“Crypto” currencies

Thanks to Ari Juels for this deck!
## Grade Discussion

<table>
<thead>
<tr>
<th></th>
<th>Attendance</th>
<th>Midterm</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AVERAGE</strong></td>
<td>74.2%</td>
<td>51.4</td>
</tr>
<tr>
<td><strong>MEAN</strong></td>
<td>79.0%</td>
<td>51.5</td>
</tr>
<tr>
<td><strong>STDDEV</strong></td>
<td>26.9%</td>
<td>18.7</td>
</tr>
<tr>
<td><strong>MAXIMUM</strong></td>
<td>106.0%</td>
<td>88.5</td>
</tr>
<tr>
<td><strong>MINIMUM</strong></td>
<td>4.0%</td>
<td>18.0</td>
</tr>
</tbody>
</table>
One of the earliest proposed uses of digital signatures (RSA) was to create virtual currency (in Ireland)

- Idea: A bank creates coins consisting of digital signatures
- Simplified version…

Virtual $ = \text{Sig}(SK, \, “I’m dollar #123”)

Everyone can check: Ver(PK, Virtual $)
The backdrop

• In 1982, “blind” digital signatures introduced by David Chaum
  • (Yes, the same Chaum who invented mix networks \texttbf{→} Tor)
  • Allowed banks to sign coins without seeing them — led to \textit{anonymous} virtual currency
  • Turned into Digicash company [1990–1998]

• Researchers published hundreds of papers on virtual currency for decades after
  • Financial Cryptography
  • PayWord and MicroMint [2001]
    • MicroMint used \textit{proof of work} to create coins
    • Turned into Peppercoin company [2001–2007]
  • 800+ citations

• But no one used virtual currency…
Bitcoin

- Created by “Satoshi Nakamoto”
  - Paper “Bitcoin: A peer-to-peer electronic cash system” [2008]
  - Source code [2009]
- As of today, $1+ Trillion market capitalization
- **But who is Nakamoto?**
Bitcoin

- Created in 2008 by “Satoshi Nakamoto”
  - Paper “Bitcoin: A peer-to-peer electronic cash system”
  - Source code
- As of today, $1+ Trillion market capitalization
- **But who is Nakamoto?**
Bitcoin

- Created in 2008 by “Satoshi Nakamoto”
  - Paper “Bitcoin: A peer-to-peer electronic cash system”
  - Source code
- As of today, $1+ Trillion market capitalization
- **But who is Nakamoto?**

And another…
How to Acquire and Spend Bitcoins
Getting started

• Let’s understand how Bitcoin (BTC) is used

• To start, anyone can create her own Bitcoin "address" / account

  • Digital wallet (app) can do this for you

  • Creates cryptographic "key pair" \((SK_x, PK_x)\)
    
    • Secret key \(SK_x\): to authorize use of your Bitcoin
    
    • Public key \(PK_x\): public identifier and to validate transactions
    
    • Address comes from public key
    
    • We’ll discuss details later…
Bitcoin wallet

- Also permits easy management of Bitcoins
- Sending and receiving…
Ways to score some BTC

- Buy through online exchange, e.g., Coinbase
  - Sent to wallet or “banked”
- "Mine" BTC
  - To be discussed…
- Have someone with BTC send some to your wallet
  - Buyer of some good you're selling, friend, etc.
  - Bitcoin ATM…
  - Exchange
1. **Get Bitcoin**

There are several ways to get Bitcoins, but the easiest is to exchange them for currency at your bank or a Bitcoin exchange. You can also buy Bitcoins from friends, accept them as payment for goods or services, or generate new Bitcoins through a process called “mining.”

[Sign Up at Coinbase.com](https://www.coinbase.com)

2. **Shop Overstock.com**

You can now pay for all your favorite products on Overstock.com using Bitcoins! As the first major retailer to accept Bitcoins, Overstock.com is expanding the possibilities of Bitcoin purchases by offering thousands of products to the Bitcoin community.

[overstock.com](http://www.overstock.com)
Bitcoin design—from basic principles
Key property #1: Bitcoin is **pseudonymous**

- What does this mean?
- Each entity $X$ has an (ECDSA) key pair $(SK_X, PK_X)$
- No association between $X$ and real-world identity
Digital signatures are used in Bitcoin

Bitcoin uses ECDSA

- “Elliptic-Curve Digital Signature Algorithm”
- Concretely, uses secp256k1 (slightly nonstandard) curve
  - Private key $SK$ is 256 bits; (uncompressed) public key $PK$ is 512 bits
Could build naïve system…

- Idea: Coins and transactions, i.e., flow of money, can be authenticated—neither is forgeable
- Thanks to public-key crypto, everyone can verify all coins and transactions (if public keys are distributed throughout system)
- But we still have the double-spending problem…

\[
\text{Sig}(SK_x, \text{"Virtual $\#123 \text{ to Y}"})
\]

\[(SK_y, PK_y)\]
Idea: Bank maintains a ledger

\[
\text{Sig}(SK_x, \text{"Virtual $\#123 to } PK_y\text{"})
\]

Bob checks \text{Sig and ledger} ✔︎
Ledger

• Ledger is up-to-date record of all transactions.

• Bob now checks the ledger to be sure that Virtual $ #123 hasn’t been spent.

• Double-spending is now prevented!
But there’s still a problem…

- You have to trust the Bank!
- Problems:
  - What if the Bank claims not to have received a transaction?
    - i.e., doesn’t put it in ledger
  - What if the Bank confiscates money?
  - Who’s going to create money? The Bank?
  - What if the Bank devalues money?
Key property #2: Bitcoin is decentralized

- No Bank!
- Ledger is agreed upon and distributed among many entities
- Called the **blockchain** in Bitcoin
- The key innovation in Bitcoin over older virtual currencies
How does Bitcoin work?

• Every "account" holder has an (ECDSA) private / public digital signature key pair ($SK, PK$)
• (Account address is $Addr = H(PK)$)
• Private keys sign (authorize) movement of money
• Simplified transaction…
  • ("Pay to PubKey Hash (P2PKH)"")
Global ledger ("blockchain")

- Publicly records all Bitcoin transactions worldwide over time
Blockchain

- Record of every transaction in Bitcoin system
- Maintained as append-only data structure
- New block added every 10 minutes (on average)
- Each block contains a bundle of latest transactions.
  - E.g., SIG\textsubscript{PKA} [“Alice sends 0.4 BTC to Bob”]
  - (Actually, there’s a scripting language, but we’ll gloss over it…)

```
height = 0
height = 1
height = 2
height = 3
```
Blockchain

- Because full chain is a complete ledger / history of all transactions…
- Computing over the full block chain reveals the state / ownership of all BTC
- No explicit “account balances”
- Structured in terms of transactions

[Figure source: http://www.righto.com/2014/02/bitcoins-hard-way-using-raw-bitcoin.html; Hi, Ken!]
But how is a block validated?

- I.e., how does system decide what transactions go into next block?
- Ideal for P2P system: All clients in the world vote on the correct block chain.
- But it’s hard to ensure one vote per machine.
  - E.g., there’s the problem of “Sybil” attacks: How to prevent one user from creating multiple identities?
- So "voting" (cleverly) in Bitcoin takes the form of hash power.
  - I.e., one vote per CPU (roughly speaking)
But how is a block validated?

• Communal, computationally-intensive process called *mining*.
  • Together, mining community defines blockchain

• Intuition:
  • All miners collectively search for hard-to-compute “signature” on new block
  • Solution proves w.h.p. that result is communal effort
  • Attacker with little computing power unlikely to mine block
Block mining

Precise mining problem: Find a ticket that yields hash image with value less than target Z.

\[
\text{SHA-256}^2(\text{Block}_{N+1}, X_{N+1}, \text{ticket}_{N+1}) = 0x0000000000001d7a1...
\]

\[
\text{SHA-256}^2(\text{Block}_N, X_N, \text{ticket}_N) = 0x000000000000c67aa...
\]
Block mining

SHA-256^2(Block_{N+1}, X_{N+1}, ticket_{N+1}) = 0x0000000000001d7a1...

SHA-256^2(Block_N, X_N, ticket_N) = 0x000000000000c67aa...

X_N = (software version, hash (Merkle-tree root) of new transactions, and current time)
This problem requires a massive amount of hash power

• The mining puzzle is called a *Proof of Work* (PoW)
• In Random Oracle Model for SHA-256, expected (double) hashes to mine a block is…
  • $2^{256} / Z$
  • = (Bitcoin “Difficulty” factor) $\times 2^{32}$
• Difficulty adjusted every 2016 blocks to achieve 10-minute block mining epoch

$$SHA-256^2(\text{Block}_{N+1}, X_{N+1}, \text{ticket}_{N+1}) \leq Z$$
This problem requires a massive amount of hash power

- In Nov. 2017, expected number of (double) hashes to mine a block was roughly $10^{22}$.
- In Nov. 2021, Whole Bitcoin network is running at about $180,000,000$ TH/s!
- Not easily duplicated, so hard for attacker to seize control of network

$$\text{SHA-256}^2(\text{Block}_{N+1}, X_{N+1}, \text{ticket}_{N+1}) \leq Z$$
What’s the incentive for miners to mine?

• Key idea: Bitcoin is a lottery.
• Every miner tries tickets until a “winning” one is found.
• The prize for the winner: Bitcoins!
  • Special transaction in block assigns BTC to winner
  • Originally, 50 BTC; today (nov 2021), 6.25 BTC ($351,000+ on 23 Nov 2021.)
  • Winner also gets transaction fees
• 21 million BTC will be produced over the lifetime of the system.

\[
\text{SHA-256}^2(\text{Block}_{N+1}, X_{N+1}, \text{ticket}_{N+1}) \leq Z
\]
What’s the incentive for miners?

- In principle, Bitcoin is democratic
- *Anyone* can mine.
- Reward is proportional to computational investment.
- But...
How do miners mine?

• In the early days, people just used their PCs.
• ASIC (Application-Specific Integrated Circuit) hardware is much more cost-effective.
• Professionals buy and replace ASICs frequently.
Researchers from Cornell University say that on multiple occasions, a single mining pool repeatedly contributed more than 51 percent of Bitcoin's total cryptographic hashing output for spans as long as 12 hours. The contributor was GHash, which bills itself as the "#1 Crypto & Bitcoin Mining Pool." During
GINI Index (Inequality Index)

Estimate for Bitcoin: 88
Other parts of Bitcoin
Mining blocks isn’t enough

• What else is needed to make a working monetary system?
  • Broadcasting transactions and blocks
  • Storing ledger / blockchain
  • Enabling users to spend and receive money
Some node types in Bitcoin network

Reference Client (Bitcoin Core)
Contains a Wallet, Miner, full Blockchain database, and Network routing node on the bitcoin P2P network.

Full Block Chain Node
Contains a full Blockchain database, and Network routing node on the bitcoin P2P network.

Solo Miner
Contains a mining function with a full copy of the blockchain and a bitcoin P2P network routing node.

Lightweight (SPV) wallet
Contains a Wallet and a Network node on the bitcoin P2P protocol, without a blockchain.

+Super Node
• Publicly accessible

+Pool Miner
• Lacks full blockchain

[Source: http://chimera.labs.oreilly.com/books/1234000001802/ch06.html]
Routing functionality

• Transactions and blocks are broadcast to *entire network of full nodes*

• Rebroadcast protocol
  • Each node transmits to 8 other (randomly selected) nodes
  • TCP on port 8333
Full nodes

• Store entire blockchain
• Enforce consensus rules, ensuring blocks in blockchain adhere to
  • 12.5 BTC reward
  • Correct signatures on transactions
  • BTC not double-spent
  • Etc., etc.
Full node distribution

GLOBAL BITCOIN NODES DISTRIBUTION
Reachable nodes as of Tue Nov 21 2017 09:10:20 GMT-0500 (EST).

10975 NODES
24-hour charts »
Top 10 countries with their respective number of reachable nodes are as follow.

<table>
<thead>
<tr>
<th>RANK</th>
<th>COUNTRY</th>
<th>NODES</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>United States</td>
<td>3090</td>
</tr>
<tr>
<td>2</td>
<td>Germany</td>
<td>1849</td>
</tr>
<tr>
<td>3</td>
<td>France</td>
<td>748</td>
</tr>
<tr>
<td>4</td>
<td>China</td>
<td>662</td>
</tr>
<tr>
<td>5</td>
<td>Netherlands</td>
<td>529</td>
</tr>
<tr>
<td>6</td>
<td>Canada</td>
<td>450</td>
</tr>
<tr>
<td>7</td>
<td>United Kingdom</td>
<td>439</td>
</tr>
<tr>
<td>8</td>
<td>n/a</td>
<td>370</td>
</tr>
<tr>
<td>9</td>
<td>Russian Federation</td>
<td>350</td>
</tr>
<tr>
<td>10</td>
<td>Singapore</td>
<td>236</td>
</tr>
</tbody>
</table>

More (99) »

Map shows concentration of reachable Bitcoin nodes found in countries around the world.
Bitcoin wallets

• You don't need to mine or run full node to use Bitcoin

• Wallet are applications that permit easy management of a Bitcoins.

• What’s going on under the hood?
Bitcoin wallets: Under the hood

- Remember: identity associated with ECDSA digital signature key pair
- SK used to sign / authorize transactions.
- PK used to identify users and verify transactions.
- Bitcoin wallet stores, protects, and allows use of SK to make transactions.
Brain wallets

• You can generate SK from a password

• Your Bitcoin are then completely portable.
Brain wallets

- Unfortunately, human brains are poor password stores…
- Cracking brainwallets at one point rumored more profitable than mining…
Bitcoin’s good features
The **blockchain** means much more than Bitcoin

- Nebulous term…
- Generally refers to *ledger*
- Distributed, robust, publicly visible piece of memory
- Good for things other than money!
  - Timestamping documents
  - Audit
  - Etc., etc.
Bitcoin’s nice properties

- Low transaction fees + no middleman
  - Low-fee payments
- Decentralized
  - Cross-border remittances

But Bitcoin basically only good for moving currency around...
Bitcoin problems
Ponzi Scheme with Huge Marketing Push

Laura Saggers releases world’s first Bitcoin love song

Including your dog…
Huge environmental impact

Major Update (September 10, 2014): Speed increase; 6TH/s Yukon is now $3,920.00 !! (Best on the Market for now)

The SP31 Yukon Power Miner

The introduction of the SP31 Yukon powerful miner is good news to the bitcoin markets. The essential 5.5 TH/s mining machine focuses on the affairs of traders, it has an amazing hash power and consumes relatively very low power. It has been understood that the hashing power of SP31 has four times the power of SP10 and relatively twice the hash to power ratio.

- **Mining Software**: cgmixer with custom plugin
- **Form Factor**: 2U rack mountable (mounting ears provided)
- **Network**: Single 10/100 Ethernet port
- **Fans**: 4 x 80 mm
- **Power Supply**: 2 x 1200 W - Drawing 1500 W "at the wall" (manufacturer)
- **Input Rating**: 90 - 264 VAC
- **Nominal Power Consumption**: 3000 W

Exclusive 1st Review: Bitmain Antminer S7, 4.8+ th/s Using Only 1250 Watts

- **Earnings**: US$2,165/day
- **Power**: 3,458 MWh/day
- **Cost of electricity**: > US$560,887/day

Impact of ZeroAccess Botnet

One of the largest P2P botnets ever known

*Botnet generates...

- 1.9Mx
- earns US$2,165/day
- Per annum earnings: Tens of millions US$!!!
Huge Environmental Impact

- 2017: $1+ billion in computing hardware invested in Bitcoin ecosystem
- 2800+ MW (http://realtimebitcoin.info/) and growing...
Huge destabilizing effect

Tor + Bitcoin = End-to-end anonymity for commercial transactions
Dear Customer:

It is time to pay for your software lease from PC Cyborg Corporation. Complete the INVOICE and attach payment for the lease option of your choice. If you don’t use the printed INVOICE, then be sure to refer to the important reference numbers below in all correspondence. In return you will receive:

- a renewal software package with easy-to-follow, complete instructions;
- an automatic, self-installing diskette that anyone can apply in minutes.

Important reference numbers:

The price of 365 user applications is US$189. The price of a lease for the lifetime of your hard disk is US$378. You must enclose a bankers draft, cashier’s check or international money order payable to PC Cyborg Corporation for the full amount of $189 or $378 with your order. Include your name, company, address, city, state, country, zip or postal code. Mail your order to PC Cyborg Corporation, P.O. Box 87-17-44 Panama 7, Panama.

Press ENTER to continue

1989 PC Cyborg
Your important files were encrypted on this computer: photos, videos, documents, etc. You can verify this by click on see files and try to open them.

Encryption was produced using unique public key RSA-4096 generated for this computer. To decrypt files, you need to obtain private key.

The single copy of the private key, which will allow you to decrypt the files, is located on a secret server on the Internet, the server will destroy the key within 72 hours after encryption completed. After that, nobody and never will be able to restore files.

To retrieve the private key, you need to pay 0.5 bitcoins.

Click proceed to payment to obtain private key.

Any attempt to remove or damage this software will lead to immediate private key destruction by server.
Not truly anonymous

- Recall Bitcoin is *pseudonymous*, i.e., traceable on per-identity basis
- E.g., suppose you’re Satoshi Nakamoto and you want to spend your 1,624,500 BTC ($1 billion) anonymously…
- Thus NSA conspiracy theory…

But...

Greetings! New to Zcash?
The Zcash network is young, but evolving quickly! Sign up and we’ll be in touch with more information about how you can get started with Zcash!

Internet money
Bitcoin and most cryptocurrencies expose your entire payment history to the public. Zcash is the first open, permissionless cryptocurrency that can fully protect the privacy of transactions using zero-knowledge cryptography.
New York one of the first states to regulate Bitcoin

Know-your-customer (KYC) at odds with pseudonymity / anonymity!
Long-term problems

• Scaling!
• Blocks are at most around 1MB in size
  • Transaction about 500B on average
  • Typically around 2000-2500 transactions per block
  • About 4 transactions / sec. throughput
• Should we:
  • Increase the block size or
  • Increase the mining rate or
  • Do something else?
• Big controversy!
• Solutions:
  • Segwit (partially) deployed in Bitcoin
  • Bitcoin Cash has 8MB blocks
Proof of Stake
Proof of Capacity