itworldcanada.com

Understanding Cybersecurity Management in DeFi (UCM-DeFi) – Blockchain Security (Article 4) - IT World Canada

Sepideh HajiHosseinKhani and Arash Habibi Lashkari

22-28 minutes

In today's digital landscape, blockchain technology has emerged as a powerful force, revolutionizing sectors like healthcare, finance, government, and commerce with its unparalleled security features. However, as with any technological advancement, it has not been immune to the cunning tactics of cybercriminals. The very features that make blockchain robust can also attract malicious actors who seek to exploit its vulnerabilities.

Understanding Cybersecurity Management in DeFi (UCM-DeFi), a five-article series, aims to discuss decentralized finance and explore a range of cybersecurity issues that impact DeFi and blockchain-based financial solutions. The articles in this series are based on the recent book titled *Understanding Cybersecurity Management for DeFi*, published by Springer this year. This fourth article aims to illuminate the various blockchain attacks and the respective countermeasures implemented to avoid or mitigate such attacks. Even though a foolproof cybersecurity solution is

currently unattainable, the countermeasures discussed herein strive to reduce the impact of attacks on blockchain technology.

The previous three articles in this series are available here:

Understanding Cybersecurity Management in DeFi (UCM-DeFi) – The Origin of Modern Decentralized Finance (Article 1)

Understanding Cybersecurity Management in DeFi (UCM-DeFi) – Introduction to Smart Contracts and DeFi (Article 2)

Understanding Cybersecurity Management in DeFi (UCM-DeFi) – DeFi Platforms (Article 3)

Contents

22 Blockchain Attacks and Their Countermeasures

Let's delve into 22 prominent and relevant blockchain attacks and explore their countermeasures to improve the security and resilience of these distributed systems.

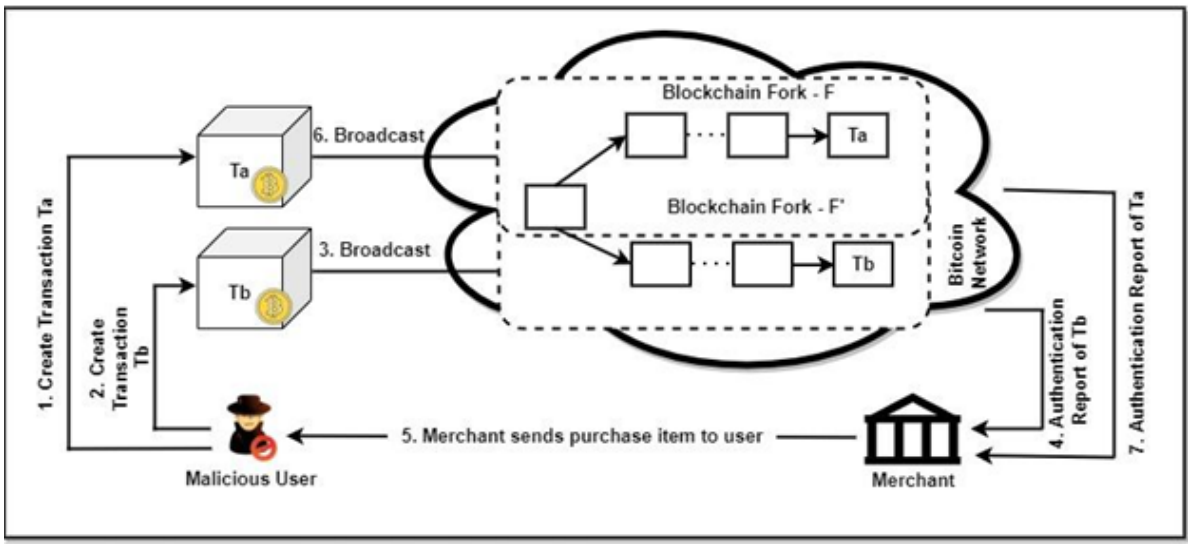
1. The Double-Spending Attack

One example of a cyber-attack that targets blockchain is the double-spending attack. This attack leverages the fact that digital money can potentially be duplicated and rebroadcasted. It's a sophisticated, five-stage process that ultimately allows the attacker to spend their already-spent money again, causing significant financial losses.

To counter this attack, an innovative solution involves preventing the removal of existing blocks to add new ones. By retaining previous transaction information, each newly added block in the blockchain preserves the entire transaction history. This ensures the permanent recording of transactions and thus helps prevent double-spending attacks.

2. The Finney Attack

The Finney Attack is a double spending attack that can occur when an individual accepts an unconfirmed transaction on the network. The attacker, who is also a miner, creates a block that includes a transaction between two addresses owned by them. Then, without broadcasting this block to the Bitcoin network, the attacker performs another transaction with the same coins.



The recipient, who accepts the transaction without confirmation, gets duped when the attacker releases the previously mined block to the network, which invalidates the recipient's transaction and enables double-spending.

The success of a Finney Attack depends on three main factors:

- The precise timing of the attack

- The acceptance of unconfirmed transactions
- The miner's hash power is also critical, with a lower hash power reducing the chances of a successful attack.

  Countermeasures to prevent this attack include waiting for multiple transactions to confirm on the Bitcoin network before considering a transaction safe and irreversible. This enables the recipient to validate a block and transaction, ensuring it cannot be reversed mid-processing and paving the way for the attack.

3. The Race Attack

The Race Attack is a form of blockchain attack where two transactions are broadcast around the same time, creating a race condition. The attacker sends a payment to a recipient while simultaneously broadcasting a conflicting transaction to their own account. If the vendor accepts the payment before the transaction is confirmed, they are at risk as the second transaction may be confirmed, mined, and accepted by the network first, effectively reversing the initial transaction.

The Race Attack does not require highly skilled attackers and tends to have a higher success rate. Its consequences can include loss of product for vendors, potential banning of genuine users, and the creation of new blockchain forks.

To counteract this attack, it's suggested that vendors disable incoming connections, selecting only outgoing ones. Additionally, the network can insert observers who are capable of rapidly communicating double spending alerts among peers.

4. The Brute Force Attack

The Brute Force or Alternative History Attack is a form of blockchain attack that aims to modify the entire history of the blockchain, including the genesis block. The attacker controls certain nodes in the Bitcoin network, which collaboratively mine blocks privately with the intention of double-spending.

In this attack, the adversary includes a double-spending transaction in a block while simultaneously expanding their private chain. If a merchant waits for ‘x’ validations before accepting a transaction, the attacker can mine ‘x’ blocks privately and broadcast them to the network, creating a longer chain than originally anticipated. This leads to a successful double-spending attack.

To mitigate this type of attack, one of the recommended countermeasures is to place observers within the network. These observers can detect malicious activities and alert merchants about potential double-spending.

5. The Vector 76 Attack

Vector 76, or One-confirmation Attack, is a double spending attack within the Bitcoin exchange network, utilizing privately mined blocks. The attacker holds a previously mined block, including a deposit transaction, and waits for the broadcast of a subsequent block. The attacker then sends both the old and new blocks to the Bitcoin exchange or to neighboring peers.

The attacker then quickly transmits another transaction, requesting the withdrawal of the same bitcoins used in the preceding transaction. If the other chain does not include the transaction used for the credit, the credit is canceled. However, the attacker

has already withdrawn the payment, resulting in a loss of bitcoins.

Countermeasures against this attack include not accepting transactions with only a single confirmation (with at least two, preferably six confirmations recommended), disabling inbound connections on the node, and monitoring and allowing outgoing node connections only to well-known nodes. These measures help prevent false information injection and sharing of state information with unwanted nodes.

6. The Balance Attack

The Balance Attack is a disruption strategy used against a Proof of Work (PoW) blockchain. It allows a node with low mining power to cause short-term disruption among similar power sub-groups. The attacker abstracts the blockchain into a directed acyclic graph, introducing delays in one sub-group while issuing and mining transactions in another. This attack enables double-spending by targeting a merchant in the sub-group and reusing the same coins for multiple transactions.

To mitigate a Balance Attack, measures should be put in place to prevent miners from mining on blocks with a higher balance in the network. This helps ensure that the blockchain remains secure and maintains its integrity.

7. Nothing at Stake Attack

The Nothing at Stake Attack, based on the Proof of Stake (PoS) consensus protocol, allows attackers to generate conflicting blocks on all potential forks, creating blockchain inefficiencies and vulnerabilities. This attack takes advantage of PoS's fork resolution

algorithm, generating multiple fork blocks and facilitating transparent forging, a method that predicts future valid block creators.

To combat these attacks, measures like reward mechanisms for honest validators and locked deposits have been proposed. The former deters opportunistic adversaries, while the latter enables the identification and punishment of dishonest validators, creating conflicting blocks. However, these countermeasures aren't foolproof against targeted attacks.

8. Selfish Mining Attack

The Selfish Mining or Block Withholding Attack is a strategy that centralizes Bitcoin mining operations to increase profits. Selfish miners create private blockchains, encouraging miners to work on futile blocks instead of achieving block rewards. As their private chain grows, they inject their blocks into the public chain, causing a protocol divergence, or fork, allowing them control over the honest blockchain's configurations.

To counter such attacks, methods like timestamp-based techniques, the DECOR+ protocol favoring fresh blocks, and the ZeroBlock technique are recommended. These strategies aim to maintain the integrity and decentralization of the blockchain.

9. Long-Range Attack

Long-range attacks involve an attacker who forks the blockchain from the genesis block, creating a new blockchain branch with a history differing from the main one. The goal is to have this new branch surpass the length of the original blockchain.

There are three types of long-range attacks: simple, posterior corruption, and stake bleeding.

1. **Simple Long-range Attack** – Nodes don't check block timestamps, allowing a malicious validator to forge timestamps and grow the new chain faster than the main one.
2. **Posterior Corruption Attack** – The attacker, unable to forge timestamps, aims to generate more blocks than the main chain. This often involves stealing or buying the private keys of retired validators to generate more blocks.
3. **Stake Bleeding Attack** – The attacker creates a forked blockchain and lets his stake on the main chain decrease by skipping his turn as slot leader. Simultaneously, he works as the only validator in the new chain, increasing his stake there.

   In all cases, the attacker aims to outpace the main blockchain by manipulating the blockchain's consensus protocol.

   For long-range attacks, one countermeasure is to enforce stricter timestamp validation rules to prevent validators from forging timestamps, as in the simple long-range attack.

   Another countermeasure is to properly safeguard the private keys of validators, even those that are retired, to prevent them from being exploited as in the posterior corruption attack. This could involve secure storage mechanisms, strict access control, or cryptographic key destruction upon retirement.

10. Block Withholding (BWH) Attack

In a Block Withholding (BWH) attack, rogue miners aim to increase their incentives by decreasing the winning chances of other

miners. They do this within the Bitcoin network's mining pool, where multiple miners join forces to combine their computational power.

Each miner in the pool must provide proof of work (PoW) to the pool administrator, demonstrating their efforts toward solving the PoW associated with a Bitcoin block. This PoW is less complex than solving the one related to the Bitcoin block and is known as partial proof of work (PPoW). PPoWs serve two purposes:

1. They confirm that the miner is expending their computational power to solve the Bitcoin system's PoW.
2. The computation of PPoWs represents valid work towards solving the Bitcoin PoW and is not a waste of the pool's computational power.

However, rogue miners launch a BWH attack by only sharing those PPoWs with the pool administrator that aren't full proofs, concealing all fully computed proofs. Unaware of the withheld blocks, the pool administrator shares their revenue with these rogue miners, as they would with honest miners, under the mistaken impression that the rogue miners are genuinely contributing to solving the PoW problem.

One countermeasure against this attack involves using honeypots to distract rogue miners, involving them in fake resources to protect the pool's computational power from their malicious activities. This solution, however, is not entirely effective.

11. Fork After Withholding (FAW) Attack

The Fork After Withholding (FAW) attack is an evolution of the Block Withholding (BWH) attack. In a FAW attack, rogue miners

unfairly gain additional rewards by intentionally generating a fork after executing a BWH attack. The rewards earned by a FAW attacker always exceed or equal those of a BWH attacker as they generate new forks, repeating their malicious activities to gain more incentives. This attack becomes more potent when two mining pools attack each other, allowing malicious attackers to exploit the situation for more substantial rewards. In such scenarios, larger pools tend to win consistently.

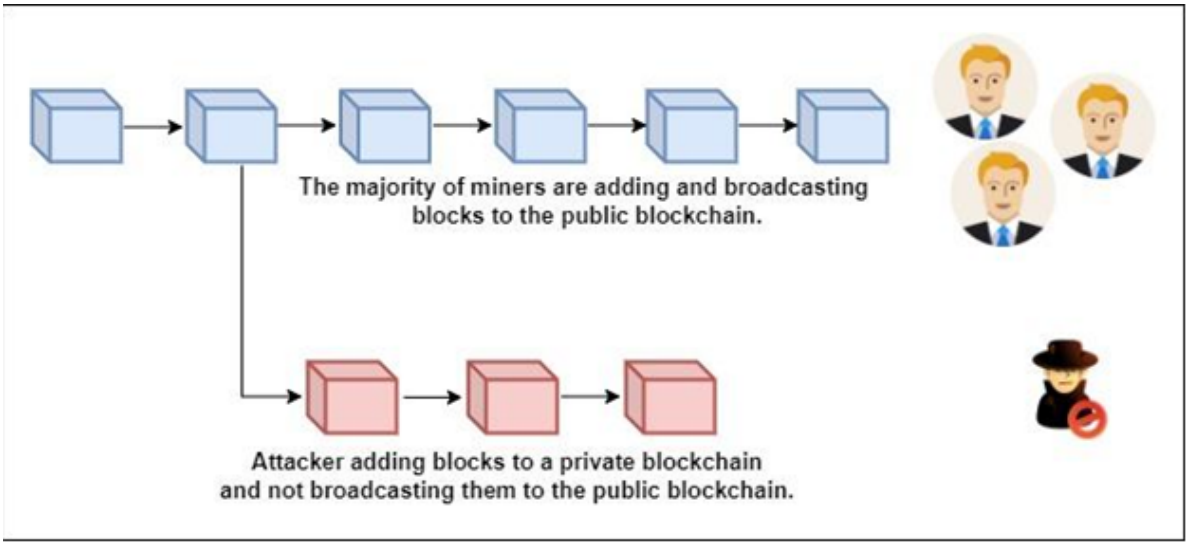
While there are some potential countermeasures, complete defense against FAW attacks remains an open problem. One strategy involves the use of backward compatibility, monitoring miners who have not updated their hardware to keep track of the computational power used. Another potential countermeasure is the use of beacon values that are updated frequently. These values award points to partial proofs of work only if they include the recent beacon value, aiding in the detection of infiltrations.

12. 51% Attack

One of the most well-known attacks within a blockchain environment is the 51% attack. In this attack, a group of miners gains control over more than 50% of the network's mining hash rate or computational power. This level of control allows the attackers to halt new transactions from being confirmed, disrupting the flow of transactions between merchants and clients.

For the attack to be successful, attackers must complete the proof of work (PoW) challenge faster than honest miners. The more computational power the attackers possess, the faster they can execute the attack. A successful 51% attack can be used to

reverse transactions and double-spend coins multiple times if the malicious miners control more than half of the mining network. The figure below showcases a depiction of a 51% attack.



To protect against this attack, observers can be placed within the network who can detect and report any instances of double spending occurring within the network. These activities can be reported to peers and used to discourage the formation of large mining pools. However, prevention and mitigation of 51% attacks remain significant challenges due to the inherent design of blockchain networks.

13. Feather and Punitive Forking Attack

Punitive forking is an attack where malicious miners refuse transactions from blacklisted addresses. This can occur with less than 50% of the network's hash power. If successful, this attack gives other miners an opportunity to gain incentives by supporting the blacklist. Essentially, punitive forking prevents certain Bitcoin addresses from using their bitcoins and requires the attacker to control the majority of hash power.

Feather forking is a modified version of punitive forking, where

blacklisting is temporary. While these attacks present a risk in terms of blacklisting, they are hard to execute since attackers often cannot gain majority hash power. Feather forking can be executed even without majority hash power by announcing temporary blacklisting of certain blocks and forking the blockchain for a limited number of blocks.

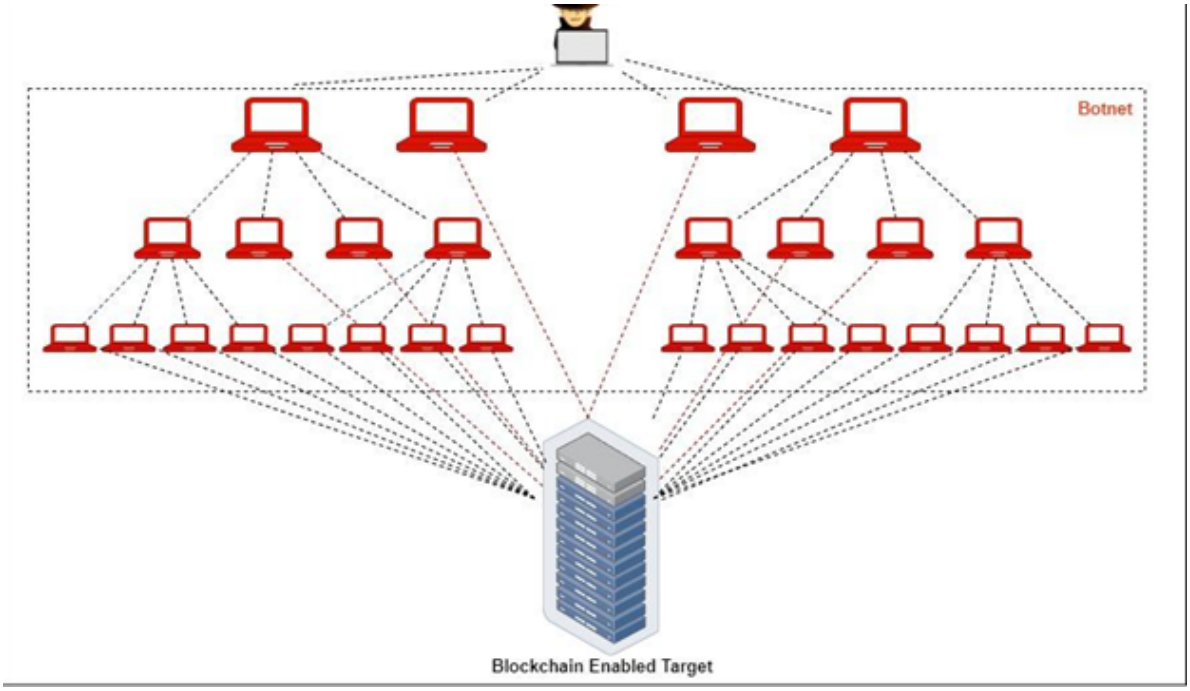
14. Eclipse Attack

In an eclipse attack, the attacker isolates a user from the network, obscuring their view of the blockchain to prepare for further attacks. By exploiting a node's limited connections due to bandwidth constraints, the attacker floods the target node with IP addresses, waiting for it to reconnect with a malicious host. This compromised node is then fed false data and can be used to disrupt the honest miner's computing power and potentially launch a 51% attack.

Countermeasures include blocking incoming connections and connecting only with trusted nodes.

15. DDoS Attack

In a distributed denial of service (DDoS) attack, multiple attackers simultaneously disrupt network tasks within the Bitcoin network, targeting currency exchanges, mining pools, eWallets, and other Bitcoin financial services. Attackers create a botnet from compromised machines to flood the network with requests, overloading honest miners and causing them to discard genuine user requests, thereby increasing the attacker's incentives and computing power.



Mitigation strategies for DDoS attacks include continuous monitoring of network traffic, employing machine learning techniques for classifying malicious traffic, and configuring the network to restrict or block malicious packets. Implementing a third-party DoS protection scheme is also recommended.

16. Liveness Denial Attack

A liveness denial attack is a form of DDoS attack specific to Proof of Stake (PoS) protocols. In this attack, validators halt the blockchain by refusing to publish new blocks, thereby preventing transactions from being confirmed. This doesn't compromise the Bitcoin network directly, but it does disrupt its operation. If the validators cannot be verified as "live," the community often opts to fork the blockchain to remove inactive validators. However, the validators initiating this attack risk their position and stake within the network.

The most effective countermeasures to liveness denial attacks are the inherent features of blockchain technology, like

decentralization and consensus mechanisms, which are also useful in mitigating DDoS attacks.

17. Refund Attack

In a refund attack, a customer wrongfully sends payments through a trusted merchant to a rogue trader, then denies the transaction. Current refund policies, such as Coinbase and BitPay, are vulnerable because they accept refund addresses via email. The refund address isn't protected, even with HTTPS communication, leading to possible misuse. While HTTPS was suggested as a solution, it only offers one-way authentication and can open the door to another attack, enabling the theft of co-signer's Bitcoins.

18. Tampering or Delay Attack

A tampering or delay attack exploits scalability measures in the Bitcoin network to delay message deliveries. In this attack, the adversary, acting as a full Bitcoin node, temporarily blocks the delivery of a specific node's message. If the adversary can advertise an object to the target node first, the node will refrain from requesting the object from others. Moreover, the target node should wait a substantial time before requesting from another peer.

The delay attack can be mitigated through dynamic timeouts and updating block advertisements. Dynamic timeouts account for heterogeneity in the Bitcoin network, as opposed to using static timeouts, which assume homogeneity. Furthermore, bitcoin nodes should monitor block advertisements to preempt any delay tactics.

19. BGP Hijacking or Routing Attack

Routing attacks exploit the fact that Bitcoin connections are transmitted over the Internet in plain text without integrity checks. These attacks, such as BGP (Border Gateway Protocol) hijacking, can eavesdrop, drop, modify, inject, or delay Bitcoin messages such as blocks or transactions.

In a BGP hijacking attack, the attacker aligns his route with a legitimate one, attracting all traffic destined for a specific node. There are two main ways to launch routing attacks: partitioning the Bitcoin network or slowing down the network. In partitioning, the adversary isolates a set of nodes, while in slowing down, the attacker delays the propagation of new blocks to certain nodes.

Countermeasures include short-term tactics like increasing node connection diversity, monitoring routing paths and statistics, and regularly refreshing connections. Long-term solutions include encrypting Bitcoin communications, using distinct control and data channels, and requesting a block on multiple connections.

20. Sybil Attack

A Sybil attack is when a hostile entity creates many fake identities to deceive a network system and undermine its trust and redundancy mechanisms. This type of attack poses a significant threat to peer-to-peer network systems, including the Bitcoin network, particularly the PoW and PoS blockchain systems.

In the Bitcoin context, a Sybil attack supports double-spending attacks by increasing the propagation delay of correct block information across the network. Fake nodes used in this attack have no computational power. Similar to the double-spending attack, a separate chain is forked, running in parallel to the main

chain. The attacker uses Sybil nodes to slow down the growth rate of the main chain.

A simple countermeasure to prevent a Sybil attack is the use of identity-based mechanisms, which restrict malicious users' access to the system.

21. Timejacking

In a timejacking attack, an adversary alters the system time of a node, replacing its dependency on network time with a hardware-based system time. This kind of attack can potentially divide the network into several sections, isolating the targeted node from the rest of the network.

To counter timejacking attacks, several measures can be taken. These include using the system time instead of network time to establish the upper limit of block timestamps, shortening the acceptable time ranges, relying only on trusted peers, and designing a node to store multiple timestamps to prevent complete alteration by an attacker. Furthermore, node timestamps can be made to depend on the blockchain timestamps.

22. Quantum Attacks

Quantum computers, potentially the most powerful future computers, could break nearly all encryptions currently safeguarding the Bitcoin network. Around a quarter of circulating Bitcoins today are susceptible to quantum attacks. Cryptography, the technique widely employed, uses public-private key pairs to encrypt sensitive data and create a hash to protect it from adversaries.

Quantum computers, known for their extraordinary computing capabilities, can perform calculations at unprecedented speed. Some quantum attacks target stored data, while others target data in transit. The decentralized nature and governance structure of blockchain makes it uniquely challenging for quantum-safe cryptography.

Cryptocurrencies are particularly vulnerable to quantum attacks in the future. One key advantage of quantum computing is its computational speed in performing the hash of a Proof-of-Work (PoW) used by Bitcoin, achieving the same computations as a classical computer in a quarter of the time.

Final Thoughts

This examination of 22 key blockchain attacks underscores the multifaceted threats posed to these networks. From Double Spending to Quantum Attacks, each assault presents unique challenges to the integrity of blockchain systems. However, identifying their strategies and implementing appropriate countermeasures can significantly enhance the resilience and security of these networks.

Despite the risks, blockchain technology continues to hold immense potential, and by maintaining a proactive and vigilant approach to cybersecurity, we can leverage its transformative capabilities while mitigating potential vulnerabilities.

What’s next

This article investigates 22 popular Blockchain attacks and their countermeasures. The next article of the series, “Understanding

Cybersecurity Management in DeFi: Smart Contracts and DeFi Security and Threats," puts forward some important vulnerabilities and threats in smart contracts that pose major challenges for smart contract designers.