Part I: Reconstructing Bitcoin
Goal

- A rational reconstruction of Bitcoin

1. Start with straw man design
2. Identify weaknesses
3. Augment design and iterate
Step 1: A signed letter of intent

- Alice: “I, Alice, am giving Bob one coin”
- Alice digitally signs message and announces bits to everyone.

Properties
- Establishment of Alice’s intent
- Limited protection from forgery

Weakness
- Coins are not unique; can be duplicated
Step 2: Unique serial nos. on coins

- Alice: “I, Alice, am giving Bob one coin, with serial number 8740348”
- Alice: “I, Alice, am giving Bob one coin, with serial number 8770431”
- Bank issues coins with unique serial numbers, keeps track of who owns coins, verifies transactions

Properties
- Establishment of Alice’s intent
- Better protection from forgery

Weaknesses
- Need trusted bank to issue coins, keep track of who owns coins, verify transactions
- Bank can link transactions to identity
Possible design

- E-cash lecture on Nov 18
  - Retain bank
  - Ensure that bank cannot link transactions to identity
  - Agents cannot double spend their electronic coins

- Key novelty in Bitcoin design
  - No centralized bank
Everyone maintains a copy of the public ledger (block chain) of transactions (keeps track of who owns coins)

Alice: “I, Alice, am giving Bob one coin, with serial number 8740348”

Bob uses his copy of the block chain to check that the coin is Alice’s; he broadcasts both Alice’s message and his acceptance of the transaction to the entire network, and everyone updates their copy of the block chain.

Weaknesses

- How to get serial numbers?
- Double-spending: What if Alice gives the same coin to Bob and Charlie at the same time?
Bob does not verify Alice’s coin by himself.  
Asks everyone on the network to verify  
When “enough” people confirm that the coin is indeed Alice’s, Bob accepts and everyone updates their block chain

Weakness:
- Sybil attack: Alice creates many fake agents who lie for her; Alice spends the same coin many times
Step 4: Proof-of-work

- Computationally costly for network users to validate transactions
- Reward network users for validating transactions

Properties
- Sybil attack won’t work unless dishonest agents put in significant computational resources
- Verifiers rewarded with fixed number of bitcoins for a batch of transactions (details soon)
- Additional ideas to ensure that ledger succinctly maintains history of all transactions (details soon)
Part II: Overview
Bitcoin primer (1/2)

- A peer-to-peer digital payment system
- Completely decentralized digital currency
  - No central mint to produce currency
  - No central bank to verify transactions
  - Once confirmed, transactions are irreversible
  - Predictable, capped, currency supply

- Key innovation in Bitcoin: coin production and verification is done by network consensus
There is actually no notion of a “coin”

- Bitcoins are exchanged from “wallet” to “wallet”
- **Transactions** are at the heart of the protocol
- Wallets are represented by **addresses** (e.g., 1VayNert…)
  - (An address is the public key of the wallet)
Alice wants to send 1 BTC to Bob

- She picks a transaction (or a group of transactions) that she has previously been the recipient of and that cumulatively contain at least 1 BTC
- She then appends Bob’s wallet address to the transaction and digitally signs it

When Bob subsequently wants to spend the 1 BTC, all he has to do is to repeat the operation
Preventing double-spending

- Bob now has 1 BTC
  - He wants to send it to Charlie...
  - ... while keeping it for himself at the same time

- To prevent this Bob (and Alice before him) has to broadcast the transaction to everybody in the Bitcoin network

- Then other peers can verify that the transaction is not a double-spend

- Once this is done, the transaction is embedded forever in a public ledger
The Block Chain of Transactions

[Diagram showing a chain of blocks with arrows pointing from one to the next, ending with the term 'most recent block'.]

[Diagram showing a similar chain with branches leading to 'Block A' and 'Block B'.]
Preventing double spending

\[ \text{Sign}_A(\text{Transfer } X \text{ to } B) \]

\[ \text{Sign}_A(\text{Transfer } X \text{ to } C) \]

Longest chain wins

Slide credit: Joe Bonneau
Bitcoin is *transaction-based*
A Bitcoin Transaction

1. {"hash":"7c4025...", // serial number: hash of transaction
2.  "ver":1, // protocol version
3.  "vin_sz":1, // no. of inputs
4.  "vout_sz":1, // no. of outputs
5.  "lock_time":0, // transaction finalized after time
6.  "size":224, // no. of bytes in transaction
7.  "in":[ // input of transaction 7-11
8.   {"prev_out": // input is an output of a previous transact.
9.     {"hash":"2007ae...", // serial number of previous transact.
10.    "n":0}, // output number of previous transact.
11.    "scriptSig":"304502...042b2d...", // signature and pub key of sender
12.    "out":[ // output of transaction 12-14
13.      {"value":"0.31900000", // outputs 0.319 BTC
14.        "scriptPubKey":"OP_DUP OP_HASH160 a7db6f OP_EQUALVERIFY OP_CHECKSIG"}] // script for verifying transaction}
Bitcoin transactions specify *scripts*

**scriptPubKey:** OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG

**scriptSig:** <sig> <pubKey>

IN:
- scriptSig ...
- scriptSig ...

OUT:
- scriptPub

IN:
- scriptSig A

OUT:
- scriptPubB, 5.0
- scriptPubA, 0.9

Redemption script:

<sig> <pubKey> OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG

*Slide credit: Joe Bonneau*
Bitcoin transactions specify scripts

```
<sig> <pubKey> OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG
```
Bitcoiın script features

https://en.bitcoin.it/wiki/Script
Part III: Mining Bitcoin
Coin production is embedded in the verification process.

Verifiers ("miners") verify batches of transactions at once:

- In exchange for which they are allowed to add a "creation" transaction to the batch and give themselves a fixed amount of money:
  - 50 BTC originally, 25 BTC now, divided by two every so often.
- Verification is combined with a "proof-of-work" scheme to ensure:
  - That transactions have proper timestamping.
  - That currency production is rate-limited.
Miners solve a cryptographic puzzle:
Find \( x \) s.t. \( H(x || l) < y \) where \( l \) is the batch of transactions.

There is no good algorithm to solve this (\( H \) is a cryptographically secure hash function)
- **Brute-force**: try \( x = 0, x = 1, x = 2, x = \ldots \)
- The lower \( y \), the harder the puzzle

Difficulty is tunable and is (by edict) designed to be inversely proportional to the total computational power of the network

The goal is to have one block every ten minutes
- Predictable supply of currency (independent of the difficulty)
- **But this limits how quickly transactions can be verified**
  - At least 10 minutes, usually 60 minutes is recommended
In addition to the bonus they get for mining, miners get “transaction fees”
- Leftover “change” voluntarily left in transactions

Because the bonus is decreasing over time, the expectation is that transaction fees will increase over time to make up for lost mining revenue
Mining rewards

Total BTC In Existence

blocks: 0 210k 420k 630k 840k 1.05M 1.26M

time: 2009 +4 years +8 +12 +16 +20 +24

0 10.5M 21.0M

25 BTC/block

50 BTC/block

12.5 6.25 3.125 1.5625 0.78125

Courtesy: Brian Warner
Total network capacity

- $2^{64}$ hashes per block (every 10 minutes!)
- $2^{75}$ hashes in 2013
  - In exchange for ~US$250M
- Consuming > 100 MW
Part IV: Using Bitcoin
## Getting Bitcoin

- **Become a miner**
  - Nowadays only profitable if dedicated (ASIC) hardware

- **Buy at an exchange**
  - CampBX, Bitstamp, BTC-e, Coinbase...
  - (Mt.Gox before they went bankrupt)
  - Very **high concentration** on exchanges through which money is exchanged
    - Exchanges fail pretty often...
  - Increasingly scrutinized by regulators

- **Buy from individuals**
  - Satoshi Square in NYC
Main Bitcoin uses

- As a speculative instrument
  - People invest in BTC, betting on its rising value
  - Dominant use thus far
Main Bitcoin uses

- As a currency
  - Only currency accepted on underground marketplaces (Silk Road, Evolution,...)
    - (Except for LiteCoin, which is a clone of Bitcoin)
    - Because of its “anonymity properties”
    - Still relatively modest
      - Entire Silk Road revenue represented in 1st half of 2012 about $15M/annum
  - Gambling, poker sites
    - Large number of transactions, volume not very high
  - Other uses still in their infancy
    - Campaign contributions, online stores (e.g., Overstock), etc
Part V: Anonymity?
Pseudonymity vs anonymity

- Wallets are public/private key pairs
  - Can create as many as you want
  - Think of them as zero-cost pseudonyms

- There is no central authority issuing Bitcoins or vetting transactions

- This means Bitcoin is anonymous, right? **NO!**
Anonymity here implies **unlinkability** of transactions

The entire ledger of **all transactions** is available, forever
- Technically in a compressed form, but transaction chains can all be reconstructed

Even if you add intermediary dummy steps wallets, linking the source and the destination of a transaction may be done by graph analysis...
- Something that computer scientists know how to do!
  - Reid & Harrigan, 2011
  - Shamir & Ron, 2012
  - Meiklejohn et al., 2013

Families of wallets can be pooled together as belonging to the same actual user...
- ...and if somehow you can get the user’s identity, the game is over
Anonymizing Bitcoin

- **Mixers**

  - Alice
    - 10 BTC
  - Bob
    - 10 BTC
  - Mixer
  - Charles
    - 10 BTC
  - Daisy
    - 10 BTC

- **Did Alice give 10 BTC to Charles or Daisy?**
Mixers in practice

Need to also introduce arbitrary delays
Introduction of change addresses, etc
Mixer can be dishonest!
It’s unclear how good existing Bitcoin mixers are

- Key difference with message mixing (Tor, mixnets)
  - You can’t implement arbitrary “padding” – money has to go somewhere eventually

- Possible measure: taint
  - Amount of money that can be traced back to a given source

- Recent research suggests existing mixers are not effective or downright dishonest
Acknowledgment

- Slides 2-10, 15, 18, 21 are mine
- Thanks to Nicolas Christin for all other slides
Mining difficulty

Bitcoin Hash Rate vs Difficulty (9 Months)

- Blue line: Hash Rate (504)
- Green line: Hash Rate (2016)
- Red line: Difficulty

Time periods: Mar, May, Jul, Sep, Nov
Difficulty adjustment

Bitcoin Block Generation Time vs Difficulty

- Block Generation Time (2009)
- Block Generation Time (2018)
- Estimated Next Difficulty
- Difficulty

- Seconds: 540, 560, 580, 600, 620
- Difficulty: 6.0e+10, 6.5e+10, 7.0e+10, 7.5e+10, 8.0e+10

Oct | Nov | Dec
Bitcoin mining hardware

TerraMiner™ IV – 2TH/s
Networked ASIC Miner

$5,999

Shipping June 2014

300 GH Bitcoin Mining Card
The Monarch BPU 300 C

$1,497.00

Pre-Order Terms: This is a pre-order. 28nm ASIC bitcoin mining hardware products are shipped according to placement in the order queue, and delivery may take 3 months or more after order. All sales are final.

Slide credit: Joe Bonneau
Should I mine bitcoins?

Chilkoot pass, Klondike 1898

Slide credit: Joe Bonneau