Binance Hack of October 7, 2022

Laasya Vajjala, Surya Pramod Vadapalli

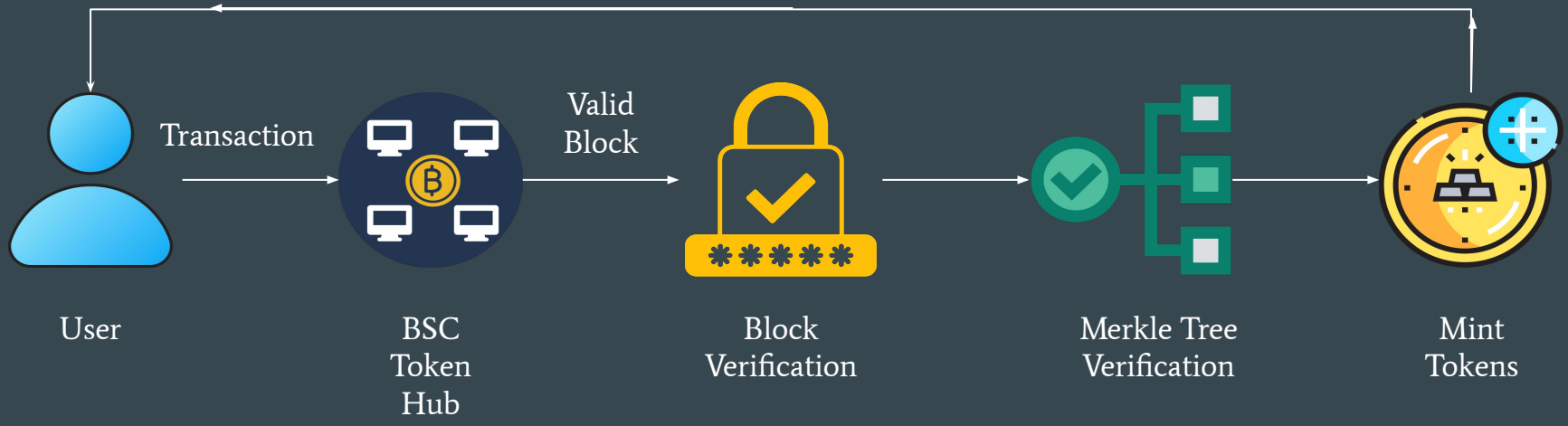
Binance?

World's largest cryptocurrency exchange platform, facilitating the trading of digital currencies such as **Bitcoin** , **Ethereum** , and its own cryptocurrency, **Binance Coin (BNB)** .

Background

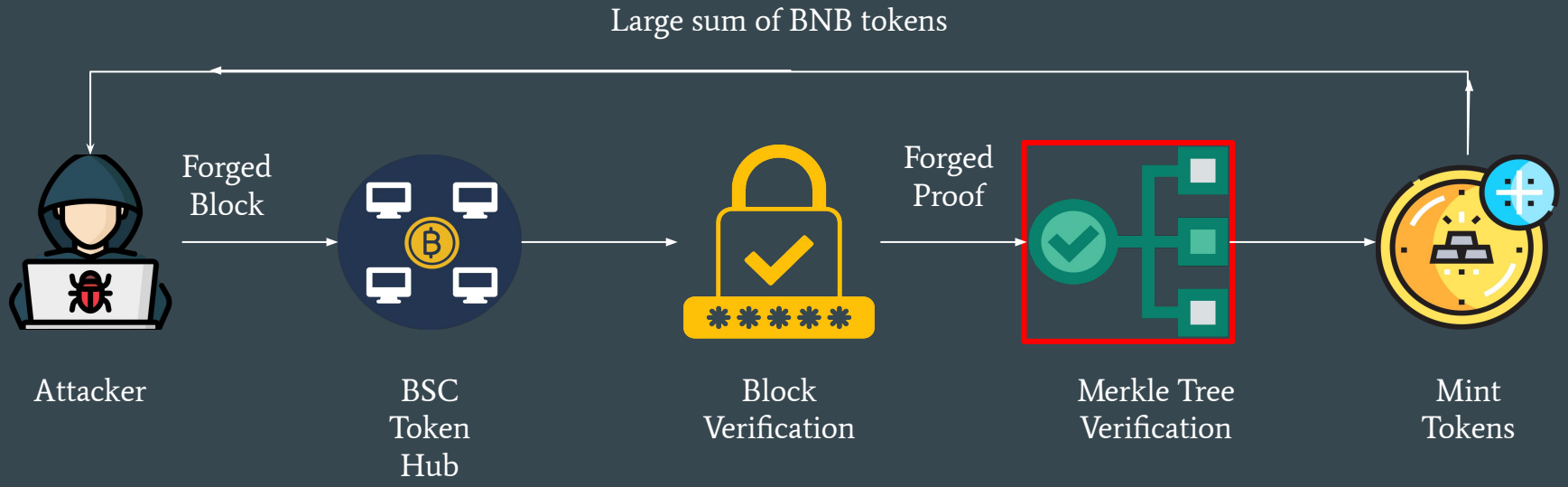
Cross-chain bridges are protocols that facilitate the transfer of assets between different blockchain networks.

BSC Token Hub

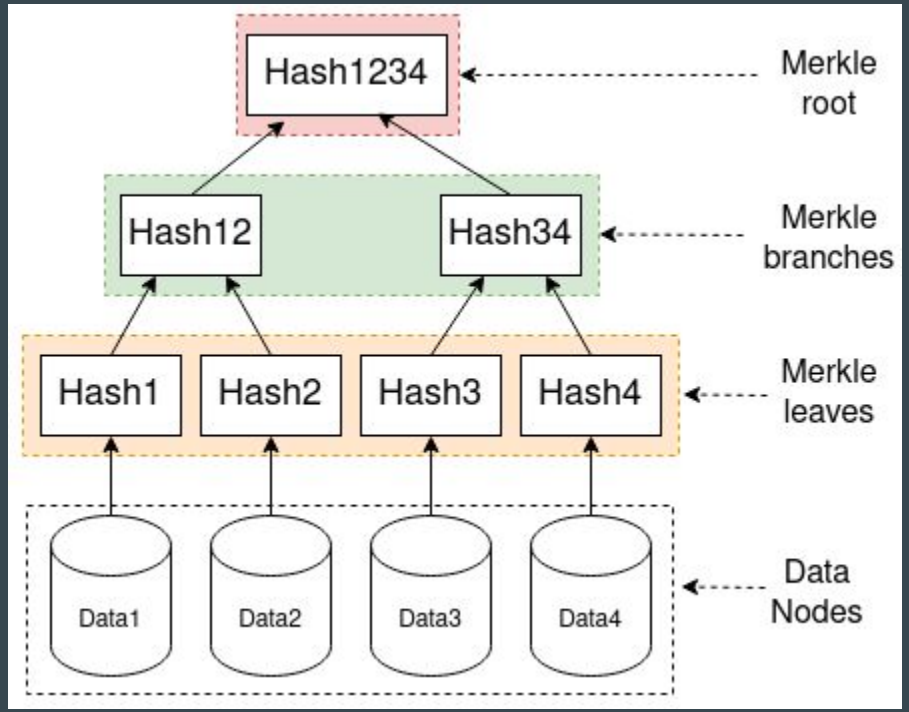


Binance Attack

The attacker exploited a vulnerability in the bridge's verification system by forging proof for a block created two years prior.

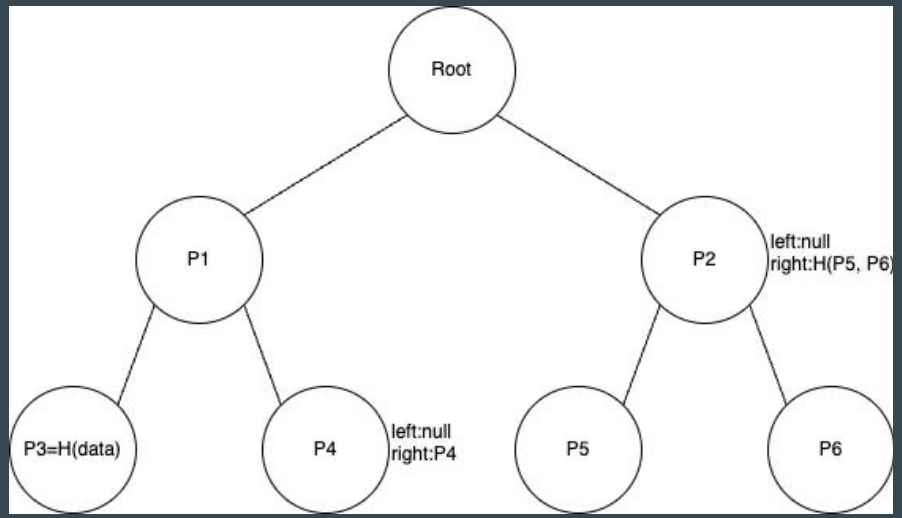


Root Cause: Failure in Merkle tree verification



- Merkle trees provide a way to verify the inclusion of data in a database without disclosing all the data.
- This is achieved by hashing the values in a tree structure where each node is a hash of its children, and the leaf nodes are hashes of the underlying data.

Root Cause: IAVL Verification



- IAVL trees extend the concept of Merkle trees by introducing additional attributes—left and right attributes—to guide the concatenation of child node hashes.
- The root cause of the exploit lies in the mishandling of these right attributes during the calculation of the root hash.

Root Cause:

The Problem:

The code only considered one child node (left or right) when calculating the hash for intermediate nodes.

An attacker could exploit this by adding a new leaf node (right child) while keeping the original left child and creating an empty intermediate node.

This manipulation wouldn't change the root hash, allowing the attacker to forge a proof for the new data.

This vulnerability could be used to inject fake data into the system without compromising the root hash.

Exploiting: Proof of concept

The attacker exploited a vulnerability by providing malicious right attributes, which allowed them to pass invalid proofs.

This was possible because the proof was user-controllable, allowing the attacker to introduce malicious data into the tree without invalidating the root hash.

- Crafting the payload
- Modifying the proof
- Hashing the malicious payload
- Verifying the new proof
- The successful execution of the PoC

Involvement

"BNB bridge exploiter"

Registering as a relayer for the Binance Bridge and manipulating verification proofs to exploit the bridge's security vulnerabilities.

Consequences

- The hack resulted in the loss of **$570 million worth** of BNB tokens.
- The incident caused the price of BNB to drop by 3.7%.
- Binance paused the network to prevent further movement of funds.

Countermeasures

Freezing funds with the cooperation of other blockchain entities, notably Tether and Circle, which froze $33.5 million in illicit assets.

Binance proposed on-chain governance votes to decide whether to offer a 10% bounty for finding the hacker and setting up a bug bounty program to reward individuals who report vulnerabilities.

Not the first hack Binance faced

- In 2019, Binance lost 7,000 Bitcoins.
- Binance has compensated users for losses.

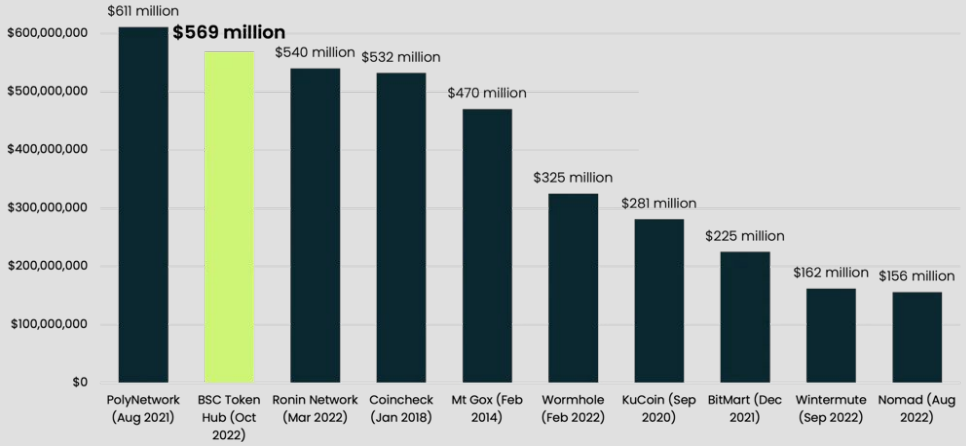
Cross-chain bridges are frequently exploited.

- Nomad Bridge lost $191 million in 2022.
- Wormhole Bridge lost $320 million in 2022.

These incidents highlight the security challenges in the crypto industry.

Why crypto companies are targeted?

- The large sums of money they manage
- Cross-chain bridges are complex and prone to vulnerabilities due to the large codebase.
- Bridges lock assets on one chain while issuing an equivalent amount on another.
- Additionally, decentralized finance (DeFi) protocols often have slower response times.



Lessons learned

Strengthen Verification Mechanisms	• Validation of cryptographic proofs across all nodes to prevent vulnerabilities.
Implement Layered Security for Bridges	• Use multiple security checks for asset transfers to protect cross-chain bridges.
Improve Monitoring Systems	• Employ real-time monitoring and automated responses to detect and mitigate attacks early.
Establish Bug Bounty Programs	• Incentivize white-hat hackers to find and report vulnerabilities.

Tools we could use:

Secure Multi-Party Computation (SMPC)	To securely perform cryptographic operations without revealing private keys.
Decentralized Identity (DID) Frameworks	Ensure secure identities and credentials within the system using DID frameworks.
Blockchain Analytics Tools	Monitor transactions and detect suspicious activity using tools like **Chainalysis** and **Elliptic** .

References

Binance Blockchain Hit by $570 Million Hack, Exposing Crypto Vulnerabilities.

$570M Binance Hack: What Happened & Who Is Responsible?

Attack mints $569 million-worth of BNB tokens in BSC bridge exploit.

Immunefi. (2022, October 7). Hack Analysis: Binance Bridge October 2022. Medium.

Security News This Week: Binance Hackers Minted $569M in Crypto—Then It Got Complicated

Icons: Freepik

Thank You
Any Questions?