Perspectives on Financial Cryptography

Ronald L. Rivest

MIT Lab for Computer Science
(RSA / Security Dynamics)
rivest@theory.lcs.mit.edu

Abstract. I present some *debatable propositions* about financial systems and financial cryptography. (Warning: the propositions expressed may or may not be believed by the author, and may be phrased in a deliberately provocative manner. They may contradict each other. This paper follows the author's slides closely, and does not have all of the ancillary comments of the author and the audience.)

1 Internet money is the same as Interstellar money

Proposition 1: *There is little difference between Internet payment schemes and interstellar payment schemes.*

In 2097, you will buy info off the GGG (the Grand Galactic Grid, successor to the WWW) with "starbucks."

Is galactic space very different than cyberspace? (Think of star systems as analogous to computers on the Internet, and interstellar radio communication as a somewhat slower version of the Internet.) Do payment systems need to depend upon physical proximity, national governments, or the ability to haul someone off to jail? One can hope that trade in the Galactic Federation will be based on more than simple barter.

2 Most payment schemes haven't worked well

Proposition 2: *Historically, most payment schemes haven't worked very well.*

Good references on payment systems are Weatherford's *History of Money*[3] and Galbraith's *Money*[2].

- *Commodities* (metal, tobacco, wampum, cocoa beans, etc.) have problems with weighing, purity, quality, deterioration, transportation, storage, theft.
- *Coins* (invented in the western world in Lydia, around 630 B.C.) have problems with shaving, debasing, theft, and government abuse.
- *Paper money* (seen by Marco Polo in China, reinvented in Italy to help get around usury laws, and used widely in colonial U.S.) has problems with counterfeiting (now using computer scanners and color printers), and government abuse (inflation).

– *Checks* (invented in England around 1770) has problems with forgery, insolvency of the signer, check-washing, etc.
– *Credit cards* (invented in the U.S. in 1950 for Diner's Club) have problems with theft, counterfeiting, non-payment, etc.

Thus, the standard that electronic money has to beat is not very high. However, electronic money may have its own risks, such as hyperinflation, system collapse, and criminal activities protected by anonymity.

3 Everyone will "make money"

Proposition 3: *Electronic cash systems will enable anyone with a PC to be a "mint" for his own brand of currency.*

The world is becoming more decentralized, more distributed, more "democratic." Just as the printing press enables the common man to possess books, the PC enables anyone to mint cryptographically secure digital money.

Thousands of digital currencies will exist and be traded. For example, multinational corporations such as McDonald's or Microsoft will issue their own currencies. Appropriate discount rates will be applied when exchanging the currencies of poorly-rated issuers.

Central banks will have a smaller role to play, as their role is just to ensure the stability of the national currencies.

4 The dollar stays around

Proposition 4: *Cyberbucks won't displace national currencies.*

For a contrary view, read *The Sovereign Individual* by James Davidson and Lord William Rees-Mogg[1] wherein governments will implode as their debts spiral and their tax base disappears into cyberspace tax havens based on gold-backed Internet dollars.

5 Privacy is already lost

Proposition 5: *Individual privacy is already lost, and must be regained.*

All information about individuals is now electronic form, and is bought and sold.

There is strong economic incentive for "user profiling" by merchants, card issuers, etc.

6 User Profiling Not So Bad?

Proposition 6: *User profiling has a definite "up side" for the user*

User profiling can result in reduction of unwanted marketing mail. Both the user and the advertiser both agree that mail sent to the user should be interesting to user.

Spending profiles aid fraud detection.

7 No anonymity for large payments

Proposition 7: *Governments will not allow payment systems to support true (payer or payee) anonymity for large payments.*

This is for law-enforcement reasons:

- *No payer anonymity:* To discourage bribery, kickbacks, and improper political contributions.
- *No payee anonymity:* To discourage extortion, blackmail, kipnapping, etc.

Thus, anonymity will only work for small payments.

8 No anonymity for small payments

Proposition 8: *Achieving payer anonymity for small payments by cryptographic means is too expensive (in terms of complexity and cpu time).*

Isn't it just easier to pass very strong privacy-protection laws about the gathering and use of personal spending data?

But implementation costs decrease over time, too...

9 Anonymity to be bought and sold

Proposition 9: *Anonymity will be a value-added feature that a user may purchase. Conversely, a user may break his own anonymity in a transaction, for a fee.*

Most users may feel that anonymity is a good that he should control, and perhaps sell, but not normally a necessity.

User may reveal his true identity, or else a pseudo-identity (to allow profiling).

10 No multi-app smart cards

Proposition 10: *Multi-application smart cards will never make it big.*

Coordinating issuers is about as easy as making peace in the Middle East.

Security issues on a multi-app card are difficult.

User are comfortable and familiar with having one card per issuer.

Of course, multiple applications from single vendor or issuer may work fine.

11 Anonymity by smart-card choice

Proposition 11: *Anonymity for small-value payments will be arise only from anonymity of card-holder/card relationship.*

Smart cards can be obtained anonymously, as frequently as desired.

Smart card ID is thus a temporary pseudonym for user.

12 Cost of breaking smartcards to rise

Proposition 12: *Smart cards will be "broken into" on a regular basis, but the cost of doing so will rise dramatically over the next decade.*

Smaller feature sizes make requisite lab equipment more expensive.

Vast number of installed smart cards will stimulate further investment into security measures and lower production costs.

Compare: history of bank vaults.

13 No large-value digital coins

Proposition 13: *Digital coins will not be used for large-value transactions.*

In a coin-based system (as opposed to an account-based system), possession of bits means possession of value. Duplication is just too significant a threat.

Identification of double-spenders is unlikely to be a sufficient deterrent to prevent major fraud. (Compare with credit-card theft.)

14 No transferable coins!

Proposition 14: *Payment schemes with off-line coin transfers between users won't make it.*

Need for off-line transfers will decrease dramatically as every device and individual can be "on-line" whenever it wants to.

No good business model: what does coin issuer gain by allowing off-line transferability? (Extra "float" doesn't compensate for extra risk. Contrast with early US bank notes...)

15 Micropayments will thrive

Proposition 15: *Micropayment schemes will be the system of choice for purchasing most information over the Web.*

Most information is low-value (less than 10 cents).

There is still a significant "price umbrella" underneath credit-card transactions (29 cents + 2%).

Latency of response is important. (Not enough time for "serious crypto.")

16 General PKI's not necessary

Proposition 16: *General-purpose public-key infrastructures (PKI's) are not necessary for financial cryptography—they can (and will) be special-cased.*

Name/key binding may be less important than attribute binding (e.g. account is in good standing; merchant has few problems).

17 Money and voting are close.

Proposition 17: *Voting systems and payment systems will be seen as being very close.*

Voting for candidate is like giving $1 coin to candidate so she can bid for and "buy" election. (Using special "registrar currency".)

Anonymity of voting is necessary. (Voting is a great example against universal key escrow or key recovery proposals.)

18 You can get anything you want...

Proposition 18: *"Alice's crypto restaurant" can serve up any feasible combination of system requirements at a workable cost (not necessarily cheap).*

Be careful what you ask for...

Some problems are not technical, but socio-political (whom do you trust?—key recovery, etc.)

19 Conclusions

"Financial cryptography" is an essential component of electronic payment schemes.

Such schemes will augment and largely replace many existing payment schemes, and will offer new features (selective anonymity, interstellar payments...)

References

1. James Dale Davidson and Lord William Rees-Mogg. *The Sovereign Individual: How to Survive and Thrive During the Collapse of the Welfare State.* Simon and Schuster, 1997.
2. John Kenneth Galbraith. *Money: Whence it came, where it went.* Bantam, 1975.
3. Jack Weatherford. *The History of Money.* Crown Publishers, 1997.

This article was processed using the LaTeX macro package with LLNCS style