CSE 127: Introduction to Security

Lecture 19: Vulnerability disclosure, personal hygiene, and cryptocurrencies

Nadia Heninger

UCSD

Winter 2023

Some material from Eric Wustrow

Lecture Outline

- Government backdoors and transparency
- Security vulnerability disclosure
- Personal security hygiene
- Cryptocurrencies

FISA background

1978 Foreign Intelligence Surveillance Act

- Passed in response to Church Committee investigation of COINTELPRO scandals
- Codified separation between domestic law enforcement activities and international intelligence activities
- FISA Court established to handle surveillance warrants for intelligence investigations in the US

After 2001, PATRIOT Act weakened some of these separations.

Snowden leaked FISA order for all Verizon Business customer information in 2013

IN RE APPLICATION OF THE
FEDERAL BUREAU OF INVESTIGATION
FOR AN ORDER REQUIRING THE
PRODUCTION OF TANGIBLE THINGS
FROM VERIZON BUSINESS NETWORK SERVICES,
INC. ON BEHALF OF MCI COMMUNICATION
SERVICES, INC. D/B/A VERIZON
BUSINESS SERVICES.

Docket Number: BR 13-80

SECONDARY ORDER

This Court having found that the Application of the Federal Bureau of Investigation (FBI) for an Order requiring the production of tangible things from **Verizon Business Network Services, Inc. on behalf of MCI Communication Services Inc., d/b/a Verizon Business Services (individually and collectively "Verizon")** satisfies the requirements of 50 U.S.C. § 1861,

IT IS HEREBY ORDERED that, the Custodian of Records shall produce to the National Security Agency (NSA) upon service of this Order, and continue production on an ongoing daily basis thereafter for the duration of this Order, unless otherwise ordered by the Court, an electronic copy of the following tangible things: all call detail records or "telephony metadata" created by Verizon for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls. This Order does not require Verizon to produce telephony metadata for communications wholly originating and terminating in foreign countries. Telephony metadata includes comprehensive communications routing information, including but not limited to session identifying information (*e.g.*, originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity (IMEI) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of call. Telephony metadata does not include the substantive content of any communication, as defined by 18 U.S.C. § 2510(8), or the name, address, or financial information of a subscriber or customer.

IT IS FURTHER ORDERED that no person shall disclose to any other person that the FBI or NSA has sought or obtained tangible things under this Order, other than to: (a) those persons to whom disclosure is necessary to comply with such Order; (b) an attorney to obtain legal advice or assistance with respect to the production of things in

TOP SECRET//SI//NOFORN

Derived from: Pleadings in the above-captioned docket
Declassify on: 12 April 2038

Updated FISA orders have continued to be approved.

Verizon Government Transparency Report

National security demands

The table below sets forth the number of national security demands we received in the applicable period. Under section 603 of the USA Freedom Act we are now able to report the number of demands in bands of 500.

	Jan 1, 2016 – Jun. 30, 2016	Jul. 1, 2016 – Dec. 31, 2016	Jan 1, 2017 – Jun. 30, 2017	July 1, 2017 – Dec. 31, 2017	Jan 1, 2018 – Jun. 30, 2018	Jul. 1, 2018 – Dec. 31, 2018	Jan 1, 2019 – Jun. 30, 2019
National Security Letters	1-499	5-499	1-499	501-999	1-499	0-499	0-499
Number of customer selectors	500-999	1000-1499	1500-1999	1500-1999	2000-2499	2000-2499	1500-1999
FISA Orders (Content)	0-499	0-499	0-499	0-499	0-499	0-499	*
Number of customer selectors	2000-1499	2000-2499	1500-1999	2000-2499	2000-2499	1500-1999	*
FISA Orders (Non-Content)	0-499	0-499	0-499	0-499	0-499	0-499	*
Number of customer selectors	0-499	0-499	0-499	0-499	0-499	0-499	*

* The government has imposed a six month delay for reporting this data.

“In the first half of 2019, we received between 0 and 499 NSLs from the FBI. Those NSLs sought information regarding between 1500 and 1999 ’selectors’ used to identify a Verizon customer. ”

Associated Press

This undated photo released by the United States government shows the National Security Agency campus in Fort Meade, Md.

commerce and banking systems, protects sensitive data like trade secrets and medical records, and automatically secures the e-mails, Web searches, Internet chats and phone calls of Americans and others around the world, the documents show.

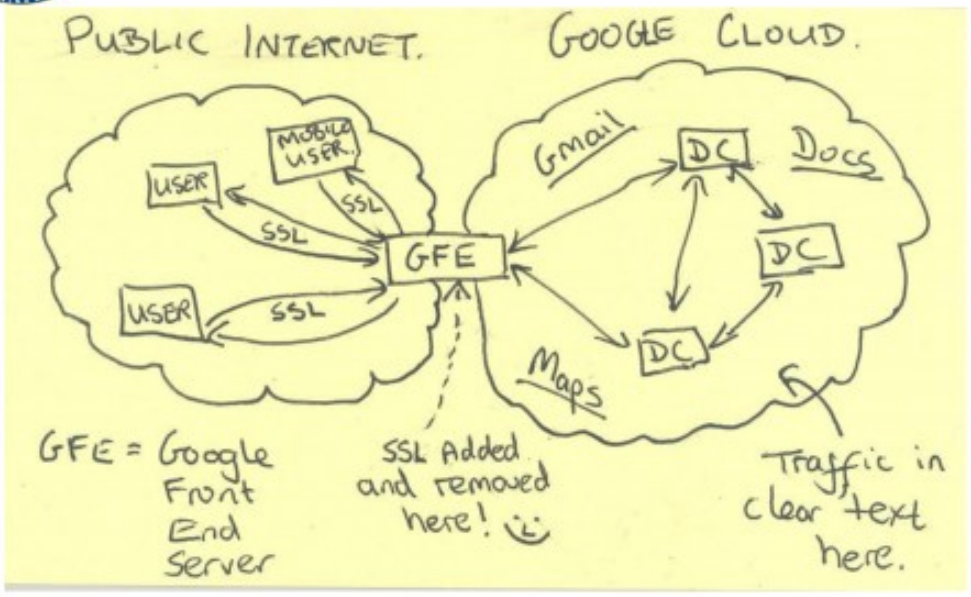
This article has been reported in partnership among The New York Times, The Guardian and ProPublica based on documents obtained by The Guardian. For The Guardian: James Ball, Julian Borger, Glenn Greenwald. For The New York Times: Nicole Perlroth, Scott Shane. For ProPublica: Jeff Larson.

Many users assume — or have been assured by Intern companies — that their data is safe from prying eyes, including those of the government, and the N.S.A. wa keep it that way. The agency treats its recent successe deciphering protected information as among its most closely guarded secrets, restricted to those cleared for highly classified program code-named Bullrun, accor to the documents, provided by Edward J. Snowden, t

October 2013: MUSCULAR

TOP SECRET//SI//NOFORN

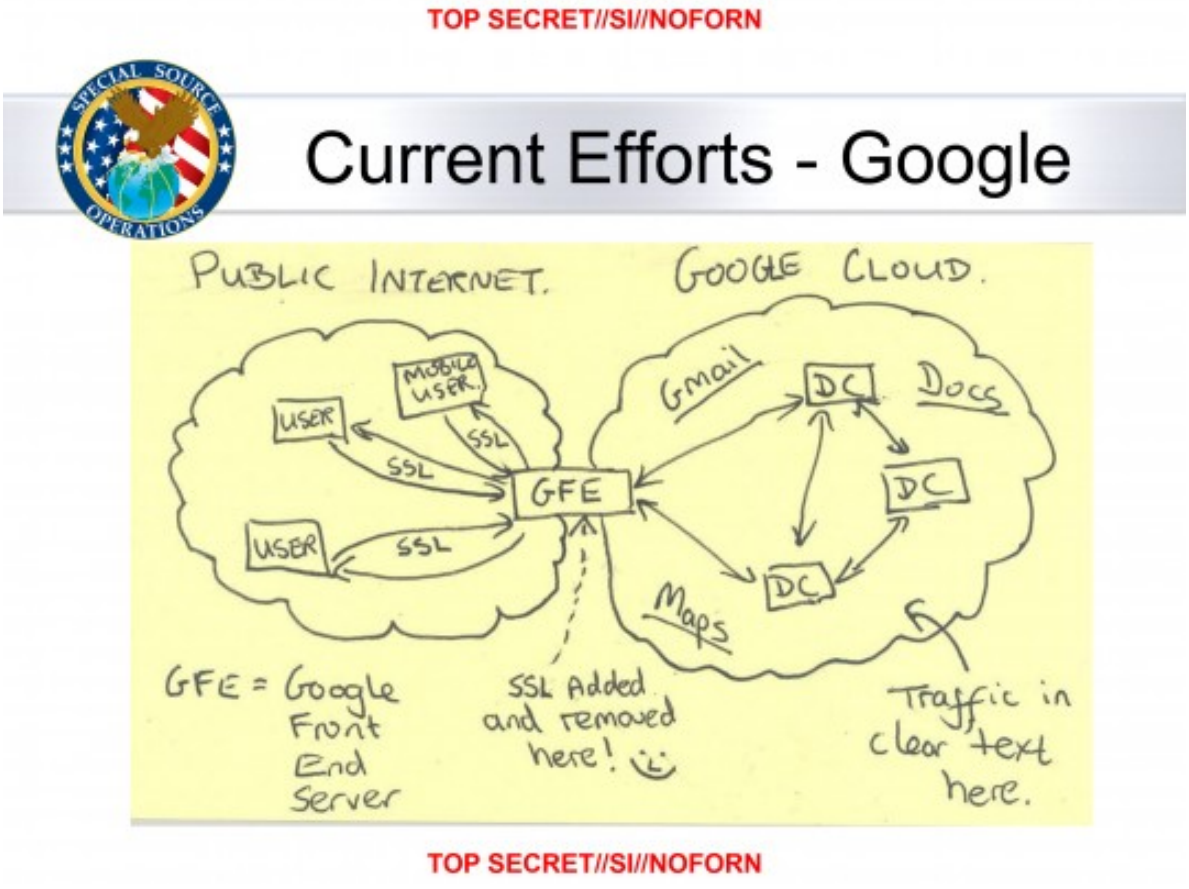
Current Efforts - Google



TOP SECRET//SI//NOFORN

Official Google statement:
“We are outraged”

October 2013: MUSCULAR



Official Google statement:
“We are outraged”

Unofficial Google statement: “Fuck these guys.”

Key Escrow and Law Enforcement Backdoors Redux

Recently, the head of the National Security Agency provided a rare hint of what some U.S. officials think might be a technical solution. Why not, suggested Adm. Michael S. Rogers, require technology companies to create a digital key that could open any smartphone or other locked device to obtain text messages or photos, but divide the key into pieces so that no one person or agency alone could decide to use it?

"I don't want a back door," Rogers, the director of the nation's top electronic spy agency, said during a speech at Princeton University, using a tech industry term for covert measures to bypass device security. "I want a front door. And I want the front door to have multiple locks. Big locks."

Law Enforcement Access Policy

Policy/ethics question: Is it preferable to have law enforcement/intelligence:

- Stockpile software vulnerabilities, write targeted malware, and hack into targets when desired
- Mandate encryption backdoors or otherwise enable mass surveillance

Unintended Consequences of Stockpiling Vulnerabilities

1. NSA develops EternalBlue exploit against Windows SMB.
2. The Shadow Brokers leak a collection of NSA exploits including EternalBlue in 2017.
3. The NSA had kept the vulnerability to itself for five years instead of informing Microsoft.
4. Microsoft released a patch for the vulnerability in 2017.
5. WannaCry, NotPetya, and other ransomware exploiting EternalBlue cause $1B+ in damages in 2017 and 2018 (NHS England, Maersk among major victims)

Unintended Consequences of Law Enforcement Access

- 2004 Greek wiretapping scandal
  - Greek politicians wiretapped through law enforcement access system present on phone network
  - System was present because of US CALEA law, not used in Greece
- 2010 China Google hack
  - Attackers entered through law enforcement access portal

Disclosure options for security flaws

- Develop fully weaponized malware and distribute on black market
- Tell no one
- Sell vulnerability to middleman and don’t report to vendor
- Report to vendor only
- Report to vendor and receive bug bounty
- Report to vendor, wait for fix, report to public (“responsible disclosure”)
- Report in full to public immediately (“full disclosure”)

The process of reporting vulnerabilities

- Some vendors have sensible reporting process
  - E.g., Firefox and Chrome teams respond and react quickly, easy to work with on fixing bugs, etc.
- Some vendors less so
  - E.g., Send email through an intermediary, receive ACK, no real conversation.
  - E.g., Send email, poke individual folks for replies, no replies. Give up.
- Some vendors are playing catch up
- Some vendors are the worst: they will try to gag/sue you

Bug bounty programs

- Many vendors have bug bounty programs: $$ for bugs
  - Mozilla and Google will even run your checkers and pay you if the checkers find real bugs
- Students have made $3-10K on some papers!

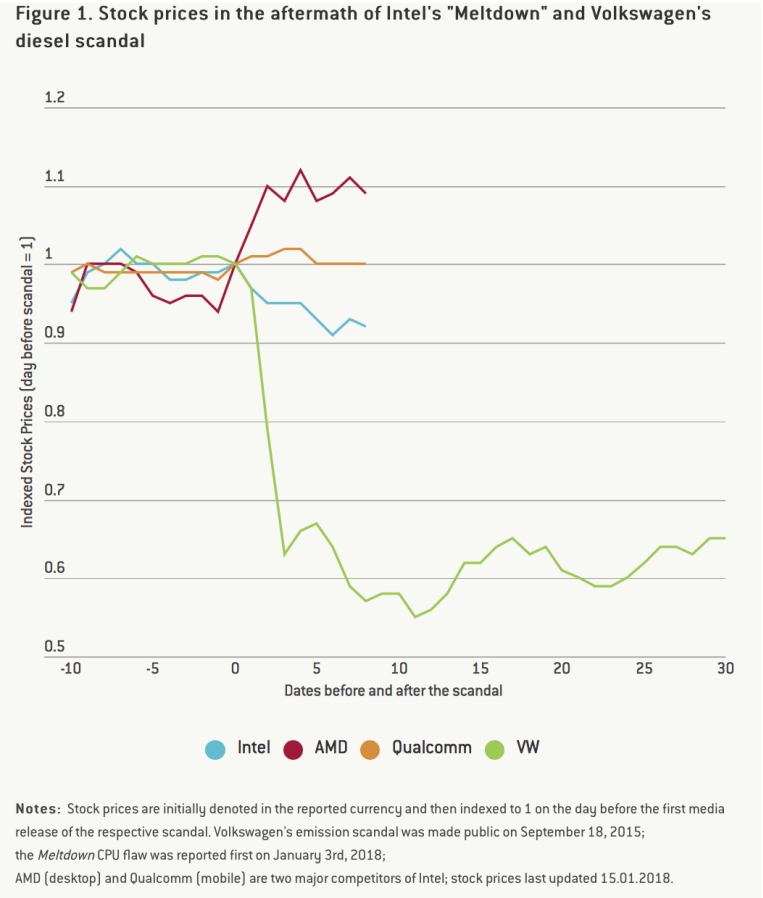
	High-quality report with functional exploit	High-quality report	Baseline
Sandbox escape / Memory corruption in a non-sandboxed process	$30,000	$20,000	$5,000 - $15,000
Universal Cross Site Scripting	$20,000	$15,000	$2,000 - $10,000
Renderer RCE / memory corruption in a sandboxed process	$10,000	$7,500	$2,000 - $5,000
Security UI Spoofing	$7,500	N/A [1]	$500 - $3,000
User information disclosure	$5,000 - $20,000	N/A [1]	$500 - $2,000
Web Platform Privilege Escalation	$5,000	$3,000	$500 - $1,000
Exploitation Mitigation Bypass	$5,000	$3,000	$500 - $1,000
Chrome OS	See below		
Chrome Fuzzer Bonus	$1,000		
Chrome Patch Bonus	$500 - $2,000		

Are companies liable for security flaws?

The FTC says yes.

- 2011 Facebook settlement for deceptive privacy policies
- 2013 HTC settlement for security flaws in phones
- 2016 LabMD liable for failure to institute reasonable security practices to protect consumer data

The stock market says not really:



nakedcapitalism.com

Policy questions around security research

- Should exploit sales be legal?
  - Code as speech principle says yes
- Is publishing exploits ethical?
- How about mixed-use tools?
  - Privacy tools like Tor or encrypted messengers used by criminals, normal people, activists
  - Cryptocurrency enables ransomware, sanction evasion
  - Random darknet shopper art piece?

Personal security hygiene.

Back up your computers

- If you can, keep a local (auto-backup to external drive) and a remote (rsync, Dropbox, Github) backup.

What threats does this help mitigate?

Password security

- Use a different password for every single web site.
- Use a password manager to store your passwords for you.
- Turn on two-factor authentication whenever it is available.
- Use public-key authentication for SSH servers.
- Be careful about phishing attempts.

What threats does this help mitigate?

Encrypt your laptop and phone hard drive

- OS X: Filevault; Windows: BitLocker; Linux: Whatever your distribution uses.
- Also set a lock screen with a password.

What threats does this help mitigate?

Maintaining computer hygiene

- Keep your OS and software up to date.
- Don’t install random software or apps
- Use Google Drive or similar to preview files
- Use a VM to open sketchy files or run software you don’t trust.

What threats does this help mitigate?

Travel and transit

- Consider using a VPN or Tor when on untrusted WiFi
- You can also use a SSH tunnel in a pinch
- Consider having a minimal travel laptop.

What threats does this help mitigate?

Encryption applications

- Encrypted chat: Signal; WhatsApp also uses Signal protocol
- Make sure your web sites support HTTPS
- PGP (ugh) is probably still the best option for sending encrypted email or files

What threats does this help mitigate?

By request: Cryptocurrencies.

Historical background: Cypherpunks

"We the Cypherpunks are dedicated to building anonymous systems. We are defending our privacy with cryptography, with anonymous mail forwarding systems, with digital signatures, and with electronic money." – Eric Hughes, A Cypherpunk's Manifesto, 1993

- 1985: David Chaum "Security without identification: Transaction systems to make Big Brother obsolete"
- In the 1990s, the Cypherpunks mailing list was extremely active; many influential members
- Software: PGP, Tor, anonymous remailers, Off-the-record messaging...
- Cypherpunk ideas: Anonymous digital currency, WikiLeaks, assassination markets, pseudonymity...
- These ideas encode libertarian-to-anarchist politics

How do you build digital currency?

A central authority can keep a balance ledger and update with each transaction.

Account	Amount
Dave	$342.87
Fred	$32,944.09
Eve	$89,218.87
Charlie	$429,718.90
Alice	$1,000.00
Bob	$0.00

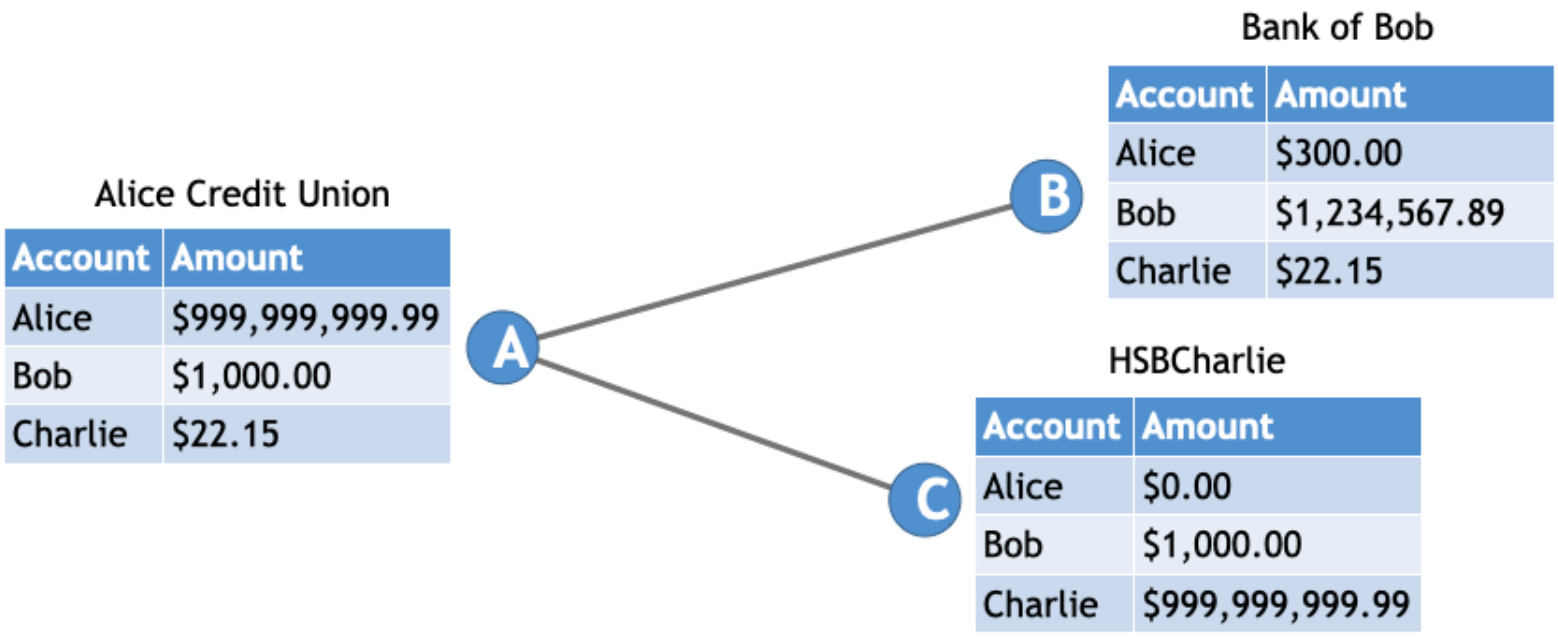
Alice pays Bob $200

Account	Amount
Dave	$342.87
Fred	$32,944.09
Eve	$89,218.87
Charlie	$429,718.90
Alice	$800.00
Bob	$200.00

How do you build a decentralized digital currency?

Without a central authority, different entities need to agree on transactions and balances.

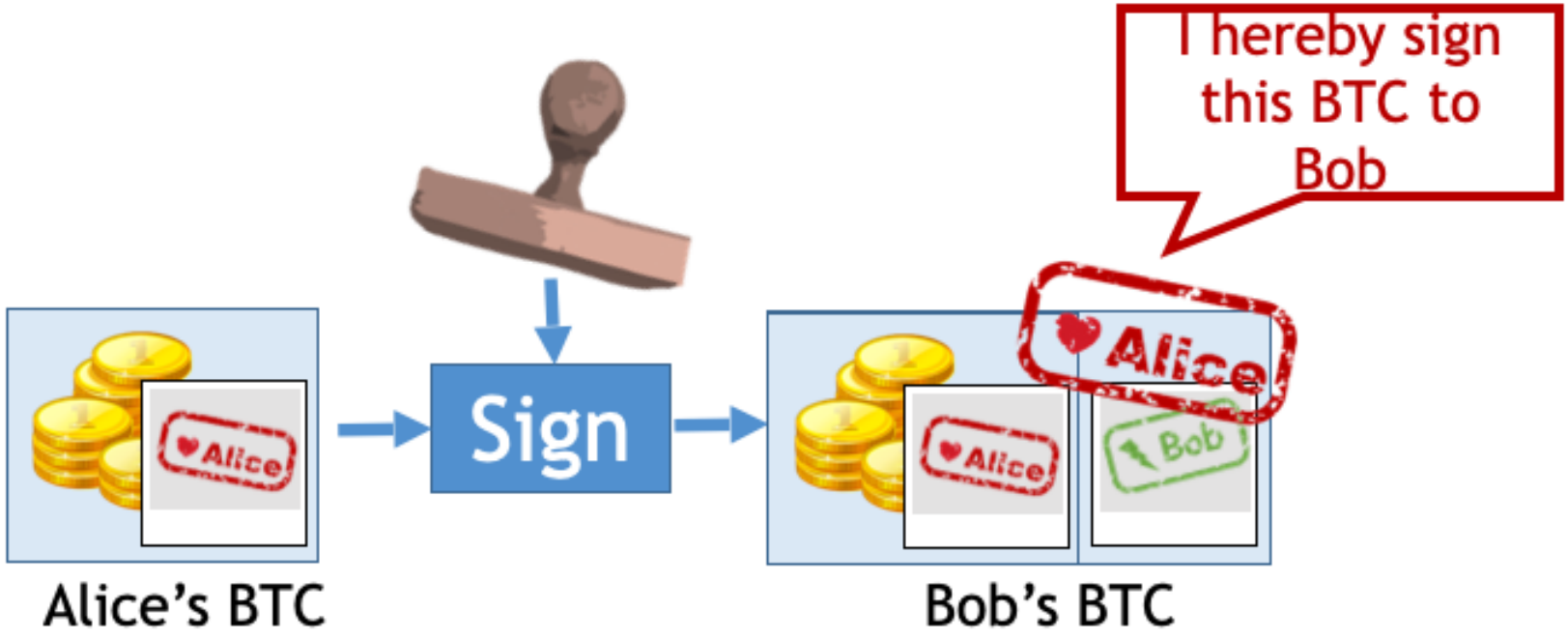
How do you keep someone from sending someone else's money to themselves?



Transactions: Use digital signatures to authenticate

A digital signature gives guarantees:

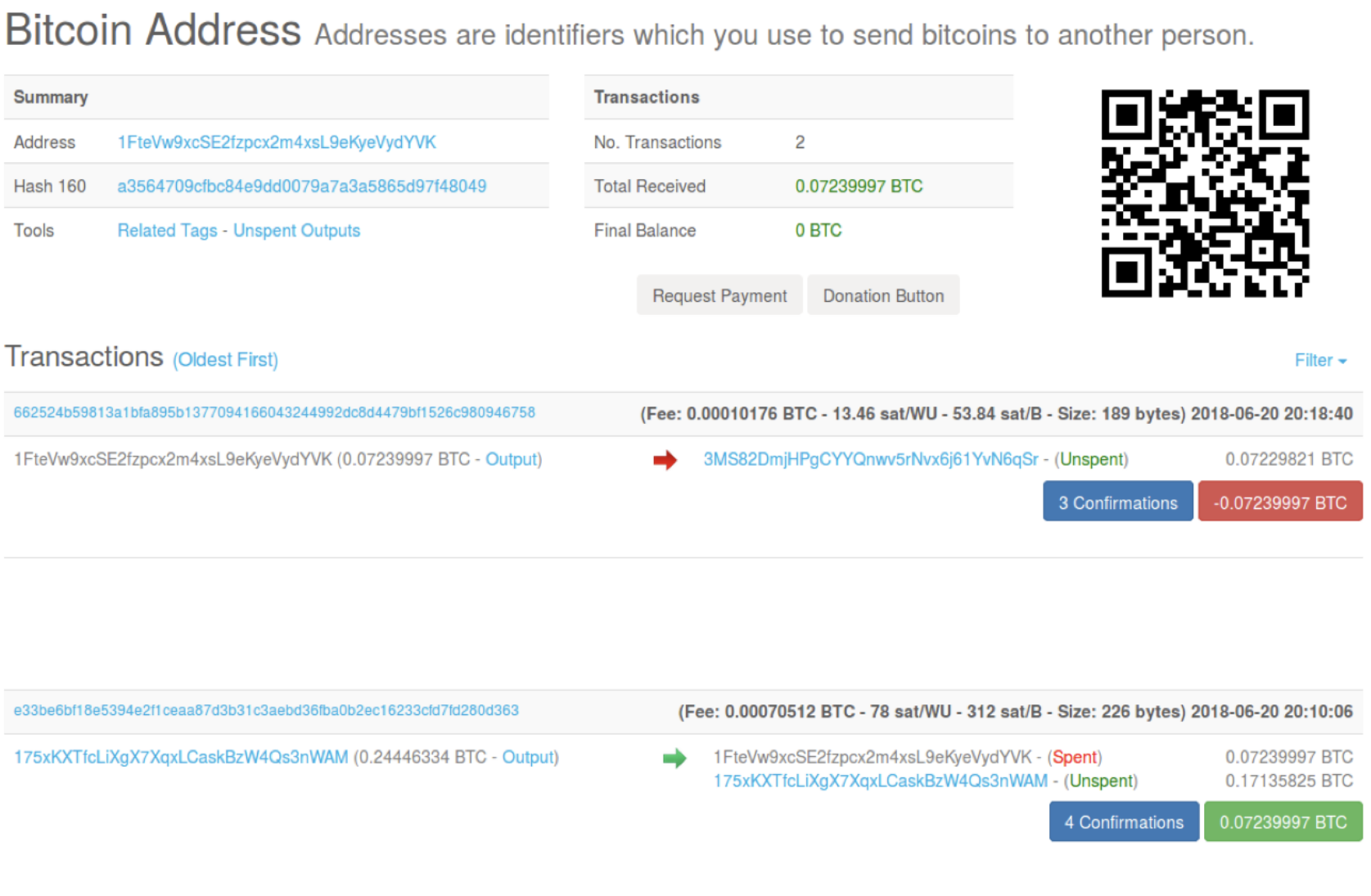
- The transaction has not been altered
- Only the entity with the private key can generate a valid signature
- Anyone can validate a signature with the public key



Pseudonymous identity: Derive from public key

Bitcoins are associated with an address.

The address is a hash of a public key.



Bitcoin Address Addresses are identifiers which you use to send bitcoins to another person.

Summary	
Address	1FteVw9xcSE2fzpcx2m4xsL9eKyeVydYVK
Hash 160	a3564709cfbc84e9dd0079a7a3a5865d97f48049
Tools	Related Tags - Unspent Outputs

Transactions	
No. Transactions	2
Total Received	0.07239997 BTC
Final Balance	0 BTC

Request Payment | Donation Button

Transactions (Oldest First) Filter

662524b59813a1bfa895b13770941660432449 92dc8d4479bf1526c980946758 (Fee: 0.00010176 BTC - 13.46 sat/WU - 53.84 sat/B - Size: 189 bytes) 2018-06-20 20:18:40

1FteVw9xcSE2fzpcx2m4xsL9eKyeVydYVK (0.07239997 BTC - Output) → 3MS82DmjHPgCYYQnwv5rNvx6j61YvN6qSr - (Unspent) 0.07229821 BTC

3 Confirmations | -0.07239997 BTC

e33be6bf18e5394e2f1ceaa87d3b31c3aebd36fba0b2ec16233cfd7fd280d363 (Fee: 0.00070512 BTC - 78 sat/WU - 312 sat/B - Size: 226 bytes) 2018-06-20 20:10:06

175xKXTfcLiXgX7XqxLCaskBzW4Qs3nWAM (0.24446334 BTC - Output) → 1FteVw9xcSE2fzpcx2m4xsL9eKyeVydYVK - (Spent) 0.07239997 BTC

175xKXTfcLiXgX7XqxLCaskBzW4Qs3nWAM - (Unspent) 0.17135825 BTC

4 Confirmations | 0.07239997 BTC

Problem: Double-spending

1. Alice has 1 token.
2. Alice sends 1 token to Bob and 1 token to Charlie.
3. Synchronization issue: each of Bob and Charlie is able to validate that Alice had a token to send, but doesn't know about the others' tokens.

A decentralized system needs some way to achieve consensus before transactions are accepted to prevent double-spending.

Bitcoin distributed ledger consensus

We would like to record all transactions in a public ledger.

Use some kind of consensus protocol to ensure everyone has same view of ledger.

Bitcoin uses a hash chain: every block of transactions includes cryptographic hash of previous block.

This means that once people agree on a block, they must agree on previous blocks.

Chaining blocks together with hash functions

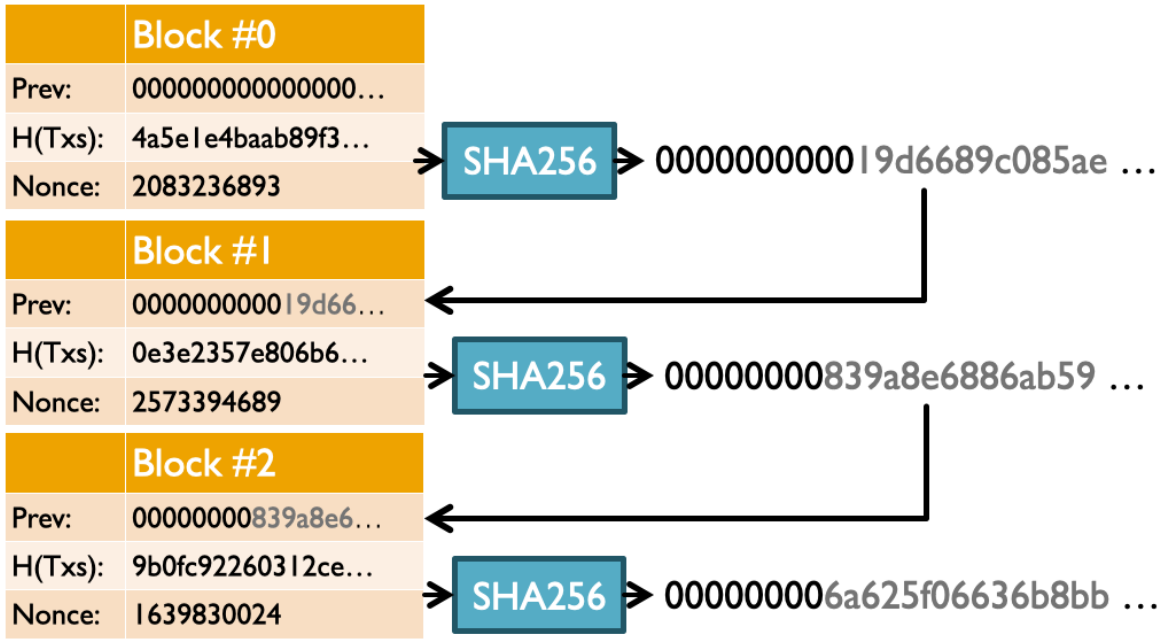
Network participants receive blocks from other nodes.

Which blockchain do you trust? The longest one.

How do you keep someone from making up a new super long blockchain?

Bitcoin uses “Hashcash” proof-of-work scheme to rate limit block creation.

Bitcoin consensus: Proof of work



- A block includes a set of transactions. "Miners" search for a nonce value that results in k leading 0s in the SHA256 hash of the block.
- We expect this to take 2^k hash function evaluations.
- The first miner to find such a value sends it to the network and work continues on the next block.
- The longest chain represents the most work: an attacker can't outcompete an honest majority.

Bitcoin Summary

Three main ideas:

- Public cryptographic keys for pseudonymous identifiers and transaction validation.
- Hash chain to ensure integrity of intermediate blocks.
- Proof-of-work-based distributed consensus scheme.

Bitcoin: Putting it all together

1. To generate an address, generate an ECDSA public key and hash it. This is your public address.
2. To receive money, another participant generates a transaction (actually a small executable script) sending bitcoin to this address and distributes it on the network.
3. Miners aggregate transactions from the network into a block and race to finish the proof of work first on that block.
4. The winning miner sends the block with proof of work on the network.
5. Once most nodes agree that the block with your transaction is part of the longest chain, you now have bitcoin.

“Smart contracts”: Ethereum

Idea: Include an expressive scripting language and have all nodes execute these scripts.

Pro: Replace governments, lawyers, accountants, and regulators with executable code.

“Smart contracts”: Ethereum

Idea: Include an expressive scripting language and have all nodes execute these scripts.

Pro: Replace governments, lawyers, accountants, and regulators with executable code.

Con: You have seen how good we are at writing secure code.

- An attacker stole $50 million of Ether from the DAO (decentralized autonomous organization) by exploiting a vulnerability in the DAO’s smart contract code.

- The Ethereum community decided to fork the blockchain to roll back the transaction.

“NFTs”: Non-Fungible Tokens

Idea: Post metadata about things to a public blockchain.

Pro: Supply-chain management? Digital rights management?

Con: Actual asset stored elsewhere.

- Idea of “cryptographic tokens” seems to have become commingled with the idea of automatic mass-produced digital art.
- Protocol flaw in most implementations: Only thing on blockchain is a URL and contents aren’t even validated.

Bitcoin and cryptocurrency criticisms

- Proof of work mining is environmentally wasteful. Bitcoin is now consuming more electricity than Argentina.

Bitcoin and cryptocurrency criticisms

- Proof of work mining is environmentally wasteful. Bitcoin is now consuming more electricity than Argentina.
  - Can replace proof of work with “proof of stake”: consensus based on coin ownership.

Bitcoin and cryptocurrency criticisms

- Proof of work mining is environmentally wasteful. Bitcoin is now consuming more electricity than Argentina.
  - Can replace proof of work with “proof of stake”: consensus based on coin ownership.

- Bitcoin is not anonymous. Transactions are all public, and addresses are only pseudonymous and can be linked to real-world identities when used.

Bitcoin and cryptocurrency criticisms

- Proof of work mining is environmentally wasteful. Bitcoin is now consuming more electricity than Argentina.
  - Can replace proof of work with “proof of stake”: consensus based on coin ownership.

- Bitcoin is not anonymous. Transactions are all public, and addresses are only pseudonymous and can be linked to real-world identities when used.
  - Zcash uses fancy crypto (zk-SNARKs) to validate transactions without publishing transactions publicly to network.

Bitcoin and cryptocurrency criticisms

- Proof of work mining is environmentally wasteful. Bitcoin is now consuming more electricity than Argentina.
  - Can replace proof of work with “proof of stake”: consensus based on coin ownership.

- Bitcoin is not anonymous. Transactions are all public, and addresses are only pseudonymous and can be linked to real-world identities when used.
  - Zcash uses fancy crypto (zk-SNARKs) to validate transactions without publishing transactions publicly to network.

- Bitcoin does not scale: The transaction rate will never be high enough to be a real payment network.

Bitcoin and cryptocurrency criticisms

- Proof of work mining is environmentally wasteful. Bitcoin is now consuming more electricity than Argentina.
  - Can replace proof of work with “proof of stake”: consensus based on coin ownership.

- Bitcoin is not anonymous. Transactions are all public, and addresses are only pseudonymous and can be linked to real-world identities when used.
  - Zcash uses fancy crypto (zk-SNARKs) to validate transactions without publishing transactions publicly to network.

- Bitcoin does not scale: The transaction rate will never be high enough to be a real payment network.
  - Various proposals (Lighting Network). Bitcoin will never be a payment network.

Bitcoin and cryptocurrency criticisms

- The cryptocurrency space is full of charlatans, ponzi schemes, and tulip mania.

Bitcoin and cryptocurrency criticisms

- The cryptocurrency space is full of charlatans, ponzi schemes, and tulip mania.

- A public blockchain is not what most people want for real-world applications.

Bitcoin and cryptocurrency criticisms

- The cryptocurrency space is full of charlatans, ponzi schemes, and tulip mania.

- A public blockchain is not what most people want for real-world applications.
  - A blockchain is just an append-only linked list.
  - Many proposed applications (healthcare? supply chain management?) better suited to a trusted third party with a database, an API, and maybe some digital signatures.
  - There are better distributed consensus algorithms for closed groups. Keyword: “Permissioned blockchain” which seems like it might soon come to refer to any multiparty computation.

Bitcoin and cryptocurrency criticisms

- The cryptocurrency space is full of charlatans, ponzi schemes, and tulip mania.

- A public blockchain is not what most people want for real-world applications.
  - A blockchain is just an append-only linked list.
  - Many proposed applications (healthcare? supply chain management?) better suited to a trusted third party with a database, an API, and maybe some digital signatures.
  - There are better distributed consensus algorithms for closed groups. Keyword: “Permissioned blockchain” which seems like it might soon come to refer to any multiparty computation.

- Irreversible transactions are not what consumers actually want in a payment system.
  - Cryptocurrencies are “speedrunning 500 years of bad economics”–Nick Weaver

Cryptocurrencies: The positives

- Renewed excitement in CS research like Byzantine fault tolerance, consensus protocols, programming language design for smart contracts, exotic cryptographic primitives...
- In a gold rush, the people who get rich are not the miners following the crowds, but the people selling equipment to the miners.

Have a great end of quarter!

Good luck on the final!