Cse291-J: Blockchain Security

Deian Stefan and Stefan Savage, Spring 2024

Bitcoin Hacks

So Bitcoin exists…. So what?

What is the incentive to attack Bitcoin?

- Vs attacking, say, poniverse.net? (largest brony fan site online)

For those who said because its valuable… why?
What enables that value?

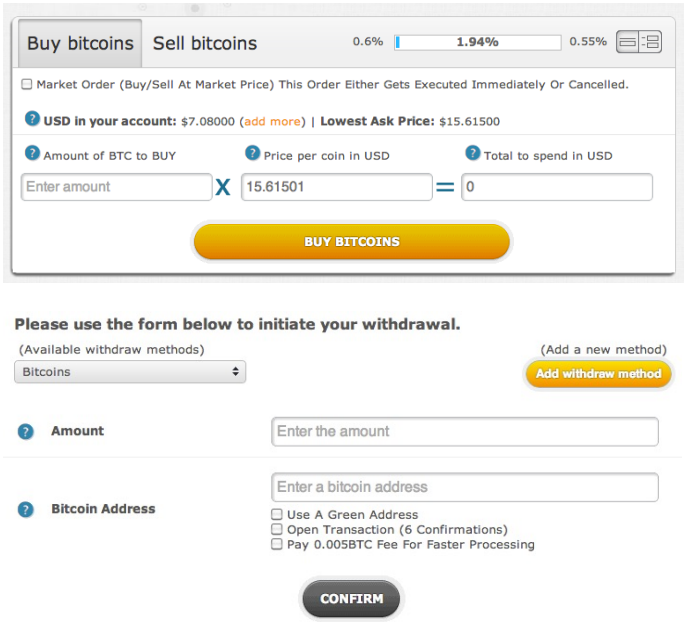
- Entities willing to accept Bitcoin for goods of services (in lieu of money)
- Entities willing to trade Bitcoin for (real) money

What needs to happen for these entities to emerge?

Bitcoin commerce for consumers

How to get Bitcoin into the hands of consumers?

- Most normal people aren't going to go mine it…
- Need parties who will sell bitcoin in exchange for $

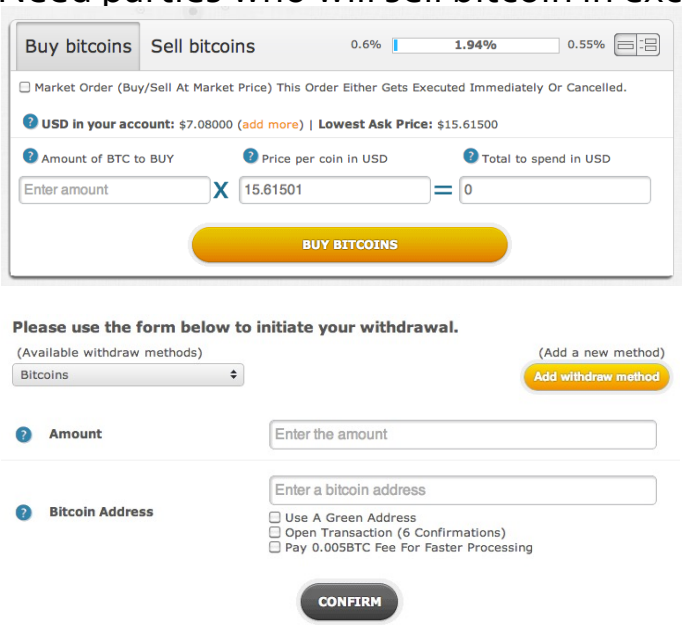


MT.GOX
BITSTAMP
bitfloor
Bitcoin-24
bitcoin.de
Bitcoin-Marketplace - Made in Germany!
Bitcoin-Central
CAMP BX
BTC e
mercadobitcoin
Bitcoin China
VirWoX
virtual world exchange
VirtEx
Canadian Virtual Exchange

Bitcoin commerce for consumers

How to get Bitcoin into the hands of consumers?

- Most aren't going to go mine it…
- Need parties who will sell bitcoin in exchange for $



What do you notice going on here?

"account"? (what is an account?)

"Price per coin in USD?" (who sets this price?)

The emergence of exchanges/banks in Bitcoin

Bitcoin has **no connection** to the existing financial system, so that must be handled out of band

- Price floats based on buyers and sellers
  (and details of particularly exchange, huge arbitrage opportunities for years – this is precisely how Sam Bankman-Freed made the money to start FTX)
- Generally centralized implementation – exchange holds private keys for coins being traded

- In the 2011-2014 period, Mt. Gox dominated

  Originally founded by Jed Caleb in 2010 as a site for trading Magic the Gathering cards (hence, the name), then turned into a Bitcoin Exchange and sold to Mark Karpelas in 2011

  By some accounts, was handling 70% of all Bitcoin trading

  Why was it so popular?

  - Instantaneous trades; traded against assets on deposit, settled manually out of band (need to trust Mt. Gox)

Mt. Gox is **also** source/recipient of large numbers of Bitcoin transactions (just file that away for now)

Attacks on exchanges

Key risk: If exchange site can be compromised can transfer crypto out

- Why do real banks not have this problem to the same extent?

What might be done to mitigate this risk?
(aside from general hardening of software)

- Segregate/protect keys (e.g. HSM) and carefully manage workflow for invoking
- Hot/cold wallets – maintain private keys for addresses managing "working capital"
  - Keep non-working deposits in "cold" wallet that is offline whose keys are not available to software
    - Quite tricky to make practical…
- Circuit breakers – alert/block on significant outflow

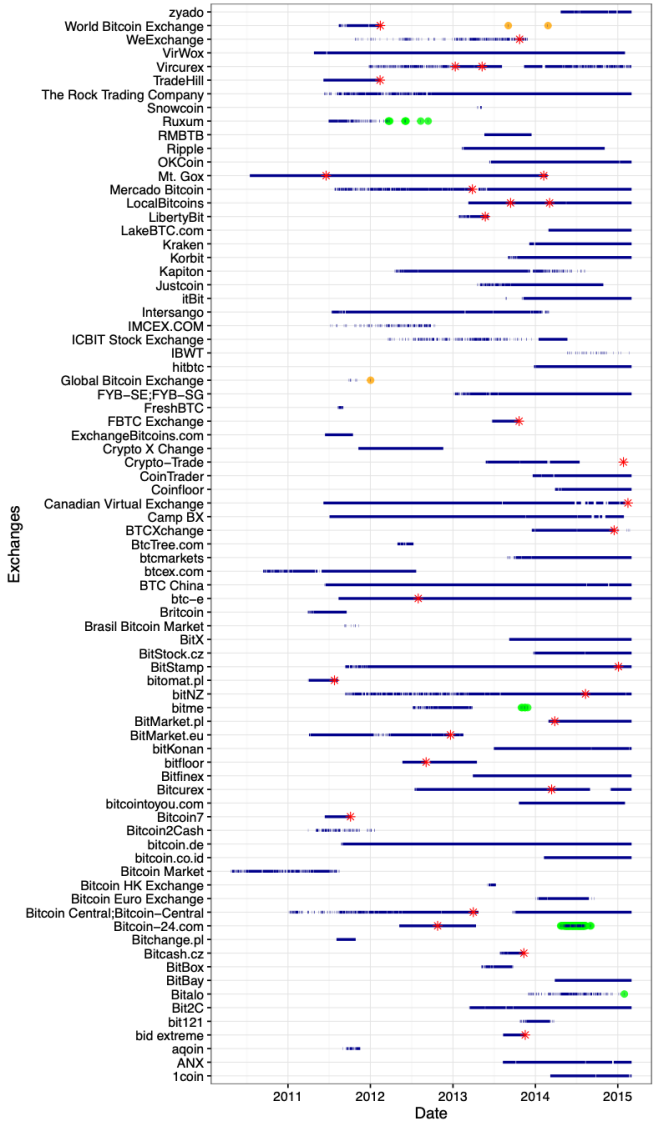
But did this really happen?

Yes – between 2011 and 2015 at least 26 Bitcoin exchanges breached (some multiple times)

By far the largest was the> 800,000 BTC stolen from Mt.Gox (blamed on malleability attack)

- After that a bunch in the 40k range
  - Linode, Bitcoina
  - If you count seizure by US Govt then Silk Road also

In 2014 $, this is ~ 1$B loss, or ~$60+B today



Bitcoin Malleability attack

Issue: various ways that you might take a valid transaction T and make a new transaction T′ from it that is also valid

- One such issue: for every ECDSA signature (r,s), the signature (r, -s (mod N)) is a valid signature of the same message

  So you can create a duplicate of a transaction message (same addresses, same operations, etc) with a *different* signature

- Similar issue (prior to v0.8.0) with non-DER encoded signatures

Why does this matter? It's the same no?

- Because the hash of the message is different and some systems use the hash as a transaction id and this can lead to a kind of "confused deputy" attack
- Because you might be… uncareful… about when a transaction is committed

Bitcoin Malleability attacks

Bad bookkeeping attack

- X transfers Bitcoin to Mt Gox and then asks to transfer them;
  Mt Gox produces transaction T to do this and submits it for mining
- X observes Mt Gox's transaction T, and produces a valid T' via malleability;
  X pushes to more miners more quickly and T' is committed instead of T
- X complains to Mt Gox that their transaction didn't happen, Mt Gox checks the blockchain for H(T) and can't find it so reasons that the transaction didn't happen and credits X with their coins again
- Fix?

Zero-confirmation attack

- X transfers 3 Bitcoin: 1 to Z and 2 to W (W is change address for X) in Transaction T1; without waiting for confirmation X then spends against W (i.e., transferring 2 BTC from W to Q in transaction T2)
- Attacker observes 1st transaction T1 and creates T1' (via malleability);
  T1' commits to blockchain and now T2 is invalid
- Fix?

Script attacks w/non-standard transactions

- If you make a script depend on the Hash
- There are ways to arrange that components of the script are not signed
  Fix?

Mt. Gox hack

Did they lose 850,000 BTC to the malleability attack?

- No.

So many problems…

- Theft starting day one under Karpeles: ~80k BTC stolen from wallet.dat before transfer (cheap at time, but not replaced) [1Feex, never moved];
  also $50k deficit on Liberty Reserve from withdrawal exploit
- Two months later (May) – 300k stolen; 99% returned for 1% finders fee
  [have moved]
- One month later (June) – cracking unsalted passwords; someone gets admin access and tries to sell 500k BTC on site; drives price of BTC to almost nothing (contained because of internal trading limits)
- Three months later (Sept) – someone gets read/write access to DB, inflates their account balance (subsequently wiped updates and logs) and withdraws 77.5k BTC [moves, parts to TradeHill and eventually some to BTC-e]
- Trading bots (Willy and Markus) – lost 22,800 BTC

Mt. Gox

The big one: ~650k BTC stolen continuously 2011-2013

- Appears to have been automated, at moment new deposits came in
  - Transferred BTC out to external wallets and erased records
  - DB still showed that Gox had that money, but on the blockchain they didn't

Current best understanding

- Alexey Bilyuchenko, Aleksandr Verner implicated in hack, Alexander Vinnik in laundering
  - Hacked Mt. Gox and then laundered via Trade Hill (until closed), Mt Gox itself and BTC-e, an exchange Vinnik and others founded largely to support laundering criminal money flows
  - Bilychenko and Verner at large
- Vinnik
  - Arrested in Greece in 2017, US and Russia request extradition; extradited to France, then France to US; already 5yrs for locky, trial date for Sept 2024
- Aliaksandr Klimenka (helped operated BTC-e)
  - Arrested in Latvia in 2023; extradited to US in 2024
- BTC-e largely shutdown; assets now under control of FSB

Irony: cashed out as BTC came in (missed rise in price); total return ~$20M

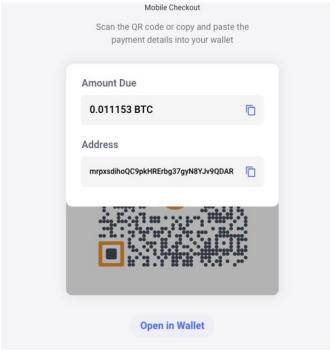
What about the merchant side?

How do merchants accept Bitcoin? What are issues?

- First, must be able to manage technical side (i.e., receive and validate transaction)
  - But… hmm… what about customer expectations…
    a Visa transaction authorizes in 2-3 seconds…. How long will a Bitcoin transaction take?
- Second, must manage volatility – how does merchant manage pricing?
  - How many Bitcoin to buy a slice of Pizza? What about in an hour?
- Third, must be able to offer merchant (real) money (most don't want to hold Bitcoin)

Bitcoin payment processors (e.g., BitPay)

- Acceptance (can provide per-merchant address and accept payments)
- Some connection to normal payment system (e.g., Paypal, ACH, etc)
- Pricing (typically merchant sets price in dollars, processor manages conversion)
- Latency management – either single confirmation (~10min) or validate *consistency* of transaction and front money
- Volatility management – Bitcoin may be worth less than payout
- Process has lots of risk, must price risk into exchange rate or separate fees



Merchant side attacks

Some similar to exchanges

- Compromise merchant side and xfer out crypto

Supply-chain

- BitPay used event-stream package; package poisoned to steal from BitPay users who also used CoPay

Vulnerabilities in payment protocol (BIP70)

- Exploiting auth vulnerability used for refunds – not clear if it ever really happened

Back to consumers… you've bought Bitcoin, do you really want to handle raw Bitcoin?

This would mean generating and managing addresses yourself |(i.e., one private/public key pair for each address)

- Note you probably don't want just one address… because Bitcoin transactions transfer **all** Bitcoin from input addresses to output addresses
  - So you typically want additional addresses on the output side to hold your ***change***

You also need to connect **directly** to BTC blockchain to execute transaction

Potential issues

- What if you lose your private key?
- What if you type the wrong destination address?
- What you don't understand this stuff and it seems really confusing?

Instead: online wallet services

Hosted wallets

- Third-party holds your private keys and offers simplified UI to reduce friction to use

  Simplest case: let your "bank" (i.e., MtGox) hold your BTC and use their "transfer out" feature to pay

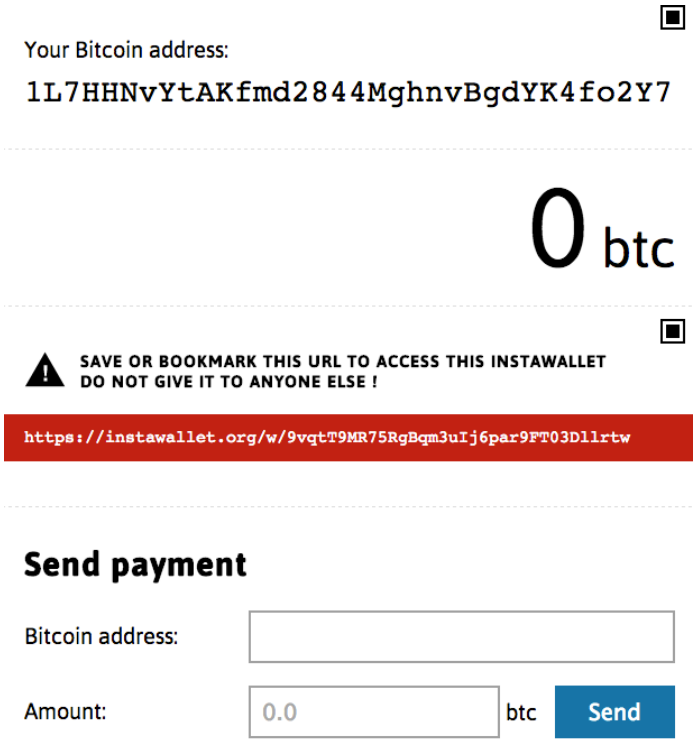
- Specialized wallet services

  Instawallet, Easywallet, WalletBit, CoinBase, Easycoin, etc

- Typically, some kind of access control that authorizes service to use your keys

Self-hosted wallets

- Hardware/software products that provide some more usable UI for using keys that you have (i.e. keys stored accessed via host software)



Attacks against hosted wallets

Phishing

- Get credentials; transfer money out
- Fix?

Defeating multi-factor auth

- SMS-based MFA
  - SIM swapping
  - Fix?
- Better MFA
  - MITM malware

EZRA REGUERRA JAN 01, 2024

Crypto phishing scams took almost $300M from 324K victims in 2023: Report

SIM-swapping ring stole $400M in crypto from a US company, officials allege

Scheme allegedly targeted Apple, AT&T, Verizon, and T-Mobile stores in 13 states.

ASHLEY BELANGER - 1/30/2024, 11:18 AM

Powerful new Oski variant 'Mars Stealer' grabbing 2FAs and crypto

By Bill Toulas February 1, 2022 01:41 PM 0

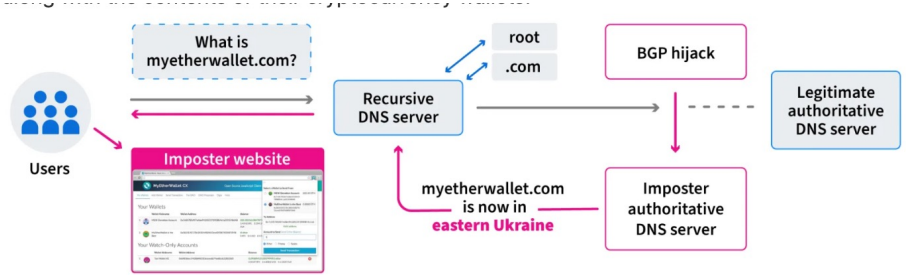
More audacious attacks

Hijacking

- Takeover DNS for service
- Takeover BGP for service
  or for DNS server for service

Typical use

- Redirect visitors to malicious version of site which captures credentials
- Then login to real site with stolen creds and transfer out $$$
  (note can MITM multi-factor auth)



KlaySwap crypto users lose funds after BGP hijack

Hackers have stolen roughly $1.9 million from South Korean cryptocurrency platform KLAYswap after they pulled off a rare and clever BGP hijack against the server infrastructure of one of the platform's providers.

CAPITAL & CRYPTO · 2 MIN READ

Cryptocurrency Exchange EtherDelta Hacked in DNS Hijacking Scheme

LAST UPDATED MARCH 4, 2021 5:02 PM
BY JOSIAH WILMOTH

Attackers Hijack DNS Entry of Stellar Lumen Wallet Application BlackWallet

Terra Website Compromised; Developers Warn Against Phishing Scam

Terra warned its users to avoid using its website after being targeted by a phishing attack.

By Oliver Knight · Aug 21, 2023 at 6:47 a.m. PDT · Updated Aug 21, 2023 at 10:43 a.m. PDT

15

Popular crypto wallet MEW hit by DNS attack that drained some users' accounts

Jon Russell @jonrussell / 10:31 AM PDT • April 24, 2018 · Comment

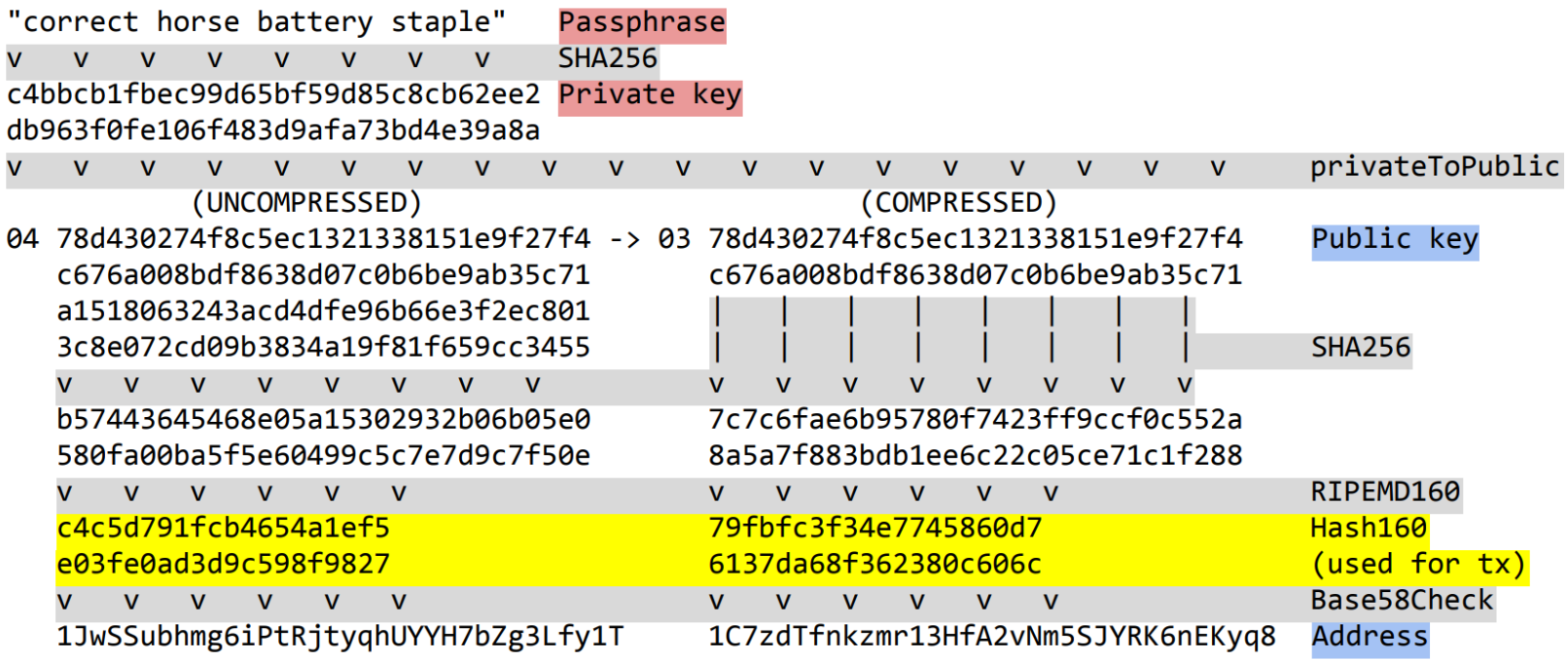
Brain wallets: passwords for crypto

Basic idea: need to encode wallet private key in a way you can remember

- ECDSA private key is 256 bits – 32 hex digits – hard to remember
- What if instead you had a memorable seed phrase (i.e., like a password, held in your brain) and we hashed this to obtain a public/private key pair?

From Ryan Castellucci DEFCON talk

How to make a brainwallet



Brain wallets: passwords for crypto

Pros: private key is only stored in your head (secret),
very easy to implement

Cons?

From Ryan Castellucci DEFCON talk

Some results

“Down the Ra

July 2012

“The Quick Br

Dot” - held ab

“” - had 50BT

- “my hovercraft is full of eels”
- “Interior Crocodile Alligator”
- “No need to worry, my accountant handles that”
- “tomb-of-the-unknown-soldier-identification-badge”
- “permit me to issue and control the money of a nation and i care not who makes its laws”
- “who is john galt”
- “Live as if you were to die tomorrow. Learn as if you were to live forever.”
- “gate gate paragate parasamgate bodhi svaha”
- “The Persistence Of Memory”
- “QTC”
- “644122178”
- “8964009”
- “que me lleve la muerte”
- “one two three four five six seven”
- “it’s a secret to everybody”
- “Ph’nglui mglw’nafh Cthulhu R’lyeh wgah’nagl fhtagn”

To summarize

None of these represent an attack on the Bitcoin blockchain

The issue is that the Bitcoin blockchain by itself is not useful

- Need way to convert BTC to/from $
- Need way for users to use BTC that is familiar to them
- Need way for merchants to accept BTC
- These points of interface are ripe for attack

None of this is unique to Bitcoin and further blockchains will add additional external attack surface (bridges, oracles, etc.)