CPSC 430
Computers & Society

Class 4C: Computer & Network Security

Dr. Firas Moosvi | 2024_S1

Slides courtesy of Dr. Kevin Leyton-Brown

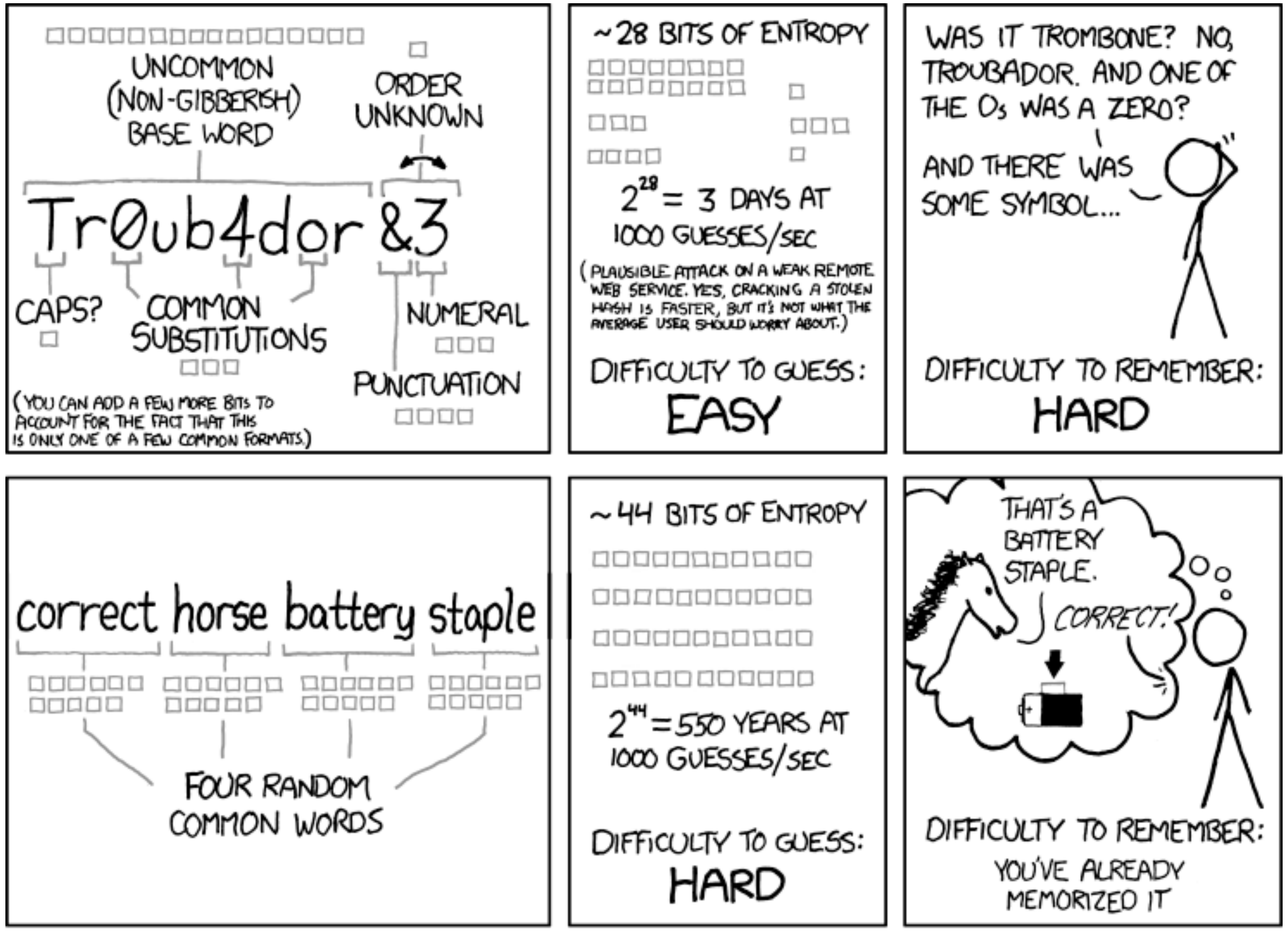
Class Outline

1. Announcements (5 mins)
2. Passwords and Hackers (30 mins)
3. Break (10 mins)
4. Mid-course Feedback (10 mins)
5. Activity (20 mins)
6. Break (10 mins)
7. Cyberwarfare (30 mins)
8. Reminders before next class (5 mins)

Announcements

Passwords and Hackers

Password Strength


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor &3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS: EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Hackers

- Hacker (original meaning):
  - Explorer, risk-taker, technical virtuoso
  - Values free exchange of information; mistrusts authority; values technical skill; holds an optimistic view of technology
- Hacker (ultimate meaning):
  - Teenagers accessing corporate or government computers
  - Stealing and/or destroying confidential information
- What hasn’t changed: hackers’ public image

Ethics of Hacking

- Parallels between hackers/phreaks & MP3 downloaders
  - Establishment overvalues intellectual property
  - Use of technology as a “joy ride”
  - Breaking certain laws considered not that big a deal
  - (Guess what the police, RIAA thinks about these arguments?)

- *Have you ever hacked anything?*
- *Which, if any, forms of hacking do you consider ethical?*
- *Is it wrong to learn hacking or phreaking skills, if these skills are never put to use?*

Malware: Evil Code that can Run on Your Computer

- **Viruses**
  - What is a virus?
  - *Have you ever (knowingly) gotten one?*
- **Worms**
  - What is a worm? How is it different from a virus?
  - *Is it wrong to distribute a virus or worm that doesn’t harm anyone?*
- **Trojan Horses**
  - What is a Trojan horse? How is it different from the first two?

- *Do the victims of a virus/worm/Trojan horse share responsibility for being attacked if their system is not up to date?*

Malware II: More Evil Code

- **Spyware/Adware**
  - What is spyware? What is adware?
  - *Is it ever moral to install spyware/adware on a user’s computer without their consent?*
- **Drive-by Downloads**
  - What is a drive-by download?
- **General-purpose Defensive Measures**
  - security patches
  - anti-malware tools
  - firewalls
  - *Anything else?*

Attacks: how mean computers hurt nice computers

- **How:**
  - **Phishing**
    - *Have you been targeted? Has an attack been successful?*
  - **[Distributed] Denial of Service**
  - **Ransomware attacks**
- **Why:**
  - **Cybercrime: professionalization of malware**
    - renting botnets (DDoS; spam)
    - stealing credit card numbers, passwords

Mid-course feedback

Mid-course feedback

Cyberwarfare

Electronic Money

- Financial transactions are increasingly moving online
- Advantages
  - easier transactions
  - easier access to credit
  - discourages black market economy
  - prevents businesses from having to carry cash floats
- Disadvantages
  - empowers a few corporations
  - less anonymity
  - security risks
- *Other advantages/disadvantages? What do you think?*

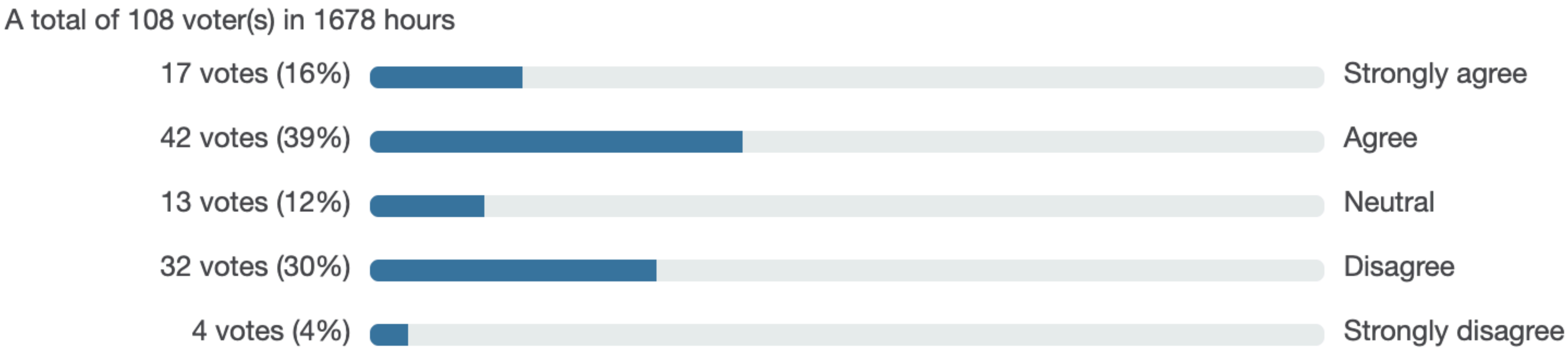
Blockchain

- Distributed ledgers offer an alternative approach to electronic money that works more like cash
- What is:
  - blockchain?
  - mining?
  - what stops someone from spending the same digital money twice?
  - what's an NFT
- But, the currency is incredibly volatile (and, not everyone even agrees that it makes sense to think of it as money)

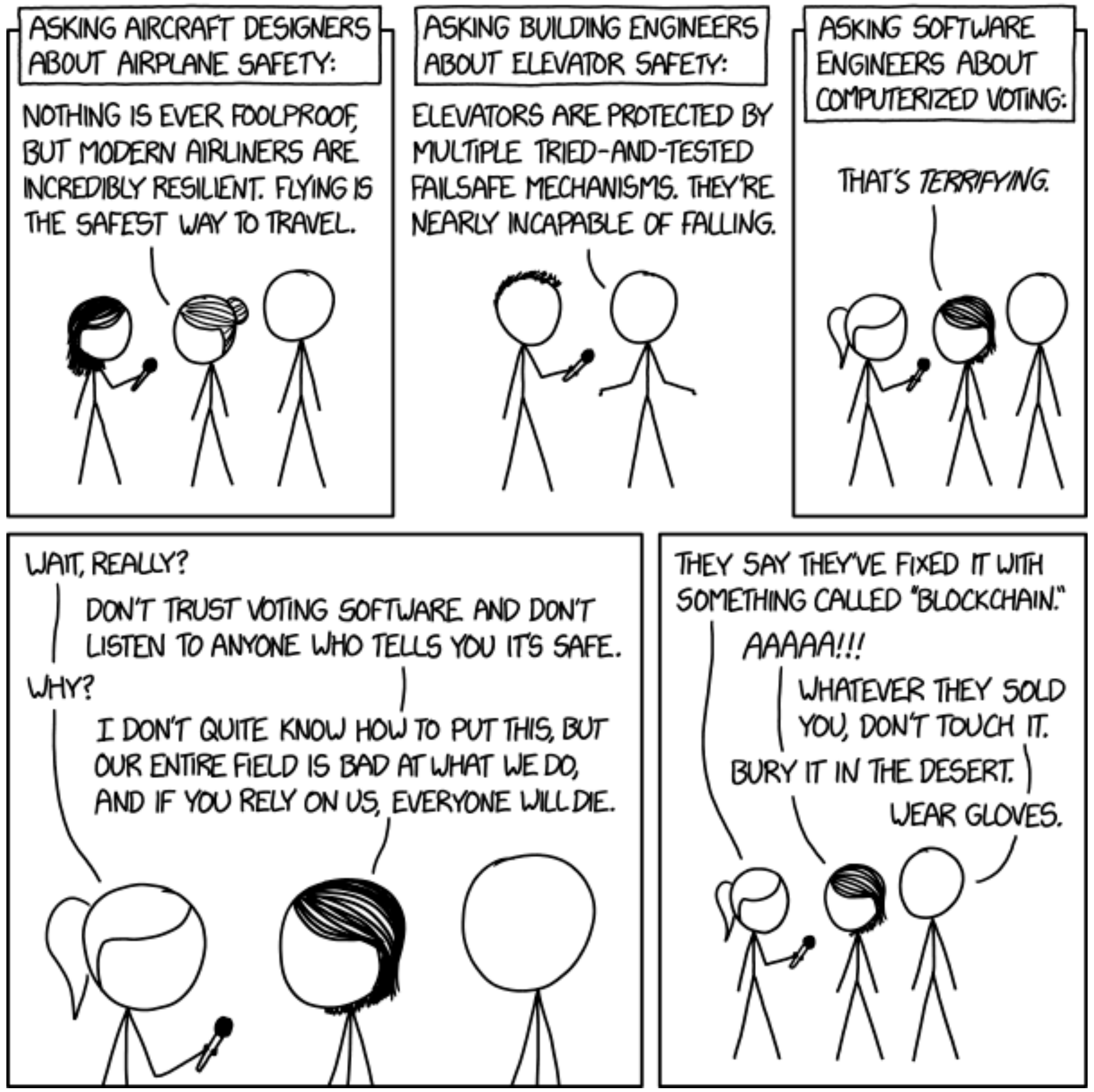
What do you think? Should governments encourage blockchain-based currencies? Do you use them?

Computer and Network Security

“Canadians should be able to vote online in federal, provincial and municipal elections.”



Online Voting


ASKING AIRCRAFT DESIGNERS ABOUT AIRPLANE SAFETY:
NOTHING IS EVER FOOLPROOF, BUT MODERN AIRLINERS ARE INCREDIBLY RESILIENT. FLYING IS THE SAFEST WAY TO TRAVEL.
ASKING BUILDING ENGINEERS ABOUT ELEVATOR SAFETY:
ELEVATORS ARE PROTECTED BY MULTIPLE TRIED-AND-TESTED FAILSAFE MECHANISMS. THEY'RE NEARLY INCAPABLE OF FALLING.
ASKING SOFTWARE ENGINEERS ABOUT COMPUTERIZED VOTING:
THAT'S TERRIFYING.
WAIT, REALLY?
DON'T TRUST VOTING SOFTWARE AND DON'T LISTEN TO ANYONE WHO TELLS YOU IT'S SAFE.
WHY?
I DON'T QUITE KNOW HOW TO PUT THIS, BUT OUR ENTIRE FIELD IS BAD AT WHAT WE DO, AND IF YOU RELY ON US, EVERYONE WILL DIE.
THEY SAY THEY'VE FIXED IT WITH SOMETHING CALLED "BLOCKCHAIN."
AAAAA!!!
WHATEVER THEY SOLD YOU, DON'T TOUCH IT.
BURY IT IN THE DESERT.
WEAR GLOVES.

- Motivation:
  - More people would vote
  - Votes would be counted more quickly
  - Cost less money
  - Avoid disputed elections like Florida 2000
  - Eliminate ballot box tampering
  - Software can prevent accidental over-, under-voting
- Risks:
  - Gives unfair advantage to those with computers
  - More difficult to preserve voter privacy
  - More opportunities for vote selling
  - Obvious target for a DDoS attack
  - Security of election depends on security of home computers
  - Susceptible to phony vote servers, manipulation by foreign governments
  - No paper copies of ballots for auditing or recounts
  - Reduction in perceived legitimacy of elections even if everything works

Hacking as a means of warfare/foreign policy

- **Cyberwarfare: states as actors or targets**
  - North Korea vs USA gov, corporate sites (2009+)
  - Russia vs Georgia, Baltic states, Ukraine (2008+)
  - Stuxnet (2009+)
  - A variety of government, activist sites during Arab Spring (2011)

What hacking/cyberwarfare activities are ethical?

Which are unethical?

What such capabilities should Canada attempt to develop?

What should Canada do to attempt to discourage and/or insulate itself from unethical attacks?

Reminders before next class