E-commerce

- **E-commerce models: amazon, clicks-n-morter (bn.com), ebay, priceline, mercata, Jango, m-commerce, L-commerce.**
- **How to make e-commerce "frictionless"**
  - 1-click, gift-click.
  - Advertising
  - How to pay?
  - How to micro-pay?

Advertising (E-commerce funnel)

Advertising models:

- **Anchor tenent (pioneered by Amazon).**
  - 100 million $ deals w/ AOL.
- **Pay per impression (CPM)**
- **Pay per click (CPC)**
- **Pay per placement (goto.com)**
- **Pay for performance**

Electronic Payment Systems

ePayment Ideas

- **Want to move money over the Internet**
- **But:**
  - Security
  - Poor interaction among payment mechanisms: credit card, bank account, payables systems, procurement
- **System design problems**
  - Keep transaction costs low
  - Scale to huge number of transactions (100 billion per day)
  - Bank systems (SWIFT, FedWire) do not talk to the Internet

Types of Money

- **Token money (a physical item)**
  - Cash, traveler's check, gift certificate, coupon
  - If it can be lost, it's token money
- **Notational money (account ledger entries)**
  - Transferred by orders (drafts, checks, frequent flier miles)
  - Can't be lost
  - Requires "clearing" and "settlement". No instant transfer (yet)
- **Hybrid**
  - Check: a token backed by notational money

Desirable Properties of Digital Money

- **Universally accepted**
- **Transferable electronically**
- **Divisible into change (pay for $10 item with $100 bill)**
- **Unforgeable, unstealable**
- **Private (no one except parties know the amount)**
- **Anonymous (no one can identify the payor)**
- **Work off-line (no need for on-line verification)**

NO KNOWN SYSTEM SATISFIES ALL OF THE ABOVE

Requirements for Electronic Payments

- **Money atomicity**
  - no money is lost or created in a transfer
- **Goods atomicity**
  - money and goods are exchanged atomically (both or none)
- **Non-repudiation**
  - no party can deny its role in the transaction
  - digital signatures

PayPal

- **Most popular electronic money service (6 million users), championed by ebay.**
- **Free for consumers (key to speed adoption).**
- **Fast – e-mail communication.**
- **private (merchants don't see your credit card number)**

How to Pay via PayPal

- **Establish an account including your checking account or credit card info.**
- **Enter recipient's e-mail address + payment amount. Eg, tell paypal send etzioni@cs.washington.edu $25.**
- **Recipient registers or just logs in and the money appears in their account.**
- **Recipient can pay someone else or "cash out."**

Analysis of PayPal

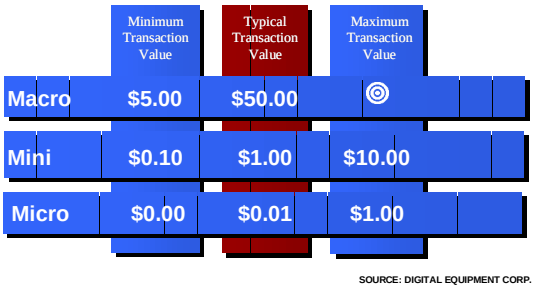
- **Particularly nice for auctions, splitting a bill, collecting money from K people (who pay for the party..).**
- **Not good for micropayments, because relies on traditional money at base!**
- **Business model: charge merchants, make money on the "float". Jury is still out..**

Paypal Demo

"Unexpected error: 3004. We are currently experiencing heavy traffic to our site. Your request was not completed. Please hit the refresh button on your browser to try again"

They should've talked to Steve!

Ecommerce Payment Ranges



SOURCE: DIGITAL EQUIPMENT CORP.

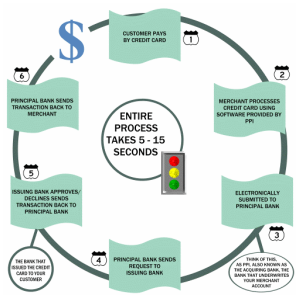
Types of Payments

- Credit card
  - SSL, SET protocols
- Check
  - Automated clearinghouse
- Aggregation
  - Centralized online account for merchant and customers (Qpass)
- Micropayment (usually below $0.10)
  - Millicent
- Ecash (paypal,..)

Credit Cards

- **The most expensive ePayment mechanism**
- **MasterCard: $0.29 + 2% of transaction value**
- **A $100 charge costs the merchant $2.29**
- **Currently the most convenient method**
- **Advantage: allows credit**
- **People can buy more than they can afford**
- **Disadvantages:**
  - doesn't work for small amounts (too expensive)
  - doesn't work for large amounts (too expensive)

Credit Card Processing

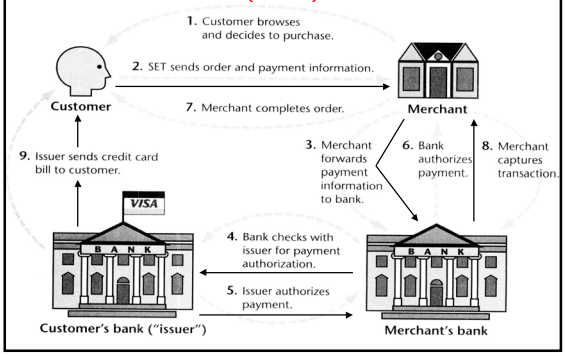


SOURCE: PAYMENT PROCESSING INC.

Credit cards on the Internet

- **How to transmit credit card info securely?**
  - Etzioni's don't-care method (not recommended).
  - Secure Electronic Transactions (SET).
  - Secure Sockets Layer (SSL)
    - Popular protocol supported by broswers (https pages).
    - Encrypts confidential info.
    - Distinct from s-http (secure http for single messages).

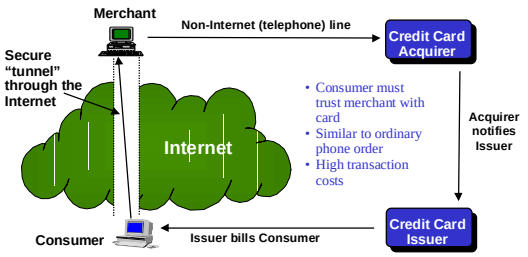
Secure Electronic Transactions (SET)



SET Properties

- **Extremely secure**
  - Fraud reduced since all parties authenticated
- **Not widely used**
- **Requires all parties to have certificates**
- **Expensive to integrate with legacy applications**
  - Estimate: $1 million
- **Scalability is still a question**

SSL (Secure Sockets Layer) Concept



How to Create Secure Tunnel?

- **Remember, people can see your packets.**
  - Need encryption to hide contents.
  - Need keys to decrypt encrypted messages.
- **Remember, people can spoof IP addresses.**
  - Need mechanism to authenticate parties.
  - Also, need accountability (digital signatures).

Public key encryption (1976)

- **Why can't Alice and Bob agree on a key?**
- **Public key encryption:**
  - Alice advertises a public key.
  - Bob sends his credit card number to Alice encrypted using her public key.
  - Alice can decrypt this message using her private key.

No one can infer the private key from the public one!!!
Is there such a scheme? How is it implemented? Is it guaranteed to work?

Micropayments

- **Payment scheme for *low-value* transactions**
  - such as 1¢ per web page access
- **Too small for credit-card "macropayments"**
  - (which may incur fee of 29 ¢ + 2%)
- **Public-key crypto relatively expensive:**
  - RSA sign (private key) 2 / sec
  - RSA verify (public key) 200 / sec
  - Hash function 20000 / sec

These slides adapted from Rivest / Shamir

Micro-payments via Aggregation

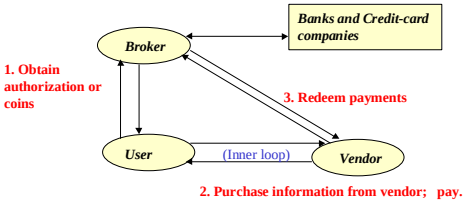
- **Only bill once every k payments (e.g., phone company). Also, Qpass (Seattle co.).**
- **Expected value payments: Suppose I owe you a dollar, would you take a 1/1000 chance to win $1000?**
- **Paypal:**

Micropayments

- **Some advanced features, such as *anonymity*, are probably just too expensive to implement in a micropayment scheme.**
- **With light-weight schemes, one must be pragmatic about fraud and abuse:**
  - The goal should be effective *risk management*, rather than total prevention.
  - "Bad apples" can be detected and eliminated from the system.

Micropayments

- **Introduce *Broker* to intermediate and aggregate:**



Efficiency Goals

- **Minimize use of public-key operations.**
- **Keep Broker "off-line" as much as possible.**
- **Make inner loop (purchase/payment) efficient,**
  - Especially for repeated small purchases.

MicroMint

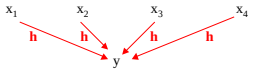
- **A digital coin should be:**
  - Hard to produce [except by Broker]
  - Easy to verify [by anyone]
- **Digital signatures "work," but are relatively expensive.**
- **MicroMint uses hash functions *only***
  - (no public-key crypto).
- **Broker utilizes *economy of scale* to produce MicroMint coins cheaply (as with a regular mint).**

The Birthday Paradox

- **The hash function: Birthday(person)=y**
  - y ranges over Y=[1…365]
  - Let |Y| = n = 365
- **How many people should we 'hash' to have a collision?**
  - What is the probability of selecting k random and DISTINCT numbers from Y?
- **P0=1*(1-1/n)*(1-2/n)*…*(1-(k-1)/n)) == e^(k(1-k)/n)**
  - P1= 1-P0 ---> at least one collistion
- **Say, P1 is at least 0.5… solve for k**
  - k == 1.17 * SQRT(n)
  - k = 22.3 for n=365

MicroMint Coins

- **Suppose hash function $h : \{0,1\}^{48} \quad \{0,1\}^{36}$ maps $m = 48$-bit strings to $n = 36$-bit strings.**
- **A *k-way collision* is a *k*-tuple $(x_1,x_2,...,x_k)$ of values such that $h(x_1) = h(x_2) = ... = h(x_k)$:**



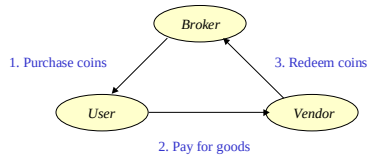
- **A MicroMint coin is a *k*-way collision (*k=4*).**
- **Verifying a coin is easy.**

Minting Coins

- **Producing coins is like tossing balls into k^n bins;**
  - *k* balls in a single bin makes one coin.
- **Producing *first* 2-way collision requires time $2^{n/2}$**
  - This is the "birthday paradox."
- **Producing *first k*-way collision requires time**
  - $N_k = 2^{n(k-1)/k}$. (e.g. 2^{27} for $k=4$, $n = 36$.)
  - (It's hard to forge even one coin.)
- **Time cN_k yields c^k coins;**
  - Once threshold of N_k is passed, coins are produced rapidly.
  - (Mint has economy of scale!!!).

Flow of MicroMint Coins

❶ **Broker mints coins and sells them to User.**
❷ **User spends coins with Vendor.**
❸ **Vendor deposits coins back to Broker.**



Security Concerns

- **Forgery: Can an adversary forge MicroMint coins? (Economically?)**
- **Double-spending: What if a user "double-spends" his MicroMint coins?**
- **Vendor fraud: What if a vendor gives copies of coins received to an accomplice?**

Protections against forgery

- **Computational difficulty of minting coins.**
- **Small-scale forgery not really a concern;**
  - Large-scale forgers will get caught.
- **Coins "expire" monthly.**
  - New hash function revealed each month,
  - Old coins exchanged for newly minted ones.
  - Broker works during May to make coins good for June;
  - Forger only learns h_{June} at beginning of June,
    - Starts out way behind.

Protection against double-spending

- **There is no "anonymity" in MicroMint:**
  - Broker keeps track of whom each coin was sold to, and
  - Notes when it is returned by vendor.
- **Small-scale double-spending not a concern.**
- **A user whose coins are consistently double-spent (with many vendors) will be caught and black-listed; he will not be sold any more MicroMint coins.**

Protection against vendor fraud

- **Vendors who consistently redeem coins that are also redeemed by other vendors will be black-listed and refused further redemption service by the Broker.**
- **Users can cooperate with Broker to identify bad vendors by identifying where coin was first spent.**

Additional protection against forgery

- **Coins may satisfy "hidden predicates" which are only announced if forgery is detected by Broker.**
  - For example, legitimate coins may all satisfy condition
  - That low-order bit of x_i = complicated f(other bits).
- **Most forged coins won't pass this "verification condition".**
- **Broker can announce several such conditions**
  - Or even one each day of month

E-commerce, E-payment Conclusions

- **E-commerce is here to stay.**
  - Some esoteric models have failed, but click-n-mortar going strong.
- **Authentication, e-payment are solved using public-key crypto.**
  - Cryptographers can finally have a job outside the NSA.
- **Micro-payment, digital cash are still topics of research/experimentation.**