Bitcoin Forum

simple machines forum

October 13, 2014, 01:34:06 PM

Welcome, **Guest**. Please login or register.

Forever Login

Login with username, password and session length

News: Bitcoin Core **0.9.3** has been released. Download.

Search

HOME HELP SEARCH DONATE LOGIN REGISTER

Bitcoin Forum > Bitcoin > Bitcoin Discussion (Moderators: hazek, tysat, malevolent) > **List of Major Bitcoin Heists, Thefts, Hacks, Scams, and Losses**

« previous topic next topic »

Pages: [**1**] 2 3 4 All

print

Author

Topic: List of Major Bitcoin Heists, Thefts, Hacks, Scams, and Losses (Read 11593 times)

dree12
Legendary

Activity: 1148

Ignore

List of Major Bitcoin Heists, Thefts, Hacks, Scams, and Losses
April 19, 2014, 01:56:22 AM

#1

Last updated: August 12, 2014, 05:49:03 PM.

List of Bitcoin Heists

Following is the result of research on prior Bitcoin-related thefts. The list strives to be as accurate and informative as possible, and where possible I have provided references for assertions made within. For disputed thefts, I have applied best judgement and included the ones that were most publicly accepted.

Because of the volatile nature of Bitcoin's exchange price, I have denominated heist estimates in ฿. Although not heists *per se*, major permanent bitcoin-denominated losses are also included in this list. If I missed any major thefts, heists, or losses, or if you have any other information to contribute to one of these events, please leave a reply in this thread.

Note that this thread is relatively new and was created because of space limitations in the original thread.

Additionally, I would be grateful if contributors write commentary for each theft. Ideally, the theft descriptions should be as detailed as possible. Much of the present commentary is inadequate.

Table of Contents

License

This entire document is licensed under the public domain. If that would is not permissible in your jurisdiction, it can then be licensed under any permissible license of your choosing.

The author of this list believes all information contained thereof to be factual; however, the author takes no responsibility for any losses associated with factual inaccuracies in the list.

Factual inaccuracies

Although I make every attempt to ensure information in the list is well-cited and factual, there is always the possibility of error (whether on my part or on my source's part). If you find a factual inaccuracy, please report it. You will be credited appropriately for such reports.

Donation

Donations are appreciated and are accepted at 1MLSW1nmYkHqaHWNNkHSAHct6exd8fYYLX. Alternatively, consider a donation to a charitable cause. Many victims of these thefts accept donations, and they likely need the donations more than I.

Scope

Without properly-defined bounds, this list could not possibly be complete. Consequently, several clauses below limit the scope of the list.

General

Generally, a major heist, theft, hack, scam, or loss must cause damage greater than or equal to 500฿, in ฿ damage only, to qualify for inclusion in this list. Thefts related to Bitcoin but with most damage in another currency do not qualify, unless customers were damaged in ฿. Borderline thefts may qualify if reasonable estimates are over or equal to 500฿. Thefts that do not strictly qualify but are of significant importance are listed in the thefts not included section.

Losses are included only if they are unintentional. This obviates the need to include many incidents where people delete wallets due to lack of value at the time before 2011, and additionally prevents the inclusion of more recent "proof-of-burn" alternative cryptocurrencies that require bitcoins to be destroyed.

If a theft is included on this list because it was thought at the time to qualify, but more recent analysis shows that it does not, it may potentially remain on this list despite not meeting the requirements.

Understood risk

Some losses of Bitcoin to third parties cannot in principle be classified as scams or losses.

While it is certainly true that some securities are intended as scams, and they should certainly be included in the list if they are, several high-profile company disasters could not be honestly included on this list. For instance, a company's failure to return funds raised during the IPO through profits is not in itself sufficient to be a scam. The risk involved here is an "understood risk".

However, this does not absolve all who create securities. Those who intend the securities to be a scam, or through negligence or willful blindness allow it to become a scam, will still be included on the list. In these scenarios, the risk to the investors is not agreed to by the investors, hence it is not an "understood risk". Incompetence by itself is however insufficient for a security to be classified as a scam.

Other trivial incidents can be excluded by the same principle. For example, a large gambling loss is obviously not a scam, because the risk was understood. But if evidence indicates that the casino rigged the games, then the risk is no longer understood, and the incident is eligible for the list.

Because sometimes the evidence is not clear-cut, this list includes or refuses to include incidents based on the best evidence available. If a reasonable interpretation of the event suggests that it was not within understood risk, it will be included in this list, even if alternative interpretations exist.

This policy does not apply to thefts.

Managing Bitcoin prices

It is well-known that Bitcoin prices are volatile. Before 2011, the value of a single ฿ was extremely low. Consequently, this list ignores most events that occurred before 2011. If a theft, hack, scam, or loss caused damage less than 5000฿ before 2011, it is not listed on this list at all.

For several years during which the Bitcoin price fluctuated greatly, there are also USD cutoff values. In those years, both the ฿ cutoff value and the USD cutoff value must be met for the theft to be included.

Cutoff values so far are below:

Year	Cutoff Value	Severity list cutoff
2009	5000฿	N/A
2010	5000฿	N/A
2011	1000฿	12000 $
2012	1000฿	12000 $
2013	1000฿	12000 $
2014	500฿	N/A

Included borderline thefts

Before 2014, another clause was used to include several thefts due to the rapidly appreciating Bitcoin price. This clause is no longer in effect. Borderline thefts, which had less than 1000฿ in total damages, may still have been included if their total damage when measured in June 2013 ฿ exceeds 500 ฿. This measurement was based on Mt. Gox price data prior to 2013-06-09, Bitstamp price data after 2013-06-10, and US CPI data published by the United States Bureau of Labor Statistics.

Instructions

For ease of navigation, I have assigned each theft a name. Note that this name is neither official nor permanent and is used solely for ease of navigation. To search for the heading that details the actual theft, simply use your browser's Find function and search for the name. This will either bring you to the theft itself, or a link to the theft. If the latter, simply click the link to be directed to the theft.

Some links will appear in commentary and in lists. These can be clicked; their destination is set to the beginning of the linked incident's section.

List of events by severity

In this section, each theft is listed alongside the value stolen when converted to a January 2014 ฿ equivalent along with the value stolen when converted to real (inflation-adjusted) USD.[1] This represents the true value stolen and is generally the best list in that regard.

Note that this list makes no effort to restrict the precision of the numbers nor to indicate what type of estimates each number represents. Please see the following list for such data.

Rank	Name	Severity (January 2014 ฿)	USD Equivalent
1	Silk Road Seizure	32716.283 ฿	26867560 $
2	Sheep Marketplace Incident	4978.276 ฿	4070923 $
NO 3	Silk Road 2 Incident	4400.000 ฿	3624866 $
4	GBL Scam	4185.734 ฿	3437446 $
5	Bitcoin Savings and Trust	3700.408 ฿	2983473 $
6	PicoStocks Hack	3679.520 ฿	3009397 $
7	MyBitcoin Theft	1395.691 ฿	1072570 $
8	CryptoRush Theft	950.000 ฿	782641 $
9	Flexcoin Theft	896.104 ฿	738240 $
10	BIPS Hack	808.140 ฿	660959 $
11	Inputs.io Hack	780.069 ฿	640615 $
12	James Howells Loss	763.965 ฿	627659 $
13	Allinvain Theft	580.983 ฿	445688 $
14	July 2012 Bitcoinica Theft	398.757 ฿	315133 $
15	Bitfloor Theft	338.861 ฿	273209 $
16	Bitcash.cz Hack	302.517 ฿	247422 $
17	Bitomat.pl Loss	301.332 ฿	231570 $
18	Bitcoin Rain	283.696 ฿	231440 $
19	Linode Hacks	281.818 ฿	223278 $
20	May 2012 Bitcoinica Hack		191638 $

		240.993 ฿	
21	ZigGap	240.128 ฿	195490 $
22	Vircurex Theft	199.938 ฿	163351 $
23	Tony Silk Road Scam	184.356 ฿	146944 $
24	Stefan Thomas Loss	162.675 ฿	124793 $
25	Just Dice Incident	132.421 ฿	108794 $
26	Cdecker Theft	129.745 ฿	104607 $
27	Ozcoin Theft	129.713 ฿	105600 $
28	Mass MyBitcoin Thefts	93.409 ฿	71656 $
29	BTCGuild Incident	88.939 ฿	72556 $
30	2013 Fork	68.094 ฿	55551 $
31	Bit LC Theft	63.434 ฿	51480 $
32	June 2011 Mt. Gox Incident	61.428 ฿	47123 $
33	Kronos Hack	53.633 ฿	42859 $
34	2012 Trojan	49.054 ฿	39146 $
35	Unnamed Event	44.860 ฿	35452 $
36	Mooncoin Theft	28.831 ฿	22346 $
37	Bitcoin7 Incident	20.703 ฿	15980 $
38	Ubitex Scam	20.189 ฿	15515 $
39	Betcoin Theft	19.490 ฿	15534 $
40	Bitcoin Syndicate Theft	18.469 ฿	14595 $
41	2012 50BTC Theft	16.678 ฿	13437 $
42	Andrew Nollan Scam	13.961 ฿	10895 $
43	October 2011 Mt. Gox Loss	10.804 ฿	8340 $
44	Bitscalper Scam	8.156 ฿	6461 $
45	Stone Man Loss	0.758 ฿	544 $
46	2014 Mt. Gox Collapse	-1.000 ฿	-824 $

List of events by ฿ value stolen

NB: This section is out of date.
In this section, each theft is listed along with its rank, severity, and time, ordered by the highest m฿ value stolen from most severe to least. To navigate to a theft, simply click on the link.

Critical (≥10 k฿)

Rank	Name	Time	Severity
1	Bitcoin Savings and Trust	2011–2012	est. 263024 ฿
2	Silk Road Seizure	October 2013	171955.09292687 ฿
3	MyBitcoin Theft	July 2011	78739.58205388 ฿
4	Linode Hacks	March 2012	l.b. 46653.46630495 ฿
5	July 2012 Bitcoinica Theft	July 2012	40000.00000000 ฿
6*	May 2012 Bitcoinica Hack	May 2012 Unresolved as of December 2012	18547.66867623 ฿ 39000 ฿ total impact

7	Allinvain Theft	June 2011	25000.01000000 ₿
8	Tony Silk Road Scam	April 2012	est. 30000 ₿
9	Bitfloor Theft	September 2012	u.b. 24086.17219307 ₿
10	*Bitomat.pl Loss*	August 2011	est. 17000 ₿

* Rank includes pass-through impact

Major (≥1 k₿)

Rank	Name	Time	Severity
11	Cdecker Theft	September 2012	9222.21195900 ₿
*	*Stone Man Loss*	August 2010	8999.00000000 ₿
12	*Stefan Thomas Loss*	June 2011	est. 7000 ₿
13	Bitcoin7 Incident	October 2011	l.b. 5000 ₿ u.b. 15000 ₿
14	BTC-E Hack	July 2012	est. 4500 ₿
15	Inputs.io Hack	October 2013	est. 4100 ₿
16	Mass MyBitcoin Thefts	June 2011	4019.42939378 ₿
17	Mooncoin Theft	September 2011	est. 4000 ₿
18	Kronos Hack	Unknown	est. 4000 ₿
19	Bitcoin Rain	2011–2013	est. 4000 ₿
20	2012 Trojan	September through November 2012	3500 ₿ a. 3457 ₿
21	Betcoin Theft	April 2012	3171.50195016 ₿
22	June 2011 Mt. Gox Incident	June 2011	l.b. 2643.27 ₿
*	*October 2011 Mt. Gox Loss*	October 2011	2609.36304319 ₿
*	Andrew Nollan Scam	February 2012	l.b. 2211.07786728 ₿
23	Bit LC Theft	February 2013	est. 2000 ₿
24	Bitcoin Syndicate Theft	July 2012	1852.61553553 ₿
25	ZigGap	2012	a. 1708.65967460 ₿
*	Bitscalper Scam	2012	est. 1350.10259806 ₿
26	Just Dice Incident	July 2013	a. 1300 ₿
27	BTCGuild Incident	March 2013	a. 1254 ₿
28	2012 50BTC Theft	October 2012	1173.51659074 ₿
*	Ubitex Scam	2011	a. 1138.98 ₿

* Unranked because USD value at time does not meet cutoff.

Borderline (<1 k₿)

Rank	Name	Time	Severity
29	2013 Fork	March 2013	960.09645667 ₿
30	Ozcoin Theft	April 2013	922.99063322 ₿

dree12
Legendary

Activity: 1148

Ignore

List of Major Bitcoin Heists, Thefts, Hacks, Scams, and Losses [2]
April 19, 2014, 01:57:04 AM

#2

List of events in rough chronological order

Stone Man Loss

Type: Loss
Time: August 09, 2010, 11:35:00 PM ± 600 s
Victim: Stone Man @BitcoinTalk
Status: Coins lost, effectively destroyed
Amount: *Exactly* 8999.00000000 ฿
Equivalent in USD: 544 $
Equivalent in January 2014 ฿: 0.758 ฿
Transaction of interest:
eb5b761c7380ed4c6adf688f9e5ab94953dcabeda47d9eeabd77261902fccccf
Due to not keeping proper wallet backups, 8999 ฿ sent as change were effectively destroyed when the private key controlling them was lost.

Ubitex Scam[2]

Time: April 2011 to July 2011
Victim: Investors on GLBSE of Ubitex
Status: Ubitex founder known, but nothing has been returned
Amount: *About* 1138.98 ฿[3]
Equivalent in USD: 15515 $
Equivalent in January 2014 ฿: 20.2 ฿
Ubitex was the first company to be listed on the now-defunct GLBSE "stock exchange", which has been criticized for its illegal operations.[4] The company was run by a minor, but this fact was not initially known.

Around 1000 ฿ of the missing investments are said to have been "spent", many of which were further scammed, or converted into USD without follow-up.

The Ubitex scam would not have been possible today. Bitcoin users at the time were enjoying their newly-acquired wealth thanks to significant appreciation. Most "investors" at the time were extremely naïve.

Stefan Thomas Loss

Type: Loss
Time: June 2011

Victim: Stefan Thomas
Status: Coins destroyed (no thief)
Amount: *Estimate* 7000 ฿[5]
Equivalent in USD: 124793 $
Equivalent in January 2014 ฿: 163 ฿
Stefan Thomas, an early adopter (and eventually developer) of Bitcoin, uses this loss to teach other Bitcoiners the importance of backups—many of them. He had three copies of his wallet, and yet lost all of them.

Allinvain Theft

Time: June 13, 2011, 05:52:00 PM ± 600 s[6]
Victim: Bitcointalk.org user "allinvain"
Status: Thief uncaught
Amount: *Exactly* 25000.01000000 ฿[7]
Equivalent in USD: 445688 $
Equivalent in January 2014 ฿: 581 ฿
Chief transaction of interest:
4885ddf124a0f97b5a3775a12de0274d342d12842ebe59520359f976721ac8c3
A polarizing theft, its authenticity has undergone much dispute. Some believe that it was set up as a ploy for donations. However, these critics often lack evidence to back up their claims. Indeed, the victim was an early adopter who mined many coins at a low cost, so there is little reason for him to sabotage Bitcoin's image.

Although the hack attracted great attention in its day, said fame has mostly subsided. Even today, however, the hack still affects Bitcoiners. A common debate among Bitcoin users is that of "tainting" coins, and this hack is often used as an example for why "tainting" coins is futile. In just a few years, coins stolen in this hack are now present in nearly every user's wallet. This rapid redistribution is often cited as a reason that a tainted coin system would certainly fail.

June 2011 Mt. Gox Incident

Time: June 19, 2011, 06:00:00 PM ± 1 h (theft), days ensuing (hacks & withdrawals)
Victim: Mt. Gox (some claim also customers)
Status: Thief uncaught
Components of theft:

- Stolen by thief: 2000 ฿[8]
- Additional withdrawn from Mt. Gox: 643.27 ฿[9] (lower bound)

Amount: *Lower bound* 2643.27 ฿
Equivalent in USD: 47123 $
Equivalent in January 2014 ฿: 61.4 ฿
Transactions: none released officially
Mt. Gox, then the leading ฿/USD exchange service, suffered a severe breach as a consequence of an ownership change. The sale conditions involved a share of revenue to be remitted to the seller. To audit this revenue, the seller was permitted an account with administrator access.[8]

The seller's administrator account was hacked by an unknown process. The priveleges were then abused to generate humungous quantities of ฿. None of the ฿, however, was backed by Mt. Gox. The attackers sold the ฿ generated, driving Mt. Gox ฿ prices down to cents. They then purchased the cheap ฿ with their own accounts and withdrew the money. Some additional money by non-attacking traders capitalizing on the dropping price and withdr time, including toasty, a member of BitcoinTalk.

Mt. Gox resolved the hack by reverting trades to a previous version. Many customers claim they have lost money from this reversion, but Mt. Gox claims it has reimbursed all customers fully for this theft. After the incident, Mt. Gox shut down for several days.[10]

The event's scale was widely disputed; some report a theft of almost 500000฿ due to related account hacking. However, these reports are sparse and disreputable. Closer inspection puts the losses at closer to 2500฿.

Aside from the direct damages of the theft, the hack involved a database leak. Some weaker passwords were used to conduct the relatively more severe Mass MyBitcoin Thefts.

Mass MyBitcoin Thefts

NB: Not to be confused with the far more severe MyBitcoin Theft.
Time: 2011-06-20 through 2011-06-21
Victim: MyBitcoin users with weak account passwords
Amount: *Exactly* 4019.42939378฿[11]
Equivalent in USD: 71656 $
Equivalent in January 2014 ฿: 93.4฿
Transactions: all to 1MAazCWMydsQB5ynYXqSGQDjNQMN3HFmEu[12]
Users with weak passwords on MyBitcoin who used the same password on Mt. Gox were in for a surprise after the June 2011 Mt. Gox Incident allowed weakly-salted hashes of all Mt. Gox user passwords to be leaked. These passwords were then hacked on MyBitcoin and a significant amount of money lost.

MyBitcoin estimates indicate 1% of MyBitcoin users were affected.[11] Users that were not affected would be later stolen from anyways, due to the subsequent MyBitcoin Theft.

MyBitcoin Theft

Time: Unknown time in July 2011 (claimed it was a process)
Victim: MyBitcoin & customers
Status: Thief unknown, planned shutdown suspected (disputed theft)
Suspects: "Tom Williams", likely pseudonym (founder of MyBitcoin)
Amount: *Exactly* 78739.58205388฿
Equivalent in USD: 1072570 $
Equivalent in January 2014 ฿: 1400฿
Transaction information: none
Little information was released about the MyBitcoin theft, however, many argue that Tom Williams ran it as a scam (and was not a theft per se). In terms of both dollars and bitcoins, this was by far the largest theft, however, it is possible it was simply a scam. Although MyBitcoin offered to release its code as a gift to the community, it failed to follow through on that promise. In the months ensuing, some evidence has been uncovered supporting mortgage broker Bruce Wagner; however, any evidence is inconclusive.

The theft resulted in the closure of MyBitcoin, which was once a successful Bitcoin company in Bitcoin's early days.

Bitomat.pl Loss

Type: Loss
Time: 2011-07-26
Victim: Bitomat.pl
Status: Coins destroyed (no thief)
Amount: *Estimate* 17000 ฿[13]
Equivalent in USD: 231570 $
Equivalent in January 2014 ฿: 301 ฿
Bitomat.pl, during a server restart, had its remote Amazon service that housed the wallet wiped. No backups were kept. Mt. Gox later bailed bitomat.pl out, and neither customers nor original owners suffered any loss from the incident.

Mooncoin Theft

Time: 2011-09-11
Victim: Mr. Moon, Mooncoin, & Customers
Status: Unknown (Federal intervention suspected)
Amount: *Estimate* 4000 ฿[14]
Equivalent in USD: 22346 $
Equivalent in January 2014 ฿: 288 ฿
Transactions: numerous
During the waning months of 2011, numerous alternative cryptocurrencies boomed, in part fuelled by Bitcoin's poor performance following the 2011 bubble. Exchanges such as Moonco.in were set up to capitalize on this alternative cryptocurrency boom. Suddenly, Mr. Moon disappeared. It is not known where the funds went.

At the time, SolidCoin was considered to be the most successful alternative cryptocurrency bar Bitcoin itself, though its success was short-lived. Moonco.in's hack had a devastating impact on that currency, with over 800000 SC removed from circulation, only to have been put back through SolidCoin 2.0. The effects on Bitcoin were also substantial, with an estimated 4000 ฿ lost. and the effect on Namecoin (another alternative cryptocurrency that was among the largest at that time) was not negligible.

Bitcoin7 Incident

Time: 2011-10-05 (UTC)
Victim: Bitcoin7 & Customers
Status: Indeterminate amount returned to customers by Bitcoin7
Suspects:

- Official story: Potential "inside job" (an employee perpetrated a theft).[15]
- Previous official story: Unknown hacker from Eastern Europe or Russia.[16]
- Suspected scam by several members of the community.

Amount: *Lower bound* 5000 ฿[15][17]
Equivalent in USD: 15980 $
Equivalent in January 2014 ฿: 207 ฿
An upstart exchange at the time, Bitcoin7, rapidly grew to the third-largest USD exchange (behind then-leaders Mt. Gox and Tradehill) but then suffered a major debilitating hack, or so the official story goes. It is widely suspected that there was no hack and Bitcoin7's operators simply ran away with the funds.

Bitcoin7 shut down because of this hack. The magnitude served as a reminder to the Bitcoin community to stop trusting new exchanges without identification.

The platform was however later sold for $10000 in 2013, and has since relaunched at Bitcoiner7.com but being branded still as Bitcoin7.

October 2011 Mt. Gox Loss

Type: Loss
Time: 2011-10-28T21:11 (UTC) [blockchain time, off by up to three hours]
Victim: Mt. Gox
Status: Coins destroyed (no thief)
Amount: *Exactly* 2609.36304319 ฿
Equivalent in USD: 8340 $
Equivalent in January 2014 ฿: 10.8 ฿
Transactions:

- 111291fcf8ab84803d42ec59cb4eaceadd661185242a1e8f4b7e49b79ecbe5
- 81f591582b436c5b129f347fe7e681afd6811417973c4a4f83b18e92a9d130
- ddddf9f04b4c1d4e1185cacf5cf302f3d11dee5d74f71721d741fbb507062e9
- 305fbc2ec7f7f2bc5a21d2dfb01a5fc52ab5d064a7278e2ecbab0d2a27b8c39
- f0137a6b31947cf7ab367ae23942a263272c41f36252fcd3460ee8b6e94a84
- 633acf266c913523ab5ed9fcc4632bae18d2a7efc1744fd43dd669e5f2869ce
- 5bd88ab32b50e4a691dcfd1fff9396f512e003d7275bb5c1b816ab071beca5
- 64c01fedd5cf6d306ca18d85e842f068e19488126c411741e089be8f4052df
- 3be0ac3dc1c3b7fa7fbe34f4678037ed733a14e801abe6d3da42bc643a6514
- 9edab6e7fadf1d6006315ff9394c08a7bf42e19cf61502200a1f73994f8da94
- 835d4dcc52e160c23173658de0b747082f1937d1184e8e1838e9394bc62c
- aebe39a99114f1b46fc5a67289545e54cbfec92d08fc8ffc92dc9df4a15ea05a
- aa62bdd690de061a6fbbd88420f7a7aa574ba86da4fe82edc27e2263f87439
- 6a86e6a5e8d5f9e9492114dafe5056c5618222f5042408ad867d3c1888855
- 7ad47a19b201ce052f98161de1b1457bacaca2e698f542e196d4c7f8f45899
- 0ca7f7299dc8d87c26c82badf9a303049098af050698c694fbec35c4b08fc3d
- 3ab5f53978850413a273920bfc86f4278d9c418272accddade736990d60bd
- 03acfae47d1e0b7674f1193237099d1553d3d8a93ecc85c18c4bec37544fe3
- 15ad0894ab42a46eb04108fb8bd66786566a74356d2103f077710733e051
- 2d00ef4895f20904d7d4c0bada17a8e9d47d6c049cd2e5002f8914bfa7f1d2
- 6d39eeb2ae7f9d42b0569cf1009de4c9f031450873bf2ec84ce795837482e7
- 07d33c8c74e945c50e45d3eaf4add7553534154503a478cf6d48e1c617b3f
- 6d5088c138e2fbf4ea7a8c2cb1b57a76c4b0a5fab5f4c188696aad807a5ba6

Mt. Gox did not pass the impacts of this incident on to customers.

dree12
Legendary

List of Major Bitcoin Heists, Thefts, Hacks, Scams, and Losses [3]
April 19, 2014, 01:57:16 AM

#3

Activity: 1148

Ignore

Bitscalper Scam[18]

Time: January 2012 to March 2012
Suspects:

- Alberto Armandi
  - bitdaytrade @BitcoinTalk
  - bitscalper @BitcoinTalk
  - jjfarren @BitcoinTalk

Victim: Users of Bitscalper
Status: MiningBuddy (bitcointalk.org user) attempted to reorganize bitscalper, but failed. No coins have been returned at all.
Amount: *Lower bound* 1350 ฿[19]
Equivalent in USD: 6461 $
Equivalent in January 2014 ฿: 8.16 ฿
Bitscalper was founded as an "arbitrage engine", and users were invited to

deposit money. It was promising extremely high and unrealistic returns. As a result, it was suspected of being a scam from the beginning, fears that were compounded due to a shady and anonymous management. After Bitscalper shut down without returning user funds, BitcoinTalk user MiningBuddy attempted to reform Bitscalper using the remnants of the engine. However, no success was found and the coins could not be returned.

Andrew Nollan Scam[20]

Time: February 2012
Victim: Investors of Shades Minoco, creditors of bitcointalk.org user "shakaru", investors of BitArb
Status: Andrew Nollan (a.k.a. shakaru[21]) (thief) known but disappeared, repaid some (not included in amount)
Amount: *Lower bound* 2211 07786728 ฿, possibly more [22]
Equivalent in USD: 10895 $
Equivalent in January 2014 ฿: 14 ฿

Linode Hacks

Time: Late 2012-03-01, Early 2012-03-02
Victim: Bitcoinica, Bitcoin.cz mining pool (Marek Palatinus), Bitcoin Faucet, possible others
Status: Thief unknown, not caught. Linode employee suspected.
Amount: *Lower bound* 46653 46630495 ฿
Composition of amount:

- *Bitcoinica*: 43554.02005417 ฿[23]
- *Bitcoin.cx*: 3094.45825078 ฿[24]
- *Bitcoin faucet*[25]: 4.98800000 ฿[26]

Equivalent in USD: 223278 $
Equivalent in January 2014 ฿: 282 ฿
Transactions of interest:

- 5a09f4ef0e91bc7bc044365cd27236fe4ac3c02088ac21ab51c93c8a11d33d
- 7b45c1742ca9f544cccd92d319ef8a5e19b7dcb8742990724c6a9c2f569ae7
- 901dbcef30a541b8b55fae8f7ad9917ef0754bda5b643705f3773e590785c4
- a57132e2cbc580ac262aa3f7bac1e441d6573f9633118bc48009618585a09
- a82ad85286c68f37a2feda1f5e8a4efa9db1e642b4ef53cb9fd86170169e5e6
- ff04763e3e8c93e43799dbbca833e183faad7e2611f20f136f47c2f1049481a
- 0268b7285b954448087539690 99f7ae43fb4193d442e3e0deebb10e2bb17
- 34b84108a142ad7b6c36f0f3549a3e83dcdbb60e0ba0df96cd48f852da0b1a
- 14350f6f2bda8f4220f5b5e11022ab126a4b178e5c4fca38c6e0deb242c40c5

In early March 2012, the New Jersey-based web and cloud hosting company Linode was suspected of robbing many popular Bitcoin services. A vulnerability in the customer support system was used to obtain administrator access to the servers. Once the Linode servers were compromised, eight accounts dealing with bitcoins were targeted.[27] The hardest hit was the bitcoin trading platform, Bitcoinica. This resulted in the unauthorized transfer of ฿ from the "hot wallets", a term used to describe operational withdrawal wallets, of the services affected. A severe bitcoin-denominated theft, the Linode theft also affected Tradehill, but no coins were stolen from them; instead, Tradehill had a short downtime because of the incident. In the aftermath of this theft, all the services migrated to other platforms. To this day, Bitcoin users fear Linode and usually refrain from using its services.

Betcoin Theft

Time:

Event	Time
Theft Commences Transaction: #1, #2	2012-04-11T10:55:54
Theft Continues Transaction: #3	2012-04-11T12:15:49
Theft Culminates Transaction: #4	2012-04-11T12:43:14

All times are blockchain time, and have possible error of up to 3 hours.

Victims: Betco.in, creditors

Status: Hacker not known. Some of creditors' deposits were repaid, around 2900 ฿ outstanding.[28]

Amount: *Exactly* 3171 50195016 ฿[29]

Equivalent in USD: 15534 $

Equivalent in January 2014 ฿: 19 5 ฿

Transactions of interest:[30]

- 266e4682abdf4932c4c271872ca9ba6bfdbe75941eb9ba4c4d81e4d3c7364
- 40fc8f6b2f222fb2871a38a245132ed1eada9ff6aec8d46ebe74b29c64fd82a
- bf70ac1d2b702dbe0e14fbefb3a0cb2ff5ee5aa425cfe4249f16d6ede7b3ff14
- 92968a2331a02a3128460a64ba16fbf8d3a2fc79ebc8882300015d3ca0e4fb

Similar to the Mooncoin Theft a year ago, and just as devastating, a gambling website's customers lost a large amount of money. This time, the owner took just as large a hit: all the deposits, plus non-live storage, were stolen. 2900 ฿ remains to be refunded to creditors today.[28]

Tony Silk Road Scam

Time: 2012-04-20

Victim: Buyers on Silk Road

Status: Scammer known to be Silk Road user "Tony76"

Amount: *Estimate* 30000 ฿[31]

Equivalent in USD: 146944 $

Equivalent in January 2014 ฿: 184 ฿

Users of Silk Road, an underground drug market using Bitcoin as the default currency, bought significant quantities of illicit drugs from trusted vendor "Tony76". Although Silk Road has an escrow system, trusted vendors are allowed to bypass the system and request that the buyers pay first. On April 20, which is a popular day for drug sales in American culture, Tony76 offered drugs at a significant discount. However, none of the products made it to the customers, revealing the sale as an elaborate sham.

May 2012 Bitcoinica Hack

NB: Impacts of this theft may continue to grow pending outcome of liquidation.

Time: May 12, 2012, 11:19:00 AM [blockchain time, off by up to three hours]

Victim: Bitcoinica, LLC

Status:

- Hacker unknown, minimal coins were returned.
- Venture capital group Wendon Group threatened legal action against

Bitcoinica Consultancy.
- Receivership in New Zealand ongoing.

Amount:
- Bitcoinica: *Exactly* 18547.66867623 ฿
- Creditors of Bitcoinica: Pending liquidation
  - BitMarket.Eu: *About* 19980 ฿

Total impact: *At least* **38527 ฿**
Equivalent in USD: 191638 $
Equivalent in January 2014 ฿: 241 ฿
Chief transaction of interest:
7a22917744aa9ed740faf3068a2f895424ed816ed1a04012b47df7a493f056e8
Zhou Tong, former founder of Bitcoinica, discovered an entry into Bitcoinica's Rackspace server through an excessively privileged compromised email address. This caused the theft of the entire "hot wallet", funds stored on-site, as well as the loss of the main database. No backups were kept. Bitcoinica shut down because of this incident. The claims process is still ongoing; however, Bitcoinica is now entering receivership.

On December 21, 2012, it was discovered that BitMarket.eu, a company run by Maciej Trębacz, lost a large portion of customer funds which were stored on Bitcoinica.[32] These customers were reportedly unaware that their funds were stored on Bitcoinica. Return of a portion of these funds is still possible, pending the outcome of liquidation.

Bitcoin Syndicate Theft

Time: July 04, 2012, 02:34:19 PM (Mt. Gox time)
Victims:
- Bitcoin Syndicate
  - Paul Mumby
  - Shareholders on GLBSE

Suspect: IP 130.83.54.115
Status: Pending
Amount: *Exactly* 1852.61553553 ฿
Equivalent in USD: 14595 $
Equivalent in January 2014 ฿: 18.5 ฿
Medium of theft: Mt. Gox
Transactions of interest: On Mt. Gox. Withdrawal transaction was 4c61d3639f010e30ad305b294cd128f381f58fc161d0badda1f39807dc2f12f7.
A hacker infiltrated the Mt. Gox account used by Bitcoin Syndicate, sold off the USD owned, and withdrew all balances.

July 2012 Bitcoinica Theft

Time: 2012-07-13 (UTC)
Victims:
- Bitcoinica, LLC
- Creditors of Bitcoinica (former users of Bitcoinica)

Suspects:

Suspect	Accused by	Defended by	Additional evidence
Zhou Tong	AurumXChange Mt. Gox	Tihan Seale	Selling bitcoins after event
Chen Jinghai	Zhou Tong		

Status: All funds returned
Amount: *Exactly* 40000.00000000 ฿[33]

Equivalent in USD: 315133 $
Equivalent in January 2014 ฿: 399 ฿
Medium of theft: On MtGox.
On July 13, 2012, a thief compromised the Bitcoinica Mt. Gox account. The thief made off with around 30% of Bitcoinica's bitcoin assets, which are likely to cost claimants of Bitcoinica debt. Additionally, 40000 USD was also reported to be stolen. The thief is still unknown at this point, but the theft has supposedly been entirely returned. This theft further complicated the [#=may_2012_bitcoinica_hack]May 2012 Bitcoinica Hack[/iurl].

BTC-E Hack

Time:

Event	Time
Commencing	2012-07-31 00:07 (UTC)
Action taken	2012-07-31 06:30 (UTC)

Victim: btc-e.com
Suspects:

- (unlikely) BTC-E chat user **MrWubbles***
  * Person has denied committing theft after initially pretending to do it. Evidence supports the faked theft admission as mere trolling.
- (unlikely) **BTC-E** (accusation of inside job): Little evidence has been provided; as BTC-E reimbursed its customers, the only thing it could gain from faking the theft was PR—and faking poor security is usually not considered useful PR.

Status: Pending
Amount: *Estimate* 4500 ฿[34]
Equivalent in USD: 35452 $
Equivalent in January 2014 ฿: 44 9 ฿
On July 31, 2012, the BTC-E Liberty Reserve API secret key was broken. This key was shorter than it needed to be at only 16 characters long. The attacker initiated many Liberty Reserve deposits and injected large amounts of USD into the system, which were quickly sold for ฿. Not all ฿ was withdrawn; official estimates state that the scope was limited to 4500 ฿. Similar to the June 2011 Mt. Gox Incident, the BTC-E market was disturbed during the duration of the hack. The handling of this hack was widely applauded after BTC-E revealed they would cover the losses and revert to a backup made just before the hack.

Kronos Hack

Date: August 2012
Suspects:

- Alberto Armandi[35]
  - bitdaytrade @BitcoinTalk
  - bitscalper @BitcoinTalk
  - jjfarren @BitcoinTalk

Victim: Kronos.io investors (Brian Cartmell)[36]
Status: Legal action possibly pending
Medium: Mt. Gox
Amount: *Estimate* 4000 ฿[35]
Equivalent in USD: 42859 $
Equivalent in January 2014 ฿: 53 6 ฿
Kronos.io, a Bitcoinica-esque startup, was hacked in an event shrouded in mystery even today. Led by Jonathon Ryan Owens, who was simultaneously running other new startups on GLBSE (an upstart Bitcoin "stock exchange"),

Kronos.io hired several well-known Bitcoin personalities to do wo and coding. One of these was Alberto Armandi, who was related t scam earlier that year.[36]

Alberto Armandi reportedly hacked into the website he himself hel vulnerability was in the withdrawal script that Alberto coded, repor intentionally as a backdoor.[36] Although incredible, Armandi has also released a story denying he hacked the website. Instead, he blamed the theft on Jonathon Ryan Owens intentionally pocketing the majority of the funds with only 1000 ฿ being stolen by an unknown hacker.[37]

Bitcoin Savings and Trust

Time: 2011–2012
Victim: Creditors of First Pirate Savings and Trust, later Bitcoin Savings and Trust
Status: **Trendon Shavers (Perpetrator) caught by SEC**[38]
Amount: *Lower bounds* **150649 ฿**[38], **193319 ฿**[39], **200000 ฿**[40]; *Estimate* 263024 ฿[41]; *Upper bound* **>700467 ฿**[42]
Equivalent in USD: 2983473 $
Equivalent in January 2014 ฿: 3700 ฿
More information on Trendon Shavers default.

Bitfloor Theft

Time:

Event	**Time**
Theft Commences Transaction: #1	2012-09-04T03:07:39
Theft Continues Transaction: #2, #3	2012-09-04T03:12:52
Theft Culminates Transaction: #4, #5	2012-09-04T03:43:33

All times are blockchain time, and have possible error of up to 3 hours.
Victims: Bitfloor, creditors
Status: Hacker not known, but IP is 178.176.218.157. Some coins repayed to creditors.
Amount: *Upper bound* 24086.17219307 ฿]
Equivalent in USD: 273209 $
Equivalent in January 2014 ฿: 339 ฿

Transactions of interest:[43]

- 83f3c30dc4fa25afe57b85651b9bbc372e8789d81b08d6966ea81f524e0a02
- d5d23a05858236c379d2aa30886b97600506933bc46c6f2aab2e05da85e61
- 358c873892016649ace8e9db4c59f98a6ca8165287ac80e80c52e621f5a26e
- f9d55dc4b8af65e15f856496335a29e2be40f128a7374c75b75529e864579f
- 42ea472060118ee5aee801cdedbc4a3403f3708a87340660f766e2669f0afe

Although the keys to the hot wallet of Bitfloor was secured, an unencrypted backup was mistakenly stored on some of the servers. After a hacker gained entry, most of not only the hot wallet but also the cold wallet was stolen. To this date, none of the coins have been returned by the hacker to Bitfloor. Although

Bitfloor briefly shut down after the incident, it has since restarted and has committed to repaying its creditors.[44] Unfortunately, Bitfloor's banks shut down the exchange's operation before all coins could be recouped.

Cdecker Theft

Time: September 28, 2012, 07:21:14 PM
Victim: Cdecker
Status: Thief IP may be 178.140.220.181[45]
Amount: *Exactly* 9222 21195900 ฿
Equivalent in USD: 104607 $
Equivalent in January 2014 ฿: 130 ฿
Transactions of interest:

- 6f85951bcecbe64999ad192275af087c5be2922ee13937693992c1ddf9ae8c
- 8e6a2d0b8132d3d9edc1fcffe1b3079de59c10c67522e2abc51c1d84b260fda

A supposedly long-time user of Bitcoin found his personal wallet emptied of a significant amount in late September 2012. Because far more severe personal thefts had occurred in the past, the theft went by without much incident.

2012 50BTC Theft

Date: 2012-10-13
Victim: 50BTC Mining Pool
Status: Unresolved.
Transactions of interest:[46]

- 9dfdb24667657365c469ff20568fcc820f6f028a125d9c22dc521ae44dcf7c5e
- bd2ad7b49c22d12cf2f8f12ef601952aed2a96907af4df732156fd90165b5ef5
- d0035ad189634e90239cca82eb53f78e08c0179620b2bd24e2cb291478c7d
- a2b642bafea45bc128d81314ef33542bc807811ba066329eaa1306bd62bec

Amount: *Exactly* 1173 51659074 ฿
Equivalent in USD: 13437 $
Equivalent in January 2014 ฿: 16 7 ฿
The 50BTC mining pool suffered a hack of the billing software in late 2012. They were unable to identify the vulnerability. After the incident, 50BTC completely rewrote the billing software.[46]

2012 Trojan

Time:

Event	**Time**
Theft Commences Transaction: #1	2012-10-18 22:56:56
Theft Continues Transaction: #2, #3, #4, #5, #6, #7, #8, #9, #10	September, October and November 2012
Mralbi @BitcoinTalk theft Transaction: #11	2012-11-16 03:30:13
Theft Culminates Transaction:	2012-11-16 03:30:13

#12, #13
Victim: Various, incl. Mralbi @BitcoinTalk
Status: Thief IP may be:

- 97.106.160.84
- 178.177.115.229

Amount:

- Through blockchain: *Exactly* **3257.00000000 ฿** +0.02450000 ฿ tx fees
- Through Mt. Gox: *Lower Bound* **200 ฿**

Amount: *About* 3457 ฿
Equivalent in USD: 39146 $
Equivalent in January 2014 ฿: 49 ฿
Transactions of interest:

- 04e378f81eb620f21927639cd4cda00e0473ca958f4d21f2255f37554b5440
- 065e7ff6b1503fc023876ffe930dcd9866531812e40bbda72835f232c2f2391
- 0723b67631588b6d5a4a406a9ef8d431c0d5282c6f1cb308fef57c7503d831
- 0ae924c33555b294a3f0b256da6a02ab996d30be00eaf184d53281009a3a5
- 3f938408deb6d20a74f6256d3ba0217df266450d4c00c40d94df7b840f66db
- 9766b624e004ad1a9369b1b461d33f57e7dddabb43942d34ac10e912cd9c
- 2db76ebd4b5eecf008334d1bdc1f63f764ca3fb9275557a2a82d52ebf52eea
- c041a74fd565c3eb247ff4b1fb6eb0ab9299c3e7d58e5172c28cbe9540858d
- 82719bedd0730511385faf68d88b9a03e269a40e3fa5f269efe4a9fc3a821f7
- 2bc69aa29f56d7051f9cb19bf923c5e2a81879b4f6a3bc849f4166f56d417c2
- 8d6602b0e8e4479d79e5dab0c35bdb4f7545513cb426411348ec1502413a
- 3a66ebef43041f230e799f1efd3a93e41f875c718da683e236632e13a70cf8
- 0197692748ba894697a0a48fdfdb3e72f3275b079005efad8be062de38b65

A trojan horse stole thousands of ฿ between September and November of 2012. BitcoinTalk user "mralbi" was a major victim, losing almost 2600 ฿.[47] The same hacker also stole 200 ฿ from Mt. Gox accounts, supposedly with the same trojan which doubled as a keylogger.

dree12
Legendary

List of Major Bitcoin Heists, Thefts, Hacks, Scams, and Losses [4]
April 19, 2014, 01:57:36 AM
#4

Activity: 1148

Ignore

Bit LC Theft

Time: Discovered February 13, 2013
Victim: Bit LC Inc. and miners
Status: Suspected theft by "Erick", could be misunderstanding.
Amount: *Estimate* 2000 ฿[48]
Equivalent in USD: 51480 $
Equivalent in January 2014 ฿: 63 ฿
Transactions of interest:
This alleged theft was unique in that coins held in the hot wallet were safe, but coins held in a cold wallet compromised. The thief is not expected to have access to the coins regardless, so there was little financial gain from this theft. Erick, allegedly the only one with physical access to Bit LC Inc.'s cold wallet, has failed to communicate and withdraw coins. Bit LC Inc. therefore was required to declare bankruptcy. There is no proof that Erick intentionally stole the coins; indeed, some evidence asserts that he or she may simply have disappeared in some manner.

BTCGuild Incident

Time: March 10, 2013
Victim: BTCGuild mining pool

Status: 16 thieves, one has returned 47฿
Amount: *About* 1254฿[49]
Equivalent in USD: 72556 $
Equivalent in January 2014 ฿: 88.9 ฿
When BTCGuild was upgrading the Bitcoind client to 0.8, the mining pool used its original upgrade plan. However, 0.8 is unique in that it reindexes the blockchain. This prompted a temporary state in which the pool was paying out for difficulty-1 shares, as that was the extent of the blockchain parsed. Sixteen separate thieves subsequently emptied the hot wallet. 47 ฿ have been returned to the pool. The pool would on the following day lose even more money thanks to a bug causing its recent upgrade to 0.8 to differ from nodes running 0.7 or lower.

2013 Fork

Time: 2013-03-11
Victims: OKPay, many mining pools including slush, BTCGuild, etc.
Status: OKPay double-spend attack resolved.
Amount: *Exactly* 960.09645667฿[50]
Equivalent in USD: 55551 $
Equivalent in January 2014 ฿: 68.1 ฿
A major blockchain fork occurred due to a bug in Bitcoin-Qt clients which had not upgraded to the new 0.8 version. Unfortuantely, those clients formed the majority of Bitcoin users at the time. The resulting fork split mining pools; those that had upgraded lost block revenue. Some mining pools took the hit, whereas others passed the cost on to miners.

The fork also made possible isolated double-spending attacks. Only one such attack was conducted, costing OKPay significantly. Luckily, the thief has since returned the money.

Bitcoin Rain

Date: 2011-10-03 to 2013-03-28
Victims: Investors in Bitcoin Rain, account holders on Mercado Bitcoin.
Perpetrator: Leandro César
Amount: *Estimate* 4000฿[51]
Equivalent in USD: 231440 $
Equivalent in January 2014 ฿: 284฿
A suspected long-running con likened to the infamous Bitcoin Savings and Trust, Bitcoin Rain finally defaulted on March 28, 2013. Leandro César claimed there was a security breach on his exchange website Mercado Bitcoin.[52] As Bitcoin Rain's funds were stored there, investors in Bitcoin Rain as well as account holders on Mercado Bitcoin lost money. Some money was reportedly paid back, but the vast majority is still outstanding.

ZigGap

Date: February to April 2013
Victim: Investors and creditors of ZigGap
Amount: *About* 1708.65967460฿[53]
Equivalent in USD: 195490 $
Equivalent in January 2014 ฿: 240฿
User aethero, who was originally a reputable Bitcoiner, founded ZigGap after two previously succesful ventures, including BitPantry. Purporting to offer easy ways to purchase ฿, ZigGap saw little business. The founder seems to have also

suffered mental illness in the latter stages of business operation.[54]

Ozcoin Theft

Time: 2013-04-19
Victim: Ozcoin mining pool
Status: Thief, a user of Strongcoin, known but not disclosed. Strongcoin seized funds and returned 568.94 ฿ to the mining pool operator.[55]
Amount: *Exactly* 922.99063322 ฿[56]
Equivalent in USD: 105600 $
Equivalent in January 2014 ฿: 130 ฿
A hacker managed to infilterate Ozcoin's payout script, such that all money was paid out to the hacker's address. Luckily, a day later Strongcoin seized most of the stolen funds and promptly returned them to Ozcoin.

Vircurex Theft

Date: 2013-05-10
Victim: Vircurex and shareholders
Transactions of interest:[57]

- cbce6bd1e274a9ea9d6946feaf4a1b0f80a5885a8482f4ebf3caa052f22bb4b
- 85489430661f3041608749acb3019a1dcbf07a60f22e4bc43acfd05b46496c

Amount: *Exactly* 1454.01500000 ฿[58]
Equivalent in USD: 163351 $
Equivalent in January 2014 ฿: 200 ฿
The hot wallet and "warm" wallet of Bitcoin to alternative cryptocurrency exchange service Vircurex was emptied in May 2013, resulting in a significant loss of three currencies: Bitcoin, Terracoin, and Litecoin.[57] Initially, Vircurex operated normally despite the loss, though it no longer paid dividends to shareholders. In March 2014, due to strain caused by large withdrawals (in addition to a default by AurumXChange, a fiat processor Vircurex used), Vircurex froze large quantities of many currencies; however, it promises to pay these back eventually.[59]

James Howells Loss

Type: Loss
Date: July 2013[60]
Victim: James Howells
Amount: *Estimate* 7500 ฿[61]
Equivalent in USD: 627659 $
Equivalent in January 2014 ฿: 764 ฿
A hard drive containing keys to bitcoins generated in 2009 were accidentally thrown away in 2013 after a period of meteoric price rallies. The owner, James Howells, reportedly attempted to retrieve the money by going to the landfill where the hard drive was buried, but gave up after learning of the difficulty of retrieving trash.[61]

Just Dice Incident

Time: 2013-07-15
Victim: Just-Dice investors, Dooglus
Suspect: Just-Dice.com user "celeste", who claims he was hacked.
Status: Bets rolled back.
Amount: *About* 1300 ฿[62]

Equivalent in USD: 108794 $
Equivalent in January 2014 ฿: 132 ฿
A player on Just-Dice.com with an especially large balance aske 1300 ฿. Because the hot wallet did not contain that much mone operator "dooglus" manually processed the transaction from the However, "dooglus" forgot to remove the balance in Just-Dice.c The Just-Dice.com user then proceeded to bet the fake balance website and subsequently lost it all. Because of the manner Just-Dice.com is structured, the website lost money even though the malicious user did not earn any money from the theft.

To recoup losses, the operator rolled back the gambling losses and corrected the wrong balance. This resulted in losses for all "investors" of Just-Dice.com; however, the operator explains that nobody actually lost money because the bet should never have happened. In conclusion, it seems that odd decisions on the malicious user's part and probability ensured no actual loss from the incident, even though 1300 ฿ was stolen. The amount was simply lost back to Just-Dice.com thanks to luck in the website's favour.

Silk Road Seizure

Dates:

- 2013-10-02: First seizure (Silk Road user funds)
- 2013-10-25: Second seizure (Ross Ulbricht's personal coins)

Victim: Silk Road, Ross Ulbricht, Silk Road users
Perpetrator: FBI seizure

Amount:

- First seizure: 27618.69843217 ฿[63]
- Second seizure: 144336.39449470 ฿[64]

Total: *Exactly* **171955**.09292687 ฿
Equivalent in USD: 26867560 $
Equivalent in January 2014 ฿: 32700 ฿
Silk Road was a former underground marketplace that dealt primarily in Bitcoin. Run by Ross Ulbricht, it was once widely known for frequent narcotic sales.[65] Although it operated under the jurisdiction of the United States, it made little attempt to comply with US law.[66] However, clever use of the Tor technology allowed Silk Road to escape the authorities for years.

Finally, in October 2013, the FBI was able to produce conclusive evidence of Ross Ulbrict's culpability. Ulbricht was found in San Francisco and arrested.[67] In the days ensuing, it seized a large portion of Ulbricht's personal wealth in addition to stored balances by Silk Road users.[68] However, the FBI has yet to successfully seize an estimated remaining 400000 BTC in Ulbricht's personal wallet.[69].

The first seizure came right as Silk Road's domain was seized, and included funds belonging to Silk Road users. The second seizure came several weeks later, seizing coins belonging to Ross Ulbricht himself.

This seizure is notable in that it is the first major legally authorized seizure. At the moment, Ulbricht is awaiting trial in New York.[70]

GBL Scam

Time: Between May 2013 to October 2013
Date of shutdown: 2013-10-26[71]
Victim: Chinese investors in "GBL".
Amount: *Estimate* 22000฿[71]
Equivalent in USD: 3437446 $
Equivalent in January 2014 ฿: 4190฿

Beijing-based "GBL" was advertised as a Hong Kong-based e
down after attracting significant investment. At the time, the
craze in China, which lasted for much of the latter half of 2013 and was credited as the leading cause of the November 2013 bubble.

Inputs.io Hack

Date: 2013-10-26[72] (disputed)
Victim: Inputs.io, passed on to creditors.
Perpetrator: Accusations of inside job.
Transaction of interest:
9536feebe3a50b94f85ca27d56e669a7209bd4188385d55c5b97227c95cf7f74[73]
Amount: *Estimate* 4100฿[74]
Equivalent in USD: 640615 $
Equivalent in January 2014 ฿: 780฿

Inputs.io, a web wallet service run by BitcoinTalk user TradeFortress, was supposedly "hacked" in October 2013 and was unable to repay user balances in full. There are many accusations of the hack being an inside job. TradeFortress had a contentious reputation and had supposedly scammed two separate people before this incident.[75][76] When the theft was announced in November 2013, TradeFortress began offering partial refunds; however, 4100฿ was not paid back as that was the shortfall from the supposed "hack".

Bitcash.cz Hack

Date: 2013-11-11
Victim: Bitcash.cz
Perpetrator: Unknown
Transaction of interest:
44f66e60460926d1ac75667ce3060429000f7cbd30e9afe5a1f3af62cae7727f[77]
Amount: *Exactly* 484 76688536฿[78]
Equivalent in USD: 247422 $
Equivalent in January 2014 ฿: 303฿

A Czech Bitcoin exchange, bitcash.cz, reported a hack in mid-November 2013. The hack was relatively minor; however, Bitcoin prices were very high at the time relative to the preceding and succeeding months.

BIPS Hack

Date: 2013-11-17
Victim: BIPS, passed on to creditors
Perpetrator: Unknown
Transaction of interest:
ec01b909b6522e005071e694e3d865056189faff1be516c5e95812720b8cf585[79]
Amount: *Exactly* 1295.00000000฿[78]
Equivalent in USD: 660959 $
Equivalent in January 2014 ฿: 808฿

The then up-and-coming payment processor BIPS suffered a major breach in mid-November 2013, a month that saw numerous other companies shut down due to hacks. BIPS refused to refund creditors, justifying the loss as inevitable for a web wallet. BIPS made an attempt to continue business despite the hack.

PicoStocks Hack

Date: 2013-11-29
Victim: PicoStocks
Perpetrator: Unknown
Transactions of interest:[80]

- d99281bae8acafc6c96cefb54d37f81e5f78898fd8ccb12493f89236bec476e
- 28c9d7b0b31c9262958b88c42b1703098d44574e0830173c0b5cfe2a7949

Amount: *Exactly* 5896 23098163 ฿[78]
Equivalent in USD: 3009397 $
Equivalent in January 2014 ฿: 3680 ฿
PicoStocks, a stock exchange using a novel means of circumventing legal regulation, reported that someone that previously had access to PicoStocks keys used them to defund both hot and cold wallets. Creditors were reportedly unaffected as, despite the magnitude of the loss, PicoStocks covered it completely.

Sheep Marketplace Incident

Date: 2013-12-02
Victim: Sheep Marketplace users
Perpetrator: Official story blames user EBOOK101; suspicion of an inside job[81]
Transactions of interest: Disputed
Amount: *Estimate* 5400 ฿[81]
Equivalent in USD: 4070923 $
Equivalent in January 2014 ฿: 4980 ฿
Czech-based underground marketplace Sheep supposedly suffered a major breach causing the loss of 5400 ฿, which was passed down to its users. This official story is disputed, with many claiming the actual loss was far more severe. However, estimates of over 90000 ฿ being stolen by the operator of Sheep were found to have accidentally tracked BTC-E internal wallet movements, thus discrediting this alternative explanation.[82]

dree12
Legendary

Activity: 1148

Ignore

List of Major Bitcoin Heists, Thefts, Hacks, Scams, and Losses [5] #5
April 19, 2014, 01:57:53 AM

Silk Road 2 Incident

NB: Not to be confused with the Silk Road Seizure.
Date: 2014-02-13
Victim: Silk Road 2 users
Perpetrator: Official story[83] blames three attackers; many suspect an inside job.
Transactions of interest: See official statement.
Amount: *Estimate* 4400 ฿[84]
Equivalent in USD: 3624866 $
Equivalent in January 2014 ฿: 4400 ฿
Defcon, an administrator at underground marketplace Silk Road 2 (not to be confused with Silk Road), noticed that funds held for the escrow service were stolen in February 2014. "Transaction malleability", an issue with the Bitcoin protocol at the time that also affected some other services, was blamed for the

theft.[83] Others note that transaction malleability is unlikely to result in coins being stolen and belive the Silk Road 2 incident to be an inside job.

Several months after the incident, it was reported that Silk Road 2 is paying users back with funds earned from commissions[85]

2014 Mt. Gox Collapse

Date: Ongoing
Victim: Mt. Gox and users
Perpetrator: Unknown
Amount: Unknown
More information will be added as the story develops.

Flexcoin Theft

Date: 2014-03-02
Victim: Flexcoin and users
Perpetrator: IP address 207.12.89.117[86]
Transactions of interest:[86]

- a1b887233c06490fbdeb2c8779fd47e1f93a68d16928766d45879dcfc39571
- e03686a33aacbd462cb0a64345513dfb6c20a442a4cc651e5e2eaeca54bfe0
- 4811e548e7f2cb3785c30daecafcb4bffa239da7228a13ee48f1226f179f0cec
- 00e2b00fb3c5cf2edb71c8f4a856111e614c3681503c583eab84cd67a2850e
- b21e9bee8a9bfe040b8bfde23c6ba26e345b22581cb96f5af8b6fcbf6579a07
- fde8ae93bb8fe82583dd9bc94528b07eebddf7257d30b7d25a1e4726948fa4
- ebc684fd60f537d26fb82e26aeb4e2f00bf570ca1fd2eb2052eb10487be465e
- 90908281e8a6039569e83c6b28b3a8ea582c6d9b9bd58f66962bca6918c49

Amount: *Exactly* 896.10380000 ฿[87]
Equivalent in USD: 738240 $
Equivalent in January 2014 ฿: 896 ฿
Canadian-based Bitcoin "bank" Flexcoin reported a security breach causing the loss of most hot wallet funds, thanks to a race condition.[86] Creditors were not reimbursed.

CryptoRush Theft

Date: 2014-03-11[88]
Victim: CryptoRush (alternative cryptocurrency exchange) and users
Perpetrator: Identified as an "IP from Ukraine".
Amount: *About* 950 ฿[88]
Equivalent in USD: 782641 $
Equivalent in January 2014 ฿: 950 ฿
Cryptocurrency exchange cryptorush.in suffered a security breach leading the the loss of almost 1000 ฿ and a significant amount of other cryptocurrencies such as Litecoin.

The exchange attempted to continue operations and withhold its insolvency from its users. Some days later, it created its own propietary cryptocurrency, purporting to pay dividends to owners.

The exchange later suffered another bug leading to the loss of cryptocurrency balances in Blackcoin. A support employee later leaked details of the theft and the attempts to cover it up.[88]

dree12
Legendary

Activity: 1148

Ignore

List of Major Bitcoin Heists, Thefts, Hacks, Scams, and Losses [6]
April 19, 2014, 01:58:23 AM
#6

This post is reserved.

dree12
Legendary

Activity: 1148

Ignore

List of Major Bitcoin Heists, Thefts, Hacks, Scams, and Losses [7]
April 19, 2014, 01:58:37 AM
#7

This post is reserved.

dree12
Legendary

Activity: 1148

Ignore

List of Major Bitcoin Heists, Thefts, Hacks, Scams, and Losses [8]
April 19, 2014, 01:58:53 AM
#8

Thefts not included

Some thefts in Bitcoin's history, although severe and damaging to Bitcoin users, did not involve the theft of over one thousand bitcoins. These thefts are listed below.

- World Bitcoin Exchange, due to fraudulent activity, stole over 5000฿ worth at the time in AUD. The total amount stolen was **25779.49 AUD**. More information: https://bitcointalk.org/index.php?topic=65867.msg923845#msg923845
- Tradehill was repeatedly hassled by Dwolla, and eventually dropped support after being scammed off 17000 USD. Later fraudulent transactions ended up costing the exchange even more, and after the March 2012 Linode Hacks they shut down, citing **100000 USD** stolen or scammed through fraud.

Minor but notable thefts

Other thefts are minor, but are unique in some manner (for example, interesting methods or a first of its kind).

- First recorded physical theft of bitcoins: https://bitcointalk.org/index.php?topic=52206.0
- Coordinated hacking of BitcoinTalk accounts allowed theft of many "loaned" bitcoins: https://bitcointalk.org/index.php?topic=61500.0
- Bitcointalk.org user "Goat" lost 400฿ through sending to a wrong address. These bitcoins were later recovered: https://bitcointalk.org/index.php?topic=82600.0

Other thefts outside the scope of this list

Too small

The thefts below, based on all available estimates, are absolutely below the requisite margin and cannot be included on this list.

- Polish exchange http://bidextreme.pl/: 170฿[89]
- Mining pool http://bitclockers.com/: Exact amount indeterminate; but lack of public outrage suggests it was not very high.
- "Exchange" Bitcoin2Cash: 100฿[90]

Borderline theft

The thefts below are near the requisite margin for the time that it took place, but all or practically all reasonable estimates put it below. New estimates may move these thefts to the main list.

- Pony Botnet [91]
  While it is conceivable that it has continued to steal digital currency, the amount given in the article is stated as an upper bound, and also includes unrelated digital currencies. Best estimates place amount stolen at 450฿.

On watch

This section is reserved for possible thefts and scams that bear mentioning. It is not an endorsement, and the presence on this list **does not imply** a scam.

- Everydice, which currently does not meet the lower bound, may reach it if the site owners disappear.[92]

Pirate default

NB: This section is mostly outdated and is preserved for historical reasons.
It's over. I personally will offer sympathy to those who may have lost.

I'm at odds about what to do about this. On one side, the implications are clear: Pirate@40 willingly scammed hundreds off their money, which best estimates put at around 500000฿. Such an amount, making up more than 5% of all ฿ in circulation, in unprecedented in the history of Bitcoin. It is my duty to include it in this list, as not doing so would be dishonest. However, by doing so, the complexity of this situation requires restructuring at the least.

I am looking for community input into this issue. There are missing data which I deem important, and I welcome any estimates for the values I list below.

- Total ฿ defaulted on
- Total investors directly with Pirate
- Total investors exposed through defaulting passthroughs
- Total investors exposed through all passthroughs, including ones that compensated partially or fully

There are also semantic issues. For example, the list of victims is large and diverse; some were affected in different ways than others. Certain passthrough owners have repaid in Pirate's name in full or in part (notme). The honest passthrough owners (to use the term to describe veracity, to withhold it not to imply malevolence) have without doubt been hurt, but then again many would have profited greatly from the 7% while offered.

I ask for input on handling of semantics. The list below will provide a general overview of decisions that need to be made.

- BS&T has paid interest. Should this amount be included in the amount scammed, or excluded?
- People have made bets. Should reference to this be included?
- Passthrough owners have been hurt in different manners. To what degree should this be highlighted?

Any other help in this complex issue, I would appreciate greatly. I also would like to take this time to, once again, offer heartfelt condolences to all who have suffered.

References & Footnotes

- [1]: Exchange rate data is mainly from Bitstamp and inflation data mainly from the United States Bureau of Labor Statistics. More precisely, Mt. Gox price data is used up until 2013-06-09, but Bitstamp price data is used starting from 2013-06-10. US CPI data published by the United States Bureau of Labor Statistics is used throughout.
- [2]: Note on the inclusion of this scam: Evidence suggests that the founder withheld information from investors, such as the fact that he was a minor. Although a portion of the losses can be attributed to incompetence, there is significant reason to believe that the founder kept a significant chunk of the invested funds to himself.
- [3]: Amount "invested" into Ubitex on GLBSE.
- [4]: Olivia Solon, "Founder reflects on the closure of Bitcoin stock exchange GLBSE".
- [5]: Wired Magazine "The Rise and Fall of Bitcoin".
- [6]: Ten minutes, or 600 seconds, represents Satoshi's estimated block transmission time.
- [7]: Allinvain's personal account.
- [8]: Mt. Gox official press release.
- [9]: Admission by BitcoinTalk user "toasty".
- [10]: Daily Tech, recap of the incident.
- [11]: Signed message by MyBitcoin operator "Tom Williams".
- [12]: Blockchain.info.
- [13]: This was the official estimate, which is likely inexact (potentially a lower bound). Since no transaction took place, there was no record on the Blockchain.
- [14]: This is a conservative estimate based on the values of SolidCoin lost, and assuming that the values of Bitcoin lost resembled those.
- [15]: Official statement by Bitcoin7 owners in a listing to sell the code behind Bitcoin7.
- [16]: Initial official statement by Bitcoin7, quoted by Stephen Gornick and retrieved on BitcoinTalk.
- [17]: 5000฿ is almost certainly a low estimate, as the source is a listing that promotes the successes of Bitcoin7 and fails to acknowledge the severity of the theft. If Bitcoin7 disappeared, then the value should be bounded above by 15000฿, which is based on the size of order books at the time.
- [18]: Note on the inclusion of this scam: Bitscalper was a Ponzi scheme, paying investors with other investor money, and failed to disclose such.
- [19]: Brief textual analysis conducted specifically for this list.

- [20]: **Note on the inclusion of this scam: Although initial business failures are a result of incompetence, Andrew Nollan later failed to communicate professionally with investors, and thereafter disappeared, indicating that investor losses were at least partially due to Nollan's intent or negligence.**
- [21]: Shakaru's DeviantArt account.
- [22]: Google Docs document.
- [23]: Bitcoinica's official statement.
- [24]: Marek Palatinus's account.
- [25]: Gavin Andresen's account.
- [26]: Blockchain.info transaction.
- [27]: Linode official statement.
- [28]: Official post-mortem report.
- [29]: Blockchain.info address listing.
- [30]: Official account; source for destination address.
- [31]: Account of a Silk Road user.
- [32]: Official statement by BitMarket.eu.
- [33]: **This was the Mt. Gox daily limit for withdrawals.**
- [34]: Official estimate.
- [35]: Statement by former GLBSE operator Nefario, quoted by Bjork @BitcoinTalk.
- [36]: **Statement by Matthew Neal Wright in email response.**
- [37]: Alberto Armandi's story blaming Jonathon Ryan Owens.
- [38]: Texan charged in ponzi scheme (Zerohedge.com)
- [39]: **Calculation based on 700467₿ raised and 507148₿ paid out.**
- [40]: Blockchain analysis by BitcoinTalk moderator.
- [41]: Daphne P. Downes of SEC, civil action.
- [42]: SEC litigation.
- [43]: Bitfloor analysis.
- [44]: Bitfloor official announcement.
- [45]: Personal account by victim.
- [46]: 50BTC Official Statement.
- [47]: User mralbi's personal report.
- [48]: Internet Archive archive of Bit LC press release.
- [49]: IRC conversation.
- [50]: **Mining cost of 748 18715667₿ and OKPay double spend of 211 90930000₿.**
- [51]: Analysis conducted specifically for this list.
- [52]: Leandro César, "Problema do Mercado Bitcoin".
- [53]: Analysis conducted specifically for this list.
- [54]: Selected example of paranoia on Reddit.
- [55]: Vitalik Buterin, Bitcoin Magazine.
- [56]: Address 16cDeEFn6sraUEJrDCt2Yg3r7j2oazSYEd
- [57]: Vircurex May 2013 Report.
- [58]: **Amount sent to thief addresses: 1454.00000000₿**
  Total transaction fees incurred: 0.01500000₿
- [59]: Official statement by Vircurex in March 2014.

- [60]: "I don't have an exact date, the only time period I can give – and I've been racking my own brains – is between 20 June and 10 August. Probably mid-July.", quoted from James Howells and reported by the Guardian.
- [61]: The Guardian.
- [62]: Coindesk article.
- [63]: **Total sent to 1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xqX, excluding dust sent *ex post facto* as blockchain graffiti.**
- [64]: **Total sent to 1FfmbHfnpaZjKFvyi1okTjJJusN455paPH, excluding dust sent *ex post facto* as blockchain graffiti.**
- [65]: Adrian Chen, *kotaku.com*.
- [66]: United States' criminal complaint.
- [67]: Emily Flitter, *Reuters*.
- [68]: James Ball, *The Guardian*.
- [69]: Alex Hern, *The Guardian*.
- [70]: Associated Press.
- [71]: Kadhim Shubbe, "$4.1m goes missing as Chinese bitcoin trading platform GBL vanishes".
- [72]: Statement by TradeFortress.
- [73]: Statement by TradeFortress.
- [74]: Official statement.
- [75]: Accusation by BitcoinTalk user "webr3".
- [76]: Accusation by BitcoinTalk user "MoneypakTrader.com".
- [77]: Analysis by Aleš Janda, reported by CoinDesk.com.
- [78]: **Blockchain. (This information was obtained directly from the Bitcoin blockchain by looking up the transaction or transactions listed in the entry.)**
- [79]: Statement by BitcoinTalk user and BIPS operator "Kris".
- [80]: Statement by BitcoinTalk user "tytus", who is likely to be a founder of PicoStocks.
- [81]: The Guardian on December 3, 2013.
- [82]: The Guardian on December 9, 2013.
- [83]: Official signed statement from "Defcon", operator of Silk Road 2.
- [84]: Nicholas Weaver's estimate, quoted in Forbes.
- [85]: Alex Richardson, "Silk Road 2.0 making users whole after hack".
- [86]: Official statement from Flexcoin.
- [87]: **Sent to 1QFcC5JitGwpFKqRDd9QNH3eGN56dCNgy6: 304**.00000000 **฿**
  Sent to 1NDkevapt4SWYFEmquCDBSf7DLMTNVggdu: 592.10000000 **฿**
  Transaction fees incurred in sending: 0.00380000 **฿**
- [88]: Leak of information apropos the CryptoRush situation by "DogeyMcDoge", support employee at CryptoRush.
- [89]: (Archived) Update posted by the exchange.
- [90]: Statement by operator.
- [91]: Pete Rizzo, "Pony Botnet Virus Steals $220,000 from 30 Types of Digital Wallets".
- [92]: Update from Everydice developer.

Credits

Thanks to the following who generously wrote commentary:

- Jennifer Pippin (Linode Hacks)

Thanks to the following who pointed some thefts out:

- Stephen Gornick
- Patrick Harnett
- Paul Mumby
- Blitz @BitcoinTalk
- cypherdoc @BitcoinTalk
- LoweryCBS @BitcoinTalk
- lunarboy @BitcoinTalk
- malevolent @BitcoinTalk
- pankkake @BitcoinTalk
- repentance @BitcoinTalk
- rudrigorc2 @BitcoinTalk
- Shermo @BitcoinTalk
- timegrinder @BitcoinTalk

dree12
Legendary

Activity: 1148

Ignore

Re: List of Major Bitcoin Heists, Thefts, Hacks, Scams, and Losses #9
April 19, 2014, 02:11:17 AM

So, an update from the last thread:

- Since the last thread was full, I moved everything to this new thread. Now 8 posts are reserved and if necessary I can consume this post.
- I added the backlog of thefts that were delayed due partially to space limitations and mostly to my personal time limitations. Some are still missing because I need to research them more. They will be added in due time.
- The rankings were originally done manually, which is becoming difficult as the list grows. Hence I have begun work on an automatic ranker. This should be finished soon, but given my propensity for delaying things, it probably will not be. In the coming weeks I will also move from June 2013 ฿ to a more recent standard.

Thank you to those who kept me updated!

Things left on the backlog waiting for more research:

- GBL
- Bitclockers.com
- Pony botnet
- Cryptorush
- Neo & Bee

(By the way: Feel free to reply now; the number of posts reserved is plenty.)

iluvpie60
Sr. Member

Activity: 294

www.youtube.cor

Re: List of Major Bitcoin Heists, Thefts, Hacks, Scams, and Losses #10
April 19, 2014, 04:29:57 AM

Quote from: dree12 on April 19, 2014, 02:11:17 AM

> So, an update from the last thread:
>
> - Since the last thread was full, I moved everything to this new thread. Now 8 posts are reserved and if necessary I can consume this post.

Ignore

> - I added the backlog of thefts that were delayed due partially to space limitations and mostly to my personal time limitations. Some are still missing because I need to research them more. They will be added in due time.
> - The rankings were originally done manually, which is becoming difficult as the list grows. Hence I have begun work on an automatic ranker. This should be finished soon, but given my propensity for delaying things, it probably will not be. In the coming weeks I will also move from June 2013 ฿ to a more recent standard.
>
> Thank you to those who kept me updated!
>
> Things left on the backlog waiting for more research:
> - GBL
> - Bitclockers.com
> - Pony botnet
> - Cryptorush
> - Neo & Bee
>
> (By the way: Feel free to reply now; the number of posts reserved is plenty.)

I am not sure a forum is the best place to display this much information, especially if you are going to update it with a ton more stuff. Although it is organized, it is cluttered in the limited format that you can post on here, IE buttons/links to other pages, or tabs for each year ETC.

dree12
Legendary

Activity: 1148

Ignore

Re: List of Major Bitcoin Heists, Thefts, Hacks, Scams, and Losses
April 19, 2014, 05:01:09 PM

#11

Quote from: iluvpie60 on April 19, 2014, 04:29:57 AM

> Quote from: dree12 on April 19, 2014, 02:11:17 AM
>
> > So, an update from the last thread:
> >
> > - Since the last thread was full, I moved everything to this new thread. Now 8 posts are reserved and if necessary I can consume this post.
> > - I added the backlog of thefts that were delayed due partially to space limitations and mostly to my personal time limitations. Some are still missing because I need to research them more. They will be added in due time.
> > - The rankings were originally done manually, which is becoming difficult as the list grows. Hence I have begun work on an automatic ranker. This should be finished soon, but given my propensity for delaying things, it probably will not be. In the coming weeks I will also move from June 2013 ฿ to a more recent standard.
> >
> > Thank you to those who kept me updated!
> >
> > Things left on the backlog waiting for more research:
> > - GBL
> > - Bitclockers.com
> > - Pony botnet
> > - Cryptorush
> > - Neo & Bee
> >
> > (By the way: Feel free to reply now; the number of posts reserved is plenty.)

> I am not sure a forum is the best place to display this much information, especially if you are going to update it with a ton more stuff. Although it is organized, it is cluttered in the limited format that you can post on here, IE buttons/links to other pages, or tabs for each year ETC.

For now, a forum post is good enough. The markup is written in an intermediate language though so it can be compiled to some other format if necessary in the future.

malevolent
can into space
Global Moderator
Legendary

Activity: 1218

Ignore

Re: List of Major Bitcoin Heists, Thefts, Hacks, Scams, and Losses
April 29, 2014, 06:44:03 PM #12

You forgot about Bitcoin to Cash:
https://bitcointalk.org/index.php?topic=344143

100 BTC @ 800 USD/BTC =~~ $80k.

I think Labcoin could also be added (another scam by Alberto Armandi), but I haven't followed it closely, so have no idea how much money is missing (7500 BTC?).

Also, ActiveMining (10k BTC?) and maybe COG could be on the list.

CoinHeavy
Full Member

Activity: 189

WTS
LiteCoin.pe
WalletReputation.
LiterCoin.com

Ignore

Re: List of Major Bitcoin Heists, Thefts, Hacks, Scams, and Losses
April 30, 2014, 11:46:27 AM #13

Incredible history you have compiled. Many thanks for sharing.

.: [For Sale] --- LiteCoin.pe --- WalletReputation.com --- LiterCoin.com --- Cointreversy.com .:

IIOII
Hero Member

Activity: 747

Ignore

Re: List of Major Bitcoin Heists, Thefts, Hacks, Scams, and Losses
April 30, 2014, 12:51:25 PM #14

Quote from: malevolent on April 29, 2014, 06:44:03 PM

> You forgot about Bitcoin to Cash:
> https://bitcointalk.org/index.php?topic=344143
>
> 100 BTC @ 800 USD/BTC =~~ $80k.
>
> I think Labcoin could also be added (another scam by Alberto Armandi), but I haven't followed it closely, so have no idea how much money is missing (7500 BTC?).
>
> Also, ActiveMining (10k BTC?) and maybe COG could be on the list.

This and you forgot the bitdaytrade-scam (several thousand BTC), also run by alleged serial scammer Alberto Armandi (Carbonia, Italy (Sardinia); now possibly HK/China).

As a starting point:

labcoin:
http://www.reddit.com/r/Bitcoin/comments/1ncckq/labcoin_has_been_outed_as

bitdaytrade:
https://bitcointalk.org/index.php?topic=88803.0
https://bitcointalk.org/index.php?topic=93445.0

FFrost
Full Member

Activity: 182

Ignore

Re: List of Major Bitcoin Heists, Thefts, Hacks, Scams, and Losses #15
May 01, 2014, 03:08:33 PM

Very Interesting read. Opened my eyes a bit!

C.Steven
Sr. Member

Activity: 378

Ignore

Re: List of Major Bitcoin Heists, Thefts, Hacks, Scams, and Losses #16
May 01, 2014, 03:12:05 PM

Thanks OP for creating and maintaining this list.
People could have avoided the loss in many cases if they don't store their bitcoin on sites.

beescrow
Newbie

Activity: 7

Ignore

Re: List of Major Bitcoin Heists, Thefts, Hacks, Scams, and Losses #17
May 01, 2014, 03:12:30 PM

You should also give the aproximate value in USD at the time those bitcoins were stolen. Because now they're obviously worth a lot, but back in 2011/2010, they weren't worth nearly as much as they are now...

MegaHustlr
Sr. Member

Activity: 406

Re: List of Major Bitcoin Heists, Thefts, Hacks, Scams, and Losses #18
May 01, 2014, 04:08:35 PM

Quote from: beescrow on May 01, 2014, 03:12:30 PM

> You should also give the aproximate value in USD at the time those bitcoins were stolen. Because now they're obviously worth a lot, but back in 2011/2010, they weren't worth nearly as much as they are now...

Ignore

I think he did do this no? He listed the value of it back then.

C.Steven
Sr. Member

Activity: 378

Ignore

Re: List of Major Bitcoin Heists, Thefts, Hacks, Scams, and Losses
May 01, 2014, 04:22:27 PM
#19

> **Quote from: MegaHustlr on May 01, 2014, 04:08:35 PM**
>
> > **Quote from: beescrow on May 01, 2014, 03:12:30 PM**
> >
> > You should also give the aproximate value in USD at the time those bitcoins were stolen. Because now they're obviously worth a lot, but back in 2011/2010, they weren't worth nearly as much as they are now...
>
> I think he did do this no? He listed the value of it back then.

Yup, there is a section "List of events by USD equivalent of mBTC at time of theft" though with a note "NB: This section is outdated.".

dree12
Legendary

Activity: 1148

Ignore

Re: List of Major Bitcoin Heists, Thefts, Hacks, Scams, and Losses
May 02, 2014, 09:02:18 PM
#20

> **Quote from: malevolent on April 29, 2014, 06:44:03 PM**
>
> You forgot about Bitcoin to Cash:
> https://bitcointalk.org/index.php?topic=344143
>
> 100 BTC @ 800 USD/BTC =~~ $80k.
>
> I think Labcoin could also be added (another scam by Alberto Armandi), but I haven't followed it closely, so have no idea how much money is missing (7500 BTC?).
>
> Also, ActiveMining (10k BTC?) and maybe COG could be on the list.

> **Quote from: IIOII on April 30, 2014, 12:51:25 PM**
>
> > **Quote from: malevolent on April 29, 2014, 06:44:03 PM**
> >
> > You forgot about Bitcoin to Cash:
> > https://bitcointalk.org/index.php?topic=344143
> >
> > 100 BTC @ 800 USD/BTC =~~ $80k.
> >
> > I think Labcoin could also be added (another scam by Alberto Armandi), but I haven't followed it closely, so have no idea how much money is missing (7500 BTC?).
> >
> > Also, ActiveMining (10k BTC?) and maybe COG could be on the list.
>
> This and you forgot the bitdaytrade-scam (several thousand BTC), also run by alleged