Optimal Good-Case Latency for Sleepy Consensus

Yuval Efron[1], Joachim Neu[2], Ling Ren[3], and Ertem Nusret Tas[2]

[1] Columbia University, ye2210@columbia.edu
[2] a16z Crypto Research, {jneu,ntas}@a16z.com
[3] University of Illinois at Urbana–Champaign, renling@illinois.edu

Abstract. In the context of Byzantine consensus problems such as Byzantine broadcast (BB) and Byzantine agreement (BA), the *good-case* setting aims to study the minimal possible latency of a BB or BA protocol under certain favorable conditions, namely the designated leader being correct (for BB), or all parties having the same input value (for BA). We provide a full characterization of the feasibility and impossibility of good-case latency, for both BA and BB, in the synchronous *sleepy* model. Surprisingly to us, we find *irrational* resilience thresholds emerging: 2-round good-case BB is possible if and only if at all times, at least $\frac{1}{\varphi} \approx 0.618$ fraction of the active parties are correct, where $\varphi = \frac{1+\sqrt{5}}{2} \approx 1.618$ is the golden ratio; 1-round good-case BA is possible if and only if at least $\frac{1}{\sqrt{2}} \approx 0.707$ fraction of the active parties are correct.

1 Introduction

The Byzantine consensus problems [15], such as Byzantine broadcast and Byzantine agreement, are among the most fundamental and well-studied problems in cryptography and distributed computing. The recent surge of cryptocurrencies and blockchain systems has rekindled interest in these problems, and also drawn the community's attention to unconventional system models that were overlooked in the decades of prior research.

One of the most prominent and striking features of the celebrated Nakamoto consensus protocol [22,10] is that it allows correct parties to participate intermittently in the protocol. At any time, only a (possibly tiny) fraction of correct parties are actively following the protocol. The rest of the correct parties are in an *inactive* (or crashed) state. Furthermore, correct parties can transition between active and inactive states at any time without prior notice, and they do not know for sure how many other parties are actively participating in the protocol at any time. A variant of this model (without reliance on proof-of-work) is formalized by Pass and Shi as the *sleepy* model [24], also interchangeably called the *dynamic participation* model.[4] In contrast, we refer to the traditional model where all correct parties are always active as the *static participation* model. Note

[4] Importantly, the *unexpected temporary crash faults* (what "dynamic participation" refers to) in the sleepy model is not to be confused with *scheduled* reconfiguration

that a variant of the CAP theorem [11,16,23] shows that a synchronous network is necessary for sleepy consensus, so we assume *synchrony* throughout this paper. The sleepy model is employed by leading blockchains such as Ethereum and Cardano [23,5,14,2].

A line of recent works has designed sleepy Byzantine consensus protocols that match static participation protocols in many aspects. Sleepy Byzantine consensus protocols can tolerate minority Byzantine faults [14,24,12,21,17,9,19,5,8,7,4], which is the same corruption threshold in the static model. Protocols in the sleepy model have also achieved expected constant rounds [21,18,17,9,19,8,7], again matching the static participation model.

In this paper, we focus on the *good-case* latency T_{gc}, measured in rounds of communication. For the Byzantine broadcast problem, the "good case" refers to the case where the designated sender is correct, while for Byzantine agreement, it refers to the case where all parties have the same input value. In addition to a certain latency requirement in the good case, the protocols are required to satisfy the usual consensus desiderata (termination, agreement, validity; see Defs. 1 and 2) even when the good-case conditions are not met. The good-case latency is a metric well-motivated by practical considerations. Most deployed consensus protocols have parties rotate to serve as the *leader*, who proposes a value (a block) for other parties to agree on. Because there are mechanisms to reward or penalize the leader based on its actions, the vast majority of leaders behave correctly. We thus would like the consensus protocol to be as fast as possible under a correct leader.

Note that no Byzantine broadcast protocol can hope to achieve latency $T_{\mathrm{gc}} \leq 1$, even in the good case, for the straightforward reason that it leaves correct parties no time to reconcile (or even detect) equivocating values they may have received from a Byzantine leader in the first communication round. Similarly, no Byzantine agreement protocol can hope to achieve good-case latency $T_{\mathrm{gc}} = 0$, for the analogous reason that it leaves correct parties no time to reconcile different input values they may have. On the other hand, an earlier work [1] has shown that for Byzantine broadcast in the traditional synchronous model with static participation, two rounds are sufficient and necessary in the good case, if the *resilience* ρ (i.e., fraction of Byzantine parties tolerable) is below $1/2$ (see Tab. 1). For Byzantine agreement in the same model, it is folklore that one round latency can be achieved in the good case, if and only if at most $1/3$ of parties are Byzantine (see Tab. 1 and Lems. 1 and 2).

Results. This paper extends the systematic study of good-case latency of Byzantine consensus to the dynamic participation (sleepy) model. We give a complete characterization of the good-case latency of Byzantine broadcast and Byzantine agreement, and the corresponding resilience (see Tab. 1). Our results for the dynamic participation model imply a complete characterization of good-case

of the membership set of parties operating the protocol (also called "stake shift" in the context of proof-of-stake blockchains). No reconfiguration of the set of operating parties takes place throughout this paper.

Table 1. Achievable and impossible resiliences for Byzantine broadcast (BB) and Byzantine agreement (BA) with varying good-case latency T_{gc} in different participation models. Notably, we provide a tight characterization under dynamic participation, where tight irrational resilience thresholds emerge: $1 - 1/\varphi \approx 0.382$ (where $\varphi = \frac{1+\sqrt{5}}{2} \approx 1.618$ is the golden ratio) and $1 - 1/\sqrt{2} \approx 0.293$.

Problem	T_{gc}	**Part. Model**	**Achiev. Resil.**	**Imposs. Resil.**
BB	2	Static P.	1/2 [1]	Open*
		Unknown P.	1/2 (Thm. 5)	Open*
		Dynamic P.	$1 - 1/\varphi$ (Thm. 3)	$1 - 1/\varphi$ (Thm. 1)
BB	≥ 3	Static P.	1/2 [1]†	Open*
		Unknown P.	1/2 (Thm. 5)†	Open*
		Dynamic P.	1/2 (Thm. 6)	1/2 [25]
BA	1	Static P.	1/3 (Folk.: Lem. 1)	1/3 (Folk.: Lem. 2)
		Unknown P.	$1 - 1/\sqrt{2}$ (Thm. 4)‡	$1 - 1/\sqrt{2}$ (Thm. 2)
		Dynamic P.	$1 - 1/\sqrt{2}$ (Thm. 4)	$1 - 1/\sqrt{2}$ (Thm. 2)‡
BA	≥ 2	Static P.	1/2 (Thm. 7)‡	1/2 [3]
		Unknown P.	1/2 (Thm. 7)‡	1/2‡
		Dynamic P.	1/2 (Thm. 7)	1/2‡

"Folk." indicates a result is folklore.

* The landscape of Byzantine broadcast in the "adversarial majority" regime remains incomplete, even under static participation. The protocol provided in [26] achieves $T_{\text{gc}} = O(\frac{n}{n-f})$. This matches the impossibility results [1] asymptotically, but concrete gaps remain. This lack of clarity seeps into the unknown participation model, since crashed honest parties can be treated as Byzantine for the purpose of protocols tolerating an adversarial majority of parties [25]. For dynamic participation, we fully characterize the good-case latency and resilience achievable for Byzantine broadcast and Byzantine agreement.

† Implied by a protocol with better latency.

‡ Implied by a protocol or impossibility result for a more demanding model.

Table 2. Earlier protocols and their good-case latency T_{gc} and resilience, for Byzantine broadcast (BB) and Byzantine agreement (BA), in different participation models.

Problem	**Part. Model**	**Protocol**	**Lat.** T_{gc}	**Resil.**
Broadcast (BB)	Static P.	ANRX'21 [1]	2	1/2
	Unknown P.	KW'21 [13]	3	1/3
	Dynamic P.	MMR'23 [19]	4	1/2
Agreement (BA)	Static P.	Folklore (Lem. 1)	1	1/3
	Static P.	MR'21 [20]	4	1/2
	Unknown P.	KW'21 [13]	3	1/3
	Dynamic P.	LG'23 [17,9]	4	1/2
	Dynamic P.†	DSTZ'23 [6]	3	1/2

† Mild stable participation assumption.

latency and resilience for Byzantine agreement and Byzantine broadcast (in the "honest majority" regime) in the *unknown participation* model [13]. The unknown participation model is weaker than the traditional static participation model, but stronger than the dynamic participation model, in the sense that the number of active correct parties is unknown to the protocol, but does not change once the protocol starts.

Perhaps the most surprising part of our findings is that the critical resilience thresholds that dictate good-case latency under dynamic and unknown participation are *irrational* numbers. For instance, Byzantine broadcast with good-case latency $T_{\text{gc}} = 2$ and resilience ρ can be achieved under dynamic participation if and only if $\rho \leq 1 - 1/\varphi \approx 0.382$, where $\varphi = \frac{1+\sqrt{5}}{2} \approx 1.618$ is the golden ratio. Byzantine agreement with good-case latency $T_{\text{gc}} = 1$ and resilience ρ can be achieved under dynamic participation and under unknown participation if and only if $\rho \leq 1 - 1/\sqrt{2} \approx 0.293$. To the best of our knowledge, this is the first time irrational corruption thresholds arise in distributed and threshold cryptography problems, such as Byzantine consensus, verifiable secret sharing, and multi-party computation.

Our results also establish separations among static, unknown, and dynamic participation. When the corruption threshold is between $1 - 1/\varphi$ and $1/2$, Byzantine broadcast under unknown participation can decide in two rounds in the good case, but requires three rounds under dynamic participation. When the target corruption threshold is between $1 - 1/\sqrt{2}$ and $1/3$, Byzantine agreement under static participation can decide in one round in the good case, but requires two rounds under unknown participation.

Related Work. Tab. 2 lists earlier consensus protocols with low good-case latency. For Byzantine broadcast, [1] achieves the optimal $T_{\text{gc}} = 2$ under static participation. For dynamic participation, [19] provides $T_{\text{gc}} = 4$ under a majority of correct active parties, which also works under unknown participation, whereas [13] gives a protocol with improved latency $T_{\text{gc}} = 3$, but only with resilience $1/3$. We provide broadcast protocols for dynamic participation with minimal good-case latency, $T_{\text{gc}} = 2$ and $T_{\text{gc}} = 3$, and optimal resilience, $1-1/\varphi$ and $1/2$, respectively (Tab. 1).

For Byzantine agreement, a folklore result (see Lems. 1 and 2) achieves the minimal $T_{\text{gc}} = 1$ with $1/3$ resilience despite synchrony and static participation. Under dynamic participation, [17,9] achieves $T_{\text{gc}} = 4$ under $1/2$ resilience, while [6] improves it to $T_{\text{gc}} = 3$ at the expense of a mild stable-participation assumption. The work of [6] also implies protocols with $T_{\text{gc}} = 3$ and $1/2$ resilience under unknown and static participation models. We provide agreement protocols for dynamic participation (and for unknown participation) with minimal good-case latency, $T_{\text{gc}} = 1$ and $T_{\text{gc}} = 2$, and optimal resilience, $1-1/\sqrt{2}$ and $1/2$, respectively (Tab. 1).

Outline. We briefly review the model and definitions in Sec. 2, before providing a technical overview of our results in Sec. 3. Then, Sec. 4 proves our impossibility results. Sec. 5 presents our BB and BA protocols with $T_{\text{gc}} = 2$ and $T_{\text{gc}} = 1$,

respectively, and proves their correctness, before Sec. 6 does the same for our BB and BA protocols with $T_{\text{gc}} = 3$ and $T_{\text{gc}} = 2$, respectively.

2 Model & Definitions

2.1 Model

Sleepy Model of Consensus. We work in the *sleepy* model [24] of Pass and Shi, also called the *dynamic participation* model. We consider a setting with N parties in total, identified by a public key infrastructure (PKI). We assume a synchronous pairwise communication network, with a known delay upper-bound of Δ on message delivery. For simplicity, we present both our upper and lower bounds for the case $\Delta = 1$, though both generalize to general Δ in a straightforward manner. We consider some known universe I of possible input values.

The Adversary. We consider a *static corruption* adversary $\mathcal{A}$, i.e., at round $t = 0$, the adversary chooses a set $F \subseteq [N]$ of parties to be *corrupt*. The remaining parties are *correct*. Corrupt parties are entirely controlled by the adversary, and may deviate arbitrarily from the protocol. Furthermore, following [24], at all rounds t, the adversary can adaptively[5] select a subset of the correct parties to be *asleep* (i.e., *inactive*), whereas the remaining correct parties are *awake* (i.e., *active*). Asleep parties are temporarily crashed: they do not execute the protocol or send messages. Messages sent to an asleep party are buffered and delivered to the party (in an adversarially selected order) the next time it wakes up. Upon waking up, parties know the current round number, i.e., we assume synchronized clocks. Note that corrupt parties are awake from round $t = 0$, and never go to sleep throughout the execution. The number of awake parties at round t is denoted by n_t. We drop the subscript when the round is clear from the context. For an adversary $\mathcal{A}$, we denote by $F_{\mathcal{A}}$ the set of parties corrupted by $\mathcal{A}$, and we usually omit the subscript when the adversary is clear from context. For a value $\rho \in [0, 1]$, we say that an adversary $\mathcal{A}$ is ρ-bounded if for all t, $|F| < \rho n_t$. Finally, whenever relevant, the adversary chooses the input values (from I) of all correct parties.

Unknown Participation Model. Some of our results pertain to the unknown participation model, introduced in [13]. Unknown participation is a special case of the dynamic participation model, which can formally be described by a restricted family of adversaries, as follows. Consider the exact same setup as above, with the following restriction on the adversary model: At time $t = 0$, the adversary picks a set $S \subseteq [N]$ of n awake parties and a set $F \subseteq S$ of corrupt parties. From this point, the adversary cannot wake up or put to sleep any party. In other words, the parties in $S \backslash F$ are correct and awake throughout the entire execution, the parties in F are corrupt and awake throughout the entire execution,

[5] The adaptive adversary is not strongly rushing, i.e., it *cannot* observe the contents of a message sent by a party, intercept it, and then put the party to sleep.

and the remaining parties are correct and asleep throughout the entire execution. Similarly to the dynamic participation adversary, we say that an adversary $\mathcal{A}$ is ρ-bounded if $|F| < \rho n$.

Cryptographic Primitives. We use a digital signature scheme on top of our PKI assumption. We assume $\mathcal{A}$ is computationally bounded, i.e., $\mathcal{A}$ cannot forge signatures on any message on behalf of parties outside of $F_{\mathcal{A}}$.

2.2 Consensus Primitives

We consider two standard consensus problems in this paper, Byzantine broadcast (BB) and Byzantine agreement (BA).

Definition 1 (Byzantine Broadcast (BB)). *In the* BB *problem, there is a designated party ℓ, referred to as the* leader*, with an* input *$u \in I$. As output, each party p* decides *a value $o_p \in I$. Let Π be a protocol to be executed by the parties. The following properties constitute the* BB *problem.*

1. ***Termination.*** *There exists a round T such that every correct party decides and halts in the first round $T' \geq T$ in which it is awake.*
2. ***Agreement.*** *There exists a value $u' \in I$ such that all correct parties that decide, decide u'.*
3. ***Validity.*** *If ℓ is correct and awake in round $t = 0$, then all correct parties that decide, decide u, i.e., ℓ's input.*

For a value ρ, we say that a protocol Π for BB *is ρ-secure under dynamic/unknown participation if it satisfies termination, agreement, and validity against any ρ-bounded adversary. The maximum ρ for which Π is ρ-secure is Π's* resilience*.*

Definition 2 (Byzantine Agreement (BA)). *In the* BA *problem, each party p has an* input *$u_p \in I$. As output, each party p* decides *a value $o_p \in I$. Let Π be a protocol to be executed by the parties. The following properties constitute the* BA *problem.*

1. ***Termination.*** *There exists a round T such that every correct party decides and halts in the first round $T' \geq T$ in which it is awake.*
2. ***Agreement.*** *There exists a value $u' \in I$ such that all correct parties that decide, decide u'.*
3. ***Validity.*** *If all correct parties that are awake in round $t = 0$ have u as input, then all correct parties that decide, decide u.*

For a value ρ, we say that a protocol Π for BA *is ρ-secure under dynamic/unknown participation if it satisfies termination, agreement, and validity against any ρ-bounded adversary. The maximum ρ for which Π is ρ-secure is Π's* resilience*.*

2.3 Good-Case Latency

Decision Latency. For a ρ-bounded adversary $\mathcal{A}$ and a ρ-secure protocol Π for BB or BA, we denote by $\mathsf{DL}_{\mathcal{A}}(\Pi)$ the random variable (over the randomness used by correct parties and the adversary) indicating the smallest round R for which every correct party *decides* (but not necessarily terminates) in the first round $R' \geq R$ in which it is awake, in the presence of $\mathcal{A}$. We say that Π has decision latency R with respect to a ρ-bounded adversary $\mathcal{A}$ if $R = \arg\min_{R' \in \mathbb{N}} \Pr[\mathsf{DL}_{\mathcal{A}}(\Pi) \leq R'] = 1$. For a family $\mathcal{F}$ of ρ-bounded adversaries we define the decision latency of Π with respect to $\mathcal{F}$ to be $\mathsf{DL}_{\mathcal{F}}(\Pi) = \sup_{\mathcal{A} \in \mathcal{F}} \mathsf{DL}_{\mathcal{A}}(\Pi)$.

Good-Case Latency. The efficiency metric we focus on in this work is that of *good-case* decision latency T_{gc}. Intuitively, this measure considers the decision latency of a protocol Π in executions in which certain favorable conditions hold, namely ℓ being correct for BB, or all correct parties having the same input for BA. More formally, we define good-case latency as follows.

1. BB: For a value ρ, and a ρ-secure protocol Π for BB under dynamic/unknown participation, consider the family $\mathcal{F}_{\mathsf{goodcase}}$ of ρ-bounded adversaries $\mathcal{A}$ for which the leader ℓ is correct, i.e., $\ell \notin F$, and the leader is awake at round $t = 0$. We define the good-case latency of Π to be $T_{\mathrm{gc}} \triangleq \mathsf{DL}_{\mathcal{F}_{\mathsf{goodcase}}}(\Pi)$.
2. BA: For a value ρ, and a ρ-secure protocol Π for BA under dynamic/unknown participation, consider the family $\mathcal{F}_{\mathsf{goodcase}}$ of ρ-bounded adversaries $\mathcal{A}$ for which $\mathcal{A}$ gives all correct parties awake at round $t = 0$ the same input value u, for some $u \in I$. We define the good-case latency of Π to be $T_{\mathrm{gc}} \triangleq \mathsf{DL}_{\mathcal{F}_{\mathsf{goodcase}}}(\Pi)$.

3 Technical Overview

The Traditional Case of Synchrony with Static Participation. To develop some intuition about the feasibility of good-case latency, let us begin by considering the traditional synchronous model with static participation, which in our formulation translates to adversaries for which all correct parties are awake in all rounds. Pondering on the BB problem for a moment, it definitely seems like in 2 rounds, we cannot do much beyond:

1. Round 0: Have the leader ℓ multicast its value.
2. Round 1: Have all parties report what they heard from the leader.

If the total number of parties is N, keeping this protocol blueprint in mind, for some value $\rho \in [0, \frac{1}{2}]$, we can expect correct parties to collect strictly more than $(1-\rho)N$ amount of "evidence" for a value u against ρ-bounded adversaries, in executions in which ℓ is correct with input u. An additional observation is that in executions with a correct leader ℓ, correct parties can also expect to collect 0 evidence for any other value. As such we can have a correct party decide after two rounds if it received sufficient evidence for a value, and *no* evidence

for any other value. One can observe that this implies that if a party p decided u, then any other correct party q observed $< \rho N$ evidence for any other value. To allow other parties to break the symmetry, all we need to stipulate is that $(1-\rho)N \geq \rho N$. Note that this bound holds for all $\rho \leq \frac{1}{2}$, and indeed $\rho = \frac{1}{2}$ turns out to be the correct corruption bound for the feasibility of 2-round good-case BB in the traditional synchronous static participation setting.

Generic Intuition. Given that this approach works for the static participation case, let us test whether the following line of thinking can yield the correct corruption bound for 2-round good-case BB in other settings: *For a bound ρ, derive a lower bound on the amount of evidence c_ρ available for the leader's input in executions with a correct leader. Given this amount, derive an upper bound on the amount of evidence a_ρ a correct party can receive for a different value. Stipulate $c_\rho \geq a_\rho$.*

Dynamic Participation. Let us apply the above intuition to dynamic participation. For a bound ρ, consider a good-case execution (Execution 1), i.e., the leader is correct with some value u and awake at round $t = 0$, for a ρ-bounded adversary $\mathcal{A}$. In a similar fashion to the previous paragraph, consider a correct party p awake in round $t = 2$, and suppose it hears from n_p parties. It can expect to hear evidence for u from at least $c_\rho = (1-\rho)n_p$ of them, and no evidence for any other value. From the perspective of p, the ρn_p parties reporting no evidence for any value are corrupt and p should ignore them and decide anyway. One might be tempted now to repeat the argument from the previous paragraph, and claim that any other correct party can receive at most ρn_p evidence for any other value, and so we again have $(1-\rho)n_p \geq \rho n_p$ yielding $\rho = \frac{1}{2}$.

The key observation is that p *does not know that the parties reporting no evidence are actually corrupt*, as it cannot be certain about the total number of participating parties. To make this concrete, consider now an alternative case (Execution 2), in which the leader is corrupt, and although p hears from n_p parties, they are all correct, and there are in fact $\frac{\rho}{1-\rho}n_p$ corrupt parties, and not just ρn_p. The corrupt leader does not send anything to $(1-\rho)n_p$ of the correct parties, and the rest of the corrupt parties do not send anything to p. From p's perspective at round $t = 2$, execution 2 is identical to execution 1, and so p decides in round $t = 2$ in both of them. In execution 2, however, a different correct party may receive $a_\rho = \frac{\rho}{1-\rho}n_p$ evidence for a value $u' \neq u$. Thus to allow other parties to break the symmetry, we must stipulate $(1-\rho)n_p \geq \frac{\rho}{1-\rho}n_p$, which yields $\rho \leq (1-\rho)^2$, which in turn gives $\rho \leq 1 - \frac{1}{\varphi}$, where φ is the golden ratio!

This intuition turns out to yield the correct solution, and we provide tight lower and upper bounds in Thm. 1, and Thm. 3, respectively. We complement these results by establishing in Thm. 6 that 3-round good-case BB is feasible under dynamic participation for $\rho = \frac{1}{2}$.

Unknown Participation. An astute reader may rush to a premature conclusion upon reading the previous part, as it seems that the same intuition from above

should apply to and yield the same bound under unknown participation. At least at first glance, it seems that the only thing we used is p's inability to distinguish between the case of n_p participating parties and $\frac{n_p}{1-\rho}$ participating parties. Perhaps, however, we were too hasty in making that assertion.

This intuition turns out to be deceiving under unknown participation. Specifically, p can more scrupulously rely on the fact that *the same set of correct parties is awake in all rounds*. In protocol terms, parties can multicast a *heartbeat* message both in round $t = 0$ and in round $t = 1$, along with the leader's proposed value; they also relay all received heartbeat messages. Now, a protocol can stipulate that having q's heartbeat relayed by a majority of the parties is a prerequisite for p to count q's contribution to the leader's purported value. It turns out that this technique allows the unknown participation model to boast 2-round good-case BB for $\rho = \frac{1}{2}$, thus establishing a separation between dynamic and unknown participation. The formal details can be found in Thm. 5.

BA. While for BB, the good-case decision latency is either 2 rounds to 3 rounds, the good-case decision latency of BA can be as small as a single round. It turns out that 2-round good-case BA is feasible for $\rho = \frac{1}{2}$ even under dynamic participation! To the best of our knowledge, this result was not known even in the static participation setting, even though it is rather straightforward in that model. For dynamic participation, however, such a result is far from trivial, and involves a novel *report participation* technique. See Thm. 7 for the full details.

This leaves us with the question: what values of ρ make 1-round good-case BA feasible? The same generic intuition we applied for BB under dynamic participation can be repeated, with the caveat that we now have to account for equivocations by corrupt parties when calculating a_ρ. The math yields that we must stipulate $\rho \leq (1-\rho)^2 - \rho(1-\rho)$, which is tight for $\rho = 1 - \frac{1}{\sqrt{2}}$. The lower and upper bounds can be found in Thm. 2, and Thm. 4, respectively. In fact, our BA lower bound (Thm. 2) applies even for unknown participation (the easier setting), while our BA upper bound (Thm. 4) applies to dynamic participation (the harder setting). Furthermore, this establishes a separation between the static participation model, for which 1-round good-case BA is feasible for $\rho \leq \frac{1}{3}$, and the unknown participation model.

4 Lower Bounds

In this section, we prove the following theorems.

Theorem 1. *Let $\varphi = \frac{1+\sqrt{5}}{2} \approx 1.618$ be the golden ratio. For all $\rho > 1 - \frac{1}{\varphi} \approx 0.382$, there is no ρ-secure protocol solving* BB *under dynamic participation with good-case latency ≤ 2.*

Theorem 2. *For all $\rho > 1 - \frac{1}{\sqrt{2}} \approx 0.293$, there is no ρ-secure protocol solving* BA *under unknown participation with good-case latency ≤ 1.*

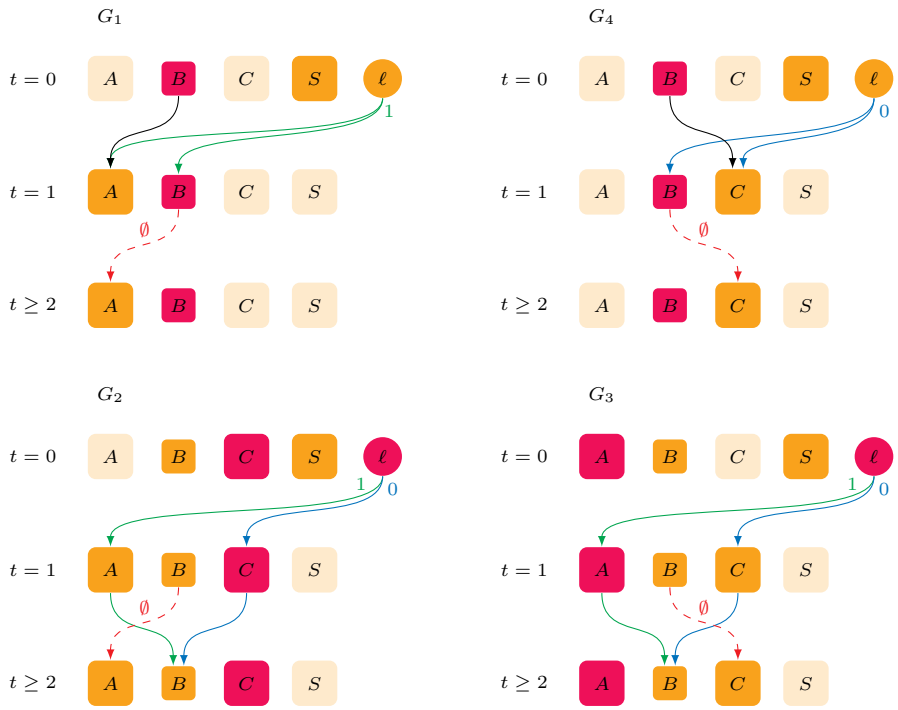

Fig. 1. Illustration of the four executions considered in the proof of Thm. 1. Green labels and arrows indicate correct behavior, or emulation of it, with input 1. Blue labels and arrows indicate correct behavior, or emulation of it, with input 0. Corrupt parties are colored red, correct parties orange. Translucent sets indicate that the set of parties is not awake at that round. The behavior of correct parties is well defined from the protocol description Π, so we omit most of the corresponding arrows to maintain simplicity. Lack of an arrow from a set of corrupt parties to a set of correct parties indicates omission of all corresponding messages. Dashed red arrows labeled "$\emptyset$" indicate messages corresponding to receiving nothing from the leader ℓ in round $t = 0$. Black arrows indicate correct round $t = 0$ behavior.

4.1 BB Lower Bound

In this section, we prove Thm. 1.

Proof of Thm. 1. Let n be a natural number and let $\rho' \in [0, 1]$ such that $\rho' > \rho := 1 - \frac{1}{\varphi}$. In particular, this implies that $\rho' > (1-\rho)^2$, as $1 - \frac{1}{\varphi}$ is a solution of the equation $x = (1-x)^2$. Assume towards a contradiction that there exists a ρ'-secure BB protocol Π under dynamic participation with good-case latency 2. Let ℓ be the designated leader. We consider some natural number n, and we define the following disjoint sets of parties A, B, C such that $|A| = |C| = \lfloor \rho n \rfloor$, $|B| = \lceil \rho(1-\rho)n \rceil$. Note that $\rho n + \rho n + \rho(1-\rho)n = (1-\rho)^2 n + \rho n + \rho(1-\rho)n = n$. As such, since none

of these added expressions are integers, we have that $|A| + |B| + |C| + |\{\ell\}| = n$. We further consider an additional disjoint set S of parties where $|S| = |A| = |C|$.

We now define and describe four executions of Π, which we denote by G_1, G_2, G_3, G_4. See Fig. 1 for an illustration.

- G_1: In round $t = 0$, the parties in S, B and ℓ are awake. The parties in S are correct. In particular, the parties in C are not active at all throughout the protocol. Furthermore, the parties in B are corrupt, and are thus awake at all rounds. The leader ℓ is correct with input 1. In round $t = 1$, the parties in S fall asleep, and the parties in A wake up and remain awake for the remainder of the execution. The parties in A are correct, and the parties in B are corrupt. Note that up to an additive factor of 1 due to the ceiling and floor, one has that $|A| + |B| = \rho n + \rho(1-\rho)n = \rho(2-\rho)n = (1-(1-\rho)^2)n = (1-\rho)n$, and thus for a sufficiently large n [6], it holds that $|B| = \lceil (1-\rho)\rho n \rceil < \rho'(|A| + |B|)$, and so the adversary is ρ'-bounded. The parties in B behave correctly in round $t = 0$, and in round $t = 1$ they behave as if they have not received the round one messages of ℓ.
- G_2: In round $t = 0$, the parties in S, B, C and ℓ are awake. S, B are correct. The leader ℓ is corrupt and the parties in C are corrupt, and are thus awake throughout the whole execution. In round $t = 1$, S fall asleep, and the parties in A wake up and remain awake for the remainder of the execution. All parties in A, B are correct. Note that for a sufficiently large n, the adversary is ρ'-bounded as $|C| + |\{\ell\}| = \lfloor \rho n \rfloor + 1$ by definition and there are n awake parties. The leader ℓ behaves to A as if it was correct with input 1 in rounds $t = 0$ and $t = 1$ and then halts; it does not send any messages to the parties in B. The parties in C do not send any round $t = 0$ messages, and do not send round $t = 1$ messages to A; they behave to B in round $t = 1$ as if they received correct round $t = 0$ messages from ℓ with input 0. Note that this is doable as ℓ is corrupt. They behave correctly for the remainder of the execution, except for pretending to have not received round $t = 1$ messages from A.
- G_3: This is the dual execution to G_2. In round $t = 0$, the parties in S, B, A and ℓ are awake. S, B are correct. The leader ℓ is corrupt and the parties in A are corrupt, and are thus awake throughout the whole execution. In round $t = 1$, S fall asleep, and the parties in C wake up and remain awake for the remainder of the execution. All parties in C are correct. Note that the adversary is ρ'-bounded by the same argument as in G_2. The leader behaves to C as if it was correct with input 0 in rounds $t = 0$ and $t = 1$ and then halts; it does not send any messages to parties in B. The parties in A do not send any round $t = 0$ messages, and do not send round $t = 1$ messages to C; they behave to B in round $t = 1$ as if they received correct round $t = 0$ messages from ℓ with input 1. Note that this is doable as ℓ is corrupt. They behave correctly for the remainder of the execution, except for pretending to have not received round $t = 1$ messages from C.

[6] Namely, n should be large enough so that ceil in $|B|$ does not violate the corruption bound ρ', which is bounded away from ρ by $\rho' - \rho > 0$.

– G_4: This is the dual execution to G_1. In round $t = 0$, the parties in S, B and ℓ are awake. The parties in S are correct. In particular, the parties in A are not active at all throughout the execution. Furthermore, the parties in B are corrupt, and are thus awake at all times. The leader ℓ is correct with input 0. In round $t = 1$, the parties in S fall asleep, and the parties in C wake up. The parties in C are correct. Note that the adversary is ρ'-bounded by the same argument as in G_1. The parties in B behave correctly in round $t = 0$, and in round $t = 1$ they behave as if they have not received the round $t = 0$ messages of ℓ.

With G_1, G_2, G_3, G_4 defined, we can now proceed with the following observations.

– The parties in A decide 1 in G_1 after 2 rounds. This is a consequence of the assumed good-case latency of 2 property of Π, the leader being correct with input 1 in execution G_1, and the adversary being ρ'-bounded.
– The parties in C decide 0 in G_4 after 2 rounds. This is a consequence of the assumed good-case latency of 2 property of Π, the leader being correct with input 0 in execution G_4, and the adversary being ρ'-bounded.
– In the first two rounds, the parties in A *cannot distinguish* between G_1 and G_2. In both executions, they receive the same set of messages from the exact same parties in the first two rounds. Thus, the parties in A decide 1 in G_2 after 2 rounds.
– In the first two rounds, the parties in C *cannot distinguish* between G_3 and G_4. In both executions, they receive the same set of messages from the exact same parties in the first two rounds. Thus, the parties in C decide 0 in G_3 after 2 rounds.
– The parties in B *cannot distinguish* between G_2, G_3. In G_2, the parties in C are corrupt and falsely claim to not have received round 2 messages from A, and in G_3, the parties in A are corrupt and falsely claim to not have received round 2 messages from C. In both G_2, G_3, the parties in A, C behave correctly after round 2. Thus, throughout both executions, B sees the exact same set of messages, from the exact same sets of parties, with the same delivery timings. Thus, by termination, eventually the parties in B decide the same value in both G_2, G_3.

Putting these observations together, we deduce, by the agreement property of Π, that B outputs 1 in G_2, and 0 in G_3. This contradicts the last observation above, thus concluding the proof. □

4.2 BA Lower Bound

In this section, we prove Thm. 2.

Proof of Thm. 2. Let n be a natural number and let $\rho' \in [0, 1]$ such that $\rho' > \rho := 1 - \frac{1}{\sqrt{2}}$. In particular, this implies that $\rho' > (1 - \rho)^2 - \rho(1 - \rho)$, as $1 - \frac{1}{\sqrt{2}}$ is a solution for $x = (1 - x)^2 - x(1 - x)$. Assume towards a contradiction that

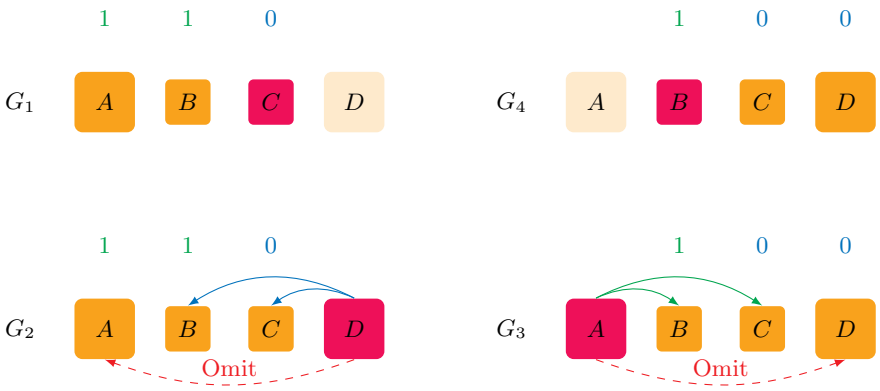

Fig. 2. Illustration of the four executions considered in the proof of Thm. 2. Green labels and arrows indicate correct behavior, or emulation of it, with input 1. Blue labels and arrows indicate correct behavior, or emulation of it, with input 0. Corrupt parties in each execution are colored red, correct parties orange. Translucent sets indicate that the set of parties is not participating in the given execution (inactive). Dashed red arrows labeled "Omit" indicate that no messages are sent from the source set of the arrow to its target set in round $t = 0$.

there exists a ρ'-secure BA protocol Π with good-case latency 1 under unknown participation. We consider a set of n parties, and a partition of them into disjoint sets A, B, C, D such that $|A| = |D| = \lceil \rho n \rceil$, and $|B| = |C| = \lfloor \rho(1-\rho)n \rfloor$. Note that by substituting ρ with $(1-\rho)^2 - \rho(1-\rho)$, one gets $\rho n + \rho(1-\rho)n + (1-\rho)^2 n = n$. Since none of these added expressions are integer, and by the fact that A, D are with ceil while B, C are with floor, we get that $|A| + |B| + |C| + |D| = n$. Hence this is a valid partition of the n parties. We now define and describe four executions of Π, which we denote by G_1, G_2, G_3, G_4. See Fig. 2 for an illustration.

- G_1: The participating parties are A, B, C. The parties in A, B are correct and C is corrupt. Note that up to an additive factor of 1, we have that $|A \cup B| = |A| + |B| = (1-\rho)^2 n$, and $|A| + |B| + |C| = \rho(1-\rho)n + (1-\rho)^2 n = (1-\rho)n$, thus for a sufficiently large n, we have that $|C| \leq \rho |A \cup B \cup C| < \rho' |A \cup B \cup C|$, which means the adversary is ρ'-bounded. The parties in A, B have input 1, and the parties in C behave as if they are correct with input 0.
- G_2: The participating parties are A, B, C, D. The parties in A, B, C are correct, and the parties in D are corrupt. Note that $|A \cup B \cup C \cup D| = n$, and that $|D| = \lceil \rho n \rceil$ as $\rho = (1-\rho)^2 - \rho(1-\rho)$. Thus, for a sufficiently large n, one has that $\lceil \rho n \rceil < \rho' n$, and so the adversary is ρ'-bounded. The parties in A, B have input 1, the parties in C have input 0. The parties in D behave as if they are correct with input 0, *except for* not sending any round $t = 0$ messages to A, and pretending to have not received round $t = 0$ messages from A. They behave correctly in all the remaining rounds.
- G_3: This is the dual execution to G_2. The participating parties are A, B, C, D. The parties in C, B, D are correct, and the parties in A are corrupt. Note that

the adversary is ρ'-bounded by the same argument as in G_2. The parties in C, D have input 0, the parties in B have input 1. The parties in A behave as if they are correct with input 1, *except for* not sending any round $t = 0$ messages to D, and pretending to have not received round $t = 0$ messages from D. They behave correctly in all the remaining rounds.
- G_4: This is the dual execution to G_1. The participating parties are B, C, D. The parties in C, D are correct, and the parties in B are corrupt. Note that the adversary is ρ'-bounded by the same argument as in G_1. The parties in C, D have input 0, and the parties in B behave as if they are correct with input 1.

With G_1, G_2, G_3, G_4 defined, we can now proceed with the following observations.

- All correct parties in G_1 have the same input 1. Thus, by the validity of BA and the good-case latency of 1 property of Π, the parties in A decide 1 at the end of the first round.
- All correct parties in G_4 have the same input 0. Thus, by the validity of BA and the good-case latency of 1 property of Π, the parties in D decide 0 at the end of the first round.
- At the end of the first round, the parties in A cannot distinguish between G_1, G_2. Thus, also in G_2, the parties in A decide 1 at the end of the first round. By the agreement property of BA, we thus have that both B, C eventually decide 1 in G_2.
- At the end of the first round, the parties in D cannot distinguish between G_3, G_4. Thus, also in G_3, the parties in D decide 0 at the end of the first round. By the agreement property of BA, we thus have that both B, C eventually decide 0 in G_3.
- The parties in B, C cannot distinguish between G_2, G_3, as in both executions they receive the exact same sets of messages, from the same sets of parties, with the same delivery timings, as both the parties in A and D claim to have not heard from the other in round $t = 1$. Thus, by termination, eventually the parties in B, C decide *the same* value in both G_2, G_3.

From the combination of the last three observations, we arrive at a contradiction, as the parties in B, C output 1 in G_2, 0 in G_3, but also the same value in both G_2, G_3. This concludes the proof. □

5 BB and BA with Optimal Good-Case Latency

In this section, we prove the following theorems.

Theorem 3. *For all $\rho \leq 1 - \frac{1}{\varphi} \approx 0.382$ where $\varphi = \frac{1+\sqrt{5}}{2} \approx 1.618$, there exists a ρ-secure protocol (namely $\Pi_{\mathsf{BB},2}$ below) solving BB under dynamic participation with good-case latency $T_{\mathrm{gc}} = 2$.*

Theorem 4. *For all $\rho \leq 1 - \frac{1}{\sqrt{2}} \approx 0.293$, there exists a ρ-secure protocol (namely $\Pi_{\mathsf{BA},1}$ below) solving* BA *under dynamic participation with good-case latency $T_{\mathrm{gc}} = 1$.*

Theorem 5. *For all $\rho \leq 1/2$, there exists a ρ-secure protocol (namely $\Pi_{\mathsf{BB},\mathsf{UP}}$ below) solving* BB *under unknown participation with good-case latency $T_{\mathrm{gc}} = 2$.*

5.1 BB with Good-Case Latency $T_{\mathrm{gc}} = 2$

In this section, we prove Thm. 3. In this protocol, we make black-box use of the BA protocol from [8], which we denote by Π_{BA}, and which is $\frac{1}{2}$-secure under dynamic participation.

Protocol 1: $\Pi_{\mathsf{BB},2}$

Setup. Leader ℓ with input value b_ℓ. Instructions for party p.

1. **Round** $t = 0$: ℓ multicasts $\langle \mathsf{echo}, b_\ell \rangle_\ell$.
2. **Round** $t = 1$: If received $\langle \mathsf{echo}, u \rangle_\ell$ for some u, then multicast $\langle \mathsf{vote}, u \rangle_p$ along with ℓ's echo message. Else, multicast $\langle \mathsf{vote}, \perp \rangle$.
3. **Round** $t = 2$: Let V denote the set of parties from which p received a valid vote message. Denote by V_u the set of parties from which p received a valid vote for value u. Let u be the value $\arg\max_{u \in I} |V_u|$, breaking ties arbitrarily. Multicast $\langle \mathsf{forward}, V_u \rangle_p$, along with the corresponding valid vote messages for u from the parties in V_u.
   Early deciding condition: If the following holds:
   (a) Did not detect equivocation from the leader ℓ. I.e., did not receive two echo (either forwarded or directly from ℓ) messages signed by the leader ℓ for values $u \neq u'$.
   (b) It holds that $|V_u| > (1 - \rho)|V|$.
   Then decide u and multicast $\langle \mathsf{decided}, u \rangle_p$.
4. **Round** $t \geq 3$**:**
   (a) **Early deciding:** For a value u', denote by $D_{u'}$ the set of parties from which p received a decided message for u', and by D^* the set of parties from which p received a forward message. If there exists a value u such that $|D_u| > (1 - \rho)|D^*|$, then decide u.
   (b) Let u' be the value for which p received the largest V_u set among all received forward messages. Run Π_{BA} as instructed that commences in round $t = 3$ with input u', and decide the output of Π_{BA}, if did not decide before.

Proof of Thm. 3. Let ρ be as in the premise of Thm. 3. Our protocol is given in $\Pi_{\mathsf{BB},2}$. We now analyze its security and efficiency. Termination follows from the termination of Π_{BA}, as all parties decide and halt once Π_{BA} terminates. We next handle agreement.

Claim. $\Pi_{\mathsf{BB},2}$ satisfies agreement against any ρ-bounded adversary.

Proof. There are two cases: Either there exists a correct party that decides from the early deciding condition, i.e., prior to participating in Π_{BA}, or not. Agreement

is straightforward in the latter case, as no correct party multicasts a decided message, and thus no correct party decides due to an early deciding condition in all rounds $t \geq 2$. Thus, due to Π_{BA} being $\frac{1}{2}$-secure and all correct parties deciding according to its output, agreement holds.

In the former case, let p be a correct party deciding a value u by the early deciding condition. Denote by V^p the set of parties from which p received a valid vote message. We first argue that there cannot be two correct parties p, q, both awake at round $t = 2$, that decide by the early deciding condition different values $u \neq u'$. If this was the case, then p has $|V_u^p| > (1-\rho)|V^p|$, and $|V_{u'}^q| > (1-\rho)|V^q|$. As the network is synchronous and $\rho < \frac{1}{2}$, this in particular implies that p has received at least one valid vote message for u from a correct party, and q received at least one valid vote message for u' from a correct party. This implies, however, that both p, q saw an equivocation from the leader ℓ at round $t = 2$, and thus none of them would have triggered the early deciding condition. This in particular implies that there exists at most one value, for which any correct party sends a decided message for, and thus all correct parties deciding due to the early deciding condition decide the same value.

It remains to show that if some correct party p decides a value u via the early deciding condition at round $t = 2$, then all parties eventually decide u. Denoting the correct parties awake at round $t = 1$ by H, we have that $H \subseteq V^p$. Furthermore, we have that $|V_u^p| > (1-\rho)|V^p|$, thus $|V_u^p| > (1-\rho)|H|$. Furthermore, p detected no equivocation from ℓ, hence no party in H multicast a vote message for a value $u' \neq u$. Denoting by F the number of corrupt parties, we have that $|F| < \rho(|H| + |F|)$, thus $|F| < \frac{\rho}{1-\rho}|H|$. In particular, we can deduce that any other correct party q receives at most $|F| < \frac{\rho}{1-\rho}|H|$ valid vote messages for values different from u. By the behavior of the protocol, p multicasts in round $t = 2$ the message $\langle \mathsf{forward}, V_u^p \rangle_p$, and so all correct parties awake at rounds ≥ 3 observe at least $(1-\rho)|H|$ vote messages in the forward message of p. Finally, note that $(1-\rho)|H| - |F| > (1-\rho)|H| - \frac{\rho}{1-\rho}|H| = \frac{(1-\rho)^2-\rho}{(1-\rho)}|H| > 0$. The last inequality holds by the assumption that $\rho < (1-\rho)^2$. Thus, all correct parties awake at round 3 commence Π_{BA} with input u. By the validity guarantee of Π_{BA}, we thus have that all parties decide u, as required. □

Finally, we handle validity and good-case latency.

Claim. $\Pi_{\mathsf{BB},2}$ satisfies validity against any ρ-bounded adversary. Furthermore, $\Pi_{\mathsf{BB},2}$ has good-case latency 2.

Proof. Assume ℓ is correct with input u. Then by the behavior of $\Pi_{\mathsf{BB},2}$, it multicasts $\langle \mathsf{echo}, u \rangle_\ell$ to all correct parties at round $t = 0$. Then, at round $t = 1$, all correct parties multicast $\langle \mathsf{vote}, u \rangle$ along with ℓ's echo message. Note that since ℓ is correct, no other valid vote for any other value other than u can be sent, by correct or corrupt parties. Thus, at round $t = 2$, no correct party detects equivocation from the leader, and all correct parties awake at $t = 2$ see a valid vote message for u from all correct parties awake at $t = 1$. As the adversary is ρ-bounded, we thus have that $|V_u^p| > (1-\rho)|V^p|$ for all correct parties p awake

at $t = 2$, and they all decide u at $t = 2$ and send corresponding decided messages. The same argument applied to the early deciding condition in rounds $t \geq 3$ then implies that any correct party p decides u in the first round $t \geq 2$ in which it is awake, as required. □

This concludes the proof of Thm. 3. □

5.2 BA with Good-Case Latency $T_{\mathbf{gc}} = 1$

In this section, we prove Thm. 4. In this protocol, we make black-box use of the BA protocol from [8], which we denote by Π_{BA}, and which is $\frac{1}{2}$-secure under dynamic participation.

Protocol 2: $\Pi_{\mathsf{BA},1}$

Setup. Each party p has input value u_p. Instructions for party p.

1. **Round** $t = 0$: Multicast $\langle \mathsf{echo}, u_p \rangle_p$.
2. **Round** $t = 1$: Denote by E the set of parties from which p received an echo message. Let u be the value $\arg\max_{u \in I} |E_u|$, breaking ties arbitrarily. Multicast $\langle \mathsf{forward}, E_u \rangle_p$, along with the corresponding echo messages for u. **Early deciding condition:** If $|E_u| > (1 - \rho)|E|$, then decide u, and multicast $\langle \mathsf{decided}, u \rangle_p$.
3. **Round** $t \geq 2$**:**
   (a) **Early Deciding:** For a value u', denote by $D_{u'}$ the set of parties from which p received a decided message for u', and by D^* the set of parties from which p received a forward message. If there exists a value u such that $|D_u| > (1 - \rho)|D^*|$, then decide u.
   (b) Let u' be the value for which p received the largest E_u set among all received forward messages. Run Π_{BA} as instructed that commences in round $t = 2$ with input u', and decide the output of Π_{BA}, if did not decide before.

Proof of Thm. 4. Let ρ be as in the premise of Thm. 4. Our protocol is given in $\Pi_{\mathsf{BA},1}$. We now analyze its security and efficiency. Termination follows from the termination of Π_{BA}, as all correct parties decide and halt after Π_{BA} outputs. Next, we handle agreement.

Claim. $\Pi_{\mathsf{BA},1}$ satisfies agreement against any ρ-bounded adversary.

Proof. There are two cases: either there exists a correct party that decides due to the early deciding condition at round $t = 1$, or not. The proof can be quickly concluded in the latter case, as then no correct party multicasts a decided message, and thus no correct party decides according to the early deciding condition in rounds $t \geq 2$. Thus all correct parties decide according to the output of Π_{BA}, which guarantees agreement.

We are now left with the case that there exists a correct party that decides a value u according to the early deciding condition at round $t = 1$. First we prove that this can occur for at most a single value. Assume that there exist two

correct parties p, q that decide according to the early deciding condition in round $t = 1$ values u, u', respectively, where $u \neq u'$. Denote by E^p, E^q the set of echo messages received by p, q, respectively. This implies that $|E^p_u| > (1-\rho)|E^p|$, and $|E^q_{u'}| > (1-\rho)|E^q|$. Denoting by H the set of correct parties awake at round $t = 0$, we have that $H \subseteq E^p$ and $H \subseteq E^q$, so $|E^p_u| > (1-\rho)|H|$, and $|E^q_{u'}| > (1-\rho)|H|$. Denoting by F^p, F^q the number of corrupt parties that sent an echo message to p, q, respectively. We have that at least $|E^p_u| - |F^p|$ of the echo messages for u received by p came from correct parties, and similarly at least $|E^q_{u'}| - |F^q|$ of the echo messages for u' received by q came from correct parties. We thus have that:

$$|E^p_u| - |F^p| > (1-\rho)(|H| + |F^p|) - |F^p| = (1-\rho)|H| - \rho|F^p|,$$

and similarly:

$$|E^q_{u'}| - |F^q| > (1-\rho)(|H| + |F^q|) - |F^q| = (1-\rho)|H| - \rho|F^q|.$$

As $F^q, F^p \subseteq F$, and $|F| < \frac{\rho}{1-\rho}|H|$, we have:

$$\begin{aligned} |E^p_u| - |F^p| &> (1-\rho)|H| - \frac{\rho^2}{1-\rho}|H| = \frac{(1-\rho)^2 - \rho^2}{1-\rho}|H| = \frac{1-2\rho}{1-\rho}|H| \\ &= (1 - \frac{\rho}{1-\rho})|H| > (1-(1-2\rho))|H| = 2\rho|H|. \end{aligned}$$

The last inequality holds due to the assumption $\rho < (1-\rho)(1-2\rho)$. This allows us to deduce that less than $(1-2\rho)|H|$ correct parties sent an echo message for a value other than u. Thus, $(1-2\rho)|H| \geq |E^q_{u'}| - |F^q| > (1-\rho)|H| - \rho|F^q|$ which implies $|F^q| > |H|$, a contradiction. Thus, there exists at most a single value u for which some correct party decides u via the early deciding condition in round $t = 1$.

This implies that correct parties can only send decided messages for a single value u, and so any correct party deciding according to the early decision condition in round $t \geq 2$ decides u as well, and agreement is maintained.

It remains to show that when a correct party p decides u due to the early deciding condition in round $t = 1$, all correct parties that decide on the Π_{BA} output also decide u. By the early deciding condition in round 1, $|E^p_u| > (1-\rho)(|H|+|F^p|)$, and at least $|E^p_u| - |F^p| > (1-\rho)|H| - \rho|F^p|$ of those echo messages for u came from correct parties. Thus, less than $\rho|H| + \rho|F^p|$ correct parties multicast an echo message for any value $u' \neq u$. This implies that the size of the $E_{u'}$ set in any forward message received by any correct party for a value $u' \neq u$ is bounded by

$$\begin{aligned} &\rho|H| + \rho|F^p| + |F| < \rho(|H| + |F^p|) + \frac{\rho}{1-\rho}|H| \\ &\overset{(1)}{<} \rho|H| + \rho|F^p| + (1-2\rho)|H| < (1-\rho)(|H| + |F^p|) < |E^p_u|. \end{aligned}$$

Where (1) holds due to the assumption $\rho < (1-\rho)(1-2\rho)$. Thus, the forward message sent by p with the set E^p_u is the largest set of echo messages witnessed

by any correct party in round $t = 2$, thus by the behavior of $\Pi_{\mathsf{BA},1}$, all correct parties awake at round $t = 2$ commence Π_{BA} with input u. The validity property of Π_{BA} then ensures that all correct parties output u from Π_{BA}, thus all correct parties agree, as required. □

Next, we handle validity and good-case latency.

Claim. $\Pi_{\mathsf{BA},1}$ satisfies validity against any ρ-bounded adversary. In particular, $\Pi_{\mathsf{BA},1}$ has good-case latency of 1.

Proof. Assume that all correct parties awake at round $t = 0$ have the same input value u, then, due to the adversary being ρ-bounded, all correct parties awake at round $t = 1$ observe $|E_u| > (1-\rho)|E|$, as all correct parties send an echo message for u. In particular, *all* correct parties awake in round $t = 1$ decide u by the early deciding condition and multicast a $\mathsf{decided}$ message for u. An identical argument then implies that any correct party p, in the first round $t \geq 2$ in which it is awake, observes $|D_u| > (1-\rho)|D^*|$, and thus p decides in the first round $t \geq 1$ in which it is awake. This proves that $\Pi_{\mathsf{BA},1}$ satisfies validity and has $T_{\mathrm{gc}} = 1$. □

This concludes the proof of Thm. 4. □

5.3 BB for Unknown Participation with Good-Case Latency $T_{\mathrm{gc}} = 2$

In this section, we prove Thm. 5. In this protocol, we make black-box use of the BA protocol from [8], which we denote by Π_{BA}, and which is $\frac{1}{2}$-secure under dynamic participation.

Protocol 3: $\Pi_{\mathsf{BB,UP}}$

Setup. Leader ℓ with input value b_ℓ. Instructions for party p.

1. **Round** $t = 0$: If $p = \ell$, multicast $\langle \mathsf{echo}, b_\ell \rangle_\ell$. Else, multicast $\langle \mathsf{echo}, \perp \rangle_p$.
2. **Round** $t = 1$: Denote by E the set of parties from which p received an echo message. Multicast $\langle \mathsf{forward}, E \rangle_p$, along with the corresponding echo messages. If $\ell \in E$ and received $\langle \mathsf{echo}, u \rangle_\ell$, multicast $\langle \mathsf{vote}, u \rangle_p$ along with ℓ's echo.
3. **Round** $t = 2$: Let G denote the set of parties from which p received a $\mathsf{forward}$ message, and let V denote the set of parties from which p received a valid vote message. Denote by E the set of parties from which p received an echo message. Denote by $E^* \subseteq E$ the set of parties p for which an echo message from p appeared in more than $\frac{|G|}{2}$ of the received $\mathsf{forward}$ messages. Let u be the value $\arg\max_{u \in I} |V_u \cap E^*|$. Multicast $\langle \mathsf{echo2}, V_u \cap E^* \rangle_p$, along with the corresponding valid vote messages.
   Early deciding condition: If the following holds:
   (a) Did not detect equivocation from the leader ℓ, i.e., did not receive two valid vote messages for values $u \neq u'$.
   (b) It holds that $|V_u \cap E^*| > \frac{|E|}{2}$.
   Then decide u and multicast $\langle \mathsf{decided}, u \rangle_p$.
4. **Round** $t \geq 3$**:**

(a) Let u' be the value for which p received the largest $V_u \cap E^*$ amongst all received echo2 messages. Run Π_{BA} as instructed that commences in round $t = 3$ with input u', and decide the output of Π_{BA}, if did not decide before.

Proof of Thm. 5. Our protocol is given in $\Pi_{\mathsf{BB,UP}}$. We now analyze its security and efficiency. Termination follows from the termination of Π_{BA}, as all parties decide and halt once Π_{BA} terminates. We next handle agreement. Denote by n the total number of parties, which is unknown to the correct parties.

Claim. $\Pi_{\mathsf{BB,UP}}$ satisfies agreement against any $\frac{1}{2}$-bounded adversary.

Proof. There are two cases: either there exists a correct party that decides from the early deciding condition, i.e., prior to participating in Π_{BA}, or not. Agreement is straightforward in the latter case, with Π_{BA} being $\frac{1}{2}$-secure and all correct parties deciding its output. We next focus on the former case.

Denote by V^p the set of parties from which p received a valid vote message, and denote by $E^p, E^{*,p}$ the E, E^* sets observed by party p in round 2, respectively. We first argue that there cannot be two correct parties p, q that decided due to the early deciding condition in round $t = 2$ values $u \neq u'$, respectively. Suppose this was the case, then p has observed $|V_u^p \cap E^{*,p}| > \frac{E^p}{2}$. Denoting by H the set of correct parties, first observe that $H \subseteq E^{*,p}$, as a correct party sends an echo message to all parties, and all correct parties include that echo message in their forward messages. Since H constitutes a majority of the parties, all correct parties observe the echo messages of correct parties as part of their E^* set. This in particular implies that there exists a correct party in $V_u^p \cap E^{*,p}$, and the same argument yields that there exists a correct party in $V_{u'}^q \cap E^{*,q}$. This implies, however, that all correct parties observed in round $t = 2$ a valid vote message for both u, u', and thus no correct party decides by the early deciding condition in round $t = 2$. This implies that there exists at most a single value u, such that a correct party decides u due to the early deciding condition in round $t = 2$. In particular, this also implies that if any correct party decides due to the early deciding condition at a round $t \geq 3$, it can only possibly decide u, as no decided message can be sent by a correct party for any other value.

Now suppose that a correct party p decided u due to the early deciding condition at round $t = 2$. This implies that $|V_u^p \cap E^{*,p}| > \frac{|E^p|}{2}$. This also implies that no correct party multicast a valid vote message for any other value. We next observe that for any correct parties p, q, we have $E^{*,p} \subseteq E^q$, and vice versa. Consider any $z \in E^{*,p}$. The echo message of z appeared in the majority of forward messages received by p, at least one of which was sent by a correct party, and thus all correct parties have seen the echo message of z. For a correct party q, denote by F^q the set of corrupt parties in $E^{*,q}$. We thus have $F^q \subseteq E^{*,q} \subseteq E^p$. We thus have that $|V_{u'}^q \cap E^{*,q}| \leq |F^q| < \frac{|H|+|F^q|}{2} \leq \frac{|E^p|}{2} < |V_u^p \cap E^{*,p}|$. Thus we have that the echo2 message from p constitutes the largest set observed by q, when intersected with $E^{*,q}$. And so, in round $t = 3$, q commences Π_{BA} with input

u. This holds for all correct parties, which triggers the validity property of Π_{BA}, and thus all correct parties output u from Π_{BA} and decide u, as required. □

Next, we handle validity and good-case latency.

Claim. $\Pi_{\mathsf{BB,UP}}$ satisfies validity against any $\frac{1}{2}$-bounded adversary. Furthermore, $\Pi_{\mathsf{BB,UP}}$ has good-case latency 2.

Proof. Assume ℓ is correct with input u. Then by the behavior of $\Pi_{\mathsf{BB,UP}}$, it multicasts $\langle \mathsf{echo}, u \rangle_\ell$ to all correct parties at round $t = 0$, and all other correct parties multicast $\langle \mathsf{echo}, \perp \rangle$ at round $t = 0$. Thus, at round $t = 1$, all correct parties multicast $\langle \mathsf{vote}, u \rangle$ and a $\mathsf{forward}$ message that includes all echo messages of all correct parties. In round $t = 2$, no party detects equivocation from ℓ due to ℓ being correct, and all parties see a valid vote message for u from all correct parties, and $H \subseteq E^{`p}$ for all correct parties p. Since the adversary is ρ-bounded, H are a strict majority of the parties, and so any correct party p observes $|V_u^p \cap E^{*,p}| > \frac{|E^p|}{2}$ at round $t = 2$. Thus, all correct parties decide u in round $t = 2$, as required. □

This concludes the proof of Thm. 5. □

6 BB and BA with Optimal Resilience

In this section, we prove the following theorems.

Theorem 6. *For all $\rho \leq 1/2$, there exists a ρ-secure protocol (namely $\Pi_{\mathsf{BB},3}$ below) solving* BB *under dynamic participation with good-case latency $T_{\mathrm{gc}} = 3$.*

Theorem 7. *For all $\rho \leq 1/2$, there exists a ρ-secure protocol (namely $\Pi_{\mathsf{BA},2}$ below) solving* BA *under dynamic participation with good-case latency $T_{\mathrm{gc}} = 2$.*

6.1 BB with Good-Case Latency $T_{\mathrm{gc}} = 3$

In this section, we prove Thm. 6. In this protocol, we make black-box use of the $\frac{1}{2}$-secure dynamic participation BA protocol from [8], which we denote by Π_{BA}.

Protocol 4: $\Pi_{\mathsf{BB},3}$

Setup. Leader ℓ has input u_ℓ. Instructions for party p.

1. **Round** $t = 0$: ℓ multicasts $\langle \mathsf{echo}, u_\ell \rangle_\ell$.
2. **Round** $t = 1$: If received $\langle \mathsf{echo}, u \rangle_\ell$ for some u, multicast $\langle \mathsf{vote}, u \rangle_p$ along with the corresponding echo message from ℓ. Else, multicast $\langle \mathsf{vote}, \perp \rangle_p$.
3. **Round** $t = 2$: Denote by V the set of parties from which p received a vote message. Multicast $\langle \mathsf{forward}, V \rangle_p$, along with the corresponding valid vote messages.
4. **Round** $t = 3$: Denote by G the set of parties from which p received a $\mathsf{forward}$ message, and by V the set of parties from which p received a vote

message, whether directly or via a forward message. Denote by V^* the set of parties q for which the following holds.

(a) p did not detect an equivocation from q, i.e., two valid vote messages signed by q for values $u \neq u'$.

(b) A valid vote message from q appears in more than $\frac{|G|}{2}$ of the forward messages received by p.

Let u be the value $\arg\max_{u \in I} |V_u \cap V^*|$. Multicast $\langle \mathsf{echo2}, V_u \cap V^* \rangle_p$, along with the corresponding vote messages.

Early deciding condition: If the following holds:

(a) p did not detect an equivocation from ℓ, i.e., two valid vote messages signed by ℓ for values $u \neq u'$.

(b) $|V_u \cap V^*| > \frac{|V|}{2}$.

Then decide u and multicast $\langle \mathsf{decided}, u \rangle_p$.

5. **Round** $t \geq 4$:
   (a) **Early deciding:** Denote by D the set of parties from which p received a decided message, and by D^* the set of parties from which p received an echo2 message. If there exists a value u such that $|D_u| > \frac{|D^*|}{2}$, then decide u.
   (b) Let u' be the value for which p received the largest $V_u \cap V^*$ (intersection with *own* V^*) among all received echo2 messages. Run Π_{BA} as instructed that commences in round $t = 4$ with input u', and decide the output of Π_{BA}, if did not decide before.

Proof of Thm. 6. Our protocol is given in $\Pi_{\mathsf{BB},3}$. We now analyze its security and efficiency. Termination follows from the termination of Π_{BA}, as all parties decide and halt once Π_{BA} terminates. We next handle agreement.

Claim. $\Pi_{\mathsf{BB},3}$ satisfies agreement against any $\frac{1}{2}$-bounded adversary.

Proof. There are two cases: either there exists a correct party that decides due to the early deciding condition at round $t = 3$, or not. The proof can be quickly concluded in the latter case, as then no correct party multicasts a decided message, and thus no correct party decides according to the early deciding condition in all rounds $t \geq 3$. Thus, all correct parties decide according to the output of Π_{BA}, which guarantees agreement.

We are now left with the case that there exists a correct party that decides a value u due to the early deciding condition at round $t = 3$. First we prove that this can occur for at most a single value. Assume that there are two correct parties p, q that decide according to the early deciding condition in round $t = 3$ values $u \neq u'$, respectively. We thus have that $|V_u^p \cap V^{*,p}| > \frac{|V^p|}{2}$, and $|V_{u'}^q \cap V^{*,q}| > \frac{|V^q|}{2}$. In particular, both $V_u^p \cap V^{*,p}$ and $V_{u'}^q \cap V^{*,q}$ contain at least one correct party. Which implies that both p, q have observed a valid vote message for both u *and* u'. This implies that both p and q have observed an equivocation by ℓ, and thus would not have decided by the early deciding condition in round $t = 3$.

We are thus left with the case that there exists a unique value u such that a correct party p awake in round $t = 3$ decides u via the early deciding condition.

First, observe that since no correct party multicasts a decided message for a value $u' \neq u$, we have that any correct party deciding via the early deciding condition in round $t \geq 4$ decides u as well. If a correct party p awake in round $t = 3$ decides u via the early deciding condition, this implies that p did not detect an equivocation from ℓ, and that $|V_u^p \cap V^{*,p}| > \frac{|V^p|}{2}$. Denoting by H the set of correct parties awake at round $t = 1$, we have that *none* of them multicast a vote message for a value $u' \neq u$, as otherwise, p would have detected an equivocation from ℓ. For some correct party $q \neq p$ awake at round $t = 4$, consider the set $V_{u'}^q \cap V^{*,q}$ for some value $u' \neq u$. Denote by F the set of corrupt parties. As we have just observed, we have that $V_{u'}^q \cap V^{*,q} \subseteq F$. Note, however, that if some $f \in F$ satisfies $f \in V_{u'}^q \cap V^{*,q}$, then a vote message from f for value u' appears in a majority of the forward messages received by q, thus at least one of them was sent by a correct party, and thus all correct parties awake at round $t = 3$, and in particular p, received a valid vote message for u'. This contradicts the assumption that p decided the value u via the early deciding condition at round $t = 3$. We thus have that $V_{u'}^q \cap V^{*,q} = \emptyset$ for all correct parties awake at round $t \geq 4$. This in particular implies that all correct q parties awake at round $t = 4$ observe u to be the value maximizing $V_u^q \cap V^{*,q}$ among all echo2 messages, and commence Π_{BA} with input u. This triggers the validity property of Π_{BA} which implies that all correct parties output u from Π_{BA}, and thus all correct parties decide u, as required. □

Next, we handle validity and good-case latency.

Claim. $\Pi_{\mathsf{BB},3}$ satisfies validity against any $\frac{1}{2}$-bounded adversary. Furthermore, $\Pi_{\mathsf{BB},3}$ has good-case latency 3.

Proof. Assume ℓ is correct with input u. Then by behavior of $\Pi_{\mathsf{BB},3}$, it multicasts $\langle \mathsf{echo}, u \rangle_\ell$ to all parties in round $t = 0$. Afterwards, again by protocol behavior, all correct parties awake in round $t = 1$, denoted by H, multicast a valid $\langle \mathsf{vote}, u \rangle_p$ message. In round $t = 2$, all correct parties multicast forward messages containing all vote messages of all correct parties awake in round $t = 1$. In round $t = 3$, note first that no correct party p detects an equivocation from ℓ, due to ℓ being correct. Second of all, note that $H \subseteq V_u^p \cap V^{*,p}$, and $|V| \leq |H| + |F|$. Thus, we have that $|V_u^p \cap V^{*,p}| > \frac{|V|}{2}$ holds for any correct party p awake in round $t = 3$. Thus, all correct parties awake in round $t = 3$ decide u and multicast a decided message for u. An identical argument then gives that all correct parties decide u in the first round $t \geq 4$ in which they are awake, due to the early deciding condition. □

This concludes the proof of Thm. 6. □

6.2 BA with Good-Case Latency $T_{\mathbf{gc}} = 2$

In this section, we prove Thm. 7. In this protocol, we make black-box use of the BA protocol from [8], which we denote by Π_{BA}, and which is $\frac{1}{2}$-secure under dynamic participation. Throughout the protocol, whenever we consider a set of

messages S, the notation S^p refers to the local view, or the purported local view, of p of the set S.

Protocol 5: $\Pi_{\mathsf{BA},2}$

Setup. Each party p has input u_p. Instructions for party p.

1. **Round** $t = 0$: Multicast $\langle \mathsf{echo}, u_p \rangle_p$.
2. **Round** $t = 1$: Denote by E the set of parties from which p received an echo message. Multicast $\langle \mathsf{forward}, E \rangle_p$, along with the corresponding echo messages.
3. **Round** $t = 2$: Denote by G the set of parties from which p received a $\mathsf{forward}$ message. Denote by E the set of parties from which p received an echo message, either directly or via a $\mathsf{forward}$ message. For a value u, denote by E_u the set of parties from which p received an echo message for u. Denote by E^* the set of parties q for which the following holds.
   (a) p detected no equivocation from q, i.e., two echo messages signed by q for values $u' \neq u$.
   (b) An echo message from q appears in more than $\frac{|G|}{2}$ of the $\mathsf{forward}$ messages received by p

   For a value u, denote by E^*_u the set $E_u \cap E^*$.
   Early deciding condition: If there exists a value u such that $|E^*_u| > \frac{|E|}{2}$, then decide u. Multicast $\langle \mathsf{decided}, u, E, E^*_u, \{\mathsf{forward}_q \mid q \in G\} \rangle$, where $\mathsf{forward}_q$ indicates the $\mathsf{forward}$ message p received from q. Else, multicast $\langle \mathsf{echo2}, E, E^*, \{\mathsf{forward}_q \mid q \in G\} \rangle$.
4. **Round** $t \geq 3$.
   - Denote by E the set of parties from which p received an echo message, and by E_u the set of parties from which p received an echo message for u .
   - Denote by E^* the set defined in an identical manner as in round $t = 2$ above.
   - Denote by G the set of parties from which p received a $\mathsf{forward}$ message.
   - Denote by T the set of parties from which p received an $\mathsf{echo2}$ message.
   - Denote by G^* the set of parties q for which a $\mathsf{forward}$ message from q appeared in more than $\frac{|T|}{2}$ of the $\mathsf{echo2}$ messages.

   (a) **Early deciding:** For a value u, denote by D_u the set of parties from which p received a $\mathsf{decided}$ message for value u. If there exists a value u such that $|D_u| > \frac{|T|}{2}$, then decide u.
   (b) For a party p, we say a $\mathsf{decided}$ message from a party q of the form $\langle \mathsf{decided}, u, E^q, E^{*,q}_u, \{\mathsf{forward}_z \mid z \in G^q\} \rangle$ is *valid* if the following holds.
   - E^q contains $E^{*,p}$.
   - G^q contains $G^{*,p}$.
   - Each $z \in E^{*,q}_u$ appears in a majority of G^q, and there are no equivocations from z in $\{\mathsf{forward}_y \mid y \in G^q\}$.
   - $|E^{*,q}_u| > \frac{|E^q|}{2}$.

   For a valid $\mathsf{decided}$ message for a value u from a party q, we refer to $|E^q|$ as its *size*. Let u' be the value for which p received the maximum size $\mathsf{decided}$ message. Run Π_{BA} as instructed that commences in round $t = 3$ with input u', and decide the output Π_{BA}, if did not decide beforehand.

Proof of Thm. 7. Our protocol is given in $\Pi_{\mathsf{BA},2}$. We now analyze its security and efficiency. Termination follows from the termination of Π_{BA}, as all parties decide and halt once Π_{BA} terminates. We next handle agreement.

Claim. $\Pi_{\mathsf{BA},2}$ satisfies agreement against any $\frac{1}{2}$-bounded adversary.

Proof. There are two cases: either there exists a correct party that decides due to the early deciding condition at round $t = 2$, or not. The proof can be quickly concluded in the latter case, as all correct parties decide according to the output of Π_{BA}, which is $\frac{1}{2}$-secure and guarantees agreement.

We are now left with the case that there exists a correct party that decides a value u due to the early deciding condition at round $t = 2$. First, we prove that this can occur for at most a single value. Assume that two correct parties p, q decide u, u' according to the early deciding condition in round $t = 2$, respectively. In particular, that implies that $|E_u^{*,p}| > \frac{|E^p|}{2}$, and $|E_{u'}^{*,q}| > \frac{|E^q|}{2}$. Note that by the behavior of the protocol we have that $E^{*,p}, E^{*,q} \subseteq E^p$, and similarly $E^{*,p}, E^{*,q} \subseteq E^q$, since every echo in $E^{*,p}, E^{*,q}$ appeared in the $\mathsf{forward}$ message of at least one correct party. Denote by F_u^p the set of corrupt parties included in $E_u^{*,p}$, and by $F_{u'}^q$ the set of corrupt parties included in $E_{u'}^{*,q}$. Note that $E_u^{*,p} \cap E_{u'}^{*,q} = \emptyset$, as otherwise p, q would have detected an equivocation from the party in the intersection, and would not have included it in their E^* set.

Denote by H^0 the set of correct parties awake at round $t = 0$, and of those, by $H_u^0, H_{u'}^0$ those with input u, u', respectively. One has that

$$|H_u^0| + |F^p| = |E_u^{*,p}| > \frac{|E^p|}{2} \geq \frac{|H^0| + |F^p| + |F^q|}{2}$$

Similarly, one has that

$$|H_{u'}^0| + |F^q| = |E_{u'}^{*,q}| > \frac{|E^q|}{2} \geq \frac{|H^0| + |F^p| + |F^q|}{2}$$

Adding these inequalities, one gets that $|H_u^0| + |H_{u'}^0| > |H^0|$, which is a contradiction.

We are then left with the case that there exists a unique value u such that a correct party p, decides u at round $t = 2$, with reported participation E^p. First note that this implies that any correct party that decides due to the early deciding condition in round $t \geq 3$ also decides u, as no correct party multicasts a $\mathsf{decided}$ message for any value $u' \neq u$. Now, assume that some correct party q, awake in round $t = 3$, received a $\mathsf{decided}$ message from a party $z \in F$ for some value u', of the form $\langle \mathsf{decided}, u', E^z, E_{u'}^{*,z}, \{\mathsf{forward}_s \mid s \in G^z\}\rangle$, with reported participation E^z, such that $|E^z| \geq |E^p|$. We now prove this cannot happen. Assume otherwise (i.e. $|E^z| \geq |E^p|$), and denote by $E_{u'}^{*,z}$ the claimed such set of z. Denote by F_u^p the set of corrupt parties in $E_u^{*,p}$. We have that $|E_u^{*,p}| = |H_u^0| + |F_u^p|$. We next note that E^p contains the set $E_{u'}^{*,z}$. This holds due to the following: A party $s \in E_{u'}^{*,z}$ must appear in a strict majority of $\mathsf{forward}$ messages reported by z, i.e., the set G^z. Since we assume that z sends a *valid* $\mathsf{decided}$ message, we have that $G^{*,q} \subseteq G^z$. Denoting by H^1 the set of correct parties awake at round $t = 1$,

we have that $H^1 \subseteq G^{*,q} \subseteq G^z$. Thus, if party s appears in a strict majority of the forward messages of the claimed set G^z, then at least one of these forward messages was sent by a correct party at round $t = 1$. Thus, p, which was awake at time $t = 2$, observes an echo message from s for u', and thus $s \in E^p$. This gives $E^{*,z}_{u'} \subseteq E^p$. Denoting by $F^z_{u'}$ the corrupt parties in $E^{*,z}_{u'}$, we in particular have $F^z_{u'} \subseteq E^p$.

In fact, note that this line of arguing actually implies a stronger property, and that is that $E^{*,z}_{u'} \cap E^{*,p}_u = \emptyset$, as p seeing an echo for u' from s implies that $s \notin E^{*,p}_u$.

From $F^z_{u'} \subseteq E^p$, and $E^{*,z}_{u'} \cap E^{*,p}_u = \emptyset$, we can deduce that: $|E^{*,p}_u| = |H^0_u| + |F^p_u| > \frac{|E^p|}{2} \geq \frac{|F^z_{u'}|+|F^p_u|+|H^0|}{2}$. We now have all we need to arrive at a contradiction. Let us summarize our observations.

- $E^{*,z}_{u'} \cap E^{*,p}_u = \emptyset$ which in particular implies that $F^z_{u'} \cap F^p_u = \emptyset$.
- $|E^{*,p}_u| = |H^0_u| + |F^p_u| > \frac{|E^p|}{2} \geq \frac{|F^z_{u'}|+|F^p_u|+|H^0|}{2}$.
- $|E^{*,z}_{u'}| \leq |H_{u'}| + |F^z_{u'}|$. This bound trivially holds.
- $|E^z| \geq |E^p|$, our assumption.
- $|E^{*,z}_{u'}| > \frac{|E^z|}{2}$, from the assumption that z's decided message is valid.

From these observation we deduce that:

$$|H^0_u| + |H^0_{u'}| + |F^p_u| + |F^z_{u'}| \geq |E^{*,z}_{u'}| + |E^{*,p}_u| > |E^p| \geq |H^0| + |F^p_u| + |F^z_{u'}|$$

This finally implies that $|H^0_u| + |H^0_{u'}| > |H^0|$, which is a contradiction. We thus have that all correct parties awake in round $t = 3$ view the decided message from p as the valid decided message with the maximum size ($|E^p|$), and so they all commence Π_{BA} with input u. This triggers the validity property of Π_{BA}, and thus all correct parties output u from Π_{BA} and decide u, and agreement holds. □

Next, we handle validity and good-case latency.

Claim. $\Pi_{\mathsf{BA},2}$ satisfies validity against any $\frac{1}{2}$-bounded adversary. Furthermore, $\Pi_{\mathsf{BA},2}$ has good-case latency 2.

Proof. Assume that all correct parties awake in round $t = 0$ have the same input u. Denoting by H^0 the set of correct parties awake in round $t = 0$ and by F the set of corrupt parties, we thus have that $E^{*,p}_u$ contains H^0 for all correct parties p, as they all send an echo message for u in round $t = 0$, and none of them equivocate. It clearly holds, for every party p, that $|E^p| \leq |H| + |F|$, and since $|H| > |F|$ we thus have that $|E^{*,p}_u| > \frac{|E^p|}{2}$ for all correct parties p in round $t = 2$. Thus, all correct parties awake in round $t = 2$ (denoted by H^2) decide u and multicast a decided message for u. Any correct party q, in the first round $t \geq 3$ in which it is awake, observes decided messages for u from all parties in H^2. This constitutes a majority of the received echo2 messages, and so any correct party q also decides u in the first round $t \geq 3$ in which it is awake. □

This concludes the proof of Thm. 7. □

Acknowledgment We thank David Tse for fruitful discussions. The work of YE was conducted in part while at a16z Crypto Research.

References

1. Ittai Abraham, Kartik Nayak, Ling Ren, and Zhuolun Xiang. Good-case latency of byzantine broadcast: a complete categorization. In *PODC*, pages 331–341. ACM, 2021.
2. Christian Badertscher, Peter Gazi, Aggelos Kiayias, Alexander Russell, and Vassilis Zikas. Ouroboros genesis: Composable proof-of-stake blockchains with dynamic availability. In *CCS*, pages 913–930. ACM, 2018.
3. Pierre Civit, Seth Gilbert, Rachid Guerraoui, Jovan Komatovic, Anton Paramonov, and Manuel Vidigueira. All byzantine agreement problems are expensive. In *PODC*, pages 157–169. ACM, 2024.
4. Francesco D'Amato, Giuliano Losa, and Luca Zanolini. Asynchrony-resilient sleepy total-order broadcast protocols. In *PODC*, pages 247–256. ACM, 2024.
5. Francesco D'Amato, Joachim Neu, Ertem Nusret Tas, and David Tse. Goldfish: No more attacks on ethereum?! In *FC (1)*, volume 14744 of *Lecture Notes in Computer Science*, pages 3–23. Springer, 2024.
6. Francesco D'Amato, Roberto Saltini, Thanh-Hai Tran, and Luca Zanolini. Tob-svd: Total-order broadcast with single-vote decisions in the sleepy model, 2023. `arXiv:2310.11331v3`.
7. Yuval Efron, Joachim Neu, and Toniann Pitassi. Fully-fluctuating participation in sleepy consensus. Cryptology ePrint Archive, Paper 2025/1455, 2025. Advances in Financial Technologies (AFT 2025). URL: `https://eprint.iacr.org/2025/1455`, `doi:10.4230/LIPIcs.AFT.2025.7`.
8. Yuval Efron and Ertem Nusret Tas. Dynamically available common subset. Cryptology ePrint Archive, Paper 2025/016, 2025. URL: `https://eprint.iacr.org/2025/016`.
9. Eli Gafni and Giuliano Losa. Brief announcement: Byzantine consensus under dynamic participation with a well-behaved majority. In *DISC*, volume 281 of *LIPIcs*, pages 41:1–41:7. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2023.
10. Juan A. Garay, Aggelos Kiayias, and Nikos Leonardos. The Bitcoin backbone protocol: Analysis and applications. *J. ACM*, 71(4):25:1–25:49, 2024.
11. Seth Gilbert and Nancy A. Lynch. Brewer's conjecture and the feasibility of consistent, available, partition-tolerant web services. *SIGACT News*, 33(2):51–59, 2002.
12. Vipul Goyal, Hanjun Li, and Justin Raizes. Instant block confirmation in the sleepy model. In *Financial Cryptography (2)*, volume 12675 of *Lecture Notes in Computer Science*, pages 65–83. Springer, 2021.
13. Pankaj Khanchandani and Roger Wattenhofer. Byzantine agreement with unknown participants and failures. In *IPDPS*, pages 952–961. IEEE, 2021.
14. Aggelos Kiayias, Alexander Russell, Bernardo David, and Roman Oliynykov. Ouroboros: A provably secure proof-of-stake blockchain protocol. In *CRYPTO (1)*, volume 10401 of *Lecture Notes in Computer Science*, pages 357–388. Springer, 2017.
15. Leslie Lamport, Robert E. Shostak, and Marshall C. Pease. The byzantine generals problem. *ACM Trans. Program. Lang. Syst.*, 4(3):382–401, 1982.
16. Andrew Lewis-Pye and Tim Roughgarden. Permissionless consensus, 2023. `arXiv:2304.14701v5`.

17. Giuliano Losa and Eli Gafni. Consensus in the unknown-participation message-adversary model, 2023. arXiv:2301.04817v2.
18. Dahlia Malkhi, Atsuki Momose, and Ling Ren. Byzantine consensus under fully fluctuating participation. Cryptology ePrint Archive, Paper 2022/1448, Version 20221024:011919, 2022. URL: https://eprint.iacr.org/archive/2022/1448/20221024:011919.
19. Dahlia Malkhi, Atsuki Momose, and Ling Ren. Towards practical sleepy BFT. In *CCS*, pages 490–503. ACM, 2023.
20. Atsuki Momose and Ling Ren. Optimal communication complexity of authenticated byzantine agreement. In *DISC*, volume 209 of *LIPIcs*, pages 32:1–32:16. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021.
21. Atsuki Momose and Ling Ren. Constant latency in sleepy consensus. In *CCS*, pages 2295–2308. ACM, 2022.
22. Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008. URL: https://bitcoin.org/bitcoin.pdf.
23. Joachim Neu, Ertem Nusret Tas, and David Tse. Ebb-and-flow protocols: A resolution of the availability-finality dilemma. In *SP*, pages 446–465. IEEE, 2021.
24. Rafael Pass and Elaine Shi. The sleepy model of consensus. In *ASIACRYPT (2)*, volume 10625 of *Lecture Notes in Computer Science*, pages 380–409. Springer, 2017.
25. Srivatsan Sridhar, Ertem Nusret Tas, Joachim Neu, Dionysis Zindros, and David Tse. Consensus under adversary majority done right. Cryptology ePrint Archive, Paper 2024/1799, 2024. Financial Cryptography and Data Security (FC 2025). URL: https://eprint.iacr.org/2024/1799.
26. Jun Wan, Hanshen Xiao, Elaine Shi, and Srinivas Devadas. Expected constant round byzantine broadcast under dishonest majority. *J. ACM*, 72(4):30:1–30:39, 2025.

A Folklore BA for Static Participation with $\rho < 1/3$ and $T_{\mathbf{gc}} = 1$

In this section we show, for completeness, the following folklore results.

Lemma 1. *For all $\rho \leq 1/3$, there exists a ρ-secure* BA *protocol (namely* $\mathsf{Sync}_{\mathsf{BA},1}$ *below) with good-case latency $T_{\mathrm{gc}} = 1$ under static participation in synchrony.*

Lemma 2. *For all $\rho > \frac{1}{3}$, there is no ρ-secure* BA *protocol with good-case latency ≤ 1 under static participation in synchrony.*

Proof. Denote by Π_{BA} an arbitrary choice of BA protocol which is $\frac{1}{3}$-secure under static participation in synchrony. We treat it as a black-box. Our protocol is given below:

Protocol 6: $\mathsf{Sync}_{\mathsf{BA},1}$

Setup. Each party p has input u_p. Instructions for party p. Denote by n the number of parties and by $f < \frac{n}{3}$ the bound on the number of corrupted parties. Initialize $o_p \leftarrow u_p$.

1. **Round** $t = 0$: Multicast $\langle \mathsf{echo}, u_p \rangle_p$.

2. **Round** $t = 1$: **Early deciding condition.** If there exists a value u such that p received $n - f$ echo messages for u, then decide u. Denote $n - f$ echo messages for a value u by $\mathcal{C}(u)$. Multicast $\langle \mathsf{decided}, \mathcal{C}(u) \rangle$.
3. **Round** $t \geq 2$**:** If received $\mathcal{C}(u)$ for some value u, set $o_p \leftarrow u$. Run Π_{BA} with input o_p that commences at round $t = 2$, and decide accordingly, if have not decided before.

Termination is clear from the termination of Π_{BA}. For agreement, if no correct party decides via the early deciding condition in round $t = 1$, then agreement holds by the agreement property of Π_{BA}. Else, let p be a correct party that decides a value u in round $t = 1$, thus p observed $n - f$ echo messages for u, since $f < \frac{n}{3}$, a quorum intersection argument implies that no $n - f$ echo messages exist for any other value, and so all correct parties set their local o variable to u in round $t = 2$. This triggers the validity property of Π_{BA}, and so all correct parties output u, as required. For validity and good-case latency, consider the case where all correct parties have the same input value u. Then by the behavior of the protocol, all correct parties see in round $t = 1$ $n - f$ echo messages for u, and decide u, as required. This concludes the proof. □

Next, we prove Lem. 2.

Proof. Let $\rho > \frac{1}{3}$, and let n be a natural number, and consider three disjoint sets of parties A, B, C, each of size $\frac{n}{3}$. Assume towards a contradiction that there exists a ρ-secure protocol solving BA under synchrony with static participation and good-case latency 1. We consider three executions G_1, G_2, G_3, as follows.

1. G_1: A, B are correct with input 1. C are corrupt, and behave as if they are correct with input 0. Note that the adversary is ρ-bounded.
2. G_2: A, C are correct, B are corrupt. The adversary is ρ-bounded. A has input 1, C has input 0. B behave in round $t = 0$ to A as if they are correct with input 1, and to C as if they are correct with input 0, B then halts.
3. G_3: Dual to G_1. B, C are correct with input 0. A are corrupt, and behave as if they are correct with input 1. Note that the adversary is ρ-bounded.

Note that in G_1, all correct parties have the same input 1, and so the parties in A decide 1 after one round. Note that up to the end of the first round, G_1, G_2 are indistinguishable from the perspective of A, and so also in G_2, A decides 1 after 1 round. A dual argument gives that C outputs 0 after one round both in G_3 and G_2. Lastly note that in G_2, the adversary is ρ-bounded, and so by assumption that Π is ρ-secure, agreement must hold and A, C output the same value in G_2, leading to a contradiction. □