Perspectives on Financial Cryptography

Ronald L. Rivest

MIT Lab for Computer Science

(RSA / Security Dynamics)

FC97 -- 2/27/97

Outline

◆ I present for your consideration 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.

Internet money ==
Interstellar money   (?)

- *P1: There is little difference between <u>Internet payment schemes</u> and <u>interstellar</u> payment schemes.*

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

Most schemes don't work well.

- *P2: Historically, most payment schemes haven't worked very well.*

- Ref: Weatherford, *History of Money.*

- <u>Commodities</u> (metal, tobacco, wampum, cocoa beans)
  - weighing, purity, quality, deterioration, transportation, storage, theft.

- <u>Coins</u> [Lydia, 630 B.C.]
  - Shaving, debasing, theft, government abuse.

Most schemes don't work well...

- ◆ <u>Paper money</u> (China, Italy, U.S. colonies)
  - – counterfeiting (scanner/printer), government abuse (inflation), or lack of money
- ◆ <u>Checks</u> (England, 1770)
  - – Forgery, insolvency, check-washing, ...
- ◆ <u>Credit cards</u> (U.S., 1950 Diner's Club)
  - – theft, counterfeiting, non-payment, …
- ◆ <u>Electronic money</u>
  - – ?? hyperinflation, system collapse, criminal activities protected by anonymity, … ??

Everyone will "make money"

- *P3: Electronic cash systems will enable anyone with a PC to be a "mint" for his own brand of currency.*

- World is becoming more decentralized, more distributed, more "democratic". (Compare with printing press.)

- Multiple (thousands) of currencies will exist and be traded. Appropriate discount rates will be used for poorly-rated issuers.

- Central banks have a smaller role to play.

The dollar stays around.

- *P4: National currencies won't go away, to be replaced by cyberspace dollars.*

- Ref: *The Sovereign Individual* (James Davidson and Lord William Rees-Mogg), for contrary view: governments will implode as debts spiral and tax base disappears into cyberspace tax havens.

Privacy is already lost

- *P5: Individual privacy is already lost, and must be regained.*

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

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

User Profiling Not So Bad?

- *P6: User profiling has a definite "up side" for the user:*
  - reduction of unwanted marketing mail; user and advertiser both agree that mail sent should be interesting to user.
  - spending profiles aid fraud detection.

No anonymity for large payments

- *P7: Governments will not allow payment systems to support true (payer or payee) anonymity for large payments.*

- This is for law-enforcement reasons:
  - payer anonymity: bribery, kickbacks, political contributions
  - payee anonymity: extortion, blackmail, kipnapping, etc.

- Anonymity will only work for small payments.

No anonymity for small payments

◆ *P8: 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 costs decrease over time, too...

Anonymity to be bought and sold

- ◆ *P9: 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).

No multi-app smart cards

- *P10: 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.

Anonymity by smart-card choice

- *P11: 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 a pseudonym for user. (Nyms are already understood by AOL users…)

Cost of breaking SC's to rise

- *P12: 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: bank safes.

No large-value digital coins

◆ *P13: 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. Replication!

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

No transferable coins!

- ◆ *P14: Payment schemes with off-line coin transfers between users won't make it.*

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

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

Micropayments will thrive

- *P15: Micropayment schemes will be the system of choice for purchasing most information over the Web.*

- Most information is low-value (<10 cents).

- Significant "price umbrella" underneath credit-card transactions (29 cents + 2%).

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

General PKI's not necessary

- *P16: 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).

Money and voting are close.

- *P17: 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. (Special "registrar currency".)

- Anonymity of voting is *necessary.* (This is a great example against key escrow or key recovery.)

You can get anything you want...

- ◆ *P18: "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.)

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…)