The Bitcoin Heist of Mt. Gox

Gousia Sultana Syeda
Graduate Engineering
Santa Clara University
Santa Clara, CA
gsyeda@scu.edu

Yae Jin Park
Graduate Engineering
Santa Clara University
Santa Clara, CA

David Marshall
Graduate Engineering
Santa Clara University
Santa Clara, CA

***Abstract*—Started as an exchange website for the famous card game Magic: The Gathering, Mt. Gox also started to provide a service for Bitcoin exchange. Soon, the website was handling and processing the majority of the Bitcoin exchange by 2014 - until the biggest hack in Bitcoin history takes place. Perhaps the hack was preventable, perhaps not. Glaring security issues of the exchange website has been existent before the hack occurred, and not solving them inevitably lead to Mt. Gox's fall. This research aims for the audience's better understanding on the concept of bitcoin exchange and the importance of security within exchanges related to said concepts through Mt. Gox's failure.**

Keywords—Bitcoin, blockchain, Mt. Gox, exchange, cryptocurrency

I. Introduction

When bitcoin started gaining popularity, the concept of trading regular, existing currencies into cryptocurrencies also started to gain attention. Mt. Gox (Magic: The Gathering Online eXchange) started as a card game trading service, then officially became a bitcoin exchange in July 2010 [1]. For several years since then, Mt. Gox was the largest bitcoin exchange where the majority of the bitcoin exchange took place, up to 70-80% of all existing trades [2]. Hence, it is not an exaggeration to state that Mt. Gox shaped the future of bitcoin. With such reputation and potential, Mt. Gox was frequently targeted by hackers and what ultimately brought the giant to collapse was the major hacking incident in 2014, known as the Mt. Gox Bitcoin Heist. Today, this unfortunate incident is still known as the biggest bitcoin heist and reminds the public of the dangers of information security.

This research paper aims to analyze the heist: Were the early warning signs there? What was the vulnerability the hackers exploited and how long was this vulnerability existent? What happened after the heist? We believe we can answer these questions and more through what we have learned about the principles of information security.

II. Basics of Bitcoin (Cryptocurrency) Exchange

A. Cryptocurrency Basics (Wallets and Blockchain)

Before analyzing the actual incident, the basic concept of how cryptocurrency transactions are executed needs to be reviewed. Imagine going into a grocery store and shopping. You hand a $20 bill to the cashier, and after the cashier takes it, you no longer have the $20. Then the transaction is recorded in a ledger. This is an example of a transaction - emulating this transaction in the digital world is the key point of cryptocurrency. Cryptocurrency is a means of peer-to-peer transaction of online payment - an electronic cash that is decentralized, meaning that it does not require a third party to regulate the transaction. The cryptocurrency that was taken in heist in the Mt. Gox incident is the Bitcoin. It is common that the majority of the population use the terms 'Bitcoin' and 'Cryptocurrency' interchangeably. While technically it is not wrong to do so, a distinction needs to be acknowledged to prevent any confusion. At present, there are many more cryptocurrencies other than Bitcoin, but Bitcoin carries a significance because it is the first cryptocurrency that was fully developed that can be exchanged like real currency.

It was mentioned previously that cryptocurrencies are decentralized, which means with the lack of a regulating third party that there needs to be a method to prevent "double payment" or possible fraud in the transaction itself that can happen within a peer-to-peer transaction system. The system implemented by the Bitcoin creators utilized a complex application of cryptography in order to make the system come to life. Without going into excessive detail, the main idea is that Bitcoin (or other cryptocurrencies in the market) transactions require verifications and digital signatures of those who are trading the digital currency. As an example, in Figure 1, Owner 1 sends Bitcoins to Owner 2 by first signing the hash of the previous transaction done by Owner 1. The hash can also be viewed as a transaction's unique identifier, or unique ID in short. Owner 1 then also signs Owner 2's public key, which defines an official transaction. Continuing such transactions between other users will build a chain of signatures by multiple Bitcoin traders, which is a way to

maintain authenticity of the exchange. This is essentially what a Bitcoin is - a chain of digital signatures. [3]

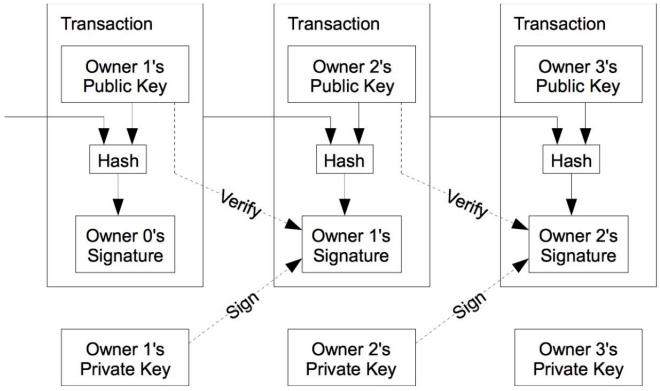

Figure 1. Conceptual diagram of a cryptocurrency

Transactions that are processed within a similar timeframe are grouped as a block, then the same blocks are stored in a chronological sequence known as the blockchain. The blockchain keeps transactions in chronological order through timestamps. As Figure 2 portrays, a blockchain hashes the block of transactions, timestamps, and the previous hash in the same chain. This system allows the system to ensure the integrity of the chain because as more blocks are added, the chain becomes more trustworthy and resistant to attack due to nested hashing. Ultimately, the system makes a blockchain a full ledger of all transactions of cryptocurrency, and users need access to this ledger in order to do any cryptocurrency transactions. When a transaction is made, it needs to be recorded in the blockchain as an announcement to all Bitcoin traders. The blockchain is immutable, and so it being a ledger of all transactions ensures prevention of fraud through technicality such as duplicate attempts in transaction.

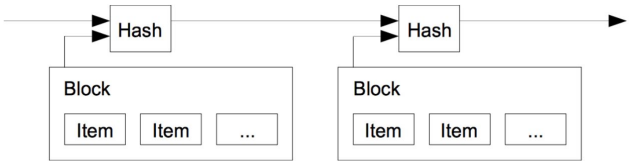

Figure 2. Conceptual diagram of a blockchain

B. Bitcoin Wallets and Bitcoin Exchange Regulation

From the cryptocurrency basics, it is now clear that in order to participate in a Bitcoin exchange, one needs a set of public and private keys in order to access Bitcoins. This is what cryptocurrency wallets are - a set of said keys. In analogy to the real world currencies, they would be the equivalent of the username and password to your bank account online. There are two types of keys: hot and cold. The main difference between the two is that hot wallets are connected to the Internet and so they allow immediate transactions. Mt. Gox had both hot and cold wallets, but in the heart of the issue was the compromise of its hot wallets. The incident will be described in detail in the later sections.

Why does cryptocurrency exchange hack pose such a risk? Despite the exchange boom that started approximately a decade ago, there are no current global regulations that keep Bitcoin (or any other cryptocurrencies) exchange in control. The degree of regulation of bitcoin mining and exchange depends on the geographical location of the trader [4], as some individual countries decided to enforce a certain degree of regulation within their jurisdiction. Individual countries' attempt to regulate the bitcoin flow within the economy can be largely divided into three categories have forbidden bitcoin mining or banks' handling of cryptocurrencies altogether:

1) Strong regulation on bitcoin trade (e.g. banning banks from handling cryptocurrency altogether, banning Initial Coin Offerings)
2) Some regulation on bitcoin, but only issued warnings on risks on potential financial damage to individuals/corporations of bitcoin trade (e.g. requiring license to start an exchange, taxing bitcoin as an asset)
3) Little to no regulation

For example, China and Iran are classified as category 1 because of their strict regulation on bitcoin exchange. Bitcoin exchange in both countries is illegal. Israel and Gibraltar are category 2 because they require certifications for launching an exchange, and Bitcoins are treated as assets that can be taxed. Belarus and Brazil would be categorized under type 3 as taxation of the trade is the maximum "regulation" for both legislations. However, not having a global regulation means there is no method to block cross-border transactions. If one resides in, for example, China, simply moving to Australia will allow said person to trade Bitcoins.

Another risk of not having a global regulation is that when a fraud or other unfortunate incidents involving the loss of Bitcoins or funding for Bitcoin occur, it is unclear who is responsible for minimizing the damage from said incidents except the traders themselves. Real currencies have governments and banks minimize the fluctuations in the currency value, but cryptocurrencies do not have the means to do the same because they are decentralized. What this means is that it is possible for a terrorist organization to hack multiple Bitcoin wallets and steal the Bitcoins, but it will be very difficult to track them because of the lack of global regulation - which country/jurisdiction is responsible for tracking the

hackers? The Mt. Gox Bitcoin Heist demonstrated this risk combined with the lack of information security within the exchange itself. We now aim to analyze the security measures taken by the Mt. Gox website prior to the heist and its vulnerabilities that foreshadowed the biggest hacking incident in bitcoin history.

III. Mt. Gox Bitcoin Heist - Before the Incident

In 2007, Jed Mc Caleb started an online website "Magic: The Gathering Online", a card game service where cards were traded like stocks. In 2009, he used the website to advertise his card game 'The Far Wilds'. It was in July 2010, when Mc Caleb decided to repurpose the domain as Mt. Gox (Magic: The Gathering Online Exchange) a bitcoin exchange domain. Due to lack of time he thought that he was not making justice to the website in bringing it to the potential it had, so he sold the website to Mark Karpeles in March 2011. Mark Karpeles was an avid programmer and a software developer based in Japan [1]. As soon as he acquired the site, he thought of reprogramming the backend software and therefore made it the world's famous Bitcoin exchange platform. But due to the massive hack of Mt Gox, Mark Karpeles resigned from the Bitcoin Foundation on Sunday 23 February 2014, and Mt Gox closed its website on Tuesday 25 February 2014.

The organization was not well structured and there were many loopholes in the way they ran the business. Mt.Gox used a cryptocurrency hot wallet where digital currencies, both public and private keys were stored. It also had a cold wallet that stored the Digital currencies. As mentioned previously in the cryptocurrency basics section, hot and cold wallets are the two types of Crypto wallets [1]. Hot storage wallets are online wallets. If you trade often, you need to acquire a hot wallet. However, they are prone to be hacked due to their online connectivity. Cold storage wallets are offline wallets that store on hardware such as USB drives or smartphones. If you don't trade often like for months or years, cold wallets are the safest choice. These wallets are vulnerable to external damage, human error and theft.

From a security standpoint, prior to the initial attack in June 2011, Mt.Gox user login was not secure and did not implement a two-factor authentication. A two-factor authentication comprises of a user-defined password and a one-time temporary PIN sent via text or email. This is a minimum requirement for logging into any financial or banking sector these days.

On the server side, the data was not completely secure. The database was easily accessible by the former owner McCaleb's old administrative account which was still active. The data was encrypted using one-way hashing function MD5 that was not suitable for securing transactional data in a financial organization. Karpeles wrote his own remote-access security ("SSH server"). He did so in the programming language *PHP,* which is a dangerously unsafe language intended for low-security applications like displaying web pages [5]. It has no error checking or safety nets of any kind. The company did not use a software version control to align their software patches and to avoid accidental code modifications. Moreover, only Karpeles, the owner of Mt.Gox could authorize changes to the source code. This would significantly delay any possible security updates to the customers. Mt.Gox did not have a testing environment in place until 2013. This indicates that no software testing was performed before the update was released to the customers [6].

Mt.Gox, though started with the right intentions, did not operate completely in an ethical manner. The company did not register with the US government as a money transmitter. It did not have a clear overview on the BTC balance in its offline/cold storage. The company was never transparent with its customers in regard to the initial attacks and the loss incurred.

In 2011, Japan didn't consider Bitcoin as a means of currency and no financial regulations were applied on Mt.Gox. The Japan government considered Bitcoin as a commodity and it was only subject to sales tax [7].

IV. Mt. Gox Incident and The Aftermath

A. Notable Issues Before the Incident

The heist that became Mt. Gox' downfall was not the first problem that the exchange experienced. In mid-2011 the market was manipulated by a hacker who accessed the former CEO's account mentioned above. The hacker then assigned a large number of coins to the account and attempted to sell them off at any price offered. This promptly created a crash in the price of bitcoin from about $17.50 to $0.01 - at which point the hacker likely purchased bitcoin at the depressed price with another account. The price recovered the next day.

Around the same time Mt. Gox discovered that code had been inserted into their database that allowed unauthorized access to usernames, emails, and password hashes. Fortunately the hackers did not fully exploit the breach, and little damage was actually done [8]. Mt Gox initially blamed users for allowing their passwords to be compromised, but had to admit fault shortly thereafter. After

the breach Mt. Gox admits that its security infrastructure was not adequate for a large financial exchange.

As the exchange entered 2014 it was dealing with a number of regulatory issues in both the US and Japan. The result was that it was taking weeks or months to make a withdrawal from Mt. Gox. A series of smaller incidents also contributed to the perception that Mt. Gox was not stable enough to handle the amount of money flowing through its coffers. Unfortunately, the critics were correct.

B. The Bitcoin Heist

On February 7th Mt. Gox shut down all bitcoin withdrawals. On the 10th it issued a press release, stating that "a bug in the bitcoin software" was responsible for allowing a third party to redirect bitcoin in a transaction from one wallet to another, effectively stealing the bitcoin [9]. This flaw in bitcoin's code can be mitigated by exchanges [10], but Mt. Gox was simply not a robust enough institution to handle the bug. Security was not Mt. Gox' priority, and that led to its downfall.

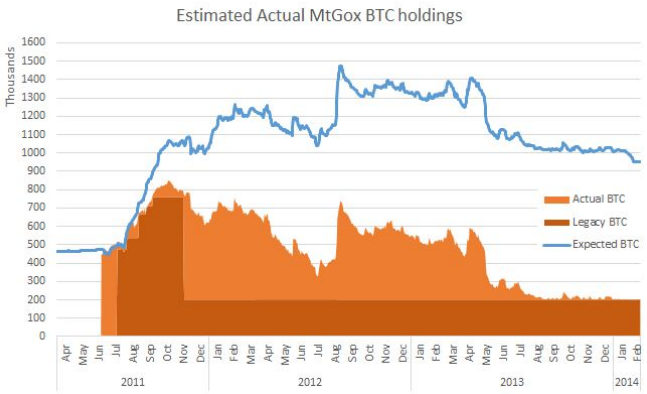

Figure 3. WizSec's data on Bitcoin value (Month vs. Dollar - Thousands)

Figure 3 is a chart from a bitcoin security company, WizSec, that performed an investigation of the heist [11]. The blue line is how many BTC Mt. Gox "should" have had on hand, based on the number and amount of deposits. The orange section below is how many BTC Mt. Gox *actually* had, with the dark orange being a portion of its holdings that were unintentionally left in a cold wallet. This portion is what was "discovered / recovered" later.

This graph illustrates the reality - the BTC was stolen slowly over time starting in September of 2011 from the hot wallet, and that Mt. Gox was actually insolvent as of mid 2012. Much like a ponzi scheme, it was only user's continuing deposits and faith in the exchange that kept it afloat.

In an unknown method, the private keys to Mt. Gox's hot wallet had been stolen. The method was simply to copy the unencrypted file containing the private keys. How this happened is not quite known - the computer with the file could have been hacked from the outside, or an insider could have simply copied the file. The keys gave hackers access to the hot wallet, but not Mt. Gox' cold wallets. However, over time, Mt. Gox as moved BTC from cold to hot wallets nearly all of their internal holdings were exposed in the hot wallet and siphoned off. Mt. Gox didn't discover the theft until February of 2014, much too late.

For the rest of February, the Mt. Gox team attempted to assess what was happening to the account. The company declared a form of bankruptcy in the Japanese courts on February 28th, 2014. It would never recover, and the bankruptcy is not resolved as of today.

C. The Aftermath

Mt. Gox filed for bankruptcy on February 28th, 2014. "nearly all the bitcoins in the exchange's possession - 850,000 of them - were missing." [12] The approximate value of 850,000 BTC on that day was $467 million. If the hackers have kept their bitcoin, those 850,000 BTC are now worth $6.2 billion. Karpeles eventually recovered about a quarter of the lost bitcoin (the cold storage mentioned above was discovered).

In 2017, US law enforcement announced that a Russian man, Alexander Vinnik, suspected of laundering much of the stolen bitcoin was arrested in Greece. His case is still ongoing. WizSec, who has to date published the most complete explanation of the hack I've found, believes that Vinnik is also responsible for or closely associated with the heist [11].

The CEO of Mt Gox, Mark Karpelès, has been in and out of legal trouble related to Mt. Gox until this year. He has been charged with embezzlement, fraud, and data manipulation in the French and Japanese courts. These cases were finally resolved in March of this year (2019) when he received a suspended sentence of 30 months in prison by the Japanese court system for falsifying data without the intent to cause harm, but was acquitted of the other, more serious charges. He reportedly still holds more than $1 billion in bitcoin.

V. Conclusion

In this paper, we analyzed the incident of the Mt. Gox Bitcoin heist by first understanding the basic technicality in cryptocurrency trading and the existing vulnerabilities of the Mt. Gox exchange website. To summarize, Bitcoin (and cryptocurrencies in general) require a hot wallet to make transactions among users, and it was these hot wallets stored in the Mt. Gox exchange that were hacked. Exactly how the keys to the hot wallets were stolen is still unknown, and it is highly recommended that a thorough investigation is performed in order for other cryptocurrency exchanges to prevent future hacking attacks. Although extremely popular for financial investment, there are still no global regulation on the value fluctuation or financial fraud for cryptocurrency, and so it is not an exaggeration to say that the exchange is the only means of protection for cryptocurrency traders.

References

[1] A. Norry, The History of Mt. Gox Hack: Bitcoin's Biggest Heist. June 7, 2019. https://blockonomi.com/mt-gox-hack/

[2] J. Frankenfield. Investopedia, Mt. Gox. June 25, 2019. https://www.investopedia.com/terms/m/mt-gox.asp

[3] G. Nash. Medium. "What Exactly Is Bitcoin?" June 27, 2017. https://medium.com/crypto-currently/what-exactly-is-bitcoin-3d5417bff390

[4] The Law Library of Congress. "Regulation of Cryptocurrency in Selected Jurisdictions." June 2018. https://www.loc.gov/law/help/cryptocurrency/regulation-of-cryptocurrency.pdf

[5] R. Falkvinge. Falkvinge on Liberty. "Security At Mt.Gox Much Worse Than Originally Imagined." March 11, 2014. https://falkvinge.net/2014/03/11/just-how-abysmal-was-gox-security-anyway/

[6] R. McMillan. Wired. "The Inside Story of Mt. Gox, Bitcoin's $460 Million Disaster." March 3rd, 2014. https://www.wired.com/2014/03/bitcoin-exchange/

[7] R. Dillet. TechCrunch. "Japan's Government Has No Plans To Regulate Bitcoin Transactions After Mt. Gox's Demise". March 7, 2014. https://techcrunch.com/2014/03/07/japan-government-has-no-plans-to-regulate-bitcoin-transactions-after-mt-goxs-demise/

[8] R. Chirgwin. The Register. "Bitcoin Collapses on Malicious Trade." June 19, 2011. https://www.theregister.co.uk/2011/06/19/bitcoin_values_collapse_again/

[9] Mt. Gox Team. Mt. Gox https://web.archive.org/web/20140210122955/https://www.mtgox.com/press_release_20140210.html

[10] The Guardian. "How a bug in bitcoin led to Mt. Gox's Collapse." https://www.theguardian.com/technology/2014/feb/27/how-does-a-bug-in-bitcoin-lead-to-mtgoxs-collapse

[11] WizSec. "The missing Mt.Gox Bitcoins." April 19, 2015. https://blog.wizsec.jp/2015/04/the-missing-mtgox-bitcoins.html

[12] J. Wagstaff. Reuters. "Mt.Gox bitcoin debacle: huge heist or sloppy glitch?" February 28, 2014. https://www.reuters.com/article/us-bitcoin-mtgox-heist/mt-gox-bitcoin-debacle-huge-heist-or-sloppy-glitch-idUSBREA1R0Y720140228