A Sybil attack occurs when a malicious actor creates multiple pseudonymous identities or nodes to gain control over a peer-to-peer (P2P) network.

Sybil attacks can undermine the integrity and security of blockchain networks and smart contracts.

This article explores the concept of Sybil attacks, examining their significance, consequences, and mitigation strategies.

What is a Sybil Attack?

A Sybil attack is a malicious act in which an attacker creates multiple fake identities or nodes to gain disproportionate influence or control over a network.

These identities, known as Sybil nodes

, are controlled by a single entity but appear as distinct entities in the network. By controlling a significant portion of the network's nodes, the attacker can manipulate transactions, disrupt communication, and undermine consensus mechanisms.

John R. Douceur coined the term in a research paper named"The Sybil Attack" in which he described using identity verification as a form of mitigation for Sybil attacks.

Types of Sybil Attack

- Direct Attacks:

involve one or more nodes impersonating multiple authentic nodes within the network. Genuine nodes unknowingly interact directly with these Sybil nodes, as they are unaware of their fraudulent nature.

- Indirect Attacks:

Sybil and normal nodes play a role in such attacks, but they have no direct interaction with each other. Instead, a Sybil node influences an intermediate node. This affected node then behaves maliciously, interacting with other nodes on behalf of the Sybil node, allowing the Sybil node to impact the network while remaining undetected.

Implications of Sybil Attacks

Sybil attacks pose a severe threat to the distributed nature of blockchain networks.

Blockchains rely on achieving consensus among nodes to validate transactions and maintain the ledger's integrity. However, malicious actors can skew the consensus process in their favor if they control many nodes.

This can lead to:

1. Network Fragmentation:

Network fragmentation occurs when communication between nodes in a blockchain network is disrupted or compromised.

In a Sybil attack, the attacker isolates nodes from the rest of the network, preventing them from participating in the consensus process or receiving valid transaction information.

This can lead to inconsistencies in the blockchain's state, as different network segments may have divergent views of the shared information.

1. Eclipse Attacks:

Eclipse attacks target individual nodes in a blockchain network, isolating them from the rest of the network and subjecting them to false or manipulated information.

This isolation prevents the node from accurately verifying transactions or participating in the consensus process.

In a Sybil attack, the attacker may create many Sybil nodes surrounding a targeted node, effectively eclipsing it from the rest of the network. Then, the attacker can feed the targeted node with false transaction information or manipulate its view of the blockchain's state.

1. 51% Attacks:

In a 51% attack, a malicious entity gains control of the majority of the network's mining power, as in Proof-of-Work (PoW), or stake, as in Proof-of-Stake (PoS), allowing it to manipulate transactions, block confirmations, and potentially reverse

transactions.

Sybil attacks can serve as a precursor to 51% attacks by enabling an attacker to amass a significant number of nodes, which can then be utilized to control a substantial portion of the network's resources. Once the attacker achieves majority control, they can execute a 51% attack.

The attacker with majority control can engage in several malicious activities, includingdouble spending, where they spend the same digital currency multiple times, blocking transactions from other participants, or reversing confirmed transactions.

Mitigating Sybil Attacks

- Sybil-Resistant Mechanisms & Economic Costs:

Sybil-resistant designs encompass various mechanisms to deter Sybil attacks within blockchain networks. These mechanisms impose economic costs

or other barriers on attackers and enhance the overall resilience of the network.

Examples include:a) PoW:

Participants are required to invest computational resources to solve computationally intensive puzzles, thereby creating significant economic barriers for potential attackers.b) PoS:

Participants must stake assets as collateral to validate transactions and secure the network, creating economic disincentives for malicious behavior.c) Proof-of-Unique-Identity:

Nodes are mandated to provide unique identifiers that cannot be easily replicated, ensuring the authenticity and uniqueness of participants within the network.

- [Byzantine Fault Tolerance (BFT)

](https://www.cyfrin.io/blog/understanding-double-spending-in-blockchain):

This mechanism ensures the network remains resilient even in the presence of malicious nodes attempting to subvert the consensus process, thereby bolstering the network's overall security.

- Reputation Systems and Social Trust Graphs:

Introducing reputation systems and leveraging social trust graphs can mitigate the influence of Sybil attackers by assessing node honesty and behavior over time. Reputation systems allow nodes to gain trust based on their historical behavior, with honest and reliable nodes accruing higher reputations. Meanwhile, social trust graphs analyze node connections in the blockchain network, employing methodologies such as sparsity-based metrics and user qualities to segment the network. The objective is to segment the network by identifying Sybil nodes while safeguarding honest ones from manipulation. While these mechanisms offer defense against Sybil attacks, they may remain vulnerable to small-scale infiltrations.

- Identity Verification:

Implementing identity verification mechanisms can mitigate Sybil attacks by ensuring each node represents a unique and identifiable entity.a) Direct Identity Validation:

a central authority validates the remote identities.

b) Indirect Identity Validation:

already-accepted identities vouch for the validity of the remote identity in question.

- Additionally, personhood validation, or Proof-of-Personhood (PoP)

goes beyond traditional identity verification by ensuring that each node represents a genuine person or entity. Advanced techniques such as biometric authentication or government-issued digital identities can be employed for robust personhood validation.

On-Chain Identity Verification and Sybil Resistance

On-chain identity solutions aim to address the challenge of Sybil attacks by providing a mechanism for authenticating and verifying the identity of participants on a blockchain network.

By integrating identity verification directly onto the blockchain, these systems enhance security, trust, and accountability, while mitigating the risk of malicious actors creating multiple fake identities to manipulate network consensus.

Some popular identity verification solutions include:

- [World ID

](https://worldcoin.org/world-id):

World ID is a universal proof of personhood. Designed to be a “human passport for the internet” leveraging decentralized identity verification. It uses a hardware biometric device called Orb to perform eye scans alongside zero-knowledge proofs for identity verification in a privacy-preserving manner. World ID establishes a verifiable and tamper-proof record of an individual's identity, reducing the likelihood of identity fraud or impersonation.To learn more about World ID, read the official WorldCoin whitepaper.

- [PolygonID

](https://polygonid.com/):

PolygonID, integrated within the Polygon blockchain network, provides users with a decentralized identity management solution. PolygonID uses verifiable credentials (VCs),

including KYC, proof of membership, government ID, and more - which can be claimed by users and accepted by verifiers.

- [Gitcoin Passport

](https://docs.passport.gitcoin.co/):

Gitcoin Passport extends identity verification functionalities to the Gitcoin platform, offering users a streamlined and secure way to authenticate their identities and participate in community-driven initiatives.Through Gitcoin Passport, users can establish a verified identity linked to their contributions and interactions within the GitHub ecosystem (e.g. followers, stars, GitHub OAuth, forks, etc), by earning verifiable credentials known as stamps

.The Passport

is a unique decentralized identifier (DID)

associated with an Ethereum address, stored on the Ceramic network. The DID can then be used to look up a user's Stamp

data, which is a collection of VCs.

- [Disco

](https://app.disco.xyz/):

Disco is a decentralized social verification protocol that enables users to verify their identities across various applications and platforms. Disco works in a similar way to Gitcoin, where the DID, known as the users’ backpack, serves as an alias for an Ethereum address (email, website or Bitcoin address, etc) and allows users to collect VCs associated with the backpack - which they can collect.

Sybil Attacks in Smart Contracts

Smart contracts are also vulnerable to Sybil attacks. In decentralized applications (dApps) relying on smart contracts, Sybil attacks can occur when attackers can perform an action multiple times which should be otherwise restricted (as with minting) or to gain a majority (as with governance tokens):

- DAOs and Governance:

DAOs usually rely on the share of governance tokens to dictate an individual's voting power. Suppose the smart contract issuing these governance tokens is susceptible to Sybil attacks. In that case, an attacker can gain a majority of the voting power by posing as multiple individuals in the DAO or gaining a majority of tokens. This is, in essence, a 51% attack.

- NFT Minting:

Some NFT mints restrict the number of NFTs an individual can mint. Examples include vouchers or tickets to an event. If these smart contracts are vulnerable to Sybil attacks, an attacker can mint multiple NFTs by posing as multiple distinct identities. This usually occurs when the contract restricts the number of mints for an individual address.

Attackers use a smart contract to deploy multiple smart contracts recursively. From within the child contract's constructor they:

1. Mint the NFT(s).
2. Send the NFT(s) to their wallet.
3. Self-destruct the child smart contract.

Since all execution is performed in the constructor, no bytecode is stored on-chain and the assembly call to check for bytecode (to prevent smart contracts from minting) will pass. The attacker will be able to exploit the system.

- Mitigation of Sybil Attacks in Minting - Off-Chain Signatures:

By using off-chain signatures, the smart-contract exploits above can be mitigated by requiring that users obtain an off-chain signature to mint. This is known as signature minting

. Refer to the following article formore information on ECDSA signatures.

Example Exploits: Sybil Attack

- [Adidas NFT drop

](https://twitter.com/Montana_Wong/status/1472023753865396227):

In 2021, Adidas released a collection of NFTs with GMoney, PUNKS comic, and Bored Ape Yacht Club. The NFT sale was limited to 2 per person (per wallet). However, an attacker was able to purchase 330 NFTs in a single transaction. They deployed a smart contract that generated 165 child smart contracts which each minted 2 NFTs from the Adidas smart contract before transferring the NFTs to their ETH address.

- [Verge

](https://news.bitcoin.com/privacy-coin-verge-third-51-attack-200-days-xvg-transactions-erased/):

In 2021, Verge network suffered more than 560,000 block reorganizations due to a 51% attack, making it one of the largest reorganizations in history.

- [TOR Attack:

](https://www.notion.so/What-are-Sybil-attacks-in-blockchain-and-smart-contracts-0653b2edd5d0468ca6dbba279f35ce61?pvs=21) In 2014 and 2020, the Tor network, a P2P private conversation network, was subject to a Sybil attack, compromising the personal data of their users.

Summary

Sybil attacks represent a significant threat to the integrity and security of blockchain networks and smart contracts.

Understanding their mechanisms and implications is crucial for devising effective mitigation strategies. By leveraging preventive measures, such as economic costs, reputation systems, and Sybil-resistant designs, blockchain ecosystems can enhance their resilience against such attacks.

Additionally, decentralized Proof-of-Personhood solutions offer promising avenues for bolstering security and trust within decentralized systems.

As Sybil attacks evolve and adapt, ongoing research and innovation are essential to safeguarding the integrity and decentralization of blockchain networks and smart contracts.

Getting your protocol audited significantly decreases the probability of an attack happening.

- To learn smart contract security and development, visit

[Cyfrin Updraft

](https://updraft.cyfrin.io/).

- To request a security review for your smart contract,

[reach out to us here

](https://cyfrin.typeform.com/to/yDUg5DK3?typeform-source=0dwqu1zc3qs.typeform.com).