CS155b: E-Commerce

Lecture 12: February 22, 2001

C2C Internet Commerce

Remarks on First Hour Exam Blue Books

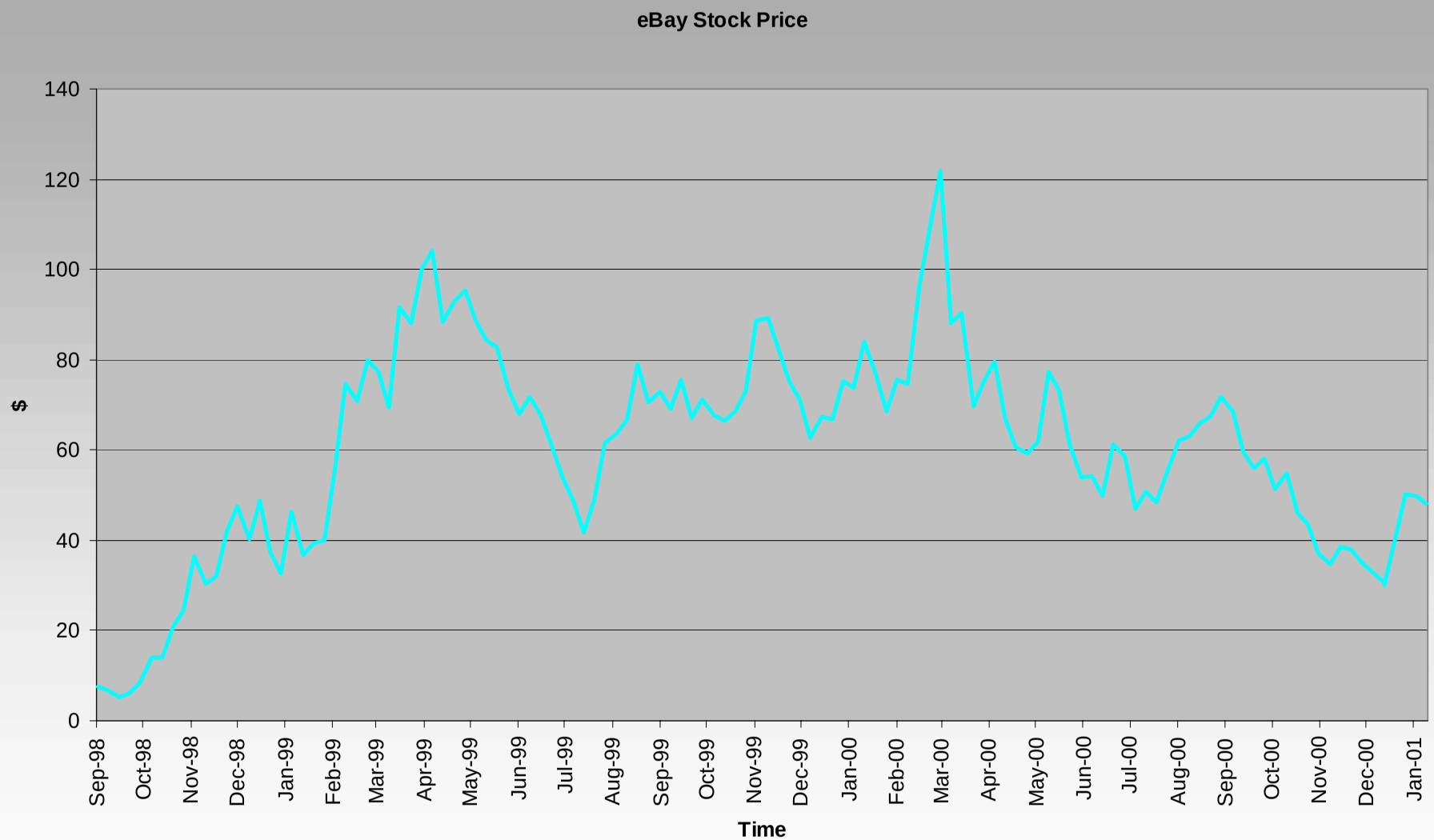
- “mass market” $\neq$ “network effects”
- “first-sale rule” $\neq$ “transfer of copyright”
- “digital signatures” $\neq$ “entity authentication”
- signatures and signed documents need not be encrypted

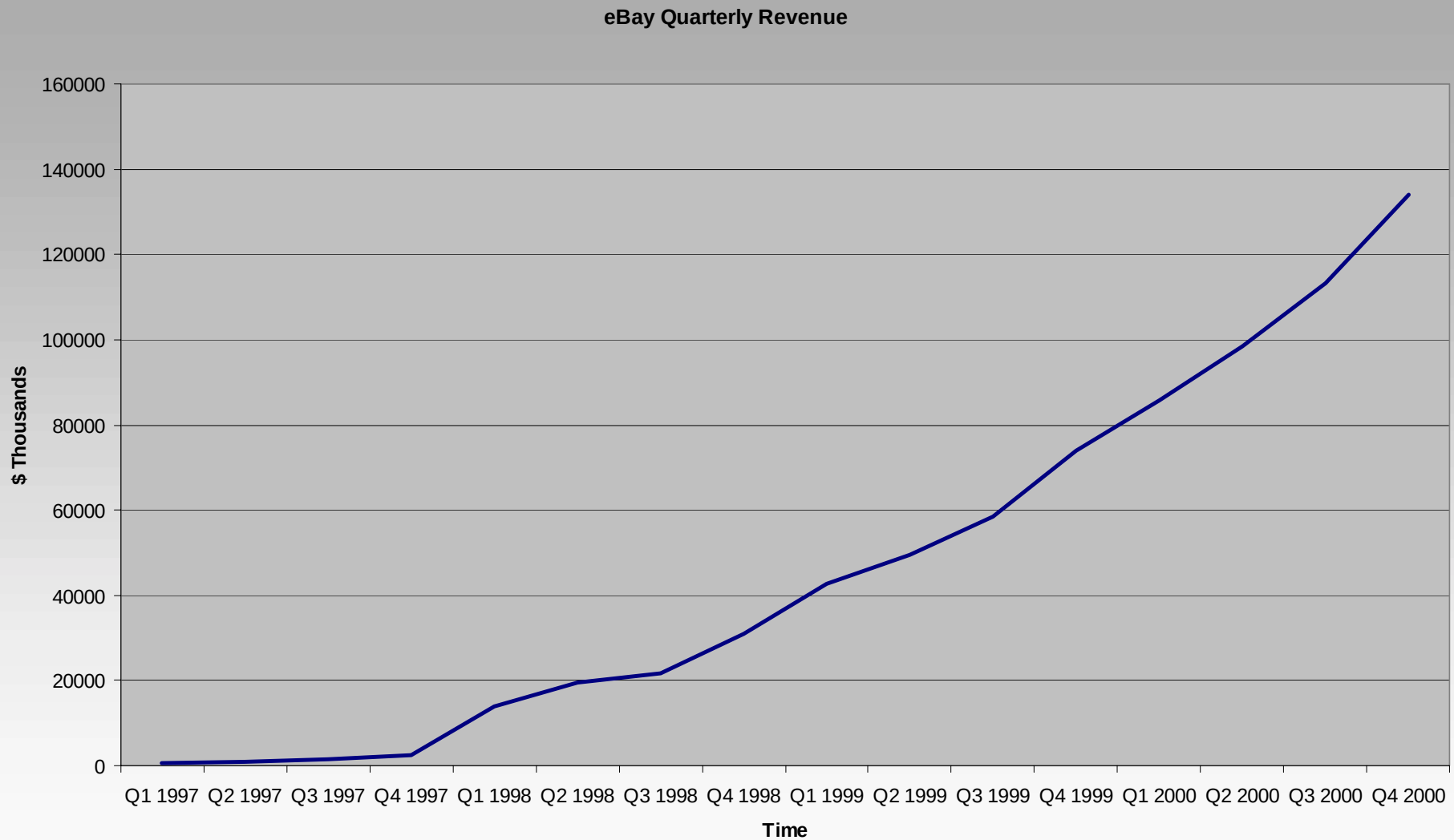
Remaining Topics

- C2C Auctions
- B2B
  - Bob Glushko (Commerce One)
  - Bradley Kuszmaul (Akamai)
- Technology Regulation
  - Matt Blaze (AT&T Labs)
- WWW Searching
- ??? B2C ???

eBay Overview

- World's largest "online trading community"
- Founded in Sept 1995 by Pierre Omidyar
- IPO in Sept 1998
- Current number of users: Approx. 20M
  (2M end of 1998; 12M middle of 2000)
- Current P/E ratio: 294


eBay Stock Price
140
120
100
80
60
40
20
0
$
Sep-98
Oct-98
Nov-98
Dec-98
Jan-99
Feb-99
Mar-99
Apr-99
May-99
Jun-99
Jul-99
Aug-99
Sep-99
Oct-99
Nov-99
Dec-99
Jan-00
Feb-00
Mar-00
Apr-00
May-00
Jun-00
Jul-00
Aug-00
Sep-00
Oct-00
Nov-00
Dec-00
Jan-01
Time


eBay Quarterly Revenue
160000
140000
120000
100000
80000
60000
40000
20000
0
$ Thousands
Q1 1997
Q2 1997
Q3 1997
Q4 1997
Q1 1998
Q2 1998
Q3 1998
Q4 1998
Q1 1999
Q2 1999
Q3 1999
Q4 1999
Q1 2000
Q2 2000
Q3 2000
Q4 2000
Time

eBay Business Model

- Sellers pay small fee (<$2) per listed item.
- eBay takes a cut (~2.5%) of each sale.
- Buyers and sellers handle exchange and payment.
- eBay has no inventory, no transportation, *no costs at all except website operation*.

Conventional wisdom: Service is *technically* commoditizable, but strong network effects favor eBay.

Technical Foundations of Internet C2C Commerce

- Market Design (*e.g.*, Auction Types)
- Payment Systems (can't always use credit cards)
- E-Market Operations
  - Website Design Issues (*e.g.*, UI)
  - ★System Reliability and Availability

Auction Types

- Ascending bid structure
- Descending bid structure
- First-price, sealed bid

★ Second-price, sealed bid (Vickrey):

  – Highest bidder gets item

  – Pays second-highest bid price

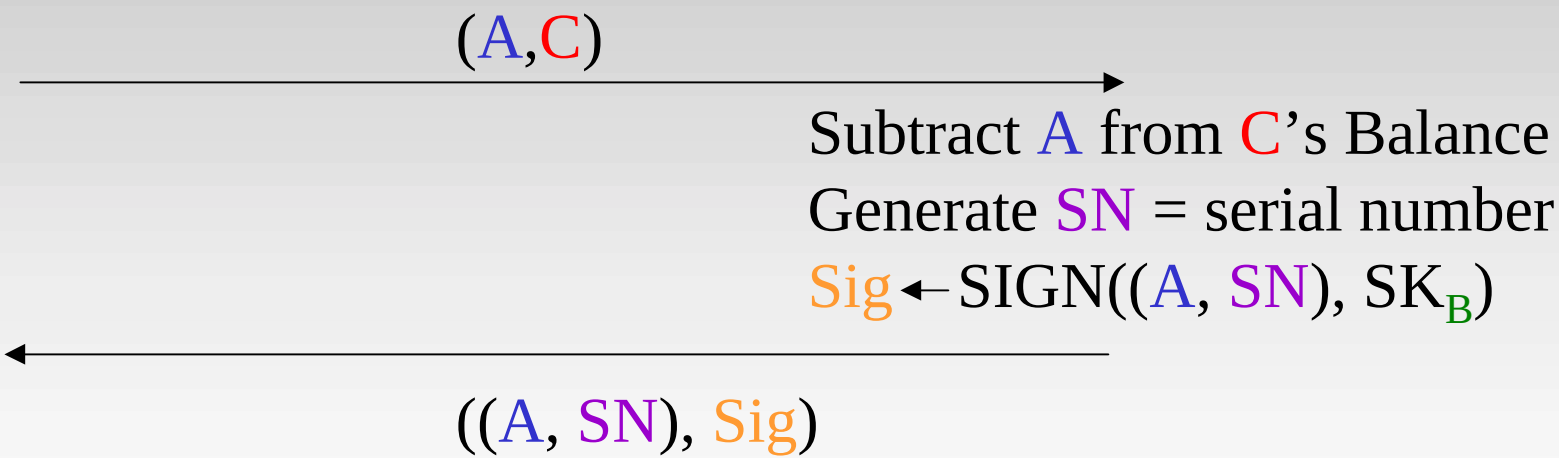
  – Advantages: “Strategyproof,” user-friendly

“E-Cash” Based on Digital Signatures

Basic Withdrawal of $A

C = Customer

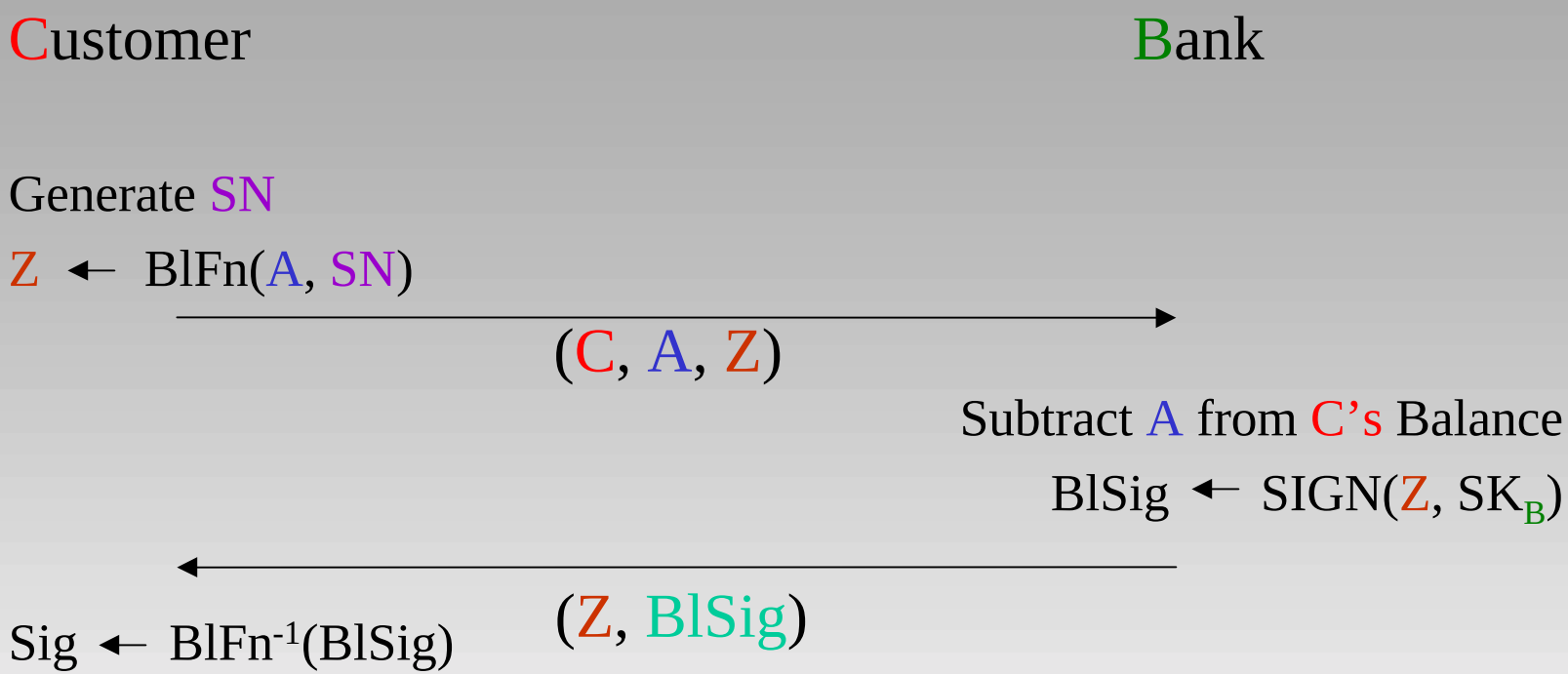
B = Bank



Basic “E-Cash” Protocols, continued

- Spending
  - Customer gives ((A, SN), Sig) to Merchant
  - Merchant runs Verify((A, SN), Sig, PK_B)
- Redemption
  - Merchant sends ((A, SN), Sig) to its bank
  - Signature verification and settlement

“Blind Signature” Withdrawal Protocol



Important Properties:

- Sig is a valid signature of (A,SN)
- C is “unlinkable” to SN during redemption

Mathematical idea: “random-self-reducibility”

“Other E-Cash” Desiderata

- Prevent “Double-spending”
- Detect double spending before redemption
- “Transferability”

Extensive body of good research.

Many protocols, trade-offs, lower bounds.

Decades of hope, work, and investment by cryptologic research community.

C2C Payment Reality

- Elegant “e-cash” technology not used.
- No-tech “solution”: PayPal

Discussion Point: When do no-tech solutions win? When should they?

Assignments for Week of February 26, 2001

Reading: Chapter 8 of Information Rules.

Written Homework: HW3 due *in class* on March 1, 2001.