7

Crypto Anarchy and Virtual Communities

Timothy C. May

Modern Cryptography

The past two decades have produced a revolution in cryptography (crypto, for short)—the science of the making of ciphers and codes. Beyond just simple ciphers, useful mainly for keeping communications secret, modern crypto includes diverse tools for authentication of messages, for digital time stamping of documents, for hiding messages in other documents (steganography), and even for schemes for digital cash.

Public key cryptography, the creation of Diffie and Hellman, has dramatically altered the role of crypto. Coming at the same time as the wholesale conversion to computer networks and worldwide communications, it has been a key element of security, confidence, and success. The role of crypto will only become more important over the coming decades. Pretty Good Privacy (PGP) is a popular version of the algorithm developed by Rivest, Shamir, and Adleman (known, of course, as RSA). The RSA algorithm was given a patent in the United States, though not in any European countries, and is licensed commercially.[1]

These tools are described in detail in various texts and conference proceedings and are not the subject of this chapter.[2] The focus here is on the implications of strong crypto for cyberspace, especially on virtual communities. Mention should be made of the role of David Chaum in

defining the key concepts here. In several seminal papers,[3] Chaum intro-
duced the ideas of using public key cryptography methods for anony-
mous, untraceable electronic mail, for digital money systems in which
spender identity is not revealed, and in schemes related to these. (I make
no claims that Chaum agrees with my conclusions about the political
and socioeconomic implications of these results.)

Virtual Communities

Notes: cyberspace, Habitat, VR, Vinge, etc. Crypto holds up the "walls"
of these cyberspatial realities. Access control, access rights, modification
privileges.

   Virtual communities are the networks of individuals or groups that
are not necessarily closely connected geographically. The "virtual" is
meant to imply a nonphysical linking but should not be taken to mean
that these are any less communitylike than are conventional physical
communities.

   Examples include churches, service organizations, clubs, criminal
gangs, cartels, fan groups, etc. The Catholic Church and the Boy Scouts
are both examples of virtual communities that span the globe, transcend
national borders, and create a sense of allegiance, of belonging, and a
sense of community. Likewise, the Mafia is a virtual community (with its
enforcement mechanisms, its own extralegal rules, etc.) Lots of other
examples: Masons, Triads, the Red Cross, Interpol, Islam, Judaism,
Mormons, Sindero Luminoso, the IRA, drug cartels, terrorist groups,
Aryan Nation, Greenpeace, the Animal Liberation Front, and so on.
There are undoubtedly many more such virtual communities than there
are nation-states, and the ties that bind them are for the most part much
stronger than are chauvinist nationalist emotions. Any group in which
the common interests of the group, be it a shared ideology or a particu-
lar interest is enough to create a cohesive community.

   Corporations are another prime example of a virtual community, hav-
ing scattered sites, private communication channels (generally inacces-
sible to the outside world, including the authorities), and their own goals
and methods. In fact, many "cyberpunk" (not cypherpunk) fiction
authors make a mistake, I think, in assuming the future world will be

dominated by transnational megacorporate "states." In fact, corporations are just one example of many of such virtual communities that will be effectively on a par with nation states. (Note especially that any laws designed to limit use of crypto cause immediate and profound problems for corporations and that countries like France and the Philippines, which have attempted to limit the use of crypto, have mostly been ignored by corporations. Any attempts to outlaw crypto will produce a surge of sudden "incorporations," thus gaining for the new corporate members the aegis of corporate privacy.) In an academic setting, "invisible colleges" are the communities of researchers.

These virtual communities typically are "opaque" to outsiders. Attempts to gain access to the internals of these communities are rarely successful. Law-enforcement and intelligence agencies (such as the National Security Agency in the United States, Chobetsu in Japan, SDECE in France, and so on) may infiltrate such groups and use electronic surveillance (ELINT) to monitor these virtual communities. Not surprisingly, these communities have been early adopters of encryption technology, ranging from scrambled cellphones to full-blown PGP encryption.[4]

The use of encryption by "evil" groups—such as child pornographers, terrorists, abortionists, and abortion protesters—is cited by those who wish to limit civilian access to crypto tools. We call these groups the "Four Horsemen of the Infocalypse," as they are so often cited as the reason that ordinary citizen units of the nation state should not have access to crypto.

This is clearly a dangerous argument to make, for various good reasons. The basic right of free speech is the right to speak in a language one's neighbors or governing leaders may not find comprehensible—encrypted speech. There's not enough space here to go into the many good arguments against a limit on access to privacy, communications tools, and crypto.

The advent of full-featured communications systems for computer-mediated virtual communities will have even more profound implications. MUDs and MOOs (multi-user domains, etc.) and 3D virtual realities are one avenue, and text-centric Net communications are another. (Someday, soon, they'll merge, as described in Vernor Vinge's prophetic 1980 novella, *True Names*.)

Observability and Surveillance

An interesting way to view issues of network visibility is in terms of the transparency of nodes and links between nodes. *Transparent* means visible to outsiders, perhaps those in law enforcement or the intelligence community. *Opaque* means not transparent, not visible. A postcard is transparent; a sealed letter is opaque. PGP inventor Phil Zimmermann has likened the requirement for transparency to being ordered to use postcards for all correspondence, with encryption the equivalent of an opaque envelope (envelopes can be opened, of course, and long have been).

Transparent links and nodes are the norm in a police state, such as the former Soviet Union, Iraq, China, and so forth. Communications channels are tapped, and private use of computers is restricted. (This is becoming increasingly hard to do, even for police states; many cite the spread of communications options as a proximate cause of the collapse of communism in recent years.)

There are interesting "chemistries" or "algebras" of transparent versus opaque links and nodes. What happens if links must be transparent but nodes are allowed to be opaque? (The answer: the result is the same as if opaque links and nodes were allowed—that is, the full implications of strong crypto. Hence, any attempt to ban communications crypto while still allowing private CPUs to exist....)

If Alice and Bob are free to communicate, and to choose routing paths, then Alice can use "crypto arbitrage" (a variation on the term, "regulatory arbitrage," the term Eric Hughes uses to capture this idea of moving transactions to other jurisdictions) to communicate with sites—perhaps in other countries—that will perform as she wishes. This can mean remailing, mixing, etc. As an example, Canadian citizens who are told they cannot access information on the Homolka-Teale murder case (a controversial case in which the judge has ordered the media in Canada and entering Canada not to discuss the gory details) nevertheless have a vast array of options, including using telnet, gopher, ftp, the Web, etc., to access sites in many other countries or even in no country in particular.

Most of the consequences described here arise from this chemistry of links and nodes: unless nearly all node and links are forced to be trans-

parent, including links to other nations and the nodes in those nations, then private communication can still occur. Crypto anarchy results.

Crypto Anarchy

"The Net is an anarchy." This truism is the core of crypto anarchy—no central control, no ruler, no leader (except by example or reputation), no "laws." No single nation controls the Net, no administrative body sets policy. The Ayatollah in Iran is as powerless to stop a newsgroup—alt.wanted.moslem.women or alt.wanted.moslem.gay come to mind—he doesn't like as the president of France is as powerless to stop, say, the abuse of the French language in soc.culture.french. Likewise, the CIA can't stop newsgroups, sites, or Web pages that give away its secrets. At least not in terms of the Net itself. What non-Net steps might be taken are left as an exercise for the paranoid and the cautious.

This essential anarchy is much more common than many think. Anarchy (the absence of a ruler telling another person what to do) is common in many walks of life—choosing books to read, movies to see, friends to socialize with, and so on. Anarchy does not mean complete freedom (we can, after all, read only the books that someone has written and had published), but it does mean freedom from external coercion. Anarchy as a concept, though, has been tainted by other associations.

First, the anarchy here is not the anarchy of popular conception—lawlessness, disorder, and chaos. Nor is it the bomb-throwing anarchy of the nineteenth century "black" anarchists, usually associated with Russia and labor movements. Nor is it the "black flag" anarchy of anarcho-syndicalism and writers such as Proudhon. Rather, the anarchy being spoken of here is the anarchy of "absence of government" (literally, "an arch," without a chief or head).

This is the same sense of anarchy used in anarchocapitalism, the libertarian free-market ideology that promotes voluntary, uncoerced economic transactions.[5] I devised the term *crypto anarchy* as a pun on crypto, meaning "hidden," on the use of "crypto" in combination with political views (as in Gore Vidal's famous charge to William F. Buckley: "You're crypto fascist!") and of course because the technology of crypto makes this form of anarchy possible. The first presentation of this term was in a 1988 "Manifesto," whimsically patterned after another famous

manifesto.[6] Perhaps a more popularly understandable term, such as "cyber liberty," might have some advantages, but crypto anarchy has its own charm, I think.

And *anarchy* in this sense does not mean that local hierarchies don't exist or that no rulers exist. Groups outside the direct control of local governmental authorities may still have leaders, rulers, club presidents, elected bodies, etc. Many will not, though.

Politically, virtual communities outside the scope of local governmental control may present problems of law enforcement and tax collection. (Some of us like this aspect.) Avoidance of coerced transactions can mean avoidance of taxes, avoidance of laws saying who one can sell to and who one can't, and so forth. It is likely that many will be unhappy that some are using cryptography to avoid laws designed to control behavior.

National borders are becoming more transparent than ever to data. A flood of bits crosses the borders of most developed countries' phone lines, cables, fibers, satellite up/downlinks, and millions of diskettes, tapes, CDs, etc. Stopping data at the borders is less than hopeless.

Finally, the ability to move data around the world at will, the ability to communicate to remote sites at will, means that a kind of "regulatory arbitrage" can be used to avoid legal roadblocks. For example, when remailing into the United States from a site in the Netherlands, whose laws apply? (If one thinks that U.S. laws should apply to sites in the Netherlands, then does Iraqi law apply in the United States? And so on.)

This regulatory arbitrage is also useful for avoiding the welter of laws and regulations that operations in one country may face, including the "deep pockets" lawsuits so many in the United States face. Moving operations on the Net outside a litigious jurisdiction is one step to reduce this business liability. Like Swiss banks, but different.

True Names and Anonymous Systems

Something needs to be said about the role of anonymity and digital pseudonyms. This is a topic for an essay unto itself, of course.

Are true names really needed? Why are they asked for? Does the nation state have any valid reason to demand they be used?

People want to know who they are dealing with, for psychological/ evolutionary reasons and to better ensure traceability should they need to locate a person to enforce the terms of a transaction. The purely anonymous person is perhaps justifiably viewed with suspicion.

And yet pseudonyms are successful in many cases. We rarely know whether someone who presents himself by some name is "actually" that person. Authors, artists, performers, etc., often use pseudonyms. What matters is persistence and nonforgeability. Crypto provides this.

On the Cypherpunks[7] mailing list, well-respected digital pseudonyms have appeared and are thought of no less highly than their "real" colleagues are.

The whole area of digitally authenticated reputations, and the "reputation capital" that accumulates or is affected by the opinions of others, is an area that combines economics, game theory, psychology, and expectations. A lot more study is needed. It is unclear if governments will move to a system of demanding "Information Highway Driver's Licenses," figuratively speaking, or how systems like this could ever be enforced. (The chemistry of opaque nodes and links, again.)

Examples and Uses

It surprises many people that some of these uses are already being intensively explored. Anonymous remailers are used by tens of thousands of persons—and perhaps abused.[8] And of course encryption, via RSA, PGP, etc., is very common in some communities (hackers, Net users, freedom fighters, white separatists, etc. . . . I make no moral judgments here about people who use these methods).

Remailers are a good example to look at in more detail. There are two current main flavors of remailers:

• Cypherpunk-style remailers process text messages to redirect mail to other sites, using a command syntax that allows arbitrary nesting of remailing (as many sites as one wishes) with PGP encryption at each level of nesting.

• Julf-style remailers are based on the original work of Karl Kleinpaste and are operated/maintained by Julf Helsingius in Finland. No encryption, and only one such site at present. (This system has been used extensively for messages posted to the Usenet and is basically successful.

The model is based on operator trustworthiness and his location in Finland, beyond the reach of court orders and subpoenas from most countries.)

The Cypherpunks remailers currently number about twenty, with more being added every month. There is no reason not to expect hundreds of such remailers in a few years. One experimental "information market" is BlackNet, a system that appeared in 1993 and that allows fully anonymous, two-way exchanges of information of all sorts. There are reports that U.S. authorities have investigated BlackNet because of its presence on networks at Defense Department research labs. Not much they can do about it, of course, and more such entities are expected.

The implications for espionage are profound and largely unstoppable. Anyone with a home computer and access to the Net or Web, in various forms, can use these methods to communicate securely, anonymously, or pseudonymously and with little fear of detection. "Digital dead drops" can be used to post information obtained, far more securely than the old physical dead drops (no more messages left in Coke cans at the bases of trees on remote roads).

Whistleblowing is another growing use of anonymous remailers, with folks fearing retaliation using remailers to publicly post information. (Of course, there's a fine line between whistle blowing, revenge, and espionage.)

Data havens for the storage and marketing of controversial information is another area of likely future growth. Nearly any kind of information—medical, religious, chemical, etc., is illegal or proscribed in one or more countries, so those seeking this illegal information will turn to anonymous messaging systems to access and perhaps purchase this information with anonymous digital cash. This might include credit databases, deadbeat renter files, organ bank markets, etc. (These are all things which have various restrictions on them in the United States. For example, one cannot compile credit databases or lists of deadbeat renters without meeting various restrictions—a good reason to move them into cyberspace or at least outside the United States and then sell access through remailers.) Matching buyers and sellers of organs is another such market with a huge demand (life and death) but various laws tightly controlling such markets.

Digital cash efforts. A lot has been written about digital cash.[9] David Chaum's company, DigiCash, has the most interesting technology and has recently begun market testing. Stefan Brands may or may not have a competing system that gets around some of Chaum's patents. (The attitude crypto anarchists might take about patents is another topic for discussion. Suffice it to say that patents and other intellectual property issues continue to have relevance in the practical world, despite erosion by technological trends.) Credit card–based systems, such as the First Virtual system, are not exactly digital cash, in the Chaumian sense of blinded notes, but they offer some advantages the market may find useful until more advanced systems are available. I expect to see many more such experiments over the next several years, and some of them will likely be market successes.

Commerce and Colonization of Cyberspace

How will these ideas affect the development of cyberspace? "You can't eat cyberspace" is a criticism often leveled at argument about the role of cyberspace in everyday life. The argument made is that money and resources "accumulated" in some future (or near future) cyberspatial system will not be able to be "laundered" into the real world. Even such a prescient thinker as Neal Stephenson, in *Snow Crash*,[10] had his protagonist a vastly wealthy man in "the Multiverse" but a near pauper in the physical world.

This is implausible for several reasons. First, we routinely see transfers of wealth from the abstract world of stock tips, arcane consulting knowledge, etc., to the real world. "Consulting" is the operative word. Second, a variety of means of laundering money, via phony invoices, uncollected loans, art objects, etc., are well-known to those who launder money.... These methods, and more advanced ones to come, are likely to be used by those who wish their cyberspace profits moved into the real world. (Doing this anonymously and untraceably is another complication. There may be methods of doing this. Proposals have looked pretty solid, but more work is needed.)

The World Wide Web is growing at an explosive pace. Combined with cryptographically protected communication and digital cash of some

form (and there are several being tried), this should produce the long-awaited colonization of cyberspace. Most Net and Web users already pay little attention to the putative laws of their local regions or nations, apparently seeing themselves more as members of various virtual communities than as members of locally governed entities.

This trend is accelerating.

Most important, information can be bought and sold (anonymously, too) and then used in the real world. There is no reason to expect that this won't be a major reason to move into cyberspace.

Implications

I've touched on the implications in several places. Many thoughtful people are worried about some of the possibilities made apparent by strong crypto and anonymous communication systems. Some are proposing restrictions on access to crypto tools. The recent debate in the United States over Clipper and other key escrow systems shows the strength of emotions generated by this issue.

Abhorrent markets may arise. For example, anonymous systems and untraceable digital cash have some obvious implications for the arranging of contract killings and such. (The greatest risk in arranging such hits is that physical meetings expose the buyers and sellers of such services to stings. Crypto-anarchy lessens, or even eliminates, this risk, thus lowering transaction costs. The risks to the actual triggermen are not lessened, but this is a risk the buyers need not worry about. Think of anonymous escrow services which hold the digital money until the deed is done. Lots of issues here. It is unfortunate that this area is so little-discussed.... People seem to have an aversion for exploring the logical consequences in such areas.) The implications for corporate and national espionage have already been touched upon. Combined with liquid markets in information, this may make secrets much harder to keep. (Imagine a "Digital Jane's," after the military weapons handbooks, anonymously compiled and sold for digital money, beyond the reach of various governments which don't want their secrets told.)

New money-laundering approaches are another area to explore.

Something that is inevitable is the increased role of individuals, leading to a new kind of elitism. Those who are comfortable with the tools

described here can avoid the restrictions and taxes that others cannot. If local laws can be bypassed technologically, the implications are pretty clear.

The implications for personal liberty are of course profound. No longer can nation-states tell their citizen-units what they can have access to, not if these citizens can access the cyberspace world through anonymous systems.

How Likely?

I am making no bold predictions that these changes will sweep the world anytime soon. Most people are ignorant of these methods, and the methods themselves are still under development. A wholesale conversion to "living in cyberspace" is just not in the cards, at least not in the next few decades. But to an increasingly large group, the Net is reality. It is where friends are made, where business is negotiated, where intellectual stimulation is found. And many of these people are using crypto-anarchy tools. Anonymous remailers, message pools, information markets. Consulting via pseudonyms has begun to appear and should grow. (As usual, the lack of a robust digital cash system is slowing things down.)

Can crypto-anarchy be stopped? Although the future evolution in unclear, as the future almost always is, it seems unlikely that present trends can be reversed:

· Dramatic increases in bandwidth and local, privately owned computer power,
· Exponential increase in the number of Net users,
· Explosion in degrees of freedom in personal choices, tastes, wishes, and goals, and
· Inability of central governments to control economies, cultural trends, and so on.[11]

The Net is integrally tied to economic transactions, and no country can afford to "disconnect" itself from it. (The U.S.S.R. couldn't do it, and they were light-years behind the U.S., European, and Asian countries.) And in a few more years, no hope of limiting these tools at all, something the U.S. F.B.I. has acknowledged.[12]

Technological Inevitability: These tools are already in widespread use, and only draconian steps to limit access to computers and communications channels could significantly impact further use. (Scenarios for restrictions on private use of crypto.)

As John Gilmore has noted, "The Net tends to interpret censorship as damage, and routes around it." This applies as well to attempts to legislate behavior on the Net. (The utter impossibility of regulating the worldwide Net—with entry points in more than a hundred nations, with million of machines—is not yet fully recognized by most national governments. They still speak in terms of "controlling" the Net, when in fact the laws of one nation generally have little use in other countries.)

Digital money in its various forms is probably the weakest link at this point. Most of the other pieces are operational, at least in basic forms, but digital cash is (understandably) harder to deploy. Hobbyist or "toy" experiments have been cumbersome, and the "toy" nature is painfully obvious. It is not easy to use digital cash systems at this time ("To use Magic Money, first create a client ..."), especially as compared to the easily understood alternatives.[13] People are understandably reluctant to entrust actual money to such systems. And it's not yet clear what can be bought with digital cash (a chicken or egg dilemma that is likely to be resolved in the next several years). Digital cash, digital banks, etc., are a likely target for legislative moves to limit the deployment of crypto anarchy and digital economies. Whether through banking regulation or tax laws, it is not likely that digital money will be deployed easily ("Kids, don't try this at home!").

Some of the current schemes may also incorporate methods for reporting transactions to the tax authorities and may include "software key escrow" features that make transactions fully or partly visible to authorities.

Conclusions

Strong crypto provides new levels of personal privacy, all the more important in an era of increased surveillance, monitoring, and the temptation to demand proofs of identity and permission slips. Some of the "credentials without identity" work of Chaum and others may lessen this move toward a surveillance society.

The implications are, as I see it, are that the power of nation states will be lessened, tax collection policies will have to be changed, and economic interactions will be based more on personal calculations of value than on societal mandates.

Is this a Good Thing? Mostly yes. Crypto anarchy has some messy aspects, of this there can be little doubt. From relatively unimportant things like price fixing and insider trading to more serious things like economic espionage, the undermining of corporate knowledge ownership, to extremely dark things like anonymous markets for killings.

But let's not forget that nation states have, under the guise of protecting us from others, killed more than 100 million people in this century alone. Mao, Stalin, Hitler, and Pol Pot, just to name the most extreme examples. It is hard to imagine any level of digital contract killings ever coming close to nationstate barbarism. (But I agree that this is something we cannot accurately speak about; I don't think we have much of a choice in embracing crypto anarchy or not, so I choose to focus on the bright side.) It is hard to argue that the risks of anonymous markets and tax evasion justify worldwide suppression of communications and encryption tools. People have always killed each other, and governments have not stopped this (arguably, they make the problem much worse, as the wars of this century have shown).

Also, there are various steps that can be taken to lessen the risks of crypto-anarchy impinging on personal safety.[14]

Strong crypto provides a technological means of ensuring the practical freedom to read and write what one wishes to. (Albeit perhaps not in one's true name, as the nation-state-democracy will likely still try to control behavior through majority votes on what can be said, not said, read, not read, etc.) And of course if speech is free, so are many classes of economic interaction that are essentially tied to free speech.

A phase change is coming. Virtual communities are in their ascendancy, displacing conventional notions of nationhood. Geographic proximity is no longer as important as it once was.

A lot of work remains. Technical cryptography still hasn't solved all problems, the role of reputations (both positive and negative) needs further study, and the practical issues surrounding many of these areas have barely been explored. We will be the colonizers of cyberspace.

Notes

1. RSA Data Security Inc., Redwood Shores, California, is the license administrator. Contact them for details.

2. Many cryptography texts exist. A good introduction is Bruce Schneier's *Applied Cryptography* (2nd ed.) (New York: Wiley, 1996). This text includes pointers to many other sources. The annual Crypto Proceedings (*Advances in Cryptology*) (Berlin: Springer-Verlag) are essential references. The annual crypto conference in Santa Barbara and the Eurocrypt and Auscrypt conferences are where most crypto results are presented.

3. David Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms," Communications of the Association for Computing Machinery 24 (February 2, 1981): 84–88 (cypherpunk-style remailers are a form of Chaum's "digital mixes," albeit far from ideal); David Chaum, "Security without Identification: Transaction Systems to Make Big Brother Obsolete," Communications of the Association for Computing Machinery 28 (October 10, 1985) (this early paper is on digital cash; be sure to consult more recent papers).

4. The political opposition in Myan Mar—formerly Burma—is using Pretty Good Privacy running on DOS laptops in the jungles for communications among the rebels, according to Phil Zimmermann, author of PGP. This life-and-death usage underscores the role of crypto.

5. David Friedman, *The Machinery of Freedom: Guide to a Radical Capitalism* (2nd ed.) (Ashland, Olt: Open Court, 1989), is leading theoretician of anarchocapitalism. Friedrich Hayek was another.

6. Timothy C. May, "The Crypto Anarchist Manifesto," July 1988, distributed on the Usenet and on various mailing lists. Also included in this book as chapter 6.

7. The Cypherpunks group was mainly formed by Eric Hughes, John Gilmore, and me. It began with physical meetings in the Bay Area and elsewhere and with virtual meetings on an unmoderated mailing list. The name was provided by Judith Milhon as a play on the cyberpunk fiction genre and the British spelling of *cipher*. The mailing list can be subscribed to by sending the single message,

subscribe cypherpunks, in the body of a message to majordomo@toad.com. Expect at least fifty messages a day. About six hundred subscribers in many countries are presently on the list. Some are pseudonyms.

8. Abuse, according to some views, of remailers is already occurring. A Cypherpunks-style remailer was used to post a proprietary hash function of RSA Data Security, Inc. to the Usenet. Let me hasten to add that it was not a remailer I operate or have control over.

9. Article on digital cash, *The Economist*, 26 November 1994, pp. 21–23. Article on digital cash, Steven Levy, *Wired* (December 1994).

10. Neal Stephenson, *Snow Crash* (New York: Bantam, 1995).

11. See Kevin Kelly's *Out of Control: The Rise of Neo-Biological Civilization* (Reading, MA: Addison Wesley, 1994) for a discussion of how central control is failing and how the modern paradigm is one of market mechanisms, personal choice, and technological empowerment.

12. During the debate on the digital telephony bill, an FBI official said that failure to mandate wiretap capabilities within eighteen months would make the bill moot as the cost would rise beyond any reasonable budget (currently $500 million for retrofit costs).

13. "Magic Money" was an experimental implementation of Chaum's digital cash system. It was coded by "Pr0duct Cypher," a pseudonymous member of the Cypherpunks list. None of us knows his real identity, as he used remailers to communicate with the list, and digitally signed his posts. Many of us found it too difficult to use, which is more a measure of the deep issues involved in using digital analogs (no pun intended) to real, physical money.

14. Robin Hanson and David Friedman have written extensively about scenarios for dealing with the threats of extortionists, would-be assassins, and so on. Much of their discussion took place in 1992 and 1993, on the Extropians mailing list.