

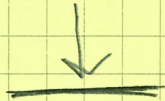
6.857 Rivest

L22.1 4/27/11

- Admin:
- Talks start Monday
 - Zeldovich talks Wed 5/11 on stuxnet

Today: "Electronic Cash"

- Basics: Atoms/Bits, Tokens/Accounts
- Electronic checks
- Properties
- Double-spending
- Coins & Peppercorn
- Anonymity



"Electronic Money"

- What properties should it have?
- " " can " " ?

Atoms vs Bits

- What can "possessing value" (money) mean?
- How can we transfer value?

Easy to answer if we use (gold) atoms to represent value:

- gold atoms are hard to make
- only one person at a time can "own" an atom

Things get complicated if we want to use bits:

- easy to generate bits
- bits can be copied \Rightarrow double-spending becomes a problem!

(Token-based)

Possession-based vs Account-based methods

- In a possession-based method, owning the representation \equiv owning the value
- In an account-based method, there is usually some TTP who "maintains accounts" (e.g. a "bank"); xactions cause value to be shifted from one acct to another.
- Most "bit-based" methods are account-based.

Simple example: Electronic checks

- Account-based: Bank has PK_B, SK_B
- \Leftarrow User has $PK_U, SK_U, \text{cert on } (U, PK_U) \text{ by bank}$
- Check = $\begin{bmatrix} \text{cert (on } PK_U, \text{ signed by } SK_B) \\ \text{sign}(SK_U, \text{"Pay, Bob \$100, date, serial \#"}) \end{bmatrix}$
- Bank deposits check just once (using ser #)
- Usual problem of overdrawn acct (bad check)
- Bank knows exact details: payer, payee, amt, date
- Merchant " " "

This works.

What else is possible?

Can we make payments more like cash?

Desirable (?) Properties

- Non-forgable (prevent fraud, inflation)
- Not double-spendable
- Reliability: can "back up" your \$
- Exclusive ownership
- Transferability: A can pay B
- Transitivity: B can use A's payment to pay C
- Variable-denominations
- Divisibility & combinability
- Efficiency (esp. for small amounts)
- On-line versus off-line transactions
- Scalability
- anonymity
- ~~security~~ security
- Conversion to "ordinary" money

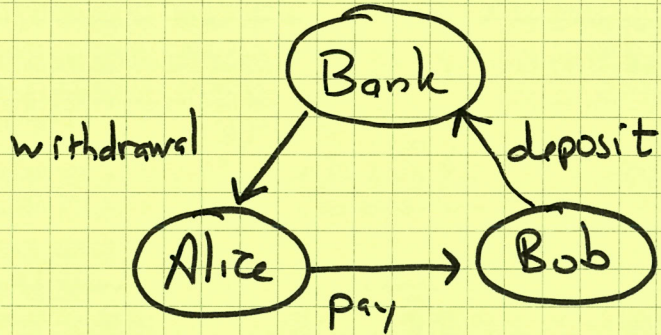
Double-spending

- essentially a "replay attack"
- if you can backup your \$, then "restore" gives you your spent money back!?
- prevention seems really tough (unless you use atoms)
- detection requires convergence of spending records (e.g. at bank) and large databases (?)
- even if you can detect double-spending - what do you do?
 - roll back/deny transaction (2nd merchant to get some electronic coin can't deposit it)
 - punishing perpetrator may be impossible if we have (true) anonymity: payer is not identifiable
 - furthermore: is payer or payee the culprit? (can merchant "frame" consumer?)
 - deterrence may be hard... how to punish (pay fine from account?)

Some approaches:

Signed coin ID

Bank (TTP)
Alice (payer)
Bob (payee)



3 protocols to support:

① withdrawal/authorization

Alice becomes "able to pay"

(e.g. cost issuance in check scheme)

② payment

③ deposit

} life of a "coin"

① withdrawal:

• Bank gives Alice $R, \text{sign}(SK_B, R)$ ← unforgeable object!
= coin R is coin ID

• Bank keeps R in database of unspent coins

• Bank debits Alice's acct for withdrawal

② payment:

Alice gives coin to Bob; Bob checks Bank sig

③ deposit:

Bob gives coin to Bank, Bank checks sig & R in DB

flags R as "spent"

- Not very efficient - bank has to sign each coin!
- Double-spending can be a problem!
- Check scheme better - merchant can't frame user!

Peppercorn (Micali & Rivest)

- "probabilistic payments":
 - paying 10¢ \equiv paying \$10 with probability 1/100
 (micropayment) \sim (macropayment, sometimes)
- based on electronic checks method
- Alice pays Bob 10¢ as follows:
 - She gives Bob electronic check for \$10 that contains condition: "This check valid if and only if E is true" (where E holds with probability 1/100)
- Bob must be able to test if E is true
 - if so, he can deposit check
 - if not, he throws check away (but gives Alice her purchase)
 - he gets paid correctly on the average
 (law of large numbers)
- Alice should not be able to tell if E is true when she writes check (else she can filter checks, ...)
- Bank should be able to tell if E is true (so "bad checks" where E is false, don't get deposited).

Peppercorn (cont.)

6.857 Rivest

L22.8 4/27/11

- Our recommendation for E

- Bob has a deterministic signature scheme

- $E \text{ true} \equiv \left[\underbrace{\text{sign}(SK_B, \text{check})}_{\text{"countersignature" on check}} \bmod 100 = 0 \right]$

- (can adjust odds based on value...)

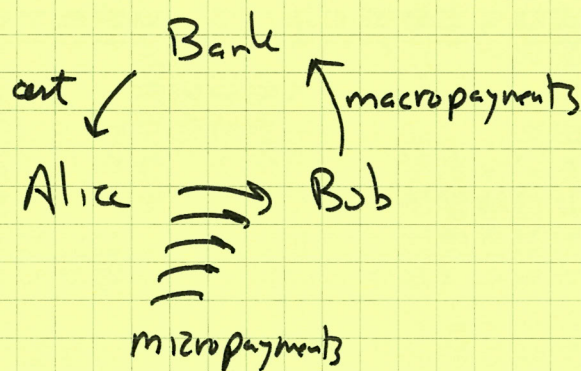
- Bob's signatures should be pseudorandom (unpredictable)

- Bank only sees 1/100 of checks, Alice writes
ideal for micropayments

- Merchant Bob may be OK with probabilistic payment;
User Alice may not be (she may get charged for
more than she paid)

Fix: Each check also gives running total of all checks
written; bank won't charge her more than that amt.
(If she tries to cheat, it will get detected, e.g.
when two checks in a row get converted to micropayments.)
Note that bank acts as buffer here...

Good efficiency: work done is all between Alice & Bob



Anonymity

- Using blind sigs to achieve anonymity (Chaum)
- catching double-spenders (Breeds)

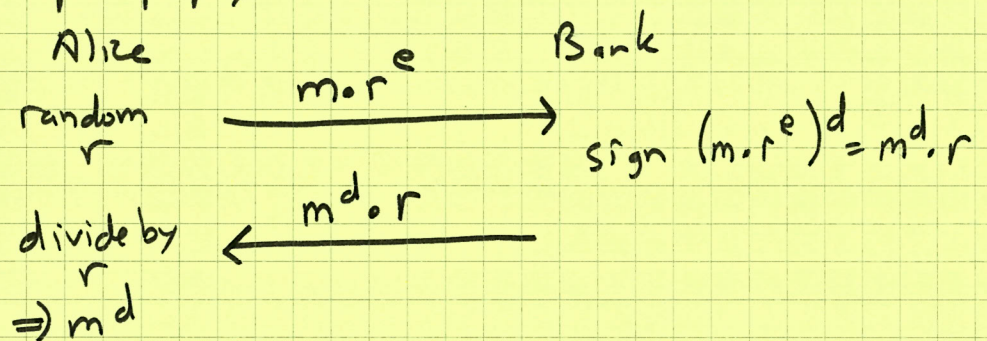
Chaum's Anonymous Cash

- Bank signs all coins
- But we now use "blind signature" method, so bank doesn't see what it is signing (!)
- E.g. with RSA sig: $SK_B = (n, d)$ $PK_B = (n, e)$

$$\text{coin} = (m, m^d) \quad \text{where } m = \text{serial \#} \\ \text{(formatted msg...)} \\ \uparrow \\ \equiv \text{sign}(SK_B, m)$$

How to get m^d from bank, without bank seeing m ?

Homomorphic property of RSA:



Value of coin is fixed (indep of m) since bank doesn't see m .

Value of coin depends only on PK.

- Double-spending a problem!

G.857 Rivest
L22.10 4/27/11

Catching double-spenders (Brands)

- coin withdrawal is anonymous (like Chaum)
- spending coin is anonymous
- but if Alice spends coin twice, her identity is revealed! (Bank can figure it out)

Ideas:

- Bank gives blind signature on coin
- User knows secret about coin
- secret tied to her identity
- payment protocol gives up "secret share" about coin secret to payee
- two secret shares \Rightarrow coin secret \Rightarrow user ID

(For details: see lecture notes L21 & L22 from 2009 G.857)

==
"Intergalactic Banking Model"??

How to make monetary system between star systems?

No TTP.

No use of force.

No atoms xferred - only bits.