

Leaderless Byzantine Fault Tolerant Consensus

Jianyu Niu, Fangyu Gai and Chen Feng

The University of British Columbia, Kelowna, Canada

I. INTRODUCTION

Byzantine fault tolerant (BFT) consensus has recently gained much attention because of its intriguing connection with blockchains. Several state-of-the-art BFT consensus protocols have been proposed in the age of blockchains such as Tendermint [5], Pala [9], Streamlet [8], HotStuff [22] and Fast-HotStuff [16]. These protocols are all leader-based (i.e., protocols run in a series of views, and each view has a delegated node called the leader to coordinate all consensus decisions). To make progress, leader-based BFT protocols usually rely on view synchronization, which is an ad-hoc way of rotating leaders and synchronizing nodes to the same view with the leader for enough overlap time. However, many studies and system implementations show that existing methods of view synchronization are complicated and bug-prone [2], [15], [18]. In this paper, we aim to design a leaderless Byzantine fault tolerant (LBFT) protocol, in which nodes simply compete to propose blocks (containing a batch of clients' requests) without the need of explicit coordination through view synchronization. LBFT also enjoys several other desirable features emphasized recently by the research community, such as the chain structure, pipelining techniques, and advanced cryptography [5], [6], [9], [16], [22]. With these efforts, LBFT can achieve both good performance (e.g., $O(n)$ or $O(n \log(n))$ message complexity) and prominent simplicity.

II. SYSTEM MODEL AND PRELIMINARIES

A. System Model

We consider a system with n nodes. We consider two roles of nodes in the system: proposers, who propose blocks, and voters, who vote for received blocks.¹ The system consists of $2m + 1$ proposers and $3f + 1$ voters.² At most m (resp. f) proposers (resp. voters) may be *Byzantine* at any time. We assume a public-key infrastructure (PKI) of voters; each voter has a pair of keys for signing messages. In addition, we assume each proposer with identical ability to produce block proofs (introduced shortly). For simplicity, all the Byzantine nodes (i.e., Byzantine proposers and voters) are assumed to be controlled by a single adversary. The adversary is computationally bounded and cannot (except for negligible probability) forge honest nodes' messages.

We assume that honest nodes are fully and reliably connected, i.e., every pair of honest nodes is connected with an authenticated and reliable communication link. We adopt the partial synchrony model of Dwork *et al.* [11], in

¹In a system, a single node may play both roles.

²Clearly, we have $n \geq 2m + 1$, $n \geq 3f + 1$, and $n \leq 2m + 1 + 3f + 1$. In particular, if every node plays both roles, then we have $n = 2m + 1 = 3f + 1$.

which there are a known delay bound Δ and an unknown Global Stabilization Time (GST) such that all message transmissions between two honest nodes arrive within the bound Δ after GST. In other words, the system is running in *synchronous* mode after GST and in *asynchronous* mode if GST never occurs.

B. Preliminaries

Block and Block Format. A block has a three-tuple $\langle parent_qc, txs, \sigma \rangle$, where $parent_qc$ denotes a quorum certificate of its previous block (also referred to as its parent block), txs is a collection of application-specific transactions, and σ is the block's proof. (The quorum certificates and block proofs will be explained shortly.) There exists a hard-coded genesis block \mathcal{G}_0 . Every block except the genesis block must specify its parent block by including a quorum certificate of that block.

Block Tree. Blocks are chained by a sequence of certificate references $\mathcal{G}_0 \leftarrow B_1 \leftarrow B_2 \leftarrow \dots$. A block's height is its distance from the genesis block. (The height of the genesis block is 0.) A chain's length is defined as the number of blocks in the chain excluding the genesis block. For example, a chain of length 2 contains three blocks, namely, the genesis block, a height-1 block, and a height-2 block. A block B is called a descendant of another block B' if there is a chain from B' to B . Conversely, block B' is an ancestor of block B . Two (distinct) blocks B and B' conflict if neither is a descendant of the other. Because of the possibility of conflicting blocks, each node maintains a block tree (referred to as *blockTree*) of received blocks.

Quorum Certificate. A block's quorum certificate (QC) is proof that more than $2f + 1$ voters have signed this block. Here, a QC could be implemented as a simple set of individual signatures or aggregated signatures [4]. We say a block is certified when its QC is received, and certified blocks are ranked by their heights. Each node keeps track of all signatures for all blocks and keeps updating the certified blocks.³

Block Proof. In LBFT, proposers participate in a lottery to win the right of producing a block, and winning probabilities are proportional to their abilities. Once winning the lottery, a proposer sends out the block together with the proof, which is also called block proof. The lottery can be realized by different cryptographic means to generate the randomness needed. For example, the solution of a Hash puzzle is used in Proof-of-Work (PoW) lottery [17], while verifiable delay functions (VDFs) and verifiable random functions (VRFs) are widely used in Proof-of-Stake (PoS) lottery [3], [13]). Here, we exclude the cryptographic realizations of the lottery since they have already been carefully studied and implemented. Instead, we only provide the necessary abstractions for us to construct LBFT and prove its safety and liveness (See Sec. IV-B for details).

C. Design Goals

We aim to design a leaderless BFT (LBFT) protocol in the partial synchronous network model. From a very high level, all proposers in LBFT can compete to propose blocks once they find some block proofs (at any time), and some of these blocks will eventually be committed. Therefore, there is no explicit leader (which is also called

³To make the signature collection more efficient, nodes keep track of some "fresh" uncertified blocks instead of all blocks. Besides, nodes can send signatures with some signed block information (e.g., hash values or height) to accelerate other nodes' verification processes.

primary in PBFT [7]). Instead, multiple nodes can propose blocks at any given interval (which is known as view [7], and phase [11]). As a BFT consensus protocol, LBFT satisfies the following safety and liveness guarantees:

- **Safety:** No two honest nodes commit to two different blocks at the same height.
- **Liveness:** If some honest proposer receives a collection of transactions txs , these txs will eventually be included in all honest nodes' committed blocks.

In particular, according to the FLP theorem [12], LBFT protocol can always keep safety regardless of the network condition but guarantee liveness only when the network is synchronous.

III. PROTOCOL DESIGN

A. Overview

In this section, we will present an overview of the LBFT protocol. Specifically, it contains three key components: **block proposing**, **voting** and **committing** rules.⁴ Proposers compete to generate new blocks to extend some certified blocks chosen by the **proposing rule**. Specifically, a proposer is allowed to generate a new block once it finds an associated block proof. Once producing a new block, the proposer immediately broadcasts the block to other nodes.⁵ After receiving the new block, nodes first check whether this new block is valid. If yes, nodes insert this block into their local *blockTrees*. Meanwhile, voters will broadcast votes for this valid block if it satisfies the **voting rule**. When nodes collect more than $2f + 1$ votes for the block, this block will be certified, and nodes will check whether there exist new committed blocks by following the **committing rule**.

Unlike other leader-based BFT protocols, LBFT has no predefined views and associated delegated leaders. Therefore, there may exist conflicts between blocks (possibly produced by different proposers). For example, when one block is being broadcast, some different blocks at the same height may be produced simultaneously. As a result, nodes may observe multiple blocks (of the same height), which leads to forks. Hence, nodes have to solve block conflicts and guarantee that only one block is eventually committed at each height through careful protocol design, which can be a challenging task. Below we will explain how the aforementioned three rules address this issue.

B. Protocol Details

In this section, we specify the block proposing, voting, and committing rules of LBFT.

Proposing Rule. A proposer tries to produce a new block on top of the *highest* certified block that it has seen. In addition, if there are two certified blocks with the same highest height, the proposer randomly chooses one to extend.⁶ Note that a valid block should contain transactions that are consistent with the transactions included in its ancestor blocks, a valid QC, and block proof.

⁴In blockchains, block proposers and voters may be two different groups of nodes.

⁵The immediate publish of proposed blocks without additional confirmation of leadership makes the system secure against the adaptive adversary. A detailed discussion will be provided in Sec.V-B.

⁶This proposing rule is similar to the longest chain rule, i.e., proposers extend the longest chain that they have seen. Here, we adopt this version for simplicity.

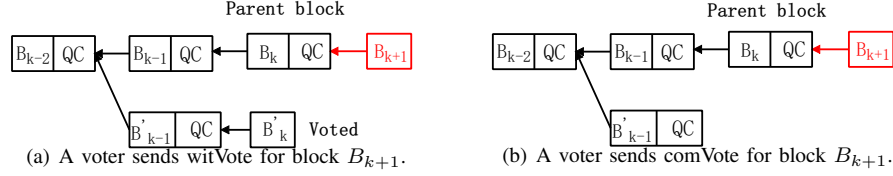


Fig. 1. A voter sends different votes for block B_{k+1} that extends the highest certified block that it has seen.

Voting Rule. When a node receives a new block, it first does the validity check for this block (including transactions, QC, and block proof). If this block does not satisfy the validity, the node will abandon this block. Otherwise, it will insert this block (not certified yet) into its *blockTree*. After that, if this node is a voter, it will check whether to vote for this block. Specifically, the voter votes for this block only if the block extends the highest certified block that it has seen. Additionally, when voting, a voter should choose the type of votes, which are mainly determined by the new block's parent block (denoted by *parent block*). That is, if there exists one conflicting block of height no lower than that of the parent block in this voter's local *blockTrees* and the voter has voted for this conflicting block before, the voter sends a *witness vote* (short for *witVote*); Otherwise, the voter sends a *commit vote* (short for *comVote*).⁷ In particular, when a voter broadcasts its *witVote*, it must include at least one proof (e.g., hash digest) of the conflicting blocks that have heights no lower than the parent block. Note that for each new block, a voter only votes once, and a block is certified if there are at least $2f + 1$ votes for this block (regardless of the type of votes).

To better understand the voting rule, we illustrate some simple cases in Fig.1. In both cases, the new arriving block B_{k+1} extends the highest certified block B_k that a voter has seen, so the voter will broadcast a vote for it. But under different conditions, the types of votes are different. In Fig.1(a), the voter sends a *witVote* for the block. This is because there exists a conflicting block B'_k whose height is the same as block B_{k+1} 's parent block B_k , and this voter has voted for block B'_k before. By contrast, the voter broadcasts a *comVote* in Fig.1(b).

Committing Rule. When having a new certified block, a node will check whether there are new committed blocks. Specifically, if the node observes that the new certified block's QC contains no less than $2f + 1$ *comVotes*, it will commit all uncommitted ancestor blocks of this block, as shown in Fig. 2. Otherwise, it will commit no new blocks. Note that nodes maintain a chain containing committed blocks, and this chain is referred to as the *main chain*.

Here, we provide some insights behind the voting rule design, especially on role of the vote types. First, limiting voters to *only* vote for blocks that extend the longest certified chain can prevent the adversary from creating blocks with low heights.⁸ Second, allowing a voter to vote for multiple blocks at the same height (which all extend the longest certified chain that it has seen) is for liveness. This is because, if voters are required to only vote for one block at each height, they may vote for different blocks with the same height, and then no block is certified with $2f + 1$ votes. As a result, no higher blocks can be produced without referencing a previous certified block, i.e., no liveness. Third, it is necessary to have two types of votes for safety. To see this, let us consider a setting where

⁷For implementation, a 1-bit field can be included to denote the type of votes.

⁸The longest certified chain extension requirement can be relaxed, which will be discussed in our future work.

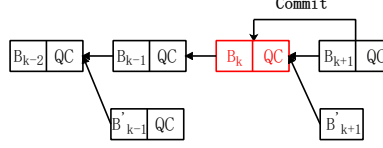


Fig. 2. **A simple case of committing block.** Block B_k and other ancestor blocks are committed when its child block B_k is certified with at least $2f + 1$ comVotes.

there is only one type of votes. Then, under our previous voting rule, nodes cannot commit blocks or guarantee that committed blocks are safe. For example, when a node recovers from a network partition and receives a chain from others, it cannot tell whether blocks in this chain are committed as there possibly exists another forking chain. Hence, another type of vote is required to carry the information that voters have confidence in some “pre-committed” blocks (the only block at the height when voting). Furthermore, if the majority of honest voters send out the promises that a parent block is the only block at the height, and they refuse to vote for any blocks which do not extend this block, this parent block will be committed and safe (i.e., no conflicting committed blocks can be produced at its height).

Remark 1: In LBFT, blocks have three possible states: valid, certified and committed. A valid block contains valid transactions, block proof and a QC of its parent block; A certified block has been voted by at least $2f + 1$ voters; A committed block will be eventually committed by every honest node.

IV. SAFETY AND LIVENESS PROOFS

In this section, we provide safety and liveness proofs for LBFT. We consider no signature forgery or hash collision events as stated in Sec. II. All the lemmas and theorems below hold except for a negligible probability (in the security parameter) due to these events.

A. Safety Analysis

The safety property guarantees that there are no conflicting committed blocks at the same height. It holds for the asynchronous network as well. Before our analysis, we present two useful lemmas here.

Lemma 1: If two certified blocks B and B' are observed by some honest nodes, there must exist an honest voter who has voted for both of them.

Proof: Let \mathcal{S} (resp. \mathcal{S}') denote the set of honest voters that have voted for block B (resp. B'). As there are at most f corrupted voters (who can voted twice for both block B and B'), set \mathcal{S} and \mathcal{S}' at least contain $f + 1$ honest voters. The intersection of these two sets (of honest voters) is $|\mathcal{S} \cap \mathcal{S}'| \geq (f + 1) + (f + 1) - (2f + 1) = 1 > 0$. This implies that at least one honest voter must have voted for both block B and B' . ■

Lemma 2: Suppose that a certified chain adopted among honest nodes contains two blocks B_k, B_{k+1} at height k and $k + 1$, respectively, and block B_{k+1} 's QC contains no less than $2f + 1$ comVotes. Then, there cannot exist a conflicting block $B'_k \neq B_k$ such that B'_k is also certified.

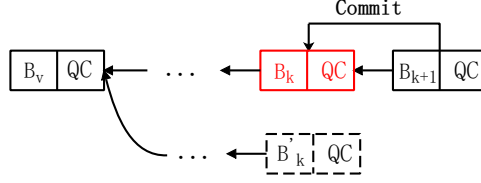


Fig. 3. The safety violation cases (impossible).

Proof: Assume for contradiction that $B'_k \neq B_k$ is certified in at least one honest node, as shown in Fig. 3. By Lemma 1, there must exist one honest voter who has voted for these two blocks. In particular, this voter has sent a comVote for block B_{k+1} . Let t_0 (resp. t_1) denote the time when this voter voted for block B_{k+1} (resp. B'_k). No matter $t_0 < t_1$ or $t_0 > t_1$, we will drive a contradiction. (Here, a voter is assumed to sequentially vote for blocks, so we do not consider the case $t_0 = t_1$.)

- $t_0 < t_1$. The honest voter first voted for block B_{k+1} . According to the voting rule, when the voter receives block B'_k , it would not vote for it. This is because the voter at least has seen a block at height k (i.e., block B_k), and obviously, B'_k does not extend the highest certified block. This leads to a contradiction.
- $t_0 > t_1$. The honest voter first voted for block B'_k . When the voter later received B_{k+1} , it would send a witVote for it according to the voting rule (because block B'_k has the same height as block B_{k+1} 's parent block B_k , and this voter has voted it.). This leads to a contradiction that this voter has sent a comVote for block B_{k+1} . ■

Lemma 2 shows that once a block B_{k+1} is certified with at least $2f + 1$ comVotes, its parent block will be the only certified block at height k . Furthermore, the parent block will be the only committed block at height k , which guarantees the safety of committing this block. However, this is not enough to prove the safety property. Recall that, according to the committing rule, all uncommitted ancestor blocks of the parent block are also committed. The following theorem will show that the safety property holds for all committed blocks.

Theorem 1 (Safety): If blocks B_k and B'_k at height k are committed by some honest nodes, then $B_k = B'_k$.

Proof: Assume for contradiction that $B'_k \neq B_k$ is committed by some honest nodes. (Note that the two blocks could also be committed by a single node.) First, according to the committing rule, there must exist two chain branches: one chain branch containing block B_k ended with two certified blocks B_v and B_{v+1} (with heights v and $v + 1$, respectively), and another one containing block B'_k ended with two certified blocks B'_m and B'_{m+1} (with heights m and $m + 1$, respectively) adopted by at least one honest node. Both QCs of blocks B_{v+1} and B'_{m+1} contain no less $2f + 1$ comVotes. By the committing rule, block B_v together with its ancestor blocks, and block B'_m together with its ancestor blocks are all committed. Obviously, $v, m \geq k$. With loss of generality, assume that $v \leq m$. By Lemma 1, there must exist one honest voter who has sent comVotes for both of blocks B_{v+1} and B'_{m+1} . Let t_0 (resp. t_1) denote the time when this voter voted for block B_{v+1} (resp. B'_{m+1}). No matter $t_0 < t_1$ or $t_0 > t_1$, we will drive a contradiction.

- $t_0 < t_1$. The honest voter first voted for block B_{v+1} . By Lemma 2, there cannot exist a certified block B'_v .

As $v \leq m$, there cannot exist certified blocks B'_m . Furthermore, this voter could not vote for block B'_{m+1} without receiving its parent block. This leads to a contradiction.

- $t_0 > t_1$. The honest voter first voted for block B'_{m+1} . By Lemma 2, there cannot exist a conflicting certified block at m . This implies $k+1 < m$. In addition, to vote for B'_{m+1} , this voter at least has received the parent block B'_m . Obviously, block B_{k+1} did not extend the highest certified block (Block B_k has a smaller height than block B'_m), this voter would not vote for it. This leads to a contradiction. ■

B. Liveness Analysis

In this section, we prove liveness for LBFT. The liveness property guarantees that honest blocks (including clients' transactions) will be eventually committed no matter what the adversary does. Specifically, the liveness property holds only when the network is synchronous, i.e., after the GST. This is because when the network is partitioned and delays can be arbitrarily long, no certified blocks can be produced (without enough votes), and consequently, no blocks can be committed.

1) *Proof Overview*: Let us first revisit the block committing case in Fig. 2. In this case, block B_k is the only certified block at height k , and is later extended by some descendant blocks B_{k+1} and B'_{k+1} . During the voting process for blocks B_{k+1} and B'_{k+1} , there are no other blocks at height k except for block B_k . Obviously, honest voters will send comVotes for blocks B_{k+1} and B'_{k+1} according to the voting rule. Eventually,⁹ when nodes receive at least $2f+1$ comVotes for either block B_{k+1} or block B'_{k+1} , they will commit block B_k together with its ancestor blocks by the committing rule. Therefore, if there exists such a certified *honest* block, and the block remains unique at its height until it is later extended by a certified descendent block (i.e., with at least $2f+1$ comVotes), the block together with its ancestor blocks will be committed. The following analysis will show that, with high probability, there always exist such certified *honest* and *unique* blocks (referred to as certified unique blocks for short), which will be committed no matter what the adversary does.

To this end, we first prove that the liveness property can hold from any time t_0 after the GST under an ideal assumption that *the adversary does not withhold any block at time t_0* . Specifically, we prove that there exist certified unique blocks with high probability no matter what the adversary does. The existence of certified unique blocks can guarantee that there are honest committed blocks after t_0 . We then relax this ideal assumption and show that the adversary can only hide a finite number of blocks at time t_0 , which does not affect the existence of certified unique blocks.

2) *Detailed Analysis*: We first introduce a mathematical model of the generation process of block proofs. For concreteness, we assume that LBFT adopts the well-known PoW lottery to generate block proofs, which implies that the generation process can be modeled as a Poisson process with rate λ [1], [10], [19], [21].¹⁰ In particular, the

⁹When the network is synchronous, it takes at most 2Δ to certify a block by Lemma 4.

¹⁰LBFT can also adopt other cryptographic means to realize the lottery. In [10], the authors provided a unified framework to model the block producing process of PoW, Proof-of-Stake, and Chia Proof-of-Space lotteries. The liveness analysis can be easily extended to different models.

generation process at each proposer is a Poisson process with rate $\lambda/(2m+1)$ as proposers have identical capability in our system model. Let β ($\beta \leq m/(2m+1)$) be the fraction of proposers corrupted by the adversary. Let λ_h and λ_a denote the rate at which the honest proposers and the adversary produce block proofs, respectively. We have $\lambda_a = \beta\lambda$ and $\lambda_h = (1-\beta)\lambda$. As $\beta < 1/2$, we have $\lambda_a < \lambda_h$. We next present some useful lemmas.

Lemma 3: If an honest node has observed a certified block at time t_0 ($t_0 \geq \text{GST}$), then every honest node observes a chain ended with this certified block by the time $t_0 + \Delta$.

Proof: First, by the strong Δ -bounded assumption during periods of synchrony, all honest nodes will have observed this block by $t_0 + \Delta$. Second, for a certified block, at least $f+1$ honest voters have signed for this block at or before time t_0 , and they must have observed a certified blockchain extended by this block by time t_0 . Hence, by the time $t_0 + \Delta$, every honest node will observe a chain ended with this certified block. ■

Lemma 4: If an honest node has observed a block B_ℓ (not certified yet) that extends a certified blockchain at time t_0 ($t_0 \geq \text{GST}$), then every honest proposer can start to produce blocks of height at least $\ell+1$ by the time $t_0 + 2\Delta$.

Proof: First, this block B_ℓ will reach all the honest nodes by time $t_0 + \Delta$ by the Δ -bounded assumption during periods of synchrony. Next, by Lemma 3, its certified ancestor blocks will reach all the honest nodes by time $t_0 + \Delta$. Then, all honest voters will send votes for this block (no matter what is the type) unless that some of the honest voters have observed a certified chain with no less than ℓ length at time $t_0 + \Delta$. If all honest voters vote for this block at time $t_0 + \Delta$, then at least $2f+1$ votes will arrive at all honest nodes by time $t_0 + 2\Delta$, and then all nodes will observe a certified chain ended with this certified block. Otherwise, at least one honest voter has seen a certified chain of no less than ℓ length at time $t_0 + \Delta$, and by Lemma 3, all nodes will observe this chain by time $t_0 + 2\Delta$. Therefore, no matter in which cases, honest nodes will observe a certified chain with no less than ℓ length at time $t_0 + 2\Delta$. Every honest proposer can start to produce blocks with at least a height of $\ell+1$. ■

Next, we introduce a special kind of honest blocks called *unique* blocks. An honest block produced at time t is called a unique block if there is no honest block produced in the previous and next 2Δ time. We have the following two lemmas for unique blocks.

Lemma 5: Suppose block B is a unique block of height ℓ , then no other honest block can be of height ℓ .

Proof: Suppose for contradiction that two honest blocks B and B' of height ℓ are produced at time t and t' respectively. Since no other honest block is produced between time $t-2\Delta$ and $t+2\Delta$, we have $t' \geq t+2\Delta$ or $t' \leq t-2\Delta$. If $t' \geq t+2\Delta$, by Lemma 4, every honest node observes a certified chain of length at least ℓ by time t' , and meanwhile, proposers produce blocks on top of it. Therefore, no honest proposer will produce a new block of height ℓ after time t' , leading to a contradiction. Similarly, if $t' \leq t-2\Delta$, every honest node observes a certified chain of length at least ℓ before the time t (or even earlier), leading to a contradiction. ■

The following lemma gives the bounds on the number of unique blocks in a time interval of t .

Lemma 6: Let $\eta = e^{-2(1-\beta)\lambda\Delta}$. For any $0 < \delta < 1$, the number of unique blocks produced in a time interval t is at least $(1+\delta)\eta^2(1-\beta)\lambda t$, except for probability $e^{-\Omega(t)}$.

Proof: Let $N_H(t)$ denote the number of honest block produced in a time interval t , and note that $\mathbb{E}[N_H(t)] = \lambda_h t = (1-\beta)\lambda t$. Then, for any $\delta_1 \in (0, 1)$, we have $\Pr[N_H(t) \leq (1-\delta_1)(1-\beta)\lambda t] \leq e^{-\delta_1^2(1-\beta)\lambda t/2} = e^{-\Omega(t)}$ by

Lemma 10. In particular, let $k = (1 - \delta_1)(1 - \beta)\lambda t$ be an integer by choosing a suitable t . We enumerate the first k honest blocks produced since the start of the time interval as blocks $1, 2, \dots, k$. Without loss of generality, we assume there is a block 0 (resp. block $k + 1$) that is the last honest block produced before (resp. after) the interval.

Let X_i denote the block interval between $(i - 1)$ -th and i -th block. Recall the block production process of honest proposers is the Poisson process with rate $(1 - \beta)\lambda$. Hence, X_i follows i.i.d. exponential distribution with the same rate. Let Y_i denote an indicator random variable which equals one if the i -th block is unique block and zero otherwise. Define $Y = \sum_{i=1}^n Y_i$. It is easy to see that the i -th block is a unique block if $X_i \geq 2\Delta$ and $X_{i+1} \geq 2\Delta$. Since X_i and X_{i+1} are independent, we have $\Pr[Y_i = 1] = \Pr[X_i \geq 2\Delta] \Pr[X_{i+1} \geq 2\Delta] = e^{-4(1-\beta)\lambda\Delta} = \eta^2$. Note that Y_i and Y_{i+1} are not independent since they both depend on the event that $X_{i+1} \geq 2\Delta$, but Y_i and Y_{i+2} are independent. Thus, Y can be broken up into two summations of independent Boolean random variables $Y = \sum_{\text{odd}} Y_i + \sum_{\text{even}} Y_i$. By Lemma 11, we have $\Pr[Y \leq (1 - \delta)\eta^2(1 - \beta)\lambda t] \leq e^{-\delta^2\eta^2(1-\beta)\lambda t/2} = e^{-\Omega(t)}$. ■

The following lemma presents the condition to guarantee that there exist certified unique blocks in the longest certified chain.

Lemma 7: Suppose $\eta^2(1 - \beta) > (1 + \delta)\beta$. In a time interval t , there exist certified unique blocks in the longest chain except for $e^{-\Omega(t)}$ probability.

Proof: Let $N_H(t)$ (resp. $N_A(t)$) denote the unique (resp. adversarial) block produced in the interval t . By Lemma 6, the number of unique blocks is $N_H(t) > (1 - \delta_1)\eta^2(1 - \beta)ft$ except for $e^{-\Omega(t)}$ probability. Similarly, the expected time for the adversary to produce a block is $\frac{1}{\lambda_a}$. In the best case, the adversary can immediately transmit a block to honest voters, and then obtain their votes without delay. This means that the adversary can immediately produce the next block on its new block. Thus, during a time interval t , the adversary can produce blocks at most $(1 + \delta_2)\lambda_a t$ except for probability $e^{-\delta_2^2\lambda_a t/3} = e^{-\Omega(t)}$ by Lemma 10.

By setting $\delta_1 = \delta_2 = \delta/4$ and noticing $\frac{1+\delta/4}{1-\delta/4} < 1 + \delta$, we have $(1 - \delta_1)\eta^2(1 - \beta) > (1 + \delta_2)\beta$. Therefore, $N_H(t) > N_A(t)$ except for $e^{-\Omega(t)}$ probability. This means that the adversary cannot create conflicting blocks to match each unique block. In other words, there exist unique blocks that every honest voter will vote for it (as it is the only block that extends the longest certified chain), and then this block will be certified. ■

Theorem 2 (Liveness): Suppose $\eta^2(1 - \beta) > (1 + \delta)\beta$. In a time interval t , there exist committed honest blocks in the main chain except for $e^{-\Omega(t)}$ probability.

Proof: By Lemma 7, there exists at least one certified unique block in the longest chain except for $e^{-\Omega(t)}$ probability. Without loss of generality, we assume that such a block B is produced at time t_1 . By time $t_1 + 2\Delta$, all honest proposers can produce the next block on block B by Lemma 4. When a new block is proposed, honest voters will send comVotes for this new block by the voting rule, and this new block will be certified at each node within 2Δ interval. By that time, the unique block B_l together with its ancestor blocks will be committed by each nodes. ■

Finally, we will relax the ideal assumption and allow the adversary to withhold some blocks from honest proposers at time t_0 and then publish them to match unique blocks produced by honest proposers. The following lemma shows that the adversary cannot hide more than a finite number of blocks that are higher than the highest block that any honest nodes know after $\text{GST} + 2\Delta$.

Lemma 8 (Bounded number of hidden blocks): At any time $t_0 \geq \text{GST} + 2\Delta$, the number of unknown blocks to any honest nodes is bounded with high probability.

Proof: Without loss of generality, we assume block B_ℓ is the highest block published by the adversary before the time $t_0 - 2\Delta$. Specifically, to produce block B_ℓ , all ancestor blocks of block B_ℓ have been certified. This implies, at least $f + 1$ honest nodes have seen and voted for block B_ℓ 's parent block before the time $t_0 - 2\Delta$. (In the ideal case, we assume the adversary immediately collect all votes for block B 's parent block, and then generate block B without delay.) By Lemma 4, all honest nodes would observe a certified chain with no less than ℓ length by time t_0 . Let $N_A(2\Delta)$ denote the number of produced adversarial blocks between the time $t_0 - 2\Delta$ and time t_0 . As the block proof production process of the adversary is a Poisson process with rate λ_h , the probability of generating k new blocks that extend block B_ℓ is $\frac{e^{-2\lambda_a\Delta}(2\lambda_a\Delta)^K}{k!}$, which drops exponentially with the increase of k . ■

This lemma implies that any honest nodes do not know a finite number of blocks that are higher than the highest block that they have known. Therefore, by increasing the interval t , LBFT can guarantee these exist certified unique blocks, which will be committed with high probability. This establishes the liveness of LBFT.

V. DISCUSSION

A. Message Complexity

In this section, we briefly discuss how to reduce the message complexity. Let us first revisit the message complexity of the current version of LBFT. When receiving a new block (satisfying the voting rule), a voter will broadcast its vote of this block to all nodes. Hence, the message complexity of broadcasting all votes equals to the product of the number of voters and the number of nodes, i.e., $O(n^2)$ message complexity. When a subsequent proposer produces a new block on this block, it has to include a QC with at least $2f + 1$ votes and broadcast the new block to all nodes, which also occurs $O(n^2)$ message complexity.

We can reduce the message complexity in the following ways. First, we can use aggregated signatures [4] for the QC to reduce the message complexity of broadcasting a block to $O(n)$.¹¹ Second, we can change the message transmitting pattern to reduce the message complexity. Specifically, we can use a gossip protocol or a leader-based pattern. With a gossip protocol, the message complexity for proposers (resp, voters) to transmit blocks (resp, votes) is $O(n \log(n))$. With a leader-based pattern, the producer of a new block becomes a "leader", and all voters only send their votes for this new block to this leader. When collecting enough votes (forming a certificate), the leader will send the QC of its block to every nodes. In this way, the message complexity of votes and blocks become $O(n)$. Note that changing the message transmitting pattern does not affect the block proposing, voting, and committing rules.

B. Adaptive Adversary

In LBFT, proposers participate in a lottery to win the right to produce a block. Once winning a lottery, proposers immediately publish their blocks. There is no further special role or actions after the block publishing is performed.

¹¹In the worst case, there are two types of votes for a block. Hence, at most two aggregated signatures of votes are needed.

Therefore, the block proposing is unpredictable, which makes LBFT secure against a fully adaptive adversary. By contrast, some leader-based BFT systems require nodes to first participate in a lottery to win the leader candidacy [14], [20]. After that, one candidate is eventually chosen as the leader by some reductions or agreements, and the single leader is responsible for coordinating the consensus decisions. However, the additional reductions or agreements may expose these candidates' identity, making it possible for a fully adaptive adversary to corrupt them. Consequently, a corrupted leader would hinder the progress.

VI. PRIOR WORK

In this section, we review several state-of-the-art BFT protocols [5], [9], [22] in the age of blockchains that are mostly related to LBFT. As we will see, LBFT enjoys many desirable features achieved by these protocols.

Tendermint. Tendermint [5] features a continuous leader rotation (also called the democracy-favoring leader rotation [9]) based on PBFT protocol. Specifically, Tendermint embeds a round-change mechanism into the common-case pattern, and the leader is re-elected from all the nodes by some desired policy after every block, resulting in better leadership fairness.

Casper FFG. Buterin and Griffith [6] proposed a protocol called Casper FFG, which works as an overlay atop NC to provide “finality gadget”. Casper FFG applies an elegant pipelining idea to the classical BFT protocol, i.e., if each block requires two rounds of voting, one can piggyback the second round on the next block's voting. This pipelining idea enables the system to have one identical round (rather than multiple rounds with different functionalities and names¹²), and so significantly simplifies the protocol design.

Pala and Streamlet. Pala [9] is a simple BFT consensus protocol that adopts the pipelining idea. However, for high throughput, it uses a stability-favoring leader rotation policy. Based on this work, Chan *et al.* [8] proposed Streamlet, which further simplifies the voting rule. Streamlet aims to provide a unified, simple protocol for both teaching and implementation.

HotStuff. HotStuff proposed by Yin *et al.* [22] creatively adopts a three-phase commit rule (rather than the two-phase commit rule used in Casper FFG, Pala, and Streamlet) to enable the protocol to reach consensus at the pace of actual network delay. In addition, HotStuff adopts the threshold signature to realize linear message complexity, and can also be pipelined into a practical protocol for building large-scale blockchains.

VII. CONCLUSION

In the paper, we propose a leaderless BFT (LBFT) consensus protocol, which does not require coordinators to make progress. Consequently, LBFT eliminates the often complicated view synchronization, leading to better security and simplicity. LBFT also enjoys many desirable features, such as the chain structure, pipelining techniques, and advanced cryptography. All these efforts make LBFT both practical (i.e., $O(n)$ or $O(n \log(n))$ message complexity after optimizations), secure and simple to be implemented for large-scale applications like blockchains.

¹²In PBFT, for committing one proposal, there are two phases: prepare and commit phases, and each phase has different functionalities.

REFERENCES

- [1] Vivek Kumar Bagaria, Sreeram Kannan, David Tse, Giulia C. Fanti, and Pramod Viswanath. Prism: Deconstructing the blockchain to approach physical limits. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS' 19)*, London, UK, November 11-15, 2019., pages 585–602, 2019.
- [2] Shehar Bano, Mathieu Baudet, Avery Ching, Andrey Chursin, George Danezis, François Garillot, Zekun Li, Dahlia Malkhi, Oded Naor, Dmitri Perelman, et al. State machine replication in the Libra blockchain, May 2020.
- [3] Iddo Bentov, Rafael Pass, and Elaine Shi. Snow white: Provably secure proofs of stake. *IACR Cryptology ePrint Archive*, 2016(919), 2016.
- [4] Dan Boneh, Craig Gentry, Ben Lynn, and Hovav Shacham. Aggregate and verifiably encrypted signatures from bilinear maps. In Eli Biham, editor, *Advances in Cryptology — EUROCRYPT 2003*, pages 416–432, Berlin, Heidelberg, 2003. Springer Berlin Heidelberg.
- [5] Ethan Buchman. Tendermint: Byzantine fault tolerance in the age of blockchains. *M.Sc. Thesis, University of Guelph, Canada*, Jun 2016.
- [6] Vitalik Buterin and Virgil Griffith. Casper the friendly finality gadget. *CoRR*, abs/1710.09437, 2017.
- [7] Miguel Castro and Barbara Liskov. Practical Byzantine fault tolerance. In *Proceedings of the Third Symposium on Operating Systems Design and Implementation*, OSDI '99, pages 173–186, Berkeley, CA, USA, 1999. USENIX Association.
- [8] Benjamin Y. Chan and Elaine Shi. Streamlet: Textbook streamlined blockchains. *IACR Cryptol. ePrint Arch.*, 2020:88, 2020.
- [9] T-H Hubert Chan, Rafael Pass, and Elaine Shi. Pala: A simple partially synchronous blockchain. *IACR Cryptology ePrint Archive*, 2018:981, 2018.
- [10] Amir Dembo, Sreeram Kannan, Ertem Nusret Tas, David Tse, Pramod Viswanath, Xuechao Wang, and Ofer Zeitouni. Everything is a race and nakamoto always wins. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security (CCS '20)*, page 859–878, New York, NY, USA, 2020.
- [11] Cynthia Dwork, Nancy Lynch, and Larry Stockmeyer. Consensus in the presence of partial synchrony. *Journal of the ACM (JACM)*, 35(2):288–323, 1988.
- [12] Michael J. Fischer, Nancy A. Lynch, and Michael S. Paterson. Impossibility of distributed consensus with one faulty process. In *Proceedings of the 2nd ACM SIGACT-SIGMOD Symposium on Principles of Database Systems*, PODS '83, page 1–7, New York, NY, USA, 1983.
- [13] Yossi Gilad, Rotem Hemo, Silvio Micali, Georgios Vlachos, and Nickolai Zeldovich. Algorand: Scaling Byzantine agreements for cryptocurrencies. In *Proceedings of the 26th Symposium on Operating Systems Principles*, SOSP '17, pages 51–68, New York, NY, USA, 2017. ACM.
- [14] Eleftherios Kokoris Kogias, Philipp Jovanovic, Nicolas Gailly, Ismail Khoffi, Linus Gasser, and Bryan Ford. Enhancing Bitcoin security and performance with strong consistency via collective signing. In *25th USENIX Security Symposium (USENIX Security 16)*, pages 279–296, Austin, TX, 2016. USENIX Association.
- [15] Andrew Miller, Yu Xia, Kyle Croman, Elaine Shi, and Dawn Song. The honey badger of BFT protocols. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, CCS '16, pages 31–42, New York, NY, USA, 2016. ACM.
- [16] Jianyu Niu Mohammad M. Jalalzai and Chen Feng. Fast-hotstuff: A fast and resilient hotstuff protocol. *arXiv preprint arXiv:2010.11454*, 2020.
- [17] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. *Working Paper*, 2008.
- [18] Oded Naor, Mathieu Baudet, Dahlia Malkhi, and Alexander Spiegelman. Cogsworth: Byzantine view synchronization. *arXiv preprint arXiv:1909.05204*, 2019.
- [19] Jianyu Niu, Chen Feng, Hoang Dau, Yu-Chih Huang, and Jingge Zhu. Analysis of Nakamoto consensus, revisited. *arXiv preprint arXiv:1910.08510*, 2019.
- [20] Rafael Pass and Elaine Shi. Hybrid consensus: Efficient consensus in the permissionless model. In *31st International Symposium on Distributed Computing (DISC 2017)*, volume 91 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 39:1–39:16, Dagstuhl, Germany, 2017.
- [21] Ling Ren. Analysis of Nakamoto consensus. *Cryptology ePrint Archive*, Report 2019/943, 2019.
- [22] Maofan Yin, Dahlia Malkhi, Michael K. Reiter, Guy Golan Gueta, and Ittai Abraham. HotStuff: BFT consensus with linearity and responsiveness. *PODC '19*, pages 347–356, 2019.

APPENDIX

A. Concentration Bounds

In this section, we provide the concentration bounds that we use in the analysis. We denote the probability of an event E by $\Pr[E]$ and the expected value of a random variable X by $\mathbb{E}[X]$.

Lemma 9 (Chernoff bound): Let X_1, \dots, X_n be independent random variables, and let $\mu := \mathbb{E}[\sum_{i=1}^n X_i]$. For $0 < \delta < 1$, we have $\Pr[\sum_{i=1}^n X_i > (1 + \delta)\mu] < e^{-\delta^2 \mu / 3}$ and $\Pr[\sum_{i=1}^n X_i < (1 - \delta)\mu] < e^{-\delta^2 \mu / 2}$.

Lemma 10 (Chernoff bounds for Poisson random variables): Let X be a Poisson random variable with mean μ . Then, for $0 < \delta < 1$, $\Pr(X \geq (1 + \delta)\mu) \leq e^{-\delta^2 \mu / 3}$ and $\Pr(X \leq (1 - \delta)\mu) \leq e^{-\delta^2 \mu / 2}$.

Lemma 11 (Chernoff bound for dependent random variables [19]): Let T be a positive integer. Let $X^{(j)} = \sum_{i=0}^{n-1} X_{j+iT}$ be the sum of n independent indicator random variables and $\mu_j = \mathbb{E}[X^{(j)}]$ for $j \in \{1, \dots, T\}$. Let $X = X^{(1)} + \dots + X^{(T)}$. Let $\mu = \min_j \{\mu_j\}$. Then, for $0 < \delta < 1$, $\Pr[X \leq (1 - \delta)\mu T] \leq e^{-\delta^2 \mu / 2}$.