TLDR

: We play devil's advocate

and consider that the security of sharding may be broken in practice.

Background

For the security analysis of a protocol it is natural to consider two types of participants:

1. Honest

: A participant following protocol rules.

1. Rational

: A participant maximising profit.

I'll call a participant "malicious" if it is neither honest nor rational. It is intuitively reasonable to assume that the vast majority of participants are non-malicious, i.e. either honest or rational. In the context of a bribing attacker we cannot both have an honest majority and a rational majority. The reason is that honesty and rationality are at odds. A non-malicious participant either needs to be honesty-favouring or rationality-favouring when a briber offers a financial incentive to deviate from the protocol rules.

The rational majority assumption is strictly stronger than the honest majority assumption. Intuitively we know that decentralised protocols are incentive-driven, hence that we should ideally be assuming a rational majority. The security of Ethereum under the bribing attacker model is proportional to the block rewards (protocol subsidies plus transaction fees). The reason is that, in a rational majority, it suffices for a briber to outbid the block rewards to have the majority of miners mine on the briber's fork.

Because the block rewards in Ethereum are high (over $10 million per day) the main chain enjoys a decent amount of security. Moreover, there is significant friction for a bribing attacker to build good-enough bribing infrastructure. These two considerations are probably why bribing attacks have stayed in the realm of academia and were never attempted in practice. In other words, the honest majority assumption was never put to test, and we don't know if it holds in practice.

From a theoretical standpoint, attacking an individual shard is similar to attacking the main chain. Unfortunately, in practice, the situation for an individual shard is much worse than for the main chain, both in terms of cost of attack and in terms of bribing infrastructure.

Cost of attack

Let's first look at the cost of attack.

- Subsidies

: The [COLLATOR_REWARD

](https://github.com/ethereum/sharding/blob/develop/docs/doc.md#constants) is provisionally set at 0.001 ETH per collation. In the best case a collation is created once every 5 blocks, corresponding to 1.152 ETH per day. The current subsidy in the main chain is over 20,000 ETH per day, so subsidies are about 17,500 times lower in an individual shard compared to the main chain. At current market prices, subsidies would provide $0.72 per 5 blocks per shard, i.e. $829 per day per shard. Note also that in the medium-term the collator subsidies are "virtual ETH" in the sense that they are non-fungible with ETH, and so will likely be worth less than "real" ETH.

- Transaction fees

: As a scaling solution sharding should dramatically reduce transaction fees. Vitalik estimates that fees for a collation should not exceed $50. Assuming conservatively that all collations in a shard have $50 transaction fees, that's $57,600 per day.

Adding subsidies and transaction fees, it seems that the cost of a bribing attack on a single shard is on the order of $100,000-$1,000,000 for a full day of transactions.

Bribing infrastructure

In the context of proposer-validator separation, the proposal scheme provides excellent infrastructure for a bribing attacker to take advantage of. The bidding mechanism allows a briber to pay rational validators to build on the fork of the briber's choosing.

The bribing infrastructure is ideal for several reasons:

- Trustless

: Validators can receive bribes trustlessly.

- Free

: The infrastructure comes out of the box for free with sharding phase 1.

- Quality

: It was designed, built and tested to a high standard by a world class team before release.

- In-band

: It is an “in-band” bribe, as opposed to being an ad hoc out-of-band bribe, e.g. coming from some other blockchain.

- Protocol-level

: Validators do not need to follow an ad hoc smart contract.

- Plausible deniability

: The validators benefit from some level of plausible deniability because of fork choice subjectivity.

Conclusion

The proposal mechanism makes attempting a bribing attack on a shard technically easy. Combined with the low cost of attack, it seems likely that bribing attacks will eventually be attempted on individual shards. When this happens the honest majority assumption will be put to test and we may discover it is inadequate in practice.