### CSci 5271 Introduction to Computer Security Day 26: Electronic cash and Bitcoin

Stephen McCamant University of Minnesota, Computer Science & Engineering

### Outline

Previous e-cash and techniques

Bitcoin design

Announcements

**Bitcoin experience** 

### Kinds of Internet payments

### Credit/debit cards: most popular

- Wide adoption among consumers, little consumer fraud liability
- Restrictive merchant procedures

### 🖲 PayPal

- Easier to accept payments
- Centrally managed to deal with fraud

### One ideal: electronic cash

- Direct transactions without third party
- No transaction fees
- Potentially anonymous
- Non-revocable: buyer bears fraud risk

### **Micropayments**

- Claim: what the web needs is small payments to support content
  - Too small for existing mechanisms
- One idea (Peppercoin): simulate small payment with small probability of larger payment
- Actual market for micropayments has been small Most buyers and sellers prefer free + other revenue

### Blinded signatures

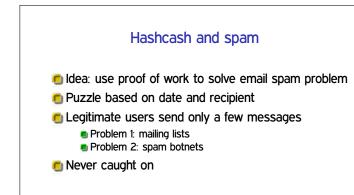
- Sign something without knowing its value
   Often used together with randomized auditing
   For RSA, multiply message by r<sup>e</sup>, r random
   Allows a bank to "mint" coins that can still be
- Allows a bank to "mint" coins that can still be anonymous

### Challenge: double spending

- Any purely electronic data can be duplicated, including electronic money
- Can't allow two copies to both be spent
- Shows ideal no-third-party e-cash can't be possible

### Puzzles / proof-of-work

- Computational problem you solve to show you spent some effort
- 0 Common: choose s so that  $h(m \parallel s)$  starts with many 0 bits
- For instance, required solved puzzles can be a countermeasure against DoS



### Hash trees and timestamp services

- Merkle tree: parent node includes hash of children
- **c** Good hash function  $\rightarrow$  root determines whole tree
- Can prove value of leaf with log-sized evidence
- Application: document timestamping (commitment) service

### Outline

Previous e-cash and techniques

### Bitcoin design

Announcements

**Bitcoin experience** 



Anyone one can send to an address, private key needed to spend

### **Global transaction log**

Basic transaction: Take  $x_1$  from  $a_1, x_2$  from  $a_2, ...,$ put  $y_1$  in  $a'_1, y_2$  in  $a'_2, ...$ 

Of course require 
$$\sum_{i} x_{i} = \sum_{j} y_{j}$$

Keep one big list of all transactions ever

Check all balances in addresses taken from are sufficient

### **Bitcoin network**

- Use peer-to-peer network to distribute transaction log
- Roughly similar to BitTorrent, etc. for old data
- Once a node is in sync, only updates need to be sent
- New transactions sent broadcast

### Consistency and double-spending If all nodes always saw the same log, double-spending would be impossible But how to ensure consistency, if multiple clients update at once? Symmetric situation: me and "me" in Australia both

Symmetric situation: me and "me" in Australia both try to spend the same \$100 at the same time

### **Bitcoin blocks**

- Group ~10 minutes of latest transactions into one "block"
- Use a proof of work so creating a block is very hard
- All nodes race, winning block propagates

### **Bitcoin blockchains**

Each block contains a pointer to the previous one
 Nodes prefer the longest chain they know
 E.g., inconsistency usually resolved by next block

### **Regulating difficulty**

- Difficulty of the proof-of-work is adjusted to target the 10 minute block frequency
- Recomputed over two-week (2016 block) average
- Network adjusts to amount of computing power available

### **Bitcoin mining**

Where do bitcoins come from originally?

- Fixed number created per block, assigned by the node that made it
- An incentive to compete in the block generation race
- Called mining by analogy with gold

### Outline

Previous e-cash and techniques

Bitcoin design

- Announcements
- **Bitcoin experience**

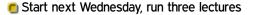
### Project progress report #3

🖲 Due tonight

### Should also include sample of report formatting

- Content can be draft or just progress material
- Choice of MS Word or LaTeX
- N.B., format is more dense than typical class report

### Group project presentations



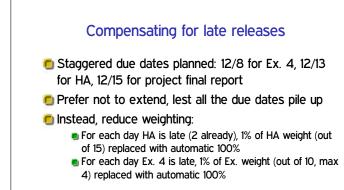
- Plan 10 minute presentation plus say 3 minutes Q&A
- One student per group presents
- Slides, BYO laptop recommended
  - Can send me backup slides (PDF, PPT) night before
  - Let me know if you'd prefer a remote Zoom presentation

### Hands-on assignment status

- Current target for VM availability is late tonight
   PDF instructions updated with . 4 monitoring
- interface
- VM-specific detailed instructions posted
- Many groups still haven't registered

### Exercise set 4

Also targeting late tonight for release
Questions covering the last few course topics



### Outline

Previous e-cash and techniques

Bitcoin design

Announcements

**Bitcoin experience** 



### What can you buy with Bitcoin?

Stuff from increasingly many online retailers

In-person purchases, still mostly a novelty

Ransomware ransoms

🖲 Illegal drugs (Silk Road successors)

Murder for hire: currently probably a fraud

### Bitcoin as a currency

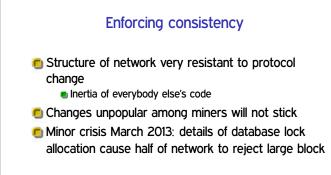
- Can be exchanged for dollars, etc.
  Currently pretty cumbersome
- In some ways more like gold than fiat currencies No central authority
  - Price changes driven more by demand than supply
- 🖲 Exchange rate trend: volatile, recently up

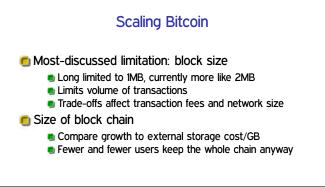
## Deflation and speculation Some people want bitcoins to spend on purchases Demand based on "velocity" Supply does not keep up with interest So, value of 1 BTC has to go up Others want bitcoins because they think the price will go up in the future Self-fulfilling prophecy

But vulnerable to steep drops if expectations change

### Bitcoin mining trends

- Exponentially increasing rates
- **©** CPU  $\rightarrow$  GPU  $\rightarrow$  FPGA  $\rightarrow$  ASIC
- Specialized hardware has eclipsed general purpose Including malware and botnets
- Recent price trends suggest continuing investment





# Speed of confirmation When is it safe to know you have received money? Safe answer: wait for several blocks Too slow for, say, in-person transactions Much faster: wait for transaction to propagate Basic rule: precedence by order seen Standard recommendation is to keep keys mostly offline

### Bitcoin (non-)anonymity

- Bitcoin addresses are not directly tied to any other identity
- But the block chain is public, so there's lots of information
  - E.g., list of largest balances easily collectable

### Zero-knowledge for privacy

- Basic idea: prove this money came from a previous transaction
  - But without revealing which
- Made possible with recent crypto constructions
  Downsides: still expensive, trusted setup
- Two rounds of academic papers lead to "Zcash"

### Different proofs of work

- Desire: avoid centralizing mining in large farms
- Common approach is to make memory rather than computation the limiting factor in cost
  - Similar constructions also used for password hashing
- Some tricky trade-offs, including desire for cheap verification

### Smart contracts

Basically, computer programs that disburse money
 Idea predates Bitcoin, but it's a natural match
 Bitcoin has a limited programming language
 Other contenders, such as Ethereum, have a richer one

