to refer to a standard relationship; these benchmark relationships would be explicit in a different part of the standard. The encoding of relationships will be difficult to do right, but at least the arguments will be about the nature of the encoding and not the nature of the relationship.

This flexibility permits a control over policy necessary to good management. Concerning failures of compatibility, there's a difference between "I don't understand this message" and "I understand it but don't know how to deal with it." The former is a systems problem and the latter is a policy problem. A lack of explicit semantic representation is a technical hindrance on the development of new policy mechanisms. Mixing the semantic (meaning) with the pragmatic (action) is a profound flaw.

**Explicit representation.** The general principle of explicit representation recurs widely and in many contexts (see Release 1.0, 10-93). Human time is an expensive resource. Computers cannot manipulate the implicit relationships embedded in the pragmatics of systems nearly so well as they can explicit representations designed for parsability. Handling implicitness always requires more human involvement somewhere. Of course, humans also deal worse with the implicit than with the explicit.

*Release 1.0* 31 March 1995
Implicitness creates misunderstanding, which leads to conflict. Increasing explicitness is a good way to reduce conflict. Equally important, imprecision limits size. The wider the system, the longer the chain of communication. Each link only implicitly understood raises the probability of conflict. The cost of dealing with conflict increases and limits the characteristic size of a system.

Prospects for EDI. Initial successes with Electronic Data Interchange were in captive supplier markets such as the auto industry. The dominant purchasers dictated that suppliers would use EDI, and lo, there was EDI. While the idea of electronically exchanging business data will clearly succeed, EDI may well not scale out of its existing high-level segment. Growth will continue along bilateral lines, but may never scale into the multiparty arrangements that are the norm outside particular sectors. The "last hop" of retail customer integration will progress especially slowly, given the vicious circle of a high cost to enter, low demand at that price and subsequent lack of software to lower the access barrier.

The idea of EDI is compelling enough and the execution of EDI constrained enough to make an opportunity for another entrant. Such an entrant would have to be lightweight, have low barriers to entry and a competitive market in implementations. Microsoft congenitally will be unable to do this; the OpenDoc consortium might provide a model for the necessary cooperation. Unix vendors understand open standards, but are only now learning about shrink wrap and ease of installation and upgrade. The time is perfect now for a more flexible open standard because existing vendors have little proprietary effort to preserve. Barring this, though, perhaps EDI will win because no one else showed up.

IDENTITY: ONE IF BY PROXY...

Transfer of identity. The floating cyberspatial identity of digital signatures offers an enormous opportunity for cost savings. It can also selectively mask parties' identities in a transaction, by design or as a byproduct of the search for cost savings. Anonymity has many useful forms.

<table>
<thead>
<tr>
<th>The principle of separability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public-key cryptography offers a general capability to informational systems. Take a set of data with structure and partition it into secret pieces and public pieces. The principle of separability is that you can publicly prove relationships between the secret pieces and the public pieces without revealing the secret pieces. As a basic example, consider the digital signature. The private key is secret, but a digital signature proves the possession of a private key matching a given public key. Unlike a password, a holder can exhibit proof without exhibiting the secret.</td>
</tr>
</tbody>
</table>

A digital signature can entirely represent a proxy relationship with a club member. Complete replacement of identity generates a substitution proxy. In this situation of complete substitution, the proxy becomes an agent not only for a financial relationship but also for identity. The financial
aspect, however, is the only salient one for the counterparty. The proxy provides an assurance that the party can fulfill obligations. The counterparty doesn't require the identity of the first party for recourse because the proxy is public and has agreed to stand in place for dispute. Note, however, that this situation does not apply to transactions between club members. Within clubs, each party acts for itself.

Digital cash is exactly this transfer of identity taken to its extreme. A more accurate term for a certificate of digital cash is a digital bank note, a promise that a bank makes to pay. The note need not contain the identity of the holder at all, because the bank has entirely substituted its own solvency for that of the holder. A complete proxy of this nature achieves counterparty anonymity. Liquidity substitutes for identity.

Proxy can generate two aspects of anonymity: anonymity by accident and anonymity by design. Anonymity by accident is the natural result of substitution proxy. Replacement of identities can lower the price of the transaction; the anonymity is a side effect.

Anonymity by design comes from a desire to eliminate the ability to link parties in a transaction. The goal is issuer anonymity (when your bank doesn't know who transacted) in addition to counterparty anonymity (when you don't know whom you've just transacted with).

**What is a thing?**

Identity and persistence are dual. Focusing on an object as time rushes by, we see its identity outside time. Focusing on the passage of time as the object remains constant, we see its persistence through time. Every persistence generates an identity. The lifetime of the identity is the length of the persistence.

This equation is hardly a pedantic exercise. No economic interchange happens instantaneously. Even the few seconds of a simple cash purchase require physical proximity. For those few seconds, each person recognizes the other by sight. Ten minutes later the two retain no memory of each other; nevertheless for those few seconds each person had an identity for the other. In fact, an otherwise anonymous account, used several times, generates a persistent identity.

At the opposite extreme, humans each have an identity that persists their whole lives. We predicate all legal relationships upon the ability to have recourse against some identity when things go wrong. The risk in dealing with a fly-by-night operation is precisely that it may not persist long enough to seek recompense if necessary; in other words, it has an insufficiently long identity.

**Sign on the bottom line.** The use of digital signatures for adjudication ultimately requires a connection between the digital signature and the human parties in the relationship. This connection consists of two fundamentally different kinds of links: a technical link between signatures and a social link between a signature and a human. The maker of a digital signature is the technical holder of the signing information -- the private key.
A party in a transaction requires a social assurance that this holder is a true counterparty. Hence, both kinds of links are necessary.

Digital signatures create a persistence that binds multiple communications by the same holder together. A party may verify that the signer of the current signature may be the same as the signer of some previous signature. This persistence is a full-fledged, completely cyberspatial identity; it is the identity of the signature as itself. This digital persistence is the root of all cryptographic identities.

Attestations\(^3\) link a digital identity to some other identity. Each of these two identities could be a digital identity, a personal identity, an account, or some other persistence. Restrictive attestations may clarify the exact relation, add time bounds, etc., but the underlying function is to link identities.

One proposed structure for these attestations is the X.509 Certification Hierarchy. Another is Pretty Good Privacy's so-called "web of trust." Neither of these attempts are anything approaching a general solution; both are particular solutions to specific problems.

The nature of the attestor depends on the purpose of the digital signatures. For transactions, that purpose is to prevent repudiation. If a party tries to repudiate a statement, the issue becomes a conflict and enters arbitration. The complainant must convince the judge that the signature is valid and offers attestations as proof. These attestations must be acceptable to the judge.

The most direct way to convince arbitrators about signatures is for them to have participated in the attestation process initially. Various suggestions are floating around for the "right" attestation agency: the Post Office, notaries, certification hierarchies, acquaintances. None of these can be correct in all cases. For legal purposes, the adjudication function must be the origin; delegation happens from there.

One straightforward way to attach an identity to a signature is to publish widely. A company who wants to distribute their public key can print it on all their sales literature, manuals and help cards. The communication to the public is also communication to the arbiter.

Other attestation mechanisms are appropriate for other purposes. The liability issues are subtle and immense. Both reward and risk are available in abundance.

Identity on a chip. Online services can authenticate their users by the technical facts about connection. In the simplest case, an online service knows which modem the user is calling in on. Because the online service maintains complete administrative control over the connection method, it

\[^3\] An attestation is a statement of the form "I claim that Z is true and I agree to take responsibility for this claim." For example, when Alice makes an attestation for identity about Bob's public key, Alice says "I claim that X is Bob's public key. If I'm wrong, sue me."
has an assurance that no one is impersonating a user, assuming no password compromise. Similarly, on private networks, all the participants know that anybody on the network has authorization to use the network. Participants can use network addresses as identities. Both these examples illustrate closed networks. The Internet, on the other hand, is an open network; Internet users will require digital signatures to authenticate themselves.

If digital signatures are to be any more useful than improved passwords, private keys must be hard to compromise. System reliability and security will remain inadequate for some time to come, so the desktop system is an inappropriate place for secret signing information. Since the signing information requires a digital storage medium, security requires another piece of hardware.

Candidate technologies include PCMCIA cards, smart cards and PDAs. Smart cards have not only limited processing capacity for this purpose but also a complete lack of sockets in machines. PDAs would work fine, but they’re too expensive for this single use. PCMCIA cards seem the best alternative. Their sockets are now standard in laptops and their form factor has enough room for sufficient silicon. Unfortunately, one maker of PCMCIA cryptography devices, National Semiconductor, has saddled its most functional devices with Clipper chip cryptography.

An impending collapse. Payment systems divide into retail and wholesale segments, corresponding respectively to low-value consumer transactions and to high-value commercial and interbank transactions. With the growth of open data networks, primarily the Internet, the most meager equipment can readily become an inseparable part of the payment system’s technical infrastructure. Distributable security technology based on public-key cryptography is sufficient for the highest-value transfers and is practical in hand-held devices. Some of the distinction between high and low is ready to disappear.

INDUSTRY: MAKING IT ALL HAPPEN

Multiparty compatibility. A software product launch is a two-party negotiation. Software vendors write products for a given operating system and persuade consumers to buy it. This is a standard retail transaction. Prospective sellers of a money system, however, have a four-party negotiation: the money system vendor, consumers, merchants and financial intermediaries. That is, there is one seller and three buyers, each of which has different system requirements.

Consumers have microcomputers or PDAs or smart cards. Merchants vary widely by size; each will have different requirements for operations size. Banks and other intermediaries require extremely reliable transaction processing systems. No single vendor will be able to meet all these requirements. Anybody who expects to provide the entire technology infrastructure for a new money system will fail outrightly and completely. Success will require partnerships at the very least. Open standards will be even more likely to succeed.

This criterion against isolation cuts out several would-be contenders from my book right away: Netbank, DigiCash and the academic projects NetBill and
Fearful symmetry

As mentioned in Release 1.0, 1-95, Mondex is a joint venture of a couple of British banks to do an electronic cash system. The customers hold smart cards whose tamper resistance prevents a suitably equipped opponent from simply going inside the card and changing the balance written there. The Mondex consortium is also looking at ways to use its system over electronic networks.

Mondex won't succeed in its current incarnation. The reason is entirely technical: Their security uses only DES, a symmetric cipher, which means that the same key must exist on both sides of any link. That means that the key necessary to charge up a Mondex card must exist within that card. The key that provides security between the Mondex system itself and its merchants must exist in the merchant terminals. Not only are technical attacks feasible, but also simple theft of a key from the center. Once a key is out, it is replicable in the same way that credit-card numbers are. If the system remains unchanged before full deployment, expect a spectacular and messy public failure.

Banker's position. Today's financial industry is still in a good position to be both technology and financial provider for electronic commerce. Its existing expertise in payment systems is still unduplicated in the software industry. This expertise is critical to making large systems efficient and competitive. Banks are developing their own capacity for software development as well. Perhaps most critical is that banks already control the current payments system.

Already online. Any company desiring to offer financial proxy services must have some relationship with its customer. Companies without such relationships will need either to develop them or to buy them. Banks have an existing customer relationship, but they've been unsuccessful in moving that relationship online. The existing online-service providers have an enormously valuable asset here. America Online and CompuServe both have large customer bases who see their providers as gateways to the outside world. Adding a financial component to that conduit is a straightforward extension of customer perception.

Home banking didn't succeed because its price was too high for a single-purpose online service. The advantage AOL, say, enjoys is that one online connection provides access to many different services, at a price comparable to home banking. A bank developing a comparable technical communications infrastructure is not going to do so as efficiently as leveraging the existing online services or the Internet.

Remember that a digital signature more authenticates a relationship than an identity. The online services are in a good position to provide a transfer of that authenticated relationship to potential merchants and other sellers. A bank trying to leverage its existing relationship for authentica-
tion will require a digital channel to its customer which, again, a bank may obtain more efficiently by using an existing service.

A Prodigy/Discover combination could do quite well here if the executives involved can imagine that it’s possible.

**Intuit and Microsoft.** Intuit is in a good position to take advantage of the medium-value networked-payment systems that will be the first to achieve moderate success. This level of transaction is good for paying bills and other small finance matters that Intuit handles well. Scaling beyond this will require more capabilities than current projects provide.

The online connection needed for electronic commerce will have to come from somewhere. If the Microsoft acquisition goes through, this leaves Intuit in a double bind. To promote the Microsoft Network (MSN), Microsoft may make any Quicken Online financial services available exclusively through MSN. Those financial services won’t be worth nearly as much if they require MSN. Binding financial services to MSN exclusively will simply replicate the closed-end payment mechanisms of today’s online services.

The multiparty cooperation necessary for a successful payment system is not part of Microsoft’s corporate culture. Their monopolistic attitude won’t go over well in the banking world. Microsoft won’t be able to create arbitrary standards in payments and expect other people to follow them. Whether they’re able to function well in an environment where they’re not in charge is an open and interesting question. Should Microsoft become able to work with financial institutions and other vendors instead of against them, they would be in a good position to prosper in that market. On the other hand, Microsoft could have another failure similar to handing the networking market to Novell and remain a niche player in payments.

**Defect and need.** Several omissions in microcomputer operating systems that are nuisances now will later be killers of confidence and seeds of lawsuits. Money is the killer application for system security. When your word processor crashes and requires a reboot and five minutes of retyping, that’s annoying. When your banking software crashes and takes five minutes of transactions with it, that’s a tort.

Foundational system reliability is just as much a part of security as predictability is. No widespread operating system is built atop the notion of a replicated, stable data object, much less the simpler notion of a backed-up hard disk. Paper is still the preferred means of storing many kinds of data because it doesn’t mysteriously vanish as file systems sometimes do. Similarly, paper envelopes provide a more stable means of sending bills and statements than electronic mail, which is even more fickle than disk files. Paper doesn’t crash.

Furthermore, we should expect to see virus attacks on money systems. The particularly nasty ones will look for the presence of modems and network interfaces. With the arrival of electronic money as a part of desktop environments, some data will be specifically more valuable than others. Once certain data become fungible, the incentive to subvert becomes more than just a hacker’s learning experience.

The relationship between system security and money creates a wild card in the operating system arena. A compelling application requiring money is
susceptible to a virus attack on one operating system but not another. The attack causes people to lose money. Users migrate to the new system just to use the new application. Now, let’s see: Intel has had memory protection standard ever since the ’386. In an alternate universe, the OS/2 team at IBM doing disassembly for Windows would surreptitiously provide useful data to virus writers. Perhaps the experience of fear will induce enough responsibility in Microsoft to make bankers out of them.

Higher ground in the OS wars. Long run, the requirement for OS-level system security in money systems may provide a significant differential advantage. If a machine crashes once a week with a downtime of two and a half minutes, that’s about one thousandth of a work week. No widespread payment system is going to cope well with that high a failure rate if a crash can corrupt a transaction in progress.

A good first improvement to an OS would be adding a transaction oriented file system that would not cache writes and would use a two phase commit to ensure that data on the disk was always well formed. Such a file system might be a separate partition of the disk or a reserved portion of some other file system. The important feature is that a money application can keep intermediate stages of a transaction in non-volatile storage as a safeguard against interruption.

Support for two hardware add-ons would improve utility for users who need higher reliability, such as merchants. Non-volatile battery backed RAM can dramatically improve the performance of a log-based file system. In addition, power management facilities should support uninterruptible power supplies, further reducing downtime.

Simply making the OS less crash-prone will be an advantage, as will protection against virus attacks. As more and more machines become part of the Internet, online security will become a serious issue, as it is already in the Unix world.

Caveat vendor. Banking is a highly regulated industry. The regulations have the specific purpose of providing a protected market for banks. This kind of regulation excludes new entrants. Do not be surprised if the banking industry uses an Internet payment systems failure as a pretext for new protection.

I’m not even going to start to address the anti-trust issues lurking here.

Internationalization of payments. I’ve mostly addressed the problems in making a scalable domestic system. The problems for an international one are much larger. They center, as always, on failure. Cross-border enforcement is hideously expensive. The increased cost generates increased risk as counterparties realize that small failures are not cost-effective to pursue. The existing international clubs for foreign-exchange trading and for international credit-card settlement have the advantage here. Any entrant in this field must certainly leverage one of these assets.
Extending the club. Clubs are useful but not scalable. The utility of a club flows beyond its membership through proxy relationships. One participant in a club, the proxy, transacts on behalf of someone outside the club, the principal. This arrangement is already the norm for extending high-value payment systems. Indeed, one of the oldest standard banking instruments, the letter of credit, is exactly a proxy relationship. Large commercial wire transfers, for example, may directly result in a single Fednet transaction. The payer and payee banks act as respective proxies for the underlying business-to-business transaction. Likewise, a correspondent banking relationship is the proxy relationship of a participant bank for some other bank. The other bank is not a participant commonly because of either small size or foreign location. These remote banks, in turn, act as proxies for their own customers.

Proxy is not merely a formal relationship. Proxies provide the added value of vetting transactions by putting themselves in the place of the principal. Critical to the efficiency of this relationship is that data for the vetting decision exists only in the proxy. The rest of the club does not need to know the reasons for the proxy's decision. This limit on information travel is exactly what makes clubs so useful. Standard methods for proxies to interact will remain useful, even though the forms they currently take will change.

Detangling levels. Club membership is a legal relationship, not a technical one. The primary facts of club membership are prior arrangements both for normal activity and for reaction to failure. Participation in the club's shared electronic network is subordinate to the legal situation. No legal reason exists to bar other participants from the club's technical means of communication. One prevailing technical consideration, on the other hand, interferes. Most current networks rely upon the means of transport to provide identity. These infrastructure-based identities don't scale well for transacting because the attestation of identity occurs at the wrong level -- the network connection.

Digital signatures provide a transport-independent identity. By using digital signatures instead of network identities, a transaction club need not rely upon network closure to prevent imposture. This opening of the data network is key to the opening of the financial network.

A digital signature authenticates the relationship between parties more than it authenticates the parties themselves. True, the relationship derives from agreements made by the parties, but when the signature matters it is the relationship that generates the activities under it, not the identity of the parties. Any relevance of the parties as identities must necessarily pass through the relationship to have pragmatic effect.

Open financial networks. As an extension of current practice, club members might effectively include nonmembers in their transaction system by making and accepting explicit statements about relationships between member proxies and nonmember principals. These statements fall under the conventions of the club. Explicit statements of proxy separate the vetting decision from the use of that vetting. The signed proxy statement is an encapsulation of the vetting decision, achieving exactly the same knowledge bounding that the club needs for existence.
As an example of a typical transaction, consider a transfer out of a demand account. The principal sends the proxy the terms of the service desired, here the amount of the withdrawal. The proxy makes a mediation decision regarding the principal and the terms and conveys the results as a signed statement. In the example, the proxy checks for sufficient funds, puts a hold on that amount, and returns certification to the principal. The principal now sends a message directly to a different club member over the open data network, requesting a transfer of funds into an account held there. The request includes the proxy certificate. When the counterparty member accepts this request, clearing is complete. Settlement between the different club members will happen subsequently and may start immediately.

The full power of explicitly mediated proxy is perhaps not evident in the simple example. The range of explicit proxy representations is much greater than just certifications, but includes guarantees, warrants, insurance, credit lines, substitutions and many more. The first party presents these proxy statements to arbitrary counterparties during negotiation and may then bind them into a complex transaction. A proxy statement also provides a good-faith assurance that can persuade a counterparty to undertake costly action, obviating the need to argue over a broken promise because the proxy has certified the promise. By unlinking the proxy decision from clearing, the proxy relationship becomes employable as a building block rather than remaining an end in itself.

Unbundling and rebundling. Explicit proxy representations permit competitive markets in every atomic proxy relationship. Service offerings previously bundled together many different contingencies into a single product. Some of these arrangements were useful each time, some rarely. A typical credit card, for example, bundles together a means of payment, an extension of credit and the ability to charge back protested purchases. Additional features can include cash back, airline miles, rental car insurance and extended warranties. Never do all the features of a particular card come into play with any transaction.

Unbundling will progress in stages as less costly alternatives poach the simple transactions. Outsourcing efficiency will greatly influence what shakes out first. Bundled offerings will get more expensive as their value-added services get more use, further stressing the bundle. Paying for car-rental insurance is only necessary when renting a car, for example, and a credit line is only needed when cash is not immediately at hand.

Simplest local decision. The local algorithm for determining approval need not be complex. Indeed, the simplest feasible local algorithm, a single numeric comparison, is perhaps the most useful. Is the payment amount less than the balance? The simplicity of the algorithm makes for less to argue about, since the explicit representation leaves nothing to interpret. This very plainness is suitable for composition into more complicated protocols.

When the transaction is a simple payment, the unbundling of authorization may not be economical. On the other hand, when a balance on deposit secures a transaction or when a credit line acts as a third party guarantor, the separation becomes more obviously useful. A higher velocity of transfer comes to emulate a multiparty barter arrangement with a small amount of money acting as grease. This speed requires long contingency chains and hence extremely low failure rates.
From a monetarist perspective, the macroeconomic effect of a more efficient use of liquidity is to reduce the demand for money. Evolutionary experiments indicate that money is an emergent property of a barter economy, as one commodity becomes valorized by its utility as a means of communicating value. Electronic networks can substitute functionally for money as a communication device. As the web of electronically mediated mutual assurances becomes richer, the need for money as liquidity, that is, as a prime signifier of immediate value, will decrease. Regarding recourse for failure, explicit agreements can substitute for liquidity.

**Questioning assumptions.** The uses of cryptography are plentiful enough to annul arguments for technological determinism. Developers may envision their desired system, then implement it. Nevertheless, often the first interpretation of some new cryptography technique has been the only use examined. Cryptographers' hidden assumptions become manifest when they speak of single purposes for their protocols.

For example, efforts in public-key distribution mechanisms have all to date fallen to this criticism: They've all referred to identities rather than simply holders. The assumption is always that the signing information exists in only one person's possession, even though for some applications (e.g. delegation) this assumption need not be true.

**Remote auditing.** The principle of separability (see page 16) applies well to auditing. An audit is a formal process for answering questions about the state of an enterprise. Is it solvent? What is its net size? How much risk is present? The answers to audit questions are compactions of the accounting records to yield simple answers from complicated data.

Remote auditing is the verification of answers to auditing questions by parties who don't have access to particulars. Using cryptography, the answers and assumptions of the audit questions are separable from the sensitive business records needed to generate results.

A company can publish its entire transaction log in a special encrypted form that, standing alone, reveals no information about individual transactions or parties. The integrity of these encrypted books derives from attestation by counterparties and proxies. Given this base of information, the company may offer proof of certain facts about the entries encrypted in the journal and not reveal the entries themselves. For instance, a company might reveal total sales figures without revealing product distribution. Remote auditing allows for both financial audits and operational audits. The former is a reduction to financial records; the latter is a reduction to attestations made about the physical plant, for example.

The simplest forms of remote auditing are powerful by themselves. A bank, for example, can publish all its account balances encrypted and reveal only its total liability, likewise all its assets. In other words, an auditor, without having interior access, can demonstrate a bank's basic solvency.

The ability to determine solvency from afar allows two different entities to split the function of asset holding from the function of accounting. The accounting entity can perform transactions between different accounts and prove externally that the total amount of money stayed the same. The asset-holding entity only performs interbank transfers subject to a proof...
of solvency, thus preventing bank directors from simply absconding with money. Indeed, any demand-deposit account can act as an asset base for such operations.

Automation of proxy. The proxy relationship is an information localization on two different time scales. The longer time scale is the policy relationship between the proxy and the principal, that is, under what circumstances the proxy will lend credence to a principal's requests. The details of the policy are typically in a contract. The policy relationship is stable between negotiations, except for parameters such as price.

The shorter time scale is the financial activity of the principal with the proxy, for example, account balances, credit granted and guarantees offered. In a standard arrangement, the proxy evaluates a decision based on knowledge in both time scales.

Remote auditing allows a separation between these two time scales. Two parties agree upon the policy, but remote auditing allows the principal to keep certain information private and yet demonstrate to the proxy that the policy is being satisfied. Allocation of a credit line to cover certain transactions, for example, could fall under this rubric. The design goal here is willful ignorance. The proxy need never have information that it might abuse.

Systemic stability. Remote auditing can reveal information about the systemic stability of cross-holdings and trading positions. This application is particularly useful in high-value systems. For example, a standard bank fraud technique is the swapped loan. Two banks lend each other money using intermediaries to make the maneuver less obvious. Now each bank has a larger asset and larger liability than before; each bank looks bigger and more solid, yet there has been no net change in viability.

If banks and other parties were to publish cross-holding information, verifiable by remote auditing, these kinds of closed liability loops would be easily detectable by potential investors or depositors. The competitive pressure to reduce circular liabilities would quickly collapse them. An efficient multiparty negotiation and binding mechanism would be necessary to reduce the transaction cost of doing so.

The result is a self-disciplining system in which market pressures could replace much, if not all, of government oversight over banking activity. Bank auditors are trustworthy parties whose answers to questions about banks are reliable and who remain silent. The cryptography of remote auditing yields substantially the same facility.

Conviviality in economics. Economic relationships must perforce be local. Competition, whatever its detriments, is a necessary check upon inefficiency and laziness. Competition induces local optimization as rivals strive for more efficiency. On the other hand, state planning and global optimization do not work, as the failure of centrally planned economies demonstrates. However desirable global optimization might be, it is extremely difficult to achieve in practice.

The dog-eat-dog interpretation of commerce has always been justification for loutish behavior. When designing new economic relationships, one must
always keep in mind that at root economic activity is convivial: It is the activity of all for the benefit of all. Increasing efficiency benefits everybody in aggregate, even when rearrangement has winners and losers. Generalizing the locality of transactions in ways that approximate global efficiency is the coming challenge. Finance and money are good starting places, immediately amenable to technology intervention.

There is no reason to compete against a hard-working and efficient enterprise that tracks the state of the art. Better returns are available by pushing the state of the art elsewhere than by simply replicating existing work. Proper use of disclosure with remote auditing techniques can create a stability in economic relationships. One might not make a killing over one's neighbor but one would also not have competitors because entry would not be economical. Owners of such enterprises could operate them for their own lifetime employment rather than for speculative gain. Stability can outcompete speculation.

---------------------

<table>
<thead>
<tr>
<th>COMING SOON</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Software for education.</td>
</tr>
<tr>
<td>• Links and link management.</td>
</tr>
<tr>
<td>• Navigation &amp; the semiotics of cyberspace.</td>
</tr>
<tr>
<td>• Advanced user interfaces.</td>
</tr>
<tr>
<td>• Web authoring tools.</td>
</tr>
<tr>
<td>• The analog world.</td>
</tr>
<tr>
<td>• And much more... (If you know of any good examples of the categories listed above, please let us know.)</td>
</tr>
</tbody>
</table>

Release 1.0 31 March 1995
RESOURCES & PHONE NUMBERS

Bill Melton, Dan Lynch, CyberCash, (703) 620-1222; fax, (703) 620-4215; melton@cybercash.com, lynch@cybercash.com; http://www.cybercash.com

David Chaum, DigiCash, 31 (20) 665-2611; fax, 31 (20) 668-5486; e-mail, david@digicash.nl; http://www.digicash.com

Lee Stein, First Virtual Holdings, (619) 759-9300; fax, (619) 759-0501; e-mail, leestein@scripps.edu; http://www.fv.com

Scott Cook, Intuit, (415) 329-2721; fax, (415) 329-6999; e-mail, scook@intuit@mcimail.com

Russ Siegelman, Microsoft, (206) 936-2057; fax, (206) 936-7329; e-mail, russs@microsoft.com

Jim Clark, Netscape Communications, (415) 254-1900; fax, (415) 528-4122; e-mail, jim@mcom.com; http://home.mcom.com

Eric Hughes, Open Financial Networks, (510) 849-4729; fax, (510) 849-4719; eric@remlaler.net

-------------------

Release 1.0 is published monthly, except for a combined July/August issue, by EDventure Holdings, 104 Fifth Ave., New York, NY 10011-6901; (212) 924-8800; fax, (212) 924-0240. It covers PCs, software, the Internet, computer-telephone integration, online services, groupware, text management, connectivity, messaging, wireless communications, artificial intelligence, intellectual property law and other unpredictable topics. A companion publication, Rel-EAST, is an information bulletin on emerging technology markets in Central Europe and the former Soviet units. Editor: Esther Dyson (edyson@eff.org); publisher: Daphne Kis (daphne@edventure.com); managing editor: Jerry Michalski (spiff@panix.com); circulation & fulfillment manager: Robyn Sturm (robym@edventure.com); executive assistant: Christina Koukkos (6877695@mcimail.com); editorial & marketing communications consultant: William M. Kutik (kutik@edventure.com). Copyright 1995, EDventure Holdings Inc. All rights reserved. No material in this publication may be reproduced without written permission; however, we gladly arrange for reprints or bulk purchases. Subscriptions cost $595 per year, $650 overseas.

Release 1.0 31 March 1995
**Release 1.0 Calendar**

**April 3-7**
32nd Internet Engineering Task Force - Danvers, MA. Sponsors: FTP Software and Nearnet. Call Stephen Coya, (703) 620-8990; fax, (703) 620-0913; e-mail, ietf-info@cnri.reston.va.us.

**April 4**

**April 4-5**

**April 5**
Infobahn Entrepreneurs: Opportunities on the Information Superhighway - Evanston, IL. Sponsored by the Kellogg Graduate School of Management, Northwestern University. Call David Berkowitz, (708) 332-1481 or James Shepard (708) 733-0713. For registration information, call (312) 409-3700; fax, (708) 467-4077; infobahn@nwu.edu, http://nuinfo.nwu.edu/infobahn/.

**April 5-7**
National Net '95 - Washington, DC. Organized by Educom NTTF. Policy focus on the National Information Infrastructure: access, community and business. Call Elizabeth Barnhart, (202) 872-4200; fax, (202) 872-4318; e-mail, net95@educom.edu.

**April 10-13**
AIIM '95 - San Francisco. Sponsor: The Association for Information and Image Management. It's not just about optical disks anymore! Call Jim Breuer, (301) 587-8202; fax, (301) 587-2711.

**April 11-12**
1995 Internet Society Summit - San Diego. Sponsored by Aldea Communications, CIX, FARNET, and the Internet Society. Call Mary Burger at the Internet Society, (703) 648-9888; fax, (703) 648-9887; e-mail, mburger@isoc.org.

**April 11-13**
Network World Unplugged - New York City. Produced by IDG World Expo in conjunction with Network World and Forbes ASAP. Call Marli Hoyt, (800) 225-4698 or (508) 879-6700; fax, (508) 872-8237; e-mail, unplugged@idgwec.com.

**April 18-19**
Online Marketplace '95 - Chicago. Sponsored by Jupiter Communications and Interactive Age. Call Harry Larson, (800) 488-4345 or (212) 941-9252; fax, (212) 941-7376.

**April 18-19**
@CreaTECH - New York City. Organized by TECH Marketing. With Jerry Michalski on making money online. Call Josh Fields, (800) CreaTECH or (914) 723-4464; fax, (914) 723-4082.

**April 18-21**
Crossroads '95 - Rancho Mirage, CA. Sponsored by Open Systems Advisors. Help open closed systems. Call Nina Lytton, (617) 859-0859; fax, (617) 859-0853; e-mail, 5066830@mcimail.com.

**April 19-21**

Release 1.0 31 March 1995
<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
<th>Location</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>April 21</td>
<td>Digital Cash and Electronic Money - New York City. Organized by Columbia University. Call Kevin Holmes, (212) 854-6222; fax, (212) 932-7816; e-mail, <a href="mailto:citi@research.gsb.columbia.edu">citi@research.gsb.columbia.edu</a>.</td>
<td>New York City</td>
<td></td>
</tr>
<tr>
<td>April 23-24</td>
<td>Licensing Law Institute - San Francisco. Sponsored by Aspen Law &amp; Business. Call Margaret Ross (201) 894-8260; fax, (201) 894-0074.</td>
<td>San Francisco</td>
<td></td>
</tr>
<tr>
<td>April 24-25</td>
<td>Multimedia Publishing for the Education Market - Chicago. Sponsored by AIC Conferences and Multimedia Week. Call (800) 826-2424 or (617) 742-5200; fax, (617) 742-1028.</td>
<td>Chicago</td>
<td></td>
</tr>
<tr>
<td>April 24-27</td>
<td>@Comdex Spring '95 - Atlanta, GA. Organized by the Interface Group. With Jerry Michalski on commerce and wireless e-mail. Call Sue Loneran, (617) 449-6600; fax, (617) 449-6953.</td>
<td>Atlanta, GA</td>
<td></td>
</tr>
<tr>
<td>April 25-28</td>
<td>1995 Distributed Object Technology Forum - Cambridge, MA. Organized by Patricia Seybold Group. Call Deb Hay, (800) 826-2424 or (617) 742-5200; fax, (617) 742-1028.</td>
<td>Cambridge, MA</td>
<td></td>
</tr>
<tr>
<td>May 1-2</td>
<td>U.S. Copyright Office Speaks - Washington, DC. Sponsored by Aspen Law &amp; Business in cooperation with The United States Copyright Office. Call Margaret Ross, (201) 894-8260; fax, (201) 894-0074.</td>
<td>Washington, DC</td>
<td></td>
</tr>
<tr>
<td>May 2-4</td>
<td>National Online Meeting &amp; Integrated Online Library Systems '95 - New York City. Sponsored by Learned Information. Bulletin boards, online services and more. Register at (609) 654-6266; fax, (609) 654-4309.</td>
<td>New York City</td>
<td></td>
</tr>
<tr>
<td>May 2-4</td>
<td>DB/EXPO - San Francisco. Organized by Bruno Blenheim. Call Annie Scully, (201) 346-1400; fax, (201) 346-1532.</td>
<td>San Francisco</td>
<td></td>
</tr>
<tr>
<td>May 2-5</td>
<td>@Ties That Bind: Converging Communities - Cupertino, CA. Organized by Apple Library of Tomorrow and the Morino Institute. See what's cooking at the local level: Freenets, civic nets and more. Call Pam Lau, (408) 974-2400.</td>
<td>Cupertino, CA</td>
<td></td>
</tr>
<tr>
<td>May 7-11</td>
<td>CHI '95: Mosaic of Creativity - Denver. Sponsored by ACM/SIGCHI. Always chock-full of inspiring ideas. Call Debbie Compere, (410) 263-5382; fax, (410) 267-0332 or Rosemary Stevens, (415) 328-3600; fax, (415) 323-2172; e-mail, <a href="mailto:chi95-office@sigchi.acm.org">chi95-office@sigchi.acm.org</a>.</td>
<td>Denver</td>
<td></td>
</tr>
<tr>
<td>May 8-11</td>
<td>@EMA '95 - New Orleans. Sponsored by Electronic Messaging Association. Call Heather Burneson, (703) 524-5550; fax, (703) 524-5558; e-mail, <a href="mailto:info@ema.org">info@ema.org</a>.</td>
<td>New Orleans</td>
<td></td>
</tr>
<tr>
<td>May 11-12</td>
<td>Electronic Banking '95 - Washington, DC. Sponsored by the Institute of International Research. Call Rosemary Stabile, (800) 345-8016 or (212) 661-8740; fax, (212) 661-6677.</td>
<td>Washington, DC</td>
<td></td>
</tr>
<tr>
<td>May 14-17</td>
<td>Interactive95 - Anaheim. Sponsored by Softbank Institute. Call David Holcombe, (800) 34-TRAIN; fax, (617) 393-3322.</td>
<td>Anaheim</td>
<td></td>
</tr>
<tr>
<td>May 15-17</td>
<td>Complexity and Strategy: The Intelligent Organization - London. Sponsored by The Santa Fe Institute and The Praxis Group. Call The Praxis Group, (800) 771-4770 or (505) 466-4400; fax, (505) 466-4012; e-mail, <a href="mailto:praxis@santafe.edu">praxis@santafe.edu</a>.</td>
<td>London</td>
<td></td>
</tr>
<tr>
<td>May 15-17</td>
<td>@The Growing Companies CEO Summit - Mexico City. Presented by World Congress. With Jerry Michalski on Internet stuff. Call Camilla Nugent, (617) 270-6207; fax, (617) 270-6204.</td>
<td>Mexico City</td>
<td></td>
</tr>
<tr>
<td>Date</td>
<td>Event Description</td>
<td>Sponsor/Contact Information</td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Multimedia Development Partnerships - San Francisco. Sponsored by AIC Conferences.</td>
<td>Call Elizabeth Lizas, (212) 952-1899 x335 or to register (800) 409-4AIC; fax, (212) 248-7374.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Networld + Interop - Frankfurt, Germany. Sponsor: Seybold Seminars. Call Christi Leer, (415) 578-6985 or (800) 488-2883; fax, (415) 525-0183.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Licensing Law Institute - New York City. Sponsored by Aspen Law &amp; Business. Call Margaret Ross (201) 894-8260; fax, (201) 894-0074.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>U.S. Copyright Office Speaks - Washington, DC. Sponsored by Aspen Law &amp; Business in cooperation with The United States Copyright Office.</td>
<td>Call Margaret Ross, (201) 894-8260; fax, (201) 894-0074.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ninth Workshop on Parallel and Distributed Simulation - Lake Placid, NY. Sponsors: AGM, IEEE/TCSIM, and SCS.</td>
<td>Call Jason Yi-Bing Lin, (201) 829-5095; fax, (201) 829-5886.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Community Networking Workshop - Princeton, NJ. Sponsored by the IEEE Communications Society.</td>
<td>Call Joel Winthrop, (908) 949-5008; fax, (908) 949-8569.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PC Expo - New York City. Organized by Bruno Blenheim. Call Annie Scully, (800) 829-3976 or (201) 346-1400; fax, (201) 346-1532.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>INET '95 - Honolulu. Sponsored by the Internet Society. Call them at (703) 648-9888; fax, (703) 648-9887; e-mail, <a href="mailto:mburger@isoc.org">mburger@isoc.org</a>.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>March 9-12</td>
<td>The Burton Group Conference on Network Computing - Colorado Springs. Sponsored by The Burton Group.</td>
<td>Call Doug Allinger, (800) 824-9924 or (801) 943-1966; fax, (801) 943-242; e-mail, <a href="mailto:info@tbg.com">info@tbg.com</a>.</td>
<td></td>
</tr>
<tr>
<td>October 15-18</td>
<td>**East-West High-Tech Forum - Bled, Slovenia. The sixth annual sponsored by EDventure Holdings. Call Daphne Kis, (212) 924-8800; fax, (212) 924-0240; e-mail, <a href="mailto:info@edventure.com">info@edventure.com</a>.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* Events Esther plans to attend.
@ Events Jerry plans to attend.

Lack of a symbol is no indication of lack of merit.
Please let us know about other events we should include. -- Christina Koukkos

Release 1.0
31 March 1995
SUBSCRIPTION FORM

Please enter my subscription to Release 1.0 at the rate of $595 per year in the U.S. and Canada. Overseas subscriptions are $650, airmail postage included. Payment must be enclosed. Multiple-copy rates available on request. Satisfaction guaranteed or your money back.

Name
Title
Company
Address
City State Zip
Telephone

☐ Check enclosed.
☐ Charge my
  ☐ American Express ☐ MasterCard ☐ Visa

Card Number ___________________ Expiration Date __________
Name on Card __________________ Signature __________________

☐ Please send me information on your multiple-copy rate.

Please fill in the information above and send to:

EDVENTURE HOLDINGS INC.
104 FIFTH AVENUE, 20TH FLOOR
NEW YORK, NY 10011

If you have any questions, please call us at 1 (212) 924-8800;
Fax 1 (212) 924-0240; e-mail info@edventure.com.

Daphne Kis
Publisher
KIDS, EDUCATION AND TECHNOLOGY, PART I
by Jerry Michalski

A tour of the software and communication tools available for grade-school education today is enough to make you wish you were five years old again. There are some wonderful products and services available now, and activity on the Internet is exploding. If you talk with entrepreneurs and activists about where those tools might be in just five years, you can feel their excitement and see the major transformation that's underway. But those conversations can often be frustrating.

When it comes to educating children, everyone seems to have an initiative, project, product, theory, association or foundation -- or at least a strong opinion. Indictments of the current system abound, such as Lew Perelman's book School's Out. Many theorists rely on blind faith in multimedia or intelligent software agents and pay little attention to the social dynamics of learning. Others attack the political dynamics and propose broader, more extreme proposals, including voucher systems and profit-oriented schools, such as Minneapolis-based Education Alternatives and Chris Whittle's revived Edison Project.

The frustration lies in how few of these instigators look to how their projects fit with others'. It's quite remarkable. It's as if everyone had seen the same movie, agrees on who was in the cast, but reports a completely different plot.

There's no single solution to the education system's woes. In fact, the perennial problem is whom to help and how to help them, or even whether to help them at all. Should one focus on teachers or students? On infrastructure, process or tools? On skill-building or theories about learning? What about kids' home lives and diets? Neighborhood safety?

Platform envy

Educational software accounts for roughly a tenth of the $6 billion spent on educational resources in the US, including textbooks, videos and laserdiscs. The home-PC market is hot, in large part because parents see PCs as a latter-day home encyclopedia, possibly the most important investment they can make for their children. CD-ROM drives are now relatively inexpensive and almost standard equipment, as are modems. CD-ROM titles and software to

OH, TO BE A KID AGAIN

INSIDE

KIDS AND EDUCATION 1
Many lead, few follow.
Ingenius.
Tenth Planet.
The market; edutainment.

EDUCATION AND THE NET 6
Points of view everywhere.
KIE and the Jason Project.
Business opportunities.

RESOURCES & CALENDAR 14
Names, phones, dates, URLs.

EDVENTURE HOLDINGS INC. 104 FIFTH AVENUE, 20TH FLOOR, NEW YORK, NY 10011 - 1 (212) 924-8800, FAX 1 (212) 924-0240
get online are bundled with most home PC systems, shrink-wrapped with magazines and handed out on airlines.

Schools are more open to technology purchases than before, but they are seriously hampered by terrible infrastructure, glacial curriculum-review procedures (see next page), occasional religious or political frays and budgets that not only can’t keep up with their appetites but are under constant pressure. Also, those in power often don’t really want to change.

These purchase and funding trends are driving wedges between the various constituencies. Fortunate, privileged schools get access to equipment and network bandwidth, while others fall behind. Parents buy their kids multimedia PCs; their kids go to schools equipped with Apple II GSs and learn from teachers who don’t have access to better technology themselves. Have-nots are not happy.

This time and next

This issue of Release 1.0 and the next one focus on the use of technology to benefit children from kindergarten through the end of high school (K-12), at home and at school. This issue is a broad survey of technology in K-12 education, salted with illustrative vignettes. Its second section examines how the Internet is changing the business. The next issue will explore various educational philosophies and the kinds of software they have led to, as well as some innovative vendors and projects. In both issues we focus principally, but not exclusively, on computer software and networking technology.

There’s plenty going on with other media. Laserdisks and videotapes are everywhere. Voicemail systems now boost attendance, list homework assignments and help parents keep in touch with teachers. Several initiatives use the cable TV infrastructure. A TCI-Reuters joint venture named Ingenius uses cable to deliver information and software to PCs (see box, opposite). The Lightspan Partnership, a venture formed by TCI, Comcast and Microsoft, with funding from Accel, Kleiner Perkins and Institutional Venture Partners, is creating entertainment-grade programming for schools and homes, for delivery over future interactive TV networks.

Roles a-morphing

Technology is a small piece of the transformation of the educational system. Every role is changing. Teachers were once imparters of canonical knowledge; now they’re coaches, mentors and guides. Students once were passive memorizers of information and essay-writers; now they’re urged to be inquisitors and creators with putatively worthy ideas. Librarians were keepers of knowledge and teachers of the Dewey Decimal System; now they’re networked information finders and linkers.

Today, students’ activities are more social, experiential and collaborative. Students create things in groups; they’re part of communities that sponsor activities; they brainstorm, revise and publish. For a short while, computer technology has turned around some traditional age relationships: Kids often grasp computer arcana more quickly than adults, and can teach people normally considered their superiors. This natural mastery is a great boost for kids. It gives them ways to participate as equals.
Ingenius ways to package news

For the last eight years, Tele-Communications Inc. (TCI) has provided a free, round-the-clock, plain-text news and lesson-plan feed called Xchange to schools over cable TV systems through a subsidiary called X.Press Information Services. Last August, TCI launched a related venture called Ingenius, which enhances the Xchange service with multimedia content provided by its joint-venture partner, Reuters New-Media. Every night, Ingenius' service, called What on Earth, delivers a complete multimedia package with six news stories, editorial pieces, lesson plans, work assignments and more to 300 beta-site schools. Journalists, educators and multimedia authors compose the pieces to fit two skill levels between grades 4 and 12.

The nightly batch is downloaded automatically over the cable system to a PC via a hybrid cable modem that is similar to a set-top box. Ingenius claims teachers can install it themselves. The service costs $210 per year per computer. Cost decreases over time, as equipment is paid off. It is available broadly across the US, even from some non-TCI operators.

In May, Ingenius will test sales of the system to homes in Denver, and later to other cities, with a potential national rollout in the first quarter of 1996. But the company expects to have to change the product to suit home use.

The concept of a curriculum is changing, too. In the old model, which is still prevalent, state boards of education approve the majority of textbooks. A few US school boards -- Texas, California and Florida -- lead or influence at least half the other states. They tackle one subject a year (say, math) and choose a few texts for each grade, often only one. That means that a small window of opportunity opens every six years through which a new curriculum item can enter the majority of the US school systems. Because large budgets are at stake, this is a highly politicized process. In addition, textbook content has become a matter of great controversy lately, and book selections are loaded issues. This process is but one example of the bureaucracy and politics that hamstring today's educational institutions. It's a difficult passage for software vendors, too (see Tenth Planet, next page).

Now computer materials are becoming central to school curricula. In addition to offering access to large bodies of information in CD-ROM encyclopedias and courseware, computers allow teachers to incorporate the newest concepts, such as chaos, swarms or neural networks, into classwork. Software makes realistic, easily understood simulations available to more people. Maxis' Sim-series (SimCity, SimEarth, SimLife, etc.; see Release 1.0, 2-93) have greatly helped popularize such software.

The home and school markets

Although they overlap in places, the home and school educational software markets are quite different. The obvious difference is that homes don't have a curriculum to worry about, unless they want to track what's going on in the classroom or undertake home schooling. In the home, educational
software competes with TV, video games and physical activities. Because of this competitive pressure and parents' greater freedom (than teachers') to buy what appeals to them, there are some beautiful, creative and entertaining children's products for home use. There are also some flashy, obnoxious ones.

Yes, there really is a Tenth Planet

One startup tackling the school market head-on is Tenth Planet Explorations. Its president and ceo, Cheryl Vedoe, formerly ran Apple's education business. The company's first product is Tenth Planet Explores K-2 Math, which follows standards set by the National Council of Teachers of Mathematics. Tenth Planet expects to have three units of geometry curriculum ready to ship this fall on Macs, with a Windows version six months later.

Tenth Planet’s approach is pragmatic, creative and sensitive to classroom dynamics and teachers’ needs. The product balances software with supplementary materials, including manipulatives (school-speak for physical props such as puzzles) and notebooks with project ideas. Projects lead to printable work products. The software comes with beautifully crafted companion print materials.

Tenth Planet uses a learning model called Into-Through-Beyond. It begins with getting children ready for and interested in a task, such as recognizing and working with patterns. Then there’s a lesson, with task-specific tools (e.g., a pattern-rich drawing tool with which they can design a quilt or floor-tile pattern) to help explore the question at hand. Each unit ends with a challenge, so children can extend and apply what they’ve learned. For this example, the "beyond" section might ask them to consider asymmetrical or irregular patterns, or patterns in three dimensions.

Founded in 1994, the company received $3 million in initial financing from Mohr, Davidow Ventures, Greylock Management and Stanford University. Tenth Planet will eventually pursue the home market. Right now, though, it will be happy to establish a foothold in schools.

The competition for software in schools -- outdated textbooks -- is far less a problem than the approval and sales process that selects software for schools. Materials for the school market fall into two segments: core curriculum and supplementary materials. Until recently, technology was considered supplementary. But now some school districts have turned major portions of their core-curriculum budgets from textbooks to technology.

The overlap between the school and home markets is in general-purpose applications such as e-mail, word processing, desktop publishing and graphics and in skill-building edutainment titles. Aside from these areas, crossing from one market to the other is difficult. It's hard to turn a home product into a school one; it may be somewhat easier the other way around.

Release 1.0

24 April 1995
Flame on

Before we throw technology at the educational system, we should spend more money to ensure that most teachers are paid a living wage, and that there are enough of them to bring class sizes down, which would allow teachers to do their job rather than to babysit. If we had money to put into the educational system, this would be our first priority. Technology would be second.

Flame off

Let us edutain you

Edutainment raises some thorny issues. Just how much fun does education have to be? Are we training a nation of point-and-clickers who expect surprises behind each object? Will all future artists rely on clip art? Yes, many of the things that kids have to learn could use a dose of wit and excitement, especially in the skill-building area. If kids sit still long enough to use a piece of software that helps teach them multiplication, typing or reading, we should all be thrilled. Some children will like the math quiz with bears and narrative; others with space aliens and shoot-'em-up arcade action.

However, when fun becomes a global mandate, things have gone too far. When educational software becomes a platform for the cross-marketing of characters on TV, cereals, action figures, movies and comics, it's probably another indicator of excess. The danger is that parents and children may get hooked on the sizzle and believe that all educational software must be this way. The fact is, children write spontaneously and at length without cute characters or multimedia action sequences. If they have access to things that have meaning to them, they get engaged. After that, it's mostly a question of getting out of their way.
EDUCATION AND THE NET

Connectivity, especially the kind the Internet offers, is the factor that will most affect companies selling software and services to the educational market over the next decade. Connectivity is not a panacea. It's a tool that, used appropriately, can loosen some of the logjams in today's educational market and cause some productive chaos.

For example, take the way the Internet puts lots of relatively raw material within teachers' reach and allows them (and their students, and parents...) to create materials for each other. This changes the traditional distribution channel, sales cycle and product economics. Certainly, it threatens software developers, but it also cuts right past the old approval-and-sales process and creates new needs. It will probably counter an obsessive emphasis on high production values (Hollywood quality! Kids demand it!) and closed, well-bounded materials. This highlights the tension between teachers' need to control the educational setting and experience and the out-of-control nature of the medium. Another opportunity.

Connectivity can make the educational process more relevant and palpable to students -- even when it's virtual. At its best, connectivity can not only improve teachers' and students' access to resources and enable new kinds of collaboration, it can also foster feelings of participation in a larger community, with concomitant feelings of responsibility. Having a real task and a larger audience can really energize children.

All of this will take a while. Most schools don't have network access. Fixing that alone could take a decade, though there's no reason it has to. Once connectivity is pervasive, the market should break open. That should be a strong incentive for all parties to help make it happen.

Grass-roots Internet efforts in education have tremendous momentum right now, and they're not all run by parents, children and teachers. Institutions and laboratories are spontaneously making useful materials available that used to be nearly inaccessible. Many assets that used to be hidden are becoming visible -- and much more useful in the process. There are many other examples, which we describe below.

Software vendors can choose to harness this energy and content in productive ways -- possibly inventing new, profitable business models in the process -- or they can proceed on their current courses and possibly be knocked out of the market by it. Here are some of our favorite examples of the Net's power in education.

Support for teachers

Online access has been a boon to those teachers who can find the time and resources to get and use accounts on the commercial services. For one thing, lesson plans can be the bane of a teacher's life. Online, grade-school teachers can share lesson plans beyond the limits of the teachers' lounge. They can avail themselves of tools created for other purposes, including college courses. They can also share anecdotes and ideas.
There are many social ways teachers can interact online, from mailing lists and discussion forums to chat rooms, MUDs and MOOs. In fact, a group of secondary-school teachers from around the world gets together every Tuesday evening on MediaMOO, a text multi-user virtual environment run by Amy Bruckman at the MIT Media Lab. These get-togethers are simply chat sessions; the participants share war stories, teaching ideas and generally hang out. They also use MediaMOO to share project work, lesson plans and insights into productive use of the medium.

A slow bootstrap process

K-12 schools usually don't have the wonderful Internet access that many universities do; they weren't part of its charter. In fact, grade school connectivity is notoriously poor. Most classrooms don't have phone lines. So informal online links in the K-12 world started in the commercial services and on bulletin boards, often with teachers' private accounts. Companies saw an opportunity forming and jumped in. Early on, for example, CNN offered lesson plans on America Online linked to particular broadcasts and current events. Recently, Infonautics launched its Homework Helper text-retrieval service on Prodigy, for a monthly add-on of $9. Now there's plenty of education-related activity on the major commercial services.

The Internet is a compelling reason for schools to get connected. It is particularly cost-effective for them. It reaches more people and resources than any single BBS or online service. Many of the important software tools are available for free and are relatively easy to use. More significantly, individuals and technically unsophisticated institutions can use those simple tools to publish to each other.

Points of view everywhere

The easy-to-use World Wide Web (see Release 1.0, 1-94) has broadened the circle of participants in the educational system enormously. Research laboratories and companies are putting their information on the Web for schoolkids to read and use. NASA sponsors projects for children, as do many other agencies and organizations. There are special-purpose places on the Web such as the Geometry Forum from Swarthmore, funded by the NSF.

Museums and research laboratories that would once have been the subject of an occasional local field trip are now available worldwide. The Exploratorium in San Francisco, the TechMuseum in San Jose and the Children's Computer Museum in Boston are all aggressively pursuing telecommunications to make their resources available. Each of them has a universe of information and fun projects for children.

Educational publishers and software vendors are participating. Many have home pages on the Web, such as Scholastic, which is also very active on

---

1 MUDs and MOOs are text-based, multi-user online environments. For details, see Release 1.0, 6-94 and 7-94.

Release 1.0

24 April 1995
America Online. Houghton-Mifflin is working with O'Reilly & Associates' Global Network Navigator to host GNN's education section, which will open its doors soon. Wentworth Media's Classroom Connect, a newsletter about educational networking, has put a site up that points to educational Internet resources around the world.

If kids are poking around the Web for classwork, how do you keep them out of the Zima 'fridge or Bianca's Smut Shack? Conversely, when you open the gates of connectivity, how do you keep out people you want to avoid?

Splendor in the grass-roots

It's not just large corporations and institutions that are making materials available. Some of the most striking sites are private individuals'. There's never been a channel like this before, through which ordinary people can inexpensively share materials, insights and even just pointers to others' resources. With the Web, for example, an enterprising Swiss named Nicolas Pioch created the WebMuseum (formerly Le WebLouvre), which features art collections around the world. Similarly, a grade-school student might assemble a personal exhibit of favorite paintings, complete with commentary.

People have built wonderful sites such as KidLink, CyberKids, MidLink (where middle school students worldwide collaborate to create Web newsletters), EdWeb (see box) and Kl2Net. There's the KID page by John Makulowich and Berit Erickson's education page. Judi Clark (whom some of you will remember as an Internet tour guide and Web developer at the 1995 PC Forum) has a site, Global Show 'n Tell, where children contribute interactive artwork. Schools have put up great Web sites. Two especially strong ones are Hillside Elementary School in Cottage Grove, Minn., and Patch American High School near Stuttgart, Germany.

Web66 lists schools that are on the Web, as does frequent Net contributor Gleason Sackman in North Dakota. Web66 is also a great site for teachers wondering how to get started publishing on the Web. (To get your kicks at these and other useful sites, see Resources, page 15.)

Integrating real life and school life

A common complaint about US schools is that they don't teach practical things, such as how to balance a checkbook or hold a job. Indeed, traditional schools often seem quite separate from the real world (except, of course, for the metal detectors at certain schools). The books they use are dated and sterile. On the Internet, real life is an appropriate and convenient subject to study. Doing so brings children into contact with professionals around the world and gives them a glimpse of their lives.

Many people would like to help teach children, but can't find an outlet for that energy. The Knowledge Integration Environment project at UC Berkeley harnesses it and fits it into a framework more like a curriculum.
Andy Carvin: EdWeb and WWWEDU

Andy Carvin has unintentionally created a wonderful role for himself in the educational-technology realm. Recently, after completing a masters degree in telecommunications science, management and policy at Northwestern University (and with full intent to use it), he started a fellowship at the Corporation for Public Broadcasting (CPB).

One of his first CPB projects was to research telecom's effects on education. In the course of his research, he uncovered a trove of useful information, especially Web sites. It made sense to publish his findings on the Web as well as on paper, so he learned HTML in a hurry. He started a Web site on his Mac and called it EdWeb. The site includes detailed stories of successful educational technology school projects, discussions of education reform and more. Soon traffic to his site grew and he had to move it to a larger server, where it is now (see Resources, page 15).

When he noticed that there was no central resource for informal discussions about how to use the Web for education, Carvin created a mailing list called WWWEDU (pronounced "we do") for the community. The list has grown quickly to 1200 members. Carvin's current project is to develop a testbed that will team up a dozen schools around the country with local public broadcasting stations (TV and radio) to create online education content. He is also attempting to coordinate a coalition called the SchoolWeb Exploration Project, which is an initiative to link schools with businesses that will make extra Web space available to schools.

The medium is changing as a quiet revolution is happening in the teaching process. The new approach that posits children as explorers and builders of their own understanding is based on a theory from Swiss psychologist Jean Piaget known as constructivism. Seymour Papert at MIT extended the idea to constructionism, emphasizing that children build models of their environment through personally meaningful projects with real-world objects. In Papert's case, the computer language Logo became an early tool.

Go on a dig! Dive to the depths!

Communication links -- from e-mail to live videoconferencing -- already bring students into space shuttles, Quonset huts in the Antarctic, archeological digs and roving submarines. Given decent access, kids in schools can get closer to real events than families in their living rooms -- or even many businesses. Sometimes classes tune into broadcasts, as with the space shuttle; other times they can build class-to-class or interpersonal relationships.

Children can act as genuine worker bees in the scientific realm. Students at the Dalton School, a private school in New York City, use a software tool the school developed called Archaeotype to explore data from a real archeological dig and come up with their own theories. In astronomy class, they use the Web as a resource for team projects. Another good example is the Jason Project (page 13).
The Knowledge Integration Environment (KIE) project at UC Berkeley explores ways to use the Web for science instruction, initially for middle schools. KIE turns the Web into an evidence network: a big, distributed scavenger hunt for evidence with which to prove or disprove scientific theories.

Researchers around the world can become Internet Science Liaisons and create evidence for KIE. The interactions create links between live domain experts and students. The systems developers have developed a series of software tools adapted to the quest, which range from evidence databases, discussion and note-taking tools to teacher planning aids. KIE is funded by Pac Bell and the National Science Foundation, and is affiliated with the School of Education and the Instructional Technology Program at UC Berkeley.

A broad, public discussion space

One thing that's easy to miss is the heightened sense of responsibility and ownership that come with participating in this medium. Students are no longer performing for a single teacher who might occasionally read their paper in front of the class. They are participating as citizens in a larger community of activity. They have access to real resources and to each other in new ways. Online, children can own their work publicly and share it with many others. Often, understanding their responsibility within a community and knowing that others rely on them raises kids' self-esteem far more effectively than stars, bonus points or grade inflation.

The traditional school day has a predictable and sometimes counterproductive rhythm: When the bell rings, everything stops. Any enthusiasm the children had worked up dissipates. It may return, but often it's gone forever. Connectivity offers a way to extend those conversations (and the events, ideas, opinions and projects they contain) over space and time. Others can participate in discussion that might have stayed inside one class session. The breadth of the audience is a design issue. It could include the class next door, the entire grade level, the local community, virtual communities or the Usenet.

Co-creators of the curriculum

For years, kids have created newsletters and newspapers with computer tools, but their distribution was always small. Now they are putting those documents on the Web. They are beginning to write e-mail and use the Web as a resource. Some even put their own art and compositions on the Web.

The next step (beyond creating personal home pages) is for children to become editors of points of view on the Web, to co-create the curriculum. As they create their own sites that explain their interests and show relationships that they care about, others will point to them, and so on, weaving a larger body of work. Kids are doing exactly that at Los Alamos High School, where they have created Web documents that describe hydrodynamics, chaos and fractals, all in collaboration with teachers and scientists at Los Alamos National Labs.

Release 1.0

24 April 1995
Access. More of it

It's painful to hear about schools that can't afford their heating bills or replace broken windows, yet struggle to incorporate computers and telecommunications into their classes. Many schools are in such disrepair that they can't be wired for LANs.

Despite schools' often slim budgets, communications companies know that they must fight to get links to classrooms quickly. Cable and interactive TV vendors, phone companies and Internet access providers know that early decisions are likely to last a long time. It's hard to justify a second link when one's already in place. A school that opts for subsidized inbound video such as Chris Whittle's ChannelOne may have a harder time getting more interactive access later, or it might find a clever way to re-use the cabling and equipment.

Several groups are working hard to ensure fair and productive access, such as the Consortium for School Networking (CoSN) and the Technology Education Resource Center (TERC). CoSN encourages usage of telecommunications in K-12 education. It's a non-profit advocacy group, not a tech-support center.

TERC's mission is to research, develop and disseminate innovative programs in science, mathematics and technology. It's running several projects, including CamMotion, which puts video camcorders in students' hands for use as scientific recording instruments, and the Testbed for Telecollaboration, a network with sophisticated software tools intended as a place for teachers to form communities of practice.

Deployment is in the details

The way a school deploys its PCs and other gear matters. A school with a computer lab that has 40 PCs lined up against the walls has to schedule kids through the lab. It's harder to encourage informal use. Those machines will probably get used more consistently, though. If the machines aren't in a lab, they could go many places. The private Dalton School in New York City places PCs in hallways and corners, as well as in classrooms. Children can sit down at any machine and log in to their accounts -- and they do, frequently.

At the ACT school near Houston, which is designed to resemble a home (complete with sofas and real towels in the bathrooms), kids carry laptops and jack in to network connectors located all over the school. Although kids with portables can carry them home, it's hard to see the machines surviving a couple of boisterous bus rides or playground fights. In yet a different model, a few colleges have begun to experiment with wireless networks, which allow students to set up a working LAN quickly.

Each design forces tradeoffs in teachers' and administrators' ability to integrate courseware, collect class materials, distribute software upgrades, forge links between schools and homes and so on.
What's the play for business?

The enthusiastic way that pioneering teachers adopt and adapt Internet materials and projects for their classes signals a new dynamic in the educational market. Their enthusiasm is not merely because the materials are often free. It's also because the materials are simple, timely, compelling and connected. Teachers can refer to and extend them; they can weave them into their classwork easily. The materials are also emerging more rapidly than commercial software can make it through the development, review, approval and sales process and into teachers' hands.

The challenge to educational publishers, online service providers and software vendors is to take advantage of the new medium's power to meet the needs of the educational market (children's needs, in the end) and still make money -- to make good by doing good. In the process of figuring out what that means, vendors may well invent new models of participation, use and payment appropriate to the medium and affordable to schools and families.

Here are some ideas for new businesses opportunities in K-12 education.

The Internet's technical shortcomings offer obvious opportunities. Servers get overloaded. They crash. Teachers can't build courses around unreliable materials. Companies can offer site mirroring and facilities management for organizations that can't or don't want to host their own materials on the Web.

The Web looks like a publishing vehicle now, but more and more special-purpose applications are emerging that use the Internet's connectivity and blend into the Web. For example, MathSoft's MathBrowser is a Web browser that allows people to share and use MathCAD files. It also encourages sales of MathCAD products. Expect to see many more specialized applications that access shared data.

Categories of software that may seem to have run out of new features will rejuvenate, including word processors and presentation software. Groupware and messaging tools benefit greatly from the improved communications infrastructure, too. Colleges and research labs will develop applications that vendors can license, bullet-proof and adapt for use in various grade levels. Next month we'll examine some of the more interesting such software projects in education.

It takes considerable work to integrate the resources available on the Web into a class. Companies can offer tools that frame the new resources and make them more amenable to classroom use. The Jason Project is a good example. It blends live exploration with multimedia communications and rich support materials (see box, opposite).

In order to prevent kids from browsing offensive materials, a service could offer filters that block access to those links, perhaps by identifying problem sites and not passing that data to special Web browsers, which would connect only to the filtering service. Alternately, special client software could do the filtering, although probably not very effectively.
Talk to scientists and run their robots in the Jason Project

In 1989, after his much-publicized attempt to raise the RMS Titanic, Dr. Robert Ballard was flooded with requests for information about his efforts. The level of interest inspired him to found the Jason Project, which mounts a two-week, seagoing scientific expedition to a remote part of the world every year. This year’s project (in February and March) explored volcanoes, observatories and other resources around Hawaii. The non-profit Jason Foundation for Education administers the Jason Project, working with the US Department of Education and other agencies. EDS is a major sponsor.

The Jason Project has an impressive communications infrastructure, including satellite links, Internet multicast video and Web pages (see Resources, page 15). It broadcasts many events live to a network of educational institutions in the US, Canada and the UK. From Primary Interactive Network Sites (PINS), students can manipulate a robot rover called Marsokhod remotely or talk directly with the scientists.

Perhaps most importantly, the Project offers substantial teacher training and mentoring. The Foundation holds workshops in the fall to prepare teachers for the following spring’s expedition. It also offers courses on cable TV through the Mind Extension University (ME/U) and has launched Jason Online. As the expedition nears, the Foundation sells resource kits at nominal cost that include CDs, videotapes, maps, posters and other materials. Afterward, it issues a report that summarizes the expedition’s findings as well as many student and teacher experiences. The report also includes data that the expedition generated and exercises that classes can do with it.

Since the Internet easily supports multi-party chat and other forms of message exchange, a service could offer people online during the day to help teachers. Think of them as virtual teachers’ aides. Or they could offer teacher tutorials after hours.

They could also provide varied points of view on the same materials or projects. How would a Montessori-trained teacher approach the Jason Project? A Waldorf specialist? Services could coach developers across the Internet on how to make their materials more useful within various teaching frameworks. They could package their particular approach to the materials as a value-added service, complete with professional-grade support materials and development workshops.

Finally, all companies can participate in and sponsor activities in this medium (see SchoolWeb, page 9). Corporations outside the educational system that would like to help can sponsor discussions, MOOs and other multi-user spaces. They can make interested employees available for online discussions, or merely to answer relevant e-mail, just as today they lend employees to local schools, colleges and other institutions. Online help is likely to be less intrusive and expensive than sabbaticals or other programs, though it could easily get very time-consuming. Of course, we always encourage the local face-to-face stuff.

Release 1.0 24 April 1995
RESOURCES & PHONE NUMBERS

Keith Kruger, Consortium for School Networking (CoSN), (202) 462-9600 x18; fax, (202) 462-9043; e-mail, keith@cosn.org

Andy Carvin, Corporation for Public Broadcasting (EdWeb), (202) 879-9824; fax, (202) 783-1019; e-mail, acarvin@k12.cnidr.org

Pegeen Wright, Houghton-Mifflin, (617) 351-5021; fax, (617) 351-1124; e-mail, wrightp@hmco.com

Terry Bryan, Ingenius, (303) 267-4125; fax, (303) 267-4172

Judi Clark, ManyMedia, (415) 494-9104; fax, (415) 494-9105; e-mail, judi@manymedia.com

Amy Bruckman, MIT Media Lab, (617) 253-5108; fax, (617) 258-6264; e-mail, asb@media.mit.edu

Cheryl Vedoe, Tenth Planet, (415) 726-5891 x260; fax, (415) 726-5995; e-mail, cvedoe@tenthplanet.com

Frank Moretti, The Dalton School, (212) 423-5360; fax, (212) 423-5372; e-mail, moretti.f@nitl.columbia.edu

Gwen Solomon, US Dept. of Education, (202) 401-1667; fax, (202) 401-3093; e-mail, gwen_solomon@ed.gov

COMING SOON

• Links and link management.
• Navigation & the semiotics of cyberspace.
• Advanced user interfaces.
• Web authoring tools.
• The analog world.
• And much more... (If you know of any good examples of the categories listed above, please let us know.)

-----------------------------

Release 1.0 is published monthly, except for a combined July/August issue, by EDventure Holdings, 104 Fifth Ave., New York, NY 10011-6901; (212) 924-8800; fax, (212) 924-0240. It covers PCs, software, the Internet, computer-telephone integration, online services, groupware, text management, connectivity, messaging, wireless communications, artificial intelligence, intellectual property law and other unpredictable topics. A companion publication, Rel-EAST, is an information bulletin on emerging technology markets in Central Europe and the former Soviet units. Editor: Esther Dyson (edyson@eff.org); publisher: Daphne Kis (daphne@edventure.com); managing editor: Jerry Michalski (spiff@panix.com); circulation & fulfillment manager: Robyn Sturm (robyn@edventure.com); executive assistant: Christina Koukkos (6877695@mciemail.com); editorial & marketing communications consultant: William M. Kutik (kutik@edventure.com). Copyright 1995, EDventure Holdings Inc. All rights reserved. No material in this publication may be reproduced without written permission; however, we gladly arrange for reprints or bulk purchases. Subscriptions cost $595 per year, $650 overseas.

Release 1.0 24 April 1995
WEB RESOURCES

Berit’s Children’s Sites http://www.coehran.com/theosite/KSites.html
EdWeb (Andy Garvin) http://edweb.cnidr.org:90/resource.cntnts.html
Geometry Forum (Swarthmore) http://forum.swarthmore.edu/index.html
Gleason Sackman’s List Of K-12 Sites http://toons.cc.ndsu.nodak.edu/sackmann/state.html
Global Schoolhouse http://k12.cnidr.org/gsh/gshwelcome.html
Global Show-n-Tell (Judi Clark) http://www.manymedia.com/show-n-tell/
Hillside Elementary School http://hillside.coled.umn.edu/
Jason Project http://seawifs.gsfc.nasa.gov/scripts/JASON.html
John Makulowich’s KID list http://www.clark.net/pub/journalism/kid.html
KidsCom http://spectracom.com/kidscom/
KIDS Web http://www.npac.syr.edu/textbook/kidsweb/
KIE Project http://kle.berkeley.edu/kie.html
Los Alamos High School http://laahs.losalamos.k12.nm.us/
MidLink Magazine http://longwood.cs.ucf.edu/MidLink/
Patch American High School (Germany) http://192.253.114.31/Home.html
Scholastic Central http://scholastic.com:2005/
Sunrise project http://www.ac1.lanl.gov/sunrise/sunrise.html
Teacher’s Place (Classroom Connect) http://www.wentworth.com/classroom/teachers.htm
Web 66 http://web66.coled.umn.edu/
WebMuseum (Nicolas Pioch) http://www.cnam.fr/louvre/
Yahoo: Education http://www.yahoo.com/Education/

Release 1.0 24 April 1995
<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>April 24-25</td>
<td>Multimedia Publishing for the Education Market - Chicago. Sponsored by AIC Conferences and Multimedia Week. Call (800) 826-2424 or (617) 742-5200; fax, (617) 742-1028.</td>
</tr>
<tr>
<td>April 24-27</td>
<td>@Comdex Spring '95 - Atlanta, GA. Organized by the Interface Group. With Jerry Michalski on commerce and wireless e-mail. Call Sue Lonergan, (617) 449-6600; fax, (617) 449-6953.</td>
</tr>
<tr>
<td>May 1-2</td>
<td>U.S. Copyright Office Speaks - Washington, DC. Sponsored by Aspen Law &amp; Business in cooperation with The United States Copyright Office. Call Margaret Ross, (201) 894-8260; fax, (201) 894-0074.</td>
</tr>
<tr>
<td>May 2-4</td>
<td>National Online Meeting &amp; Integrated Online Library Systems '95 - New York City. Sponsored by Learned Information. Bulletin boards, online services and more. Register at (609) 654-6266; fax, (609) 654-4309.</td>
</tr>
<tr>
<td>May 2-5</td>
<td>@Ties That Bind: Converging Communities - Cupertino, CA. Organized by Apple Library of Tomorrow and the Morino Institute. See what's cooking at the local level: Freenets, civic nets and more. Call Pam Lau, (408) 974-2400.</td>
</tr>
<tr>
<td>May 5</td>
<td>The Future of Wireless Communication: Recent Developments - New York City. Organized by the Columbia Business School Institute for Tele-Information. Call Bruce Egan or Kevin Holmes at (212) 932-7816; fax (212) 854-4222; e-mail, <a href="mailto:citi@research.gsb.columbia.edu">citi@research.gsb.columbia.edu</a>.</td>
</tr>
<tr>
<td>May 7-11</td>
<td>CHI '95: Mosaic of Creativity - Denver. Sponsored by ACM/SIGCHI. Always chock-full of inspiring ideas. Call Debbie Compere, (410) 263-5382; fax, (410) 267-0332 or Rosemary Stevens, (415) 328-3600; fax, (415) 323-2172; e-mail, <a href="mailto:chi95-office@sigchi.acm.org">chi95-office@sigchi.acm.org</a>.</td>
</tr>
<tr>
<td>May 11-12</td>
<td>Electronic Banking '95 - Washington, DC. Sponsored by the Institute of International Research. Call Rosemary Stabile, (800) 345-8016 or (212) 661-8740; fax, (212) 661-6677.</td>
</tr>
</tbody>
</table>

Release 1.0 24 April 1995
May 14-17  Interactive95 - Anaheim. Sponsored by Softbank Institute. Call David Holcombe, (800) 34-TRAIN; fax, (617) 393-3322.

May 15-17  Complexity and Strategy: The Intelligent Organization - London. Sponsored by The Santa Fe Institute and The Praxis Group. Call The Praxis Group, (800) 771-4770 or (505) 466-4400; fax, (505) 466-4012; e-mail, praxis@santafe.edu.


May 22-23  Multimedia Development Partnerships - San Francisco. Sponsored by AIC Conferences. Call Elizabeth Lizzas, (212) 952-1899 x335 or to register (800) 409-4AIC; fax, (212) 248-7374.


May 29-June 2  Networld + Interop - Frankfurt, Germany. Sponsor: Seybold Seminars. Call Christi Leer, (415) 578-6985 or (800) 488-2883; fax, (415) 525-0183.

May 31-June 2  Data Fusion - Washington, DC. Sponsor: Seybold Seminars. Call Christi Leer, (415) 578-6985 or (800) 488-2883; fax, (415) 525-0183.

May 31-June 2  The Global Online Services Summit - Brussels. Sponsored by Jupiter Communications. Call Harry Larson, (212) 941-9252; fax, (212) 941-7376; e-mail, jupiter@jup.com.

June 1-2  Licensing Law Institute - New York City. Sponsored by Aspen Law & Business. Call Margaret Ross (201) 894-8260; fax, (201) 894-0074.

June 4-6  cyber.Xpo.95 - Las Vegas. Sponsored by Sysop News. Call Denise Northop, (614) 452-4541 x3124; fax, (614) 452-2552; e-mail, cyberxpo@muskingum.edu.

June 5-6  U.S. Copyright Office Speaks - Washington, DC. Sponsored by Aspen Law & Business in cooperation with The United States Copyright Office. Call Margaret Ross, (201) 894-8260; fax, (201) 894-0074.

June 5-7  Digital World - Los Angeles. Sponsor: Seybold Seminars. Call Alison Murdoch, (415) 578-6887 or (800) 488-2883; fax, (415) 525-0183.


June 7-9  TAG's Retail Compass Conference - San Jose. Sponsored by TAG's Channel Compass, TWICE magazine and SMART magazine. Call Linda Gillette, (415) 957-9433; fax, (415) 957-0504.


June 12-16  WIN-DEV 1995/The International Developers Conference for Windows - Boston. Organized by the Boston University Center
June 13-16
Ninth Workshop on Parallel and Distributed Simulation - Lake Placid, NY. Sponsors: ACM, IEEE/TCSIM, and SCS. Call Jason Yi-Bing Lin, (201) 829-5095; fax, (201) 829-5886.

June 14-15

June 19-20

June 20-22
Community Networking Workshop - Princeton, NJ. Sponsored by the IEEE Communications Society. Call Joel Winthrop, (908) 949-5008; fax, (908) 949-8569.

June 20-22
@PC Expo - New York City. Organized by Bruno Blenheim. Call Annie Scully, (800) 829-3976 or (201) 346-1400; fax, (201) 346-1532.

June 27-28
@Interactive Advertising - New York City. Sponsored by AIC Conferences. With Jerry Michalski playing emcee the first day. Call Trina Johnston, (212) 952-1899, x334; fax, (212) 248-7374.

June 28-30
INET '95 - Honolulu. Sponsored by the Internet Society. Call them at (703) 648-9888; fax, (703) 648-9887; e-mail, mburger@isoc.org.

July 9-12
The Burton Group Conference on Network Computing - Colorado Springs. Sponsored by The Burton Group. Call Doug Allinger, (800) 824-9924 or (801) 943-1966; fax, (801) 943-242; e-mail, info@tbg.com.

July 17-20

July 23-26

August 16-19
AI-ED '95: 7th World Conference on Artificial Intelligence in Education - Washington, DC. Sponsor: Association for the Advancement of Computing in Education. Call Gary Marks, (804) 973-3987; fax, (804) 978-7449; e-mail, AACE@virginia.edu.

August 16-20

August 20-25

August 23-25

September 11-15
EGSW '95 - Stockholm. Sponsor: Foundation for Cooperative Work Technology. Call Yngve Sundblad, 46 (8) 102-477; fax, 46 (8) 790-6280; e-mail, ecschw95@kth.se.

September 11-15
Information Superhighway Summit - Santa Clara. Produced by IDG World Expo. To register call (800) 225-4698 or (508) 879-

Networks Expo '95 - Dallas. Organized by Bruno Blenheim. Call Annie Scully, (800) 829-3976 or (201) 346-1400; fax, (201) 346-1532.

@Unix Expo - New York City. Organized by Bruno Blenheim. Call Annie Scully, (800) 829-3976 or (201) 346-1400; fax, (201) 346-1532.


PC Expo Home - New York City. Organized by Bruno Blenheim. Call Annie Scully, (800) 829-3976 or (201) 346-1400; fax, (201) 346-1532.


PC Expo - Chicago. Organized by Bruno Blenheim. Call Annie Scully, (800) 829-3976 or (201) 346-1400; fax, (201) 346-1532.


**East-West High-Tech Forum - Bled, Slovenia. The sixth annual sponsored by EDventure Holdings. Call Daphne Kis, (212) 924-8800; fax, (212) 924-0240; e-mail, info@edventure.com.

OOPSLA-95 - Austin. Organized by OOPSLA-95 Conference Committee. Call Karen Breedlove, (503) 691-0890; fax, (503) 691-1821; e-mail, oops95@applelink.apple.com.

8th International Symposium on AI - Monterrey, Mexico. Organized by ITESM. Call Jose Sanchez, 52 (8) 328-4197; fax, 52 (8) 328-4189.

* Events Esther plans to attend.
@ Events Jerry plans to attend.

Lack of a symbol is no indication of lack of merit.
Please let us know about other events we should include. -- Christina Koukkos

Release 1.0 24 April 1995
Please enter my subscription to Release 1.0 at the rate of $595 per year in the
U.S. and Canada. Overseas subscriptions are $650, airmail postage included. Payment
must be enclosed. Multiple-copy rates available on request. Satisfaction guaranteed
or your money back.

Name _____________________________________________
Title _____________________________________________
Company ___________________________________________
Address ___________________________________________
City________________________________ State ________ Zip________
Telephone ________________________________________

☐ Check enclosed.
☐ Charge my
  ☐ American Express ☐ MasterCard ☐ Visa
  Card Number ___________________________ Expiration Date ____________
  Name on Card ________________________ Signature __________________

☐ Please send me information on your multiple-copy rate.

Please fill in the information above and send to:

EDVENTURE HOLDINGS INC.
104 FIFTH AVENUE, 20TH FLOOR
NEW YORK, NY 10011

If you have any questions, please call us at 1 (212) 924-8800;
Fax 1 (212) 924-0240; e-mail info@edventure.com.

Daphne Kis
Publisher