CS 161: Computer Security

Lecture 11

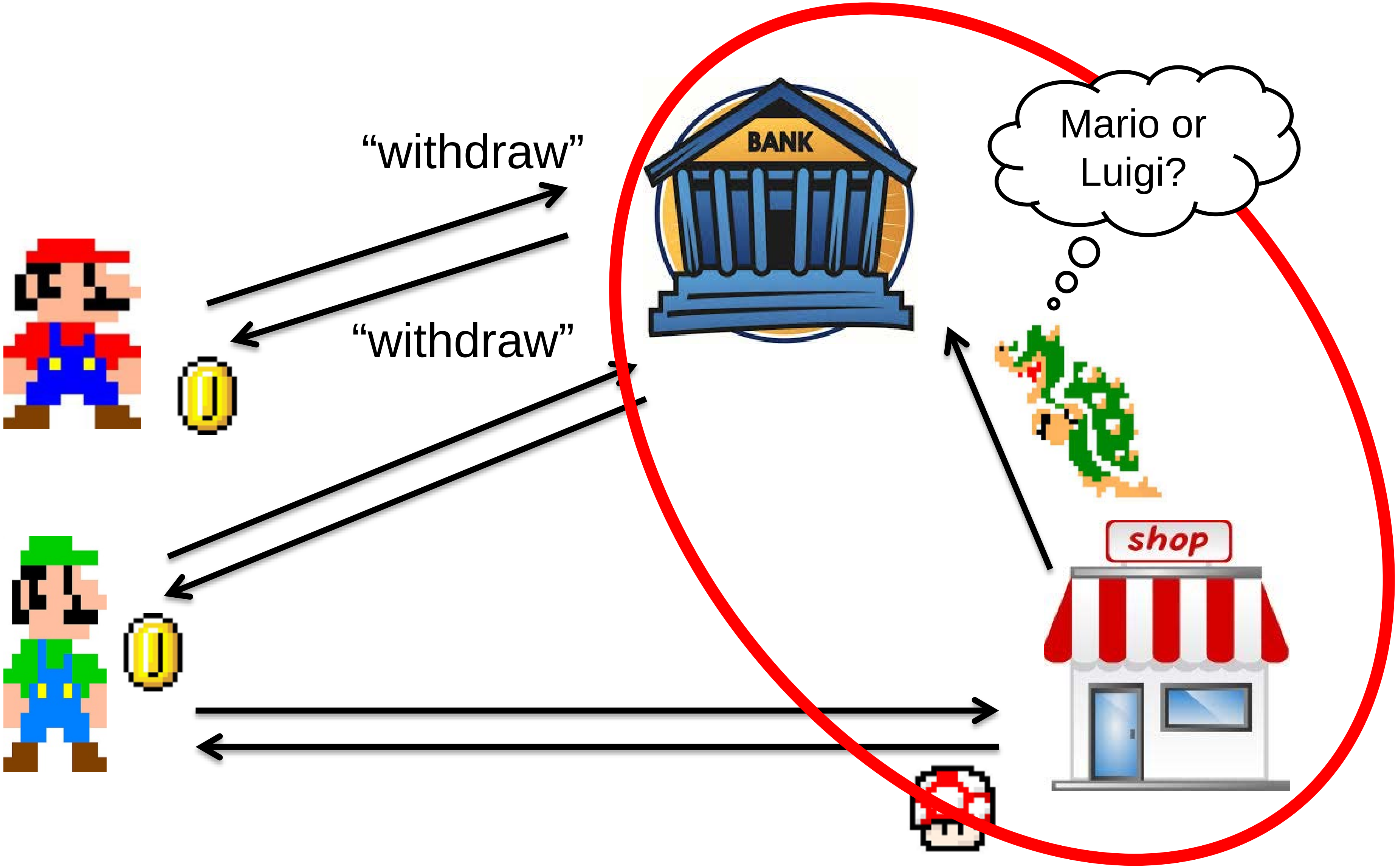
October 8, 2015

The 1990s
David Chaum and anonymous ecash

“The difference between a bad electronic cash system and well-developed digital cash will determine whether we will have a dictatorship or a real democracy”

-- Attributed to David Chaum

Anonymous payments



Chaum’s anonymous digicash

anonymous

secure (no double-spending)

only **transfer** (no creation/storage)

…and **bankrupt** in 1998

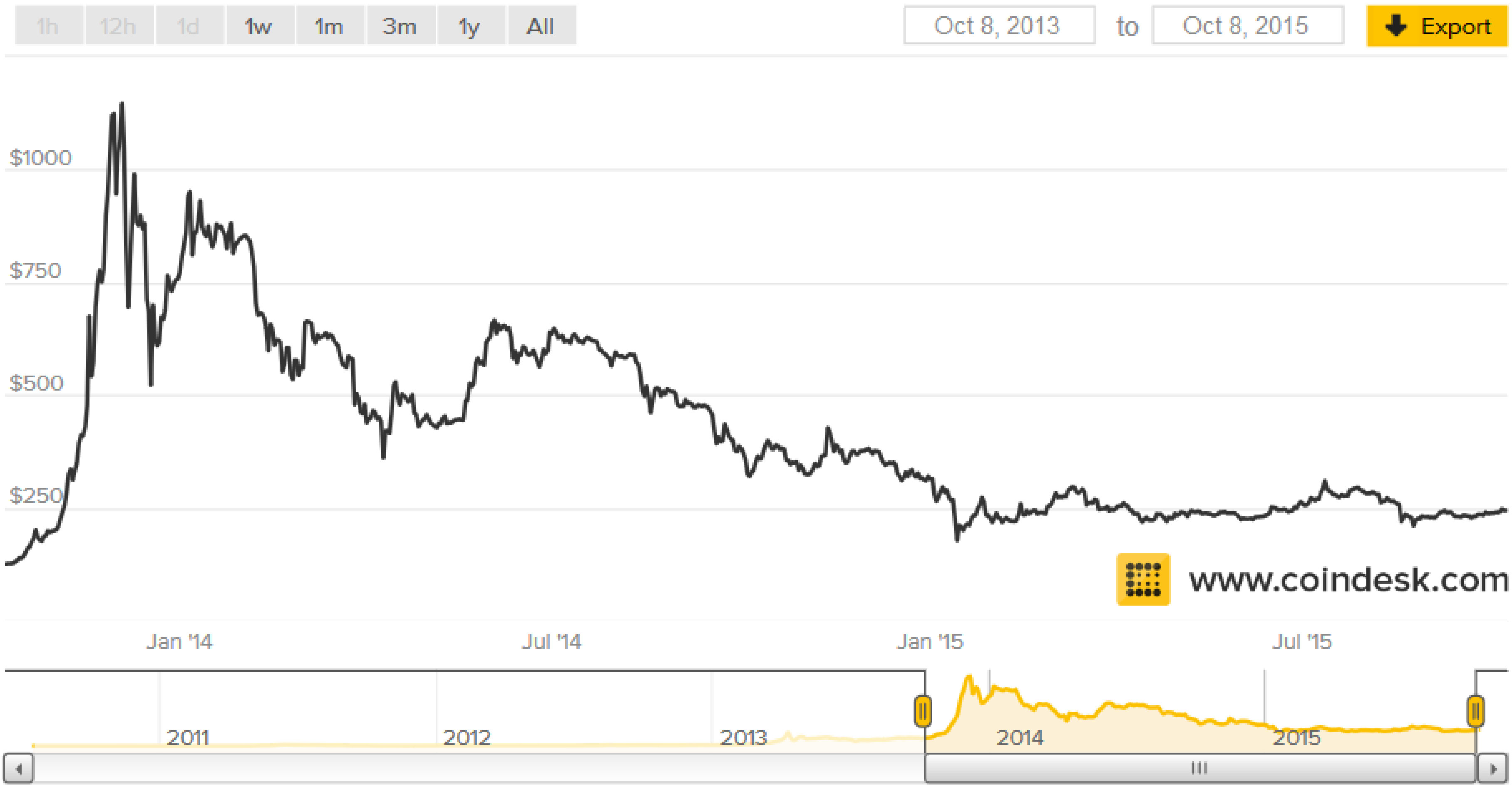
The advent of Bitcoin

- 2008: **Bitcoin announced** by Satoshi Nakamoto
  - Pseudonym for person or group of person
- 2009: First bitcoin transaction
- 2010: 10,000 bitcoins spent on a pizza (worth about $25)
- 2011: Silk Road opens
- 2013: FBI shuts down Silk Road
- 2013: **Bitcoin price skyrockets**
- 2013: China’s Central Bank bans Bitcoin transactions
- 2014: Bitcoin accepted by Paypal
- 2015: Major banks (BofA, Citi, JP Morgan, etc.) investigate using Bitcoin

Size of the Bitcoin Economy

- Bitcoins in circulation: 14.7 million
  - (October 2015)
  - Max bitcoins: 21 million
- Bitcoin transactions 100/min
  - Visa credit card transactions 200,000/minute
  - Max Visa transaction rate 1,400,000/minute

Bitcoin value over time



Oct 8, 2013 to Oct 8, 2015

Virtual currency issues

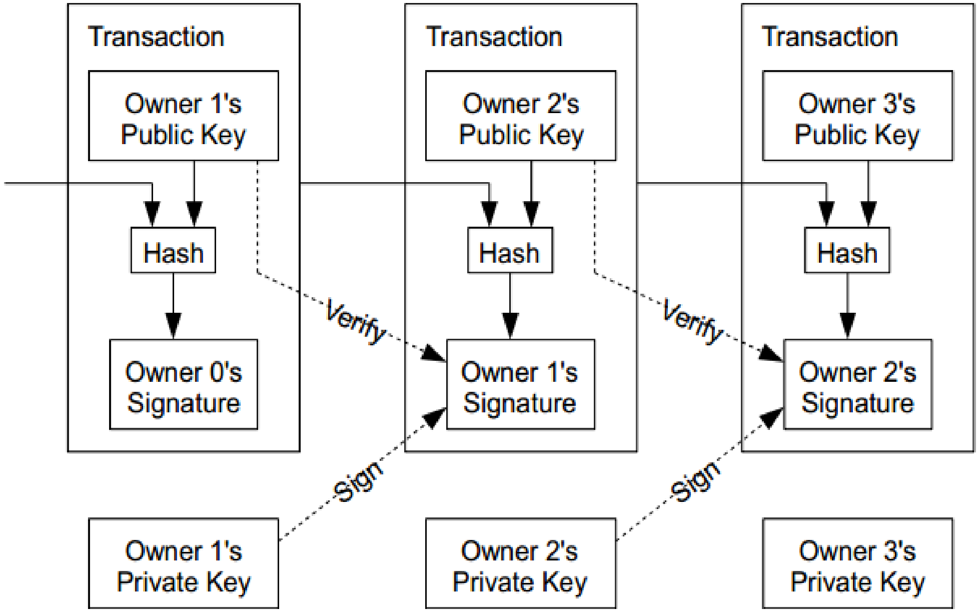
- How is virtual currency created?
- How do you prevent inflation?
- How do you test legitimacy of currency?
- How do you prevent double spending?
- Bitcoin takes a infrastructure-less approach
  - Rely on proof instead of trust
  - No central bank or clearing house

(Video references)

- Video:
  - https://www.youtube.com/watch?v=Lx9zgZCMqXE
- Write-up:
  - http://www.imponderablethings.com/2013/07/how-bitcoin-works-under-hood.html

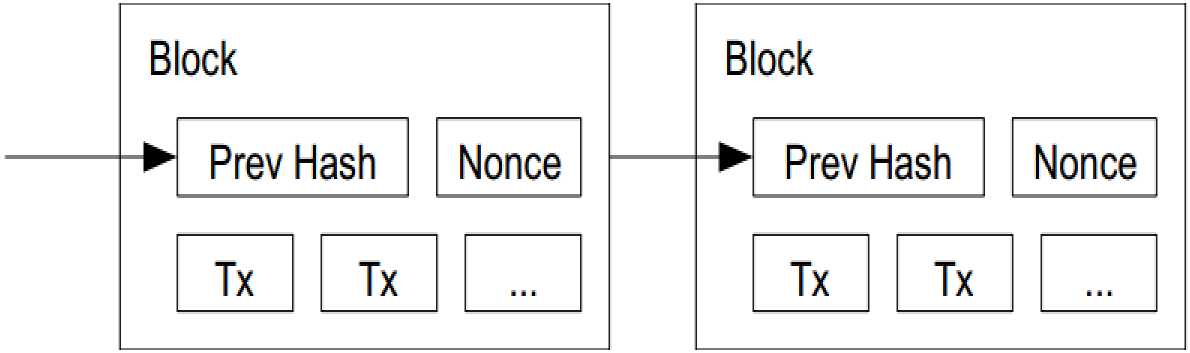
Bitcoin

- Electronic coin = chain of digital signatures
- Bitcoin transfer: Sign(Previous transaction + New owner’s public key)
- Anyone can verify (n-1)th owner transferred this to the nth owner.
- Anyone can follow the history of a bitcoin
- 1 BTC = 10^8 satoshis



Using Cryptographic Hashes

- Proof of work
  - Block contains transactions to be validated & previous hash value
  - Pick a nonce such that H(prev hash, nonce, Tx) < E
  - E is a variable that the system specifies. Find a hash value with leading bits of zero. Work exponential in number of zero bits required
  - Verification is easy. But proof-of-work is hard



Double spending

- All transactions published
- Each node (miner) verifies this is first spending of this particular bitcoin by payer
- When verified it generates proof-of-work and attaches to current chain.

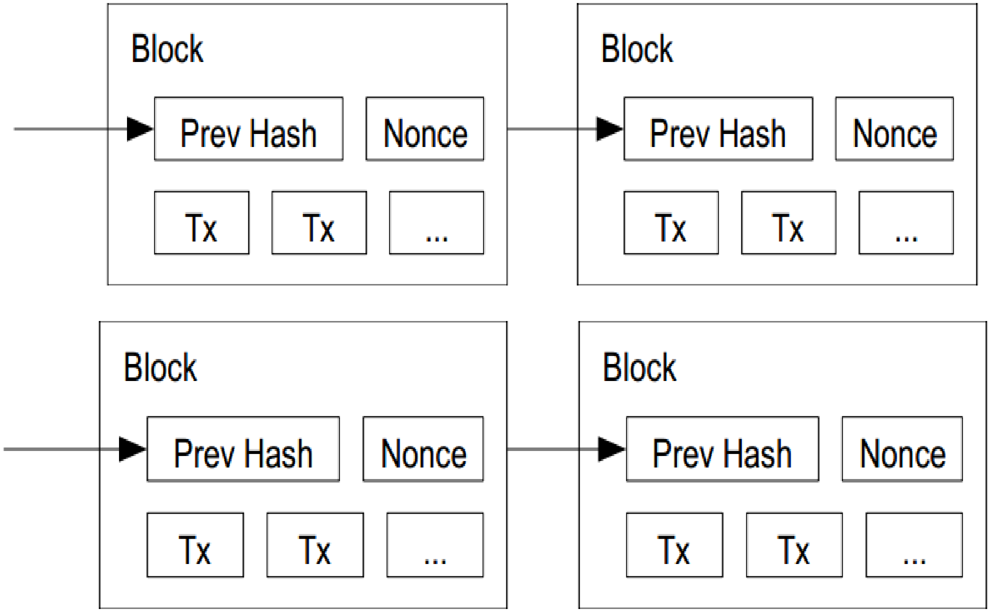
Bitcoin Network

- Each P2P node runs the following algorithm:
  - New transactions broadcast to all nodes
  - Each node collects new transactions into a block
  - Each node works on finding a proof-of-work for its block. (Lottery)
  - When node finds proof-of-work, broadcasts block to all nodes
  - Nodes accept the block only if all transactions in it are valid (digital signature checking) and not already spent (check all the transactions)
  - Nodes express their acceptance by working on next block in the chain, using the hash of the accepted block as the previous hash

Tie breaking

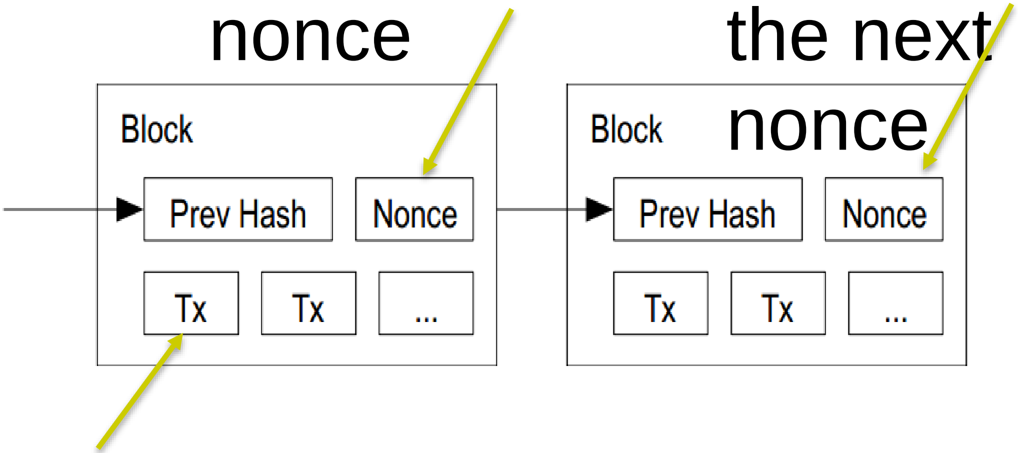
- Two nodes may find a correct block simultaneously
  - Keep both and work on the first one
  - If one grows longer than the other, take the longer one

Two different block chains (or blocks) may satisfy the required proof-of-work.



Reverting is hard…

- Reverting gets exponentially hard as the chain grows



2. Recompute nonce

3. Recompute the next nonce

1. Modify the transaction (revert or change the payer)

Mining

- Today mining is only cost-effective with ASICs
- Mining is dominated by large “mining pools”
  - GHash achieved a 55% monopoly in June
- Bitcoin users ***assume*** that no single group controls more than 50% of bitcoin mining

Verification can take time

- At least 10 mins to verify a transaction
  - Agree to pay
  - Wait for one block (10 mins) for the transaction to go through
  - For a large transaction ($$$) wait longer (more secure). For large $$$, wait for six blocks (1 hour)

Bitcoin Economics

- Rate limit new block creation
  - Adapt to “network capacity”
  - New block created every 10 mins (six blocks every hour)
    - How? Difficulty is adjusted every two weeks to keep the rate fixed as capacity/computing power increases
- N new bitcoins per each new block: credited to the miner → incentives for miners
  - N was 50 initially. In 2013, N=25
  - Halved every 210,000 blocks (every four years)
  - Total number of bitcoins will not exceed 21 million. (After this miner takes a fee)

FBI

Federal Bureau of Investigation

Intelligence

Assessment

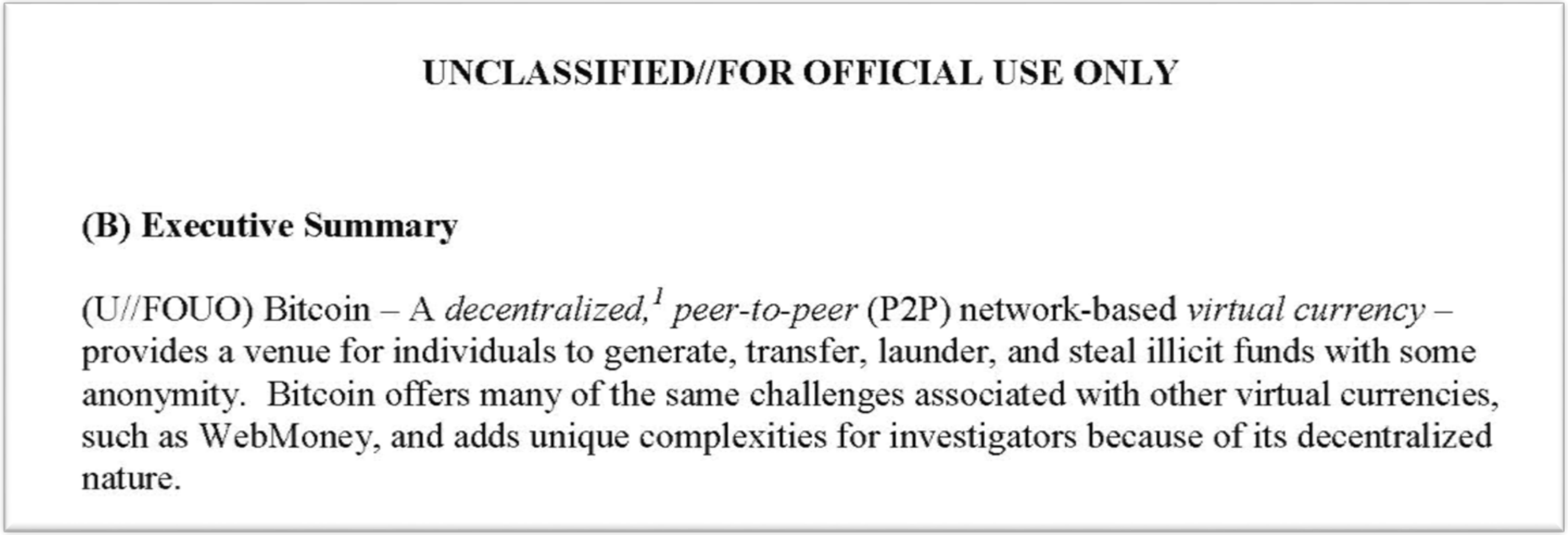
Intelligence Assessment

(U) Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity

24 April 2012

UNCLASSIFIED

FBI

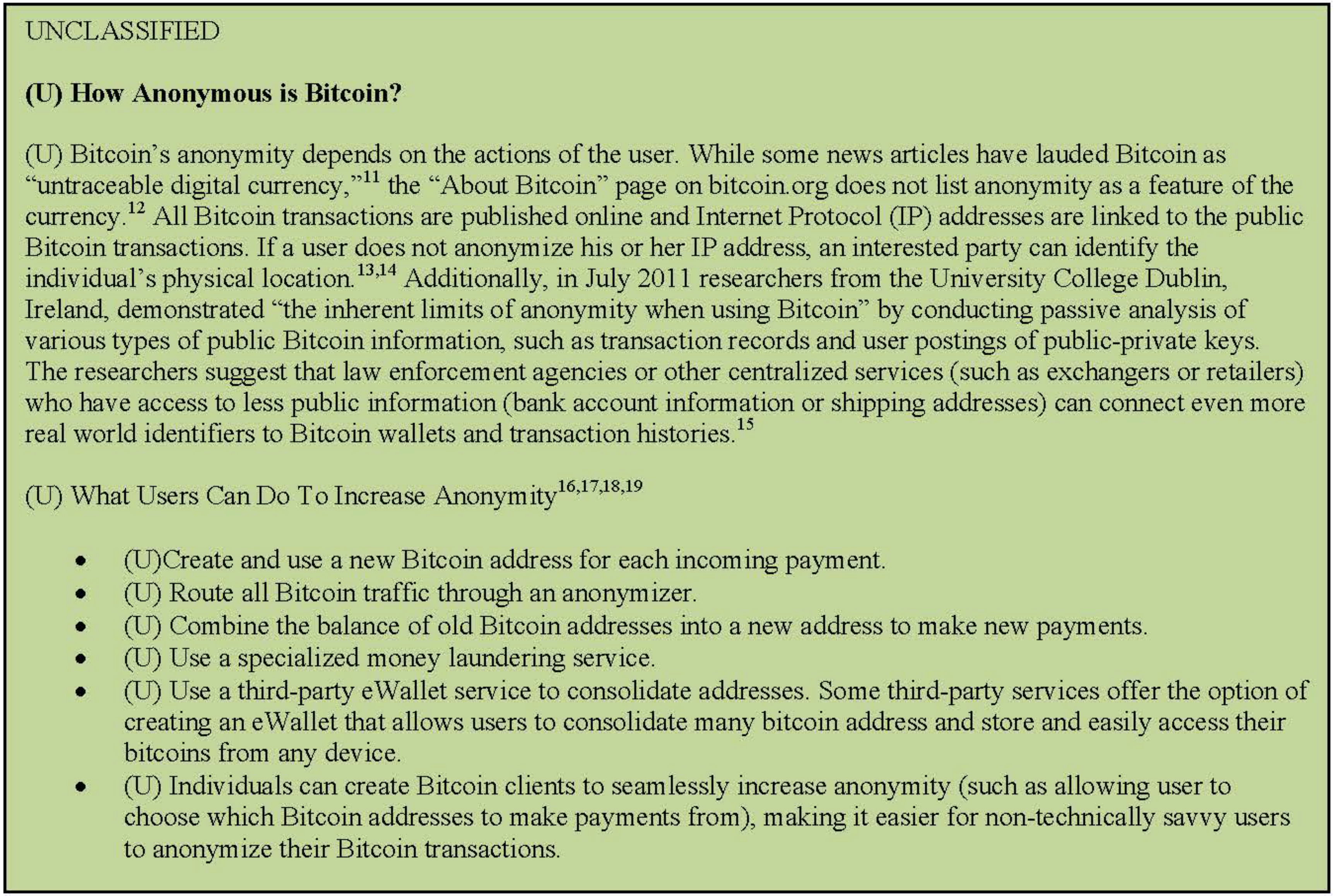


UNCLASSIFIED//FOR OFFICIAL USE ONLY

(B) Executive Summary

(U//FOUO) Bitcoin – A *decentralized,*[1] *peer-to-peer* (P2P) network-based *virtual currency* – provides a venue for individuals to generate, transfer, launder, and steal illicit funds with some anonymity. Bitcoin offers many of the same challenges associated with other virtual currencies, such as WebMoney, and adds unique complexities for investigators because of its decentralized nature.

FBI



UNCLASSIFIED

(U) How Anonymous is Bitcoin?

(U) Bitcoin's anonymity depends on the actions of the user. While some news articles have lauded Bitcoin as "untraceable digital currency,"[11] the "About Bitcoin" page on bitcoin.org does not list anonymity as a feature of the currency.[12] All Bitcoin transactions are published online and Internet Protocol (IP) addresses are linked to the public Bitcoin transactions. If a user does not anonymize his or her IP address, an interested party can identify the individual's physical location.[13,14] Additionally, in July 2011 researchers from the University College Dublin, Ireland, demonstrated "the inherent limits of anonymity when using Bitcoin" by conducting passive analysis of various types of public Bitcoin information, such as transaction records and user postings of public-private keys. The researchers suggest that law enforcement agencies or other centralized services (such as exchangers or retailers) who have access to less public information (bank account information or shipping addresses) can connect even more real world identifiers to Bitcoin wallets and transaction histories.[15]

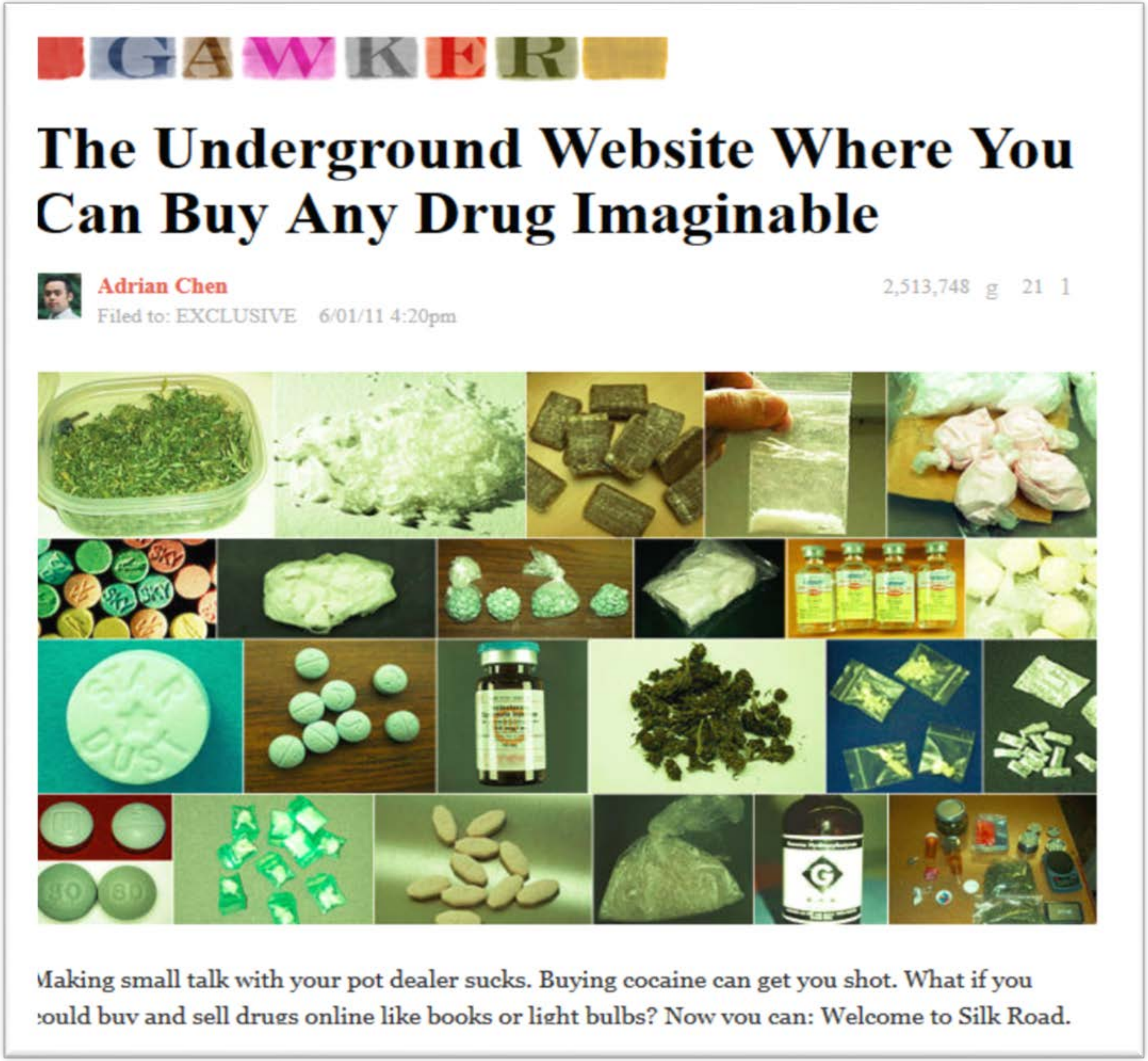
(U) What Users Can Do To Increase Anonymity[16,17,18,19]

- (U)Create and use a new Bitcoin address for each incoming payment.
- (U) Route all Bitcoin traffic through an anonymizer.
- (U) Combine the balance of old Bitcoin addresses into a new address to make new payments.
- (U) Use a specialized money laundering service.
- (U) Use a third-party eWallet service to consolidate addresses. Some third-party services offer the option of creating an eWallet that allows users to consolidate many bitcoin address and store and easily access their bitcoins from any device.
- (U) Individuals can create Bitcoin clients to seamlessly increase anonymity (such as allowing user to choose which Bitcoin addresses to make payments from), making it easier for non-technically savvy users to anonymize their Bitcoin transactions.

IRS View

- Bitcoin income is taxable
- Getting your wallet stolen and losing income is not claimable
- Rules for digital currencies are unclear
- Tax preparers do not understand digital currencies
- Bitcoin on foreign servers is foreign currency… or is it?
- Recognizes that laws need to be clarified

Silk Road



GAWKER

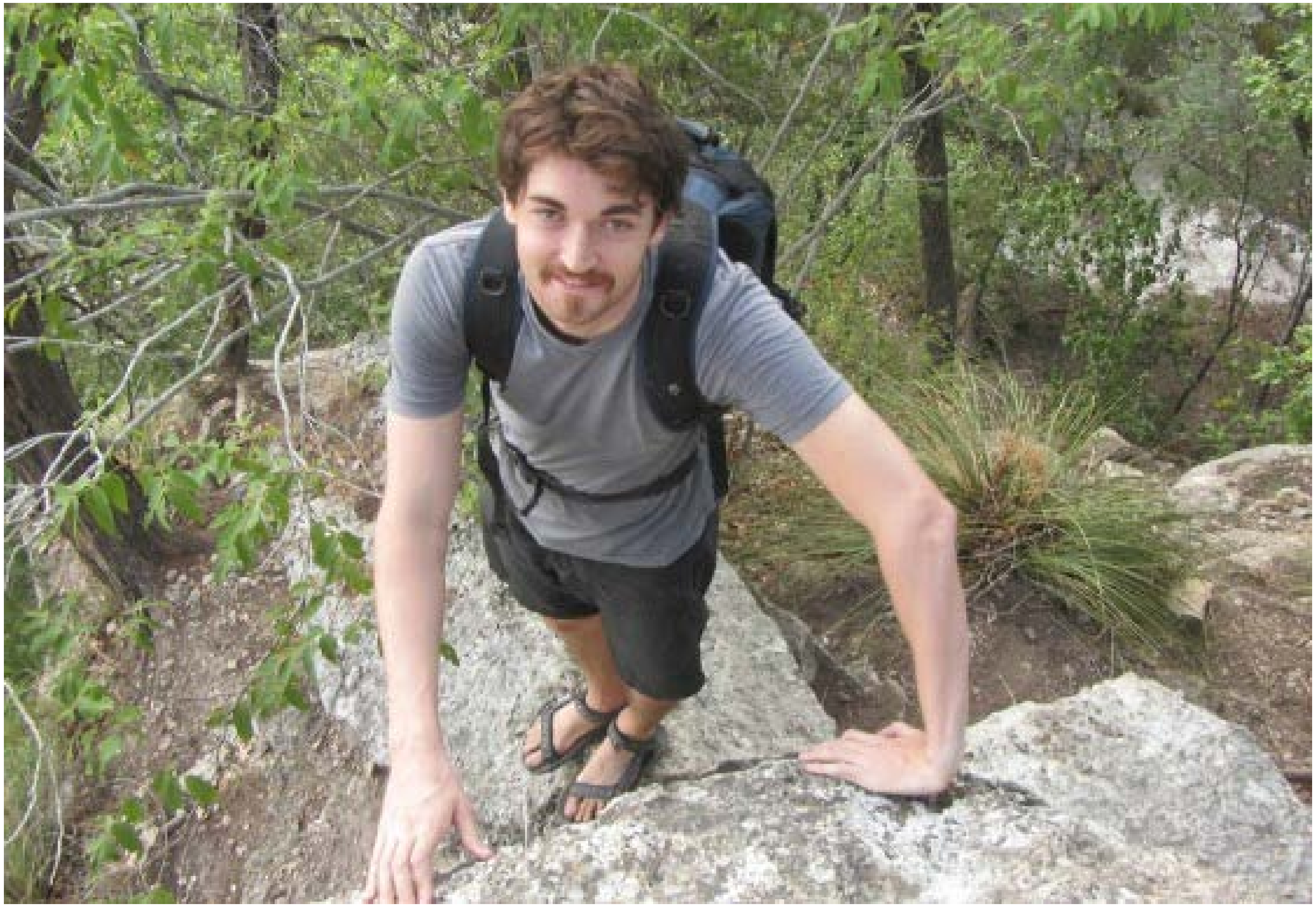
The Underground Website Where You Can Buy Any Drug Imaginable

Adrian Chen
Filed to: EXCLUSIVE 6/01/11 4:20pm

2,513,748 g 21 1

Making small talk with your pot dealer sucks. Buying cocaine can get you shot. What if you could buy and sell drugs online like books or light bulbs? Now you can: Welcome to Silk Road.

Dread Pirate Roberts (Ross Ulbricht)



Silk Road

- Silk Road only allowed purchases with bitcoins
- 70% of product offered was illegal drugs
  - (March 2013)
- Commisions 614,305 BTC ($79.8 million)
- Had 146,947 buyers 30% in the U.S.
- 3877 Vendors
- Site shutdown by FBI October 2013

Bitcoin Discussion

- What are methods for laundering bitcoins?
- Exchanging/mixing bitcoins (tumbling)
- MtGox
- Is bitcoin a short-term currency or a long-term investment?
- Is it ethical to build a system that relies upon wasting CPU cycles (and thus energy)?