Lecture 20: Cryptography, continued

- some history
  - Caesar cipher, rot13
  - substitution ciphers, etc.
  - Enigma (Turing)

- modern secret key cryptography
  - DES, AES

- public key cryptography
  - RSA, digital signatures, cryptographic hashing

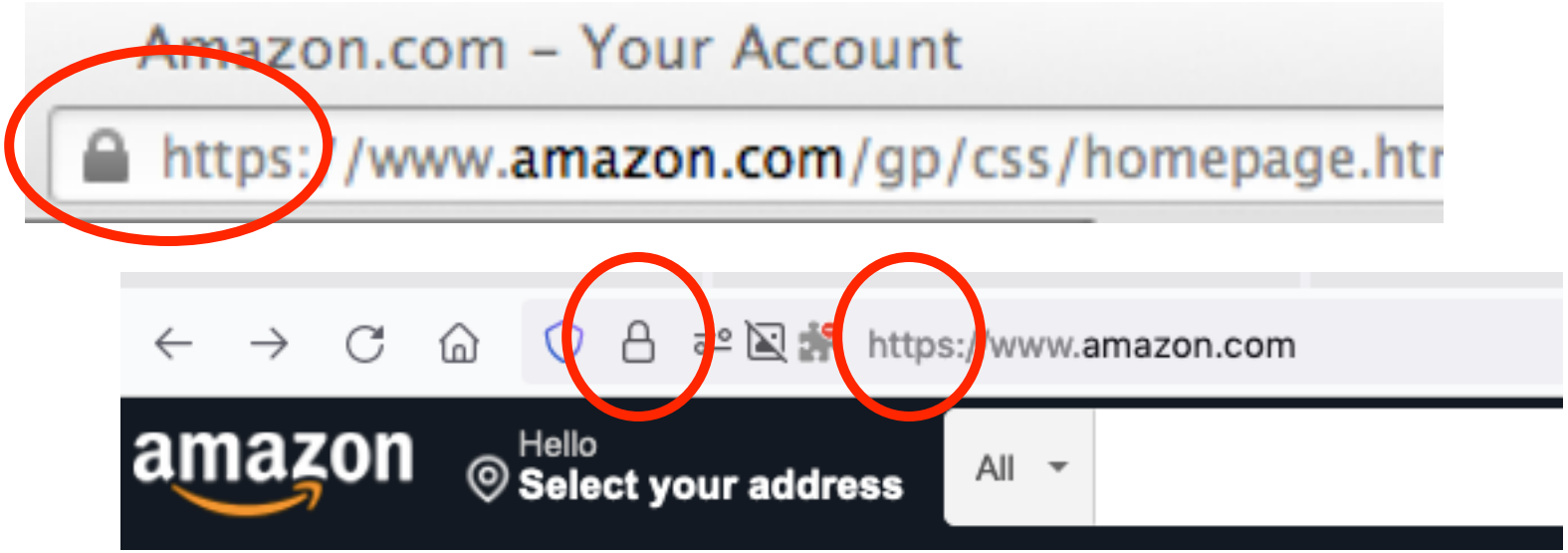
- cryptography in practice
  - e-commerce
  - Tor browser
  - Bitcoin, blockchain
  - politics

Encrypted transactions, online shopping

- browser says "prove that you're really Amazon"
- Amazon says "here's my signed certificate from a CA"
  - encrypted with the CA's private key
- browser decrypts certificate with CA's public key

- browser generates a random key, encrypts it with Amazon's public key, sends it to Amazon

- browser and Amazon use AES to talk securely



Government surveillance / Snowden revelations

- 2013: Edward Snowden, contractor at NSA, left his job
- flew to Hong Kong
- met several trusted journalists
- handed over thousands of highly classified documents
- that revealed global surveillance by NSA, and similar agencies in other countries
- with cooperation of telecomm and Internet companies

- went to Russia, given asylum
  - citizenship in Sept 2022
- called both traitor and hero in the US

Tor: The Onion Router

- anonymous routing through the Internet using TCP
  - receiver can't determine the sender's address

- sender creates a random path through a network of Tor relays
  - path is changed frequently
- each part of the path is encrypted
  - separate encryption keys for each hop
- each relay only knows who gave it data and who it sends data to
  - no relay knows the whole path
- messages are wrapped up with nested encryptions, one for each component of the path
  - each relay removes one layer of encryption before passing it on
- potentially vulnerable to some attacks
  - traffic correlation at end points
  - exit nodes can be blocked or monitored

Bitcoin and other cryptocurrencies

- how do we create a currency that is anonymous like cash
  - can't tell who spends or receives it
- is not dependent on any government
  - i.e., not a "fiat currency" like $, £, €, ...
- has the other desirable properties of money:
  - portable, durable, divisible, recognizable, difficult to counterfeit
- one solution:

  use cryptography to control the creation and transfer of money, without relying on any central authority

Bitcoin

- exists only in digital form: nothing physical like gold
  - no central authority or control
  - anonymous ownership and transfer
  - value fluctuates wildly
- how are bitcoins created?
- how is ownership validated & transferred without double spending?

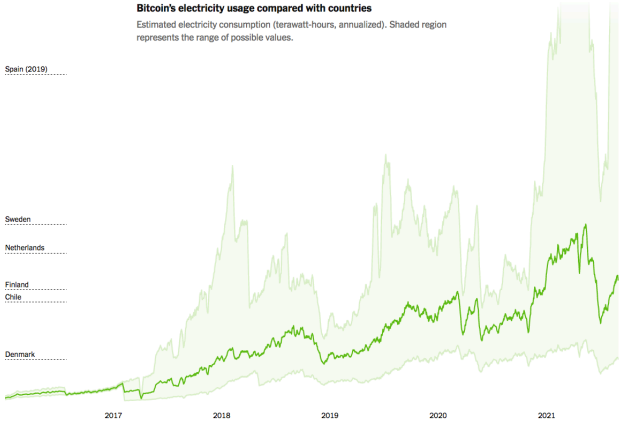
- blockchain: a shared public ledger of *all* transactions
- a transaction transfers value from one wallet to another
  - signed digitally by the sender
  - broadcast via peer to peer network so the block chain can be updated
- "mining" confirms transactions by adding them to the blockchain
  - competitive distributed consensus algorithm
  - takes work to confirm; new bitcoins are created as a reward
  - blocks are protected by cryptographic hashing; each new one depends on all previous ones

Blockchain

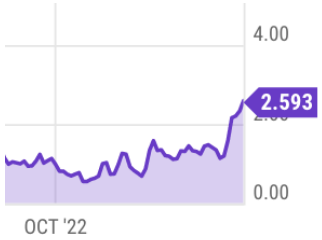
- a distributed ledger of transactions stored as a sequence of data blocks
- the blocks are protected and linked by cryptographic hashing
- a block can't be changed without changing all blocks that precede it
- cryptocurrencies are the most frequent use, but not the only one
  - Ethereum blockchain, ETH currency

Crypto and its discontents

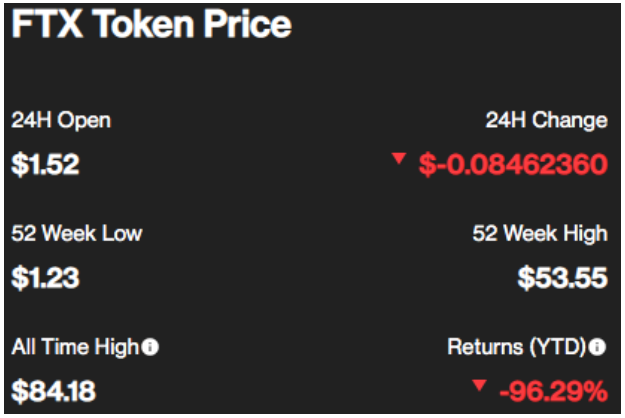
- volatility of cryptocurriences
- energy cost of mining Bitcoin (proof of work consensus computation)



- slowness / cost of transactions



- fraud, abuse, Ponzi schemes, ...



Crypto politics

- cryptographic techniques as weapons of war?
  - (strong) cryptography was classified as "munitions" in USA
  - fell under International Traffic in Arms Regulations and follow-ons
- export control laws prohibited export of cryptographic code
  - though it was ok to export books and T-shirts with code
    and everyone else in the world had it anyway
  - changed during 2000, but there are still restrictions
- does the government have the right/duty ...
  - to control cryptographic algorithms and programs?
  - to require trapdoors, key escrow, or similar mechanisms?
  - to prevent reverse-engineering of cryptographic devices?
  - to prevent research in cryptographic techniques?
- do corporations have the right ...
  - to prevent publication of cryptographic techniques?
  - to prevent reverse-engineering of cryptographic devices?
- how do we balance individual rights, property rights, & societal rights?

Summary of crypto

- secret/symmetric key algorithms: AES, ...
  - key distribution problem: everyone has to have the key
- public key algorithms: RSA, ...
  - solves key distribution problem, but authentication is still important
  - also permits digital signatures
  - much slower than secret key, so used mainly for key exchange
- security is entirely in the key
  - “security by obscurity” does not work: bad guys know everything
  - brute force attacks work if keys are too short or easy
- good cryptography is hard
  - you can't invent your own methods
  - you can't trust “secret” or proprietary methods
- people are the weak link
  - complicated or awkward systems will be subverted, ignored or misused
  - social engineering attacks are effective

    ignorance, incompetence, misguided helpfulness
- if all else fails, try bribery, burglary, blackmail, brutality

Cryptography is important

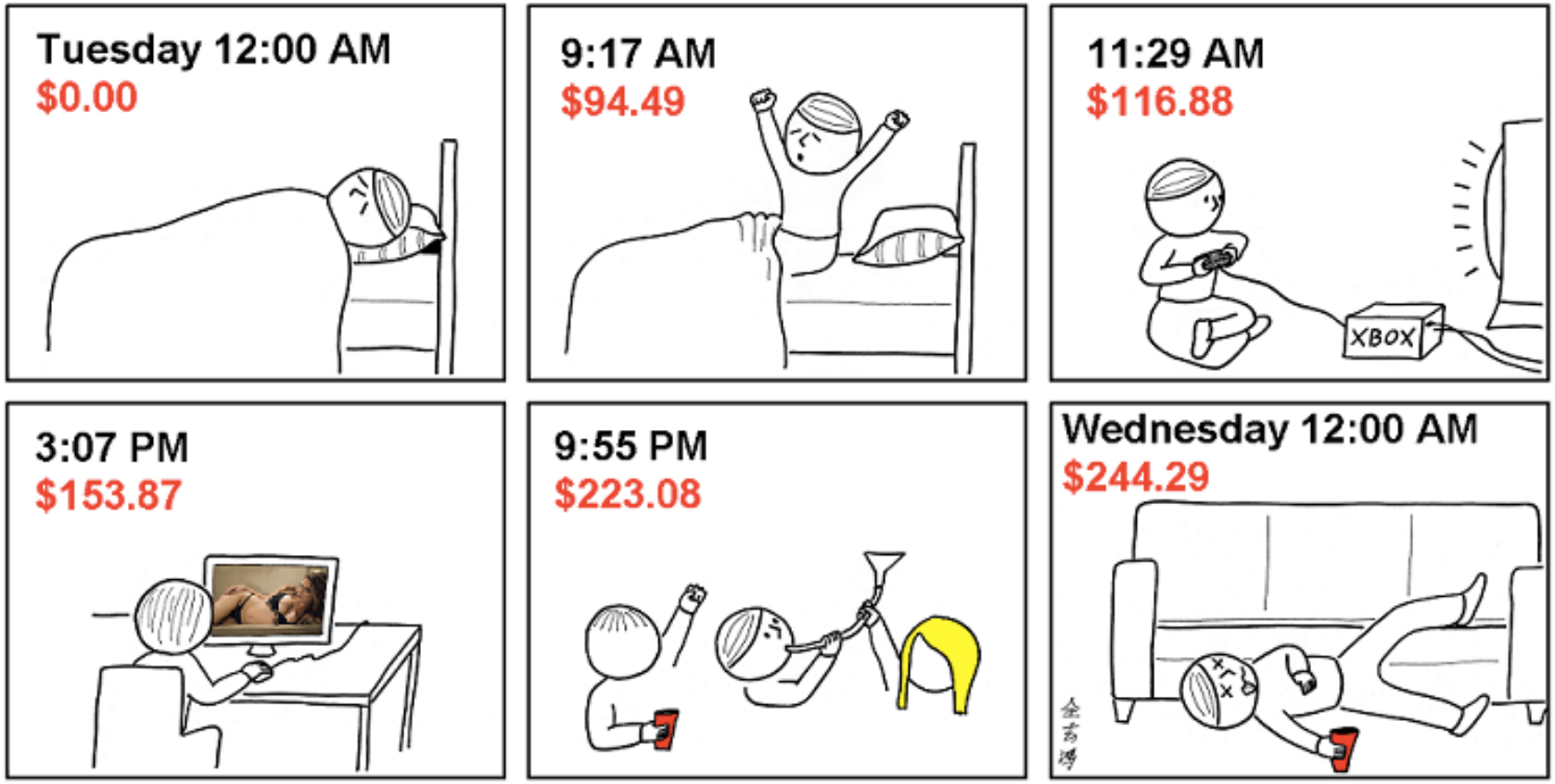
- it protects our privacy and security
  - access to computers
  - email
  - online shopping, banking, taxes
  - electronic voting
  - ...

- it can restrict our rights and freedoms
  - digital rights management: limits on what we can do with music, movies, software, ...

- it helps good guys and bad guys alike

just a reminder...

...to my friend's nephew, 'Ryan'...



Your parents are paying $0.1696 every minute for your fancy Ivy League education, so please... enjoy your freshman year of college.

abstrusegoose.com/180