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.