Appendix A: Table of Blockchain Attack Lineage

Attack Name	Attack Type	Description	Parent(s)	Child(ren)
Private Key Retrieval Attack	Client Application / Wallet	An attacker compromises a wallet and retrieves the user's private keys.	Wallet Malware Attack; Impersonation Attack	
Wallet Malware Attack	Client Application / Wallet	An attacker exploits a user's wallet via malware.	Application Attack	Cryptojacking; Code Injection Attack; Ransomware Attack; Private Key Retrieval attack
Coding Flow	Client Application / Wallet	An attacker compromises a bug written into the wallet or smart contract.	Application Attack	Fake Deposit Exploit; Call to the Unknown; Source Code Vulnerability Exploit
Wallet Phishing Attack	Client Application / Wallet	An attacker steals a user's wallet credentials through social engineering means.	Application Attack	Deanonymization Attack; Coindash Attack; Cryptojacking
Ransomware Attack	Client Application / Wallet	An attacker exploits a user's wallet via ransomware.	Wallet Malware Attack	
Dictionary Attack	Client Application / Wallet	An attacker guesses a user's wallet password by brute-force.	Impersonation Attack	Credentials Reuse
Flawed Key Generation Exploit	Client Application / Wallet	The user's public/private key pair is generated improperly or with insecure characteristics.	Key Attack	
SQL Injection Attack	Client Application / Wallet	An attacker injects SQL to gain access to a user's wallet.	Code Injection Attack	
Wallet Availablility Attack	Client Application / Wallet	An attacker makes a user's wallet unavailable via a variety of means.	Application Attack	
Ballot Stuffing Attack	Client Application / Wallet	An eVoting application, based on blockchain, allows an attacker to cast more than one vote	Double Spend Attack	
Deanonymization Attack	Client Application / Wallet	An attacker links transactions to profile other users and then social engineer or extort them.	Wallet Phishing Attack	
Ether Stealing Attack	Client Application / Wallet	An attacker repeatedly calls the smart contract via the intermediate state and uses those calls to steal Ether.	Reentrancy Vulnerability Attack	
Identity Attack	Client Application / Wallet	An attack on a blockchain user's identity.		Impersonation Attack; DNS Attack
Application Attack	Client Application / Wallet	An attack on the application-layer of the blockchain, such as the wallet application.		Exchange Attack; Dynamic Libraries Attack; Domain Hijacking; Coding Flow Attack; Ether Delta Attack; Wallet Availability Attack; Wallet Phishing Attack; Wallet Malware Attack
Code Injection	Client Application / Wallet	An attacker injects code into a web application to gain access to a user's wallet.	Wallet Malware Attack	SQL Injection Attack
Credentials Reuse	Client Application / Wallet	An attacker reuses priorly-compromised passwords in a brute-force attempt to gain access to a user's wallet.	Dictionary Attack	
Domain Hijacking	Client Application / Wallet	An attacker manipulates the domain registration of the application website.	Application Attack	
Dynamic Libraries Attack	Client Application / Wallet	An attacker compromises the dynamically-linked libraries at runtime.	Application Attack	
Ether Delta Attack	Client Application / Wallet	An attacker replaces an entire cryptocurrency website with a vulnerable one to steal user credentials.	Application Attack	
Exchange Attack	Client Application / Wallet	Attacker compromise the wallet exchange website.	Application Attack	
Fake Deposit Exploit	Client Application / Wallet	An attacker exploits a bug that deposits fake cryptocurrency into a user's wallet.	Coding Flow Attack	
Impersonation Attack	Client Application / Wallet	An attacker impersonates a user in order to gain access to their wallet or the chain.	Identity Attack	Private Key Retrieval Attack; Posterior-Corruption Attack; Message Spoofing; Man in the Middle Attack; Dictionary Attack
RPC API Exploit	Client Application / Wallet	An attacker exploits the remote procedure call (RPC) API used within the smart contract.	Source Code Vulnerability Exploit	
Source Code Vulnerability Exploit	Client Application / Wallet	An attacker exploits a bug in the source code.	Coding Flow Attack	RPC API Exploit; Fault Injection
Majority Attack (51% Attack; Goldfinger)	Consensus Mechanism	Attackers control a group of miners that represents over half the consensus, allowing the attackers to control which blocks are added to the chain.	Consensus Protocol Attack	Accumulating Coin Age Attack; Alternative History Attack; Stake-Bleeding Attack; Attack From Afar; Uncle Block Attack
Double Spend Attack	Consensus Mechanism	An attacker spends a single unit of cryptocurrency more than once.	Consensus Protocol Attack	Large-Weight Attack; Ballot Stuffing Attack; Replay Attack; Multiple Withdrawal Attack; Prediction Attack; Bribery Attack; Finney Attack; Race Attack
Selfish Mining	Consensus Mechanism	An attacker mines blocks privately, without publishing them to the blockchain.	Consensus Protocol Attack	Stalker Attack; Stubborn Mining; Block Withholding Attack
Block Withholding Attack	Consensus Mechanism	An attacker does not publish mined blocks to raise the computing power required for the nodes to reach consensus.	Selfish Mining	Liveness Denial; Pool Block Withholding Attack; Selfholding Attack; Block Discarding Attack; Fork After Withholding Attack
Finney Attack	Consensus Mechanism	An attacker uses a pre-mined block in a transaction.	Double Spend Attack	Vector76 Attack
Fork After Witholding Attack	Consensus Mechanism	An attacker forks the mining pool after withholding the block, increasing the reward they receive.	Block Withholding Attack	Punitive & Feather Forking; Uncle Block Attack
Race Attack	Consensus Mechanism	An attacker sends a fraudulent transaction to a target pool and a legitimate transaction to another mining pool to see if the fraduluent transaction is accepted before the legitimate one.	Double Spend Attack	Vector76 Attack; Stale/Orphaned Block Attack
Bribery Attack	Consensus Mechanism	An attacker creates a legitimate transaction to get transaction confirmations, then creates a fradulent transaction and bribes the miners to use the fradulent branch.	Double Spend Attack	Whale Attack; P+Epsilon Attack
Long Range Attack	Consensus Mechanism	An attacker joins a Proof-of-Stake blockchain close to its creation to gain a higher stake and influence the chain at a later date.	Consensus Protocol Attack	
Pool Hopping Attack	Consensus Mechanism	A malicious miner hops across mining pools depending on their expected revenue, leaving honest miners with little computing resources.	Consensus Protocol Attack	Coin Hopping Attack
Vector 76 Attack	Consensus Mechanism	An attacker creates a large fraudulent transaction and a small legitimate transaction with the same currency, mines a block, and broadcasts both transactions at the same time.	Finney Attack; Race Attack	

Attack Name	Attack Type	Description	Parent(s)	Child(ren)
Nothing-At-Stake Attack	Consensus Mechanism	A malicious miner mines on every new branch after a fork on a Proof-of-Stake blockchain, guarranteeing a reward and controlling which branch wins.	Consensus Protocol Attack	
Alternative History Attack	Consensus Mechanism	Attackers control administrator nodes or greater than 50% of standard user nodes in the chain and either fork the chain back or rewrite chain history.	Majority Attack	
Block Discarding Attack	Consensus Mechanism	An attacker purposefully disposes of mined blocks instead of adding them to the chain.	Block Withholding Attack	
Grinding Attack	Consensus Mechanism	An attacker forces themselves to become the slot leader within a PoS chain, increasing how frequently they can make blocks.	Consensus Protocol Attack	
Splitting Attack	Consensus Mechanism	An attacker splits the mining power between groups of nodes with malicious intent.	Consensus Protocol Attack	
Stale/Orphaned Block Attack	Consensus Mechanism	An attacker forces blocks rejected due to race conditions into the chain.	Race Attack	
Stubborn Mining Attack	Consensus Mechanism	An attacker hides a chain of mined blocks.	Selfish Mining	
P+Epsilon Attack	Consensus Mechanism	Proof-of-Work consensus protocol blockchain attack in which an attacker offers a payout to other miners to gain an advantage, and then payout is not received.	Bribery Attack	
Punitive & Feather Forking	Consensus Mechanism	An attacker gives honest miners incentives to withhold their blocks and then extends a forked chain.	Fork After Withholding Attack	
Selfholding Attack	Consensus Mechanism	A two-part attack in which attackers attack an honest mining pool via BWA and also create a malicious pool for selfish mining.	Block Withholding Attack	
Stake-Bleeding Attack	Consensus Mechanism	Attackers who hold a large part of the pool, but not the majority, can slowly bleed the chain and gain control.	Majority Attack	Eclipse-Based Stake-Bleeding Attack
Accumulating Coin Age Attack	Consensus Mechanism	In blockchains that use coin age as network user share measurements, an attacker splits their coins and brings them back in, much older, to control the chain.	Majority Attack	
Attack From Afar	Consensus Mechanism	An attacker outside the chain, with enough computing power, attempts to build an alternative chain and insert it into the legitimate chain to create a new chain over which they have full control.	Majority Attack	
Black Bird Attack	Consensus Mechanism	An adversary creates a network of zombie nodes to gain the majority consensus of a network.	Uncle Block Attack	
Censorship Attack	Consensus Mechanism	A malicious node colludes with nodes in a Delegated Proof of Stake chain.	Consensus Protocol Attack	
Coin Hopping Attack	Consensus Mechanism	A malicious pool manager hops between pools to gain extra rewards.	Pool Hopping Attack	
Difficulty Raising Attack	Consensus Mechanism	A malicious miner raises the difficulty level in a Proof-of-Work chain to find the highest paying blocks and only mine those.	Consensus Protocol Attack	
Frontrunning Attack	Consensus Mechanism	An attacker adds a higher transaction fee than their peers to ensure their transaction is added to the chain first.	Whale Attack	
Large-Weight Attack	Consensus Mechanism	An attacker carries out a double spending attack to increase their weight and invalidate other transactions.	Double Spend Attack	
Pool Block Withholding Attack	Consensus Mechanism	An attacker withholds a generated block from a pool they have just entered to retain the new blocks it just discovered.	Block Withholding Attack	
Prediction Attack	Consensus Mechanism	An attacker privately builds a chain and attempts a double spending attack to overtake the correct chain.	Double Spend Attack	
Resource Exhaustion Attack	Consensus Mechanism	An attacker attempts to use all the resources outlined in the smart contract.	Consensus Protocol Attack	Fake-Stake Attack; Gas Limit Block Stuffing Attack
Stalker Attack	Consensus Mechanism	An attacker that uses seflish mining with the intention of preventing a specific node from putting blocks on the chain.	Selfish Mining	
Uncle Block Attack	Consensus Mechanism	An attacker compromises multiple pools and exploits the forking blocks, which it submits at the end of the round to gain multiple reward in a round.	Fork After Withholding Attack; Majority Attack	Balance Attack; Black Bird Attack
Whale Attack	Consensus Mechanism	An attacker motivates miners to mine on a forked chain by issuing transactions with higher fees that result in higher rewards.	Bribery Attack	Frontrunning Attack
Zero Spend Attack	Consensus Mechanism	An attacker adds a block to the chain without spending anything to do so.	Consensus Protcol Attack	
Consensus Protocol Attack	Consensus Mechanism	An attacker gains an mining advantage by manipulating the consensus protocol.		Resource Exhaustion Attack; Pool Hopping Attack; Nothing-At-Stake Attack; Grinding Attack; Zero Spend Attack; Long Range Attack; Difficulty Raising Attack; Double Spend Attack; Censorship Attack; Selfish Mining; Splitting Attack; Majority Attack
Key Attack	Off-Chain Application Logic	An attacker generates a symmetric key for authentication from their own device.	Cryptography Algorithm Attack	Flawed Key Generation Exploit
Quantum Attack	Off-Chain Application Logic	An attacker breaks the cryptography used on the chain using quantum computing.	Cryptography Algorithm Attack	
Cryptojacking	Off-Chain Application Logic	An attacker compromises a computer and uses it to mine cryptocurrency.	Wallet Phishing Attack; Wallet Malware Attack	
Refund Attack	Off-Chain Application Logic	An attacker manipulates a cryptocurrency payment policy to gain fraduluent refunds.		
Hashing Algorithm Attack	Off-Chain Application Logic	An attacker causes hash collisions or other hash manipulations to create invalid blocks.	Cryptography Algorithm Attack	Hash Collision Resistance Attack; Preimage Attack; Collusion Attack
Preimage Attack	Off-Chain Application Logic	An attacker uses the hash function and an output to find another output with the same hash.	Hashing Algorithm Attack	
Cryptography Algorithm Attack	Off-Chain Application Logic	An attacker exploits a cryptographic key vulnerability or a cryptographic hashing vulnerability.		Key Attack; Tradeoff Attack; Hashing Algorithm Attack; Quantum Attack; Rollback Vulnerability Exploit

Attack Name	Attack Type	Description	Parent(s)	Child(ren)
Coindash Attack	Off-Chain Application Logic	An attacker compromises a web page and changes wallet links to their wallet.	Wallet Phishing Attack	
Collusion Attack	Off-Chain Application Logic	An attacker uses similar hash values to gain secondary rewards.	Hashing Algorithm Attack	
Fake Receipt Attack	Off-Chain Application Logic	An attacker creates a fake transaction receipt.		
Fake Token Attack	Off-Chain Application Logic	An attacker creates a fake cryptocurrency token.		
Hash Collision Resistance Attack	Off-Chain Application Logic	An attacker tries to find two inputs to a hash function which result in the same output.	Hashing Algorithm Attack	
outsourcing attack	Off-Chain Application Logic	An attacker outsources their storage, granting themselves excess computing power.		
Overlay Network DoS	Off-Chain Application Logic	An attacker commits a Denial of Service attack on the abstracted overlay network.	DoS/DDoS Attack	
Posterior-Corruption Attack	Off-Chain Application Logic	An attacker uses an old node's signature to sign their blocks in a Proof-of-Stake chain.	Impersonation Attack	
Rollback Vulnerability Exploit	Off-Chain Application Logic	An attacker tries to roll back the cipher used within the cryptographic application.	Cryptography Algorithm Attack	
Tradeoff Attack	Off-Chain Application Logic	An attacker makes a tradeoff between time and memory in the favor of transaction data.	Cryptography Algorithm Attack	
Reentrancy Vulnerability Attack (DAO)	On-Chain Application Logic	An attacker exploits a smart contract fallback function that allows them to repeatedly recall a function and consume all available gas.	Call to the Unknown	Ether Stealing Attack
Timestamp Dependence Attack	On-Chain Application Logic	An attacker changes the block creation timestamp to gain a higher profit.	Transaction Ordering Dependence Exploit	Routing Attack; Timejacking; N-Confirmation Attack
Call to the Unknown	On-Chain Application Logic	An attacker forces the smart contract to invoke the fallback function because they called a function which doesn't exist.	Coding Flow Attack	Reentrancy Vulnerability Attack
Gasless Send Exploit	On-Chain Application Logic	An attacker forces a transaction to send without using any gas by invoking the out-of-gas exception	Excpetion Disorder Vulnerability Exploit	
Transaction Ordering Dependence Exploit	On-Chain Application Logic	An attacker exploits the fact that blocks are chained by timestamp.		Timestamp Dependence Attack
Overflow Attack (type casts)	On-Chain Application Logic	An attacker manipulates the type variable within the smart contract, forcing an overflow.	Exception Attack Vulnerability Exploit	
Vulnerable Multisig Exploit	On-Chain Application Logic	An attacker changes a centralized library contract owner wallet address to their own.	Changing System Parameters Attack	
Exception Disorder Vulnerability Exploit	On-Chain Application Logic	An attacker causes an exception within the smart contract to be handled improperly.	Design Flow Attack	False Top-Up Attack; King of the Ether Throne Attack; Gasless Spend Exploit; Overflow Attack
Stack Size Exploit	On-Chain Application Logic	An attacker manipulates the stack size on the smart contract to cause an overflow.	Design Flow Attack	
Delegate Function Exploit	On-Chain Application Logic	The attacker injects a call to the delegate function within the smart contract.	Design Flow Attack	
EVM Randomness Exploit	On-Chain Application Logic	An attacker manipulates the randomness within the virtual machine running the bytecode to cheat as a miner.		
Forcible Balance Transfer	On-Chain Application Logic	A smart contract vulnerability where an attacker can transfer balance and create failing transactions.	Design Flow Attack	
Immutable Bug Attack	On-Chain Application Logic	An attacker exploits a smart contract vulnerability that cannot be mitigated due to the immutable nature of the chain.	Design Flow Attack	Rubixi Attack
Keeping Secret Exploit	On-Chain Application Logic	An attacker exploits a private field within the smart contract.	Design Flow Attack	Governmental Attack; False Top-Up Attack
King of the Ether Throne Attack	On-Chain Application Logic	An attacker forces the smart contract to call the send command and not check for an exception when the call fails, causing an unsuccessful payment.	Exception Disorder Vulnerability Exploit	
Bad Mouthing Attack	On-Chain Application Logic	A malicious node lies about a transaction, affecting chain reputation.	Reputation Attack	
Block Size Attack	On-Chain Application Logic	A malicious administrator changes the number of transactions that can be included in a block to a very large/small number so that the blockchain is too long or the block never gets published.	Changing System Parameters Attack	
Blockchain Poisoning Attack	On-Chain Application Logic	Attacker attaches malicious files into a block and force nodes to download them.	Tampering Attack	
Changing System Parameters Attack	On-Chain Application Logic	An malicious administrator changes the system parameters within the smart contract.	Design Flow Attack	Block Size Attack; Vulnerable Multisig Exploit
Design Flow Attack	On-Chain Application Logic	An attacker exploits a bug in the design of the smart contract.		Forcible Balance Transfer; Fraud in Programming; Immutable Bug Attack; Self-Destruction Attack; Keeping Secret Exploit; Exception Disorder Vulnerability Exploit; Multiple Function Attack; Stack Size Exploit; Delegate Function Attack; Changing System Parameters Attack; Opcode Exploit
Fake-Stake Attack	On-Chain Application Logic	An attacker compromises a distributed ledger and wastes resources within a Proof-of-Stake chain.	Resource Exhaustion Attack	
False Top-Up Attack	On-Chain Application Logic	An attacker changes the status field within a transaction receipt and causes the transfer function to run without throwing an exception.	Keeping Secret Exploit; Exception Disorder Vulnerability Exploit	
Fault Injection	On-Chain Application Logic	An attacker modifies smart contract execution by sending it faulty transaction.	Source Code Vulnerability Exploit	
Fraud in Programming	On-Chain Application Logic	An attacker exploits bugs in a smart contract to remove intrinsic properties of a blockchain from the chain.	Design Flow Attack	
Gas Limit Block Stuffing Attack	On-Chain Application Logic	An attacker submits many transactions to purposefully fill up a smart contract's gas limit.	Resource Exhaustion Attack	
Generation Attack	On-Chain Application Logic	A malicious node reuses data to increase changes of being rewarded.	Tampering Attack	
Governmental Attack	On-Chain Application Logic	A an attacker overflows a smart contract due to an embedded vulnerability within the smart contract that cannot be mitigated.	Keeping Secret Exploit	
Multiple Function Attack	On-Chain Application Logic	An attacker exploits a bug in the smart contract with allows them to track a transaction without a transaction ID.	Design Flow Attack	

Attack Name	Attack Type	Description	Parent(s)	Child(ren)
Multiple Withdrawal Attack	On-Chain Application Logic	An attacker is able to make multiple withdrawals using the same currency.	Double Spend Attack	
On-Off Attack	On-Chain Application Logic	A malicious node behaves honestly, earns trust from other nodes, and makes a fraduluent transaction while creating a new block.	Reputation Attack	
Reputation Attack	On-Chain Application Logic	An attacker attempts to change their reputation and fool the other peers on the network.	Manipulation Attack	Bad Mouthing Attack; On-Off Attack; Whitewashing Attack
Rubixi Attack	On-Chain Application Logic	An attacker exploits a naming bug within a smart contract that allows them to assign themselves as owner of the contract.	Immutable Bug Attack	
Self-Destruction Attack	On-Chain Application Logic	An attacker utilizes the self-destruct method within a smart contract to send Ether to a desired address.	Design Flow Attack	
Tampering Attack	On-Chain Application Logic	An attacker tampers with a block's integrity.		Generation Attack; Blockchain Poisoning Attack
Whitewashing Attack	On-Chain Application Logic	A user with a bad reputation creates a new user with a neutral reputation that cannot be linked back to them.	Reputation Attack	
Eclipse Attack	P2P Network	An attacker targets a single node on the peer-to-peer network and blocks them from the chain, eclipsing their access.	Partitioning Attack	Eclipse-Based Stake-Bleeding Attack
Sybil Attack	P2P Network	An attacker creates and manages fraudulent nodes on the peer-to-peer network from which to launch attacks.	Delay Attack	
DoS/DDoS Attack	P2P Network	An attacker sends too many requests for the network to handle.	Routing Attack	DoS with Revert; Overlay Network DoS; Spam Attack
BGP Hijacking	P2P Network	An attacker exploits a BGP router to intercept network communication between a miner and the mining pool server.	Routing Attack	Partitioning Attack
Balance Attack	P2P Network	An attacker mines a majority of a branch on the chain before another branch, influencing consensus branch selection.	Uncle Block Attack	
Delay Attack	P2P Network	An attacker exploits the amount of time elapsed between hops during block publication broadcast messages.	Routing Attack	Sybil Attack; Batch Time Attack; Consensus Delay
Routing Attack	P2P Network	An attacker segments a node or nodes from the blockchain for a period of time.	Manipulation Attack; Timestamp Dependence Attack	BGP Hijacking; Delay Attack; Transaction Malleability; Triangle Attack; DoS/DDoS Attack
DNS Attack	P2P Network	An attacker exploits or corrupts DNS requests or the DNS cache to exploit a user's identity.	Identity Attack	
Timejacking Attack	P2P Network	An attacker uses an incorrect time and has their block inaccurately validated by other nodes on the network.	Timestamp Dependence Attack	
Liveness Denial	P2P Network	An attacker delays the transaction confirmation by privately holding onto the block, allowing them to build a private chain separate from the public chain.	Block Withholding Attack	
Dust Attack	P2P Network	An attacker creates many small transactions to congest the network.	Spam Attack	
Partitioning Attack (Node Isolation)	P2P Network	An attacker partitions the P2P network to isolate a group of nodes and intercept their network traffic.	Manipulation Attack; BGP Hijacking	Eclipse Attack; Boycott Attack; Certificate Authority Attack; Attack on Shards; Attack of the Clones
Certificate Authority Attack	P2P Network	An attacker exploits a third-party Certificate Authority or the root Certificate Authority.	Partitioning Attack	Blacklisting Attack
Incorrect Transaction Attack	P2P Network	An attacker manipulates the P2P network into verifying an incorrect transaction.	Manipulation Attack	Short Address Attack
Spam Attack	P2P Network	An attacker spams the network with transactions to congest the network	DoS/DDoS Attack	Dust Attack
Man in the Middle Attack	P2P Network	An attacker sits in-between two nodes to disrupt their conversation and impersonate one of the nodes.	Impersonation Attack	Packet Sniffing
Manipulation Attack	P2P Network	Attacks in which an attacker can manipulate network participants or network availability		Misleading Attack; Reputation Attack; Incorrect Transaction Attack; Partitioning Attack; Routing Attack
Packet Sniffing	P2P Network	An attacker sits in-between two nodes to collect their network traffic.	Man in the Middle Attack	
Triangle Attack	P2P Network	A malicious node withholds transaction advertisements and block broadcasts from fellow nodes.	Routing Attack	
Attack of the Clones	P2P Network	An attacker clones a private key to convince honest nodes that a transaction is valid, before erasing the transaction.	Partitioning Attack	
Attack on Shards	P2P Network	An attacker compromises the consensus nodes in a subgroup of the chain.	Partitioning Attack	
Batch Time Attack	P2P Network	A malicious node increases the time between receiving a transaction and creating a block.	Delay Attack	
Blacklisting Attack	P2P Network	An adversary revokes a certificate to force nodes to lose access to the network.	Boycott Attack; Certificate Authority Attack	
Boycott Attack	P2P Network	A malicious MSP denies one node new certificates while granting another node new participants.	Partitioning Attack	Blacklisting Attack
Consensus Delay	P2P Network	An attacker delays nodes from reaching consensus by attempting to inject fradulent blocks into the chain.	Delay Attack	
Message Spoofing Attack	P2P Network	An attacker spoofs a transaction source or destination address.	Impersonation Attack	
Misleading Attack	P2P Network	An attacker misleads some of the network computing power to gain an advantage over the network.	Manipulation Attack	
N-Confirmation Attack	P2P Network	An attacker uses the confirmation timestamp on a block to exploit the P2P network.	Timestamp Dependence Attack	
Transaction Malleability	VM/Language	An attacker modifies a transaction between transaction creation and block creation.	Routing Attack	

Attack Name	Attack Type	Description	Parent(s)	Child(ren)
Replay Attack	VM/Language	An attacker replays a transaction already accepted by the consensus network.	Double Spend Attack	
Short Address Attack	VM/Language	An attacker grants themself many more tokens than they purchased by exploiting a token-creating bug.	Incorrect Transaction Attack	
DoS with Revert	VM/Language	An attacker increases the number of addresses that need refunds in the smart contract, exhausting all available gas.	DoS/DDoS Attack	
Opcode Exploit	VM/Language	An attacker compromises the opcode used to interpret the smart contract virutal machine's bytecode.	Design Flow Attack	