

Fast-HotStuff: A Fast and Robust BFT Protocol for Blockchains

Mohammad M. Jalalzai^{*†}, Jianyu Niu^{*†}, Chen Feng^{*†} and Fangyu Gai^{*†}

^{*}School of Engineering, The University of British Columbia, Kelowna, Canada

[†]Blockchain@UBC, The University of British Columbia, Vancouver, Canada

{m.jalalzai, jianyu.niu, chen.feng, fangyu.gai}@ubc.ca

Abstract—The HotStuff protocol is a recent breakthrough in Byzantine Fault Tolerant (BFT) consensus that enjoys both responsiveness and linear view change by creatively adding a round to classic two-round BFT protocols like PBFT. Despite its great advantages, HotStuff has a few limitations. First, the additional round of communication during normal cases results in higher latency. Second, HotStuff is vulnerable to certain performance attacks, which can significantly deteriorate its throughput and latency. To address these limitations, we propose a new two-round BFT protocol called Fast-HotStuff, which enjoys responsiveness and efficient view change that is comparable to the linear view-change in terms of performance. Our Fast-HotStuff has lower latency and is more robust against the performance attacks that HotStuff is susceptible to.

Index Terms—BFT, Blockchain, Consensus, Latency, Performance, Security.

I. INTRODUCTION

Byzantine Fault Tolerant (BFT) consensus has received considerable attention in the last decade due to its promising application in blockchains. Classic BFT-based protocols suffer from the scalability issue due to the high-cost when the leader is replaced¹. For example, in PBFT, $O(n^3)$ authenticators/signatures are exchanged and processed during a leader replacement (where n corresponds to the network size) [1]. More recent protocols like SBFT [2], Zyzzyva [3] and BFT-Smart [4] have reduced the number of signatures transmitted and processed within the network to $O(n^2)$. Still, the cost of view change is high for a large n , causing an enormous delay. This becomes an even bigger problem when a rotating primary² protocol is used where the primary is replaced after each block proposal.

Several state-of-the-art BFT protocols, including Tendermint [5] and Casper FFG [6], have been proposed to address the issue of expensive view change. These protocols not only support linear message complexity by using advanced cryptography (such as aggregated or threshold signatures), but also enable frequent leader rotation by adopting the chain structure (which is popular in blockchains). Moreover, these protocols can be pipelined, which can further improve their performances, and meanwhile, make them much simpler to implement. These protocols operate with a synchronous core,

and there is a pessimistic bound Δ on the network delay. Hence, the protocol has $O(\Delta)$ latency (instead of the actual network latency), therefore lacking responsiveness.

The HotStuff protocol is the first to achieve both linear view change³ and responsiveness, solving a decades-long open problem in BFT consensus. Linear view change enables fast leader rotation while responsiveness drives the protocol to consensus at the speed of wire $O(\delta)$, where δ is the actual network latency. Both are desirable properties in the blockchain space. In BFT protocols, a decision is made after going through several phases, and each phase usually takes one round of communication before moving to the next. HotStuff introduces a chained structure borrowed from blockchain to pipeline all the phases into a unifying propose-vote⁴ pattern which significantly simplifies the protocol and improves protocol throughput. Perhaps for this reason, pipelined HotStuff (also called chained HotStuff) has been adopted by Facebook’s DiemBFT [8] (previously known as LibraBFT), Flow platform [9], as well as Cypherium Blockchain [10]. Throughout the paper, we refer to the pipelined version of HotStuff (not the basic HotStuff).

To achieve both properties (responsiveness and linear view change), HotStuff uses threshold signatures and creatively adopts a three-chain commit rule. In the three-chain commit rule, it takes two uninterrupted rounds of communication plus one another round (not necessarily uninterrupted) among replicas to commit a block. For example, for a block at round r to get committed, two consecutive rounds $r+1$, $r+2$ and one another round $r+k$, where $k > 2$ must be completed successfully. This is in contrast with the two-chain commit rule commonly used in most other BFT protocols [1], [5], [6], [11], [12].

In this paper, we mainly focus on the chained (pipelined) version of HotStuff with a rotating primary. In the rotating primary mechanism, a dedicated primary is assigned each time to propose a block. The rotating primary mechanism provides two additional important properties to a partially synchronous protocol (that cannot be achieved through the stable primary mechanism, where the primary is changed only upon failure). First, by randomly selecting the rotating primary nodes, the protocol limits the time window for malicious adversaries

¹A leader is also called primary. A primary proposes a value to the network. The network tries to reach a consensus to serially execute the proposal.

²View is a number that is deterministically mapped to the ID of the primary/leader. Hence, when a view is changed, the primary is changed in the protocol.

³In HotStuff [7], the linear view change has been defined as the linear number of signatures/authenticators sent over the wire during consensus.

⁴A primary proposes the next block once it receives $n-f$ votes for the previous block without waiting for the previous block to get committed.

to perform a Denial-of-Service attack on the primary node [8]. Secondly, by rotating primary nodes, each node gets an equal opportunity to propose a block. This can be a very important property when nodes receive rewards by proposing blocks. Moreover, pipelining significantly improves the protocol throughput.

HotStuff has made trade-offs to achieve linear view change and responsiveness. First, it adds a round of consensus to the classic two-round BFT consensus. Secondly, to achieve higher throughput, a rotating primary in pipelined HotStuff proposes a block without waiting for its child block to get committed (proposals are pipelined).

This results in the formation of forks, which can be exploited by Byzantine primaries to overwrite blocks from correct primaries before they are committed. It should be noted that classic BFT protocols [1], [2], [13] do not allow fork formation. The main reason for the generation of forks is that a proposed block is not yet committed while the next block is being proposed by the following primary. Furthermore, forking also breaks the requirement for three consecutive rounds to commit a block, resulting in additional delay. As shown in Figure 1, the last three blocks in replica i 's chain have been added during rounds r , $r+1$, and $r+2$ (where the block during $r+2$ is the latest block in replica i 's chain). Now, a Byzantine primary during the round $r+3$ proposes a block that points to the grandparent of the latest block as its parent. In this case, the block proposed during the round $r+3$ points to the block proposed during the round r as its parent block instead of pointing to the block of the round $r+2$. This is acceptable according to HotStuff's voting rule. A replica accepts a proposal and votes for it as long as it does not point to the predecessor of the grandparent of the latest block. Hence, allowing the formation of forks in HotStuff results in lower throughput and higher latency. Byzantine replicas will break the consecutive order of blocks added to the chain through forking. As it can be seen in Figure 1 initially the blocks were added to the chain through consecutive rounds (r , $r+1$ and $r+2$). But after forking, the consecutive rounds in the chain are broken by the block in the round $r+3$. As a result, the new block sequence in the chain is r and $r+3$. Since $r+3$ is the most recent block, the next primary will extend the block proposed during $r+3$. Therefore, averted transactions have to be re-proposed. Furthermore, new consecutive rounds have to be completed for the block in round r , to get committed. This causes an increase in latency and throughput degradation. It should be noted that forking attacks in HotStuff can be prevented if a stable primary mechanism (instead of rotating) is used. But in that case, the protocol will lose its ability to limit the window of time in which an adversary can launch a Denial-of-service attack (when primary nodes are selected randomly). Moreover, by not using rotating primary, each node will not be able to get an equal chance of adding a block to the chain.

Therefore, a natural question arises here that:

Is it possible to design a consensus protocol that avoids the trade-offs made by HotStuff while still having responsiveness and efficient view change (with rotating primary mechanism)?

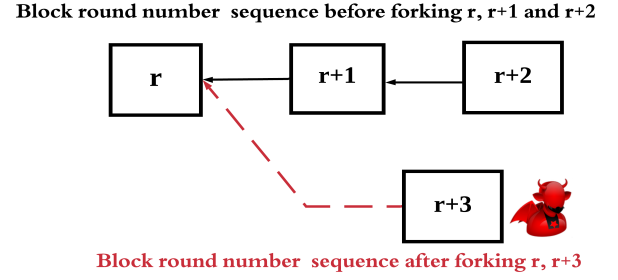


Fig. 1: **The primary of the round $r+3$ performs the forking attack.**

To answer the above question, we designed Fast-HotStuff. Fast-HotStuff is robust against forking attack and has lower latency in comparison to the HotStuff. Moreover, similar to the HotStuff, Fast-HotStuff provides efficient view change and responsiveness.

Forking attack cannot be performed in Fast-HotStuff. This is because in Fast-HotStuff a primary has to provide proof that the proposed block is extending the latest block seen by the majority of replicas. Based on Figure 1, the primary of the round $r+3$ has to provide a proof that the parent of its proposing block is the latest block seen by the majority of replicas. Any replica will not vote for a block unless it satisfies the requirement for the proof of extending the latest block seen by the majority of replicas. This prevents Byzantine primaries to propose a block that points to an older block as its parent, as done in Figure 1. As a result, fork formation is avoided.

Similarly, in the absence of failure after two rounds of communication, a replica in Fast-HotStuff commit a block without waiting for the third round. The protocol guarantees that if a single replica commits a block, other replicas will eventually commit the same block at the same height. This guarantee can be achieved in HotStuff in the absence of failure after three rounds of communication.

There are mainly two types of view change in Fast-HotStuff, 1) Happy path, in which a block is successfully proposed by a primary and $n-f$ votes are collected for it by the next primary in line and 2) The unhappy path in which the primary failed to propose a block, majority of replicas timeout and move to the next view (primary). In Fast-HotStuff in the absence of primary failure, during normal rotation or happy path of the primary (view change) no overhead is needed. This means when no primary failure occurs, then the primary rotation or the view change requires only one authenticator to send and verify. Therefore, the happy path in Fast-HotStuff is linear. Unfortunately, we are not able to avoid the transfer of quadratic view change messages over the wire during view change due to primary failure (also called unhappy path). But we were able to reduce the number of signatures to be processed (verified) by each replica by the factor of $O(n)$. The number of authenticators (aggregated signatures) to be verified in Fast-HotStuff during the unhappy path is reduced to only two. This is in contrast with other two-chain responsive BFT protocols [2]–[4], [14], [15]

where at least $O(n)$ authenticators need to be verified by each replica ($O(n^2)$ for n replicas). Therefore, reducing the number of signatures to be verified significantly improves performance for large n . The tradeoff for improvements achieved in Fast-HotStuff is a small overhead in the block each time a primary fails (unhappy path). For example, this overhead is at most $\approx 1.4\%$ of the block size (1MB) and $\approx 0.7\%$ of 2MB block for the network size of 100 replicas. We also show in Sections V and VII that this overhead does not have a significant impact on performance.

Overall, during the unhappy path, the view change is optimized by reducing the number of authenticators to be verified by each replica. Whereas during happy path the protocol enjoys linear view change similar to HotStuff.

The rest of the paper is organized as follows. In Section II, we describe the system model. In Section III, we present an overview of HotStuff protocol. Section IV, discuss in detail the tradeoffs made by HotStuff to achieve linear view change and responsiveness. Section V provides algorithms for basic Fast-HotStuff and pipelined Fast-HotStuff protocols. Section VI provide safety and liveness proofs for the basic and pipelined Fast-HotStuff. Evaluation and related work are presented in Sections VII and VIII, respectively. The paper is concluded in Section IX.

II. SYSTEM MODEL AND PRELIMINARIES

A. System Model

We consider a system with $n = 3f + 1$ parties (also called replicas) denoted by the set N in which at most f replicas are Byzantine. Byzantine replicas may behave arbitrarily, whereas correct (or honest) replicas always follow the protocol. We assume a *partial synchrony model* presented in [16], where there is a known bound Δ on message transmission delay (when the network is in the synchronous mode). This Δ bound holds after an unknown asynchronous period called *Global Stabilization Time* (GST). In practice, the system can only make progress if the Δ bound on message delivery remains for a sufficiently long time. Furthermore, assuming the Δ bound is everlasting simplifies the discussion. All exchanged messages are signed. Adversaries are computationally bound and cannot forge signatures or message digests (hashes) but with negligible probability. Moreover, Fast-HotStuff uses a static adversary model. In the static adversary model, nodes are chosen to be corrupted at the beginning of the protocol.

B. Preliminaries

View and View Number. During each view, a dedicated primary is responsible for proposing a block. Each view is identified by a monotonically increasing number called view number. Each replica uses a deterministic function to translate the view number into a replica *ID*, which will act as primary for that view. Therefore, the primary (or leader) of each view is known to all replicas.

Signature Aggregation. Fast-HotStuff uses signature aggregation [17]–[19] to obtain a single collective signature of constant size instead of appending all replica signatures when

a primary fails. As the primary p receives the message M_i with their respective signatures $\sigma_i \leftarrow \text{sign}_i(M_i)$ from each replica i , the primary then uses these received signatures to generate an aggregated signature $\sigma \leftarrow \text{AggSign}(\{M_i, \sigma_i\}_{i \in N})$. The aggregated signature can be verified by replicas given the messages M_1, M_2, \dots, M_y , where $2f + 1 \leq y \leq n$, the aggregated signature σ , and public keys PK_1, PK_2, \dots, PK_y . To authenticate message senders as done in previous BFT-based protocols [1], [13], [20] each replica i keeps the public keys of other replicas in the network. Fast-HotStuff can use any signature scheme where message sender identities are known. HotStuff uses threshold signature [17], [21], [22] where identities of message senders are not known. We also show in practice, that aggregated signature used by Fast-HotStuff and threshold signatures used by HotStuff have comparable performance.

Quorum Certificate (QC) and Aggregated QC. A block B 's quorum certificate (QC) is proof that more than $2n/3$ nodes (out of n) have voted for this block. A QC comprises an aggregated signature or threshold (from $n - f$ signatures from distinct replicas) built by signing block hash in a specific view. A block is certified when its QC is received, and certified blocks' freshness is ranked by their view numbers. In particular, we refer to a certified block with the highest view number that a node knows as the *latest/highest* certified block. The latest QC a node knows is called *highQC* (in HotStuff). Fast-HotStuff considers a global view for *highQC* to avoid the additional round. Therefore, *highQC* in Fast-HotStuff is the latest QC held by the majority of replicas or the QC with the higher view than the latest QC held by the majority of replicas. The block proposal includes the *highQC* as well as the proof of *highQC* within itself. It should be noted that unlike classic BFT in HotStuff and Fast-HotStuff the QC is also used to point to the parent block. An aggregated QC or *AggQC* is simply a vector built from a concatenation of $n - f$ or $2f + 1$ QCs.

Block and Block Tree. Clients send transactions to primary, who then batch transactions into blocks. A block also has a field that it uses to point to its parent. In the case of HotStuff and Fast-HotStuff, a QC (which is built from $n - f$ votes) is used as a pointer to the parent block. Every block except the genesis block must specify its parent block and include a QC for the parent block. In this way, blocks are chained together. As there may be forks, each replica maintains a block tree (referred to as *blockTree*) of received blocks. Two blocks B_{v+1} and B_{v+2} are conflicting if neither B_{v+1} is predecessor nor ancestor to the block B_{v+2} , nor B_{v+2} is predecessor or ancestor to the block B_{v+1} . But conflicting blocks have a common predecessor block (B_v in this case). The parent block B_v is the vertex of the fork, as shown in Figure 2.

Chain and Direct Chain. If a block B is being added over the top of a block B' (such that $B.\text{parent} = B'$), then these two blocks make one-chain. If another block B^* is added over the top of the block B , then B' , B , and B^* make two-chain and so on. There are two ways that the chain or tree of blocks grows. First, the chain grows in a continuous manner where the chain is made between two consecutive blocks. For example, for two blocks B and B' we have

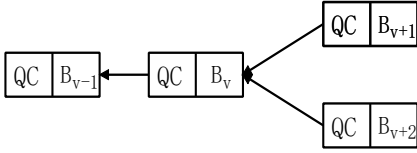


Fig. 2: A simple case of conflicting blocks. Block B_v is a fork vertex, and blocks B_{v+1} and B_{v+2} are two conflicting blocks.

$B.curView = B'.curView + 1$ and $B.parent = B'$. Thus, a direct chain exists between block B and B' . This is also called one-direct chain. If $B.curView = B'.curView + 1$ and $B.parent = B'$ and $B*.curView = B.curView + 1$ and $B*.parent = B$, then we can say a two-direct chain exists among blocks B' , B and B^* . But there is also the possibility that one or more views between two views fail to generate block due to primary being Byzantine or network failure. In that case $B.curView = B'.curView + k$ where $k > 1$ and $B.parent = B'$ and direct chain does not exist between B' and B .

III. HOTSTUFF IN A NUTSHELL

In this section, we provide a brief description of the three-chain HotStuff protocol. There are two variants of the three-chain HotStuff protocol, the basic and pipelined HotStuff. Since pipelined HotStuff is mainly used due to its higher throughput, here, we will focus on pipelined HotStuff.

We describe the pipelined HotStuff operation beginning in the view v . At the beginning of the view v a dedicated primary is selected by replicas operating in the view number v . The primary proposes a block B_v (multicast to all replicas) that extends the block certified by the *highQC* it has seen. Upon receipt of the first proposed block from the primary, each replica sends its vote (a signature on the block) to the primary of view v . Upon receipt of $n - f$ votes, the primary of the view v builds a *QC* and forwards the *QC* to the primary of the view $v + 1$ ⁵. The *QC* of the view v is the *highQC* that the primary of the view $v + 1$ is holding. Therefore, the primary in the view $v + 1$ will propose its block (B_{v+1}) with the *QC* from the view v , as shown in the Figure 3.

Every replica has to keep track of two local parameters in HotStuff 1) *last_voted_view*, the latest view when the replica has voted and 2) *last_locked_view*, the view of the grandparent block of the *last_voted_view*. As it can be seen from the Figure 3, when a replica votes for the block B_{v+2} during view $v + 2$, its *last_voted_view* will be $v + 2$ and it locks the grandparent block of the block B_{v+2} . Hence, *last_locked_view* will be the view v . In order to vote, each replica makes sure that the received block satisfies the voting conditions. Voting conditions include 1) the proposed block extends the block at the *last_locked_view* or 2) the view number of the received block's parent is greater than the *last_locked_view*. If either of the voting conditions is satisfied, then the replica will vote and update its *last_voted_view* and the *last_locked_view* to

⁵If the primary of the view v is Byzantine, then it may not share the *QC* for the view v with the primary of the view $v + 1$.

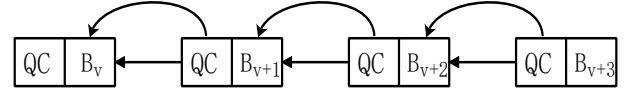


Fig. 3: The chain structure of pipelined HotStuff. Curved arrows denote the Quorum certificate references.

some new values. For example, when the replica receives the block for view $v + 3$ (B_{v+3}), it then makes sure the voting conditions are met. As it can be seen, the block B_{v+3} extends the *last_locked_view* (view v), satisfying the first condition (though the second condition is also satisfied as the view of the parent of B_{v+3} is greater than v or $v + 2 > v$). Therefore, the replica will vote for B_{v+3} . The replica then increments its *last_voted_view* to $v + 3$, its *last_locked_view* to $v + 1$. Then the replica checks its *block tree* to see if there is any block that needs to be committed. If there are three blocks added over the top of each other during consecutive (uninterrupted) views (B_v, B_{v+1}, B_{v+2}) and extended by at least one another block (in this case B_{v+3}), then the replica will commit the block B_v and all its predecessor blocks. The first three blocks added to the chain during consecutive uninterrupted views make a two-direct chain. For the first block in the two-direct chain to get committed, an additional block (may not form a direct chain) is need to extend it and make it a three-chain.

Overall, the HotStuff primaries propose blocks, and replicas vote on the proposed blocks. Replicas commit a block if there is a two-direct chain extended by another block, making a three-chain. Replicas move to the next view either when they receive a valid block with a *QC* or when the primary fails to propose the block, and replicas timeout (wait for a proposal until timeout period).

IV. LIMITATIONS OF HOTSTUFF

A. Higher Latency During Happy Path

To achieve linear view change and responsiveness, HotStuff adds a round of communication. In HotStuff the message propagation depends on the primary. Therefore, at the end of the second round, a replica cannot commit a block because it is not sure if other replicas will eventually complete the same round successfully. Only at the end of the three successful consecutive rounds for a block, a replica can be sure that other replicas at least have completed the first two rounds successfully. Though at the end of the second round, a replica in HotStuff locks on the *last_locked_view*, as it suspects some replicas might have committed the value at the *last_locked_view*. The lock is only released if the primary proves that no one has committed the value at the *last_locked_view*.

The lock provides the safety guarantee, but a third round is required to achieve liveness. If a replica commits a block after two rounds, then the *last_locked_view* will be the view of the parent of the most recent block. In this scenario, there can be a case where the *QC* lock generated for the *last_locked_view* is missing for the majority of nodes infinitely, hence creating a hidden lock problem [7], [23].

For example, during a view $v-1$ a primary proposes a block b . Upon receipt of b , each replica votes for b and the primary for the view v collects votes and builds a QC (qc) certificate/lock for b . The primary of v can only send a new proposal b' (containing the QC for b) to a single replica r_v before it fails. Now replica r_v has the most recent lock (the lock/ QC for the view v). Replicas move to the view $v+1$ and the primary of the view $v+1$ receives responses (containing the lock for $v-1$ as the most recent lock) from $2f+1$ replicas (not including r_v). The primary for the view $v+1$ prepares a message b' and adds the QC qc' (such that $qc'.view = v-1$). Since qc' is not the latest lock and b' conflicts with b (forming a fork), replica r_v rejects it and remains locked with the lock qc . The primary for the view $v+1$ sends b' only to one replica r_{v+1} , before it fails. The replica r_{v+1} gets locked with the QC for block b' in the view $v+1$. This process can repeat indefinitely.

Replicas r_v and r_{v+1} reject the proposal as they are holding a more recent lock (QC) than the one in the proposal. Unlocking these replicas requires assuring them that the block (they have locked) has not been committed. In Fast-HotStuff, during a primary failure, the next primary aggregates and sends back all the locks it has received from replicas as proof (while only two locks need to be verified). This allows any replica holding the higher lock to release it (as it knows that the locked value has not been committed by any replica) and take part in consensus.

Therefore, the HotStuff protocol achieves consensus during the happy path in three rounds (whereas many other BFT protocols often use two rounds) [1], [2], [4], [12]. Such additional latency might discourage blockchain developers from building applications on top of HotStuff, as users have to wait more time in order to receive the notification that their transactions have been committed.

B. Forking Attack

A Byzantine primary in pipelined HotStuff can deliberately generate forks to override the blocks from the correct (honest) primary [24]. As it can be seen in Figure 4, blocks B_{v+1} and B_{v+2} are honest blocks and the Byzantine primary will propose the block B_{v+3} using the QC for the block B_v . Other replicas will vote for B_{v+3} as it satisfies the voting rule (B_{v+3} extends B_v). Since B_{v+3} has higher view than B_{v+2} , next primary will extend B_{v+3} . Byzantine primary may choose to use the QC from the block B_{v+1} to override only a single block B_{v+2} . This may happen in case when the block B_v has been proposed by another Byzantine primary.

As a result of forking, the resources (computing, bandwidth, etc.) spent on forked blocks are wasted. Similarly, transactions of reverted blocks will have to be re-proposed by another primary. Hence, these transactions encounter additional latency. Furthermore, since forking overrides the honest blocks it also breaks the direct chain relation among blocks (refer to Section II). This results in delaying the block commitment as the commit rule says that for a block to get commit, at least the first two blocks over the top of it should make a two-direct chain (two blocks from consecutive views). Forking attack

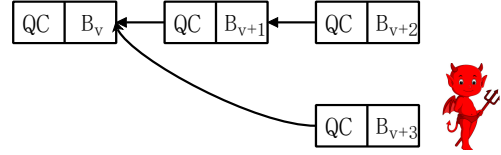


Fig. 4: Forking attack by the primary of the view $v+3$.

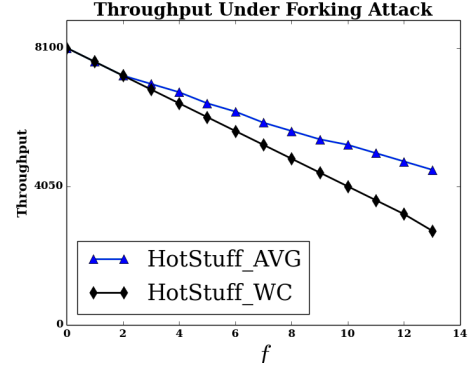


Fig. 5: Throughput decreases under Forking Attack.

makes it difficult to design an incentive mechanism like PoS over the top of HotStuff as blocks from correct primaries will not be able to get committed, and hence correct primaries will be less likely to earn rewards⁶.

Average Performance Due to Forking. It is important to know how HotStuff's average performance is affected by the forking attack. To find this out, we performed an experiment to show the tension between the number of faulty (Byzantine) replicas and the throughput in HotStuff as shown in Figure 6. The network size $n = 40$ and $f = 13$. The fraction of Byzantine replicas was initially zero and gradually increases to f . The throughput achieved in the absence of forking attack (in the absence of Byzantine replicas) is 8100 tx/sec, but as the fraction of f increases (x -axis) the average capacity of the network to process transactions decreases under forking attack as shown by the blue curve.

Worst Case Performance Due to Forking. As previously mentioned, each Byzantine primary can override at most two blocks from correct primaries. Worst case is possible when primaries are selected in round-robin manner. We show a pattern of primary selection, where the HotStuff will fulfill the two-direct chain commit condition only once. This means, after n views, only once a block (and any prior uncommitted block in its chain) that meet the commit condition will be committed. In this case, each Byzantine primary avert two blocks proposed by correct/honest primaries. Hence, f Byzantine primaries will avert $2f$ honest blocks. As a result, during n views (assuming no timeout occurs), only $f+1$ blocks get committed. In these $f+1$ blocks committed during n views only 1 block is from a correct primary. Whereas, the remaining f committed blocks are from Byzantine primaries. This empowers Byzantine primaries to

⁶More details about this will be provided in our future work.

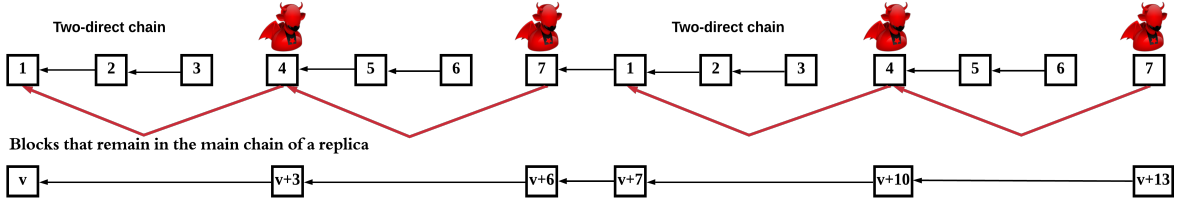


Fig. 6: Worst case forking attack that is possible under round-robin mechanism of primary selection.

censor or significantly delay specific transactions. As it can be seen in Figure 6 two-direct chain condition is satisfied after n views (during $v+2$ and $v+9$, when primary 3 is in charge). Once two-direct condition is met, for example in view $v+9$, $f+1 = 2+1 = 3$ blocks from views $v+7, v+6$ and $v+3$ get committed. Whereas primaries in views $v+7$ and $v+3$ are Byzantine.

The worst-case throughput (under the different number of Byzantine replicas), in HotStuff, is presented by the black curve in the Figure 5. As mentioned, only $f+1 = 13+1$ blocks from primaries will end up in the main chain. Where f number of blocks belonging to Byzantine primaries and only one block is from a correct primary. Here, Byzantine primaries do not reduce the size of their proposed block. The throughput of the network can be further reduced if Byzantine primaries propose smaller blocks. It should be noted that the worst case can be avoided by determining the primary rotation order via opening a common coin [25], [26].

V. FAST-HOTSTUFF

Fast-HotStuff operates in a series of views with monotonically increasing view numbers. Each view number is mapped to a unique dedicated primary known to all replicas. The basic idea of Fast-HotStuff is simple. The primary has to convince voting replicas that its proposed block is extending the block pointed by the *highQC*. Once a replica is convinced, it checks if a two-chain is formed over the top of the parent of the block pointed by the *highQC* (the first chain in the two-chain formed has to be a one-direct chain in case of pipelined Fast-HotStuff). Then a replica can safely commit the parent of the block pointed by the *highQC*.

Unlike HotStuff (where a block is committed in three rounds), in the Fast-HotStuff protocol, a replica i can optimistically commit/execute a block during at the end of the second round while guaranteeing that all other correct replicas will also commit the same block in the same sequence eventually. This guarantee is valid when either one of the two conditions is met: **1) the block proposed by the primary is built by using the latest QC that is held by the majority of replicas, or 2) by a QC higher than the latest QC being held by a majority of replicas.** Therefore, the primary has to incorporate proof⁷

⁷The proof of *highQC* is the proof provided by the primary in the proposed block that shows the latest QC in the block is the latest QC held by the majority of replicas or the latest QC included in the block is more recent than the latest QC held by the majority of replicas.

of the *highQC* (being held by the majority of replicas or higher than the *highQC* held by the majority of replicas) in every block it proposes, which can be verified by every replica.

Interestingly, the inclusion of the proof of the *highQC* by the primary in Fast-HotStuff also enables us to design a responsive two-chain consensus protocol. Indeed, the presence of the proof for the *highQC* guarantees that a replica can safely commit a block after two-chain without waiting for the maximum network delay as done in two-chain HotStuff [7], Tendermint [5], and Casper [6]. Therefore, Fast-HotStuff achieves responsiveness only with a two-chain structure (which means two rounds of communication) in comparison to the three-chain structure in HotStuff (three rounds of communication).

Algorithm 1: Utilities for replica i

```

1 Func CreatePrepareMsg(type, aggQC, qc, cmd):
2   b.type  $\leftarrow$  type
3   b.aggQC  $\leftarrow$  aggQC
4   b.qc  $\leftarrow$  qc
5   b.cmd  $\leftarrow$  cmd
6   return b
7 End Function
8 Func GenerateQC(V):
9   qc.type  $\leftarrow$  m.type : m  $\in$  V
10  qc.viewNumber  $\leftarrow$  m.viewNumber : m  $\in$  V
11  qc.block  $\leftarrow$  m.block : m  $\in$  V
12  qc.sig  $\leftarrow$  AggSign(qc.type, qc.viewNumber, qc.block, i,
    {m.Sig | m  $\in$  V})
13  return qc
14 End Function
15 Func CreateAggQC( $\eta_{Set}$ ):
16  aggQC.QCset  $\leftarrow$  extract QCs from  $\eta_{Set}$ 
17  aggQC.sig  $\leftarrow$  AggSign(curView,
    {qc.block | qc.block  $\in$  aggQC.QCset}, {i | i  $\in$  N},
    {m.Sig | m  $\in$   $\eta_{Set}$ })
18  return aggQC
19 End Function
20 Func BasicSafeProposal(b, qc):
21  return b extends from qc.block
22 End Function
23 Func PipelinedSafeBlock(b, qc, aggQC):
24  if QC then
25    return b.viewNumber  $\geq$  curView  $\wedge$  b.viewNumber ==
      qc.viewNumber + 1
26  end
27  if AggQC then
28    highQC  $\leftarrow$  extract highQc from AggregatedQC
29    return b extends from highQC.block
30  end
31 End Function

```

Since HotStuff has two three-chain variants (the basic and the pipelined HotStuff), therefore we present two-chain basic Fast-HotStuff as well as pipelined Fast-HotStuff protocols. First, we present the basic optimized two-chain Fast-HotStuff and then extend it to an optimized two-chain pipelined Fast-HotStuff protocol. Moreover, basic Fast-HotStuff needs the proof for the *highQC* in the form of $n - f$ *QCs* attached in the proposed block by the primary in order to be able to guarantee safety and liveness as a two-chain protocol. In the case of blockchains since block size is usually large (multiples of Megabytes), this overhead has little effect on performance metrics like throughput and latency. We also show that the protocol requires only two *QCs* to be verified instead of $n - f$ *QCs*. Then, we further optimized pipelined Fast-HotStuff by introducing proposal pipelining. Moreover, for pipelined Fast-HotStuff, the block includes a single *QC* during the happy path, and similar to the basic Fast-HotStuff only two *QCs* need to be verified in case of the primary failure.

A. Basic Fast-HotStuff

The algorithm for two-chain responsive basic HotStuff is given in Algorithm 2. Below, we describe how the basic Fast-HotStuff algorithm operates. Fast-HotStuff operates in three phases PREPARE, PRECOMMIT and COMMIT. The function of each phase is described below.

PREPARE phase. Initially, the primary replica waits for new-view messages $\eta = \langle \text{"NEWVIEW"}, curView, prepareQC, i \rangle$ from $n - f$ replicas. The NEWVIEW message contains four fields indicating message type (NEWVIEW), current view (*curView*), the latest *PrepareQC* known to replica *i*, and replica id *i*. The NEWVIEW message is signed by each replica over fields $\langle curView, prepareQC.block, i \rangle$. *prepareQC.block* is presented by the hash of the block for which *prepareQC* was built (hash is used to identify the block instead of using the actual block). The primary creates and signs a prepare message ($B = \langle \text{"Prepare"}, AggQC, commands, curView, h, i \rangle$) and broadcasts it to all replicas, as shown in Algorithm 2. We can also use the term block proposal or simply block for PREPARE message. *AggQC* is the aggregated *QC* build from valid η messages collected from $n - f$ replicas.

Upon receipt of a PREPARE message *B* from the primary, a replica *i* verifies *AggQC*, extracts the *QC* with the latest/highest view among *QCs* (*highQC*) as well from PREPARE message, and then checks if the proposal is safe. Verification of *AggQC* involves verification of aggregated signatures built from $n - f$ η messages and verification of the latest *PrepareQC*. Signature verification of each *QC* is not necessary, a replica only needs to make sure messages are valid. *BasicSafeProposal* predicate (shown in Algorithm 1 and used in Algorithm 2, line 12) makes sure a replica only accepts a proposal that extends from the *highQC.block*. In other words, a proposal is safe if the primary provides the proof of *highQC* for the *QC* in the proposal.

If a replica notices that it is missing a block, it can download it from other replicas. At the end of PREPARE phase, each replica sends its vote *v* to the primary. Any vote

message *v* sent by a replica to the primary is signed on tuples $\langle type, viewNumber, block, i \rangle$. Each vote has a type, such that $v.type \in \{PREPARE, PRECOMMIT\}$ (Here again block hash can be used to represent the block to save space and bandwidth).

PRECOMMIT phase. The primary collects PREPARE votes from $n - f$ replicas and builds *PrepareQC*. The primary then broadcasts *PrepareQC* to all replicas in PRECOMMIT message. Upon receipt of a valid PRECOMMIT message, a replica will respond with a PRECOMMIT vote to the primary. Here (in line 25-27 Algorithm 2) replica *i* also checks if it has committed the block for *highQC* called *highQC.block*. Since the majority of replicas have voted for *highQC.block*, it is safe to commit it.

COMMIT phase. Similar to PRECOMMIT phase, the primary collects PRECOMMIT votes from $n - f$ replicas and combines them into *PrecommitQC*. As a replica receives and verifies the *PrecommitQC*, it executes the commands. The replica increments *newNumber* and begins the next view.

New-View. Since a replica always receives a message from the primary at a specific viewNumber, therefore, it has to wait for a timeout period during all phases. NEXTVIEW is an auxiliary utility that determines the timeout period. As a replica waits for the receipt of a message (during any phase), if NEXTVIEW (viewNumber) utility interrupts waiting, the replica increments viewNumber and starts the next view.

Efficient View Change. As a replica moves to the next view, it will send its NEWVIEW (η) to the next primary. The primary aggregates $n - f$ η messages and their signatures into an *AggQC* and sends back to all replicas. Upon receipt of a block containing an *AggQC*, first the aggregated signature for the $n - f$ (η) messages needs to be verified. The first check (verification of aggregated signature of *AggQC*) verify that the *AggQC* that is built from η messages has $n - f$ valid *QCs* (*QCs* come from $n - f$ distinct replicas). It further guarantees that at least $f + 1$ *QCs* out of $n - f$ are from correct replicas.

Therefore, a replica only needs to find a *QC* with the highest view among *QCs* in *AggQC* by looping over the view numbers of *QCs*. Next, the replica has to verify the aggregated signature of *highQC* or latest *QC*. As a result, we do not need to verify the remaining $n - f - 1$ *QCs* as a replica only needs to verify *highQC* and make sure if the block extends *highQC.block*. This helps to reduce the signature verification cost for *AggQC* ($n - f$ *QCs*) during view change by the factor of $O(n)$ independent of signature scheme used. This optimization can be used by any two-chain BFT-based consensus protocol during view change where replicas have to receive and process $n - f$ *QCs*.

This optimization can also be used by the primary while receiving η messages. The primary only needs to verify the signature of the sender of the η message and the latest *QC* (*highQC*) among $n - f$ *QCs* (*prepareQC* in η).

While receiving a block with the *AggQC* from the primary, there is a possibility that the η message containing *highQC* is invalid (because the primary is malicious). It means η does not meet formatting requirements, its view number, or the *highQC* is invalid (its aggregated signature cannot be verified). Formatting requirements involve incorrect message types or

Algorithm 2: Basic Fast-HotStuff for replica i

```
1 foreachin curView  $\leftarrow 1, 2, 3, \dots$ 
2   ▷ Prepare Phase
3   if  $i$  is primary then
4     wait until  $(n - f)$   $\eta$  messages are received:
5        $\eta_{Set} \leftarrow \eta_{Set} \cup \eta$ 
6        $aggQC \leftarrow CreateAggQC(\eta_{Set})$ 
7        $B \leftarrow CreatePrepareMsg(Prepare, aggQC, client's$ 
8         command)
9       broadcast  $B$ 
10    end
11    if  $i$  is normal replica then
12      wait for prepare  $B$  from primary(curView)
13       $highQC \leftarrow extract highQc from B.AggQC$ 
14      if BasicSafeProposal( $B, highQC$ ) then
15        Send vote  $v$  for prepare message to
16        primary(curView)
17      end
18    end
19    ▷ Pre-Commit Phase
20    if  $i$  is primary then
21      wait for  $(n - f)$  prepare votes:  $V \leftarrow V \cup v$ 
22       $PrepareQC \leftarrow BasicGenerateQC(V)$ 
23      broadcast  $PrepareQC$ 
24    end
25    if  $i$  is normal replica then
26      wait for  $PrepareQC$  from primary(curView)
27      Send Precommit vote  $v$  to primary(curView)
28      if have not committed  $highQC.block$  then
29        commit  $highQC.block$ 
30      end
31    end
32    ▷ Commit Phase
33    if  $i$  is primary then
34      wait for  $(n - f)$  votes:  $V \leftarrow V \cup v$ 
35       $PrecommitQC \leftarrow GenerateQC(V)$ 
36      broadcast  $PrecommitQC$ 
37    end
38    if  $i$  is normal replica then
39      wait for  $PrecommitQC$  from primary(curView)
40      execute new commands through  $PrecommitQC.block$ 
41      respond to clients
42      ▷ New-View
43      check always for nextView interrupt then
44        goto this line if nextView(curView) is called
45        during "wait for" in any phase
46        Send  $\eta$  to primary( $curView + 1$ )
47      end
48    end
49  end
```

fields. In this case, the replica can reject the block proposal. Furthermore, a replica can use this proof to punish (blacklist) the primary. The proof can be shared with other replicas and a correct primary will use the proof to propose a transaction to blacklist the Byzantine primary [12].

B. Pipelined Fast-HotStuff

Pipelined Fast-HotStuff has been optimized in different ways in comparison to the basic Fast-HotStuff. First, similar to the pipelined HotStuff, it pipelines requests and proposes them in each phase to increase the throughput. Secondly, during normal view change when no primary failure occurs, the protocol only

requires the block to carry a single QC instead of $n - f$ QC s. The proof of *highQC* in pipelined Fast-HotStuff carries a small overhead (*AggQC*) in the block during view v if the primary in view $v - 1$ fails. The pipelined Fast-HotStuff algorithm can be summarized as follows: The primary of the view v collects $n - f$ votes, builds a QC , adds the QC to the block, and propose the block for the view v . If the view $v - 1$, has failed, then the primary, collects $n - f$ η (NEWVIEW) messages. Subsequently, the primary aggregates η messages into *AggQC*, adds *AggQC* to the block and proposes the block for the view v .

Blocks can be added into the chain either during the happy path with no failure or the primary fails, and the next primary will have to add its block into the chain. Unlike HotStuff, pipelined Fast-HotStuff addresses these two cases differently. Indeed, there are two ways a primary can convince replicas that the proposed block extends the *highQC*. In the case of contiguous chain growth (happy path), a primary can only propose a block during the view v if it can build a QC from $n - f$ votes received during the view $v - 1$. Therefore, in a contiguous case, each replica signs the vote, the primary will build a QC from $n - f$ received votes and include it in the next block proposal. Therefore, the block will contain only the QC for view $v - 1$. As a result, for the block during view v , the QC generated from votes in $v - 1$ is the proof of *highQC*. It should be noted that in pipelined Fast-HotStuff, a replica commits a block if two-chain (with the first chain needing to be a direct-chain) is formed over the top of it. Similarly, if a primary during view v did not receive $n - f$ votes from view $v - 1$ (this means the primary during view $v - 1$ has failed), then it can only propose a block if it has received $n - f$ η (NEWVIEW) messages from distinct replicas for view v . In this case, the primary during view v has to propose a block with aggregated QC or *AggQC* from $n - f$ replicas.

The signatures on η are aggregated to generate a single aggregated signature in *AggQC*. Therefore, two types of blocks can be proposed by a primary: a block with QC if the primary is able to build a QC from the previous view or a block with *AggQC* if the previous primary has failed. It should be noted that to verify *AggQC* a replica only needs to verify the aggregated signature of *AggQC* and the *highQC* in the *AggQC* as described previously. The *highQC* can simply be found by looping over view numbers of each QC and choosing the highest one.

The chain structure in pipelined Fast-HotStuff is shown in Figure 7. Here, we can see that upon receipt of block B_{v+2} (during the view $v + 2$), a two-chain with a direct chain is completed for the block B_v . Now a replica can simply execute the block B_v . Since there is no primary failure for views v through view $v + 2$, only *highQC* is included in the block proposal. Similarly, the primary for the view $v + 3$ has failed, therefore, the primary for the view $v + 4$, has to propose a block with *AggQC* (small overhead). Upon receipt of B_{v+4} , the *highQC* can be extracted from *AggQC*. In this case, the QC for the block B_{v+2} has been selected as the *highQC*.

As it can be seen the algorithm for the pipelined Fast-

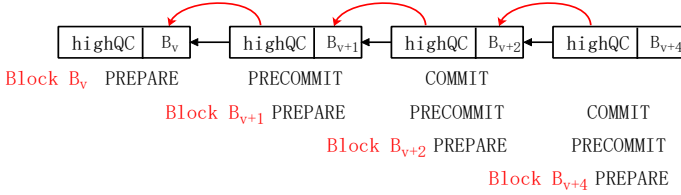


Fig. 7: **Pipeined/Chained Fast-HotStuff** where a QC can serve in different phases simultaneously. Note that the primary for view $v+3$ has failed.

HotStuff mainly has two components: the part executed by the primary and the part run by replicas. The *primary* either receives votes that it will aggregate into a QC or NEWVIEW messages containing QC from $n-f$ replicas that the primary will aggregate into *AggQC* (Algorithm 3 lines 23-25 and 2-9). The primary then builds a proposal in the form of PREPARE message also called a block. PREPARE also contains QC or *AggQC* depending on if it has received $n-f$ votes or NEWVIEW messages (Algorithm 3 lines 2-11). The primary then proposes the block to replicas ((Algorithm 3 line 10)).

Upon receipt of block B (containing a QC) through a proposal, each replica can check the condition $B.viewNumber == B.QC.viewNumber + 1$ and accept the proposal if the condition is met. On the other hand, if the block contains a valid *AggQC*, then each replica extracts the *highQC* from *AggQC* and checks if the block extends the *highQC.block*. These checks are performed through *PipelinedSafeBlock* predicate (Algorithm 1). If the check was successful, each replica sends back a vote to the next primary (Algorithm 3 lines 13-16). After that, each replica commits the grandparent of the received block if a direct-chain is formed between the received block's parent and its grandparent. (Algorithm 3, lines 17-21). Hence, once the commit condition is met for a block in pipelined Fast-HotStuff, the block is committed after two rounds of communication without waiting for the maximum network delay.

Resilience against Forking Attack . Unlike pipelined HotStuff, pipelined Fast-HotStuff is robust to forking attacks. In Fast-HotStuff the primary has to provide the proof of the latest QC (known to the majority of replicas or a QC more recent than the latest one known by the majority of replicas) included in the block. This proof can be provided in two ways. First, if there is no primary failure, then for the proposed block B^* and the QC it contains (qc), we have $B.view = qc.view + 1$. Secondly, if there is a primary failure in the previous view then the primary has to include the *AggQC* ($n-f$ QCs). This guarantees at least one of the QCs in the *AggQC* is the latest QC held by the majority of replicas or a QC higher than the latest QC being held by the majority of replicas. The inclusion of proof within the block prevents the primary from using an old QC to generate forks. If a primary does not provide appropriate proof, its proposal can be rejected. Furthermore, such a proposal can be used as proof to blacklist the primary (by proposing a blacklisting transaction with the proof).

Algorithm 3: pipelined Fast-HotStuff for block i

```

1 foreachin curView  $\leftarrow 1, 2, 3, \dots$ 
2   if  $i$  is primary then
3     if  $n-f$   $\eta$  msgs are received then
4        $aggQC \leftarrow CreateAggQC(\eta_{Set})$ 
5        $B \leftarrow CreatePrepareMsg(Prepare, aggQC, \perp, client's\ command)$ 
6     end
7     if  $n-f$   $v$  msgs are received then
8        $qc \leftarrow GenerateQC(V)$ 
9        $CreatePrepareMsg(Prepare, \perp, qc, client's\ command)$ 
10    end
11    broadcast  $B$ 
12  end
13  if  $i$  is normal replica then
14    wait for  $B$  from primary( $curView$ )
15    if  $PipelinedSafeBlock(B, B.qc, \perp) \vee$ 
16       $PipelinedSafeBlock(B, \perp, B.aggQC)$  then
17      Send vote  $v$  for prepare message to
18      primary( $curView+1$ )
19    end
20    // start commit phase on  $B^*$ 's grandparent if a direct
21    chain exists between  $B^*$ 's parent and grandparent
22    if  $(B^*.parent = B'') \wedge (B''.parent = B') \wedge B''.view =$ 
23       $B'.view + 1$  then
24      execute new commands through  $B'$ 
25      respond to clients
26    end
27  end
28  if  $i$  is next primary then
29    wait until  $(n-f) v/\eta$  for current view are received:
30     $\eta_{Set} \leftarrow \eta_{Set} \cup \eta \vee V \leftarrow V \cup v$ 
31  end
32  ▷ Finally
33  check always for nextView interrupt then
34    goto this line if nextView( $curView$ ) is called during
35    "wait for" in any phase
36    Send  $\eta$  to primary( $curView + 1$ )
37  end

```

VI. PROOF OF CORRECTNESS FOR HOTSTUFF

A. Correctness Proof for Basic Fast-HotStuff

Correctness of a consensus protocol involves proof of safety and liveness. Safety and liveness are the two important properties of consensus algorithms. In this section, we provide proof of the safety and liveness properties of Fast-HotStuff. A proposal of view v being committed by a replica i means that the network has decided on the proposal. The node i can execute the proposal to update its state, which reflects the ordered execution of the predecessor proposals. We begin with two standard definitions.

Definition 1 (Safety). A protocol is safe if the following statement holds: if at least one correct replica commits a block at the sequence (blockchain height) s in the presence of f Byzantine replicas, then no other block will ever be committed at the sequence s .

Definition 2 (Liveness). A protocol is live if it guarantees progress in the presence of at most f Byzantine replicas.

Next, we introduce several technical lemmas. The first lemma shows that for each view, at most one block can get certified (get $n - f$ votes).

Lemma 1. *If any two valid QCs, qc_1 and qc_2 with same type $qc_1.type = qc_2.type$ and conflicting blocks i.e., $qc_1.block = B$ conflicts with $qc_2.block = B'$, then we have $qc_1.viewNumber \neq qc_2.viewNumber$.*

Proof. We can prove this lemma by contradiction. Furthermore, we assume that $qc_1.viewNumber = qc_2.viewNumber$. Now let's consider, N_1 is a set of replicas that have voted for block B in qc_1 ($|N_1| \geq 2f + 1$). Similarly, N_2 is another set of replicas that have voted for block B' and whose votes are included in qc_2 ($|N_2| \geq 2f + 1$). Since $n = 3f + 1$ and $f = \frac{n-1}{3}$, this means there is at least one correct replica j such that $j \in N_1 \cap N_2$ (which means j has voted for both qc_1 and qc_2). But a correct replica only votes once for each phase in each view. Therefore, our assumption is false, and hence, $qc_1.viewNumber \neq qc_2.viewNumber$. \square

The second lemma proves that if a single replica has committed a block at the view v then all other replicas will commit the same block at the view v .

Lemma 2. *If at least one correct replica i has received PrecommitQC for block B (committed block B), then the PrepareQC for block B will be the highQC for next (child of block B) block B' .*

Proof. The primary begins with a new view $v + 1$ as it receives $n - f$ NEWVIEW messages. Here for ease of understanding, we assume $v + 1$. B' could have been proposed during any view $v' > v$. We show that any combination of $n - f$ NEWVIEW messages have at least one of those NEWVIEW message received by the primary containing highQC (PrepareQC for block B) for block B .

We know that in the previous view v , replica i has committed block B . This means a set of replicas R_1 of size $|R_1| \geq 2f + 1$ have voted for PrepareQC (which is built from votes for block B). Similarly, another set of replicas R_2 of size $|R_2| \geq 2f + 1$ have sent their NEWVIEW messages to the primary of view $v + 1$ after the end of view v . Since the total number of replicas is $n = 3f + 1$ and $f = \frac{n-1}{3}$, therefore, $R_1 \cap R_2 = R$, such that, $|R| \geq f + 1$, which means that there is at least one correct replica in R_2 that has sent its PrepareQC as highQC in NEWVIEW message to the primary. Therefore, when primary of view $v + 1$ proposes B' , the PrepareQC for block B will be the highQC. In other words, B' will point to B as its parent (through highQC). \square

The third lemma proves that if a replica commits a block, then it will not be reverted.

Lemma 3. *A correct replica will not commit two conflicting blocks.*

Proof. From lemma 1 we know that each correct replica votes only once for each view and therefore view number for conflicting blocks B and B' will not be the same. Therefore,

we can assume that $B.curView < B'.curView$. Based on lemma 2 we know that if at least one correct replica has received PrecommitQC for block B (have committed B), then the PrepareQC for block B will be the highQC for the next block B' (child of block B). Therefore, any combination of $n - f$ PrepareQCs in AggQC for B' will include at least one highQC such that $highQC.block = B$ or $highQC.block.view = B.view$. But for B' to be conflicting with B it has to point to the parent of B at least. Consequently, first, it is not possible for a primary to build a valid PREPARE message B' in which $highQC.block.view < B.view$. Secondly, if a primary tries to propose a block with invalid AggQC, it will be rejected by the replica based on Algorithm 2 line 12. \square

Lemmas 1, 2 and 3 provide a safety (Definition 1) proof for basic Fast-HotStuff consensus protocol. To ensure liveness (Definition 2), Fast-HotStuff has to make sure in each view a replica is selected as a primary deterministically (eventually rotating through all replicas) and the view number is incremented. Moreover, we should also show that the protocol will eventually add a block to the chain/tree of blocks (a block to the blockchain) or will result in view change in the case of failure.

The NEXTVIEW maintains the timeout value (interval), and the timer is set upon entering a view. If a replica times out (without reaching a decision), it can employ exponential-backoff used in PBFT [1] to double its timeout value and calls the NEXTVIEW (to advance the view). This guarantees that eventually after GST there will be a period of synchrony when timeout values from all correct replicas overlap for a long enough interval (T_f), the primary will be correct and at least $n - f$ honest/correct replicas will be in the same view. As a result, it can be shown that this period is enough to reach a decision during consensus. Below we provide liveness (Definition 2) proof for our Fast-HotStuff protocol.

Lemma 4. *After GST, there is a time T_f , when there is a correct primary and all correct/honest replicas are in the same view. As a result, a decision is reached during T_f .*

Proof. Based on Lemma 2, at the beginning of a view, the primary will have the latest PrepareQC or highQC from $n - f$ replicas. As per assumption, after GST the period that T_f bound on message delivery holds is sufficiently large. Therefore, when all correct replicas are in the same view (due to exponential-backoff as explained), the correct primary will propose a PREPARE message with AggQC containing the latest PrepareQC, which is extracted by each replica. Since all replicas are in the same view until bounded T_f time, therefore all replicas can successfully complete PREPARE, PRECOMMIT, and COMMIT phase. \square

B. Correctness Proof for Pipelined Fast-HotStuff

We can establish the safety (Definition 1) and liveness (Definition 2) of pipelined Fast-HotStuff in a way similar to what we have proven for the basic Fast-HotStuff. For safety, we want to prove that if a block is committed by a replica,

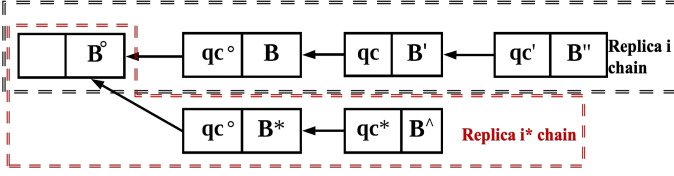


Fig. 8: Safety violation scenario.

then it will never be revoked. Moreover, if a replica commits a block then all other replicas will eventually commit the same block at the same block sequence/height.

Lemma 5. *If B and B' are two conflicting blocks, then only one of them will be committed by a correct replica.*

Proof. From lemma 1, we know that each correct replica votes only once for each view and therefore view number for conflicting blocks $B.curView < B'.curView$ and we assume that block B is already committed. Now, a replica r receives a PREPARE message in the form of block B' . Since B' is a conflicting block to B therefore, the *highQC* in the block must point to an ancestor of block B . In this case we consider B^* as the parent of B ($B.parent = B^*$) and $B'.QC.block = B^*$. In case of *AggQC*, since B' extends from B^* which is parent of B , therefore first condition in *PipelinedSafeBlock* predicate fails because *highQC* in B' ($B'.QC$) extends the parent of B (B^*) but not B (invalid *AggQC*). Any valid *AggQC* will have at least one *QC* for block B or any other block that extends from block B (Lemma 2). Similarly, second condition in *PipelinedSafeBlock* predicate also fails because $B'.viewNumber = B'.QC.viewNumber + k$, where $k > 1$. \square

Lemma 6. *If a block B is committed by a correct replica i , then no other correct replica i^* in the network will commit another block B^* that conflicts with the block B .*

Proof. For the sake of contradiction let's assume that it is possible that if a block B is committed only by a single correct replica i then at least one another correct replica i^* can commit another block B^* which conflicts with the block B . The chain of each replica i and i^* is given in the Figure 8. Now we analyze different cases that arise from our assumption.

Case 1: When $qc^*.view < qc.view$. In this case, since $qc^*.view < qc.view$ therefore, $qc^*.view < highQC.view$. As a result, qc^* will not be selected as *highQC* by any correct replica (based on Lemma 2).

Case 2: When $qc^*.view == qc.view$. Two *QCs* pointing to two different blocks cannot be the same.

Case 3: When $qc'.view > qc^*.view > qc.view$. In the third case, there is a possibility that several replicas hold a *QC* qc^* such that $qc^*.view > qc.view$. qc^* has not been propagated to the majority of correct replicas due to the network partition. The $qc^*.block = B^*$ is conflicting block to block B . After the view change the new primary p (that is aware of qc^*) includes qc^* in the *AggQC*. If qc^* is accepted, then other replicas may prefer replica i^* 's chain (colored in red in Figure 8). As a

result, replicas may commit the block B^* which is conflicting to block B . But this is not possible due to the two-direct chain requirements to commit a block ($qc.view + 1 = qc'.view$) in Algorithm 3 lines 18-20. Therefore, there can be no such qc^* , with a view $qc'.view > qc^*.view > qc.view$ when replica i has committed the block B .

Case 4: When $qc^*.view == qc'.view$. Two *QCs* pointing to two different blocks cannot be the same.

Case 5: When $qc^*.view > qc'.view$. We know that qc' has been built from $n - f$ replica votes that have seen the qc . Therefore, the qc is the *highQC* for $n - f$ replicas of which at least $f + 1$ are correct. Hence, when the primary collect $n - f$ η messages (NEWVIEW) during view change at least one of η will contain qc or a *QC* that extends the qc (based on Lemma 2). Therefore, qc^* that does not extend qc will not be formed. Hence, our assumption is proved to be false. Therefore, if a block is committed by a correct replica i , then no other conflicting block can be committed by any other correct replica. \square

This lemma confirms that if a single replica commits a block B , then no conflicting block to B will be committed by another replica. This lemma is developed to address a subtle safety violation scenario due to the network partition that was reported in Gemini [27] (that simulates Byzantine scenarios at scale) by Facebook's Novi group. We also successfully verified the safety of Fast-HotStuff using the Twins simulator for Fast-HotStuff developed by Novi team⁸.

Lemma 7. *After GST, there is a time T_f , when there are at least two consecutive correct primaries and all correct/honest replicas are in the same view. As a result, a decision will eventually reach.*

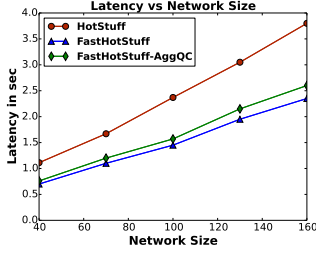
Proof. As T_f period is sufficiently large after the GST, while two correct primaries are selected consecutively and correct replicas are in the same view, a one-direct chain will be formed between blocks proposed by the correct primaries. Since two-chain (with the first chain as one-direct chain) are required for a block to get committed, the third block will eventually be added by another correct primary. For brevity, more details about pipelined Fast-HotStuff liveness are presented in the Appendix. \square

VII. EVALUATION

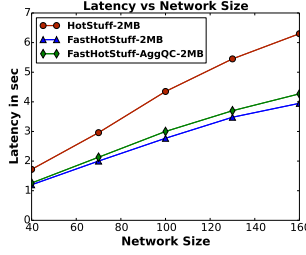
As pipelined HotStuff is widely adopted due to its higher throughput, we implemented prototypes of pipelined Fast-HotStuff and pipelined HotStuff using the Go programming language. For cryptographic operations, we used dedis advanced crypto library in Go [28]. Dedis library supports both BLS aggregated signatures as well as threshold signatures (used during evaluation) [17]. Moreover, for hashing values, we used SHA256 hashing in the Go crypto library⁹. We tested Fast-HotStuff's performance on Amazon cloud (AWS) with different

⁸<https://github.com/asonnino/twins-simulator>

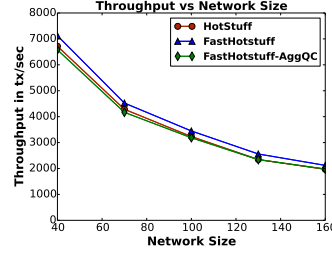
⁹<https://golang.org/pkg/crypto/sha256/>



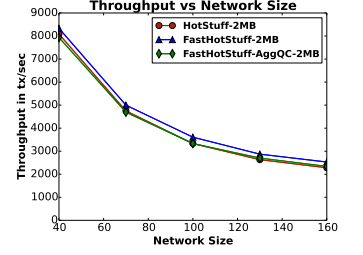
(a) Latency for 1MB Block Size



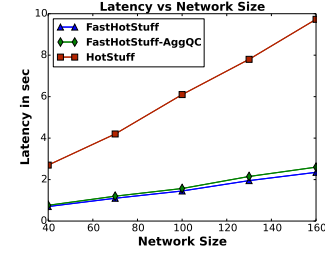
(b) Latency for 2MB Block Size



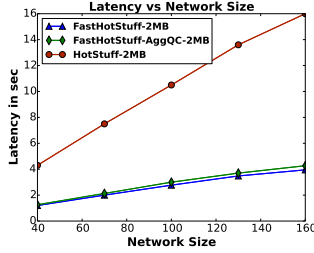
(a) Throughput for 1MB Block Size



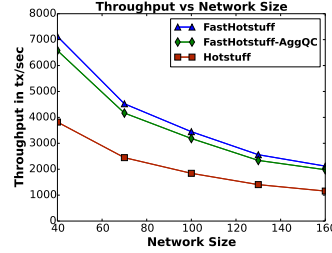
(b) Throughput for 2MB Block Size



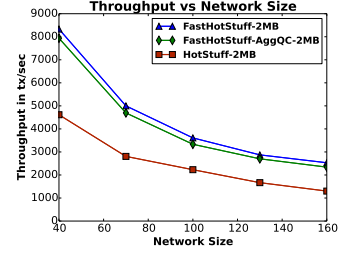
(c) The Latency under the Forking Attack for 1MB Block Size.



(d) The Latency under the Forking Attack for 2MB Block Size.



(c) The Throughput under the Forking Attack for 1MB Block Size.



(d) The Throughput under the Forking Attack for 2MB Block Size.

Fig. 9: The latency comparison of HotStuff and Fast-HotStuff in LAN environment.

Fig. 10: The Throughput comparison of HotStuff and Fast-HotStuff in LAN environment.

network sizes 40, 70, 100, 130, 160 (to compare performance and scalability) and different block sizes (1MB and 2MB). We used *t2.micro* replicas in AWS, where each replica has a single vCPU (virtual CPU) comparable to a single core with 1GB memory. The bandwidth was set to 500 Mb/sec (62.5 MB/sec) and the latency between two endpoints was set to 50 msec. We also performed forking a attack on each network of different sizes, $k = 1000$ times, and took the mean of the average throughput of the network and the latency incurred by blocks affected by this attack.

We compared pipelined Fast-HotStuff's performance (throughput and latency) against pipelined HotStuff in three scenarios: 1) during happy path (when no failure occurs), therefore, the primary only includes the *QC* in the block (red vs blue curves), 2) when the previous primary fails and the next primary in the Fast-HotStuff has to include the aggregated *QC* ($(n - f)$ *QCs*) in the block (red vs green curves), and 3) when HotStuff and Fast-HotStuff come under forking attack. Results achieved from each case are discussed below:

- 1) As the results shown in Figure 9(a) and 9(b), during happy path when no failure occurs, Fast-HotStuff outperforms HotStuff in terms of latency. HotStuff's throughput (in red) slightly decreases against Fast-HotStuff's throughput (in blue) due to $O(n^2)$ time complexity for interpolation calculation at the primary (for threshold signatures in HotStuff) when n increases (Figure 10(a) and 10(b)).
- 2) We did not consider the timeout period taken by replicas to recover, as our main objective is to show that even

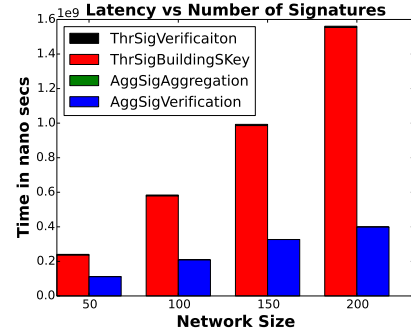
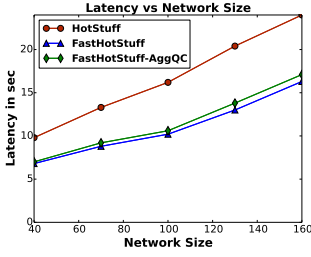
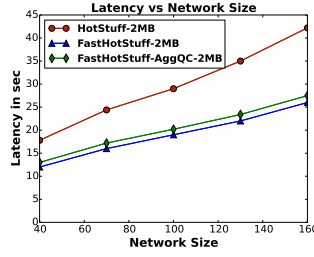


Fig. 11: Comparing threshold and Aggregated Signature Latency.

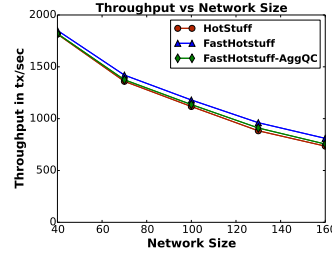
the inclusion of aggregated *QC* (small overhead) after a primary failure has a negligible effect on pipelined Fast-HotStuff's performance. Therefore, just after GST (after primary failure), when an honest (correct) primary is selected, HotStuff does not incur additional overhead. However, HotStuff needs an additional round of consensus during happy (normal) as well as unhappy (failure) cases in comparison to Fast-HotStuff. As a result, the throughput and latency of HotStuff during the happy path or unhappy path just after primary failure is the same and is shown by the red curve (by ignoring the timeout period). Though, Fast-HotStuff's throughput slightly decreases, due to the *AggQC* (a small overhead) as shown in 10(a) and 10(b), but the throughput is still comparable to the HotStuff throughput. On the other



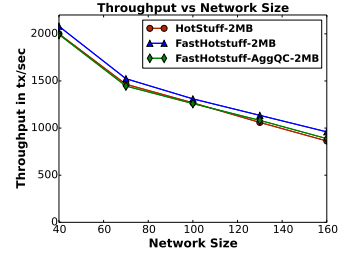
(a) Latency for 1MB Block Size



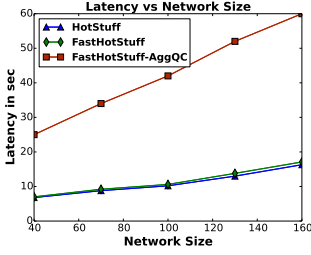
(b) Latency for 2MB Block Size



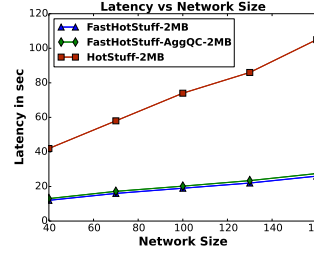
(a) Throughput for 1MB Block Size



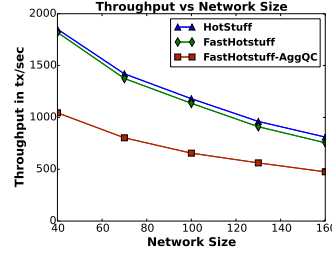
(b) Throughput for 2MB Block Size



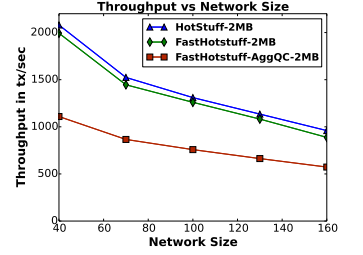
(c) The Latency under the Forking Attack for 1MB Block Size.



(d) The Latency under the Forking Attack for 2MB Block Size.



(c) The Throughput under the Forking Attack for 1MB Block Size.



(d) The Throughput under the Forking Attack for 2MB Block Size.

Fig. 12: The latency comparison of HotStuff and Fast-HotStuff in WAN environment.

Fig. 13: The Throughput comparison of HotStuff and Fast-HotStuff in WAN environment.

hand, Fast-HotStuff's latency (in green) is lower than HotStuff's latency (in red) as shown in Figure 9(a) and Figure 9(b).

- 3) Forking attack effects in Fast-HotStuff and HotStuff can be observed in Figure 9(c) and 9(d) and Figure 10(c) and 10(d). Forking attack (the use of older QC in a block) is allowed in HotStuff, but since forking is not allowed in Fast-HotStuff, the proposal will be rejected and the proposer will not be chosen again. Hence, forking attack has no significant effect on Fast-Hotstuf performance.

Choice of Signatures HotStuff uses t -out-of- n threshold signatures [17] and the Fast-HotStuff uses aggregated signatures as stated previously. To better understand the effects of signature schemes on each protocol's performance, we also compared the latency caused by each signature type during consensus. Higher latency caused by cryptographic operations during consensus will result in higher latency and lower throughput.

In both aggregated signature (used in Fast-HotStuff) as well as threshold signature (used in HotStuff) there are three main steps for signature verification in HotStuff and Fast-HotStuff. First, each replica signs a message (vote, *NEWVIEW*) and sends it to the primary. Second, the primary build an aggregated signature or threshold signature from $n - f$ messages received from distinct replicas and sends it back to each replica. Third, each replica verifies the aggregated or threshold signature associated with the messages received from the primary. The cost for the first step is small and constant (for constant size message) for both threshold signature as well as aggregated

signature. Therefore, we ignore this cost. The computation cost of aggregating signatures into a single constant size aggregated signature by the primary replica in Fast-HotStuff is small, resulting in a negligible delay. It is shown by the green bar stacked over top of the blue bar in Figure 11. But since the time taken by signature aggregation in Fast-HotStuff's primary is so small, it is hardly visible in the graph. However, the cost of building the threshold signature from $n - f$ partial signatures received by the primary replica in HotStuff from $n - f$ replicas (shown by the red bar) in the threshold signatures in HotStuff is quadratic as it uses $O(t^2)$ ($t = n - f$) time polynomial interpolation. Conversely, the computation cost of verification in threshold signature is small per replica, shown by the black bar stacked over the red bar in Figure 11. However, the cost of verifying aggregated signature in the aggregated signature scheme is linear, resulting in a linear delay shown by the blue bar. In summary, we can see that building threshold signatures in the primary from partial signatures is expensive in threshold signatures. Although threshold signatures have constant verification costs, the latency induced in the primary prevents threshold signatures from having performance gain in comparison to the aggregated signature scheme.

WAN Performance Furthermore, to better understand the effect of high latency over the Wide Area Network (WAN), we did performance tests over the Wide Area Network (WAN). Nodes are arranged in three different AWS regions including US-East-1 (North Virginia) region, EU-Central-1 (Frankfurt), and US-East-1 (North Virginia). The latency between the US-East-1 (North Virginia) region and EU-Central-1 (Frankfurt)

was 88ms, US-East-1 (North Virginia) and South-America-East-1 (Sao-Paulo) was 140ms and EU-Central-1 (Frankfurt), and South-America-East-1 (Sao-Paulo) was 227ms. It can be seen both protocols experience lower throughput over the WAN in comparison to the throughput within a single data center.

Similarly, in the WAN setting, Fast-HotStuff has lower latency than the HotStuff (as shown in Figure 12(a) and 12(b)). During the normal case, a block of 1MB in HotStuff will take at most 8 seconds (approximately) more than a 1MB block in Fast-HotStuff (with network size 160). This means clients have to wait for an additional 8 seconds to get transaction confirmation. But the situation can get worse if a forking attack is performed by Byzantine nodes (shown in the Figure 12(c)). In such a case, on average a single block can take additional 40 seconds to get confirmed. This additional block confirmation time in HotStuff can reach more than 16 seconds during normal cases and more than 70 seconds when a forking attack is performed with a 2MB block size (with network size 160) as shown in Figure 12(d). This high latency is due to the reason that in chained HotStuff four blocks (with at least the first three with consecutive views also called two-direct chain) have to be added for the first block (among the four) to get committed. But during the forking attack, the chain of blocks from consecutive views breaks, hence the network has to wait for the completion of the *two-direct chain* condition to meet so that block/s can get committed. Similarly, HotStuff's throughput in WAN is comparable with the Fast-HotStuff's throughput but significantly degrades under a forking attack (as shown in Figure 13).

VIII. RELATED WORK

There have been multiple works on improving BFT protocols performance and scalability [2], [4], [13]. But these protocols suffer from expensive view changes where either the message complexity or the number of signatures/authenticators to be verified grows quadratically. Moreover, these protocols do not employ a primary rotation mechanism. Current solutions (see Table I) suffer from at least one of the shortfalls below.

Lack of optimistic responsiveness Protocols that offer a simple mechanism of leader/primary replacement include Casper [6] and Tendermint [5]. But both of these protocols have synchronous cores, where, replicas in the network have to wait for the maximum network latency before moving to the next round. In other words, these protocols lack responsiveness, which will result in high-performance degradation. The BFT consensus protocol proposed in [29] is responsive if the number of Byzantine replicas is less than $n/4$ ($f < n/4$). The protocol loses responsiveness and waits for the maximum network delay, when $f \geq n/4$. Fast-HotStuff is always responsive regardless of the value of f and can tolerate $f < n/3$ Byzantine replicas.

Expensive View Change PBFT [1] has quadratic message complexity during happy path or normal operation. During view change, each replica has to process at least $O(n^2)$ signatures. Moreover, PBFT does not use a rotating primary. On the other hand, Fast-HotStuff uses a rotating primary, pipelined Fast-HotStuff has linear view change during normal primary rotation

(view change). In case of failure, primary rotation in Fast-HotStuff in each replica has to process only two aggregated signatures.

SBFT [2] has linear communication complexity during normal operation. SBFT does not employ a rotating primary mechanism. When Fast-HotStuff and SBFT use the same signature scheme, replicas in Fast-HotStuff will have to verify $O(n)$ signatures less than the SBFT.

To address the higher latency and vulnerability to the forking attack, in a concurrent research effort DiemBFT has switched to a two-chain protocol in its new release. During the normal phase, the new DiemBFT(V4) behaves similar to the Fast-HotStuff, it employs PBFT [1] based quadratic view change (as an intermediary solution). Fast-HotStuff has $O(n)$ times lower signature verification cost, during the unhappy path than this variant of DiemBFT(v4). As a further improvement, the DiemBFT is implementing the asynchronous fallback from [30] for the view change so that the protocol can even make progress in the event of asynchrony (including Denial-of-Service attacks on the primary).

While asynchronous view change improves resilience, it suffers from high bit complexity. For example, for a network of $n = 100$ replicas with the block size as $b_s = 1MB$, the total number of bits sent by the primary is $n \times b_s + n \times 1.4 \times \frac{b_s}{100} = 100MB + n \times \frac{1.4MB}{100} = 101.4MB$ (block plus overhead sent to n replicas). The added overhead in this case in Fast-HotStuff is $n \times 1.4MB/100 = 1.4MB$. For a proposal in [30] since each replica has to broadcast a block of size b_s , therefore n replicas broadcast n blocks out of which only one block will eventually be added to the chain. In this case, we have $n \times n \times b_s = 100 \times 100 \times 1MB = 10^4MB$ complexity. Therefore, $10^4 MB$ data have to be exchanged for a single block of 1MB to be committed (by each one of 100 replicas). Hence, only 100 MB of data is being consumed (committed) by the network. The additional $10^4 - 100 = 9900MB$ is overhead. Therefore, all resources involved in the transmission and processing of this large amount of data are wasted. Hence, in the above-mentioned setup, the view change overhead in Fast-HotStuff, though quadratic, is 1.4MB whereas, in [30] is 9900MB. Similarly, in the Fast-HotStuff, signature verification cost during view change is $O(n)$ times lower than this variant of DiemBFT(v4). As a result, deployment of this protocol [30] (as a variant of DiemBFT(v4)) will require high resources including bandwidth, processor (as each transaction within block and signatures have to be verified), and memory (for keeping blocks until only one chain is selected). Moreover, values of n and b_s have to remain in check.

Suboptimal latency HotStuff [7] is designed to not only keep a simple leader change process but also maintain responsiveness. These features along with the pipelining optimization have provided an opportunity for wide adoption of the HotStuff [8] protocol. HotStuff has linear view change, but we show that in practice during primary failure (unhappy path) Fast-HotStuff's view change performance is comparable to HotStuff. LibraBFT (DiemBFT) [8] is a variant of HotStuff. Unlike the HotStuff which uses threshold signatures, LibraBFT uses

TABLE I. Comparison of BFT Protocols

Protocol	Authenticators Sent During View Change	Optimistic Responsiveness	# of Rounds During Happy Path	Leader Paradigm	Authenticators Verified during View Change	# of Rounds from View Change to receiving first block
PBFT [1]	$O(n^2)$ or $O(n^3)$	Yes	2	stable	$O(n^2)$ or $O(n^3)$	2
SBFT [2]	$O(n^2)$	Yes	1-2	stable	$O(n^2)$	2
Tendermint [5]	$O(n)$	No	2	Rotating	$O(n)$	1
Casper FFG [6]	$O(n)$	No	2	Rotating	$O(n)$	1
HotStuff [7]	$O(n)$	Yes	3	Rotating	$O(n)$	1
LibraBFT (DiemBFT)	$O(n)$	Yes	3	Rotating	$O(n)$	1
Fast-HotStuff	$O(n)$ or $O(n^2)$	Yes	2	Rotating	$O(n)$	1

aggregated signatures. LibraBFT uses broadcasting during primary failure. LibraBFT also has a three-chain structure and is susceptible to forking attacks.

View change latency View change latency cannot be bounded during the asynchronous period. Therefore, we consider the number of rounds when a replica intends to change the view to the first time it receives a proposal from a correct primary (during the period of synchrony). This period can determine how quickly the protocol recovers when synchrony conditions meet in the presence of a correct primary. It takes two rounds by a replica running PBFT or SBFT to receive the first proposal while having a successful view change.

Another beautiful concurrent work (Wendy) in [23] has also addressed the higher latency during the happy path in HotStuff while supporting rotating primary. Wendy has successfully avoided the quadratic authenticator complexity during the view change while maintaining only two rounds of latency during the happy path. The tradeoff Wendy has made is that if the failed primary or the new (selected) primary (when less than $f+1$ correct nodes are holding locks) is Byzantine, then it can force the protocol to incur additional latency costs during the view change (in terms of the number of rounds). Furthermore, the paper also assumes that there is a known fixed bound on the difference among the views of replicas in the network. On the other hand, Fast-HotStuff is resilient against such performance attacks and does not have such an assumption. By contrast, the tradeoff Fast-HotStuff has made is that a primary has to send $O(n^2)$ authenticators after a view change. And we showed that the bandwidth cost of this overhead is small in practice and improved the signature verification of the protocol by $O(n)$.

The verification cost of authenticators depends on the type of signature schemes used by the protocol. For example, the verification cost of aggregated signatures is linear to the number of signatures being aggregated. Whereas, the verification cost of threshold signatures is constant. But on the other hand, as previously observed during experiments, the quadratic computational cost of Lagrange interpolation adds additional latency to the protocol. Lagrange interpolation is used by the primary to build a threshold signature from partial signatures.

As a result, the constant size and verification cost of threshold signatures do not benefit the protocol performance. Though a recent work [31] has tried to address the high computational cost of interpolation in threshold signatures with a tradeoff in verification and communication cost.

IX. CONCLUSION

In this paper, we presented Fast-HotStuff which is a two-chain consensus protocol with efficient and simplified view change. It achieves consensus in two rounds of communication. Moreover, Fast-HotStuff is robust against forking attacks. Whereas HotStuff lacks resilience against forking attacks. Fast-HotStuff achieves these unique advantages by adding a small amount of overhead in the block. This overhead is only required in rare situations when a primary fails. Our experimental results show that whether the overhead is included in the proposed block or not, Fast-HotStuff outperforms HotStuff in terms of latency. Fast-HotStuff outperforms HotStuff in terms of latency and throughput under forking attacks.

REFERENCES

- [1] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in *Proceedings of the Third Symposium on Operating Systems Design and Implementation*, ser. OSDI '99. Berkeley, CA, USA: USENIX Association, 1999, pp. 173–186.
- [2] G. Golan-Gueta, I. Abraham, S. Grossman, D. Malkhi, B. Pinkas, M. K. Reiter, D. Seredinschi, O. Tamir, and A. Tomescu, "SBFT: a scalable decentralized trust infrastructure for blockchains," *CoRR*, vol. abs/1804.01626, 2018.
- [3] R. Kotla, A. Clement, E. Wong, L. Alvisi, and M. Dahlin, "Zyzyva: Speculative Byzantine fault tolerance," *Commun. ACM*, vol. 51, no. 11, pp. 86–95, Nov. 2008.
- [4] A. Bessani, J. Sousa, and E. E. P. Alchieri, "State machine replication for the masses with bft-smart," in *2014 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, 2014, pp. 355–362.
- [5] E. Buchman, "Tendermint: Byzantine fault tolerance in the age of blockchains," Jun 2016.
- [6] V. Buterin and V. Griffith, "Casper the friendly finality gadget," *arXiv preprint arXiv:1710.09437*, 2017.
- [7] M. Yin, D. Malkhi, M. K. Reiter, G. G. Gueta, and I. Abraham, "Hotstuff: Bft consensus with linearity and responsiveness," in *Proceedings of the 2019 ACM PODC*, ser. PODC '19. New York, NY, USA: Association for Computing Machinery, 2019, p. 347–356.
- [8] M. Baudet, A. Ching, A. Chursin, G. Danezis, F. Garillot, Z. Li, D. Malkhi, O. Naor, D. Perelman, and A. Sonnino, "State machine replication in the libra blockchain," 2019.

- [9] A. Hentschel, Y. Hassanzadeh-Nazarabadi, R. M. Seraj, D. Shirley, and L. Lafrance, "Flow: Separating consensus and compute - block formation and execution," *ArXiv*, vol. abs/2002.07403, 2020.
- [10] Y. Guo, Q. Yang, H. Zhou, W. Lu, and S. Zeng, "System and methods for selection and utilizing a committee of validator nodes in a distributed system," *Cypherium Blockchain*, Feb 2020, patent.
- [11] T.-H. H. Chan, R. Pass, and E. Shi, "Pala: A simple partially synchronous blockchain," *Cryptology ePrint Archive*, Report 2018/981, 2018, <https://eprint.iacr.org/2018/981>.
- [12] M. Jalalzai, C. Feng, C. Busch, G. R. III, and J. Niu, "The hermes bft for blockchains," *IEEE Transactions on Dependable and Secure Computing*, no. 01, pp. 1–1, sep 5555.
- [13] M. M. Jalalzai and C. Busch, "Window based BFT blockchain consensus," in *iThings, IEEE GreenCom, IEEE (CPSCoM) and IEEE SSmartData 2018*, July 2018, pp. 971–979.
- [14] Y. Amir, B. Coan, J. Kirsch, and J. Lane, "Byzantine replication under attack," in *2008 IEEE International Conference on Dependable Systems and Networks With FTCS and DCC (DSN)*, vol. 00, June 2008, pp. 197–206. [Online]. Available: doi.ieeecomputersociety.org/10.1109/DSN.2008.4630088
- [15] M. M. Jalalzai, C. Busch, and G. G. Richard, "Proteus: A scalable bft consensus protocol for blockchains," in *2019 IEEE International Conference on Blockchain (Blockchain)*, 2019, pp. 308–313.
- [16] C. Dwork, N. Lynch, and L. Stockmeyer, "Consensus in the presence of partial synchrony," *J. ACM*, vol. 35, no. 2, pp. 288–323, Apr. 1988.
- [17] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," in *Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology*, ser. ASIACRYPT '01. Berlin, Heidelberg: Springer-Verlag, 2001, p. 514–532.
- [18] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and verifiably encrypted signatures from bilinear maps," in *Proceedings of the 22nd International Conference on Theory and Applications of Cryptographic Techniques*. Berlin, Heidelberg: Springer-Verlag, 2003, pp. 416–432.
- [19] D. Boneh, M. Drijvers, and G. Neven, "Compact multi-signatures for smaller blockchains," in *Advances in Cryptology – ASIACRYPT 2018*, T. Peyrin and S. Galbraith, Eds. Cham: Springer International Publishing, 2018, pp. 435–464.
- [20] L. Lamport, R. Shostak, and M. Pease, "The Byzantine generals problem," *ACM Trans. Program. Lang. Syst.*, vol. 4, no. 3, pp. 382–401, Jul. 1982.
- [21] C. Cachin, K. Kursawe, and V. Shoup, "Random oracles in constantinople: Practical asynchronous Byzantine agreement using cryptography," *J. Cryptol.*, vol. 18, no. 3, pp. 219–246, Jul. 2005.
- [22] V. Shoup, "Practical threshold signatures," in *Proceedings of the 19th International Conference on Theory and Application of Cryptographic Techniques*, ser. EUROCRYPT'00. Berlin, Heidelberg: Springer-Verlag, 2000, p. 207–220.
- [23] N. Giridharan, H. Howard, I. Abraham, N. Crooks, and A. Tomescu, "No-commit proofs: Defeating livelock in bft," *Cryptology ePrint Archive*, Paper 2021/1308, 2021, <https://eprint.iacr.org/2021/1308>. [Online]. Available: <https://eprint.iacr.org/2021/1308>
- [24] J. Niu, F. Gai, M. M. Jalalzai, and C. Feng, "On the performance of pipelined hotstuff," in *IEEE INFOCOM 2021 - IEEE Conference on Computer Communications*, 2021, pp. 1–10.
- [25] M. O. Rabin, "Randomized byzantine generals," in *24th Annual Symposium on Foundations of Computer Science (sfcs 1983)*, 1983, pp. 403–409.
- [26] C. Cachin, K. Kursawe, and V. Shoup, "Random oracles in constantinople: Practical asynchronous byzantine agreement using cryptography," *J. Cryptol.*, vol. 18, no. 3, p. 219–246, Jul. 2005.
- [27] S. Bano, A. Sonnino, A. Chursin, D. Perelman, Z. Li, A. Ching, and D. Malkhi, "Gemini: Bft systems made robust."
- [28] P. Jovanovic, J. R. Allen, T. Bowers, and G. Bosson, "dedis kyber," 2020.
- [29] N. Shrestha, I. Abraham, L. Ren, and K. Nayak, "On the optimality of optimistic responsiveness," in *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '20. New York, NY, USA: Association for Computing Machinery, 2020, p. 839–857. [Online]. Available: <https://doi.org/10.1145/3372297.3417284>
- [30] R. Gelashvili, L. Kokoris-Kogias, A. Sonnino, A. Spiegelman, and Z. Xiang, "Jolteon and ditto: Network-adaptive efficient consensus with asynchronous fallback," 2021.
- [31] A. Tomescu, R. Chen, Y. Zheng, I. Abraham, B. Pinkas, G. G. Gueta, and S. Devadas, "Towards scalable threshold cryptosystems," in *2020 IEEE Symposium on Security and Privacy (SP)*, 2020, pp. 877–893.
- [32] M. Correia, A. N. Bessani, L. C. Lung, and G. S. Veronese, "Spin one's wheels? byzantine fault tolerance with a spinning primary," in *Reliable Distributed Systems, IEEE Symposium on (SRDS)*, vol. 00, 09 2009, pp. 135–144. [Online]. Available: doi.ieeecomputersociety.org/10.1109/SRDS.2009.36

APPENDIX

A. Performance Penalty of Direct Chain Condition.

The direct chain has a high cost in HotStuff protocol due to the forking attack. Each time when a Byzantine primary over-rides blocks for honest primaries it not only reduces the throughput but also prevents direct chain formation. This results in increased latency. On the other hand, since a forking attack is not possible in Fast-HotStuff, a direct parent cannot be broken through forking. It is also possible (in HotStuff as well as Fast-HotStuff) that a direct chain is broken when a primary fails to propose a block during a specific view (v) and replicas timeout. In such a case, not only the failed primary does not propose any block but it also does not distribute the QC for the block from the previous view ($v-1$). For example, as it can be seen in Figure 14, the primary in the view v has failed. Therefore, it could not disseminate the block for the view v along with the QC for the view $v-1$. As a result, the next primary, $v+1$, will have the QC for the view $v-2$ as the *highestQC*. Hence, the block proposed in the view $v+1$ will have the QC from $v-2$. Byzantine primaries can exploit the rotating primary behavior to timeout regularly and also avert one block from the previous view. A primary that times out frequently can be blacklisted as done in [32]. There can be up to f number of blacklisted primaries. If an additional primary needs to be added then, the first primary from the blacklist queue is removed. In this way, the negative effect of primaries that deliberately timeout on performance can be significantly reduced.

B. Primary Selection and Liveness

In addition to the other generic BFT requirements for the liveness, in HotStuff and its variants, it is also important to make sure that the direct chain conditions meet eventually. If the protocol is not able to fulfill direct chain condition, then even if an honest primary is in-charge and the network is synchronous, liveness may not be guaranteed. Because no block will be committed and hence, clients will not receive response about successful execution of their transactions. Therefore, below we provide additional component of liveness proof for Fast-HotStuff under different primary selection mechanisms.

Random Primary Selection: In this case the primary is chosen randomly and uniformly from a set of N replicas. The probability of an honest primary selected is approximately $(\frac{2}{3})$. The probability of a bad event where two consecutive honest primaries not selected is $P_b = 1 - (\frac{2}{3}) \times (\frac{2}{3})$. By treating such a bad event as the Bernoulli trial, we have that the bad event is triggered k consecutive times with probability at most P_b^k . As it can be seen P_b^k approaches fast to 0 at an exponential rate as k grows linearly. Moreover, by blacklisting up-to f primaries for frequent failure (as stated previously), a one-direct chain can be achieved more quickly and frequently. Therefore, in case of random primary selection one-chain will be formed eventually.

Round-robin Primary During happy cases when there is no primary failure we know that a Byzantine primary can't perform

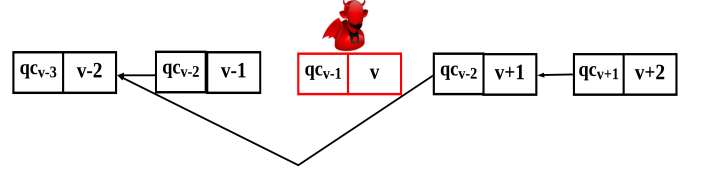


Fig. 14: **Breaking one-chain through timeout by a Byzantine primary.**

a forking attack. Hence, one-chain will be formed between two consecutive blocks during T_f . During the view change due to the primary failure, we try to pick the best attack strategy for Byzantine primaries to prevent the formation of one-chain between two blocks from honest primaries (to cause liveness failure). The formation of one-chain can only be prevented if at least one Byzantine replica is selected as primary after each honest primary. In other words, honest primaries should never be selected consecutively to avoid one-chain formation. The best strategy for Byzantine primaries will be to prevent the maximum number of honest primaries from one-chain formation. There is at most f number of Byzantine replicas out of $n = 3f + 1$ replicas. This means if each Byzantine replica is selected as a primary after one honest primary, then the f honest primaries will not be able to make one-chain. But the remaining $f + 1$ honest primaries can make one-chain. For $f = 0$, since no Byzantine replica will be selected as a primary, hence, no block proposed by an honest primary will be averted. Therefore, one-chain commit condition is satisfied. For $f \geq 1$, we have $f + 1 \geq 2$, hence there will be at least two consecutive honest primaries whose blocks will form one-chain and fulfill the commit condition. Therefore, if primaries are selected in a round-robin manner Fast-HotStuff holds liveness.