BitMEX Research

The bitcoin flash crash to $0.01 in June 2011

19 July 2018

Abstract

We look at the events surrounding the bitcoin price rally in June 2011 to $32 and the following temporary flash crash down to $0.01, on the MtGox exchange. We look at the incompetence of MtGox and examine the causes of the crash. We then look at the political battle and uncertainty which occurred in the aftermath of the crash.

BitMEX Research

Filtering out the hype with unbiased, evidence-based reports on the crypto-coin ecosystem.

BitMEX Research is also active on Twitter and Reddit.

https://research.bitmex.com

Previous reports:

A brief history of Stablecoins (Part 1)
(02/07/2018)

Bitcoin Economics – Deflationary Debt Spiral (Part 3)
(31/05/2018)

New Ethereum Miner Could be a Game Changer
(24/04/2018)

Complete guide to Proof of Stake – Ethereum's latest proposal & Vitalik Buterin interview
(11/04/2018)

Bitcoin price correlation: Record high against the S&P 500
(28/03/2018)

Update: SegWit transaction capacity increase compared to Bitcoin Cash
(22/03/2018)

Overview

If one likes price volatility and scandals, the summer of 2011 was an exciting time for Bitcoin. Over the course of a few days, bitcoin plummeted in value from a peak of $32 to just $0.01 on the MtGox exchange, a trading platform based in Tokyo, which was dominant at the time. This was after a recent rally, with bitcoin trading at around $2 a couple of months earlier. The crash down to $0.01 is now a famous part of Bitcoin history.

In this piece, we look at the cause of the crash and its aftermath. Although the major exchange of the time, MtGox, was shown to the community to be largely negligent, which may not have been the best advertisement for Bitcoin. In our view the engaging nature of the events which occurred that summer, ironically made a significant contribution to the level of interest in the space.

MtGox security issues & the context of the event

There was significant uncertainty surrounding the hack at MtGox which caused the June 2011 price crash and the issues surrounding it were never fully explained. The Bitcoin community was riddled with rumours about whether MtGox was solvent and how much bitcoin was stolen.

Thanks to a report published in 2017 by Kim Nilsson, we now have a relatively strong understanding of what occurred in 2011 and the damage that this caused to MtGox. Ironically, despite the huge impact on the market and the company's reputation, in terms of MtGox's solvency, this event was largely insignificant compared to other security incidents. For many however, a new window into MtGox was opened up, which illustrated a severe lack of monitoring systems, governance, controls and security measures.

The table below lists some of the major security incidents at the MtGox exchange, with the June 2011 hack highlighted in green. This incident may have only directly cost the exchange 2,000 bitcoin, an inconsequential amount, compared to roughly 837,000 bitcoin of total losses.

List of known MtGox losses

Date	Incident name	Description	USD lost	BTC Lost
20 Jan 2011	Liberty Reserve withdrawal exploit		50,000	
30 Jan 2011	Liberty Reserve withdrawal exploit 2	A user supposedly withdrew US$2billion from their account which never existed. Although it seems no wire transfer actually occurred and therefore there may have been no losses		
1 March 2011	Wallet theft 1	Hackers obtained the MtGox *wallet.dat* file from the server. This is believed to be the withdrawal transaction. As of 19 July 2018, the stolen 80,000 bitcoin has never been moved.		80,000
22 May 2011	Wallet theft 2	Somebody is believed to have accessed a wallet containing 300,000 bitcoin, which was kept unencrypted on a public drive. The thieves decided to return 297,000 bitcoin, keeping a 1% fee. The return transactions are believed to be for 280,000 and 17,000.		3,000
19 June 2011	Price crash to $0.01	Hacker gained access to Jed McCaleb's administrative account, and sold bitcoins to crash the price, to withdraw as many bitcoins as possible within the US$1,000 per day limit. Other users who purchased bitcoin at low prices may have also withdrawn funds.		2,000
11 Aug 2011	Bitomat	Took over the debts of Bitomat after the company deleted its private keys		17,000
Sept 2011	Database hacked	A hacker gained write access to the database and inflated balances to withdraw funds		77,500
Sept 2011	Wallet theft 3	A hacker obtained the main *wallet.dat* file again and began withdrawing funds in October 2011. MtGox appears not to have noticed this.		603,000
Oct 2011	Incorrect deposits	The change from the above hacker's withdrawal transactions were incorrectly booked as new MtGox deposits, totalling 44,300 bitcoin. This resulted in customers seeing new deposit balances in their accounts. In some ways the hackers therefore caused more damage to MtGox than the value of coins which were stolen. Some of these errors were corrected & the net impact may be around 30,000 bitcoin.		30,000
28 Oct 2011	Destroyed bitcoin	A software bug caused funds to be sent in such a way that they could not be redeemed. Example of such transactions can be found here & here		2,609
May & Aug 2013	US law enforcement seizures	Federal agencies in the US seized funds from MtGox's Dwolla account due to allegations the exchange was not complaint with US regulations.	5,000,000	
May 2013	Coinlab dispute	Coinlab sued MtGox in a dispute over a licensing agreement.	5,000,000	
2011 to 2013	Willy Bot	MtGox trading program designed to make up some of the above losses, but actually ended up making things worse.	51,600,000	22,800
Total			**61,650,000**	**837,909**

(Source: Cracking MtGox, BitMEX Research)

Overview of the events in June 2011

In the weeks leading up to 19 June, many users of MtGox were reporting that their accounts had been hacked. At around the same time a database of MtGox users, including an MD5 hash of their passwords (with an unclear/inconsistent salt policy) was leaked and made available. Many passwords were identified. Some traders used the same credentials at the rival exchange, Tradehill, who also experienced security issues. Despite this, MtGox did not suspend trading, a decision which many traders questioned.

On 19th June 2011 (3am on 20th June Tokyo time), there were large sell orders on the exchange and the price crashed from around $17.50 to $0.01 and trading continued at this level for several minutes before recovering. This lead to a high degree of uncertainty, with some assuming there may be a problem with the Bitcoin network.

It now seems likely that what actually happened was that a hacker may have obtained access to the account of Jed McCaleb, the founder of MtGox who sold the exchange to Mark Karpeles around three months earlier. This account appears to have retained administrative rights to the database and therefore the hacker was able to manipulate account balances and grant themselves a large number of bitcoins on the MtGox system. The hacker is the likely to have begun selling some of these coins.

Due to the poor management of MtGox, in our view it is unlikely that the company were aware of this, even in the aftermath of the hack, and therefore the explanations provided at the time of the events were incomplete or inaccurate.

The withdrawal limits

At the time, MtGox had a daily withdrawal limit of US$1,000, this applied to both bitcoin and USD (via Dwolla). This meant that the hacker (or any others who benefited from the hack by buying bitcoin at low prices), would be unable to benefit by withdrawing the funds, except within the US$1,000 limit. However, the US$1,000 bitcoin limit was based on the market price of bitcoin on the platform and since the price fell to $0.01, in theory the maximum each user could withdraw was 100,000 bitcoin, certainly not a small amount.

Fortunately, however, MtGox appeared to also have a bitcoin based withdrawal limit, that many users were unaware of. As the Mark Karpeles said at the time:

> *"2011-06-20 00:16:43 MagicalTux the btc withdrawal limit saved us"*
> *- IRC, Note: MagicalTux is the CEO & owner of MtGox, Mark Karpeles*

Mark then mentioned that only 2,000 bitcoin were withdrawn in the aftermath of the event, which was a relatively positive result for MtGox.

> *"Got about 2,000 BTC out"*
> *- IRC*

There was widespread scepticism about this number at the time, with many believing much more was stolen. Ironically, this 2,000 bitcoin figure now seems about right, although MtGox had lost far more in other incidents. However, due to the price crash and suspension of trading, this incident was very public at the time and resulted in the incompetence of the MtGox platform being exposed to the community.

The rollback debate

Many trades took place at the artificially low price of around $0.01 during the crash. Some traders & investors were unhappy at missing out on the price rally from around $1 to $32, and therefore had buy orders waiting in the system, all the way down the order book to $0.01. To them, this crash is exactly what they were waiting for. To the dismay of many of these traders, in the aftermath of the incident MtGox said they would reverse the trades which occurred during the crash:

> *"The bitcoin will be back to around 17.5$/BTC after we rollback all trades that have happened after the huge Bitcoin sale that happened on June 20th near 3:00am (JST). One account with a lot of coins was compromised and whoever stole it (using a HK based IP to login) first sold all the coins in there, to buy those again just after, and then tried to withdraw the coins. The $1000/day withdraw limit was active for this account and the hacker could only get out with $1000 worth of coins. Apart from this no account was compromised, and nothing was lost. Due to the large impact this had on the Bitcoin market, we will rollback every trade which happened since the big sale, and ensure this account is secure before opening access again."*
> *- MtGox*

After this announcement there was significant debate in the community as to whether the rollback should occur. Obviously many participants in the debate had a financial interest in the outcome and this was no doubt effecting their views. In many ways, there were some parallels between this rollback and the 2016 DAO "rollback" on the Ethereum network, with some similar arguments being made.

Supporting the rollback	Opposing the rollback
	MtGox should take responsibility and compensate all parties involved. In particular MtGox did not act appropriately in the weeks prior to this event when many users reported that their accounts were hacked and they allowed trading to continue.
Most traditional exchanges tend to roll back trades in exceptional circumstances, particularly if trades occur at extremely unusual prices. The prices in this instance were certainly extreme.	MtGox had no policy with respect to the matter and should therefore honour the trades.
The bitcoin were stolen and therefore users should not benefit from stolen goods.	If MtGox reversed the trades in this case, then users may not trust them again.
The bitcoin may never have existed and may only have been entries in MtGox's database and therefore it may not be possible to deliver the coins.	Reversal is an arbitrary process, would MtGox reverse trades if a much smaller amount of money was stolen? This is one rule for the rich and another for the poor.
	Although there are some examples of major traditional exchanges reversing trades in exceptional circumstances, there are examples where they have not done so.
	Honouring the trades is more consistent with the no bailout, dog eat dog, 24×7 uptime, immutability type culture in the community, which was in some ways more prevalent at the time than it is today

The community appeared to be split on this issue, with some even favouring a vote to decide.

The trader who bought 260,000 bitcoins for US$2,622

The day after the incident, a trader called "Kevin", claims to have purchased around 260,000 bitcoins during the crash and was arguing that he should be able to keep the coins. As he explained:

> *"I had around $3,000 USD in my MtGox account, from earlier sales I'd made. I looked at the market stats, and realized that there were tons of orders to buy BTC at $0.01 that would likely eat up any remaining bitcoins this seller had on the order. I figured if I put a buy order in for $0.0101, my order would execute first and I could buy a huge amount of bitcoins."*
> *- Bitcointalk*

Kevin posted what he claimed to be the trade confirmation:

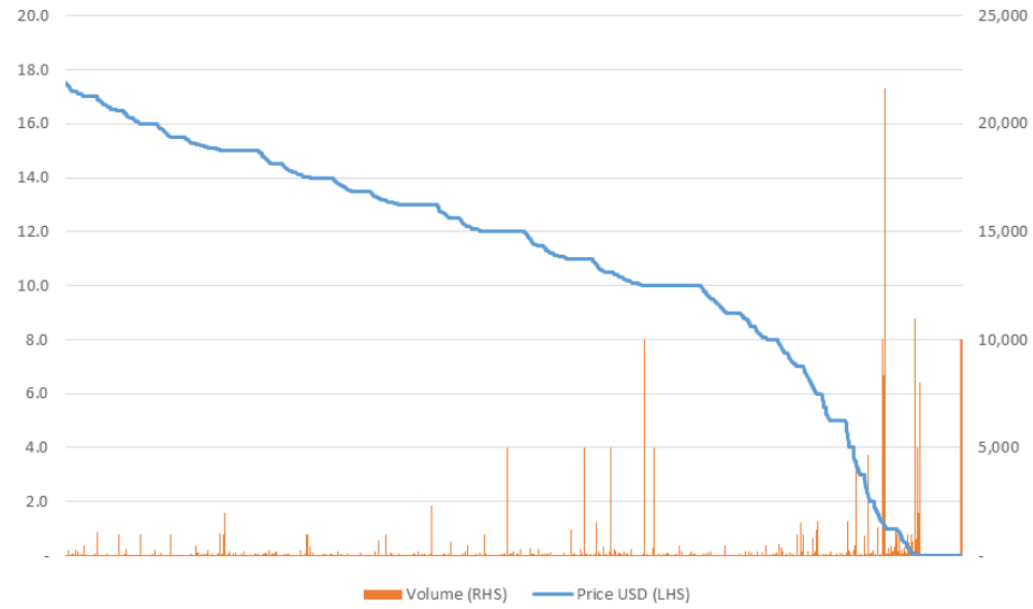
> *"06/19/11 17:51 Bought BTC 259684.77 for 0.0101."*

Kevin then went on to explain the likely reason behind the price crash, which was that the seller was trying to manipulate the price down so that they could withdraw more coins within the US$1,000 limit. In our view this part of Kevin's story is likely to be an accurate explanation for the price crash. This logic contradicts the claim from MtGox that the person who conducted the hack was also the buyer of the bitcoin.

> *"I could place a reasonably sized sell order for $0.001, crash the market again, and withdraw probably all of the bitcoins, since they'd be valued at $0.001 each and would fit under the $1,000 USD limit. I also decided against this, when I realized that whoever placed the gigantic sell order was probably doing so for the exact same reason"*

However, some have doubted the accuracy of Kevin's story, claiming the volume of trades he claims is not consistent with the MtGox feed. The feed appeared to show trading volume of only 55,000 bitcoins during the crash past $0.0101 and only 238,000 bitcoins traded in the period. Only 3,000 bitcoin seem to have been traded at the $0.0101 price. These figures are lower than those implied by Kevin, although Kevin's trades could have been excluded from this data for a variety of reasons. The feed was also notoriously unreliable and it was not clear if there was a precise definition of some for the information in the feed. In our view, there is no reason to believe the whole truth of any of the parties involved in this incident, but Kevin's explanation for the crash itself seems plausible to us.

MtGox price feed during the crash



(Source: BitMEX Research, MtGox. Note: Volume in bitcoin)

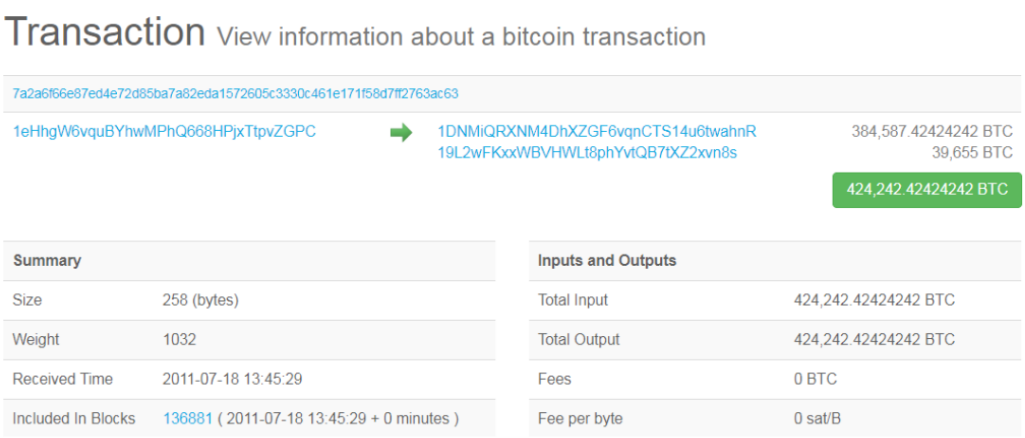
The proof of reserves

The MtGox exchange was down for several weeks and many users were becoming anxious about the solvency of the platform. There was uncertainty over the amount of bitcoin which were lost and users were concerned about a run on MtGox, eventually leading to the exchange going into liquidation and users losing funds. In an attempt to reduce some of these concerns, as the chat log and bitcoin transaction show below, MtGox attempted to prove it had access to a significant quantity of bitcoin, by conducting an onchain transaction on 18th July 2011.

IRC Chat log & bitcoin transaction – 18 July 2011

```
<geist_> theres a lot of people crying wolf saying gox doesnt have their btc anymore
<wumpus> don't send them to the bitcoin eater please :)
<go1dfish> mabus: tux is shuffling large numbers of bitcoins to show they are still under his control
<MagicalTux> anyway, going to send to 1eHhgW6vquBY... the 424242.42424242 btc
<geist_> ok
```

(Source: IRC logs)



(Source: blockchain.info)

At the time, the above action seemed to settle the nerves of many of the traders.

Conclusion

A few weeks after these events, after many false starts, trading at MtGox eventually resumed and the bulk of the trades were reversed. However, to this day, as far as we are aware, MtGox has not been able to provide a coherent explanation for what occurred. The lack of a consistent narrative from MtGox lead many to believe that MtGox had poor monitoring and controls of its systems and that the company was run negligently. Many concluded "never to trust MtGox again".

Unfortunately, however, MtGox somehow continued to dominate the exchange ecosystem for another three years. However one views the conduct and transparency of some of the platforms and players in the ecosystem today, we can at least conclude that things have significantly improved since 2011.

Disclaimer

Transacting on BitMEX is not offered or available to any resident of (I) the United States of America, (ii) Cuba, Crimea and Sevastopol, Iran, Syria, North Korea, Sudan, or any other sanctioned jurisdiction, or (iii) any jurisdiction where the services offered by BitMEX are restricted.

This material should not be the basis for making investment decisions, nor be construed as a recommendation to engage in investment transactions and is not related to the provision of advisory services regarding investment, tax, legal, financial, accounting, consulting or any other related services, nor is a recommendation being provided to buy, sell or purchase any good or product.

Any views expressed are the personal views of the authors of the report. BitMEX (or any affiliated entity) has not been involved in producing this report and the views contained in this report may differ from the views or opinions of BitMEX.

The information and data herein have been obtained from sources we believe to be reliable. Such information has not been verified and we make no representation or warranty as to its accuracy, completeness or correctness. Any opinions or estimates herein reflect the judgment of the authors of the report at the date of this communication and are subject to change at any time without notice. BitMEX will not be liable whatsoever for any direct or consequential loss arising from the use of this publication/communication or its contents.