

Lecture 14: Waste!

Identity;
Proofs of Work;
Environmental Impacts

CMSC 25910

Spring 2023

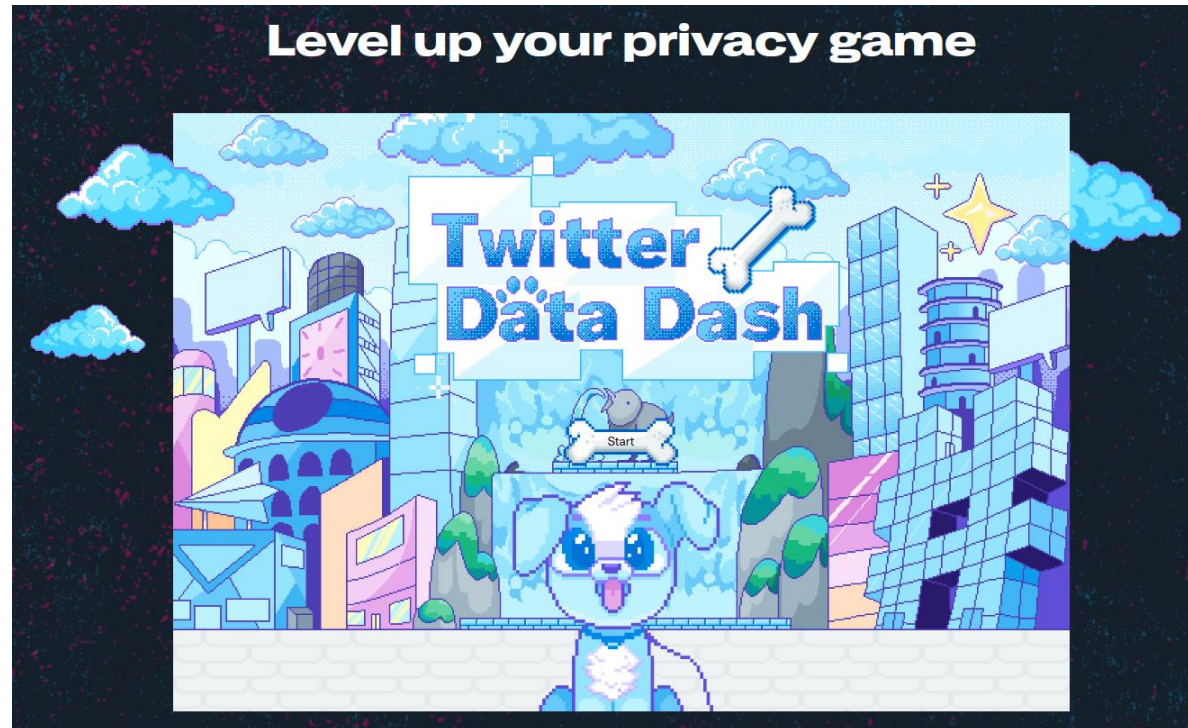
The University of Chicago



Gamification of Privacy Policies: A Potential Waste?

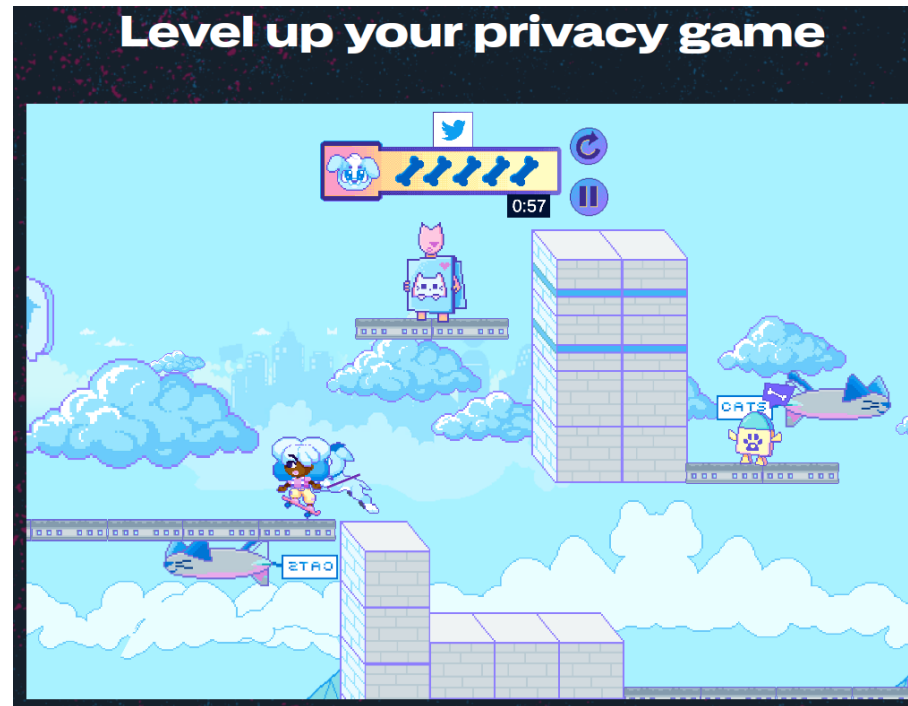
Twitter Data Dash

- Twitter released an online game to discuss some of its privacy concepts to users
 - <https://twitterdatadash.com/>



Twitter Data Dash

- Twitter released an online game to discuss some of its privacy concepts to users
 - <https://twitterdatadash.com/>



Proving You Are Human

CAPTCHA

- **C**ompletely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part (Luis von Ahn et al.)

Match the characters in the picture [Help](#)

To continue, type the characters you see in the picture. [Why?](#)



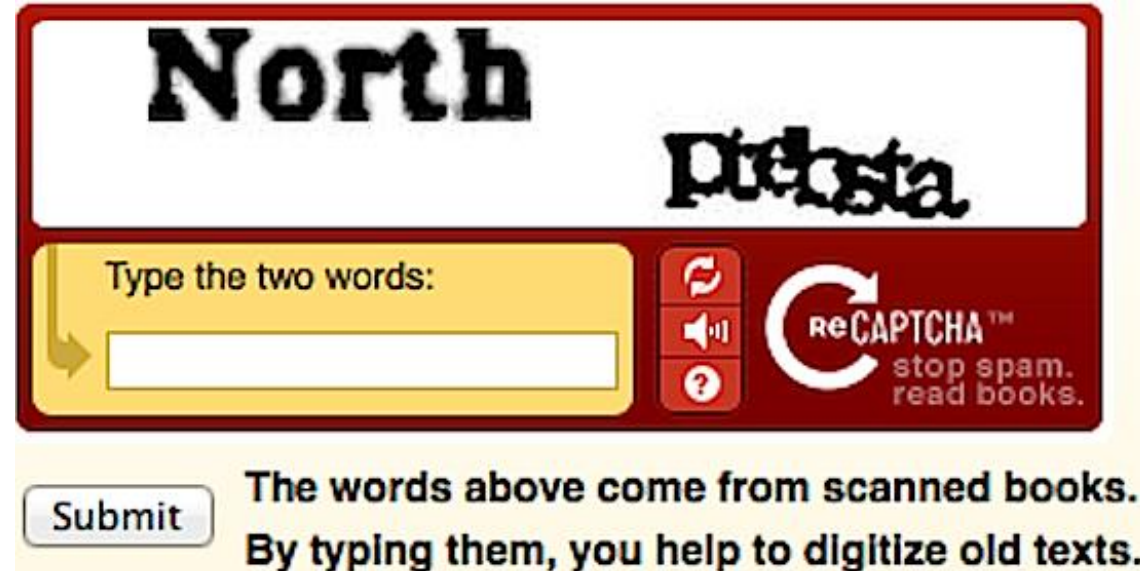
The picture contains 8 characters.

Characters:

Continue

reCAPTCHA

- Book digitization
 - NY Times, Google Books
- “One of the wavy words quite likely came from a digitized image from an old, musty text...the scanning programs made a lot of mistakes.”

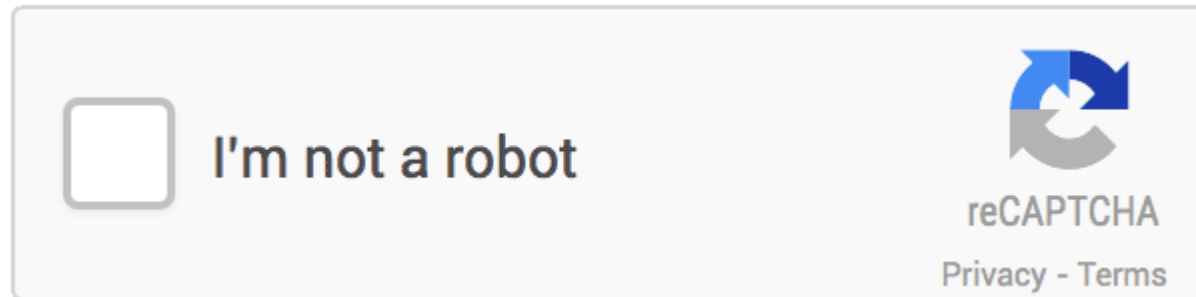


reCAPTCHA

- “ReCaptcha flags as “suspicious” any word that is deciphered differently by the two programs or that does not appear in an English dictionary... Then each suspicious word is turned into a Captcha. It is crucial to understand that the Captcha is a distorted version of the word as printed in the original photographic image. It is not made from the O.C.R.’s imagined translation, which is often unintelligible. The unknown word is then paired with a second Captcha word whose correct translation is already known. This is the “control.”

reCAPTCHA

- Google Maps (and presumably self-driving cars):
- “Checking a box”



- Are CAPTCHAs accessible?



Duolingo

- Original (and perhaps future?) idea: use power of humans learning a language to create translations



<https://www.npr.org/2020/05/22/860884062/recaptcha-and-duolingo-luis-von-ahn>

<https://digital.hbs.edu/platform-digit/submission/duolingo-using-the-wisdom-of-crowds-to-translate-language/>

See also <https://www.npr.org/sections/money/2019/04/24/716854013/episode-908-i-am-not-a-robot>

Identity: Preventing Multiple Accounts from One Person

Identity (in systems)



Create your Google Account

First name

Last name

Username

@gmail.com

You can use letters, numbers & periods

[Use my current email address instead](#)

Password

Confirm

Use 8 or more characters with a mix of letters, numbers & symbols

☐ Show password

[Sign in instead](#)

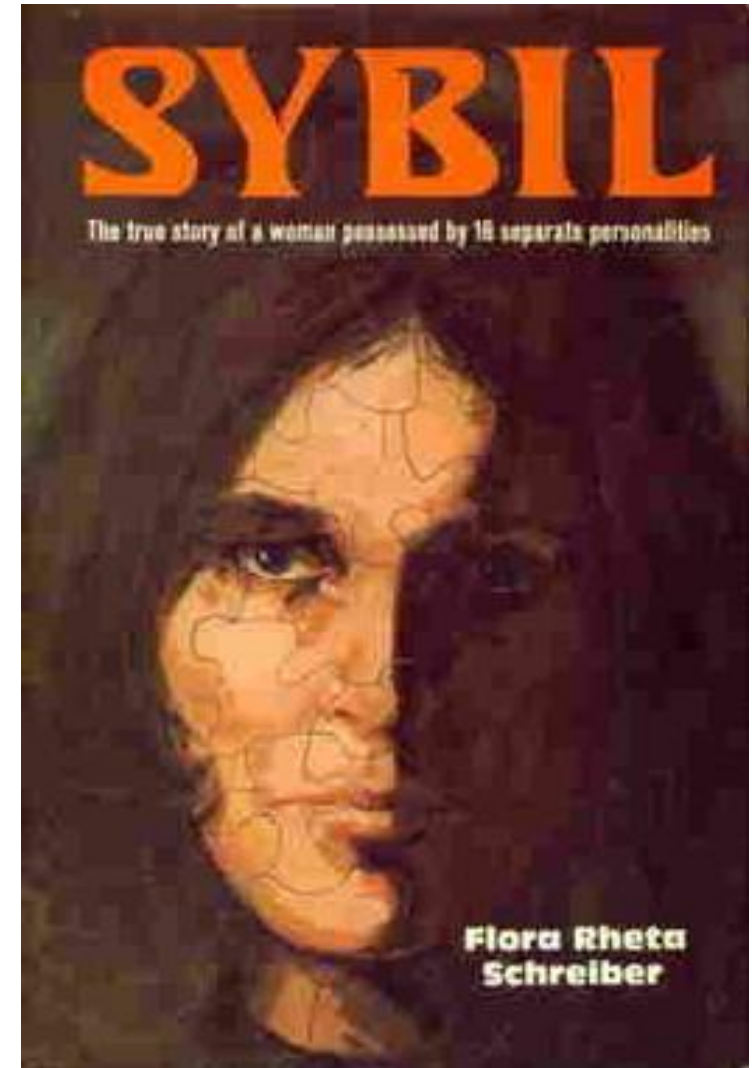
Next



One account. All of Google working for you.

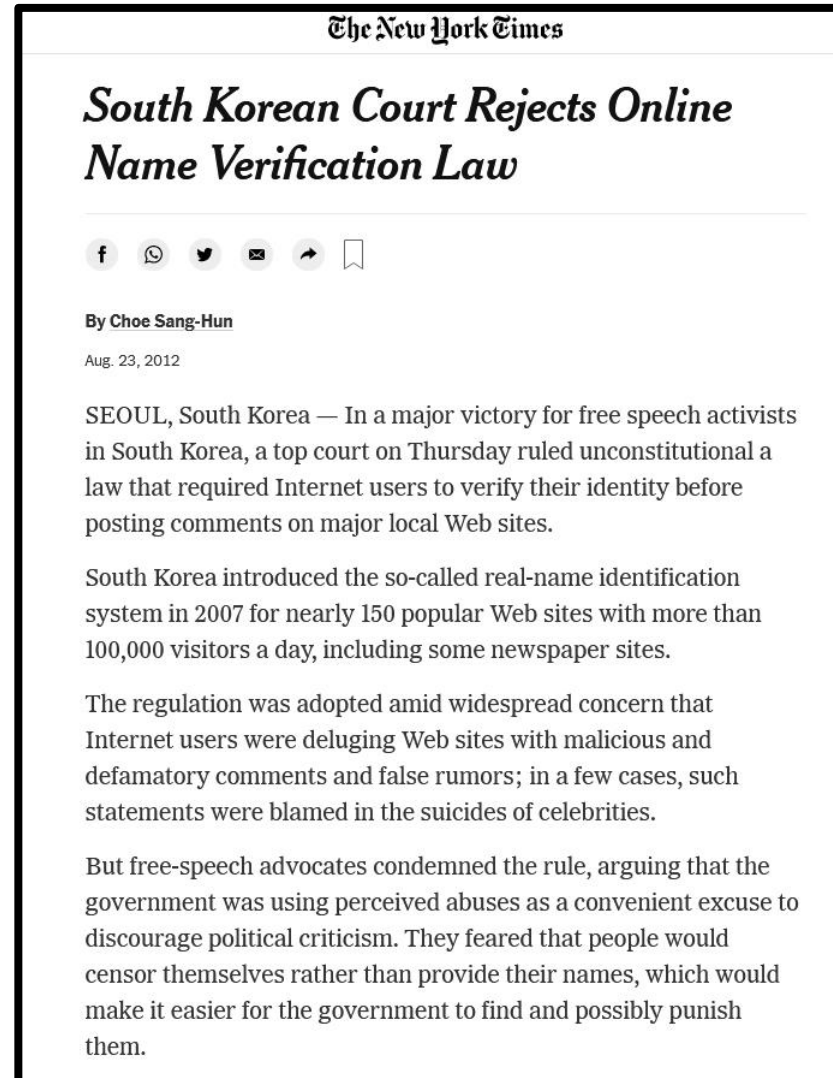
Sybil Attacks

- One individual creates many pseudonymous identities
- For instance, one individual creates many accounts
- Namesake: Sybil (pseudonym of a person who had a dissociative identity disorder)
- Also called: sock puppets (false identities)
- Why is this a problem for computer systems?



Tie Accounts to Real Identities

- IP address
- Mailing address
- National identity card
- Telephone number
 - What precise protocol?



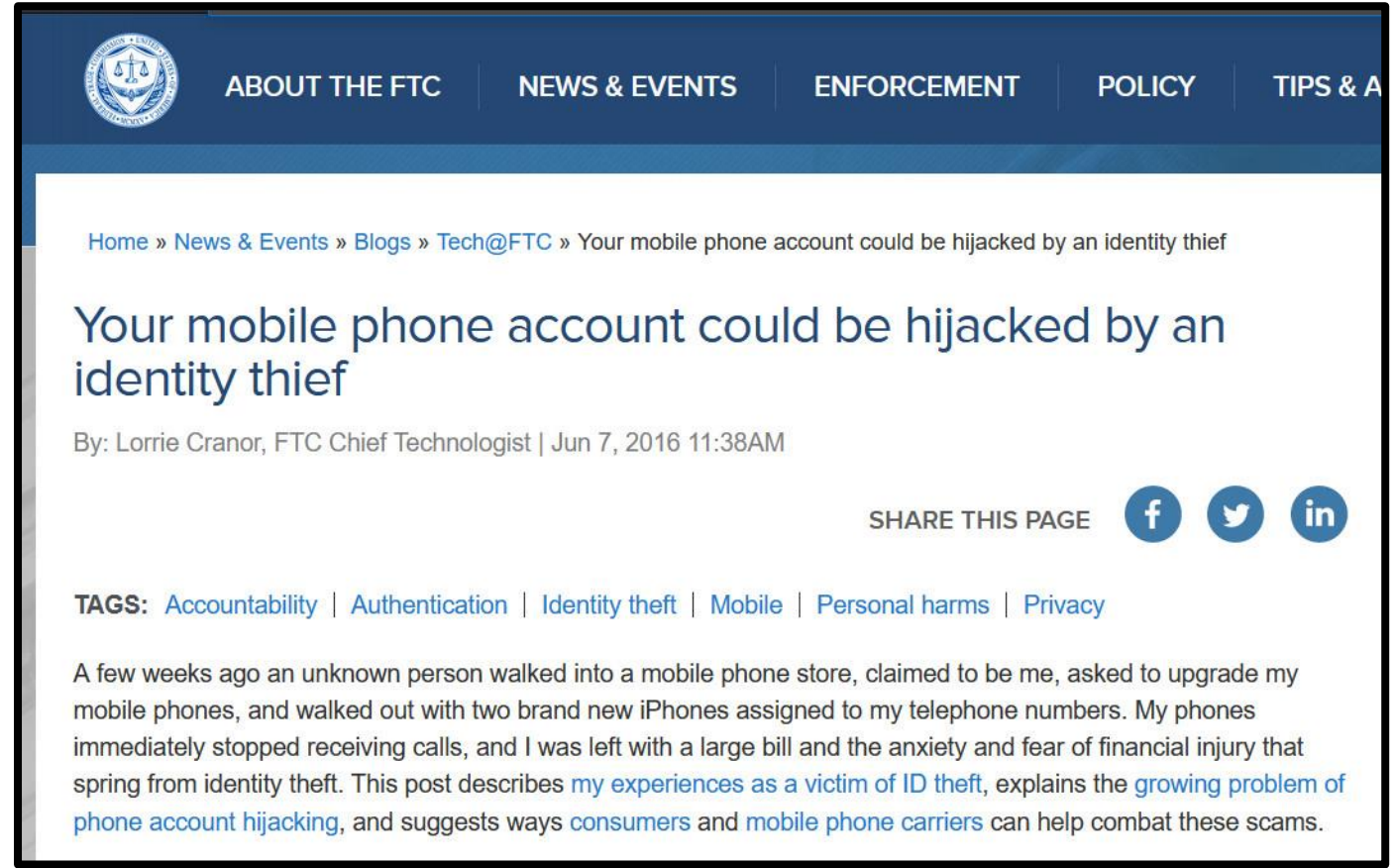
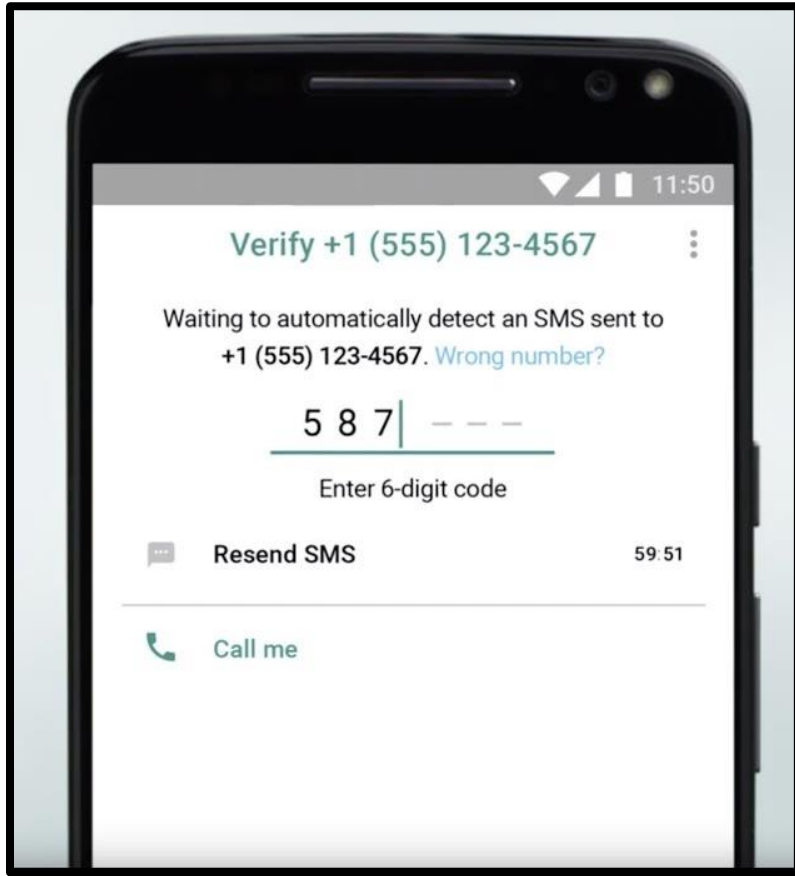
Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)

Article 24: Network operators handling network access and domain name registration services for users, handling stationary or mobile phone network access, or providing users with information publication or instant messaging services, shall require users to provide real identity information when signing agreements with users or confirming the provision of services. Where users do not provide real identity information, network operators must not provide them with relevant services.

National ID Cards

- Some national ID cards include a microprocessor
 - Online authentication becomes possible

Vulnerabilities of SMS Codes



<https://www.youtube.com/watch?v=AWemFbRf95g>

<https://www.ftc.gov/news-events/blogs/techftc/2016/06/your-mobile-phone-account-could-be-hijacked-identity-thief>

Proof of Work

Prerequisite: Hashing

- One-way function
- Similar inputs result in very different outputs
- md5("blase") = 12B872ADB2588C668D706D847FC1DA7E
- md5("blasé") = 29AFE9B75D98D3C4ECFCB34FDFC422A2

Need for Proofs of Work

- Example (problematic) system: You upload some data to a computer system and it trains a neural network with that data
- Example (problematic) system: You upload the product of two large prime numbers to a system and it factorizes it
- What's the problem?

Need for Proofs of Work

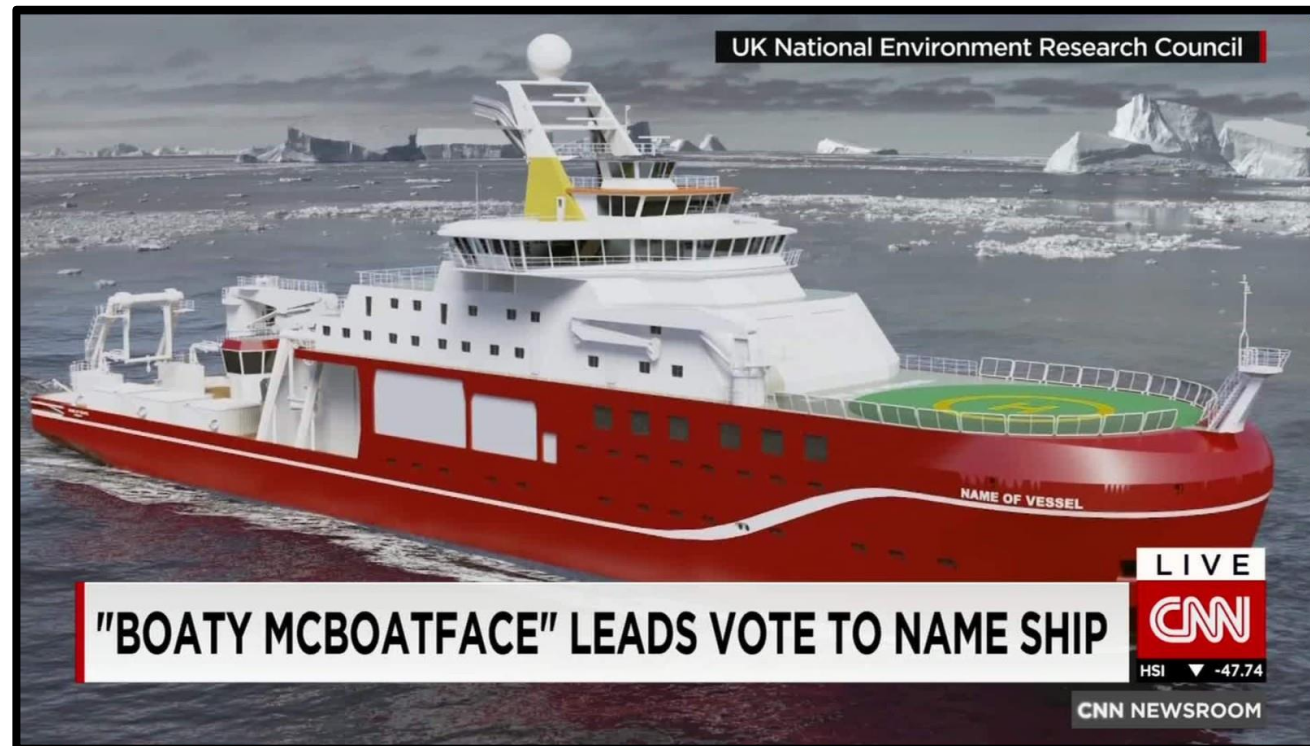
- Example (problematic) system: You upload some data to a computer system and it trains a neural network with that data
- Example (problematic) system: You upload the product of two large prime numbers to a system and it factorizes it
- What's the problem? **Denial of Service (DoS) attacks**

Need for Proofs of Work

- Example (problematic) system: Everyone can vote on who wins the CS 25910 Memelord award
- What's the problem?

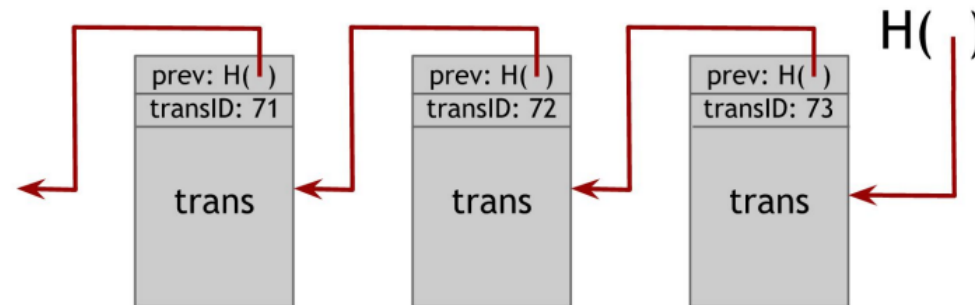
Need for Proofs of Work

- Example (problematic) system: Everyone can vote on who wins the CS 25910 Memelord award
- What's the problem? **Does one person = one vote?**



Blockchain

- Blocks of transactions are linked together into a chain
- Hashes connect the blocks
- *Emergent consensus*: The hash chain representing the most cumulative work is considered valid
- Blocks (in Bitcoin) are mined every 10 minutes



Blockchain

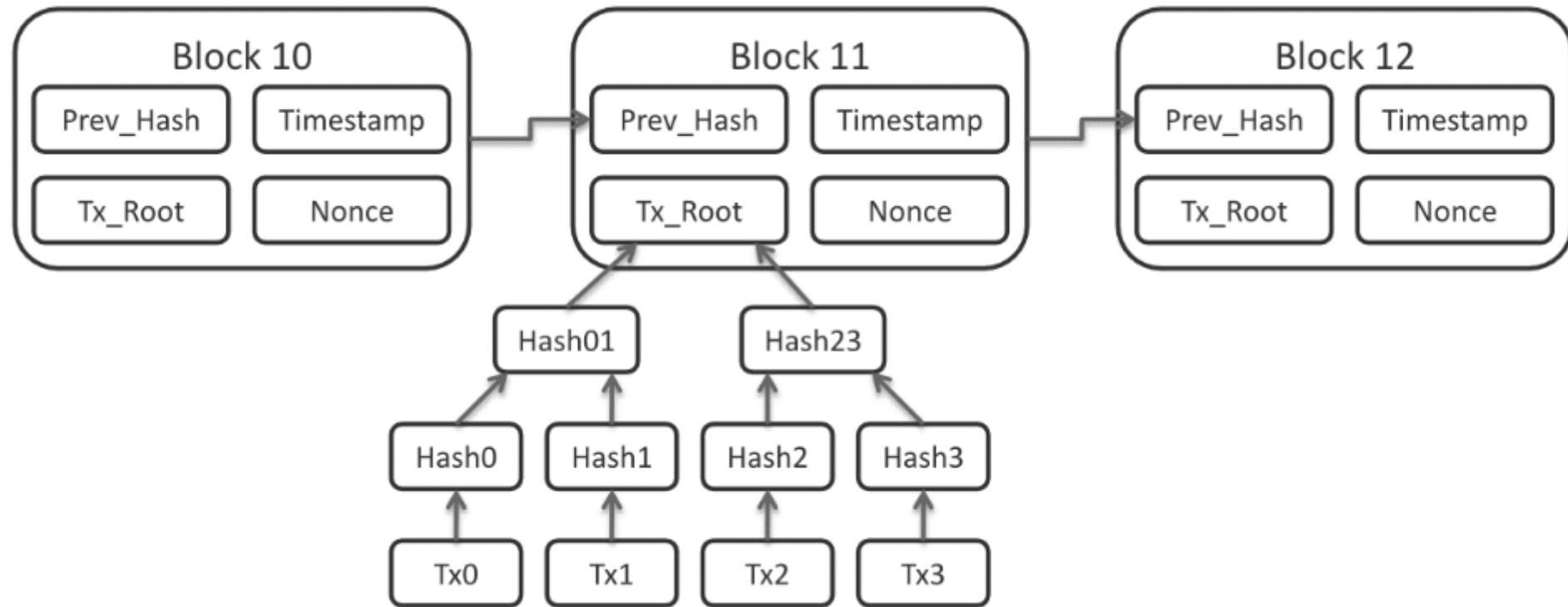


Image taken from <https://coincentral.com/what-is-a-nonce-proof-of-work>

Blockchain as Used in Bitcoin

- Transactions include transfers of the cryptocurrency
- Sign transactions with a secret (private) key
- Broadcast transactions throughout the network
- Transactions are assembled into the ledger

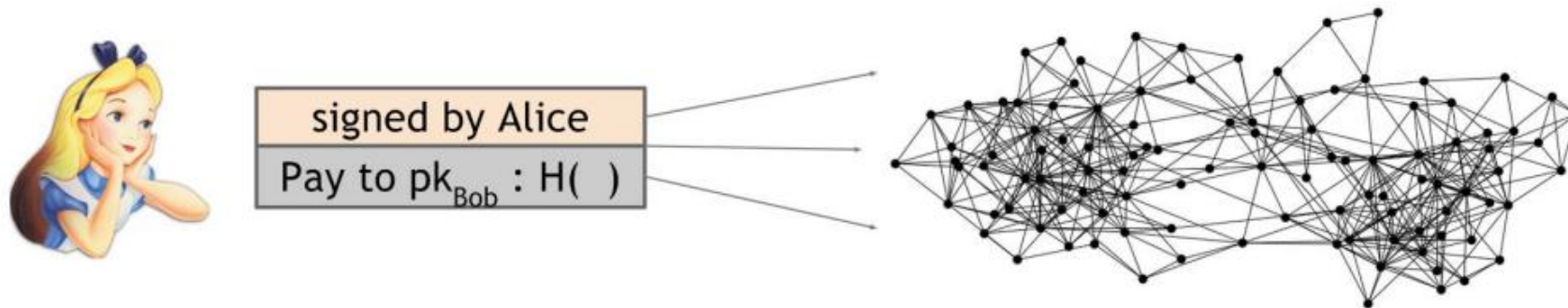


Figure 2.1 Broadcasting a transaction In order to pay Bob, Alice broadcasts the transaction to the entire Bitcoin peer-to-peer network.

Blockchain as a Distributed Ledger

- Conceptual (but impractical) idea: ledger of accounts

Create 25 coins and credit to Alice	ASSERTED BY MINERS
Transfer 17 coins from Alice to Bob	SIGNED(Alice)
Transfer 8 coins from Bob to Carol	SIGNED(Bob)
Transfer 5 coins from Carol to Alice	SIGNED(Carol)
Transfer 15 coins from Alice to David	SIGNED(Alice)

Figure 3.1 an account-based ledger

Blockchain as a Distributed Ledger

- More practical (and what is actually done): ledger of transaction; future transactions connected to a previous one

1	Inputs: $\emptyset$ Outputs: 25.0→Alice	
2	Inputs: 1[0] Outputs: 17.0→Bob, 8.0→Alice	SIGNED(Alice)
3	Inputs: 2[0] Outputs: 8.0→Carol, 9.0→Bob	SIGNED(Bob)
4	Inputs: 2[1] Outputs: 6.0→David, 2.0→Alice	SIGNED(Alice)

Figure 3.2 a transaction-based ledger, which is very close to Bitcoin

Distributed Consensus in Bitcoin

Bitcoin consensus algorithm (simplified)

This algorithm is simplified in that it assumes the ability to select a random node in a manner that is not vulnerable to Sybil attacks.

1. New transactions are broadcast to all nodes
2. Each node collects new transactions into a block
3. In each round a random node gets to broadcast its block
4. Other nodes accept the block only if all transactions in it are valid (unspent, valid signatures)
5. Nodes express their acceptance of the block by including its hash in the next block they create

Simplification!



Distributed Consensus in Bitcoin

- We are going to be hashing blocks, which include:
 - A pointer to the previous block and a hash of its contents (*prev_hash*)
 - The transactions captured in this block of the ledger (*tx...*)
 - A nonce, which you'll guess (over and over and over)
- Try to find a nonce that solves the following:

$$H(\textit{nonce} || \textit{prev_hash} || \textit{tx} || \textit{tx} || \dots || \textit{tx}) < \textit{target}$$

- Note that you include a transaction paying yourself, so your block (and thus the relevant nonce) is specific to you

Iterating on a Nonce

Example 8-10. SHA256 output of a script for generating many hashes by iterating on a nonce

```
$ python hash_example.py
```

```
I am Satoshi Nakamoto0 => a80a81401765c8eddee25df36728d732...
I am Satoshi Nakamoto1 => f7bc9a6304a4647bb41241a677b5345f...
I am Satoshi Nakamoto2 => ea758a8134b115298a1583ffb80ae629...
I am Satoshi Nakamoto3 => bfa9779618ff072c903d773de30c99bd...
I am Satoshi Nakamoto4 => bce8564de9a83c18c31944a66bde992f...
I am Satoshi Nakamoto5 => eb362c3cf3479be0a97a20163589038e...
I am Satoshi Nakamoto6 => 4a2fd48e3be420d0d28e202360cfbaba...
I am Satoshi Nakamoto7 => 790b5a1349a5f2b909bf74d0d166b17a...
I am Satoshi Nakamoto8 => 702c45e5b15aa54b625d68dd947f1597...
I am Satoshi Nakamoto9 => 7007cf7dd40f5e933cd89fff5b791ff0...
I am Satoshi Nakamoto10 => c2f38c81992f4614206a21537bd634a...
I am Satoshi Nakamoto11 => 7045da6ed8a914690f087690e1e8d66...
I am Satoshi Nakamoto12 => 60f01db30c1a0d4cbce2b4b22e88b9b...
I am Satoshi Nakamoto13 => 0ebc56d59a34f5082aaef3d66b37a66...
I am Satoshi Nakamoto14 => 27ead1ca85da66981fd9da01a8c6816...
I am Satoshi Nakamoto15 => 394809fb809c5f83ce97ab554a2812c...
I am Satoshi Nakamoto16 => 8fa4992219df33f50834465d3047429...
I am Satoshi Nakamoto17 => dca9b8b4f8d8e1521fa4eaa46f4f0cd...
I am Satoshi Nakamoto18 => 9989a401b2a3a318b01e9ca9a22b0f3...
I am Satoshi Nakamoto19 => cda56022ecb5b67b2bc93a2d764e75f...
```

Clarifications About the Overall Process

- Validate blocks (e.g., no invalid transactions)
- Select the chain with the most proof of work

Proof of Stake

Proof of Stake (PoS)

- An alternative approach to proof of work
 - See, e.g., <https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/>
- Prospective validator offers some of their own coins in the system to be permitted to validate a block
 - e.g., Ethereum requires that 32 ETH be staked
 - Multiple validators have to agree on the block for it to be accepted
 - Lose your staked coins if you attest to a malicious block
- Fear: what if some entity controls 51% of the cryptocurrency
- Typically selected randomly from among staked users

Environmental Impacts

Electronic Waste

Bloomberg CityLab

The Toxic Effects of Electronic Waste in Accra, Ghana

Sorting through used electronics is a livelihood for many in the Agbogbloshie area, but toxic e-waste poses serious health risks.

Peter Yeung
May 29, 2019, 2:20 PM CDT



Abraham Daouda came to Accra from Niger two years ago. He collects used water sachets and scrap metal, and hopes to buy his own taxi one day. But when it rains at Agbogbloshie, he finds it difficult to breathe. Peter Yeung

Heavy, acidic gusts of smoke billow across the Agbogbloshie dump, a wasteland dotted with burning mounds of trash in Ghana's capital, Accra.

Up to 10,000 workers wade through tons of discarded goods as part of an enormous, informal recycling process, in what has become one of the world's largest destinations for used electronic goods.

SHARE THIS ARTICLE
f Share
T Tweet
in Post
E Email

CNN World Africa Americas Asia Australia China Europe India Middle East United Kingdom LIVE TV Edition

MARKETPLACE
AFRICA

The rising e-waste crisis is being reckoned with in Rwanda, one gadget at a time

By Daniel Renjifo, CNN
Updated 1:21 PM ET, Fri February 26, 2021



< 04:48 04:48 04:57 03:58 05:31 >

How Rwanda is leading e-waste recycling efforts in Africa

How Flutterwave's unicorn status could sprout more innovation in African fintech

How international demand for Nigerian cotton is suiting well for small farmers

How big data is fostering expansion for this South African logistics enterprise

How ghost are coming South Africa

(CNN) — For Eric Nshimiyanain, who owns two small electronic repair shops in Kigali, Rwanda, the startup chime of an old Windows laptop is the sound of a business opportunity.

He refurbishes broken PCs, laptops, phones and secondhand gadgets classified as electronic waste, or "e-waste" that would otherwise end up as trash in Nduba, Rwanda's only open-air dump in the outskirts of the capital.

<https://www.bloomberg.com/news/articles/2019-05-29/the-rich-world-s-electronic-waste-dumped-in-ghana>

<https://www.smithsonianmag.com/science-nature/burning-truth-behind-e-waste-dump-africa-180957597/>

<https://www.cnn.com/2021/02/26/africa/marketplace-africa-ewaste-electronics-recycle-rwanda-spc-intl/index.html>

Diurnal Patterns of Energy Usage

COMMUNICATIONS
OF THE
ACM

HOME | CURRENT ISSUE | NEWS | BLOGS | OPINION | RESEARCH | PRACTICE

[Home](#) / [Magazine Archive](#) / [February 2021 \(Vol. 64, No. 2\)](#) / [Driving the Cloud to True Zero Carbon](#) / [Full Text](#)

EDITOR'S LETTER

Driving the Cloud to True Zero Carbon

By Andrew A. Chien
Communications of the ACM, February 2021, Vol. 64 No. 2, Page 5
10.1145/3445037
[Comments](#)

VIEW AS:     

SHARE:       



The right vision is to operate the cloud with zero-carbon emission from power (scope 2). Not just offsetting through renewable energy purchases. Not just 24x7 matching. True zero carbon in electric power consumed, and with no increase as the cloud continues to grow. That's the right vision for our proud computing technology community to lead the fight against climate change, and to see increasing use of computing as a positive force to slow climate change.^{a,b}

Why must we act? The power grid is decarbonizing, but progress is slow. Aggressive states (for example, California and New York) have zero-carbon goals 20 or more years in the future, 2045 and 2040. Nationally, the U.S. produced 19% of its electric power from renewable resources (2020), and with "datacenter alley" reporting 12% renewables^c (Northern Virginia). This trails the world's 26% renewables today, and U.S.