Nama : Diah Aisyah

NIM : 1103184023

Three Attacks on Proof-of-Stake Ethereum

Recently, two attacks were presented against Proof-of-Stake (PoS) Ethereum: one where short-range reorganizations of the underlying consensus chain are used to increase individual validators' profits and delay consensus decisions, and one where adversarial network delay variants of these attacks, considerably relaxing the requirements on adversarial stake and network timing, and thus rendering the attacks more third attack which allows an adversary with vanishingly small fraction of stake and no control over network message propagation (assuming instead probabilistic message propagation) to cause even long-range consensus chain reorganizations. Honest-but-rational or ideologically motivated validators could use this attack to increase their profits or stall the protocol, threatening incentive alignment and security of PoS Ethereum. The attack can also lead to destabilization of consensus from congestion The Proof-of-Stake (PoS) Ethereum consensus protocol is constructed by applying the finality gadget Casper FFG on top of the fork choice rule LMD Participants with stake that allows them to vote as part of the protocol of PoS Ethereum is given by the Gasper protocol Recent workshave presented two attacks on Gasper and PoS The first attack uses short-range reorganizations (reorgs) of the short-range reorgs also allow validators to increase their earnings from participating in the protocol As a result, honest-but-rational validators will deviate from the protocol, threatening a vanishing fraction of adversarial validators to stall the protocol indefinitely. An adversary who could perform a reorg of k blocks (k-reorg) adversary can stall PoS Ethereum using techniques similar to [18,16]: we show assumed to model networks under normal operation, together with a still vanishingly small (albeit slightly larger than before) fraction of adversarial validators suffices for the adversary to be able to effectively stall the protocol. combine techniques from both refined attacks to devise a long-range reorg attack which requires only an extremely small number of adversarial validators and no adversarial (but only probabilistic) network delay. This third attack is particularly severe for PoS Ethereum for three reasons: 1. Honest-but-rational validators might adopt the strategy as they can use it to votes can be processed timely, reducing resilience against adversarial validators Related Work In both selfish mining and our attacks the adversary withholds our attacks do not lead to an increased block production reward. attacks showcase how consensus instability can arise from reorgs incentivized diminishing block rewards in Bitcoin in the future.Time-bandit attacks point out that MEV earned in past blocks can incentivize and subsidize reorgs and other attacks in the future, e.g., for renting hash power or bribing validators. Outline PoS Ethereum and its network model are reviewed in Section 2. Sections 3 and 4 each first introduce a recent attack and then describe our refined long-range reorg attack in Section 5. presented long-range reorg attack on various aspects of PoS Ethereum. 2 Proof-of-Stake Ethereum: The Gasper Protocol We provide a concise summary of the PoS Ethereum/Gasper protocol and the Gasper and the PoS Ethereum beacon chain protocol specifications [2,4,1]. Three Attacks on Proof-of-Stake Ethereum 3 We assume a static pool of N protocol participants (called validators or nodes), Validators follow the protocol as prescribed, except for a fraction β which are under adversarial control and can deviate from the protocol – Liveness: If some honest validator becomes aware of a transaction, then not by any honest validator (i.e., ‘good things do happen’, ‘transactions enter – Safety: The ledgers output by different honest validators at different points Given an SMR protocol, we seek to understand for which adversarial fractions β the ledger output by that protocol is both safe and live (and hence secure). Being a composite with the LMD GHOST fork choice rule as the basis and Casper FFG as a finality gadget on top, PoS Ethereum consensus proceeds For each slot, one block proposer and a The following LMD GHOST rule is used to determine a canonical block (and its prefix of blocks as a canonical chain) in a node’s view in slot t: “Starting at the highest block b0 ‘justified’ by Casper FFG (see below), sum for each child block b the number of unique (i.e., one per slot and slot’s committee member, breaking ties adversarially) valid (i.e., only from earlier than the current slot, for every validator only its most recently cast vote (LMD). slot, the slot’s proposer determines a block using LMD GHOST and extends it Half way into each slot (i.e., Δ time after the proposal a block using LMD GHOST in their view and vote for it (votes are also called (At the same time they also cast a Casper FFG vote, as described later.) An exact confirmation rule of LMD GHOST/Gasper is not specified. On a high level, Casper FFG is a two-phase traditional propose-and-vote-style Byzantine fault tolerant (BFT) consensus protocol proposals are supposed to be generated consistently across honest nodes by the Casper FFG proceeds as follows: Blocks first become finalized, roughly when a super-majority votes ‘from them’ for a subsequent block. among which validators cast their votes during an epoch are the so-called epoch vote for the highest epoch boundary block that is consistent with the highest justified block they have observed, which in turn extends the latest finalized Due to the super-majority required to advance a proposal, as well as the two-phase confirmation (called finalization), Casper FFG the Casper FFG level is to output the latest finalized block and its prefix. 3 A Refined Reorg Attack the attack leverages strategic timing of broadcasting blocks and attestations, strategy of [19], an adversarial block proposer in slot n keeps its proposal hidden. adversary can now use its committee members’ votes from both slots n and n+ 1 to vote for the withheld block of slot n in an attempt to outnumber honest votes As a result, blocks proposed by honest validators In [19] this reorg strategy is part of a bigger scheme to delay consensus. adversary validators required is significantly reduced, from a set of size linear in the total number of validators to a constant-size set – indeed for a one-block reorg as little as one adversarial validator is sufficient.

Proof of Stake Made Simple with Casper

We study the recent paper Buterin and Griffith introducing Casper, a proof of stake consensus algorithm for blockchains. Proof of stake has several advantages compared to proof of work, and represents what blockchains will look like in the A set of validators cast public votes to decide on which blocks to finalize. They follow some rules which guarantee safety and liveness, and Byzantine Fault Proof of Stake. Most public blockchains like Bitcoin and Ethereum rely on proof of work to reach consensus. Finally, the only way proof of work prevents attackers from breaking consensus is by spending a lot of computational effort on the main Proof of stake uses a set of validators to reach consensus on the main chain. an amount of the blockchain’s cryptocurrency and cast votes weighted by their stake. electricity is consumed, and the system is fully decentralized as there is no economy of scale. biggest advantage of Casper-like proof of stake is that attackers can be identified and their deposit can In proof of work, you can’t destroy an attacker’s hardware after an attack. Our goal is to explain in details what is proof of stake and what is Casper. protocol, the role of a validator, and how to finalize a block. The idea of proof of stake was first formerly introduced in King and Nadal for a cryptocurrency The coin features a mix of proof of work and proof of stake to reach consensus Peercoin represents a first category called chain-based proof of stake that imitate the proof of work mechanism by having randomly chosen validators propose new blocks. Casper (Buterin and Griffith and Algorand come from a second category called Byzantine fault tolerant (BFT) based proof of stake. Casper requires validators to vote and cryptographically sign their vote message before broadcasting it to all other validators. Casper represents an intermediary step to keep using proof of work but also add proof of stake as an additional layer of finality. At first, Casper was following traditional consensus algorithms by using a prepare and commit Validators would first try to prepare a block, and then commit it to finalize it. . The most recent version of Casper (Buterin and Griffith The Casper Protocol The goal of any blockchain consensus is to finalize blocks of transactions. Finalized blocks conflicting blocks (in different forks) can never be both finalized. In proof of work, a block is finalized when it has enough chained descendants (6 for Bitcoin for In proof of stake like Casper, validators vote to decide which blocks get finalized and belong to the Safety guarantees prove that if 2/3 of validators follow the protocol, there can never be two finalized conflicting blocks. Validator and Votes a validator, a user can deposit an amount of the currency on the blockchain and agrees to lose its This deposit represents the stake of the validator. vote is proportional to its stake.