Lecture 14:
Wasted Work

Identity;
Proofs of Work;
Environmental Impacts

CMSC 25910

Spring 2022

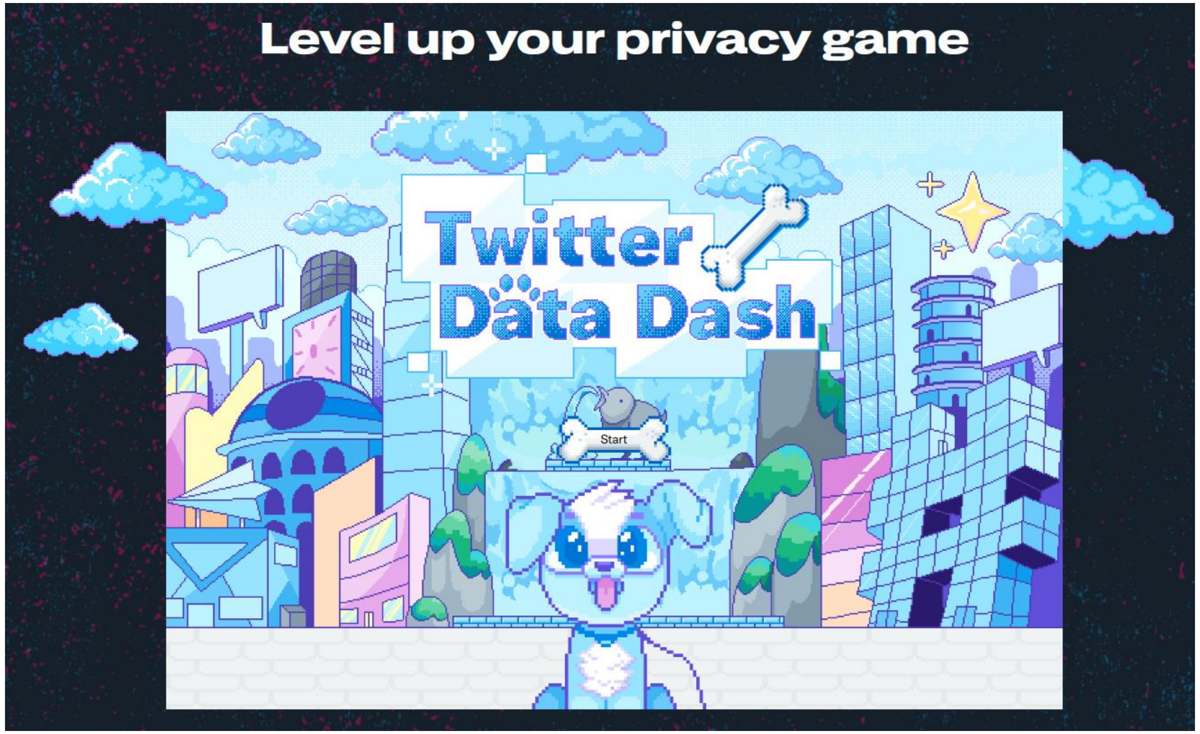
The University of Chicago

THE UNIVERSITY OF CHICAGO

Gamification of Privacy Policies: A Potential Waste?

Twitter Data Dash

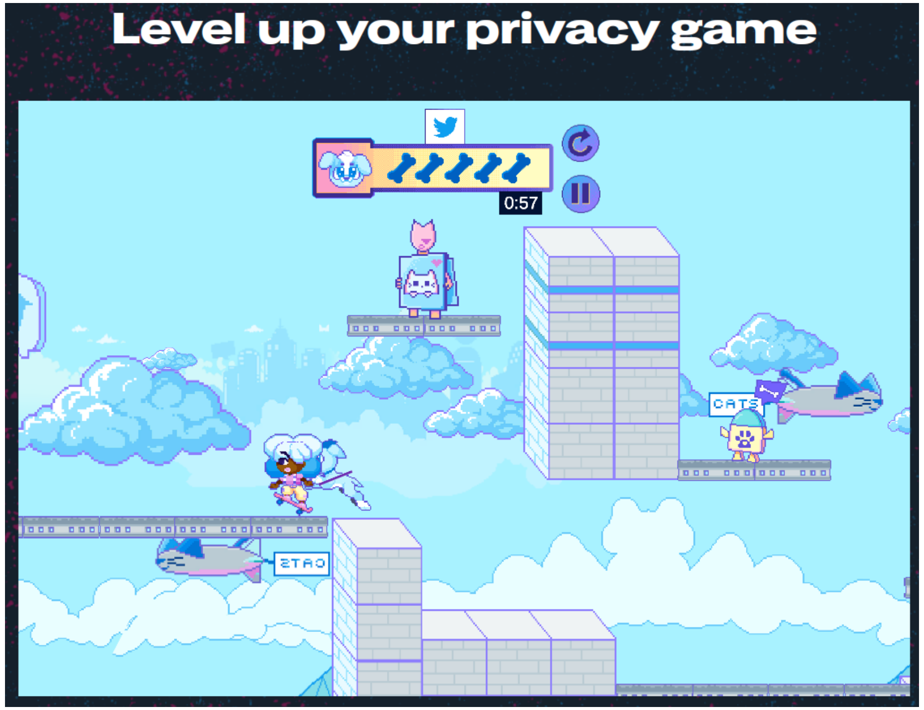
- Twitter released (yesterday) an online game to discuss some of its privacy concepts to users
  - https://twitterdatadash.com/



https://gizmodo.com/twitter-privacy-policy-video-game-data-dash-1848912387

Twitter Data Dash

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

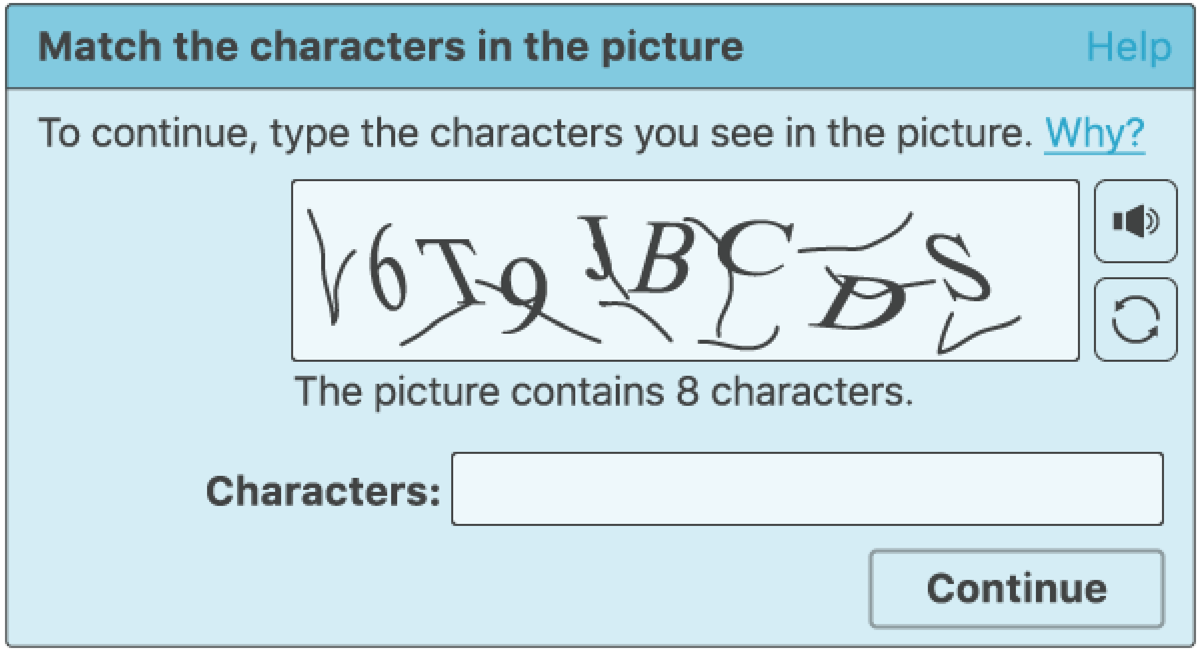


https://gizmodo.com/twitter-privacy-policy-video-game-data-dash-1848912387

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.)



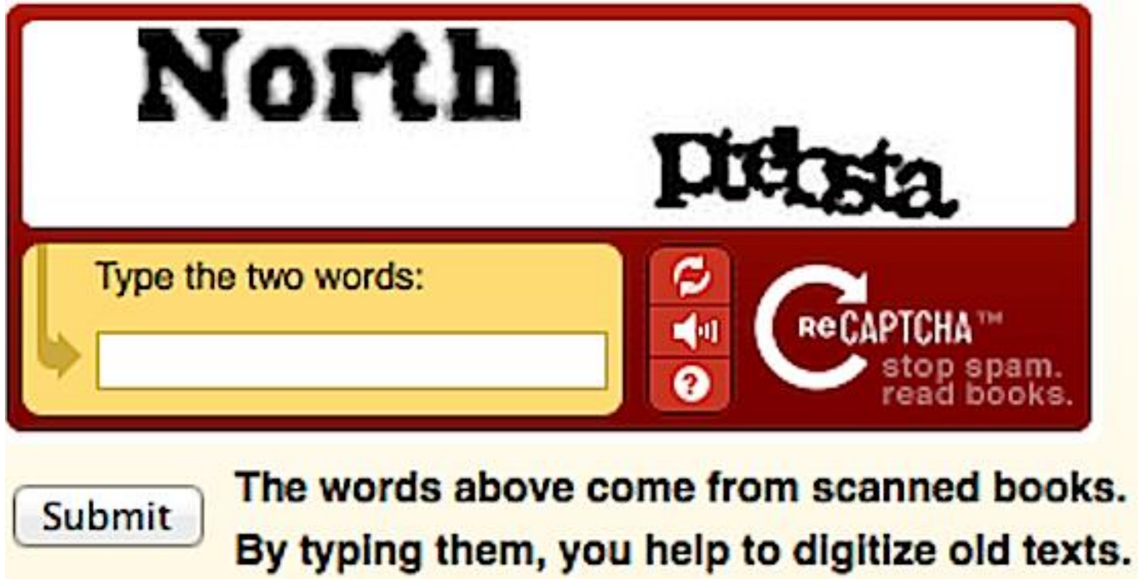
Match the characters in the picture

To continue, type the characters you see in the picture. Why?

The picture contains 8 characters.

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.”



The words above come from scanned books.
By typing them, you help to digitize old texts.

https://www.nytimes.com/2011/03/29/science/29recaptcha.html and https://freakspot.net/en/como-explota-Google-con-CAPTCHAs/

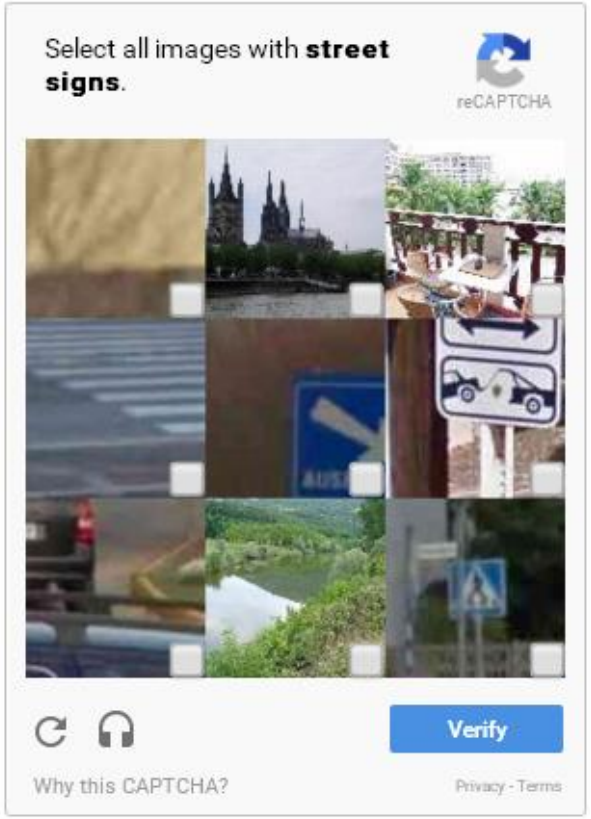
reCAPTCHA

- “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.”

https://www.nytimes.com/2011/03/29/science/29recaptcha.html

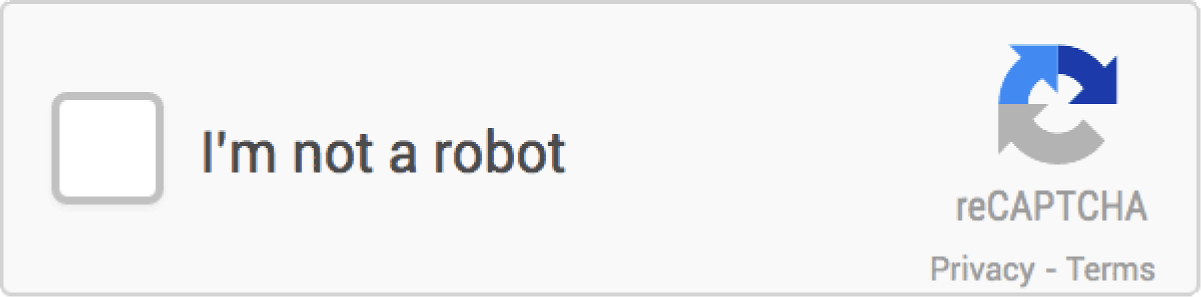
reCAPTCHA

- Google Maps (and presumably self-driving cars):



Select all images with **street signs**.

- “Checking a box”



- Are CAPTCHAs accessible?

Images taken from https://freakspot.net/en/como-explota-Google-con-CAPTCHAs/
See also https://www.npr.org/sections/money/2019/04/24/716854013/episode-908-i-am-not-a-robot

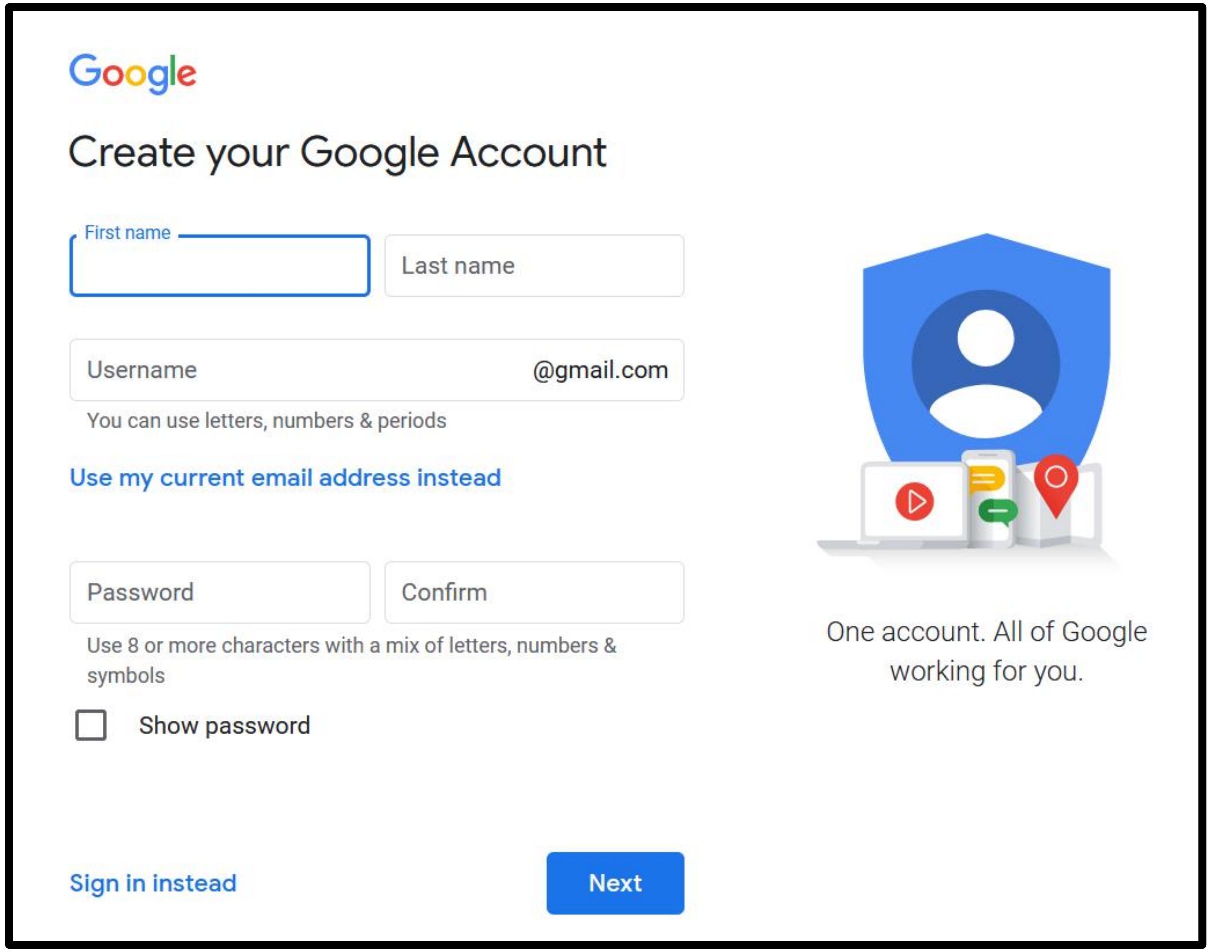
Duolingo

- 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)



Google

Create your Google Account

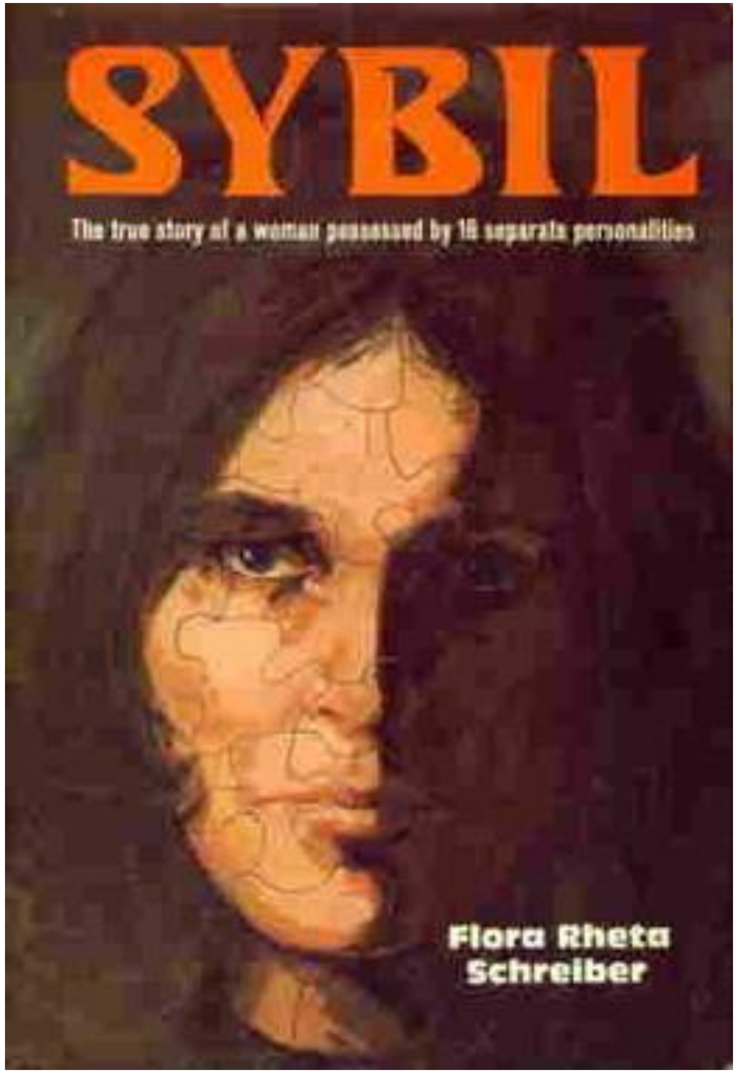
You can use letters, numbers & periods

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

One account. All of Google working for you.

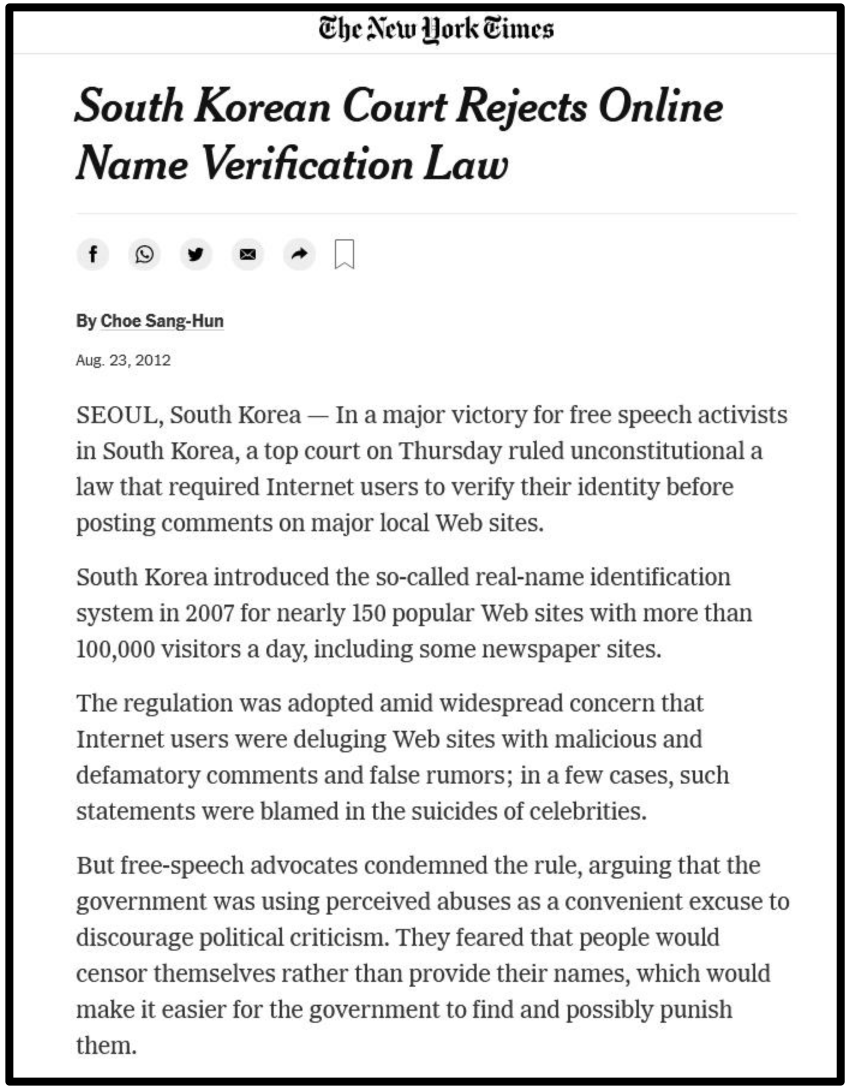
Sybil Attacks

- 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?


SYBIL
The true story of a woman possessed by 16 separate personalities
Flora Rheta Schreiber

Tie Accounts to Real Identities

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



The New York Times

South Korean Court Rejects Online Name Verification Law

By Choe Sang-Hun

Aug. 23, 2012

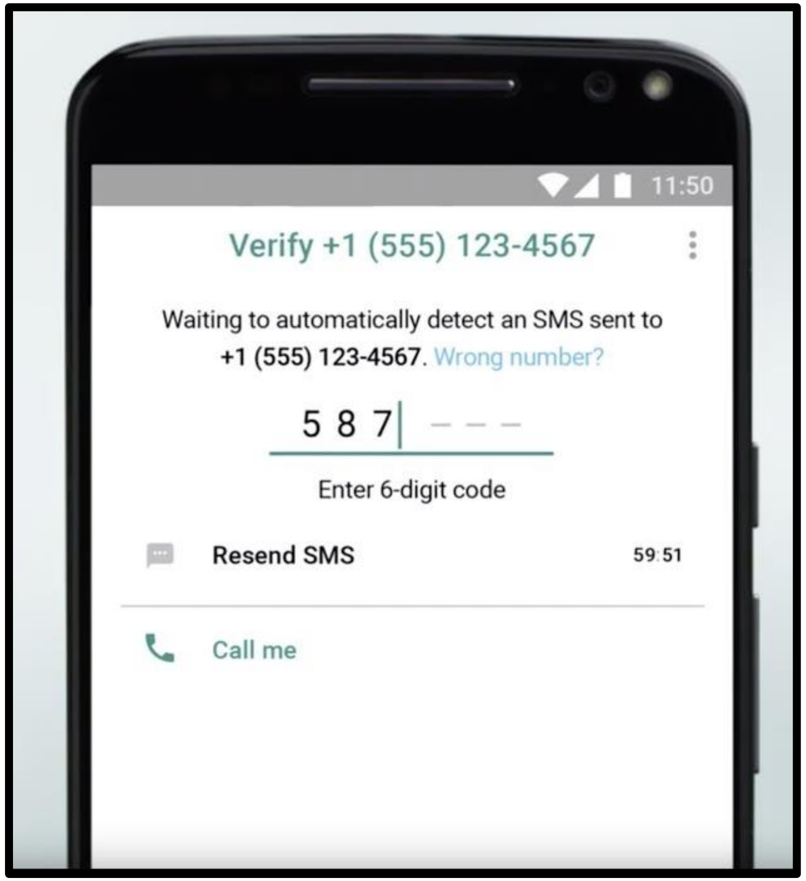
SEOUL, South Korea — In a major victory for free speech activists in South Korea, a top court on Thursday ruled unconstitutional a law that required Internet users to verify their identity before posting comments on major local Web sites.

South Korea introduced the so-called real-name identification system in 2007 for nearly 150 popular Web sites with more than 100,000 visitors a day, including some newspaper sites.

The regulation was adopted amid widespread concern that Internet users were deluging Web sites with malicious and defamatory comments and false rumors; in a few cases, such statements were blamed in the suicides of celebrities.

But free-speech advocates condemned the rule, arguing that the government was using perceived abuses as a convenient excuse to discourage political criticism. They feared that people would censor themselves rather than provide their names, which would make it easier for the government to find and possibly punish them.

Vulnerabilities of SMS Codes

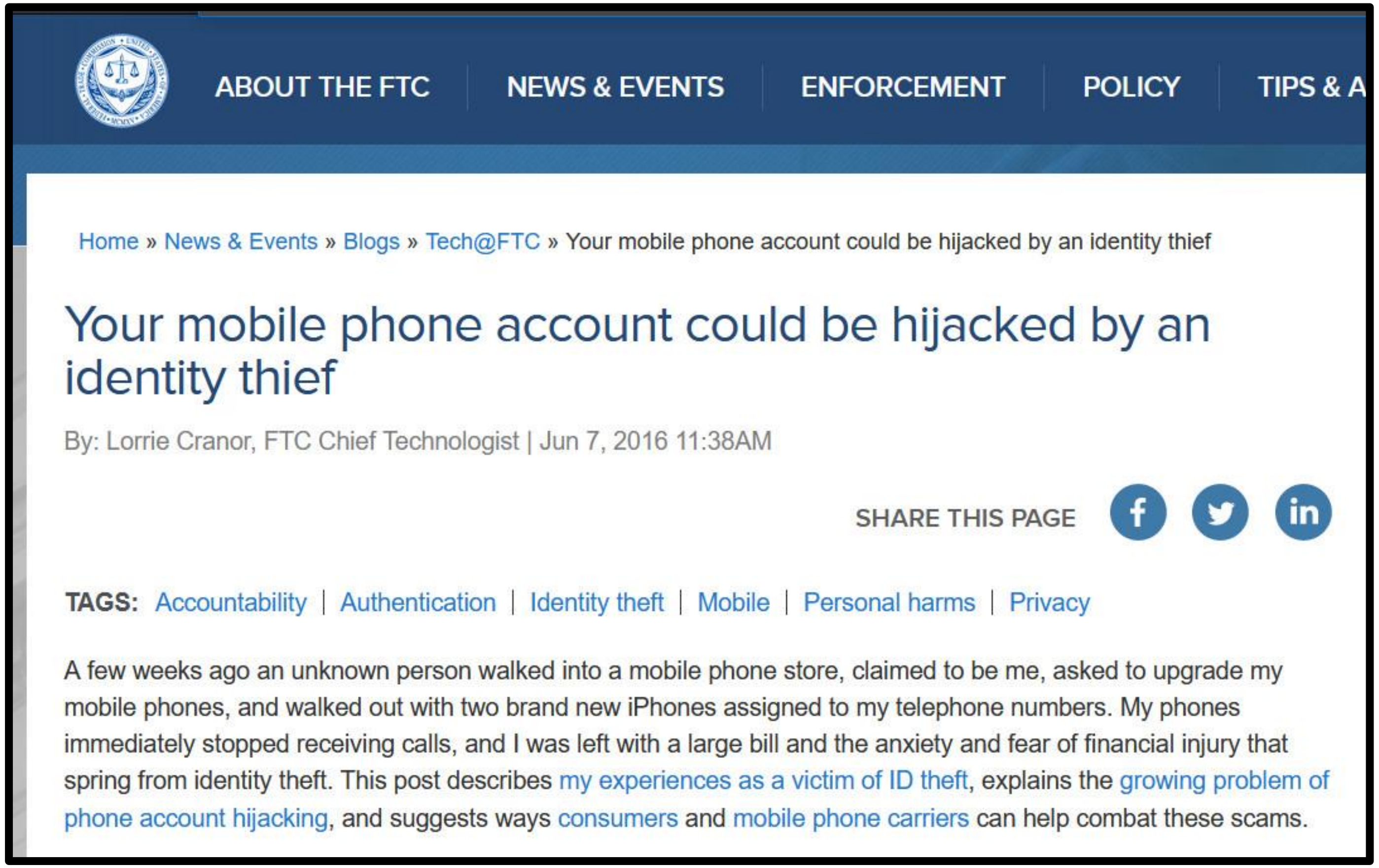


Verify +1 (555) 123-4567

Waiting to automatically detect an SMS sent to +1 (555) 123-4567. Wrong number?

5 8 7 – – –

Enter 6-digit code



Home » News & Events » Blogs » Tech@FTC » Your mobile phone account could be hijacked by an identity thief

Your mobile phone account could be hijacked by an identity thief

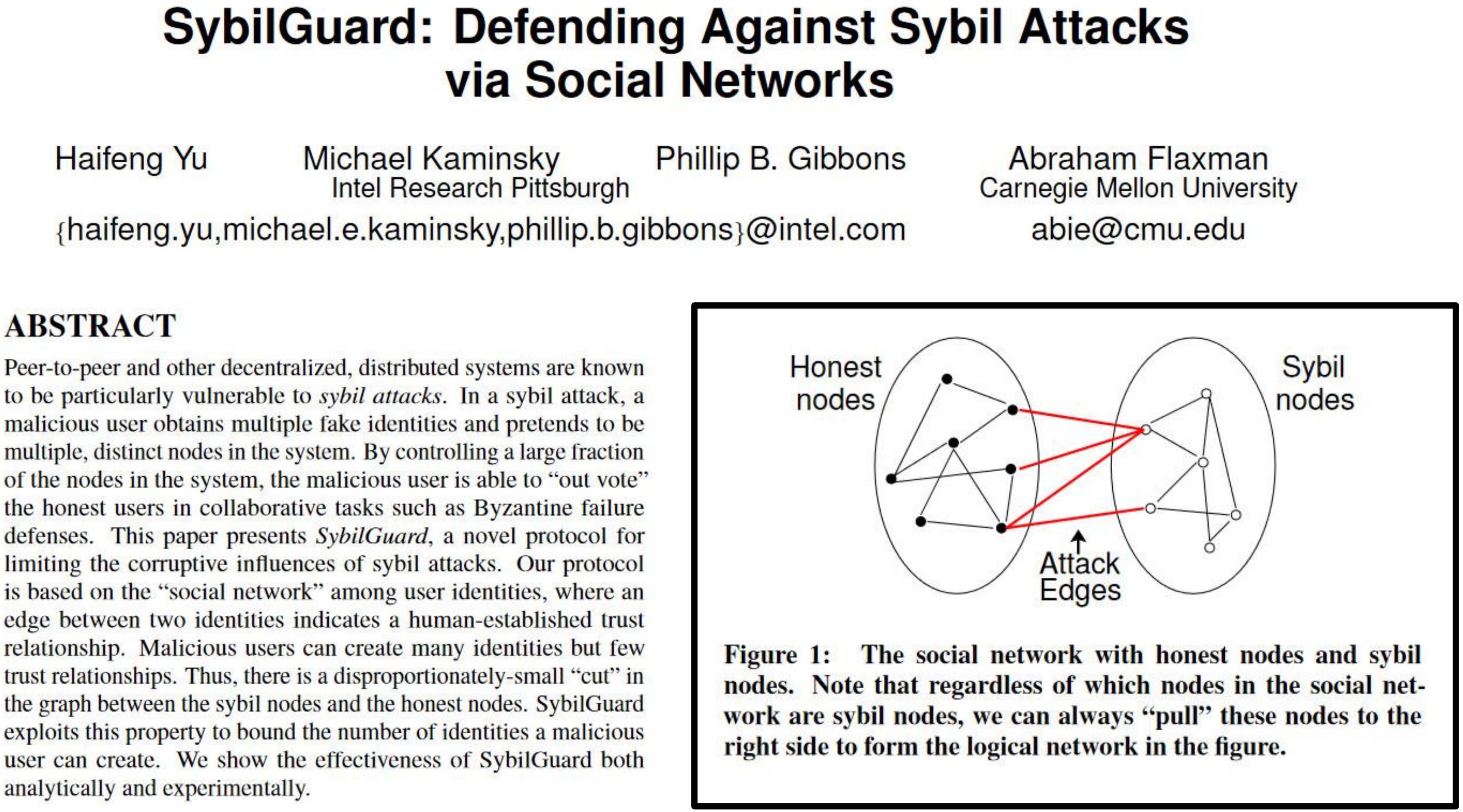
By: Lorrie Cranor, FTC Chief Technologist | Jun 7, 2016 11:38AM

TAGS: Accountability | Authentication | Identity theft | Mobile | Personal harms | Privacy

A few weeks ago an unknown person walked into a mobile phone store, claimed to be me, asked to upgrade my mobile phones, and walked out with two brand new iPhones assigned to my telephone numbers. My phones immediately stopped receiving calls, and I was left with a large bill and the anxiety and fear of financial injury that spring from identity theft. This post describes my experiences as a victim of ID theft, explains the growing problem of phone account hijacking, and suggests ways consumers and mobile phone carriers can help combat these scams.

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

Rely on Real-world Trust Relationships



SybilGuard: Defending Against Sybil Attacks via Social Networks

Haifeng Yu Michael Kaminsky Phillip B. Gibbons
Intel Research Pittsburgh
{haifeng.yu,michael.e.kaminsky,phillip.b.gibbons}@intel.com

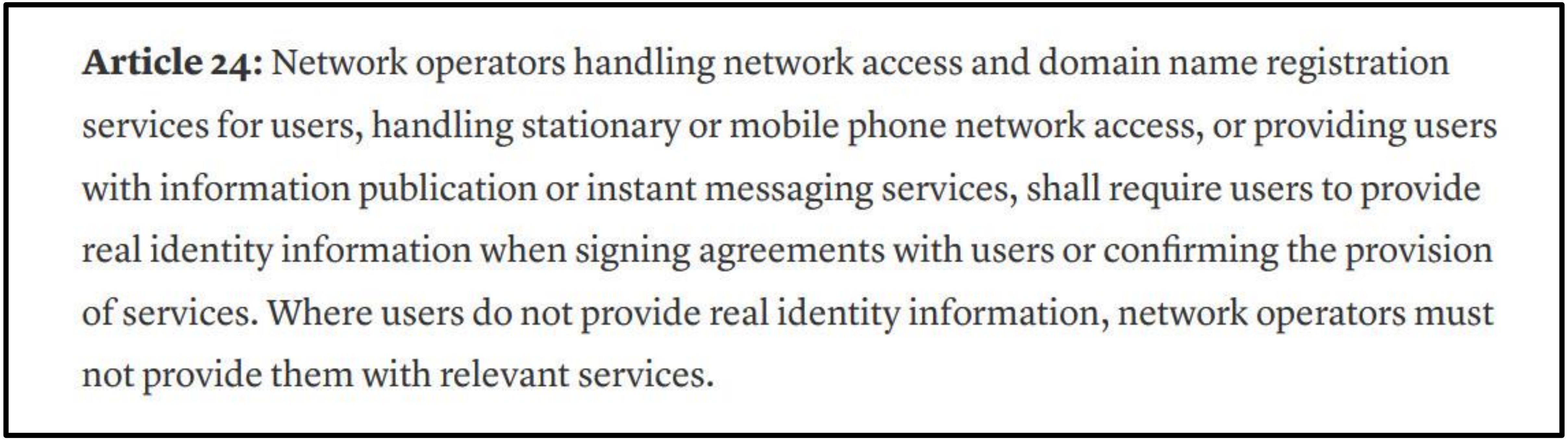
Abraham Flaxman
Carnegie Mellon University
abie@cmu.edu

ABSTRACT

Peer-to-peer and other decentralized, distributed systems are known to be particularly vulnerable to *sybil attacks*. In a sybil attack, a malicious user obtains multiple fake identities and pretends to be multiple, distinct nodes in the system. By controlling a large fraction of the nodes in the system, the malicious user is able to "out vote" the honest users in collaborative tasks such as Byzantine failure defenses. This paper presents *SybilGuard*, a novel protocol for limiting the corruptive influences of sybil attacks. Our protocol is based on the "social network" among user identities, where an edge between two identities indicates a human-established trust relationship. Malicious users can create many identities but few trust relationships. Thus, there is a disproportionately-small "cut" in the graph between the sybil nodes and the honest nodes. SybilGuard exploits this property to bound the number of identities a malicious user can create. We show the effectiveness of SybilGuard both analytically and experimentally.

Figure 1: The social network with honest nodes and sybil nodes. Note that regardless of which nodes in the social network are sybil nodes, we can always "pull" these nodes to the right side to form the logical network in the figure.

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.

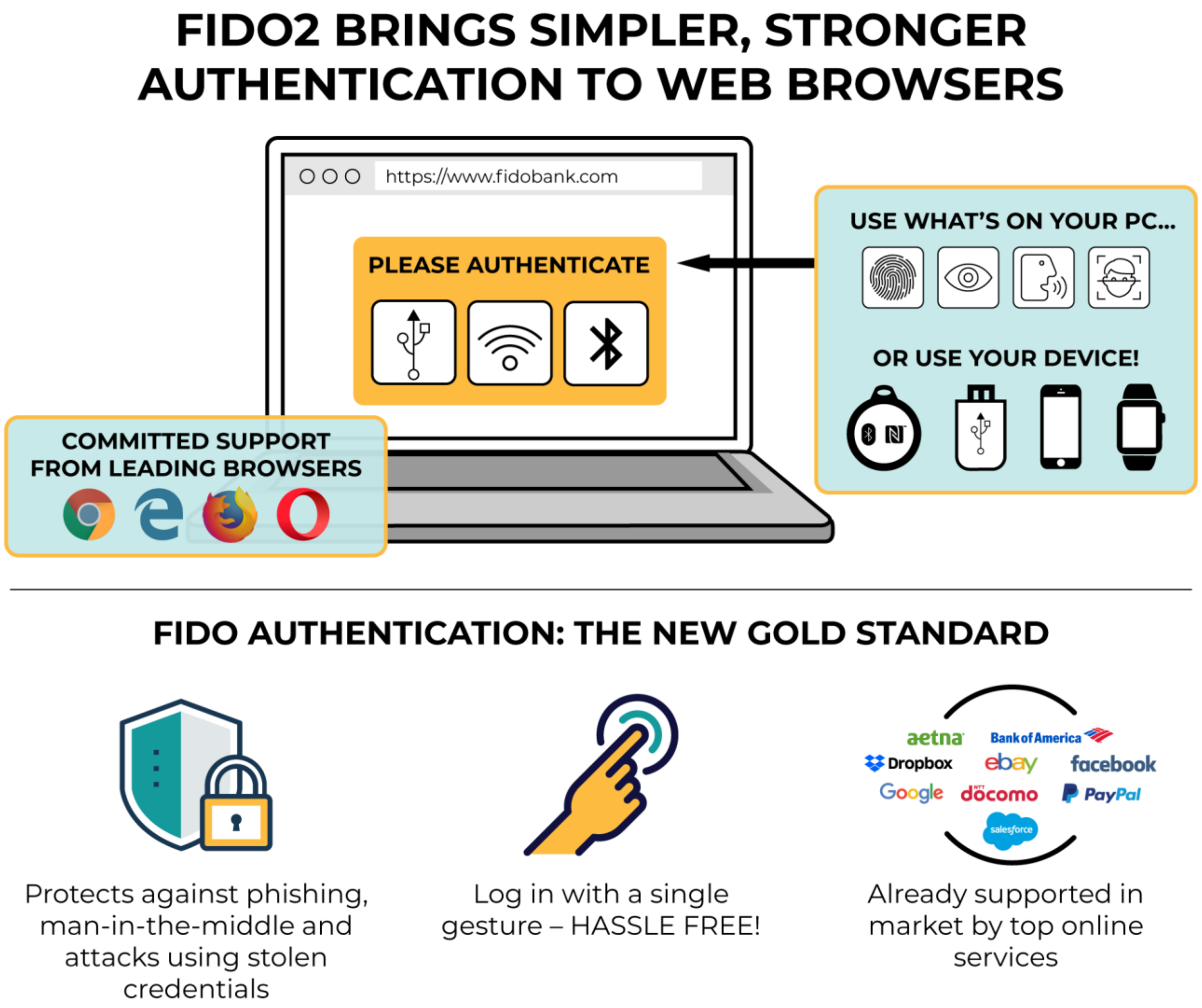
https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/

National ID Cards

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

https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/identity/2016-national-id-card-trends

Authentication with Asymmetric Crypto



FIDO2 BRINGS SIMPLER, STRONGER AUTHENTICATION TO WEB BROWSERS

https://www.fidobank.com

PLEASE AUTHENTICATE

USE WHAT'S ON YOUR PC...

OR USE YOUR DEVICE!

COMMITTED SUPPORT FROM LEADING BROWSERS

FIDO AUTHENTICATION: THE NEW GOLD STANDARD

Protects against phishing, man-in-the-middle and attacks using stolen credentials

Log in with a single gesture – HASSLE FREE!

Already supported in market by top online services

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

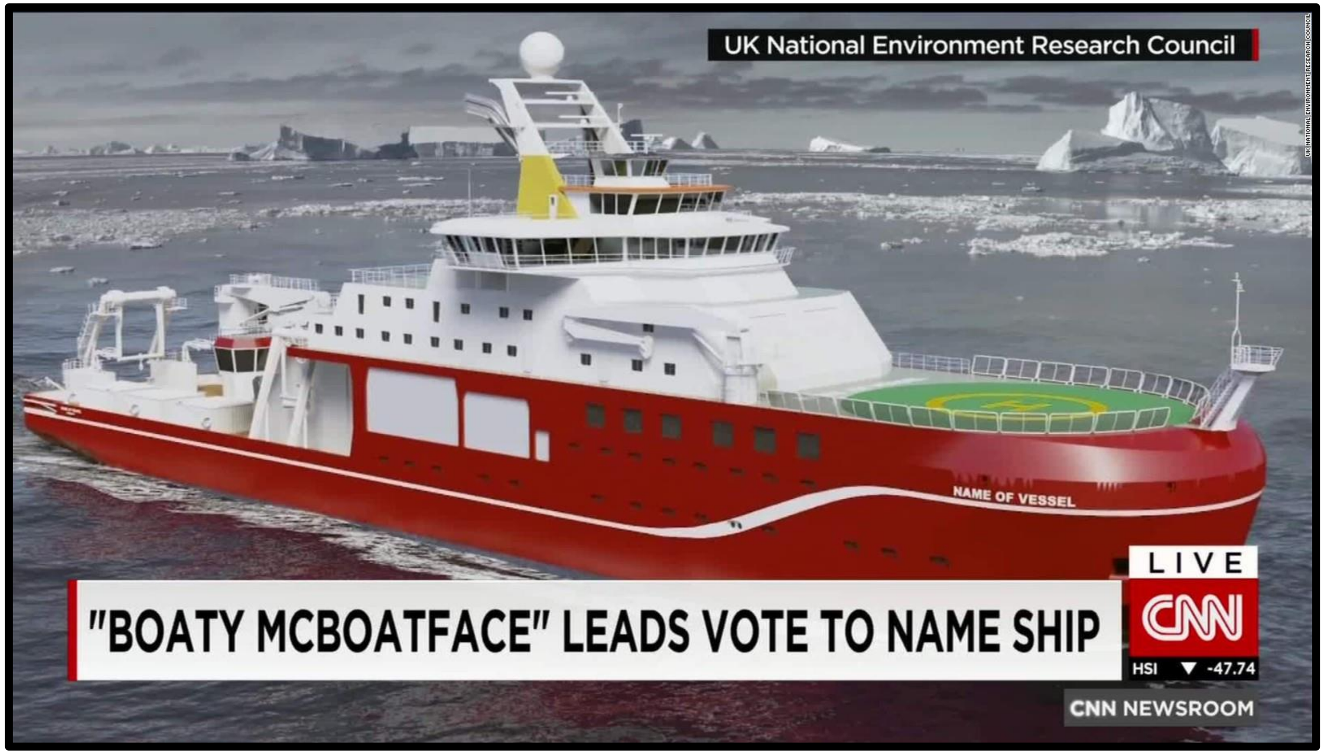
- Example (problematic) system: You upload some data to a computer system and it trains a neural network with that data
- Example (problematic) system: You upload the product of two large prime numbers to a system and it factorizes it
- What’s the problem? **Denial of Service (DoS) attacks**

Need for Proofs of Work

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

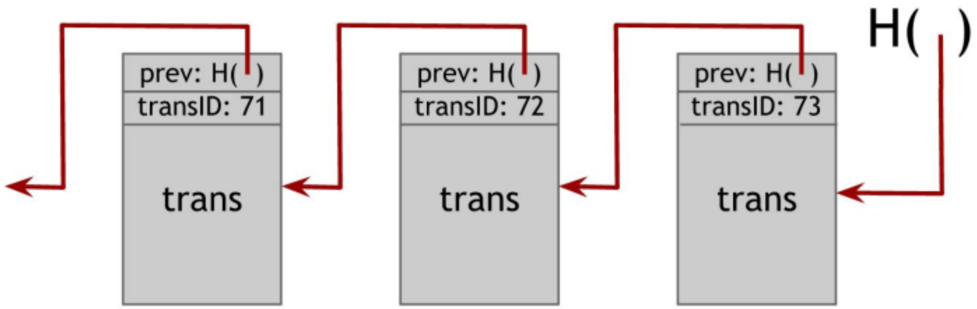
Need for Proofs of Work

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


UK National Environment Research Council
NAME OF VESSEL
LIVE
CNN
"BOATY MCBOATFACE" LEADS VOTE TO NAME SHIP
HSI ▼ -47.74
CNN NEWSROOM

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



Text and images taken from https://d28rh4a8wq0iu5.cloudfront.net/bitcointech/readings/princeton_bitcoin_book.pdf and https://www.oreilly.com/library/view/mastering-bitcoin/9781491902639/ch08.html

Blockchain

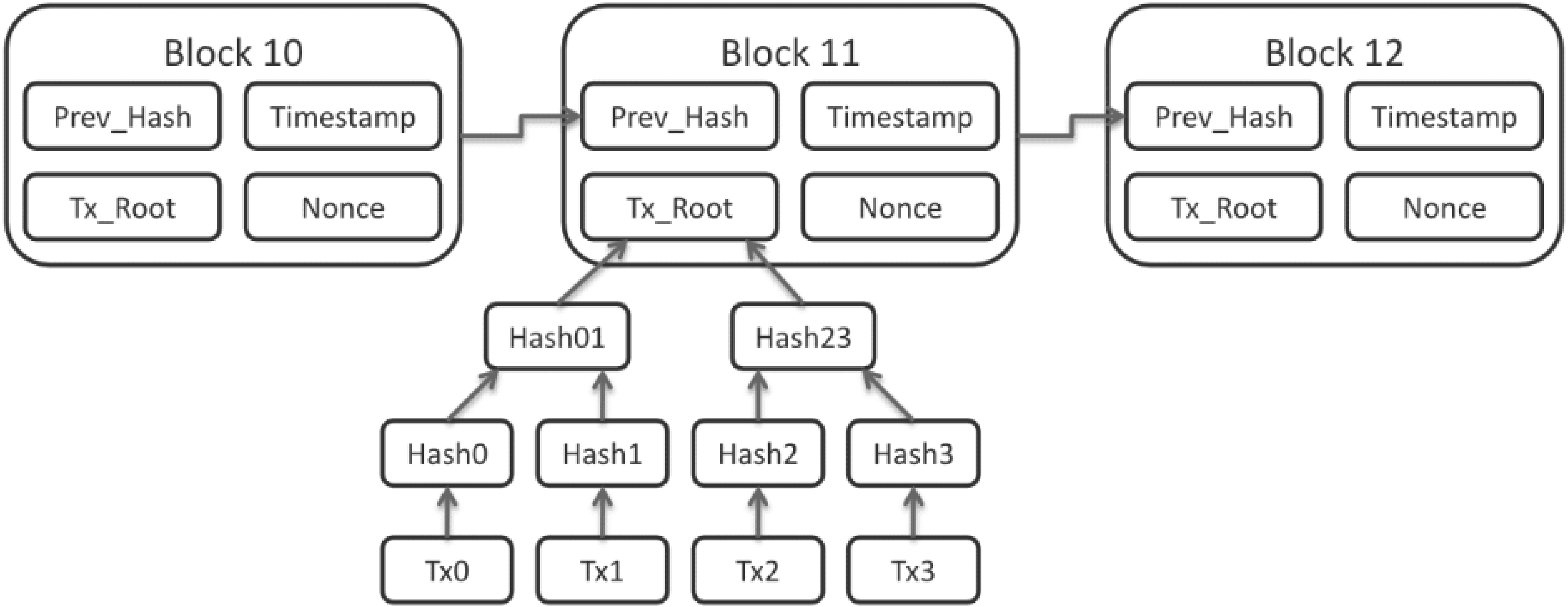


Image taken from https://coincentral.com/what-is-a-nonce-proof-of-work

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

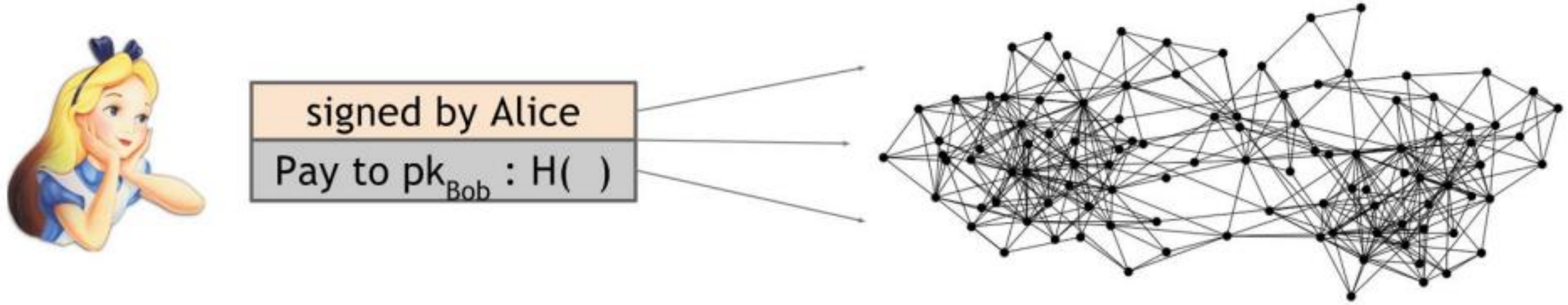
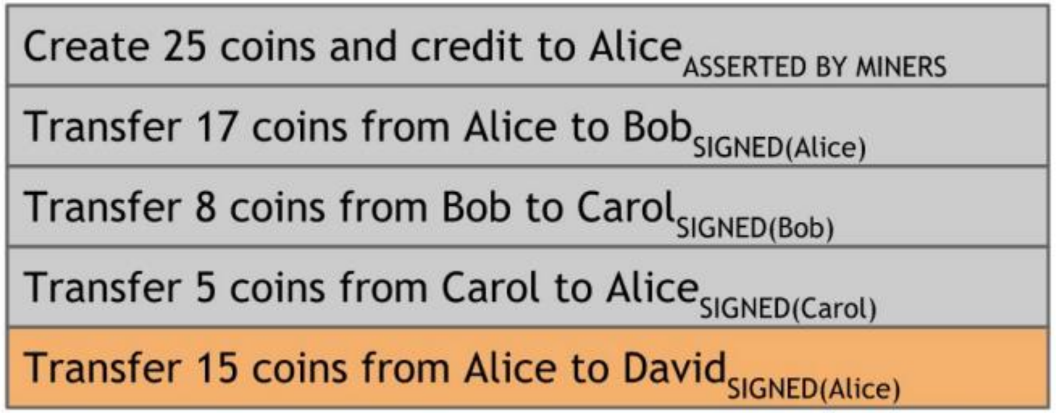


Figure 2.1 Broadcasting a transaction In order to pay Bob, Alice broadcasts the transaction to the entire Bitcoin peer-to-peer network.

Text and images taken from https://d28rh4a8wq0iu5.cloudfront.net/bitcointech/readings/princeton_bitcoin_book.pdf and https://www.oreilly.com/library/view/mastering-bitcoin/9781491902639/ch08.html

Blockchain as a Distributed Ledger

- Conceptual (but impractical) idea: ledger of accounts



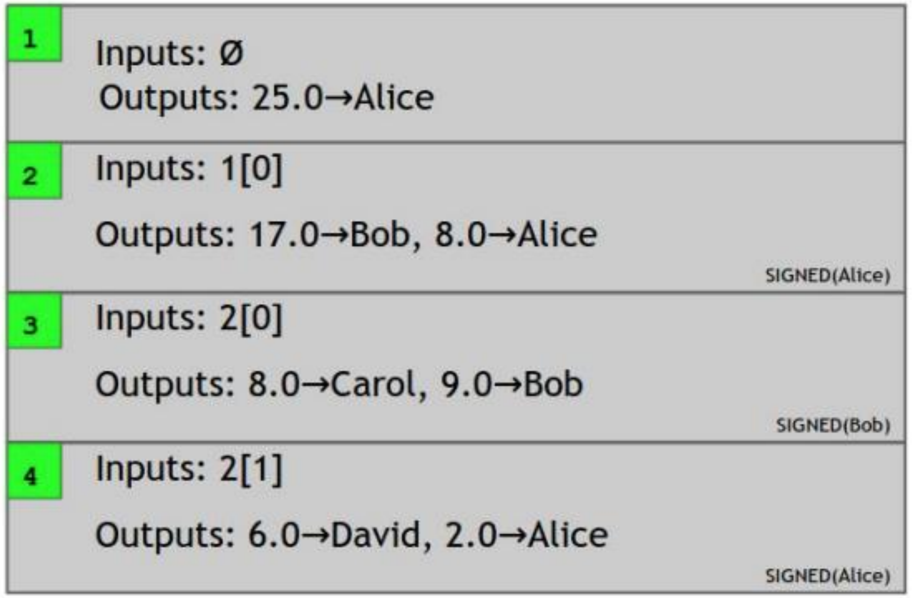
Create 25 coins and credit to Alice$_{\text{ASSERTED BY MINERS}}$
Transfer 17 coins from Alice to Bob$_{\text{SIGNED(Alice)}}$
Transfer 8 coins from Bob to Carol$_{\text{SIGNED(Bob)}}$
Transfer 5 coins from Carol to Alice$_{\text{SIGNED(Carol)}}$
Transfer 15 coins from Alice to David$_{\text{SIGNED(Alice)}}$

Figure 3.1 an account-based ledger

Text and images taken from https://d28rh4a8wq0iu5.cloudfront.net/bitcointech/readings/princeton_bitcoin_book.pdf and https://www.oreilly.com/library/view/mastering-bitcoin/9781491902639/ch08.html

Blockchain as a Distributed Ledger

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



1 Inputs: Ø
Outputs: 25.0→Alice

2 Inputs: 1[0]
Outputs: 17.0→Bob, 8.0→Alice
SIGNED(Alice)

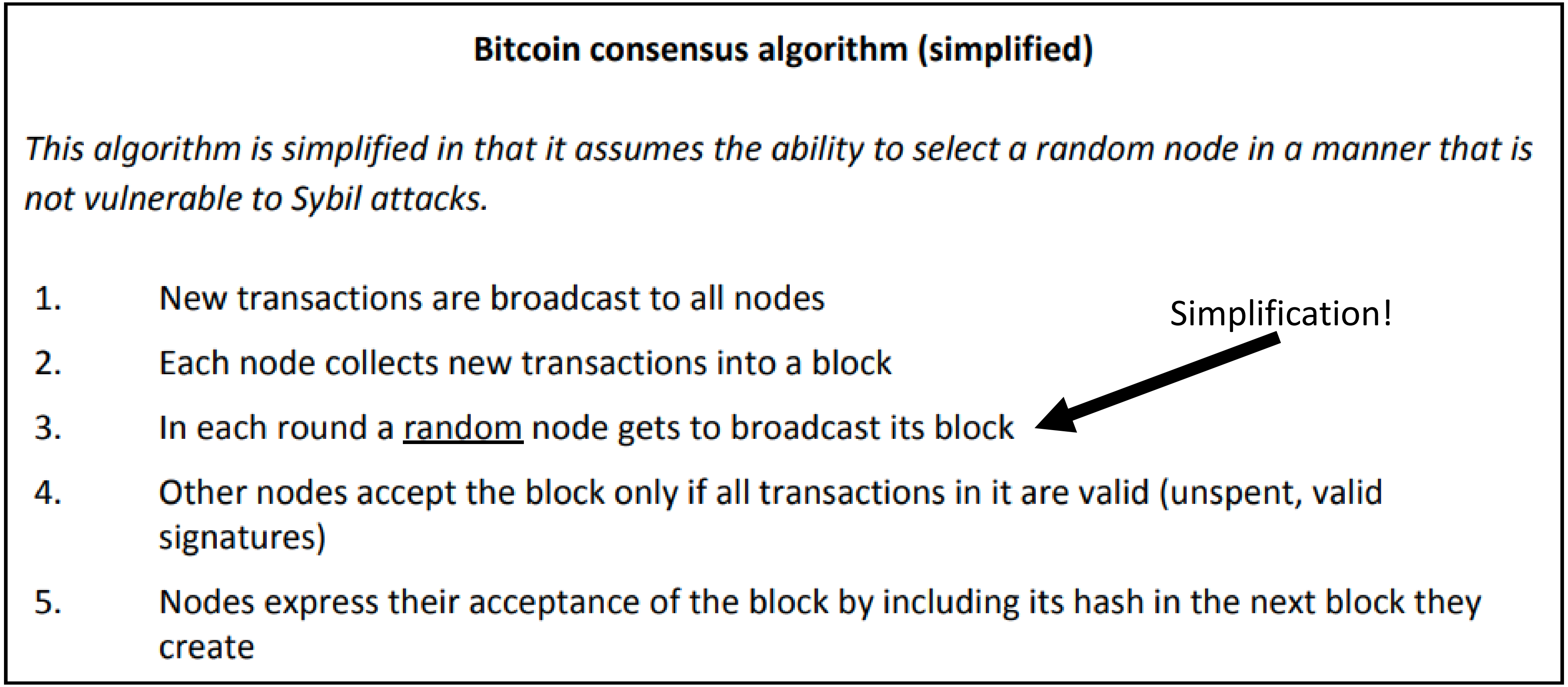
3 Inputs: 2[0]
Outputs: 8.0→Carol, 9.0→Bob
SIGNED(Bob)

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

Text and images taken from https://d28rh4a8wq0iu5.cloudfront.net/bitcointech/readings/princeton_bitcoin_book.pdf and
https://www.oreilly.com/library/view/mastering-bitcoin/9781491902639/ch08.html

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!

Text and images taken from https://d28rh4a8wq0iu5.cloudfront.net/bitcointech/readings/princeton_bitcoin_book.pdf and https://www.oreilly.com/library/view/mastering-bitcoin/9781491902639/ch08.html

Distributed Consensus in Bitcoin

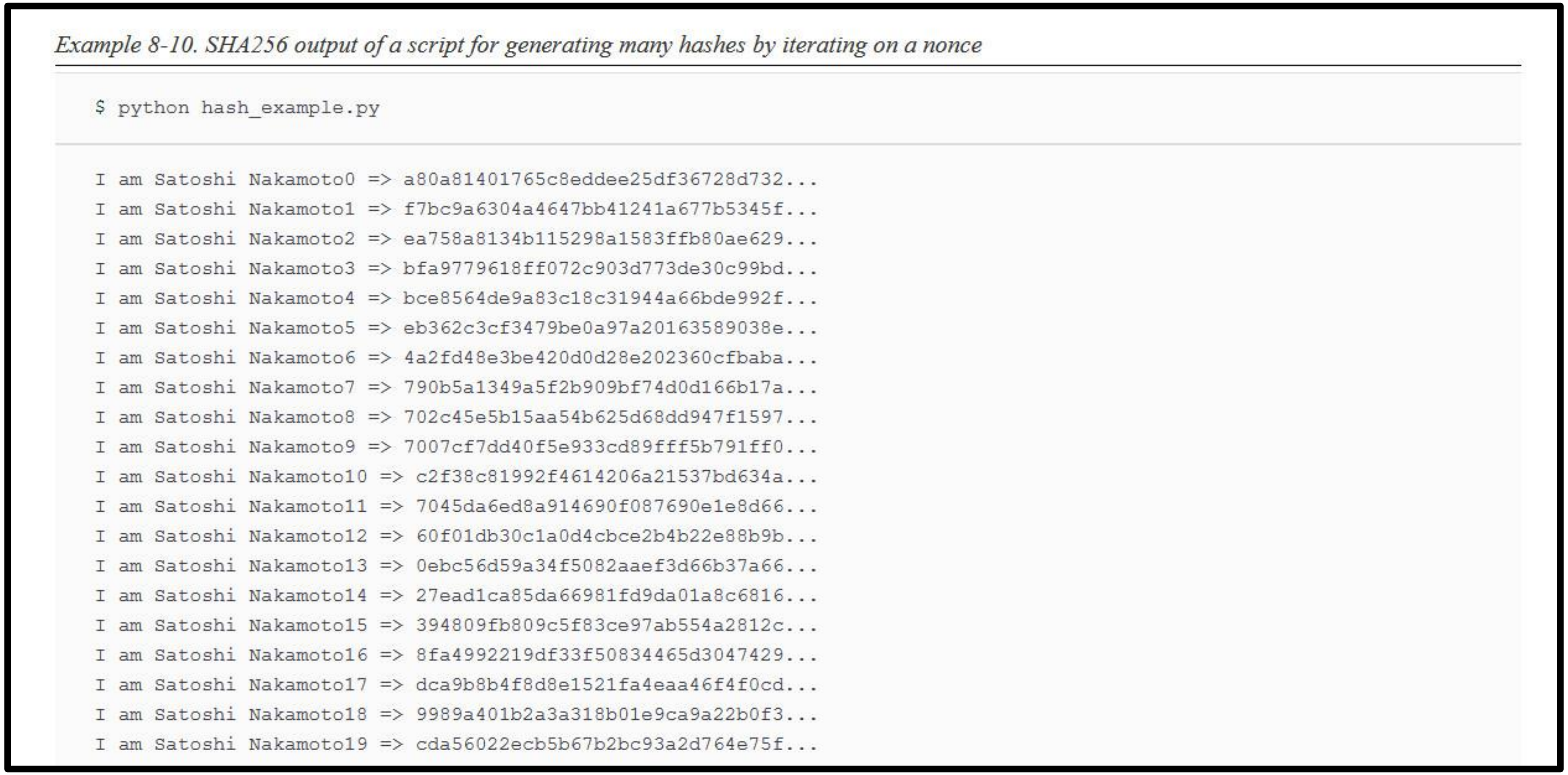
- We are going to be hashing blocks, which include:
  - A pointer to the previous block and a hash of its contents (*prev_hash*)
  - The transactions captured in this block of the ledger (*tx*…)
  - A nonce, which you'll guess (over and over and over)
- Try to find a nonce that solves the following:

$$H(nonce \,\|\, prev\_hash \,\|\, tx \,\|\, tx \,\|\, \ldots \,\|\, tx) < target$$

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

Text and images taken from https://d28rh4a8wq0iu5.cloudfront.net/bitcointech/readings/princeton_bitcoin_book.pdf and https://www.oreilly.com/library/view/mastering-bitcoin/9781491902639/ch08.html and https://www.vox.com/2015/11/3/18053556/how-does-the-bitcoin-network-process-transactions

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...
```

Text and images taken from https://d28rh4a8wq0iu5.cloudfront.net/bitcointech/readings/princeton_bitcoin_book.pdf and https://www.oreilly.com/library/view/mastering-bitcoin/9781491902639/ch08.html

Clarifications About the Overall Process

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

Text and images taken from https://d28rh4a8wq0iu5.cloudfront.net/bitcointech/readings/princeton_bitcoin_book.pdf and https://www.oreilly.com/library/view/mastering-bitcoin/9781491902639/ch08.html

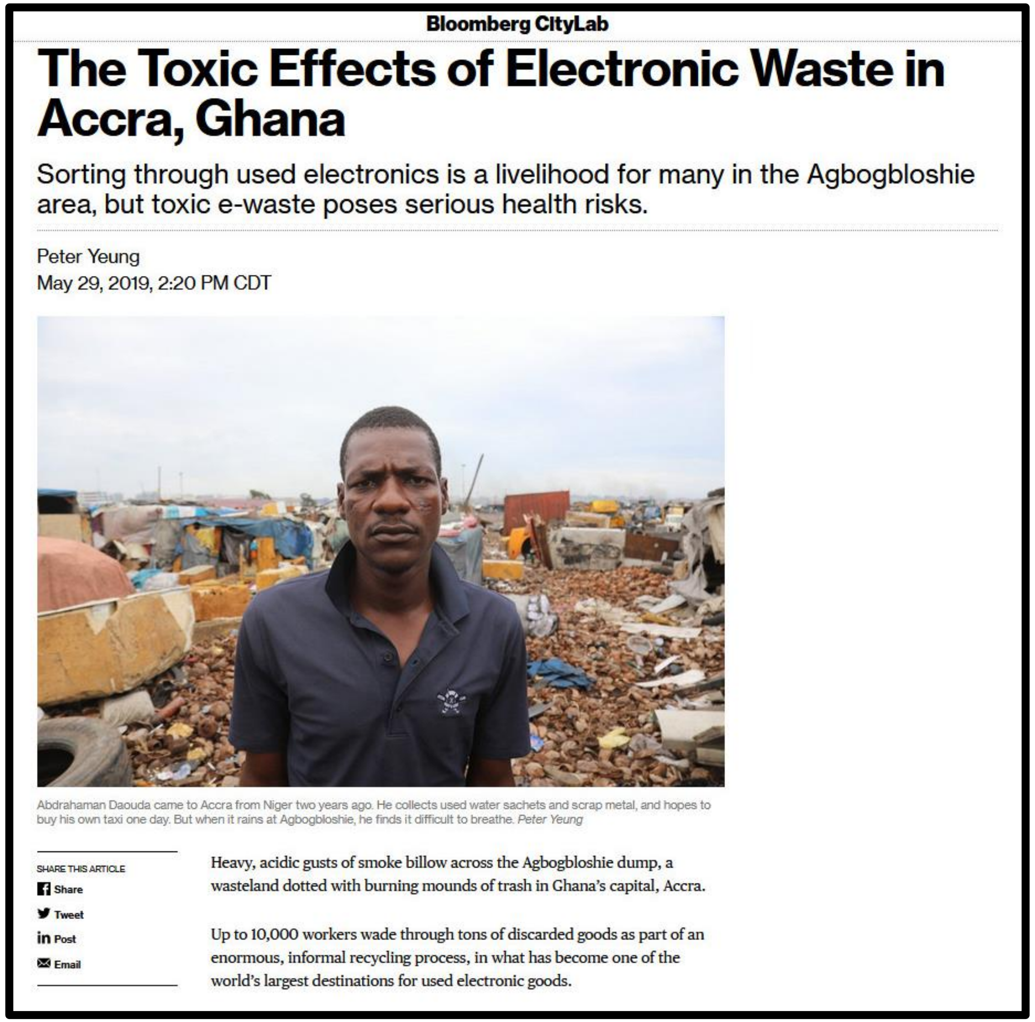
Proof of Stake

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

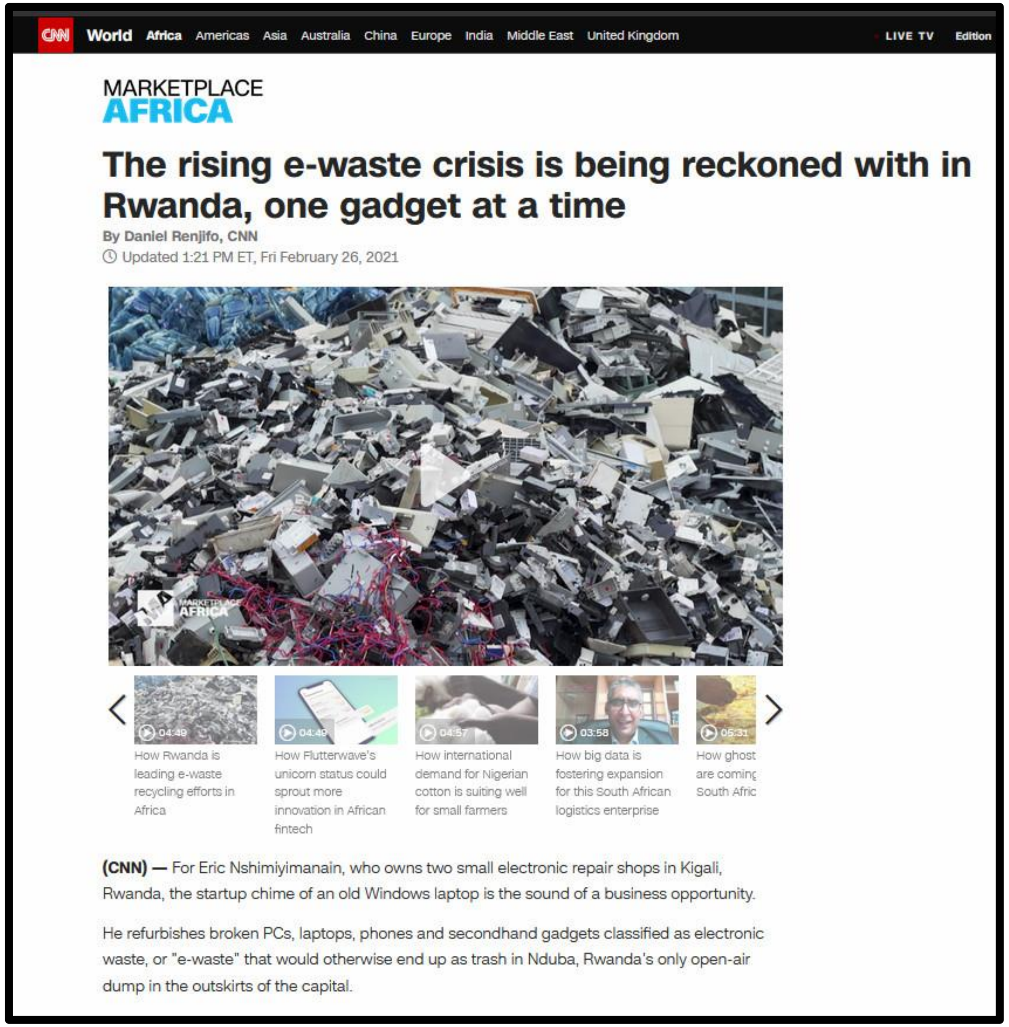
Sorting through used electronics is a livelihood for many in the Agbogbloshie area, but toxic e-waste poses serious health risks.

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

Abdrahaman 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.



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

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

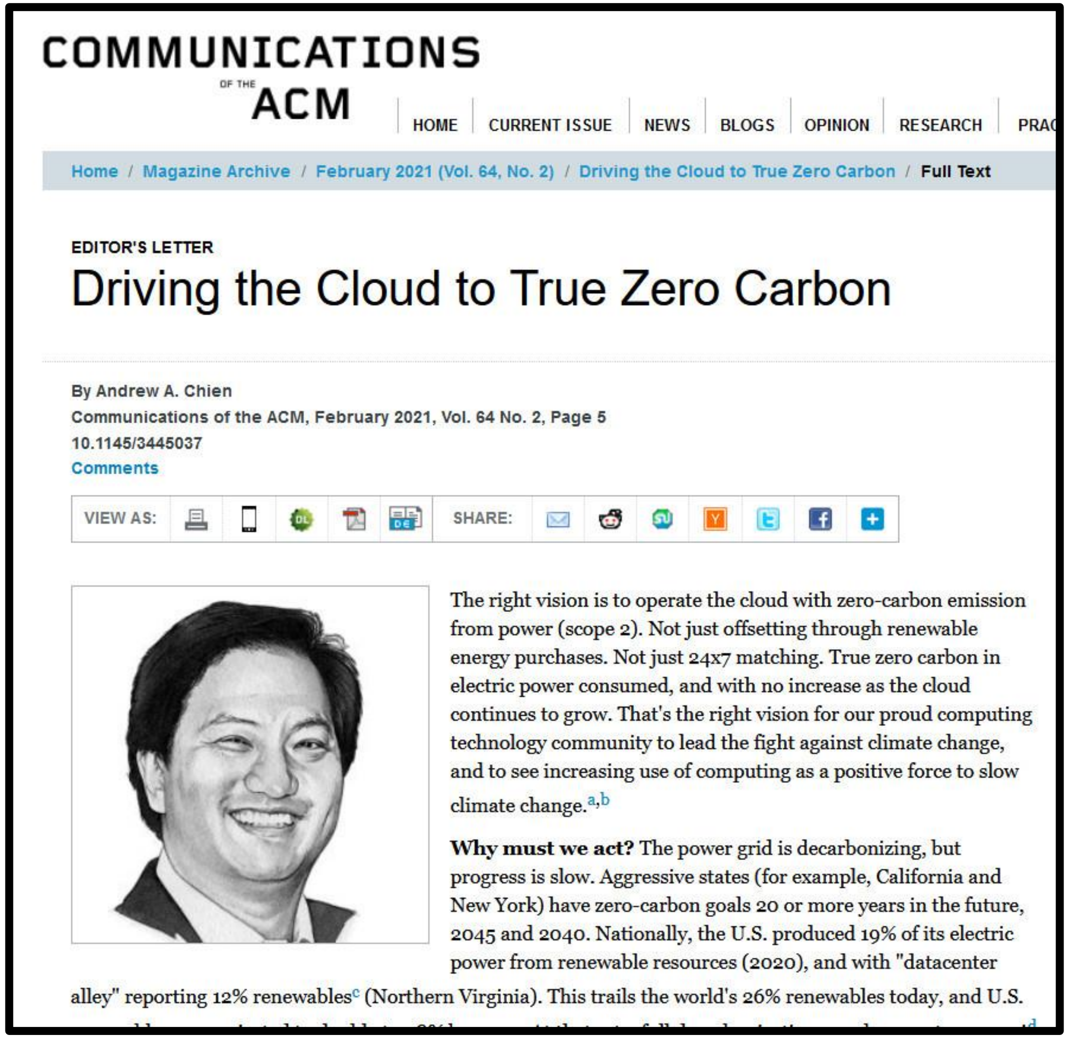
04:49
How Rwanda is leading e-waste recycling efforts in Africa
04:49
How Flutterwave's unicorn status could sprout more innovation in African fintech
04:57
How international demand for Nigerian cotton is suiting well for small farmers
03:58
How big data is fostering expansion for this South African logistics enterprise
05:31
How ghost are coming South Afric

(CNN) — For Eric Nshimiyimanain, 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 / 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

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.

https://cacm.acm.org/magazines/2021/2/250064-driving-the-cloud-to-true-zero-carbon/fulltext