Do Bitcoiners Want a Bailout? No.

MtGox filed for bankruptcy protection today, and in so doing, disclosed that it has 127,000 customers who are owed on average the equivalent of $3500 each. One might expect this sort of thing to trigger angry cries from customers for government intervention and/or bail-outs.

Indeed, some do think this is the case:

While that tweet may have been mostly in jest, it did strike me that I've noticed ZERO calls for government intervention from MtGox customers. People are obviously angry; mostly at MtGox management, and somewhat at themselves. The various calls for action are mostly calls for new, better-run, more transparent businesses, better redundant storage of funds, and development of decentralized exchanges that cannot become insolvent. In short, even at the height of customer shock and anger, the calls from within the community are mostly for a **change in consumer behavior**, and development of **better technology**. Bailouts are not considered a desired or long-term viable solution.

On one hand, this doesn't come as much of a surprise, with bitcoin's roots and early userbase coming from a libertarian ethos. But usually when people lose money, real and/or irrational feelings come out. The lack of calls for intervention shows a deep belief in bitcoin's potential to serve the greater good **without** explicit central management. Here are some quotes from the "Official Money Lost in Mt. GOX Thread":

"417.8923 BTC…
Stupid me… Was going to withdraw and move elsewhere, but the price kept falling so… Greed."
source

"8 BTC (0 EUR/USD)
I bought the BTC less than 24 hours before the trading stopped…
I don't even regret it. Yes, I am a little said [sic], but I was aware what I am doing and I would do this again."
source

"Looks like 38BTC gone. I knew better but trading was fun."
source

"$0 and $0 BTC. The only person I trust with my private keys is myself."
source

"2.08 BTC. 274 USD… Should've cashed out earlier, but I got greedy."
source

“About 4k in USD…I should have seen the writing on the wall and converted back to BTC and pulled it.”
source

“they better go bankrupt and stay bankrupt, for bitcoin”
source

“I pretty much have my life savings on Gox/MtGox whatever. When I first joined gox and the bitcoin community as a whole back in 2011 I had £1000 to my name.

I took a lot of huge gambles over the last 2 years and in my opinion did fairly well in fact I had over 17k euros by the “end” sitting on gox. Not counting the money I withdrew to live on.

Easy come easy go and with the risks I was taking along the way this was always a very real possibility.

Bitcoin was still a great experience for me and I’m glad I was in for the ride (yes I’m still a believer).

I wouldn’t want a single donation from anyone and would refuse it respectfully as I was a risk taker from the get go Grin

I think the best thing this community can do is offer support in a form that would potentially prevent the very real chance of suicides.
Its ow so easy to forget there are real people behind the curtain of the internet and many of them are hurting and suffering.”
source

The above quotes are not cherry-picked. At 11-pages long, with some people claiming millions-o--dollars equivalent in losses, there’s not a single call for intervention in that thread. Bitcoin enthusiasts are a consistent bunch.

What MtGox Did Wrong

tl;dr: Everything.

A friend emailed me yesterday and asked “Why aren’t others vulnerable?” That’s a good question. For those of us who pay attention to bitcoin every day, it’s been clear for months (even years for some) that MtGox was a unique risk in the bitcoin ecosystem. It’s always been considered unwise to leave significant funds in *any* exchange for very long, but starting in summer 2013, it started looking downright insane to keep money in Gox.

The problems arguably started much earlier. A timeline of MtGox's troubles:

May 20th, 2011 – Files incorrect banking application.

MtGox CEO Mark Karpeles opens a business banking account at Wells Fargo, and fails to declare MtGox as a "Money Transmitting Company".

June 19th, 2011 – Customer database hacked. Market compromised.

MtGox gets hacked, and a single massive sell order is executed, causing the price to drop to pennies within minutes. I had the fortune of watching this flash-crash in real time; a fascinating lesson in market liquidity. MtGox's failure here was tangential: as a result of this incident, it became clear that MtGox was hashing their customers' passwords with MD5, a hashing algorithm long considered inappropriate for modern use by even novice security consultants. This was a very telling early insight into MtGox's security and technology practices.

April, 11-12, 2013 – Trading halted due to bad technology.

MtGox suspends trading, calling it a necessary "market cooldown". In reality, it was due to their inability to mitigate DDoS attacks and/or handle high-load on their systems due to high bitcoin trading volume. Either way, MtGox was a very profitable business and had months of warning (years, really) to realize they needed to upgrade their systems.

The trading halt on MtGox was the trigger for the end of the massive Spring 2013 bitcoin bull market. Prices crashed from over $200 to $50 in one day. This was the 2nd time failures at MtGox caused a market panic.

May 2nd, 2013 – Bad deal with CoinLab results in lawsuit

MtGox's alleged failure to honor the terms of their merger deal with then pseudo-exchange CoinLab (now effectively defunct), is aggressively terminated by CoinLab with a $75M lawsuit. To be fair, it's unclear who was at fault, but it's likely both parties made serious faulty business decisions.

May 15th, 2013 – DHS seizes $5.5M from MtGox.

MtGox's real trouble begins. The US Department of Homeland Security seizes MtGox's Dwolla account, apparently containing $5.5M in funds. This is a direct result of Karpeles decision in 2011 to not check the "Money Transmitting Business" box on his Wells Fargo banking forms.

While clearly an egregious error, especially after FinCEN's guidance, to be fair, bitcoin was essentially a toy until 2013. Few took it seriously, and in that context, it was easy for many non-diligent early bitcoin business operators to dismiss existing money services regulations as not applicable.

June, July 2013 – Dollar withdrawals restricted.

MtGox suspended US dollar withdrawals on June 20th, and resumed them on July 4th. Unfortunately, despite the resumption of withdrawal processing, customers were unable to get funds out in a reasonable timeframe. Withdrawals usually took in excess of 4 weeks to complete. Rumor has it that MtGox's tenuous banking partnerships (or the DHS) were imposing wire-transfer

limitations on the company.

If the prior incidents were not sufficient warning, this was the huge red-flag. Naturally, this was also the point at which the price of bitcoin on MtGox started to diverge from the price on other exchanges. Due to the dollar withdrawal issues, traders had to buy bitcoin and transfer it out in order to withdraw funds from MtGox in a timely fashion. The MtGox price therefore started to steadily trade 10% (or more) higher than increasingly popular exchanges Bitstamp, Coinbase, and BTC China.

Many in the bitcoin community began more vocally advising traders to retain control of their own funds, and to specifically remove their funds from MtGox. The writing was on the wall.

February, 7-10 2014 – Bitcoin withdrawals suspended.

MtGox suspends bitcoin withdrawals, citing a known-since-2011 issue in the bitcoin protocol called "transaction malleability". They claim that the issue is preventing them from reliably processing bitcoin withdrawals and that they have to freeze withdrawals while they sort it out. Not good.

The thing about transaction malleability is that it's been a known issue/quirk of the bitcoin protocol since 2011. Briefly, there's a several minute window between when a transaction is broadcast and when it's confirmed in the bitcoin blockchain. It's possible during that window to broadcast an identical transaction (same sender, same recipient, same quantity of bitcoin), but with a different transaction-hash. Only one of these transactions will make it into a block, with the other being considered a double-spend, and therefore dropped. Since this is a known issue, no diligent bitcoin service implementation uses the transaction-hash as a sole identifier for transactions in their internal accounting systems.

But MtGox apparently did. That meant that malicious individuals could withdraw bitcoin from MtGox, immediately issue a re-broadcast of the transaction with a different hash, and then if that re-broadcast transaction made it into the blockchain, the person could then contact MtGox support and say "Hey! My withdrawal never happened; see, the original transaction hash is not in a block! Send it to me again!". Apparently MtGox even had an *automated* process for withdrawal resends!

While other exchanges did end up temporarily suspending withdrawals to evaluate their own code in this context, they all re-opened quickly and without issue. MtGox was the only exchange demonstrating such careless accounting and withdrawal processes.

February, 24th 2014 – MtGox finally dies.

MtGox suspends trading entirely, deletes their twitter history, and leaks documents alleging 744,000 missing bitcoin. **What?!**

We still don't know the details, but CEO Mark Karpeles said today that the leaked documents are "more or less" legit.

Which begs the question: *How on earth do you lose track of 744,000 bitcoin*?! The document says the bitcoins "are missing due to malleability-related theft which went unnoticed for several years." If true, that implies some unbelievably bad accounting practices, business operations, financial management, executive diligence, etc, etc. It's not hard to check a bitcoin cold-wallet balance, and

at least roughly reconcile accounts on a frequent basis.

The document also states: “The cold storage has been wiped out due to a leak in the hot wallet.” Again, **What?!** That can’t happen in a properly implemented system, and reeks of even more egregious technical incompetence.

Other possibilities, of course, include insider theft, or far more damage from the 2011 hack than has been admitted to date. **UPDATE**: Or MtGox may have simply lost the private keys to their coldest & oldest storage, or maybe the US Government has them. We may never know the truth, but one thing is for sure: Bitcoin is better off without such amateur-hour incompetent businesses as MtGox.

UPDATE: February, 28th 2014 – Bankruptcy.

MtGox declares bankruptcy, disclosing 127,000 customers owed an average of $3500 equivalent each.

In Summary

MtGox’s failures were many: regulatory, technical, business-strategy, accounting, management… The specific failures that made MtGox uniquely vulnerable to this kind of catastrophic implosion were:

1) Using a custom bitcoin implementation and not sufficiently updating it or handling long-known issues.
2) Not treating regulatory issues seriously.
3) Poor general security practices.
4) Poor business decisions/relationships.
5) Technology unable to handle predictable load and/or DDoS attacks.
6) Improper bitcoin funds management (cold/hot wallet).
7) Egregious accounting practices.

All these factors led to the situation MtGox is in today. No business should operate with this level of incompetence. MtGox was the last big holdover from early-bitcoin, where enthusiasts built initial services whose popularity quickly exceeded the innovators’ ability to manage the business. As Roger Ver said:

“Gox is the worst-run business in the history of the world.”

And that’s coming from “Bitcoin Jesus”.

Ultimately, the dramatic failure of MtGox marks the transition from early-adopters and a niche market, to seasoned professionals increasingly serving a mass-market. The current crop of bitcoin businesses is a different breed than the first generation: venture backed, run by proven talented entrepreneurs, and aggressively compliant with existing regulatory frameworks. These are the businesses that are driving bitcoin’s next phase of adoption.

Bitcoin Phase-1 is Over. On to Phase-2

It's one of those days in bitcoin. MtGox internal documents allegedly leaked. 744,000 BTC potentially "missing" from MtGox's books. NYTimes and Wired running articles with dramatic headlines and several FUD paragraphs…

Nobody ever said bootstrapping the world's first truly global, ideal-for-our-times, decentralized currency was going to be easy. As the media circus surrounding MtGox's likely demise begins in earnest tomorrow, let's brush off the attacks on Bitcoin in general, and look to the next generation of bitcoin businesses.

MtGox was a holdover from early bitcoin, where clearly incompetent people/operations handled massive amounts of customer funds. That phase of bitcoin's development has been ending, with the termination of MtGox being the final chapter.

The next phase will be driven by professional, larger-scale, audited, transparent companies. They will look to use the transparency, proof, and segmented control features of bitcoin to build trust, and demonstrate the unique power of bitcoin. Look soon for an exchange offering real-time proof-o--reserves, and multi-sig account control.

The next phase may not be as roller-coaster exciting as bitcoin's birth, but it'll change many more lives for the better. The next 100 million users await.

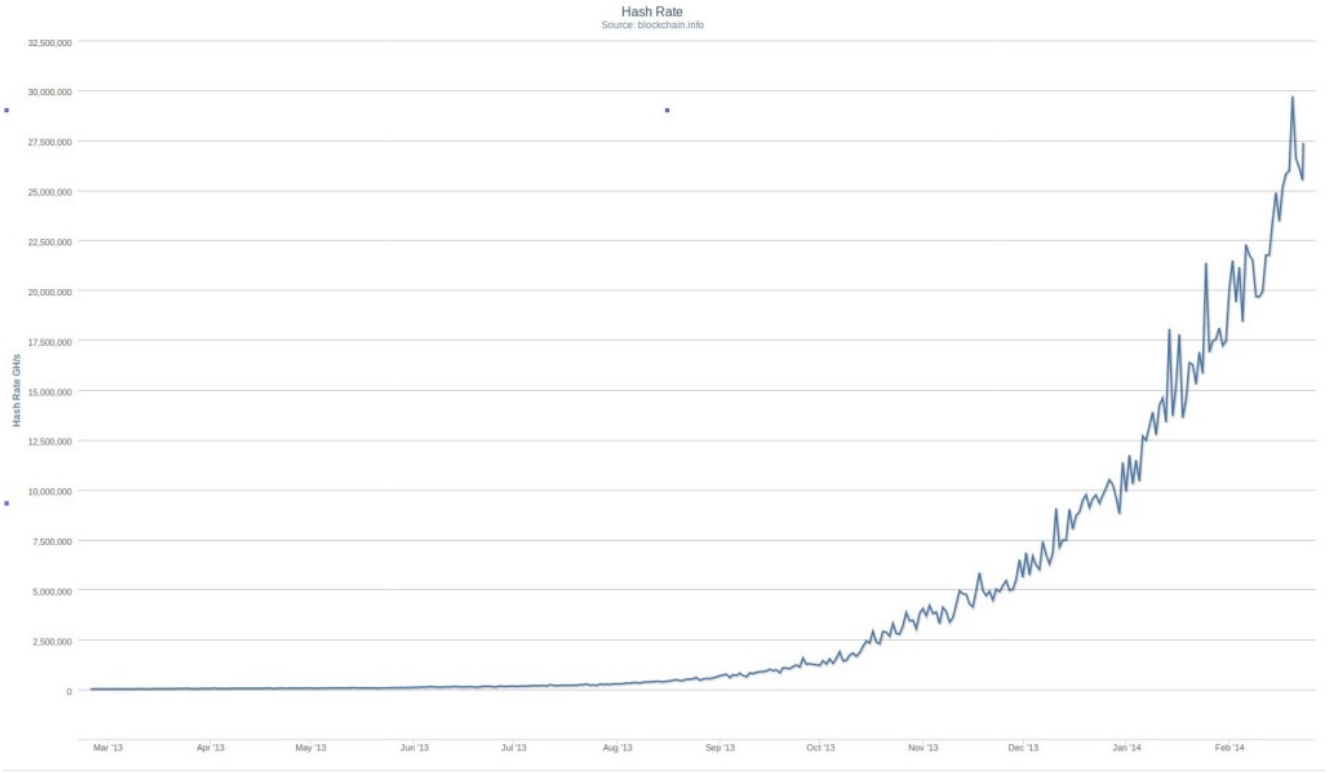
ASICS - Are They Evil?

As the arms race in bitcoin mining continues unabated, the flurry of misinformation and bad logic surrounding the issue is as intense as ever. Since litecoin originally launched and attempted to boast itself as having an "ASIC resistent" mining algorithm, people have been creating and touting various marginal alt-coins as the ultimate bitcoin successor because of supposed resistance to ASICs and mining centralization. This is flat out wrong. Any successful proof-of-work based crypto-coin that develops high enough value will experience the same kinds of mining dynamics we're seeing with bitcoin. It's all about the money.

The Arms Race

Now that each bitcoin is worth hundreds of dollars, the 25BTC block-reward distributed by the protocol to bitcoin "miners" every 10 minutes is very enticing. More and more serious, and well-

funded, mining operations are appearing. You only need to glance briefly at a bitcoin-mining hashrate chart to understand that something explosive is going on here:



What are ASICS?

ASIC stands for Application Specific Integrated Circuit; ie, a specialized computer chip. Back in late 2012 when it became clear to some that bitcoin was likely to keep gaining in value, engineering teams started to work on developing ASIC chips for bitcoin mining. These chips could mine at 10-100x greater power-efficiency than the standard GPU (graphics-card) mining hardware at the time.

So what's the controversy?

ASICs are expensive. A single top-of-the-line ASIC rig (the chip + supporting hardware) can cost $5,000-$10,000. That makes cutting-edge bitcoin-mining hardware out of reach for many people. No longer can someone spend a few hundred dollars on a fast GPU card, stick it in any old computer, and profitably mine bitcoins.

That has some people in the bitcoin community forecasting doom at the hands of big-money, centralized, corporate bitcoin mining operators. The fear is that, eventually, there will just be a few huge bitcoin miners that are susceptible to less-than-honest practices or government interference.

How is this a problem with ASICs?

It isn't. People are just associating "big money" and centralized power structures with ASICs because ASICs cost "big money". The problem is not ASICs; it's the fact that when a coin achieves enough value, it suddenly becomes rational to throw significant money into mining it. This has already started happening to litecoin, with multi-thousand-dollar GPU rigs fairly common, and

scrypt-ASICs around the corner (something that litecoin's proponents originally said would never happen).

It's simply the case that people are going to invest money into mining gear if there's profit to be made. Whether the specific mining algorithm lends itself to ASICs, GPU farms, CPU farms, lots of memory, or something else, those with the ability to throw lots of money and compute power at the problem are going to get a greater share of the mining market. Eventually, this centralizes to those with the most power-efficient hardware, no matter what the algorithm.

So make no mistake: proof-of-work mining will be done at data-center scale in any mature and valuable coin.

First Take on Ben Lawsky's Reddit AMA

New York Superintendent of Financial Services, Ben Lawsky, took to Reddit today to do an hour-long "Ask Me Anything". He seemed reasonably open and thoughtful about the bitcoin space, taking care to mention several times that his team wants: "…to move carefully and not go so fast that we fail to see the unintended consequences of the framework".

Some highlights…

Regarding banks' unease with bitcoin-related activity:

"I think new, careful regulations, especially related to preventing money laundering, will make banks more comfortable with Bitcoin-related activity over time."

Clarifying his innovation-quashing comment from January's NYDFS hearings:

"In context, I was also trying to emphasize that money laundering is not to be taken lightly — in many ways it is the lifeblood of terrorism around the world. My hope is that if we can get appropriate guardrails in place to prevent money laundering, we can take a deep breath and really focus on trying to ensure that virtual currency firms flourish and continue to develop and innovate. I'm very excited about what the future could hold for this very powerful technology."

In response to an "on-ramp" for small virtual currency companies/startups, and the similarities to regulating small banks that don't have big budgets for compliance:

"We've had some success in getting these regulations amended so they don't crush smaller community banks. Any regulations we issue for virtual currency firms will have to be carefully

tailored with this in mind."

On the existence and potential of bitcoin and crypto-currency in general:

"Hard to put the genie back in the bottle. I can't predict the future but Bitcoin is certainly a new powerful technology that holds a lot of promise for the future if we can mitigate some of the potential negatives like money laundering."

"Bitcoin holds the potential to bring the costs of international transactions way down. That could be huge for the thousands and thousands of New Yorkers who today send money back to their families in their home countries at great expense."

What does Superintendent mean?

"No one knows what Superintendent means anyway."

Comments on incenting US-based exchanges:

"We hope regulatory clarity will attract exchanges to the United States. I suspect that they are staying offshore right now because they don't know what the rules of the road here are or will be. 2. We do hope that regulation will create a level of certainty that could incentivize banks to promote not stifle these innovations. I also suspect there are banks who are quite interested in the technology but are being risk averse for now in the absence of regulatory clarity."

He noted that his own thoughts/impressions on bitcoin have evolved significantly, saying:

"I've personally evolved a lot on the issue the more I have learned. I wouldn't compare it to a Rocky-IV-final-scene about-face and it has taken time for all of us at DFS to get our minds around it, but certainly our views have changed."

Regarding bitcoin mixers/tumblers:

"We are looking closely at "tumblers" and have been getting some feedback both pro and con. Don't have answer yet on that and would welcome additional thoughts people have. At our hearing, it was clear the use of tumblers was something that had created issues for law enforcement in their investigations. At the same time, we understand there can be legitimate uses for tumblers and we get that there can be real value in having privacy when it comes to financial transactions. Again, it becomes a question of getting the balance right."

On financial privacy:

"I think financial privacy is an important value. …. At the same time, there is an important competing value in preventing money laundering which often requires that those engaging in financial transactions (especially when large) provide some identifying information so we can make sure we're not permitting things like terrorist financing…"

MtGox [Update: below quote is from before MtGox's Feb 24th complete shutdown]:

"The Mt. Gox shutdown was a reminder that this is still a young industry and there are still problems getting worked out sometimes on a daily basis. I think we should stay positive about that. We're

seeing a shaking out of the industry and that's as it should be — it will lead to improvements. … Maybe more importantly, the Mt. Gox issue underscored for us that it would be far easier if we had some exchanges locally that we could interact with, allowing us to better understand these issues so as to protect those engaging in trades with the exchanges. We're hopeful that clear regulations, if done in a smart, modern way, may incentivize some of these exchanges to come ashore (hopefully here in NY)."

Bitcoin in general:

"I think Bitcoin or the underlying technology has a lot of potential on numerous levels. As Professor Athey said at our hearings, even the experts don't know today how the technology will evolve and what it will ultimately look like. But I do think it holds a lot of promise (if money laundering can be adequately addressed), both on its own and in terms of causing existing payments system technologies to up their game."

All in all, it's clear that Mr. Lawsky is looking deeply into the bitcoin space, and both sees the potential as a technology as well as the regulatory challenges. Let's hope Mr. Lawsky takes special care to allow the innovation to happen by keeping compliance burdens for innovators and small startups to a bare minimum. If you have a comment for Mr. Lawsky, he's active on Twitter: @BenLawsky

---

Bitcoin: Too Good to Hoard

At one point during last night's bitcoin debate between Jeffrey Tucker and Andrew Schiff, Andrew asked the audience: "How many of you have bought something with bitcoin?" Half the audience raised their hands. He then asked: "And how many of you regret it, given that bitcoin is worth 100 times what it used to be?" Almost all hands went back down.

There's something about bitcoin that traditional economists and finance people keep missing. Having spent their academic and professional lives theorizing about "rational" economic actors, they can't get over the fact that bitcoin's purchasing power changes a lot from month to month, sometimes hour to hour. Why would anyone use it under those conditions when they can just use something stable like dollars?

What they're missing is that bitcoiners **expect** the price to be volatile, and view that as a necessary and obvious price-discovery step in the rapid-adoption phase of a fascinating new technology. We see the potential, we understand how ground-breaking it is, and we want to use it **now**. We know it'll either be worth a lot more or a lot less in the future, but we're jump-starting the next phase of money here, and we're not gonna wait for "stability" to make use of it.

But don’t take my word for it. How about the guy who bought 10,000 BTC pizzas less than four years ago? Writing a week ago, he said:

“…I was pretty happy to trade 10,000 coins for pizza. I mean people can say I’m stupid, but it was a great deal at the time.”

He actually did this several times, eventually spending over 80,000 BTC (worth $50 million today) on pizzas:

“The pizza thing was a lot more popular than I thought so I made good on as many trades as I could.Other than a little bit of single digit change, I spent everything I mined.”

Transactions	
No. Transactions	3320
Total Received	81,432.09 BTC
Final Balance	0 BTC

Bitcoin is simply better money. It’s a pleasure to use. When I made my first bitcoin transaction, it struck me full-force that “THIS is how money should work.” Frictionless, secure, private, instant, decentralized. Using dollars online has none of those properties, and using bitcoin makes it obvious just how much of a problem that is.