KIT711
Tor and Bitcoin

Lecture 10

Anonymisation Tools

- Introduction
- Tor
- Bitcoin

Philosophy of Identity Privacy

- We know who we are
- We want the people we communicate to know that it is truly us when we communicate with them
- But
  - Do we want other people to know who we are communicating with?
  - Do we want the government to know?
  - Do we want companies to know?

Philosophy of Identity Privacy

- In the context of us communicating, what types of communications do we send? Or are people likely to send?
  - Purchasing products
  - Personal details or information
  - Political opinion
  - Private company information
  - Whistle blowing

Philosophy of Identity Privacy

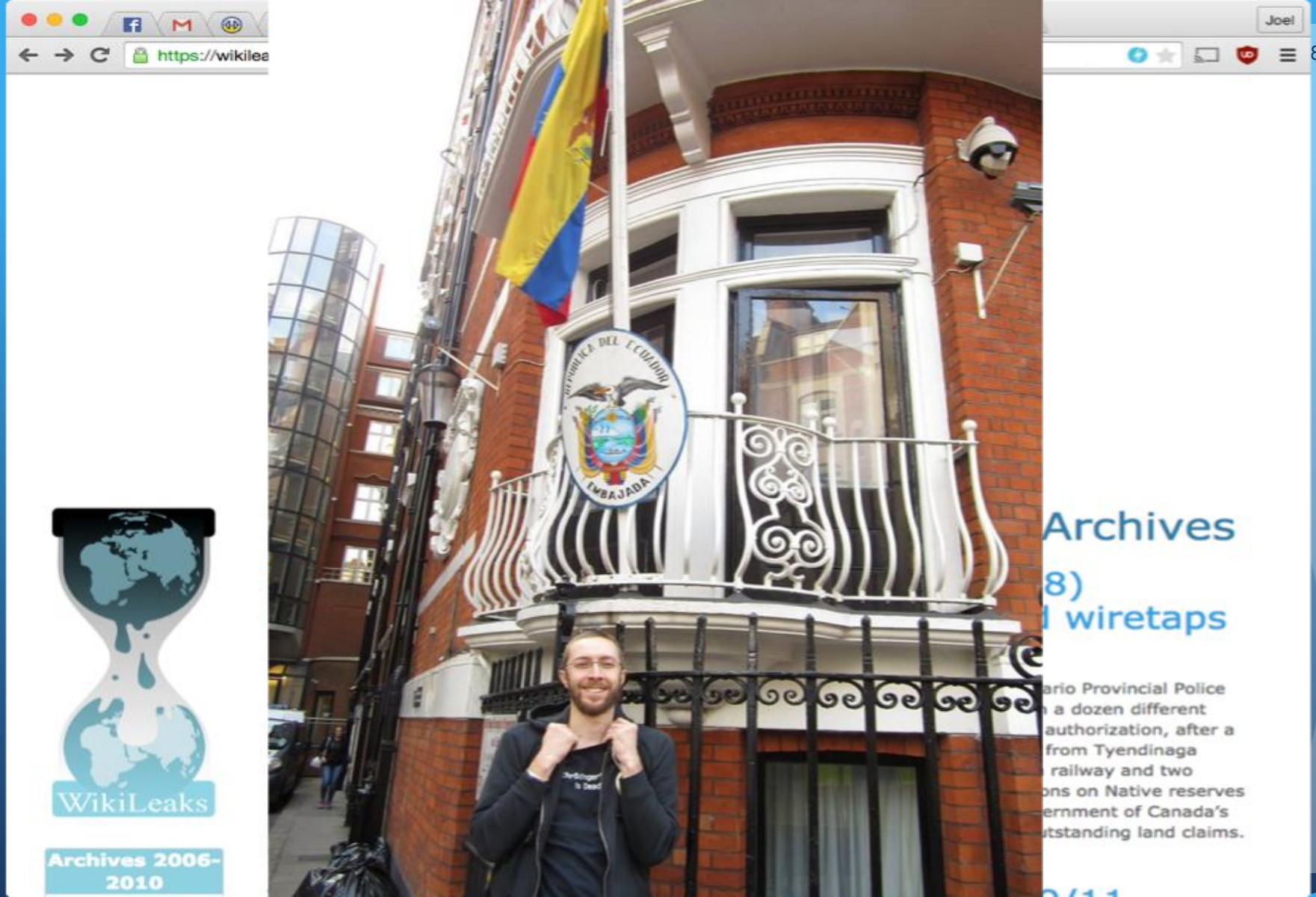
- So far in this unit we have talked about VPNs
  - These keep the data private, and provide authentication
- Privacy concerning location/identity of users is usually ignored
  - Or helps us to pretend to be somewhere we aren't but rather simplistic
- Inherently a difficult problem, since location and identity are usually core to routing and delivery
- SSL to purchase item from a business may result in them having our financial details

Philosophy of Identity Privacy

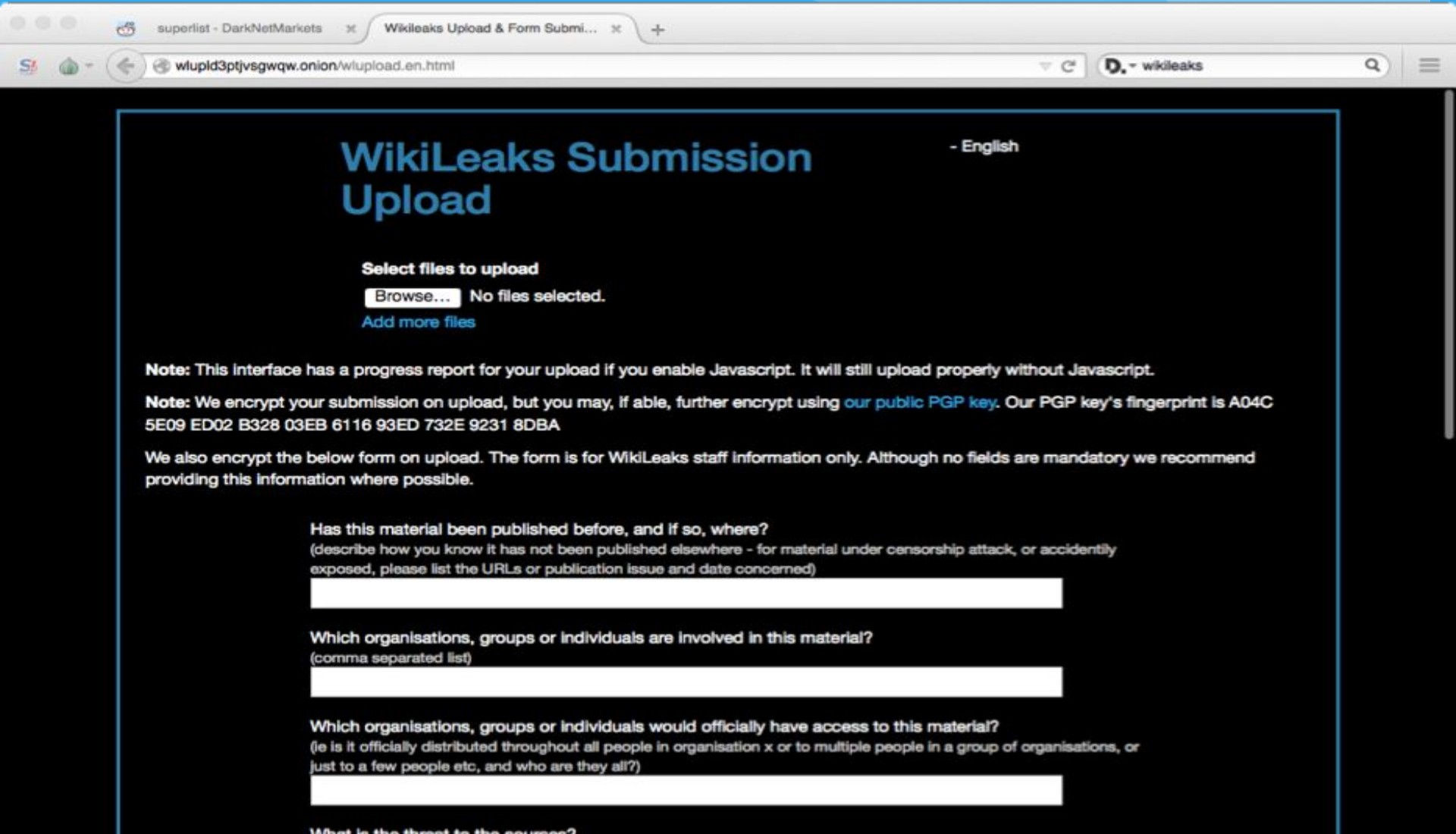
- In this lecture we are going to consider two different cryptographic tools that address these two major issues
- Tor
  - Aims to hide our geographic location in a more robust system than a point to point VPN solution
- Bitcoin
  - Anonymises our payment details

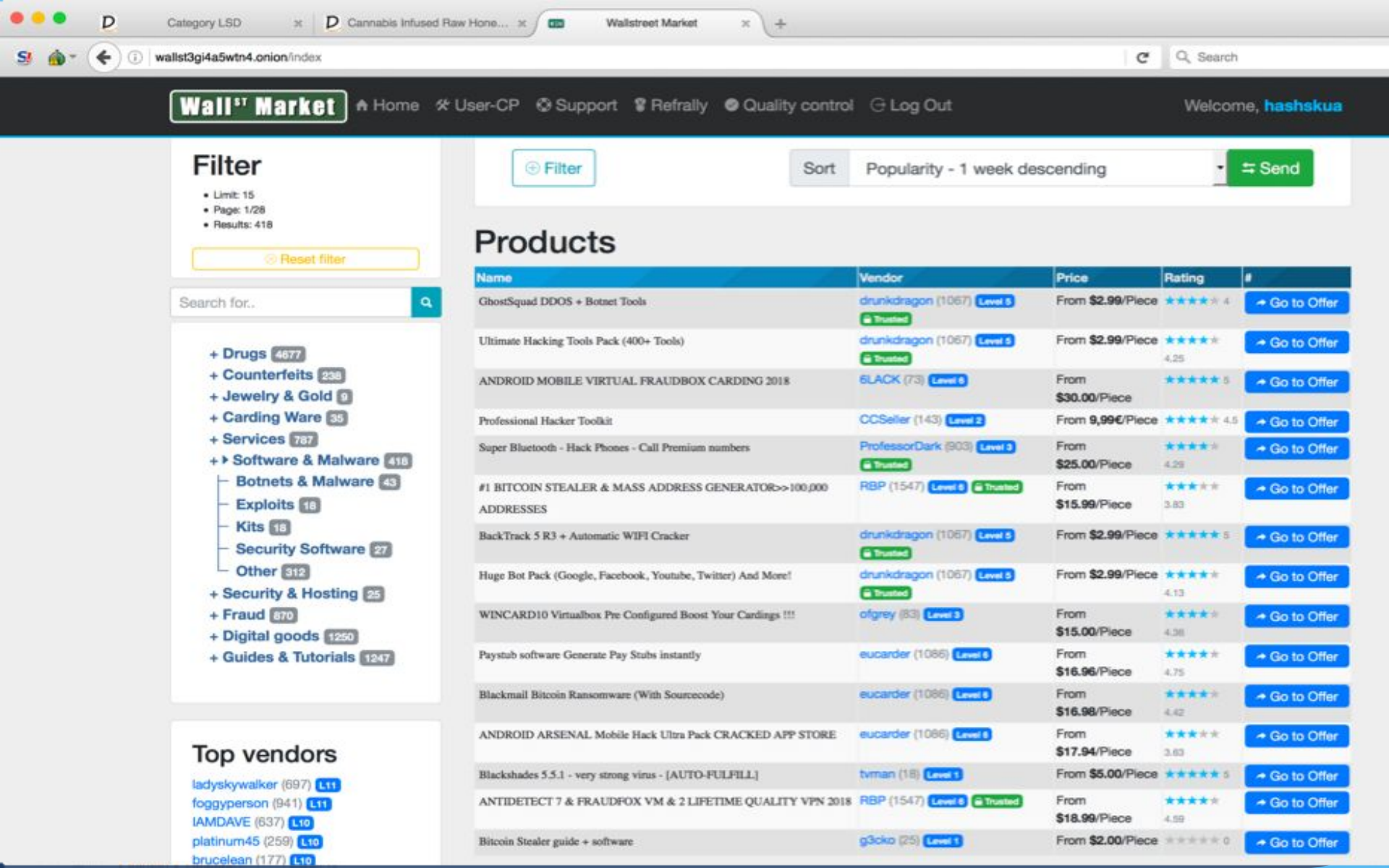
Tor

- “If you’re not doing anything wrong, you shouldn’t have anything to hide.”
  - Implies that anonymous communication is for criminals
- The truth: who uses Tor?
  - Journalists
  - Law enforcement
  - Human rights activists
  - Normal people
  - Business executives
  - Military / Intelligence Personnel
  - Abuse Victims
- Tor was/is developed by the U.S Navy


Joel
https://wikilea
WikiLeaks
Archives 2006-2010
Archives
8)
wiretaps
ario Provincial Police
a dozen different
authorization, after a
from Tyendinaga
railway and two
ons on Native reserves
ernment of Canada's
tstanding land claims.

wlupld3ptjvsgwqw.onion




Category LSD
Cannabis Infused Raw Hone...
Wallstreet Market
wallst3gi4a5wtn4.onion/index
Search
Wall ST Market
Home
User-CP
Support
Refrally
Quality control
Log Out
Welcome, hashskua
Filter
Limit: 15
Page: 1/28
Results: 418
Reset filter
Search for..
+ Drugs 4677
+ Counterfeits 238
+ Jewelry & Gold 9
+ Carding Ware 35
+ Services 787
+ Software & Malware 418
Botnets & Malware 43
Exploits 18
Kits 18
Security Software 27
Other 312
+ Security & Hosting 25
+ Fraud 870
+ Digital goods 1250
+ Guides & Tutorials 1247
Top vendors
ladyskywalker (697) L11
foggyperson (941) L11
IAMDAVE (637) L10
platinum45 (259) L10
brucelean (177) L10
Filter
Sort
Popularity - 1 week descending
Send
Products
Name
Vendor
Price
Rating
#
GhostSquad DDOS + Botnet Tools
drunkdragon (1067) Level 5 Trusted
From $2.99/Piece
Go to Offer
Ultimate Hacking Tools Pack (400+ Tools)
drunkdragon (1067) Level 5 Trusted
From $2.99/Piece
4.25
Go to Offer
ANDROID MOBILE VIRTUAL FRAUDBOX CARDING 2018
6LACK (73) Level 6
From $30.00/Piece
Go to Offer
Professional Hacker Toolkit
CCSeller (143) Level 2
From 9,99€/Piece
4.5
Go to Offer
Super Bluetooth - Hack Phones - Call Premium numbers
ProfessorDark (903) Level 3 Trusted
From $25.00/Piece
4.29
Go to Offer
#1 BITCOIN STEALER & MASS ADDRESS GENERATOR>>100,000 ADDRESSES
RBP (1547) Level 6 Trusted
From $15.99/Piece
3.83
Go to Offer
BackTrack 5 R3 + Automatic WIFI Cracker
drunkdragon (1067) Level 5 Trusted
From $2.99/Piece
Go to Offer
Huge Bot Pack (Google, Facebook, Youtube, Twitter) And More!
drunkdragon (1067) Level 5 Trusted
From $2.99/Piece
4.13
Go to Offer
WINCARD10 Virtualbox Pre Configured Boost Your Cardings !!!
ofgrey (83) Level 3
From $15.00/Piece
4.38
Go to Offer
Paystub software Generate Pay Stubs instantly
eucarder (1086) Level 6
From $16.96/Piece
4.75
Go to Offer
Blackmail Bitcoin Ransomware (With Sourcecode)
eucarder (1086) Level 6
From $16.98/Piece
4.42
Go to Offer
ANDROID ARSENAL Mobile Hack Ultra Pack CRACKED APP STORE
eucarder (1086) Level 6
From $17.94/Piece
3.63
Go to Offer
Blackshades 5.5.1 - very strong virus - [AUTO-FULFILL]
tvman (18) Level 1
From $5.00/Piece
Go to Offer
ANTIDETECT 7 & FRAUDFOX VM & 2 LIFETIME QUALITY VPN 2018
RBP (1547) Level 6 Trusted
From $18.99/Piece
4.59
Go to Offer
Bitcoin Stealer guide + software
g3cko (25) Level 1
From $2.00/Piece
Go to Offer

Category LSD | LSD 100ug Tabs x 10 | Cannabis Infused Raw Hone...

4buzlb3uhrjby2sb.onion/viewProduct?offer=90532.32190

Search

Dream Market

lchudifyeqm4ldjj.onion
Established 2013

Shop | Messages: 0 | hashskua

Bitcoin (BTC) ฿0 | 0 | Logout

Browse by category

- Drugs 62120
  - Psychedelics 4237
    - 2C 540
    - 5-MeO 43
    - DMT 261
    - **LSD 2606**
    - Mescaline 73
    - Mushrooms 308
    - NB 93
    - Other 97
    - Salvia 31
    - Spores 34
- Digital Goods 50886
- Drugs 62120
- Drugs Paraphernalia 316
- Services 4273
- Other 4032

Onion mirrors

4buzlb3uhrjby2sb.onion
verified

jd6yhuwcivehvdt4.onion
t3e6ly3uoif4zcw2.onion
7ep7acrkunzdcw3l.onion
vilpaqbrnvizecjo.onion
igyifrhnvxq33sy5.onion
6qlocfg6zq2kyacl.onion
x3x2dwb7jasax6tq.onion
bkjcpa2klkkmowwq.onion

LSD 100ug Tabs x 10

Vendor Dr_Seuss (1800) (4.97★) (1000, 4.79/5) (฿ 87/1/9) (417/2/1) (0, N/A)
Price ฿0.00341 ($30.16)
Ships to Europe, Worldwide
Ships from UK
Escrow Yes

Product description

This auction is for 10 LSD tabs, dosed at 100ug, measuring 8x8mm each. This is a UK listing, shipping to the EU and North America only, via Royal Mail 1st Class, no tracking available, no signature required.

Please read this listing, check the top of our profile for important updates, and read Section 3 of our profile (regarding shipping and correct address format) in full, BEFORE ORDERING!

Finally we have completed work on our new DS-2.0 crystal, using an improved flash chromatography purification process to achieve 99% purity. This is the first batch of our DS-2.0 crystal, laid on our classic 100ug blotter art, and the results speak for themselves.

Links

- Forum
- Help
- Conferences
- Vendor application
- Earn money

฿ Exchange

BTC	1.0
mBTC	1000.0
BCH	7.8
XMR	35.1
USD	8841.0
EUR	7218.9
GBP	6316.6
CAD	11507.0
AUD	11543.1
mBCH	7828.0
SEK	73655.3
NOK	69208.4
DKK	53767.0
TRY	35373.0
CNH	56250.8
HKD	69858.1
RUB	509155.3
INR	578840.2
JPY	934137.3

News

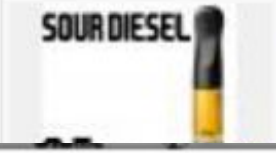
- New forum 06/02/2018
- Downtime & Recovery 13/09/2017
- Deposit delays 27/10/2016
- Forum under maintainance 12/08/2016

Category Drugs | Cannabis Infused Raw Hone...

4buzlb3uhrjby2sb.onion/?category=104

Search

0.5ml Organic THC Vape Pen Cartridge. Sour Diesel



฿0.002117
party.makerrr (120) (4.99★)
US → US

4GR PURE #3HEROIN *** FREE SHIPPING ***

฿0.01976
DutchTurtles (220) (4.74★)
NL → WW, EU

Order

★ 3.5g ★PREMIUM WEED ✓ FREESHIP

฿0.00531
AUD 61.36
Vendor
GreenCo (4600) (4.94★)
Ships to Australia, Australia
Ships from AUSTRALIA
Escrow Yes

View offer

OMO

฿0.00282
etofiesta (1450) (4.62★)
DE → WW

Order

฿0.0329
tBear707 (2400) (4.94★)
US → US

Order

✲ 5G Pure R-Ketamine

฿0.01944
Deutsche-Post (80) (4.80★)
DE → DE

Order

☆25g prenium marocan pur hash skuf hight qua

฿0.01613
mmice (500) (4.82★)
FR → EU

Order

Ecstasy Tablets Masterchef x 50

(10x) XTC Neon-Yellow Zwitsal 270mg MDMA (STRONG)

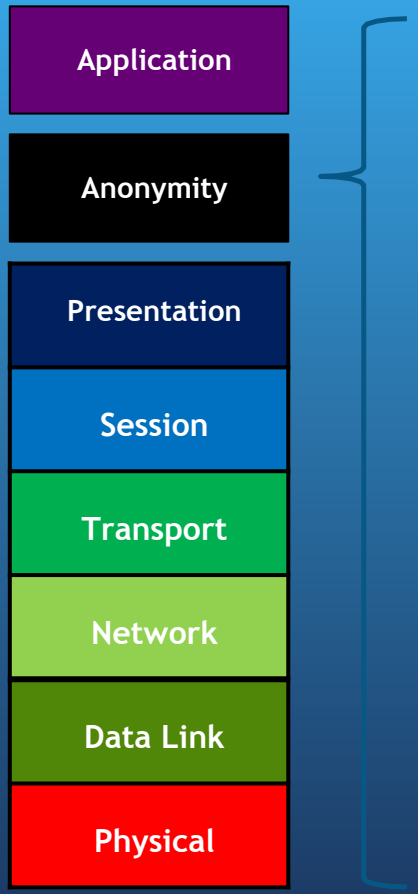
Deployment and Statistics

- Largest, most well deployed anonymity preserving service on the Internet
  - Publicly available since 2002
  - Continues to be developed and improved
- Currently ~7000 Tor relays around the world
  - All relays are run by volunteers
  - It is suspected that some are controlled by intelligence agencies
- 2 million daily users globally
  - 25-30k users daily in Australia

Top 10 Countries by Usage

Country	Mean daily users
Germany	909846 (29.89 %)
United States	447007 (14.68 %)
United Arab Emirates	346244 (11.37 %)
Russia	243919 (8.01 %)
Ukraine	119519 (3.93 %)
France	89137 (2.93 %)
Indonesia	77466 (2.54 %)
United Kingdom	64664 (2.12 %)
Netherlands	55940 (1.84 %)
Canada	43073 (1.41 %)

Adding an Anonymity Layer to OSI



- Function:
  - Hide the source, destination, and content of Internet flows from eavesdroppers
- Key challenge:
  - Defining and quantifying anonymity
  - Building systems that are resilient to deanonymization
  - Maintaining performance

Quantifying Anonymity

- How can we calculate how anonymous we are?
  - Larger anonymity set = stronger anonymity

Crowds

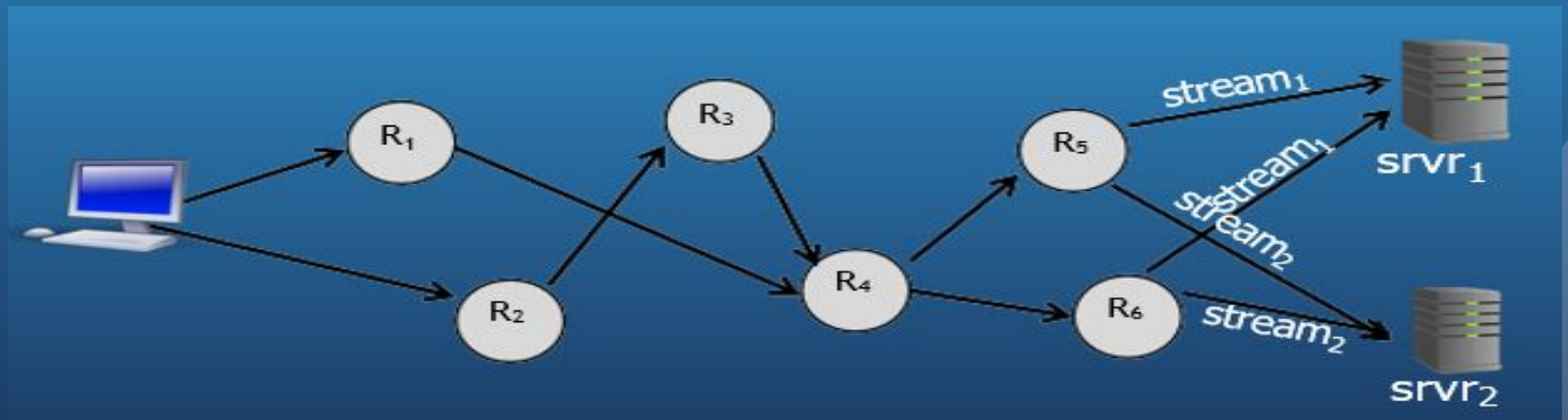
- Key idea
  - Users' traffic blends into a crowd of users
  - Eavesdroppers and end-hosts don't know which user originated what traffic
- High-level implementation
  - Every user runs a proxy on their system

Unlinkability and Unobservability

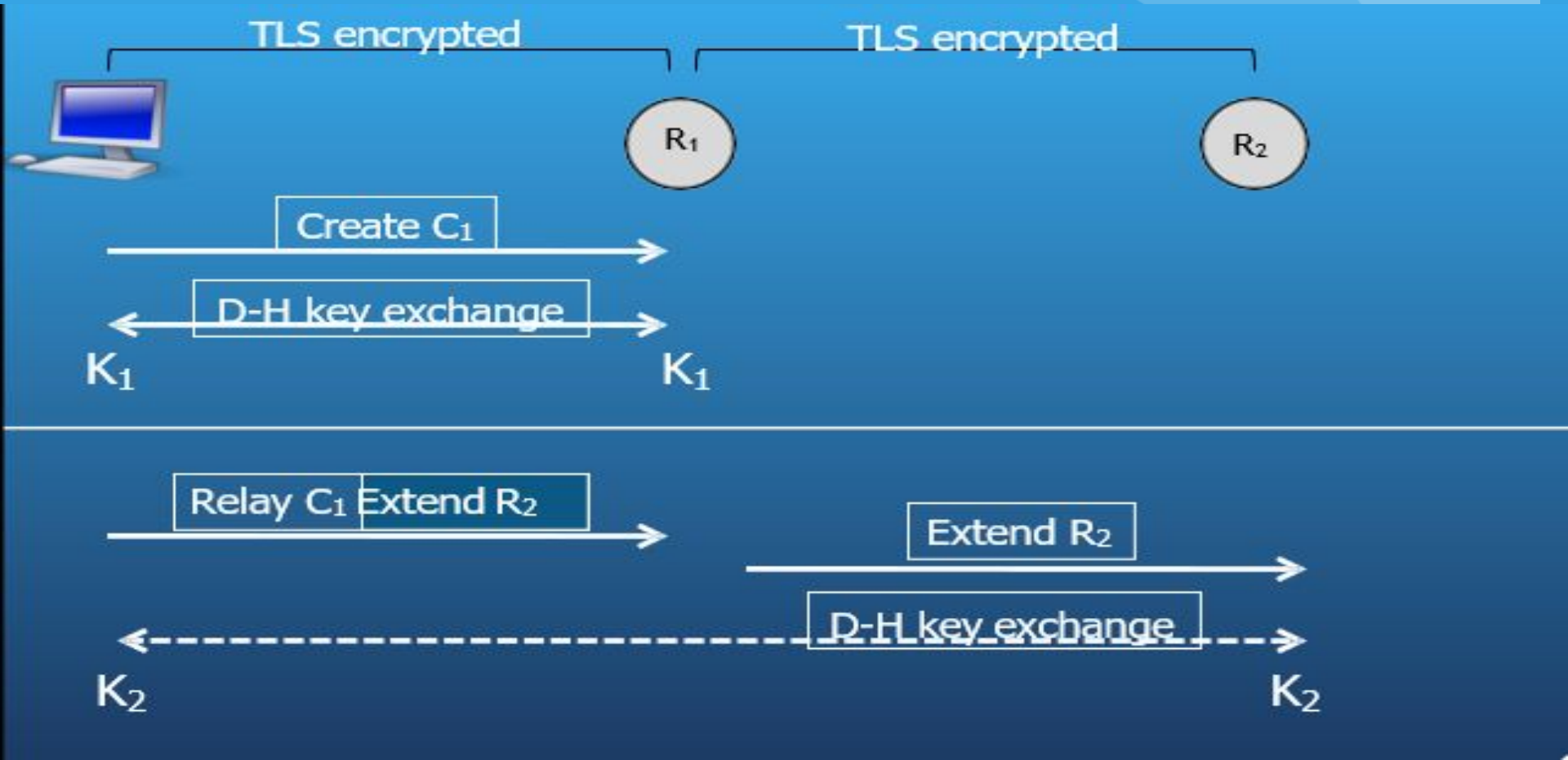
- Unlinkability
  - From the adversaries perspective, the inability the link two or more items of interest
    - E.g. packets, events, people, actions, etc.
  - Three parts:
    - Sender anonymity (who sent this?)
    - Receiver anonymity (who is the destination?)
    - Relationship anonymity (are sender A and receiver B linked?)
- Unobservability
  - From the adversaries perspective, items of interest are indistinguishable from all other items

The Tor design

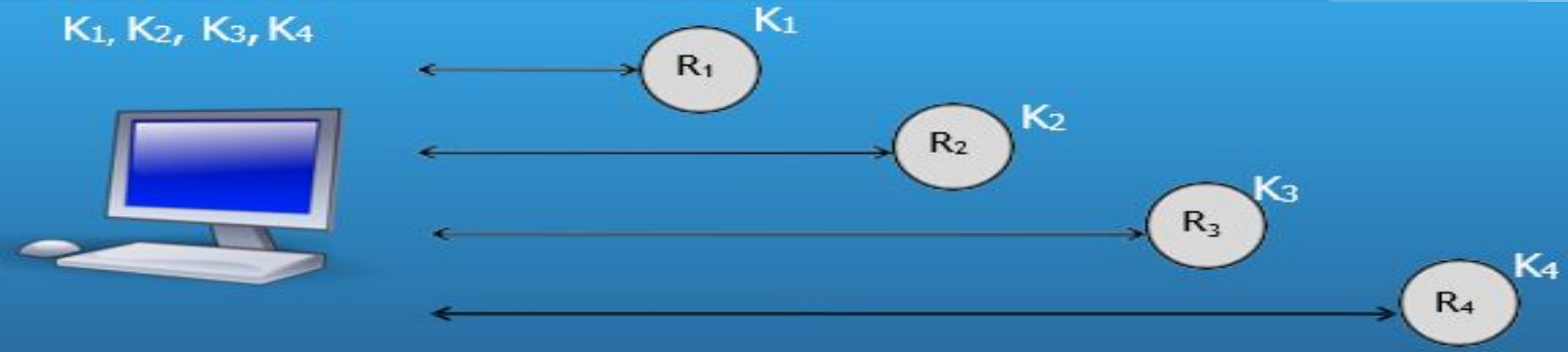
- Trusted directory contains list of Tor routers
- User's machine primitively creates a circuit
  - Used for many TCP streams
  - New circuit is created once a minute



Creating Circuits

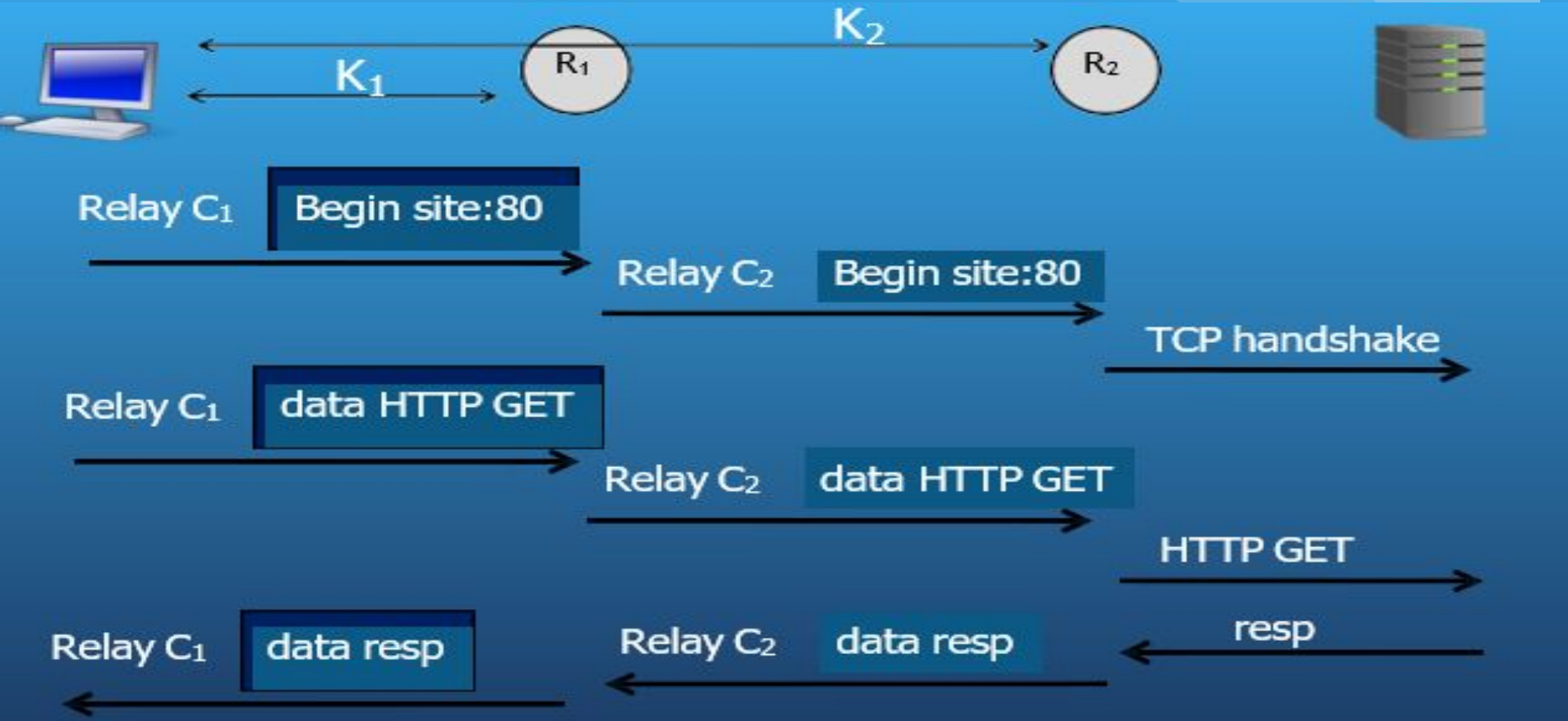


One circuit is created

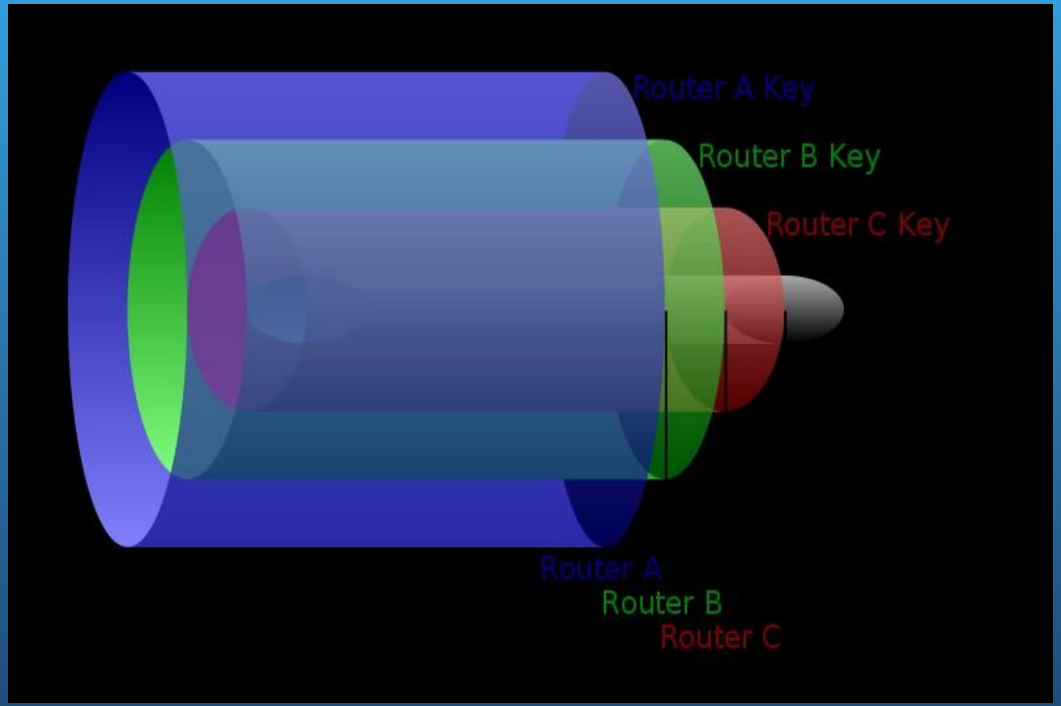


- User has shared key with each router in circuit
- Routers only know ID of successor and predecessor

Sending Data



Encrypted Channel



General Properties

- Performance:
  - Fast connection time: circuit is pre-established
  - Traffic encrypted with AES: no pub-key on traffic
- Tor crypto:
  - Provides end-to-end integrity for traffic
  - Forward secrecy via TLS

Traffic Mix

- Mix collects messages for t seconds
- Messages are randomly shuffled and sent in a different order
- Hinders timing attacks
  - Messages may be artificially delayed
  - Temporal correlation is warped
- Problems:
  - Requires lots of traffic
  - Adds latency to network flows

Dummy Traffic

- To add further to the confusing factor of the system for an outside observers dummy traffic is also sent
- A circuit is established, sending data through the overlay network, but it never leaves
  - No goal
- So our Tor client will establish a circuit, and then on the final node there is no final packet to deliver

Tor Bridges

- Anyone can look up the IP addresses of Tor relays
  - Public information in the consensus file
- Many countries block traffic to these IPs
  - Essentially a denial-of-service against Tor
- Solution: Tor Bridges
  - Essentially, Tor proxies that are not publicly known
  - Used to connect clients in censored areas to the rest of the Tor network
- Tor maintains bridges in many countries

How Do You Use Tor?

1. Download, install, and execute the Tor client
   - The client acts as a SOCKS proxy
   - The client builds and maintains circuits of relays
   - Configure your browser to use the Tor client as a proxy
2. Any app that supports SOCKS proxies will work with Tor
3. All traffic from the browser will now be routed through the Tor overlay

Tor Summary

- Tor, or onion routing, is a protocol that aims to hide where packets are coming from on the Internet
- It is achieved by the usage of a circuit route in packet delivery which encrypted the packet multiple times
  - Each onion router only knows the previous hop, and the next hop, not the source or destination

What is Blockchain

- An append-only sequential data structure comprised of hash pointers in a linked list of blocks
- Usually this data structure is distributed
  - (some, in business contexts might opt to do a centralised chain, but this is not the norm)
- As it is append only, can't alter the past, without then recreating every thing in the list since then- and as distributed you need everyone else to agree to change
  - So won't happen, that is by design

Consensus Mechanisms

- Proof of Work
  - Most common
  - Bitcoin uses this, and we will explain how it works shortly
- Proof of Stake
  - Stake holders start with coins, and are selected to add blocks, getting paid by transaction fee
  - If attempt something bad they lose coins
    - Chance of being selected to add block based on number of coins

Consensus Mechanisms

- Proof of Burn
- Proof of Activity
- Proof of Capacity
- Proof of Space

Three “Levels” of Blockchain

- Storage for digital records
- Exchanging digital assets (called tokens)
- Executing smart contracts
  - Ground rules – Terms & conditions recorded in code
  - Distributed network executes contract & monitors compliance
  - Outcomes are automatically validated without third party

Storage

- Core fundamental is the Ledger
- This provides a public* record of the data being stored, or at least the process of its storage
  - * there are now some proprietary blockchains, and even private blockchains, is this context they aren't actually public, but they are visible to the stakeholders
- Core fundamental goal of most ledgers is integrity

Tokens

- A broader use is supported by the digital infrastructure introduced through Bitcoin, as represented by “tokens”
- Tokens may use similar codebases but different blockchain databases
- Token buyers are buying private keys, which are similar to API keys
- Tokens have a value and therefore a price
- Tokens can be sold internationally over the internet and are always open for business
  - Tokens decentralize the funding / control

Smart Contracts

- Current paper-based systems drive $18 trillion in transactions per year
  - Project I am on (mentioned in lecture to CTS a few weeks back) is about using smart contracts in the supply chain of lobster sales from Tasmania into China
- Consensus protocols are key to determining the sequence of actions resulting from the contract's code
  - Enables peer-to-peer trading of everything from renewable energy to automated hotel room bookings.

Bitcoin Whitepaper – 2008.10.31

Bitcoin: A Peer-to-Peer Electronic Cash System

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

Bitcoin

- Bitcoin is a crypto-currency, meaning it relies on mathematical encryption rather than a central bank for regulation
- Bitcoin are virtually impossible to duplicate or forge due to incredibly complicated mathematical encryption
- Bitcoin circulation is completely digital
- Completely peer to peer. That means instant, untraceable transmissions with no middleman

Bitcoin

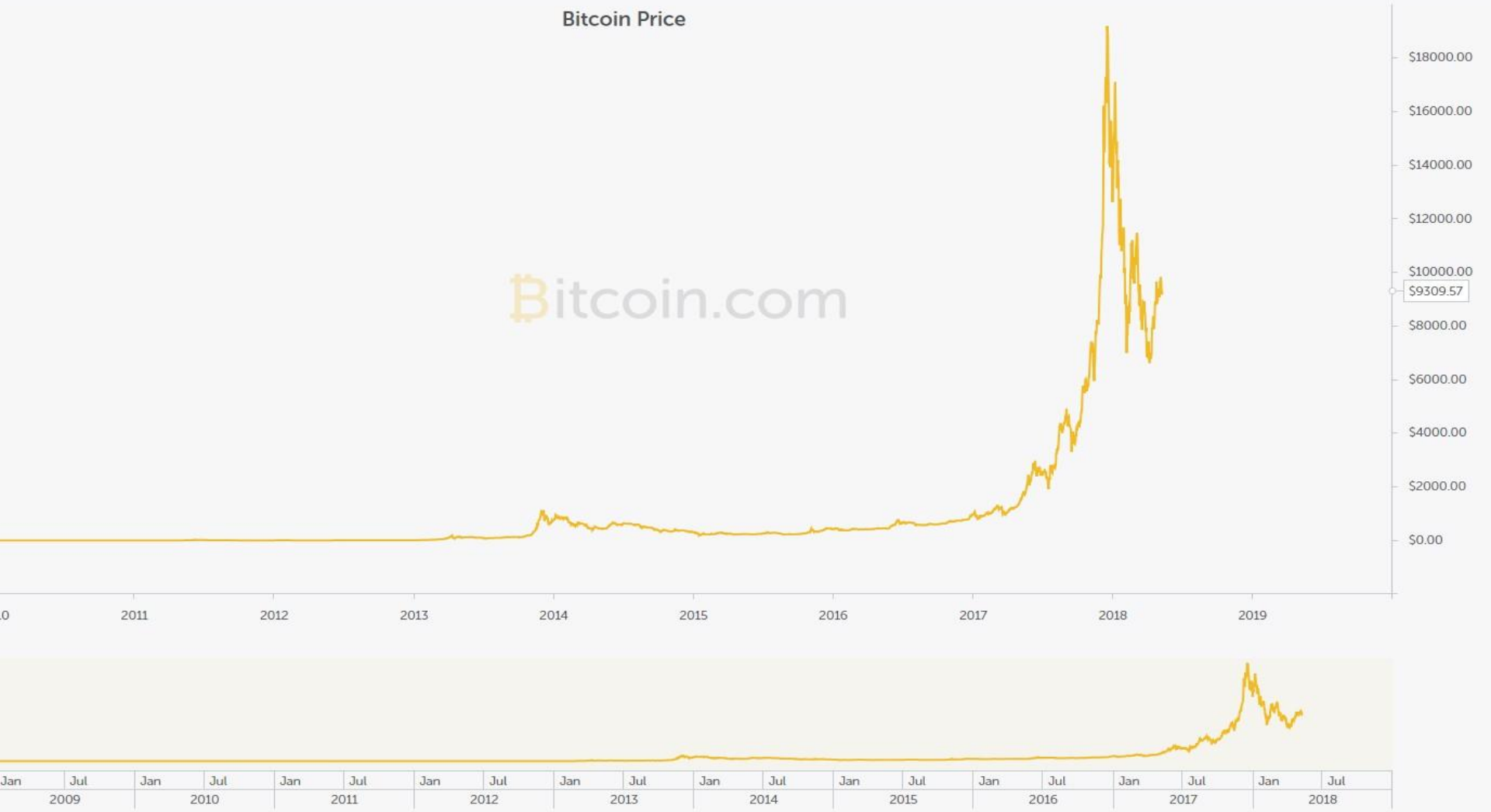
- Bitcoin can be traded across borders with no interference-24/7/365, Bitcoin is Live (no public hols)
- Internet connection is only requirement for transactions
- Bitcoin can be exchanged for any global currency
- Currently worth 100 billion USD in circulation (143 billion AUD)
  - $5689USD per bitcoin is current price..
- 21 million coins in existence only 17.6 million mined

Bitcoin

- Bitcoin can also be used to pay for goods and services.
- Over 100,000 vendors accept Bitcoin as payment
- Some are brick and mortar establishments, most are e-commerce firms
- Some offer services that are illegal

Bitcoin Value

- A good currency must be:
  - Scarce, portable, durable, fungible, divisible, current
  - Does not need to have “intrinsic” value
- The value of each unit of currency is determined by equilibrium between supply and demand
  - Total value of a currency is proportional to total trade using it
  - Value per unit = Total value / Number of units
- Bitcoin amounts can be specified with 8 decimal places
  - Therefore there are 2.1 quadrillion atomic units


Bitcoin Price
Bitcoin.com
$18000.00
$16000.00
$14000.00
$12000.00
$10000.00
$9309.57
$8000.00
$6000.00
$4000.00
$2000.00
$0.00
2011
2012
2013
2014
2015
2016
2017
2018
2019
Jan Jul Jan Jul Jan Jul Jan Jul Jan Jul Jan Jul Jan Jul Jan Jul Jan Jul Jan Jul
2009 2010 2011 2012 2013 2014 2015 2016 2017 2018

Where do Bitcoins come from?

- Fifty coins generated in the “Genesis Block”
- More are generated with each transaction
  - Whoever verifies a transaction first gets a reward
    - Generating these rewards is called “mining”
    - The first reward amounts were 50 BTC
    - The reward halves every 210,000 validated transactions
      - Roughly once every four years, so it’s happened once so far; current reward is 12.5 BTC ($71,113 USD)
    - In 2140 CE, the reward will vanish and transaction fees will be the sole benefit of mining.

Bitcoin System Components

- A transaction structure for specifying and changing ownership
- A p2p network for propagating, verifying and storing transaction data
- A proof-of-work system (hashing, “mining”) for:
  - Synchronizing transactions
  - Determining initial distribution of coins

Bitcoin

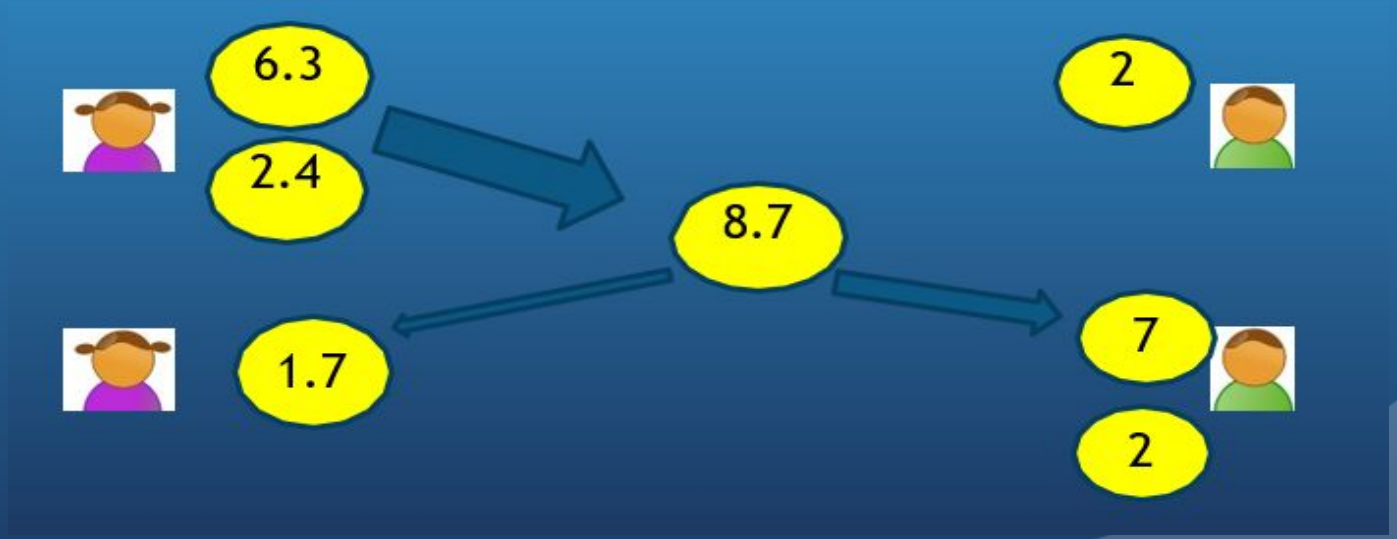
- A Bitcoin is actually made of
  - Unique ID
  - Quantity (denomination) – arbitrary number with 8 decimal places
  - Owner ID

Transactions

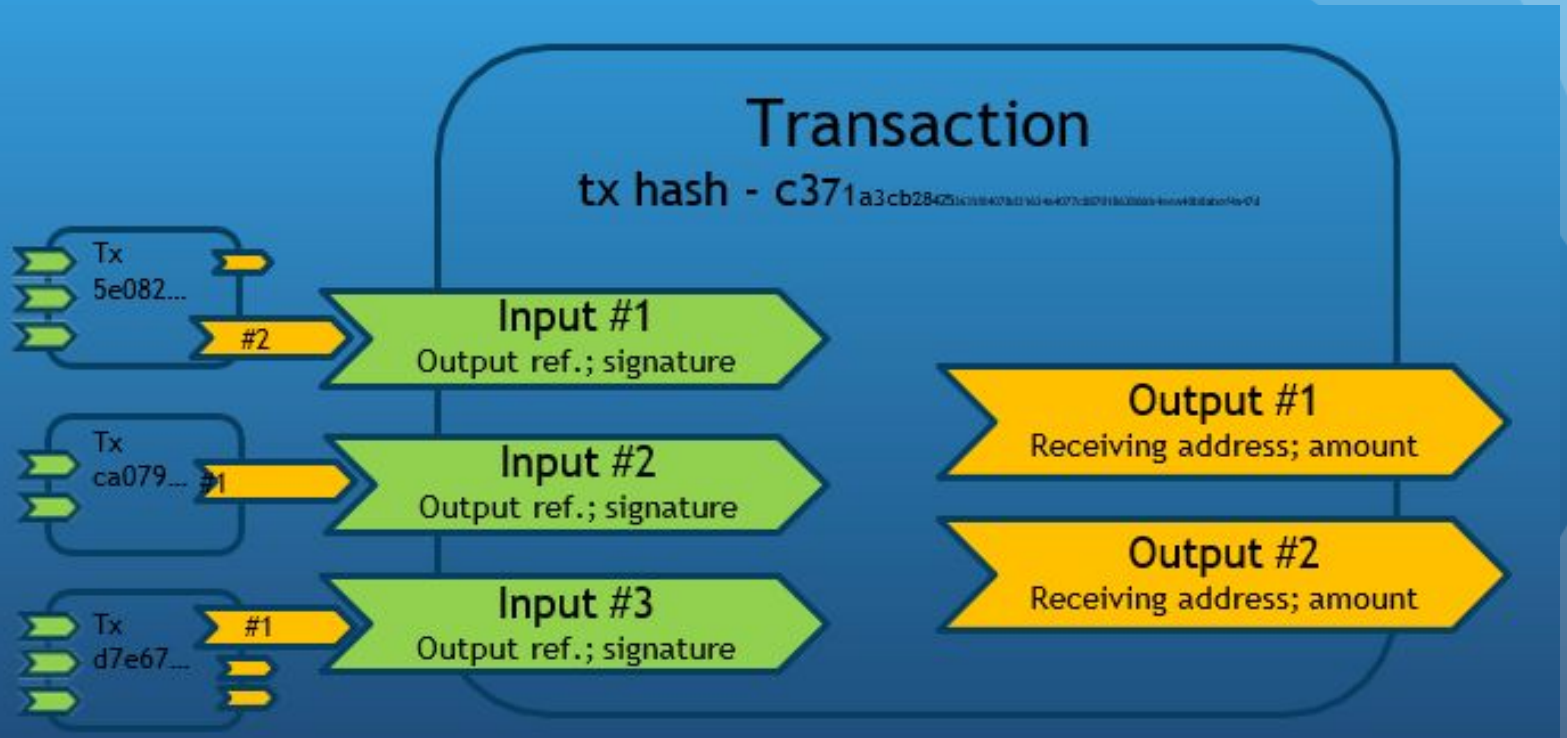
- The owner of a coin is identified by an “address”
- Each address is associated with a private key
- To use a coin, the owner must provide a digital signature with the associated private key
- The process where coins are merged and split is called a “transaction”
  - Used to move Bitcoin from one owner to another

Coins

- Coins can be split and merged
- If Alice wants to send Bitcoin to Bob, she will merge some of her coins and split the result between her and Bob



Transaction Structure

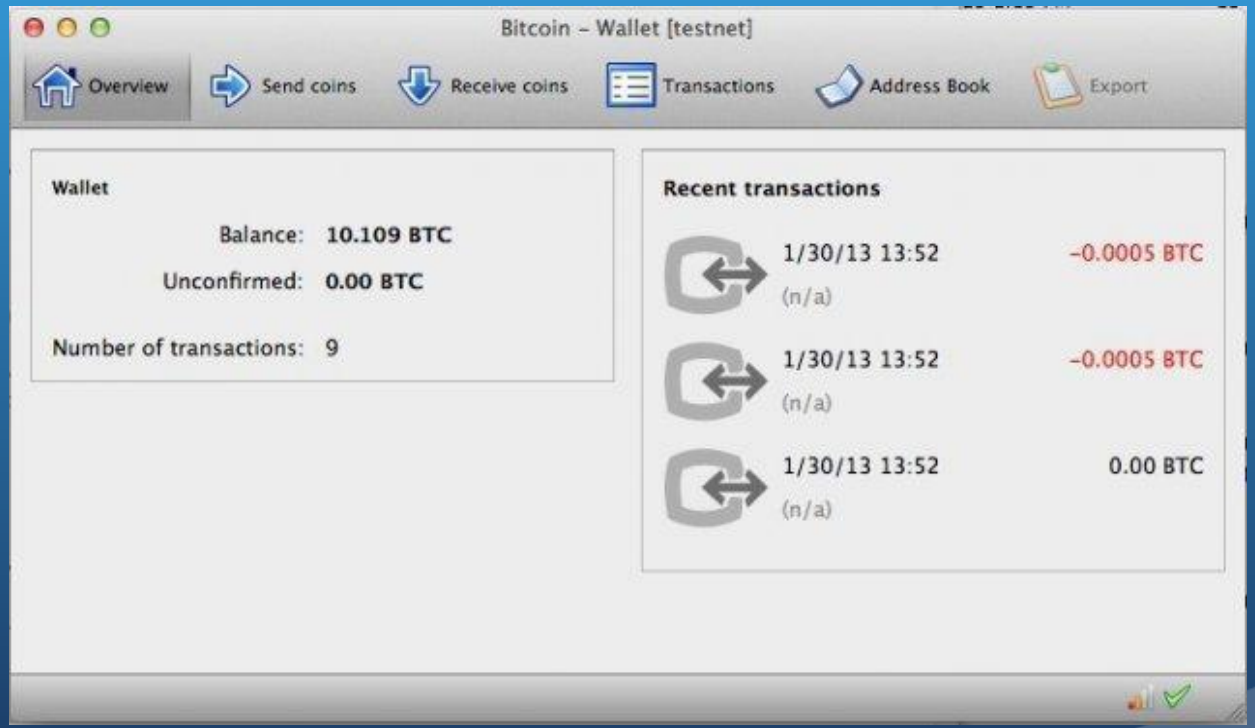


Transaction Fees

- Verifying transaction is (purposely) hard
  - That's why you get so much money for doing it!
- There are also transaction fees paid to the verifier
  - These have normally been set to 0 since the reward for mining is already pretty good
  - Lately the fees have risen to provide an added incentive
  - The fees are taken from the payer as a "tax"
  - In 2140 CE, transaction fees will be the only incentive remaining

How does Bitcoin actually work?

- You start by installing a “wallet” program



Bitcoin Address

- To receive money, you tell your wallet to generate an "address"
  - This causes the wallet to generate a public-key/secret-key pair
  - The private key is hashed and published as your "address"
  - You publish your address
    - Or just tell the payer your address

Receiving Money

- Suppose I want to pay you 1 BTC
- I need your address
- I generate a “transaction” record and sign it
  - Contains the amount, transaction ID, and your address
    - Also has hash of previous transaction that granted me the money I’m using
  - Signed by my secret key
    - If I lose the secret key associated to the transaction that granted me the Bitcoins I’m sending you, I lose that money!

Verifying Transactions

- Why not just check to see if I properly signed the transaction record?
  - I could be cheating!
    - Maybe I don't own the coins I'm sending
    - Maybe I already spent those coins with someone else
- So instead the "Bitcoin network" verifies the transaction
  - This is hard-by-design because there is a nice payoff for doing it
  - It also means a cheater would have to have more computing power than the rest of the network

The Blockchain

- Every verifier (or “miner”) on the network has an entire history of all transactions
  - Called the “blockchain”

- This is a chain of transactions that tracks where each Bitcoin has been
  - Every transaction has the hash of the previous transaction that granted the coins
  - Once a transaction has been verified, it is added to the blockchain by all nodes of the network

How to Mine Bitcoins

- Suppose you want to verify a transaction
  - Suppose the transaction is “hello” + random data
  - The Bitcoin system has a level of “work” required to earn the verification reward. For hello, lets have the example of needing to get get 4 leading zeros on the hash, so wee need to try different random inputs
  - Compute SHA256(“hello:0”)
    - a61bb398117fe…
  - Compute SHA256(“hello:1”)
    - 61b7a90017562…
  - …
  - Compute SHA256(“hello:917712”)
    - 0000718a5dce3… Winner!

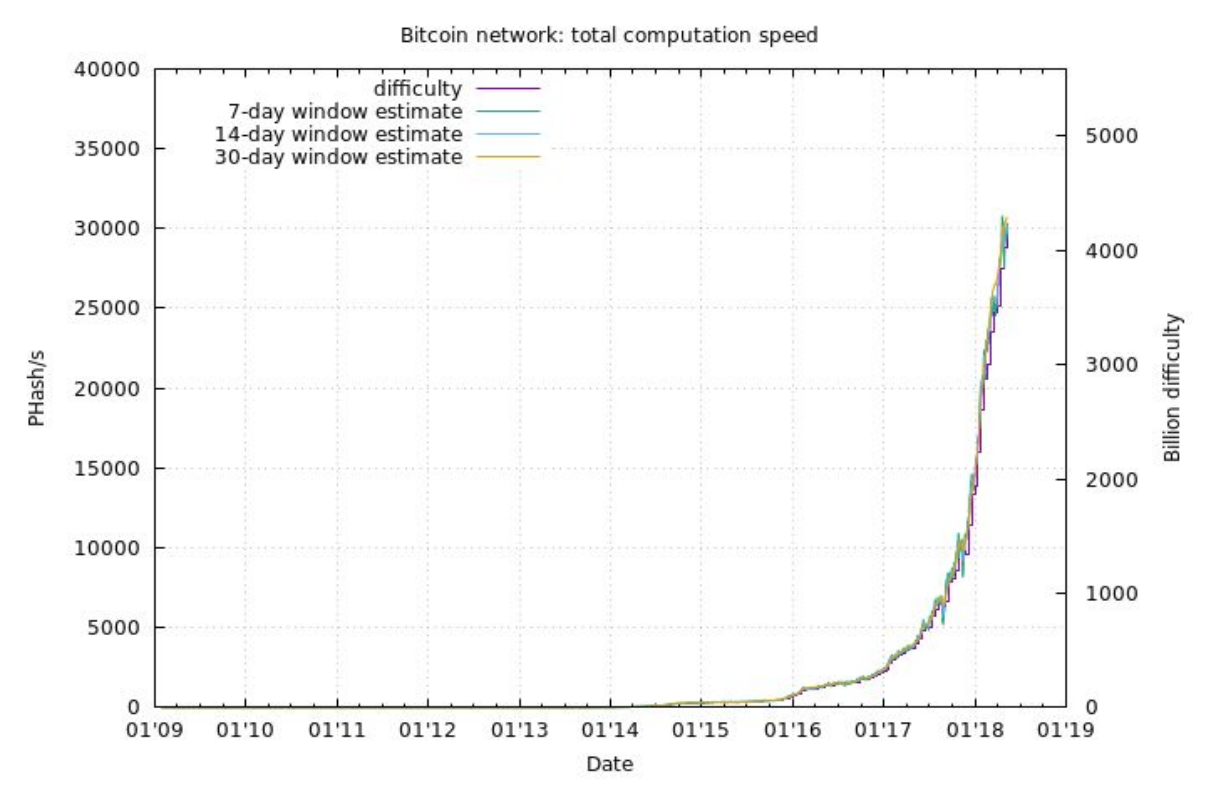
How hard is this?

- To get a leading 0 digit in hex, assuming SHA256 is random
  - 1/16 chance
  - 16 expected trials
- Two leading 0's
  - 256 expected trials
- In reality, to verify a Bitcoin transaction you have to get below expected number of trials due to "luck"
  - This should take about 10 mins given the power of the network
  - This is recalibrated every 2 weeks to keep at that level

Current Exp # Hashes for Target

- For the current target we need about
  - $2^{64.8975}$ hashes to get below the target
  - This can be parallelized of course
  - Full scaling when parallelized
  - Great use of botnets!
  - Many people have studied the economics of how much power is worth exerting to get rewards

Growth in Computation Speed



Should you mine Bitcoin?

- No

Digital Coins

MAJOR:

-**BTC Bitcoin** - first, strongest, most accepted, most mined, high volume market, a true currency
-**LTC Litecoin** - second only to BTC , faster than BTC, Smaller efficiency gap between GPUs and CPUs , ASIC-hostile
-**NMC Namecoin** merged mined with BTC, used for alternative p2p domain system
-**PPC PPcoin** Proof Of Stake [very innovative, low energy] , compatibile with BTC miners

MINOR:

-**TRC Terracoin** based on BTC, fast difficulty adjustment, initialy flaved but corrected
-**DVC Devcoin** merged mined with BTC, 90% of generation goes to foundation, 10% to miners
-**IXC IxCoin** merged mined with BTC, premined 580k coins but still alive
-**NVC NovaCoin** - scrypt hashing[like LTC] , proof of stake [like PPC] , controversial start
-**FRC Freicoin** - back alive. 4.89% anual demurrage. for the first 3 years 80% block subsidy goes to foundation, 20% to miners
-**FTC FeatherCoin**- LTC clone with 4x more coins.

CANDIDATES:

-**BTE Bytecoin**- the 1:1 bitcoin copy, nothing changed. extremally high starting hype/hashrate.
-**BQC BBQCoin**- forgotten after 51% attack on launch, now revived and active. super fast version of LTC.
-**MNC Mincoin**- similar to BBQ, but very bad launch [no binaries + 25000% superblocks] giving 10% of all coins to insiders.
-**CNC CHNCoin**- similar to BBQ, announced on chinese forum first, very big hashrate.
-**BTB BitBar**- scarce version of NovaCoin. low starting diff like FTC and CNC, but quick adjustment.
-**JKC Junkcoin**- started as a joke, but now working ok. low starting diff and slow retarget like BTE, FTC, MNC, CNC
-**YAC YACoin**- Yet Another altCoin. NovaCoin fork, with modified hashing - for now CPU-ONLY
-**RYC Royalcoin**- Another LTC clone, starting with low diff and superblocks like MNC ...
-**FRK Franko**- Another faster LTC, again 0.00... starting diff. scarce.

DEAD / DYING :

-**FTC Gamecoin**- yes, FTC. clone so bad it was 51%'ed the first day.
-**LQC Liquidcoin** made to be very fast at constant difficulty, dead [pool closed, exchange closed]
-**SC Solidcoin** - dying (10-20% fee), designed to improove IxCoin, hard to be neutral on this one, 1.0 was a premine scam, 2.0 says BTC is pyramid scheme.

Bitcoin Summary

- Crypto currency is a method of conducting commerce without using a national currency
- It also provides you with a degree of anonymity of transactions
- Built upon the same cryptographic building blocks that we have seen in other protocols
- Even if Bitcoin fails ultimately, we are likely to always have crypto currencies moving forward

Final Thought

- Neither Tor or Bitcoin solve the problems they are aiming to solve perfectly
  - There is no magic bullet
- Anonymity is defined as not being named or identified
  - Even when using Tor (or Bitcoin, or whatever) every service has at least one piece of information that can be used to distinguish different users
  - If you then combine this with whatever it is that you are doing (i.e logging into some other service)this information could then reveal information about the true identity of the user
- Key is to weigh the security risks, and not be ignorant of what your tool is really providing you in relation to your security