ECE 595: Foundations of Blockchain Systems **November 30, 2020**

Lecture 16: Proof of Stake and Scaling

Lecturer: Sreeram Kannan *Scribe: Jiarong Qian*

Outline: This lecture continues the discussion on the disadvantages the proof of stake protocol and introduces the proof of stake with arrow of time as an improvement to solve the problem.

16.1 Recap

In the last lecture, a protocol called Verifiable Random Functions (VRF) was introduced to prevent the adversary from predicting the leadership within the block chain. The random source used in VRF can be updated periodically, which requires other consensus mechanisms.

16.2 Disadvantages of Proof of Stake

In this proof of stake protocol, there are several disadvantages compared to the proof of work protocol

- Leadership is locally predictable, that is, a node can still predict when it becomes the leader.
- The protocol is not fully dynamically available.

For instance, given a proof of stake network, in the first year, there was no adversary stake and rises to 10% in the next year. While the honest stake was 5% in the first year and rises to 90% in the next year. In the first year, there was a chain built up. However, at the start of the next year, the adversary could instantaneously create a longer private chain than the public longest chain in the past time slots due to costless simulation, while the honest nodes only mine on the longest public chain. This is the long range attack. This attack is not possible in a proof of work protocol such as bitcoin, since it requires time to do the mining.

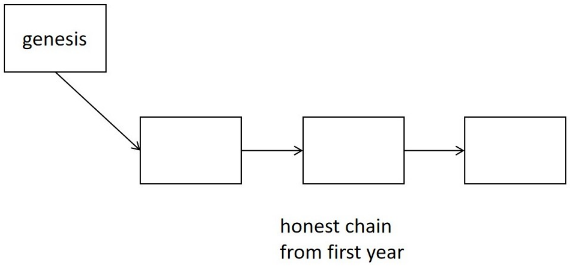

Figure 16.1: The block chain at the first year

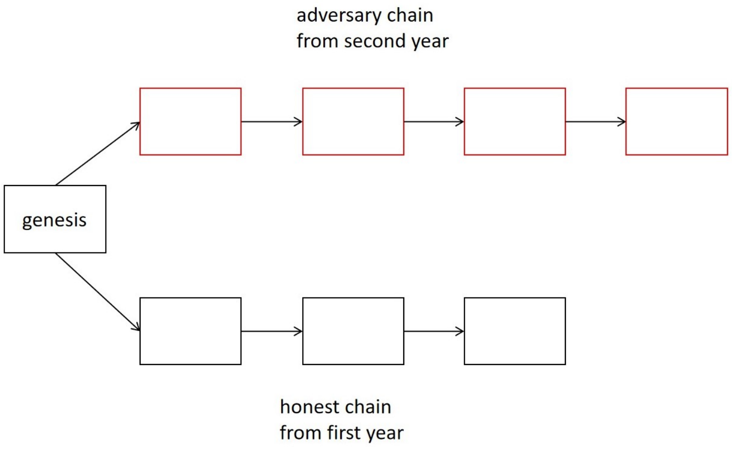

Figure 16.2: The block chain at the start of the second year

16.3 Proof of Stake with Arrow of Time

The Proof of Stake with Arrow of Time protocol uses Verifiable Delay Functions (VDF) to deal with the long range attack. VDF is a mechanism to certify the passage of time. VDF calculates $H^{\ell}(x)$, the hash of x sequentially for ℓ steps. The computation is not parallelizable. If it takes time T to calculate the hash function, then the sequential hashing would take $T\ell$ time. The computation time is generally the same across different computers so no one can get a significant advantage. The result of VDF is not easy to verify because the verification would take the same time as the hashing, but there are some cryptographical mechanism to create short proof π that

$H^\ell(x) = y$. The prover calculates and provides $Hl(x)$ and a proof π to the verifier so the verifier can verify quickly. The leadership computation becomes

$$H^\ell(random\ source, public\ key) < th \cdot stake(public\ key)$$

The random source now comes from the leadership certificate from the previous block instead of being fixed at genesis. There is no notion of time required in the protocol. With VDF, the adversary cannot go back in time and create a longer chain than the honest chain immediately, because creating a longer chain now requires time. While the adversary chain is growing, the honest chain is growing at a larger speed. The time to create a leadership certificate is also unpredictable even to the node itself, given that ℓ is a random variable.

16.4 Nothing at Stake Attack

Nothing at stake attack happens when the adversary tries to grow blocks everywhere on the chain and tries to surpass the longest honest chain. This is possible because the adversary can use the same stake to mine block at many places.

Suppose the inter-arrival time of blocks is 1. After time T, without attack, the length of the longest chain is T. However, due to nothing-at-stake attack, the adversary can grow a private chain but whose length is bounded by $e * T$. The protocol is secure as long as $\lambda_h > e * \lambda_a$. There is a protocol called c-correlation protocol that can further improve the security to condition of $\lambda h > \phi c * \lambda a$.

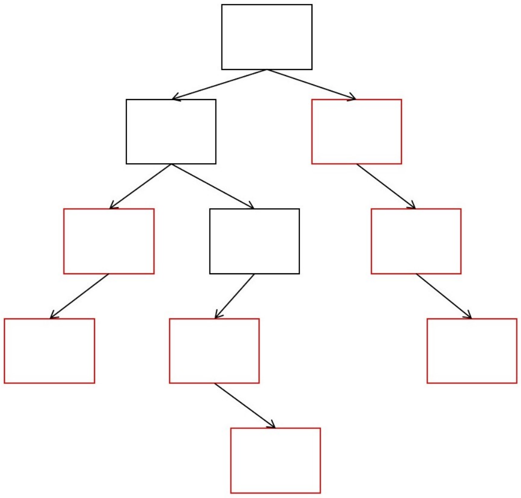

Figure 16.3: Nothing at Stake Attack