# Top Ranked Engineering College in Kolhapur, Sangli, Satara, Ratnagiri| KIT'S College Of Engineering (Autonomous)

# Kolhapur Institute of Technology’s College of Engineering (Autonomous)

**Gokul Shirgaon, Kolhapur**

**Department of Computer Science and Engineering**

**Case Study on**

# Mt. Gox Bitcoin exchange

**Submitted to**

**Mr. S. S. Rabade**

**Submitted by,**

## Amit Khadke

**Division: A Roll no: 42**

# Magic: The Gathering Online eXchange (Mt. Gox)

Mt. Gox was the biggest bitcoin exchange in the world in the 2010s, until they were hit by a software error that ultimately proved fatal.

The glitch led the exchange to create transactions that could never be fully redeemed, costing up to $1.5 million in lost bitcoins.

But Mt. Gox’s woes didn’t end there. In 2014, they lost more than 850,000 bitcoins (valued at roughly half a billion USD at that time but now it would be worth more than $19 Billion) in a hacking incident. Around 200,000 bitcoins were recovered, but the financial loss was still overwhelming and the exchange ended up declaring bankruptcy.

### BACKGROUND:

Mt. Gox was a Bitcoin exchange that was established in 2010 by Jed McCaleb, a programmer and entrepreneur based in the United States. The name "Mt. Gox" stood for "Magic: The Gathering Online Exchange," as the platform originally started as a marketplace for players of the popular trading card game.

However, in 2011, McCaleb sold Mt. Gox to Mark Karpelès, a French software developer who moved the company's headquarters to Tokyo, Japan. Under Karpelès' leadership, Mt. Gox became one of the largest Bitcoin exchanges in the world, with an estimated 70% to 80% of global trading volume at its peak.

Mt. Gox's success attracted a large user base and millions of dollars' worth of Bitcoin transactions daily. However, the exchange experienced multiple security breaches and technical issues, leading to the loss of a significant amount of Bitcoin. In February 2014, Mt. Gox halted all Bitcoin withdrawals, citing technical issues.

### WHAT HAPPENED?

When you send bitcoins to an address, what happens inside the Bitcoin transaction is more complicated than we can imagine. The transaction contains a tiny computer program in the Bitcoin Script language, and this program is executed to determine if the bitcoins can be sent. Normally the program requires a public key and signature in order to send the bitcoins. The program checks that the public key matches the address you sent the bitcoins to, and the signature is valid, proving the sender of the bitcoins has the private key. If everything matches, the bitcoins can be sent.

Here the idea is that, by providing a programming language, Bitcoin allows many different types of transactions, such as escrow transactions or more complex contracts. Going into a bit more detail, a typical scriptPubKey program looks like:

OP\_DUP

OP\_HASH160

f2e63314c350094550c703fcdcd4850ad37d8310

OP\_EQUALVERIFY

OP\_CHECKSIG

This program is part of a transaction that sent bitcoins to the address 1P9LHy6K2c9cwbfSfdaaoYVAprqUYtcFnB (which in hex is the f2e633... value above).

In order for that address to redeem the bitcoins, the receiver must provide the public key for the address 1P9L... and provide the signature for the sending transaction (which proves they have the private key). Walking through the execution of the program, it first duplicates the provided public key, computes the 160-bit hash of it, and verifies that it is equal to the provided public key address. Then it checks the signature for validity. If all goes well, the bitcoins can be sent. If there is a problem, the transaction is rejected.

In Mt Gox's bad transactions, they made a small but costly error. The script is:

OP\_DUP

OP\_HASH160

0

OP\_EQUALVERIFY

OP\_CHECKSIG

In place of the destination address hash, this transaction has the byte 0, representing OP\_0, which pushes an empty array of bytes. Since it's impossible for the 160-bit hash to match an empty array, it's impossible for this script to complete successfully, and the bitcoins can never be sent.



**PROXIMATE CAUSE:**

The proximate cause of the Mt. Gox software failure was a flaw in the exchange's software that allowed hackers to exploit a bug in the Bitcoin protocol called "transaction malleability." This flaw enabled attackers to manipulate the transaction ID of a Bitcoin transfer, causing it to appear as if the transfer had not been completed, which allowed the attacker to withdraw the same Bitcoins multiple times.

This flaw had been known in the Bitcoin community for some time, and other exchanges had taken steps to mitigate its effects. However, Mt. Gox had not implemented these measures, leaving the exchange vulnerable to the attack.

The flaw was exacerbated by a lack of proper accounting procedures and oversight at Mt. Gox. The exchange's management did not have an accurate understanding of the extent of the problem, and this lack of oversight allowed the hackers to continue exploiting the flaw undetected for an extended period, resulting in the loss of hundreds of thousands of Bitcoins.

**UNDERLYING ISSUES:**

1.Poor security practices:

Mt. Gox had a history of poor security practices, including storing customer funds on an insecure, online-based system and failing to implement basic security protocols like two-factor authentication.

2.Lack of accounting controls:

The exchange had poor accounting controls and a lack of oversight, which meant that management did not have an accurate understanding of the extent of the company's financial losses.

3.Technical issues:

Mt. Gox's software was not able to handle the high volume of transactions on the platform, leading to a range of technical issues and frequent outages.

4.Poor management practices:

Under the leadership of Mark Karpelès, Mt. Gox lacked proper management practices, including failing to communicate effectively with customers and the wider Bitcoin community.

5.Lack of transparency:

Mt. Gox was not transparent about the issues it was facing, leading to speculation and confusion among customers and investors.

6.Cybersecurity threats:

The exchange was vulnerable to cybersecurity threats, including hackers exploiting a bug in the Bitcoin protocol called "transaction malleability."

**VERIFICATION AND VALIDATION:**

Mt. Gox’s software code was not reviewed by any of the third party so no one had an idea that whether it met the industry standards or not. The exchange’s software was not tested properly and without testing the software they made it available for the people.

Mt. Gox technical staff didn’t conduct peer reviews and because of that errors were introduced in the software.

Mt. Gox could have undergone regular compliance audits to ensure that the exchange was operating within the bounds of relevant regulations and legal requirements but they didn’t do that. The exchange’s software was not tested by the sample group of users to ensure that whether it met with their needs and expectations.

**PREPARATIONS AND UNDERSTANDING:**

1.Understanding the technology:

Mt. Gox's leadership and technical staff didn’t have a thorough understanding of the Bitcoin protocol and the associated security risks.

2.Prioritizing security:

The exchange didn’t prioritize security and they didn’t implement best practices such as two-factor authentication, encryption, and regular security audits.

3.Implementing effective accounting controls:

Mt. Gox didn’t implement effective accounting controls to ensure that the company had a clear understanding of its financial position and was not vulnerable to fraud.

4.Communicating effectively with stakeholders:

Mt. Gox didn’t communicate effectively with its customers, investors, and the wider Bitcoin community about the challenges the exchange was facing, rather they provided improper information.

5.Developing a disaster recovery plan:

Mt. Gox didn’t develop a disaster recovery plan in case of unexpected events such as a security breach.

**AFTERMATH:**

1.Financial loss for customers:

Customers of Mt. Gox lost hundreds of thousands of Bitcoins when the exchange collapsed, resulting in significant financial losses for many individuals and businesses.

2.Reputation damage for Bitcoin:

The Mt. Gox failure damaged the reputation of Bitcoin and other cryptocurrencies, contributing to negative perceptions about their reliability and security.

3.Regulatory scrutiny:

The failure of Mt. Gox prompted increased regulatory scrutiny of Bitcoin and other cryptocurrencies, leading to new regulations and laws aimed at improving security and preventing fraud.

4.Industry-wide changes:

The Mt. Gox failure prompted changes in the cryptocurrency industry, including improved security measures, increased transparency, and the development of new technologies and platforms.

5.Changes in the exchange landscape:

The collapse of Mt. Gox led to the rise of new cryptocurrency exchanges, some of which incorporated the lessons learned from the Mt. Gox failure into their operations.