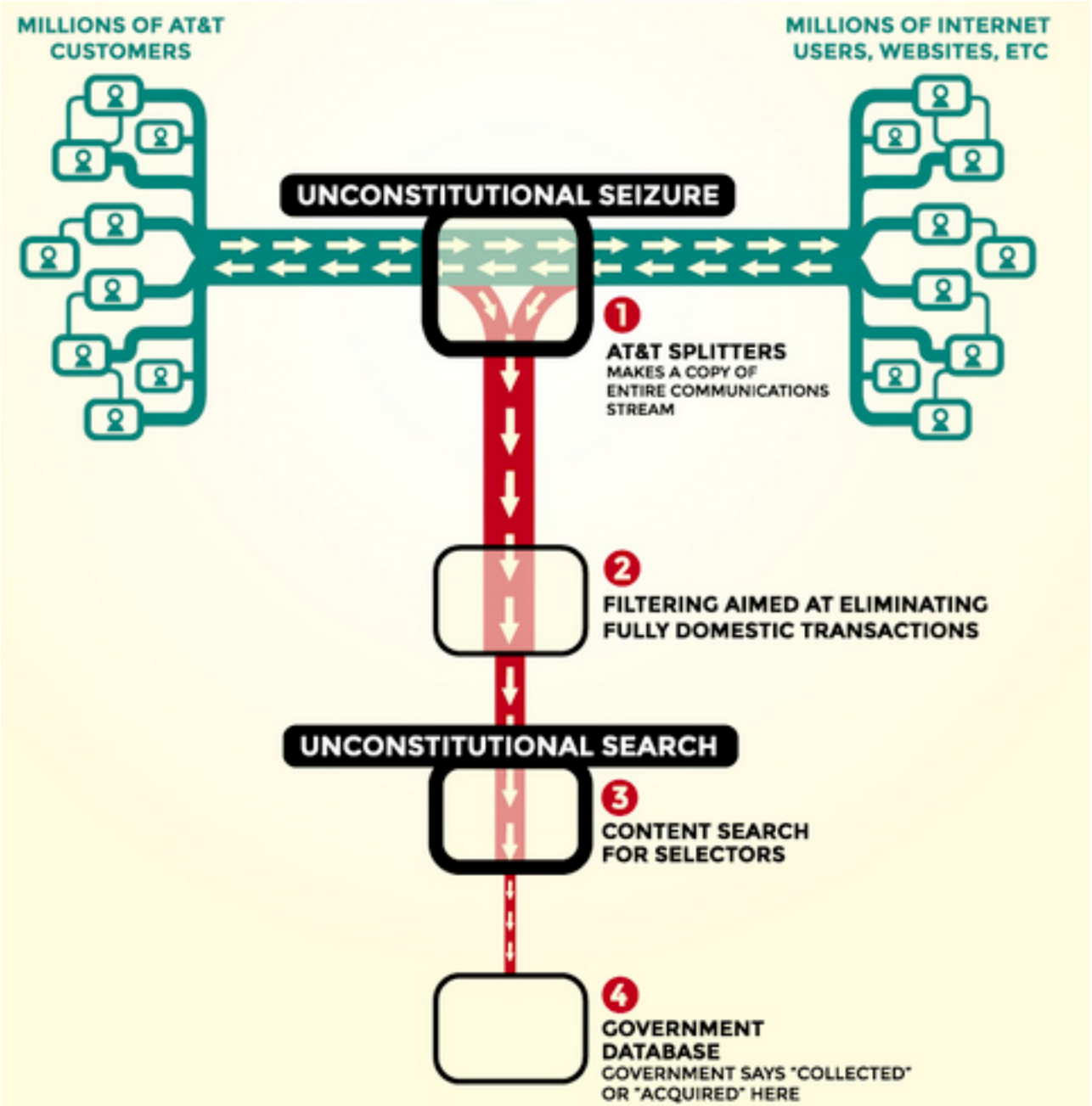
Lecture 20:
Crypto, continued

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
- called both traitor and hero in the US

Domestic Internet Backbone Surveillance (eff.org)



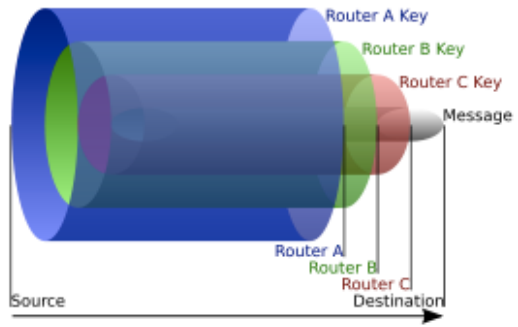
Tor: The Onion Router

- 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

Data structure [edit]

An onion is the data structure formed by "wrapping" a message with successive layers of encryption to be decrypted ("peeled" or "unwrapped") by as many intermediary computers as there are layers before arriving at its destination. The original message remains hidden as it is transferred from one node to the next, and no intermediary knows both the origin and final destination of the data, allowing the sender to remain anonymous.[12]



In this example onion, the source of the data sends the onion to Router A, which removes a layer of encryption to learn only where to send it next and where it came from (though it does not know if the sender is the origin or just another node). Router A sends it to Router B, which decrypts another layer to learn its next destination. Router B sends it to Router C, which removes the final layer of encryption and transmits the original message to its destination.

Onion creation and transmission [edit]

To create and transmit an onion, the originator selects a set of nodes from a list provided by a "directory node". The chosen nodes are arranged into a path, called a "chain" or "circuit", through which the message will be transmitted. To preserve the anonymity of the sender, no node in the circuit is able to tell whether the node before it is the originator or another intermediary like itself. Likewise, no node in the circuit is able to tell how many other nodes are in the circuit and only the final node, the "exit node", is able to determine its own location in the chain.[12]

Using asymmetric key cryptography, the originator obtains a public key from the directory node to send an encrypted message to the first ("entry") node, establishing a connection and a shared secret ("session key"). Using the established encrypted link to the entry node, the originator can then relay a message through the first node to a second node in the chain using encryption that only the second node, and not the first, can decrypt. When the second node receives the message, it establishes a connection with the first node. While this extends the encrypted link from the originator, the second node cannot determine whether the first node is the originator or just another node in the circuit. The originator can then send a message through the first and second nodes to a third node, encrypted such that only the third node is able to decrypt it. The third, as with the second, becomes linked to the originator but connects only with the second. This process can be repeated to build larger and larger chains, but is typically limited to preserve performance.[12]

When the chain is complete, the originator can send data over the Internet anonymously. When the final recipient of the data sends data back, the intermediary nodes maintain the same link back to the originator, with data again layered, but in reverse such that the final node this time removes the first layer of encryption and the first node removes the last layer of encryption before sending the data, for example a web page, to the originator.[12]

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"
- has the other desirable properties of money:
  - portable, durable, divisible, recognizable, difficult to counterfeit
- use cryptography to control the creation and transfer of money,
- don't rely on central authorities.

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

Original Bitcoin paper: 2007

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

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

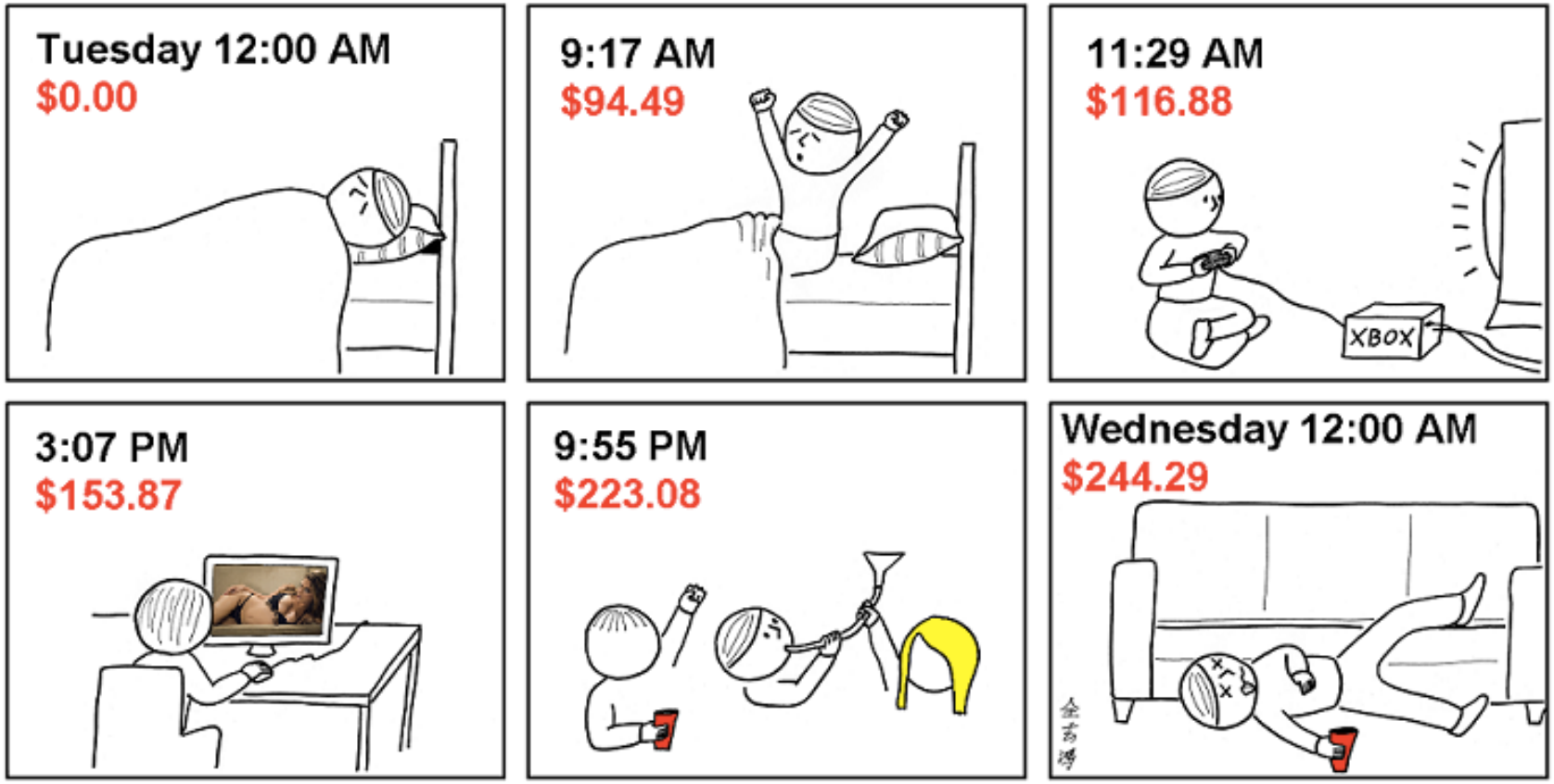
- it protects our privacy and security
  - access to computers
  - email
  - online shopping, banking, taxes
  - electronic voting
  - ...

- 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