Lecture #18:
Electronic Currencies

Prof. Dr. Sven Seuken
24.5.2012

Housekeeping

- Guest: David C. Parkes:
  - Talk today: 17:15-18:15 (IfI Kolloquium)
    → Mechanism Design for Kidney Exchange
- Exam topics + questions → on Monday
- Last lecture: review session
  → prepare questions!
- Homework assignments:
  - Recommender systems → due now
  - Very last hw → out now, due in one week
- Questions? Concerns?

Recap: Transitive Trust Mechanisms

- What is transitive trust?
- Example domains?
- The mechanism design view?
- Vs. Reputation Systems?
- Vs. Recommender Systems?
- Manipulability vs. Informativeness
  - Shortest-Path vs. PageRank?

Today's Topic: Electronic Currencies

- Barter Economies

- Advantages Using Currency:
  - Transferable: solves "double coincidence of wants" problem
  - Divisible
  - Storable/durable

Gold standard vs. Fiat Money

- Gold standard
  - E.g., trade with gold coins…
  - …or government promises exchange rate with gold
  - Fixed amount of currency
  - Intrinsic value
- Fiat currency
  - No intrinsic value
  - Based on trust in government/central bank
  - Central bank can “print money”

Electronic Currencies

- Not issued by government or central bank
- No central entity (in contrast to Visa or Paypal)

- Advantages:
  - Costs
  - Privacy
  - Decentralization
  - Trust
- Challenges:
  - Money Printing
  - Double Spending
  - Trust

Credit Networks

- Idea: issue an “IOU” (I owe you)
- Requires bilateral trust
  - For B to accept an IOU from A, B must trust A
- Can make use of pre-existing trust (e.g., social network)
- Can build up trust
  →bilateral (simultaneous) work exchanges

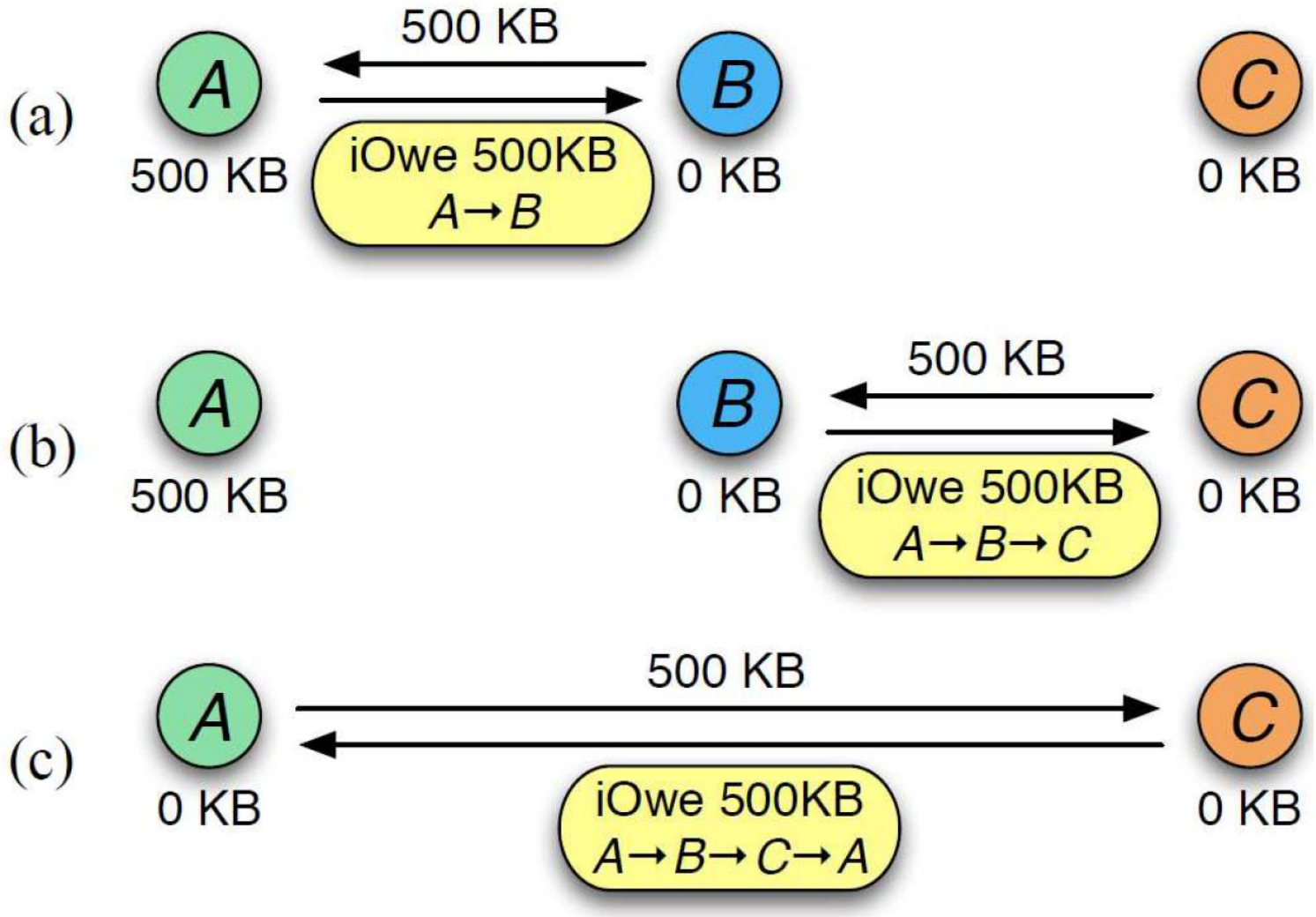
Public-Key Cryptography

- Each user i has a (PK_i, SK_i) pair
  - Public key PK_i known to everyone
  - Private (secret) key SK_i known only to user i
- Possible operations
  - **Sign** a document X with private key
    → every user can verify who signed the document
  - PK_i can be **associated** with document X
    → user i can use SK_i to prove that X belongs to him

iOwe

- Iotas:
  - Can be created by everyone
  - Can be transferred
  - Can only be redeemed at original creator
  - Based on trust
- Three operations:
  - Creating iotas: $I =< A, resource, expiry - time, nonce >$
  - Spending iotas:
    - $spend_A(I, PK_B)$produces $I_{A \to B} = [I, PK_B]SK_A$
    - $spend_B(I_{A \to B}, PK_C)$produces $I_{A \to B \to C} = [I_{A \to B}, PK_C]SK_B$
  - Redeeming iotas: spending iota at original creator

iOwe: Examples



Challenges in iOwe

- Attacks:
  - Double-spending attacks
  - Sybil attacks
  - Step-omission attacks

- Policies against Manipulation
  - P1: Grim-trigger on Double-spenders
  - P2: Chain-of-Trust
  - P3: Grim-trigger on step-omitters
  - P4: Threshold-trigger on alleged step-omitters

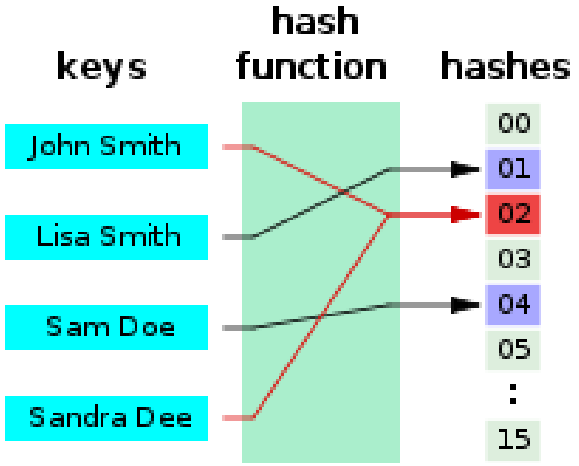
Drawbacks of iOwe

1. Policies are not centrally enforced?
   →compare to Bitcoin?
   →the real problem: no incentive to follow policies!
2. Necessity to bootstrap trust bilaterally
3. No transitive trust → chain-of-trust policy
4. Each iota has a different creator → different value
5. Finding and generating public/private keys
6. Saving the whole chain requires lots of memory

Bitcoin

- Ideas:
  - No central entity (as in Bitcoin)
  - Expensive to create currency: proof-of-work
  - Prevent double spending by using a P2P network that checks all transactions
    → provide an incentive for checking transactions!

Hash Functions



- Input: variable length (long)
- Output: fixed length (short)

→ "Collisions" are very rare

- One-way functions
  - Given a key, easy to compute the hash
  - Given a hash, very hard to compute a corresponding key

- Proof-of-work Idea:
  - Take a document X, add a "nonce" value n → compute hash
  - Require that the hash begins with "l" 0's

$$0000000000000d9cd5eb346d316b7101ed4a4167bd861ca008b25ff8e730978c$$

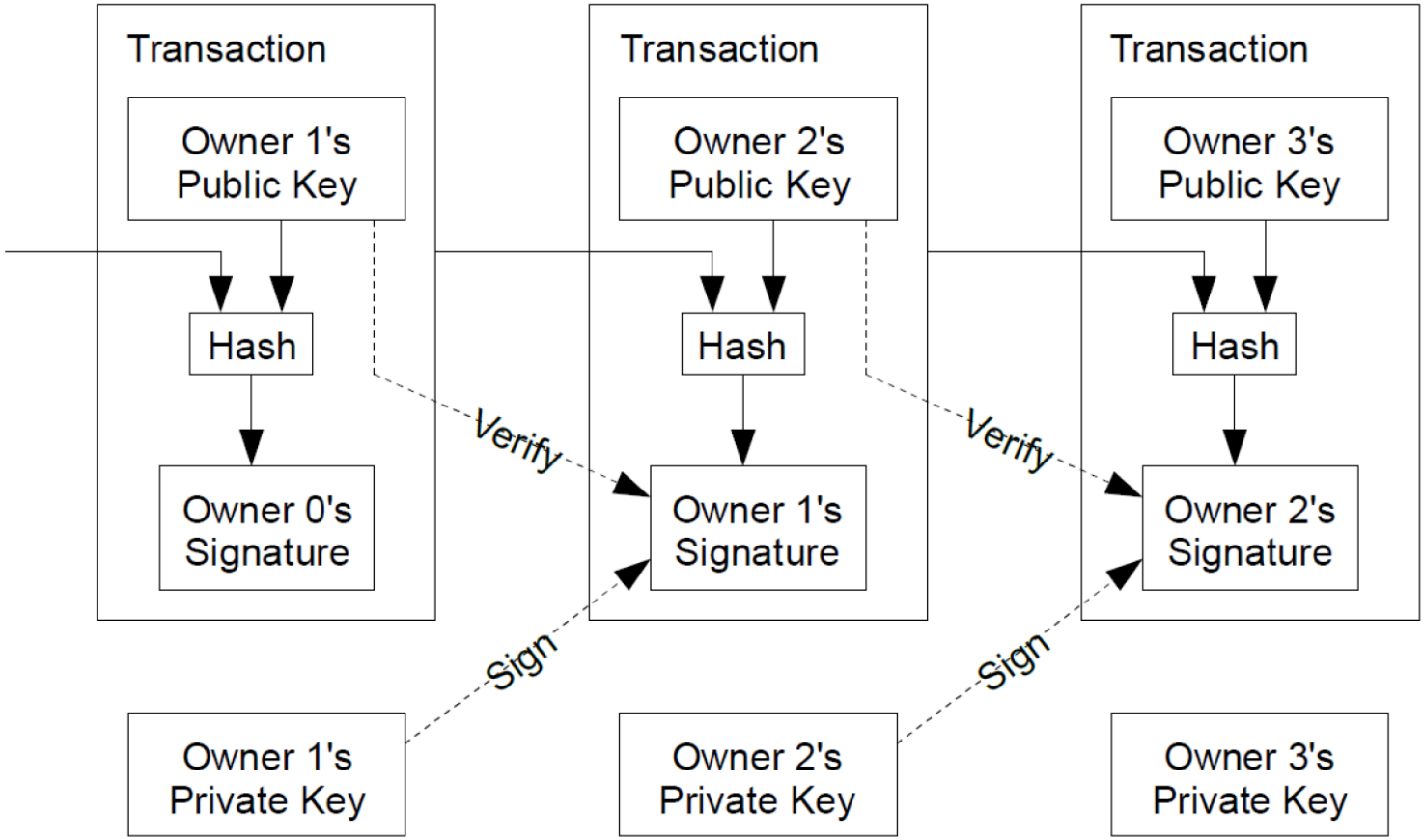
  - Trial and error to find nonce n that produces desired hash

Bitcoin Mechanism

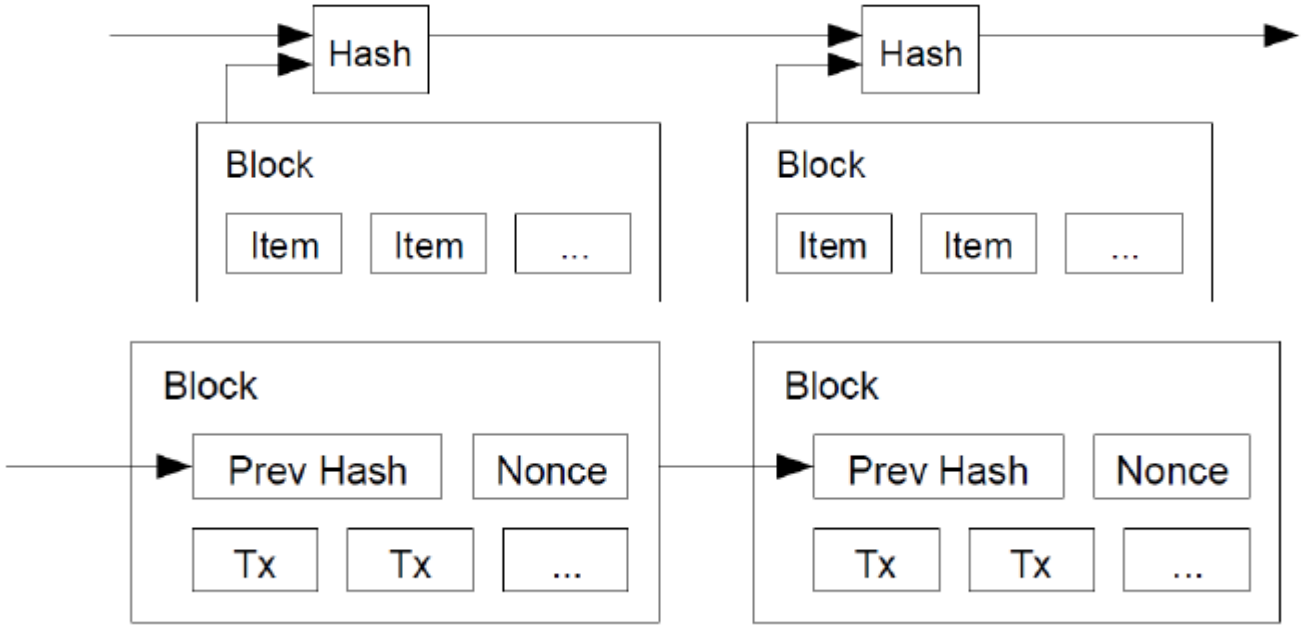
1. Transaction
2. Distributed Time-Stamping
   - Blocks
   - Block Chains
3. Incentives:
   - Mining Coins
   - Transaction Fees

Bitcoin Transactions

- Transferring one coin from user A to B



Blocks and Block Chains



Definition 18.2 (**Acceptable Blocks**). Given a set of transactions t, a previous hash h, a nonce value n, let B(t; h; n) denote the corresponding block and H(B(t; h; n)) denote the hash value of that block. The block is acceptable if and only if the hash string H(B(t; h; n)) starts with at least l entries that are the `0' character.

$$0000000000000d9cd5eb346d316b7101ed4a4167bd861ca008b25ff8e730978c$$

Incentives

- All users in the network help to find new blocks
  → “time-stamp” transaction!
- Finding a new block is costly!

- Incentives:
  - “Mining” new coins (out of thin air)
  - Transaction fees

Attacks on BitCoin

- Possible Attack:
  - User A gives 1 BTC to user B
  - A waits until the transaction is verified (new block)
  - A gives the same BTC to C
  - A creates two new blocks:
    - One block with the new transaction (C instead of A)
    - One more block, to be the longest block chain

→ unlikely to succeed: competing with the whole network

→ “vote” on correct transactions with one vote per CPU!

Strengths of Bitcoin

- New market participants can easily enter (Nico)
- Independent of governments (Andrea)
- No single centralize entity (Malte)
- Coins are unique and cannot be copied (Evgeny)
- Decentralized (Alex)
- You can’t just create your own money (Basil)
- Very robust against attacks (Jan)
- All users eventually agree on all transactions (Jessica)

Weaknesses of Bitcoin

- No central (trusted) entity (Alex)
- Currency is costly to generate and the total is fixed (Martin)
- Possibility of security problems (Andrea)
- Your electronic wallet could be stolen (Nico)
- Mining and transaction delays are confusing for users (Balz, Malte)
- The 10 min delay prevents some useful transactions (Jan)
- System is complex to understand (Andrin)
- No transparency regarding value of coins (Basil)
- No association between transactions and real people (Evgeny)

- Every transaction will eventually be known to each user
- Scalability
- New users must first download the whole block chain
- In the case of double spending, lots of transactions must be canceled

Would you use Bitcoin?

- YES!
  - I trust Bitcoins more than regular money (Evgeny)
  - Independence of Swiss Franc (Andrea)
  - Transaction fees (Basil)
  - Exchange rates (Basil)
- NO!
  - I trust the government/central bank (Jessica, Martin)
  - Risk due to currency fluctuations (Alex)
  - Transaction fees are low enough (Alex, Jessica)
  - PayPal/Credit cards work fine (Alex, Martin)
  - Very few stores accept Bitcoins (Andrin, Evgeny, Malte, Martin)
  - I don’t do lots of online shopping (Balz, Jessica, Mengia)
  - It doesn’t seem to be safe against hacking (Jan)
  - I don’t worry about my privacy yet (Jessica)
  - I would need a powerful computer to mine (Malte)
  - Exchange of Bitcoins to Euros (Malte)
  - How would I earn Bitcoins? (Nico)