CIS / TCOM 551
Networks and Computer Security

Lecture 24

Electronic Commerce

- Credit Card Transactions
  - Physical world requires a signature
  - Credit card companies charge merchant per transaction (usually $0.25)
  - Not good for small payments
- Digital Cash
  - Anonymity
  - Untraceability
  - Unforgeability
- Micropayments

Protocols

- EDI security: ANSI X12.58 or S/MIME.
- Secure Electronic Transaction (SET).
  - Visa and MasterCard.
- CyberCash.
  - Intermediary between Web-based merchants and credit card banks.
- CheckFree.
  - Electronic checks.
- First Virtual.
  - Credit card payments via email.

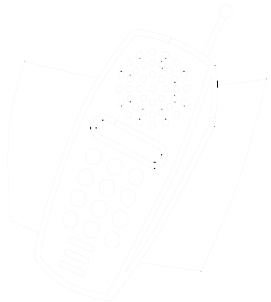
What is a “micropayment”?

(Slides adapted from talks given by Ron Rivest.)

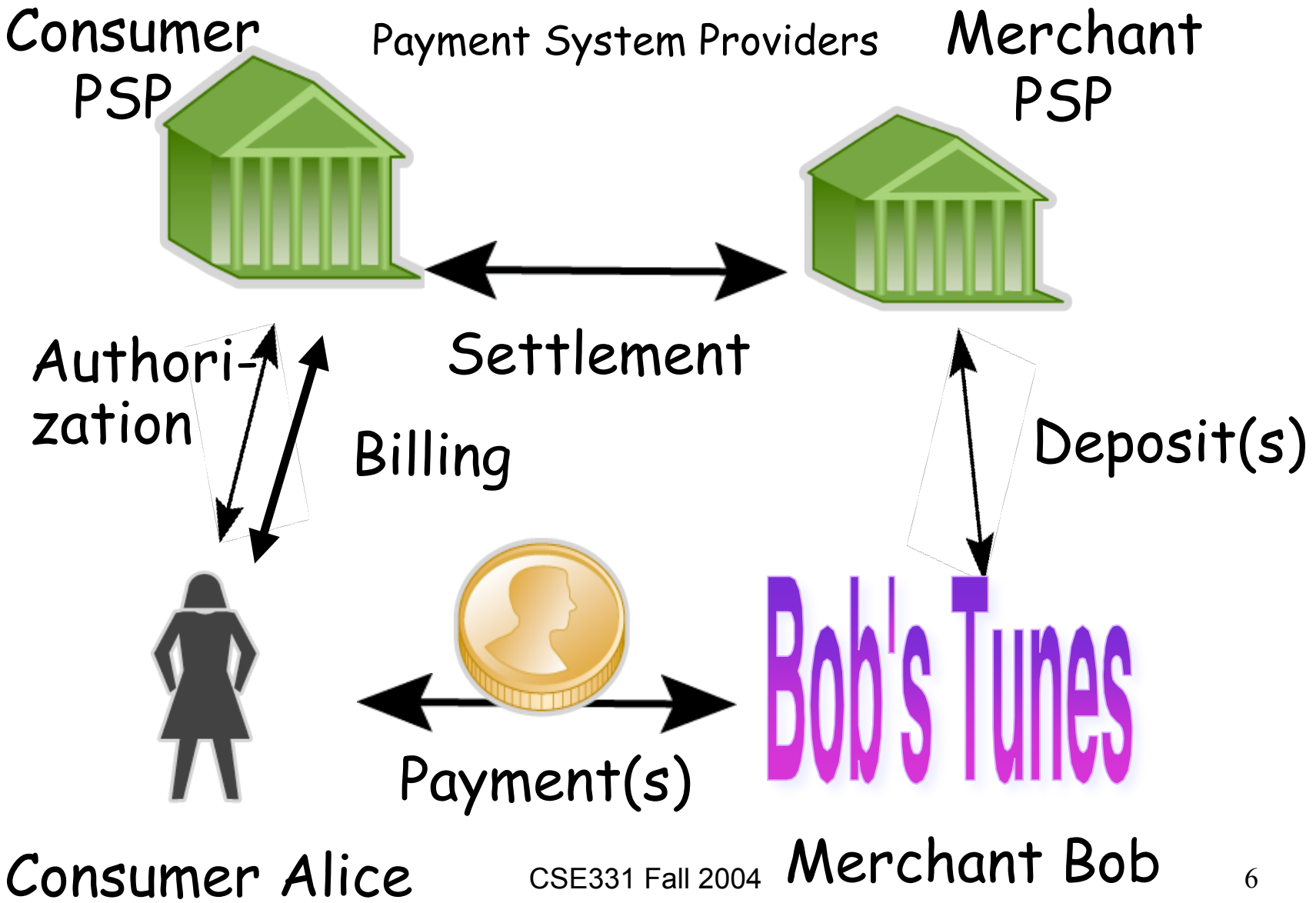
- A payment small enough that processing it is relatively costly.
  - Note: processing one credit-card payment costs about 25¢
- A payment in the range 0.1¢ to $10.
- *Processing cost* is the key issue for micropayment schemes.
  - There are other issues common to all payment schemes

The need for small payments

- "Pay-per-click" purchases on Web:
  - Streaming music and video
  - Information services
- Mobile commerce
  - Geographically based info services
  - Gaming
  - Small "real world" purchases
- Infrastructure accounting:
  - Paying for bandwidth



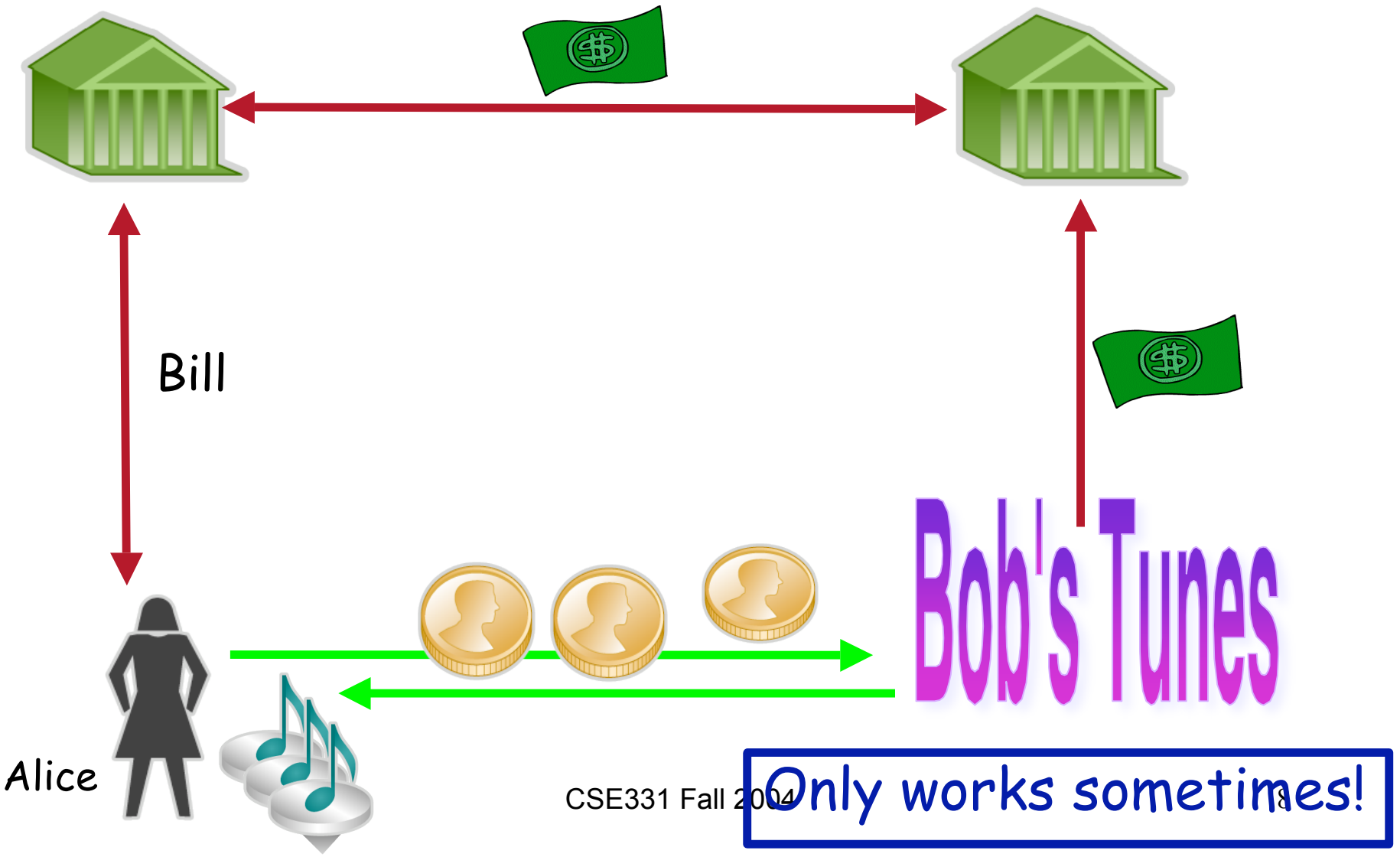
Generic Payment Framework



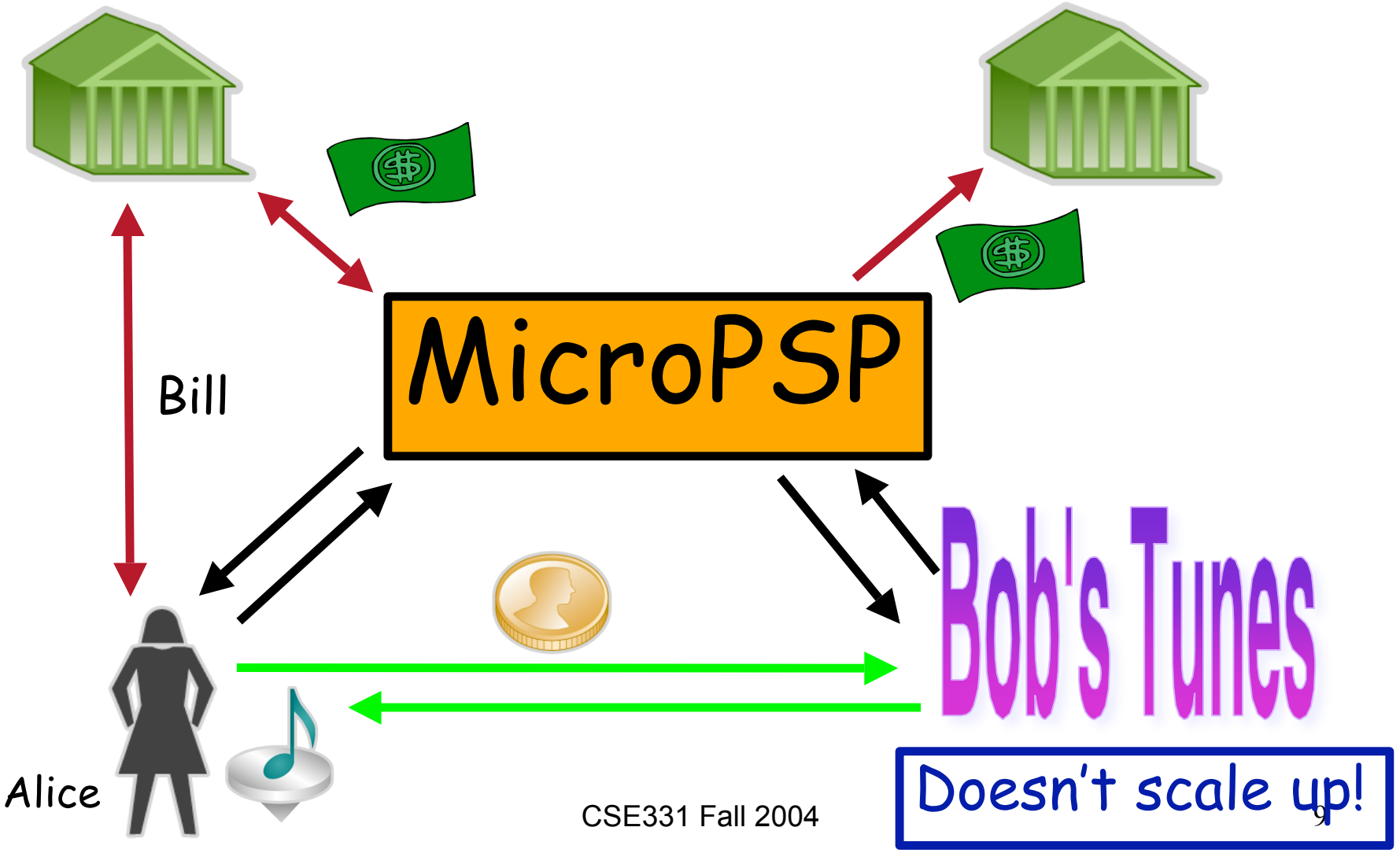
Aggregation

- To reduce cost, ***micropayments*** must be aggregated into fewer ***macropayments***.
- Possible levels of aggregation:
  - **None**: Every payment deposited with PSP
  - **Merchant-level**: A consumer's payments are aggregated by merchant
  - **MicroPSP**: Monopoly service that disintermediates existing payment services; doesn't scale well
  - **Universal**: Payments aggregated across all users and merchants, even those supported by different cooperating PSPs

Merchant-Level Aggregation



MicroPSP Aggregation



Universal Aggregation

- ***Universal aggregation*** dramatically reduces processing cost, independent of spending patterns.
- *Also called* ***many/many/many aggregation****:* Aggregates payments from
  - *Many* consumers
  - *Many* merchants
  - *Many* PSP's

  in any combination. No need to aggregate sales per consumer.

Universal Aggregation Idea

- Would merchant prefer:

  (a) twenty *50 cent payments*, or

  (b) *$0 for 19 payments, and $10 for one?*

  No difference to merchant, on average

Universal Aggregation Idea

- Would merchant prefer:

  (a) twenty *50 cent payments*, or

  (b) *$0 for 19 payments, and $10 for one?*

  No difference to merchant, on average.

What if processing costs 20 cents per payment?

(a) nets only 30 cents per payment

(b) nets 49 cents net per payment!

Merchant strongly prefers (b) !

Electronic Lottery Tickets

- "Electronic Lottery Tickets as Micropayments" – Rivest '97

- Payments are *probabilistic*
- First schemes to provide global aggregation: payments aggregated across all user/merchant pairs.

“Lottery Tickets” Explained

- Merchant gives user hash value $y = h(x)$
- User writes Merchant check: “This check is worth $10 if three low-order digits of $h^{-1}(y)$ are 756.” (Signed by user, with certificate from PSP.)
- Merchant “wins” $10 with probability 1/1000. Expected value of payment is 1 cent.
- Bank (PSP) sees only 1 out of every 1000 payments.
- Merchant provides x as evidence for the Bank’s billing.

Peppercoin's Universal Aggregation

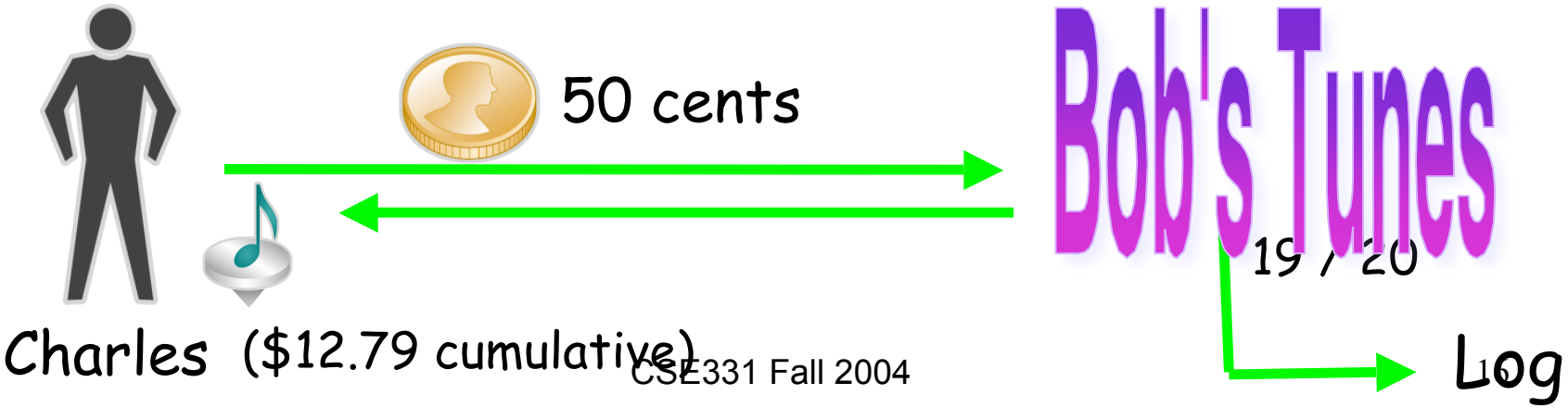
www.peppercoin.com

50 cents

Alice ($8.50 cumulative)

Log

Peppercoin's Universal Aggregation



Peppercoin's Universal Aggregation