Bitcoin Threat Model

In this document, we use ABC [5] to build a threat model for Bitcoin.

System Description. Bitcoin is a virtual currency that utilizes basic cryptographic primitives, a proof-of-work based mining process, a consensus protocol, and a permissionless peer-to-peer network to provide a decentralized currency exchange medium. Participants are known by their Bitcoin addresses and classified into two categories: miners and clients. Miners are responsible of maintaining and extending the blockchain, while clients use the payment service and keep track of their transactions. The network model of Bitcoin is depicted in Figure 1. As shown, clients announce new transactions to the network, which are validated by the miners and added to the blockchain. Miners are motivated to do that in order to collect the mining rewards and the transaction fees of the new blocks they mine.

The network agrees on the current state of the blockchain through a consensus protocol with the core concept of adopting the longest branch. Miners run a network protocol that defines how to connect to other peers, process transactions, validate and mine blocks. Lastly, the security of the system holds under the assumption that the majority of the mining power is honest.

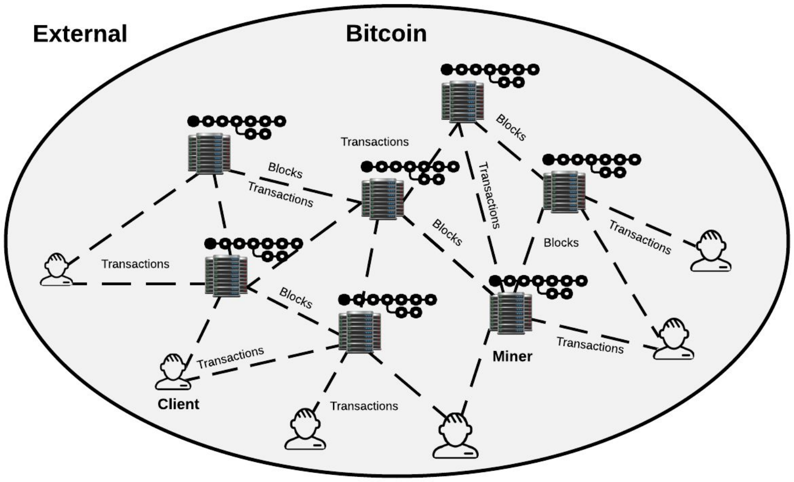


Figure 1: Bitcoin network model.

Participants. Miners and clients.

Assumptions. Bitcoin makes the following set of assumptions:

- Asynchronous communication network.

- The majority of the mining power is honest.

Assets. The currency exchange medium assets, namely, the blockchain, transactions, the currency, and the communication network.

Threat categories identification. By mapping the assets of Bitcoin to the ABC threat categories (see Table 1 in [5]), we find that the following threats need to be investigated:

- **Currency asset related threats:** Currency theft.
- **Blockchain asset related threats:** Inconsistency, invalid block adoption.
- **Transaction asset related threats:** Deanonymization.
- **Communication network asset related threats:** Denial of service.

Note that in Bitcoin all transactions must be signed. This rules out the tampering and repudiation threats of the transaction asset. In addition, the use of proof-of-work for mining rules out the biased mining threat. We elaborate more on these points under the discussion of the currency theft threat. Moreover, the chain freezing threat to the blockchain is discussed as part of the DoS attack against the communication network.

Threat scenario enumeration and reduction. We construct five collusion matrices, one for each threat, and enumerate/reduce all possible threat scenarios. This involves crossing out the unlikely-to-happen threat cases and merging the ones that have identical effect.

In these matrices, the cells that are in black represent the ruled out cases while the cells in pink represent the merged ones. Inside these cells the rationale behind the omission or merging is outlined. Cells that contain right arrow and a comma-separated threat numbers indicate that colluding attackers do not become stronger than when acting individually. Each one may attack the system on its own and perform the attack(s) it is capable of from the comma-separated list.

We split the roles of the parties in the threat model. An external party, for example, can join the system as a client/miner and perform any of their activities. Same for clients/miners, they can perform any attack strategy an external is capable of. However, we do not repeat the same strategy for each one, but instead list it only once.

1) *Currency theft threat*

An attacker may pursue a currency theft threat by performing any of the following strategies:

1. An attacker forges valid transactions that spend other's currency.
2. An attacker tampers transactions issued in the system to make itself the destination of the currency transfer.

3. A miner pretends to be the owner of a newly mined block to collect the mining rewards.
4. An attacker double spends its currency.
5. An attacker spoofs parties in the system so the source, voluntarily, sends funds to this attacker instead of the legitimate destination, e.g., fake donations.

As mentioned previously, in Bitcoin all transactions must be signed as a proof that the sender owns the private key that spends the input currency. Under the assumption that the used digital signature scheme and hash function are secure, an efficient attacker has negligible probability to succeed in forging correct transactions or generate correct signatures for tampered ones. In addition, the transactions' malleability vulnerability in Bitcoin has been fixed [1, 2]. Hence, tampering a single bit in a transaction invalidates its signature. As a result, the first and second strategies are ruled out.

In addition, under the assumption that the hash functions used are secure, an attacker succeeds in performing the third strategy with negligible probability. This is due to the fact that a block is accepted by honest miners if it is valid, i.e. includes valid transactions, and if the hash of its header along with the announced nonce value is less than the network difficulty. Changing the coinbase transaction that defines the block owner leads to changing the header of the block, which in turn changes its hash. Hence, the attacker needs to edit the block in a way that produces the same hash value that meets the network difficulty. This means finding a hash collision which is ruled out under the security of hash functions. Or this attacker must find a new nonce value that solves the proof-of-work puzzle, which is reduced to the case of working in an honest way to mine blocks on the blockchain. Thus, the third strategy of the currency theft threat is ruled out.

The collusion matrix of the currency theft threat is found in Figure 2. Analysing this matrix leads to the following threat cases (listed as tuples of threat type, attacker, and target):

- **Threat 1 (Currency theft, attacker is client, target is client):** An attacker client double spends its currency, hence, he steals promised payments from someone's else.
- **Threat 2 (Currency theft, attacker is client, target is client):** An attacker spoofs other parties in the system to claim being the legitimate destination of a currency transfer.

Target → Attacker ↡	*Client*	*Miner*	*Client and Miner*
Client	**(1)** double spending. **(2)** spoofing other parties in the system to become the destination of fund transfer.	**Reduced to the case of attacking a client, miners are viewed as clients when they transact with their currency.**	
Client and Miner	**→ (1), (2)** **Colluding with miners makes double spending easier.**		
External	**Reduced to the case of an attacker client, miners/externals are viewed as clients when they transact with their currency.**		
Client and External			
Miner			
Miner and External			
Client, Miner, and External	**Reduced to the case of an attacker client colluding with miners.**		

Figure 2: Currency theft threat collusion matrix.

2) *Blockchain inconsistency threat*

We consider all strategies that may cause the blockchain to be inconsistent across miners either instantly or in the future. In other words, an attacker's actions may either make miners hold inconsistent copies of the blockchain now, or later on once the differing blocks are confirmed. These strategies include the following:

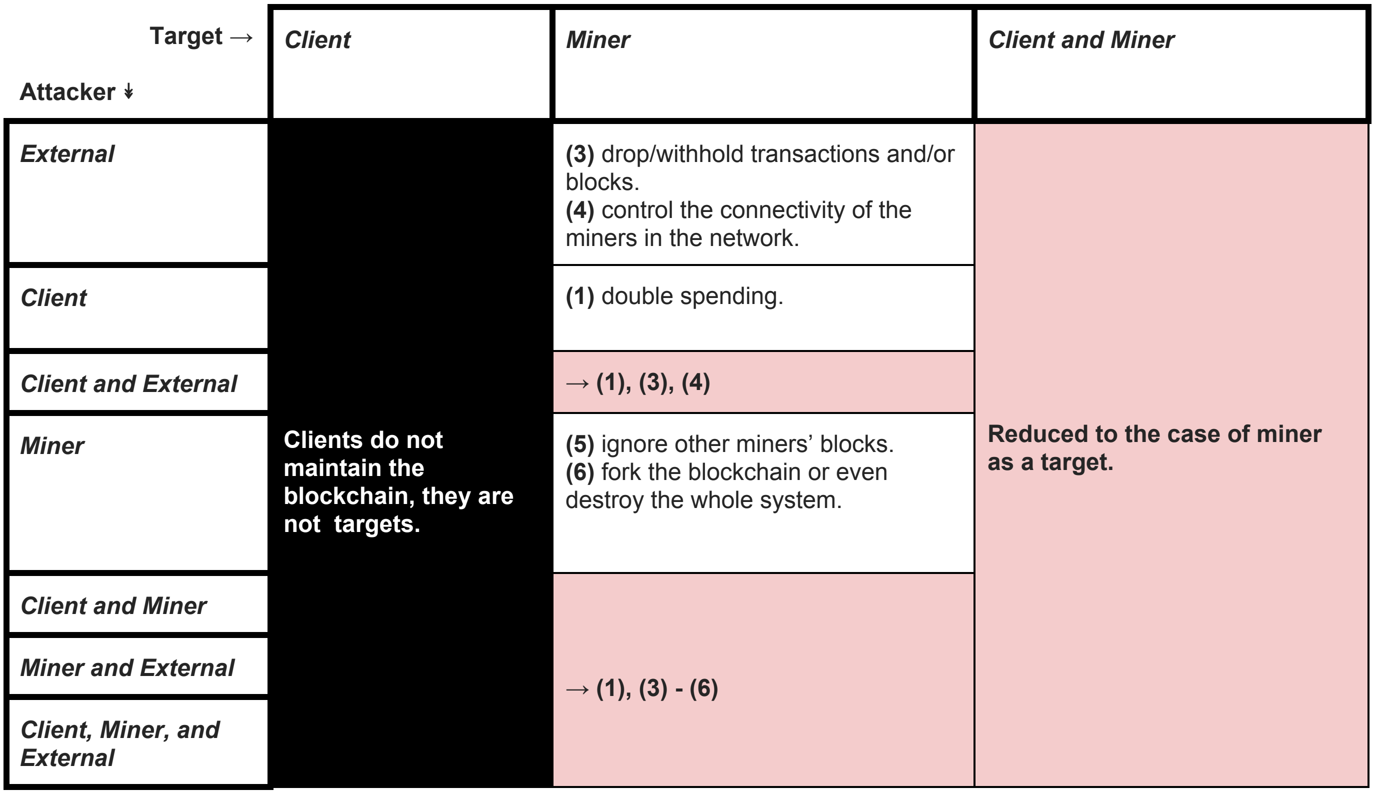
1. An attacker makes miners process different versions of a transaction by performing double spending.
2. An attacker drops/withholds transactions/blocks after being accepted by some miners.
3. An attacker controls the network connections of miners, i.e., control their view of the network, to make them build different versions of the blockchain.
4. An attacker forks the blockchain beyond the latest unconfirmed blocks and announces new branches to different groups of miners.

Note that the aforementioned strategies do not involve tampering of transactions and blocks. This is due to the requirement of signing all announced transactions and blocks as discussed earlier.

Analyzing the collusion matrix of this threat, which is depicted in Figure 3, produces the following threat cases:

- **Threat 3 (Blockchain inconsistency, attacker is anyone, target is miner):** An attacker drops/withholds transactions and/or blocks causing miners to work on different branches of the blockchain.

- **Threat 4 (Blockchain inconsistency, attacker is anyone, target is miner):** An attacker controls the network view of the miners, i.e., what transactions/blocks they receive, by controlling their connectivity. Thus, miners build different copies of the blockchain.
    - This is called an eclipse attack against the network [3]. Such threat needs large power that is not in the hand of average attackers. Other than that, this threat can be addressed by having each miner connect to several peers.
- **Threat 5 (Blockchain inconsistency, attacker is miner, target is miner):** A miner ignores blocks coming from other miners, and hence, does not consider these blocks when extending the blockchain.
- **Threat 6 (Blockchain inconsistency, attacker is miner, target is miner):** An attacker may try to fork the blockchain by building a longer different chain than the current longest one. This also may take forms represented by colluding mining pools (e.g., can perform Godfinger attack [6]), or miners that do not agree to comply with updates on the network protocol (which leads to hard forks in the system).



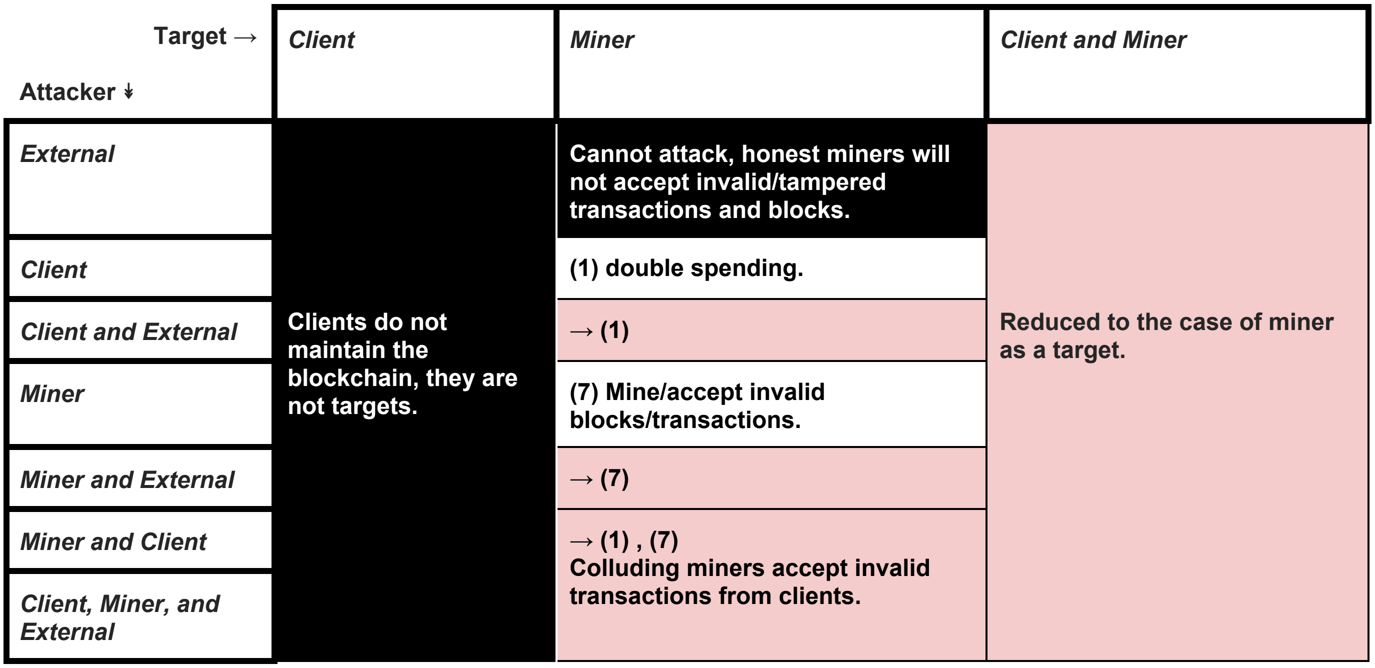
Target → **Attacker ↡**	***Client***	***Miner***	***Client and Miner***
External	**Clients do not maintain the blockchain, they are not targets.**	**(3)** drop/withhold transactions and/or blocks. **(4)** control the connectivity of the miners in the network.	**Reduced to the case of miner as a target.**
Client		**(1)** double spending.	
Client and External		**→ (1), (3), (4)**	
Miner		**(5)** ignore other miners' blocks. **(6)** fork the blockchain or even destroy the whole system.	
Client and Miner		**→ (1), (3) - (6)**	
Miner and External			
Client, Miner, and External			

Figure 3: Blockchain inconsistency threat collusion matrix.

3) Invalid block adoption threat

The collusion matrix of this threat is depicted in Figure 4. Again, miners are the only targets here because they are responsible of maintaining the blockchain. As shown, the matrix is reduced to the following threat case (double spending has been already discussed under the currency theft threat):

- **Threat 7 (Invalid blocks adoption, attacker is miner, target is miner):** A miner adds invalid transaction to the blocks it is mining, or mine on top of an invalid branch of the blockchain.



Target → Attacker ↡	*Client*	*Miner*	*Client and Miner*
External	Clients do not maintain the blockchain, they are not targets.	Cannot attack, honest miners will not accept invalid/tampered transactions and blocks.	Reduced to the case of miner as a target.
Client		(1) double spending.	
Client and External		→ (1)	
Miner		(7) Mine/accept invalid blocks/transactions.	
Miner and External		→ (7)	
Miner and Client		→ (1) , (7) Colluding miners accept invalid transactions from clients.	
Client, Miner, and External			

Figure 4: Invalid block adoption threat collusion matrix.

4) Transaction deanonymization threat

Bitcoin is susceptible to this threat because the full content of the blockchain is public, and transactions can be tracked and linked together [4]. Hence, the whole matrix of this threat, which we omit, is reduced to the following threat case:

- **Threat 8 (Transaction deanonymization, attacker is anyone, target is anyone inside the system):** An attacker is able to read the transaction content on the blockchain and may compromise users' anonymity and privacy.

5) Communication network denial of service threat

This threat covers the following strategies:

- Introduce delays in the communication network while relaying the transactions/blocks. This could be caused by external entities or the miners, either deliberately or unintentionally due a poorly-connected network. (Threat 3 described earlier.)

- Miners ignore announced transactions/blocks. (Threat 3/5 described earlier.)
- An external party isolates nodes in the network and control their view. (Threat 4 described earlier.)
- An external party takes the system down, i.e. Goldfinger attack.
- Issue huge number of transactions to overwhelm the network/miners.

As mentioned before, this threat includes chain freezing threat where the blockchain growth rate is slowed down. Figure 5 depicts the collusion matrix of DoS, which shows the following threat cases:

- **Threat 9 (Communication network DoS, attacker is anyone, target is the system network):** An attacker takes the whole network down.
  - This is a general problem in any distributed system. However, it needs powerful attackers with large amount of resources to be performed.
- **Threat 10 (Communication network DoS, attacker is client/miners, target is the system network):** A client/miner overwhelms the network with huge number of transactions/blocks.
  - This is a general problem in any distributed system.

Target → Attacker ↡	*Client*	*Miner*	*Client and Miner*
External	**(3/5) intercept communication and delay or drop transactions/blocks.** **(4) isolate nodes in the network.** **(9) take the system down.**		
Client	**(10) Overwhelm the miners by issuing large number of transactions.**		
Miner	**(3/5) ignore/withhold/delay transactions/blocks received.**		
Client and Miner	**Can perform any of the previous attacks based on the attackers combination.**		
Client and External			
Miner and External			
Client, Miner, and External			

Figure 5: DoS threat collusion matrix.

References

[1] Bitcoin Transaction Malleability, https://en.bitcoin.it/wiki/Transaction Malleability

[2] Decker, C., Wattenhofer, R.: Bitcoin transaction malleability and mtgox. In: European Symposium on Research in Computer Security. pp. 313–326. Springer (2014)

[3] Heilman, E., Kendler, A., Zohar, A., Goldberg, S.: Eclipse attacks on bitcoin's peer-to-peer network. In: USENIX Security Symposium. pp. 129–144 (2015)

[4] Koshy, Philip, Diana Koshy, and Patrick McDaniel. "An analysis of anonymity in bitcoin using p2p network traffic." In International Conference on Financial Cryptography and Data Security, pp. 469-485. Springer, Berlin, Heidelberg (2014)

[5] Almashaqbeh, G., Bishop, A., Cappos, J.: ABC: A Cryptocurrency-Focused Threat Modeling Framework. In: The 2nd INFOCOM 2019 Workshop on Cryptocurrencies and Blockchains for Distributed Systems (CryBlock), 2019.

[6] Kroll, Joshua A., Ian C. Davey, and Edward W. Felten. "The economics of Bitcoin mining, or Bitcoin in the presence of adversaries." In: WEIS (2013)