EE 374: Blockchain Foundations **Stanford, Winter 2023**

Lecture 17: BFT Protocols: Streamlet

March 15th, 2023

Lecturer: Prof. David Tse

1 BFT vs longest chain protocols

So far we have been focusing on PoW and PoS longest chain protocols. Such protocols, as we showed, use the k-confirmation rule and suffer from long confirmation latency - $O(k\Delta/f)$. (Δ/f is the average block time.) This latency is long due to several reasons:

1. To avoid collision between blocks proposed at the same time, f has to be made mall.
2. To have small probability of violation of the common prefix property, k has to be made large. Moreover, the closer the honest advantage is to 0, the larger k has to be.

But is it possible to have blockchains with fast block confirmation?

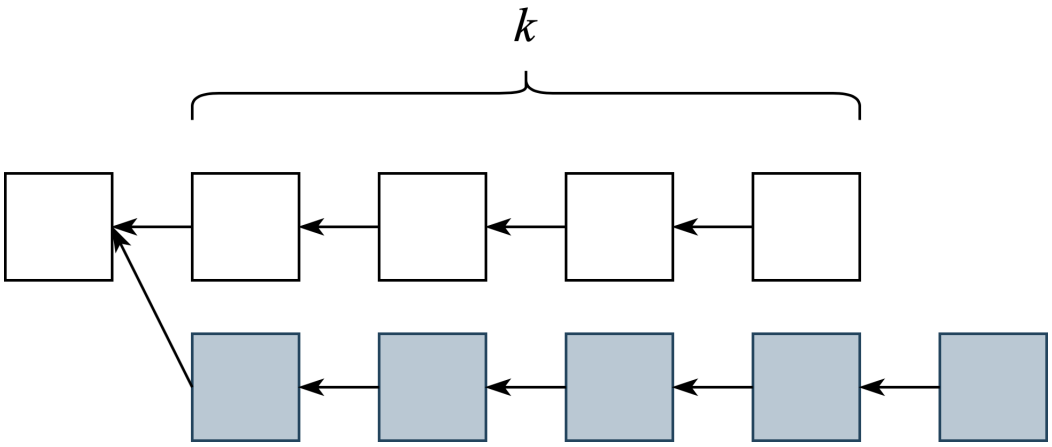

Figure 1: k-confirmation rule: if we choose k too small, the adversary can cause safety violations.

BFT (Byzantine Fault Tolerant) protocols achieve fast confirmation. In such protocols, safety and liveness is guaranteed as long as no more than t out of n nodes are malicious. In BFT protocols, all parties vote *in parallel*, while in longest chain protocols, parties are randomly sampled to vote one at a time (when they propose a block). Hence, the latency of BFT protocols are better. However, because voteres vote in parallel, there are more attack vectors. Hence, BFT protocols are usually pretty complex so in this lecture we will focus on a simple example of such protocols - Streamlet.

1.1 Streamlet Protocol

1. The system consists of n nodes, their public keys $pk_1, pk_2, \ldots, pk_n$ are fixed and known to every protocol participant.

2. The network is synchronized with a delay bounded by Δ. Time is divided into epochs of length 2Δ.

3. Every epoch has a leader L, which is randomly selected via hash function $H(e) \to \{1 \ldots n\}$.

4. Leader L proposes a block B extending the longest *notarized* chain. Initially, only the genesis block is notarized. The header of B has the format $(s\|x\|e\|\sigma^L)$, where s is the hash of the previous block, x is the Merkle root of the transactions in the block, e is the epoch the block is proposed and σ^L is the signature of the leader L.

5. Each node votes on the first valid block it receives by sending a signed message. A block is considered valid if it is proposed in the current epoch by the epoch leader and extends the longest notarized chain. The vote from validator j has the format $(s\|x\|e\|\sigma^j)$, where σ^j is the signature of node j.

6. Notarized blocks are defined as those blocks that contain at least $q = \frac{2}{3}n$ votes.

We defined what it means for a Streamlet block to be notarized but what is a *confirmed* block? Let us try to design the confirmation rule. To do so, we will first look into a simple strawman confirmation rule and see if the resulting protocol is safe.

1.2 Streamlet strawman confirmation rule

Let us confirme a block once it is notarized and extends the longest notarized chain. Can adversary attack such a protocol? She can cause a safety violation if she manages to produce another notarized block at the same height.

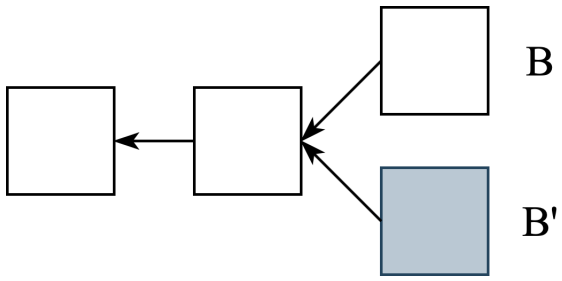

Figure 2: Safety violation in streamlet with strawman confirmation rule

First, let us consider an attack in which an adversary proposes both B and B' from the same epoch. For the attack to be successful, both blocks B and B' illustrated in Figure 2 should be notarized. Additionally, assume that the adversary controls less than $\frac{1}{3}n$ nodes. As it was stated earlier in the protocol description, every notarized block has at least $\frac{2}{3}n$ votes. Therefore, by the quorum intersection argument illustrated in 3, at least $\frac{1}{3}n$ nodes voted on both blocks B and B'. Since adversary controls $< \frac{1}{3}n$ nodes, there must exist at least one honest node that voted for two

blocks in the same epoch, which is not possible. Thus, the adversary cannot cause a violation this way. Is there another attack vector where B and B' are not from the same epoch? We will explore it in the next lecture.

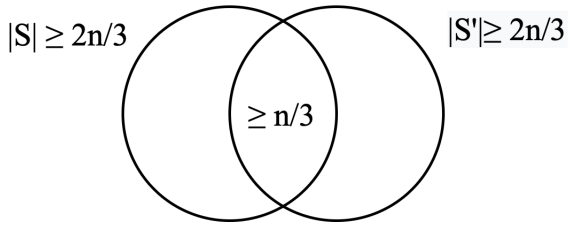

Figure 3: Venn diagram for the quorum intersection argument: let S and S' denote the sets of nodes that voted for the blocks B and B', respectively. By the definition on notarized block, $|S| \geq \frac{2}{3}n$ and $|S'| \geq \frac{2}{3}n$, so $|S \cap S'| \geq \frac{n}{3}$.

References

[1] B. Y. Chan and E. Shi. Streamlet: Textbook streamlined blockchains. In *AFT*, pages 1–11. ACM, 2020.