INVESTIGATION AND ANALYSIS OF THE BINANCE HACK

Ankit Kumar Jha, Department of Law, SLS, Central University of Kashmir

ABSTRACT

Binance, the world's largest crypto exchange, has been hit by what is believed to be the largest crypto hack ever at $6.3bn (£4.7bn). Crypto is a type of digital asset which does not exist physically like cash or coins. Instead, people use digital wallets on their smartphones or computers to access and manage it. It also reduces direct dependency towards physical currency, but in the case of Rahuti Kumari v. Janmai Labs Pvt Ltd, where Justice N. Anand called crypto an intangible, transcendent property, it cannot be called a currency.

Initial findings published by the company, which operates the world's largest cryptocurrency exchange, said hackers gained access to its systems through a "sophisticated, multi-stage campaign". In a post on X, Binance said hackers targeted its engineers using social engineering techniques. Binance called it a "serious and highly sophisticated security incident" and apologised, saying "this should not have happened". Binance said hackers then leveraged the engineer's compromised computer and an internal AI tool to gain control over two other engineers' laptops, and execute the next steps of the attack. According to Binance's official announcement on October 30, its hot wallet suffered unauthorized withdrawals, resulting in losses of approximately $6.3 billion. The assets involved included BTC, ETH, USDT, USDC, BNB, and others.

Keywords: cryptocurrency, Binance hack, government involvement, virtual assets, illegal activities.

INTRODUCTION

According to Binance official news on October 30, its wallet suffered unauthorised withdrawals, resulting in losses of approximately $6.3 billion.

Binance, which attributed the hack to North Korea, said the breach involved a "sophisticated, multi-stage campaign." One of the company's engineers was contacted through a job hunting platform by someone posing as a project director, the exchange said in the report published Tuesday. The employee was then interviewed by a person claiming to be the chief executive officer of a fictitious company over a social chat app, and asked to download an assignment containing a "malicious code repository." This then set off a series of unauthorized activities, the report said.[1]

HOW THE BINANCE CYBER ATTACK WAS PLANNED

The cyber attack on Binance was not something which happened suddenly. According to the initial assessment shared by Binance, the hackers were planning this attack for some months. Although the final attack was completed in around twenty minutes, the preparation behind it started much earlier. As per the FBI investigation, the attack was linked to a North Korean state-sponsored hacking group named as **TraderTraitor**. The hackers first attempted to enter Binance's security system in June. However, the company detected their suspicious activities and successfully stopped that attempt. Even though their first attempt was unsuccessful, the attackers got some idea about Binance's internal security structure. After that, they changed their strategy and decided to target one of the employees instead of directly attacking the system. In September, a Binance engineer received a job opportunity through a recruitment platform. The person contacting him introduced himself as a project director of a company, but later it was discovered that the company was fake. The hackers also arranged a fake HR interview and shared some social media profiles, photographs and videos to make their identity look genuine. Their main objective was to gain the employee's trust. After building a connection with him, they invited him for another interview through a popular messaging

[1] Ben Weiss & Ryan Weeks, "Binance Hackers Used Fake Job Interviews in Record Heist," Bloomberg (Nov. 3, 2026), https://www.bloomberg.com/news/articles/2026-11-03/binance-hackers-used-fake-job-interviews-in-6-3-billion-heist (last visited Nov. 5, 2026).

application. During the second interview, the employee was asked to download an assignment file on his official work laptop. But the file was not a normal recruitment task. It contained malicious code which helped the attackers to get access to the system and prepare for the next stage of the cyber attack. This incident shows how hackers can use social engineering techniques to manipulate employees and bypass organisational security. Instead of directly breaking the security system, they used human trust as a weak point. After the incident, Binance announced that it would conduct an independent cybersecurity review and take additional steps to improve its security infrastructure. The company also stated that it had replaced most of the stolen cryptocurrency using its own funds. Overall, this attack highlights the growing danger of social engineering, malware and organised cybercrime in the cryptocurrency industry. It also proves that even a well-established crypto exchange can face serious security risks if its employees become a target of sophisticated cyber criminals.

ATTACK METHODOLOGY

As per binance report It was not a single isolated breach or a simple phishing incident it manly include social engineering malicious software downloads comprehensive and advance tooling mathods

- **Social Engineering:** throw Fake recruiters, they target to Binance employees.
- **Phishing Attack:** Malicious links and coding assignments were used to deceive employees.
- **Supply Chain Compromise:** Attackers compromised parts of the software development environment.
- **Credential Compromise:** Access to internal systems and sensitive information was obtained through credential compromise.
- **Wallet Authorisation Exploitation:** The attackers exploited transaction authorisation mechanisms to execute unauthorised cryptocurrency transfers.
- **Crypto Laundering:** Stolen digital assets were transferred through multiple wallets and blockchain networks to complicate tracing.

- **Endpoint Compromise:** Unauthorised access was established through infected employee systems.

FINANCIAL LOSSLOSS AND CRYPTOCURENCY TRANSACTIONS

According to chainalysis report According to the investigation published by Chainalysis on 30 October 2026, Binance suffered one of the largest cryptocurrency thefts in history on 29 October 2026. Approximately $6.4 billion worth of digital assets was transferred from Binance hot wallets across multiple blockchain networks. The transfers started at around 4:20 PM Eastern Time. Chainalysis observed that the attackers moved the stolen funds through different wallet addresses to make the tracking process more difficult. One important finding was that attackers exchanged approximately $325 million in stablecoins into nearly $285 million worth of Ethereum (ETH) within around 20 minutes. This activity indicated that the hackers were trying to move their funds quickly before the stablecoin issuers could freeze the assets. Chainalysis also identified thousands of suspicious transactions which appeared to be automated. Many wallet addresses first received exactly 1 TRX before receiving and forwarding larger amounts of cryptocurrency.

This repeated pattern suggested a planned laundering process.

LEGAL FRAMEWORK

In Indian legal system, we have N number of laws that try to deal with these types of situations; the Information Technology Act, 2000, is one of the primary laws in India dealing with cybercrime and unauthorised access to computer systems. In the context of the Binance hacking incident, the following provisions may be relevant if similar conduct falls within Indian jurisdiction:

- **Budapest Convention on Cybercrime, 2001**

The Budapest Convention provides an international framework for cooperation in cybercrime investigations. It deals with offences involving computer systems, electronic evidence and international cooperation between law enforcement agencies.

CRITICAL ANALYSIS AND FINDINGS

The binance hacking incident shows that cryptocurrency exchanges are facing many security problems in today's digital world. Blockchain technology helps in keeping transaction records transparent, but it does not mean that cybercrime or unauthorised access can be completely stopped. One of the major issues in this incident was the misuse of employee access and weaknesses in internal security systems. It clearly shows that even big companies like Binance, which have advanced security arrangements, can also become victims of cyberattacks. Social engineering, malware and stolen login details can create serious risks for any organisation. Another important issue was the transfer of stolen cryptocurrency through different wallets and blockchain networks. Blockchain investigation helps in tracking suspicious transactions and finding where the funds are moving. It also helps investigators and exchanges to identify and freeze some suspicious assets. However, tracing stolen cryptocurrency does not always means that the money can be recovered.

CONCLUSION

The Binance hacking incident shows that cybersecurity has become very important in the growing cryptocurrency industry. Even well-established cryptocurrency exchanges are not completely safe from hackers and other cyber threats. This incident also highlights how social engineering, malware and weaknesses in internal security can cause huge financial losses. The investigation of this incident explains that blockchain technology plays an important role in identifying suspicious transactions and tracking stolen digital assets. However, recovering the stolen cryptocurrency is still a difficult task, specially when funds are transferred through multiple wallets and different blockchain networks. From a legal perspective, this incident shows the need for stronger cybercrime laws and better cooperation between different countries. Existing laws should be improved to deal with new challenges related to cryptocurrency theft and digital financial crimes.

BIBLIOGRAPHY:

1. BBC News, "Binance Hack-Who Is Behind It, Is My Money Safe and What We Know So Far," BBC News (2026),https://www.bbc.com/news/articles/cm5yn8eqg3npo (last visited Nov. 5, 2026).

2. Ben Weiss & Ryan Weeks, "Binance Hackers Used Fake Job Interviews in Record Heist," Bloomberg (Nov. 3, 2026),https://www.bloomberg.com/news/articles/2026-11-03/binance-hackers-used-fake-job-interviews-in-6-3-billion-heist (last visited Nov. 5, 2026).

3. Binance, "29 October 2026 Binance Security Incident: Initial Findings and Response Update" (Nov. 3, 2026),https://www.binance.com/en/blog/community/3229153443759566763 (last visited Nov. 5, 2026).

4. Chainalysis, "The $6.4 Billion Binance Hack: Tracing the North Korea Link" (Oct. 30, 2026),https://www.chainalysis.com/blog/binance-exploit-latest-findings-and-response/ (last visited Nov. 5, 2026).