Synchronous Consensus with Optimal Asynchronous Fallback Guarantees

Erica Blum* Jonathan Katz* Julian Loss†

Abstract

Typically, protocols for Byzantine agreement (BA) are designed to run in either a *synchronous* network (where all messages are guaranteed to be delivered within some known time Δ from when they are sent) or an *asynchronous* network (where messages may be arbitrarily delayed). Protocols designed for synchronous networks are generally insecure if the network in which they run does not ensure synchrony; protocols designed for asynchronous networks are (of course) secure in a synchronous setting as well, but in that case tolerate a lower fraction of faults than would have been possible if synchrony had been assumed from the start.

Fix some number of parties n, and $0 < t_a < n/3 \leq t_s < n/2$. We ask whether it is possible (given a public-key infrastructure) to design a BA protocol that (1) is resilient to any t_s corruptions when run in a synchronous network and (2) remains resilient to t_a faults even if the network happens to be asynchronous. We show matching feasibility and infeasibility results demonstrating that this is possible if and only if $t_a + 2 \cdot t_s < n$.

1 Introduction

Byzantine agreement (BA) [22,31] is a classical problem in distributed computing. Roughly speaking, a BA protocol allows a group of n parties, each holding some initial input value, to agree on their outputs even in the presence of some threshold of corrupted parties. Such protocols are used widely in practice for ensuring consistency among a set of distributed processors [6,19,21,26], and have received renewed interest in the context of blockchain protocols. They also serve as a core building block for more complicated protocols, e.g., for secure multiparty computation. There is an extensive literature on Byzantine agreement, and many different models in which it can be studied. We focus here on the setting in which a *public-key infrastructure* (PKI) is available.

Typically, protocols for Byzantine agreement are designed and analyzed assuming either a *synchronous network* (where messages are guaranteed to be delivered within some known time bound Δ) or an *asynchronous network* (where messages can be delayed arbitrarily). Existing results precisely characterize when the problem can be solved in each case [5,8,10,22,31]: in a synchronous network, it is possible if and only if $t_s < n/2$ parties are corrupted, while in an asynchronous network it can be achieved only when there are $t_a < n/3$ corruptions. In each case, protocols tolerating the optimal threshold and running in expected *constant* rounds are known [5,18].

In real-world deployments of Byzantine agreement, the network conditions in which a protocol are run may be unclear. For example, the network may generally be synchronous but intermittently

*Dept. of Computer Science, University of Maryland. **Email:** {erblum,jkatz}@cs.umd.edu.
†Ruhr University Bochum. **Email:** julian.loss@rub.de.

experience congestion that prevents messages from being delivered in a timely fashion. This results in the following dilemma when deciding which type of protocol to use:

- Protocols designed for a synchronous network are, in general, completely insecure if the assumption of network synchrony fails.
- Protocols designed for an asynchronous network will (of course) be secure when the network is synchronous. But in this case the fraction of faults that can be tolerated is *lower* than what could have been tolerated if the protocol were designed for the synchronous setting.

Fix some thresholds t_a, t_s with $0 < t_a < n/3 \leq t_s < n/2$. We ask the following question: is it possible to design a BA protocol that is (1) resilient to any t_s (adaptive) corruptions when run in a synchronous network and also (2) resilient to t_a (adaptive) corruptions even if the network happens to be asynchronous? We completely resolve this question by showing matching feasibility and infeasibility results demonstrating that this is possible if and only if $t_a + 2 \cdot t_s < n$.

Positive result. The protocol achieving our positive result is constructed by combining two sub-protocols $\Pi_{\mathsf{SBA}}, \Pi_{\mathsf{ABA}}$ for Byzantine agreement, where Π_{SBA} is secure in a synchronous network and Π_{ABA} is secure in an asynchronous network. The key to our analysis is to separately analyze the validity, consistency, and liveness guarantees of these sub-protocols. Specifically, we design Π_{SBA} so that it also satisfies a certain validity guarantee *even when run in an asynchronous network*. We also design Π_{ABA} so that it achieves validity (in an asynchronous network) *even beyond* $n/3$ *corruptions*. We then use these properties to prove security of our main protocol, for different thresholds, when run in either a synchronous or asynchronous network.

Impossibility result. We also show that our positive result is *tight*, namely, that if $t_a + 2 \cdot t_s \geq n$ then there is no protocol that is simultaneously resilient to t_s corruptions when run in a synchronous network and also resilient to t_a faults in an asynchronous network. In fact, we show an result that is slightly stronger: it is not possible to achieve validity for t_s faults in the synchronous setting while also achieving a weak notion of consistency for t_a faults in an asynchronous network.

1.1 Related Work

The question of designing protocols suitable for either synchronous or asynchronous networks is a natural one. It is therefore somewhat surprising that it has only recently begun to draw attention in the literature. The recent work by Guo, Pass, and Shi [15] is most closely related to our own. Guo et al. consider a model motivated by *eclipse attacks* [17] on blockchain protocols, whereby an attacker temporarily disconnects some subset S of honest parties from the rest of the network S', e.g., by delaying or dropping messages between S and S'. Clearly, parties in S will not be able to reach agreement with honest parties in S'; nevertheless, as observed by Guo et al., it may be possible to provide certain guarantees for the parties in S' if their network is well-behaved (i.e., synchrony continues to hold for messages sent between parties in S'). Guo et al. gave BA protocols tolerating the optimal corruption threshold in this model, and Abraham et al. [2] extended their work to achieve similar guarantees for state-machine replication. The main difference between these works and ours is that they continue to assume synchrony in part of the network, and their protocols fail completely if the network is fully asynchronous.

Work of Kursawe [20] is also closely related to ours. Kursawe shows a protocol for asynchronous BA that reaches agreement more quickly in case the network is synchronous. In contrast to our work, that protocol does not achieve better fault tolerance (and, in particular, cannot tolerate $n/3$ or more faults) in the synchronous case.

Other recent work has looked at designing protocols for synchronous BA that achieve good *responsiveness* when the network latency is low. That is, these protocols ensure that if the actual message-delivery time is $\delta < \Delta$ then the time to reach agreement is proportional to δ rather than the upper bound Δ. This problem was considered by Pass and Shi [27, 28], who gave protocols that rely on a leader and are therefore not adaptively secure, as well as by Loss and Moran [24], who avoid the use of a leader. The work of Loss and Moran was extended by Liu-Zhang et al. [23] to the case of general secure computation. None of these works provides any security in case the synchrony assumption fails.

Several prior works [3, 7, 12, 30] consider a model in which synchrony is assumed to be available for some (known) limited period of time, and asynchronous otherwise. Fitzi et al. [11] and Loss and Moran [24] study trade-offs between the validity, consistency, and liveness properties of BA that inspired our asynchronous BA protocol in Section 3 and our lower bound in Section 5.

1.2 Paper Organization

We introduce our model as well as definitions for Byzantine agreement and related tasks in Section 2. In Section 3 we describe two protocols for Byzantine agreement and prove various properties about them. Those protocols are used, in turn, as sub-protocols of our main protocol in Section 4 that achieves security (for different thresholds) in both synchronous and asynchronous networks. Finally, in Section 5 we show that the bounds we achieve are tight.

2 Model and Definitions

Throughout, we consider a network of n parties $P_1, \ldots, P_n$ who may communicate over point-to-point authenticated channels. We also assume that the parties have established a public-key infrastructure in advance of the protocol execution. This means that all parties hold the same vector $(pk_1, \ldots, pk_n)$ of public keys for a digital signature scheme, where each honest party P_i holds the honestly generated secret key sk_i associated with pk_i. (Malicious parties may choose their keys arbitrarily.) A *valid* signature σ on m from P_i is one for which $\mathsf{Verify}_{pk_i}(m, \sigma) = 1$. We make the standard convention of treating signatures as idealized objects; i.e., throughout our analysis, signatures are assumed to be perfectly unforgeable. When the signature scheme used is existentially unforgeable under chosen-message attacks we thus obtain security against computationally bounded adversaries, with a negligible probability of failure.

When we say a protocol tolerates t corrupted parties we always mean that it is secure against an adversary who may *adaptively* corrupt up to t parties during execution of the protocol and coordinate the actions of those parties as they deviate from the protocol in an arbitrary manner. An honest party is one who is not corrupted by the end of the protocol.

We consider protocols running in one of two possible settings. When we refer to a protocol running in a *synchronous* network, we assume that all messages that are sent are delivered within a known time bound Δ. We allow the adversary to arbitrarily schedule delivery of messages subject to this bound, which implies in particular that we consider a *rushing* adversary who may obtain messages sent to it before sending messages of its own. When we refer to a protocol running in an *asynchronous* network, we allow the adversary to arbitrarily schedule delivery of messages without any upper bound on their delivery time. We do, however, require that all messages that are sent are eventually delivered. Importantly, honest parties do not know *a priori* which type of network the protocol is running in.

We assume parties each have a local clock that progresses at the same rate. This allows us to consider protocols that execute in a series of *rounds*, where execution of the protocol begins at time 0 and the rth round refers to the period of time from $(r-1)\cdot\Delta$ to $r\cdot\Delta$. When we say a party receives a message in round r we mean that it receives a message in that time interval; when we say it sends a message in round r we means it sends that message at the beginning of that round, i.e., at time $(r-1)\cdot\Delta$. Thus, in a synchronous network all messages sent in round r are received in round r (but in an asynchronous network this need not be the case).

We assume a *coin-flip mechanism* $\mathsf{CoinFlip}$ available as an atomic primitive. This can be viewed as an ideal functionality, parameterized by a value t_a, that upon receiving input k from t_a+1 parties generates an unbiased coin $\mathsf{Coin}_k \in \{0,1\}$ that is sent to all parties. (When run in an asynchronous network, messages to and from $\mathsf{CoinFlip}$ can be arbitrarily delayed.) The key property this ensures is that, if at most t_a parties are corrupted, at least one honest party must send k to $\mathsf{CoinFlip}$ before the adversary can learn Coin_k. Several protocols for realizing such a coin flip in an asynchronous network, for $t_a < n/3$ faults, are known[1] [1, 5, 25, 29] based on general assumptions. It is also possible to realize this primitive using a threshold unique signature scheme [4, 13, 16, 24].

2.1 Definitions

We are ultimately interested in *Byzantine agreement*, but we find it useful to define the related notions of *broadcast* and *graded consensus*. Relevant definitions follow.

Byzantine agreement. Byzantine agreement allows a set of parties who each hold some initial input to agree on their output. We consider several security properties that may hold for such protocols. For simplicity, we consider the case of agreement on a bit; this is without loss of generality as one can run any such protocol ℓ times to agree on a string of length ℓ.

We consider Byzantine agreement protocols where, in some cases, parties may not terminate immediately after generating output, or may never terminate. For that reason, we treat termination separately in the definition that follows. By convention, any party that terminates generates output before doing so; however, we allow parties to output the special symbol $\perp$.

Definition 1 (Byzantine agreement). *Let Π be a protocol executed by parties $P_1, \ldots, P_n$, where each party P_i begins holding input $v_i \in \{0,1\}$.*

- **Weak validity:** Π *is t-*weakly valid *if the following holds whenever at most t of the parties are corrupted: if every honest party's input is equal to the same value v, then every honest party outputs either v or $\perp$.*
- **Validity:** Π *is t-*valid *if the following holds whenever at most t of the parties are corrupted: if every honest party's input is equal to the same value v, then every honest party outputs v.*
- **Validity with termination:** Π *is t-*valid with termination *if the following holds whenever at most t of the parties are corrupted: if every honest party's input is equal to the same value v, then every honest party outputs v and terminates.*

[1]Some of these realize a p-weak coin flip, where honest parties agree on the coin only with probability $p < 1$. We can also rely on such protocols, at an increase in the expected round complexity by a factor of $O(1/p)$.

- **Weak consistency:** Π *is* t-weakly consistent *if the following holds whenever at most* t *of the parties are corrupted: there is a* $v \in \{0,1\}$ *such that every honest party outputs either* v *or* $\perp$.
- **Consistency:** Π *is* t-consistent *if the following holds whenever at most* t *of the parties are corrupted: there is a* $v \in \{0,1,\perp\}$ *such that every honest party outputs* v.

  (In the terminology of Goldwasser and Lindell [14], weak consistency might be called "consistency with abort" and consistency might be called "consistency with unanimous abort.")
- **Liveness:** Π *is* t-live *if whenever at most* t *of the parties are corrupted, every honest party outputs a value in* $\{0,1\}$.
- **Termination:** Π *is* t-terminating *if whenever at most* t *of the parties are corrupted, every honest party terminates. If* Π *is* n*-terminating it is said to have* guaranteed termination.

If Π *is* t*-valid,* t*-consistent,* t*-live, and* t*-terminating, then we say* Π *is* t-secure.

While several of the above definitions are not standard, our notion of security matches the standard one. In particular, t-liveness and t-consistency imply that whenever at most t parties are corrupted, there is a $v \in \{0,1\}$ such that every honest party outputs v. Note that t-validity with termination is weaker than t-validity plus t-termination, as the former does not require termination in case the inputs of the honest parties do not agree.

Broadcast. Protocols for *broadcast* allow a set of parties to agree on a value chosen by a designated sender. We only consider broadcast protocols with guaranteed termination, and so do not consider termination separately in the following definition.

Definition 2 (Broadcast). *Let* Π *be a protocol executed by parties* $P_1, \ldots, P_n$*, where a sender* $P^* \in \{P_1, \ldots, P_n\}$ *begins holding an input* $v^* \in \{0,1\}$ *and all parties are guaranteed to terminate.*

- **Weak validity:** Π *is* t-weakly valid *if the following holds whenever at most* t *of the parties are corrupted: if* P^* *is honest, then every honest party outputs either* v^* *or* $\perp$.
- **Validity:** Π *is* t-valid *if the following holds whenever at most* t *of the parties are corrupted: if* P^* *is honest, then every honest party outputs* v^*.
- **Weak consistency:** Π *is* t-weakly consistent *if the following holds whenever at most* t *of the parties are corrupted: there is a* $v \in \{0,1\}$ *such that every honest party outputs either* v *or* $\perp$.
- **Consistency:** Π *is* t-consistent *if the following holds whenever at most* t *of the parties are corrupted: there is a* $v \in \{0,1,\perp\}$ *such that every honest party outputs* v.
- **Liveness:** Π *is* t-live *if whenever at most* t *of the parties are corrupted, every honest party outputs a value in* $\{0,1\}$.

If Π *is* t*-valid,* t*-consistent, and* t*-live, then we say it is* t-secure.

Graded consensus. As a stepping stone to Byzantine agreement, it is also useful to define *graded consensus* [9]. Here, each party outputs both a value as well as a *grade* $g \in \{0,1,2\}$. As in the case of Byzantine agreement, we consider protocols that may not terminate; however, parties terminate upon generating output.

Definition 3 (Graded consensus). *Let* Π *be a protocol executed by parties* $P_1, \ldots, P_n$*, where each party* P_i *begins holding input* $v_i \in \{0,1\}$ *and all parties terminate upon generating output.*

- **Graded validity:** Π *achieves* t-graded validity *if the following holds whenever at most* t *of the parties are corrupted: if every honest party's input is equal to the same value* v*, then all honest parties output* $(v, 2)$.

- **Graded consistency:** Π *achieves* t-graded consistency *if the following hold whenever at most* t *of the parties are corrupted: (1) If two honest parties output grades* g, g'*, then* $|g - g'| \leq 1$*. (2) If two honest parties output* (v, g) *and* (v', g') *with* $g, g' \geq 1$*, then* $v = v'$.

- **Liveness:** Π *is* t-live *if whenever at most* t *of the parties are corrupted, every honest party outputs* (v, g) *with either* $v \in \{0,1\}$ *and* $g \geq 1$*, or* $v = \perp$ *and* $g = 0$.

If Π *achieves* t*-graded validity,* t*-graded consistency, and* t*-liveness then we say it is* t-secure*.*

3 Useful Sub-Protocols

We introduce two sub-protocols that we rely on when constructing our main protocol. In Section 3.1 we show a protocol that is secure for some threshold of corrupted parties when run in a synchronous network, and achieves weak validity—for a lower threshold—even when run in an asynchronous network. The protocol we describe in Section 3.2 is secure for some threshold when run in an asynchronous network; we show that it achieves validity for a higher threshold.

3.1 Synchronous Byzantine Agreement with Fallback (Weak) Validity

In this section we introduce a protocol for synchronous BA with a fallback validity property. That is, the protocol is secure when run in a synchronous network (for some threshold t_s of corrupted parties), and achieves weak validity even when run in an asynchronous network (though liveness and weak consistency may not hold) for a lower threshold t_a.

Protocol Π_{DS}

Round 1: P^* signs its input v^* to obtain a signature σ^*. It sets $\mathsf{SET} := \{\sigma^*\}$ and sends (v^*, SET) to all parties.

Rounds 1 to $\mathbf{n-1}$**:** Each P_i begins with $\mathsf{ACC}_i = \emptyset$, and then acts as follows: upon receiving an r-correct message (v, SET) in round r, add v to ACC_i. If $r < n-1$, then also compute a signature σ_i on v, let $\mathsf{SET} := \mathsf{SET} \cup \{\sigma_i\}$, and send (v, SET) to all parties in the following round. (This is done at most once for each (v, r) pair.)

Output determination: At time $(n-1) \cdot \Delta$, if ACC_i contains one value, then output that value and terminate. In any other case, output $\perp$ and terminate.

Figure 1: The Dolev-Strong broadcast protocol Π_{DS}.

Our protocol relies on a variant of the Dolev-Strong broadcast protocol [8] as a subroutine. Since we use a slightly non-standard version of that protocol, we describe it in Figure 1 for completeness. In the protocol, we say that (v, SET) is an *r-correct message* (from the point of view of a party P_i) if SET contains valid signatures on v from P^* and $r-1$ additional, distinct parties other than P_i.

Lemma 1. *Broadcast protocol Π_{DS} satisfies the following properties:*

1. *When run in a synchronous network, it is n-valid and n-consistent.*

2. *When run in an asynchronous network, it is n-weakly valid.*

Proof. The standard analysis of the Dolev-Strong protocol shows that, when run in a synchronous network with any number of corrupted parties, $\mathsf{ACC}_i = \mathsf{ACC}_j$ for any honest parties P_i, P_j. This implies n-consistency. Since an honest P^* sends a 1-correct message to all honest parties, and the attacker cannot forge signatures of the honest sender, n-validity holds.

The second claim follows because an attacker cannot forge the signature of an honest P^*. □

We now define a BA protocol using Π_{DS} as a sub-routine. This protocol is parameterized by a value t_a which determines the security thresholds the protocol satisfies.

Protocol $\Pi_{\mathsf{SBA}}^{t_a}$

Each P_i initially holds a bit v_i. The protocol proceeds as follows:

- Each party P_i broadcasts v_i by running Π_{DS} as the sender.
- Let v_j^i denote the output of P_i in the jth execution of Π_{DS}.
- Each P_i generates output as follows: if there are at least $2t_a + 1$ values v_j^i that are in $\{0, 1\}$, then output the majority of those values and terminate. Otherwise, output $\perp$ and terminate.

Figure 2: A Byzantine agreement protocol, parameterized by t_a.

Theorem 1. *For any t_a, t_s with $t_a < n/3$ and $t_a + 2 \cdot t_s < n$, Byzantine agreement protocol $\Pi_{\mathsf{SBA}}^{t_a}$ satisfies the following properties:*

1. *When the protocol is run in a synchronous network, it is t_s-secure.*

2. *When the protocol is run in an asynchronous network, it is t_a-weakly valid.*

Moreover, every honest party terminates in time at most $n \cdot \Delta$ regardless of the network behavior or the number of corrupted parties (and so the protocol has guaranteed termination).

Proof. The claim about termination is immediate, since Π_{DS} terminates in time $(n-1) \cdot \Delta$.

When run in a synchronous network with t_s corrupted parties, at least $n - t_s > 2t_a$ of the executions of Π_{DS} result in boolean output for all honest parties (by n-validity of Π_{DS}) and so all honest parties generate boolean output in $\Pi_{\mathsf{SBA}}^{t_a}$; this proves t_s-liveness. By n-consistency of Π_{DS}, all honest parties agree on the $\{v_j\}$ values they obtain and hence $\Pi_{\mathsf{SBA}}^{t_a}$ is t_s-consistent (in fact, it is n-consistent). Finally, n-validity of Π_{DS} implies that when all honest parties begin holding the same input $v \in \{0, 1\}$, then all honest parties will have v as their majority value. This proves t_s-validity (in fact, the protocol is $(n-1)/2$-valid).

For the second claim, assume all honest parties begin holding the same input v, and t_a parties are corrupted. Any honest party P_i who generates boolean output must have at least $2t_a + 1$ boolean values $\{v_j^i\}$, of which at most t_a of these can be equal to $\bar{v}$. Hence, any honest party who generates boolean output will in fact output v. □

3.2 Validity-Optimized Asynchronous Byzantine Agreement

In this section we construct a protocol for asynchronous Byzantine agreement that is t_a-secure, and achieves validity with termination even for $t_s > t_a$ corrupted parties. That is:

Theorem 2. *For any t_a, t_s with $t_a < n/3$ and $t_a + 2 \cdot t_s < n$, there is an n-party protocol for Byzantine agreement that, when run in an asynchronous network, is t_a-secure and also achieves t_s-validity with termination.*

Throughout this section we only consider protocols running in an asynchronous network, and so drop explicit mention of this from now on.

Our proof of Theorem 2 proceeds in a number of steps. In Section 3.2.1 we describe a "validity-optimized" protocol $\Pi_{\mathsf{GC}}^{t_a}$ for graded consensus that is t_a-secure and also achieves t_s-graded validity. Then, in Section 3.2.2, we show a Byzantine agreement protocol $\Pi_{\mathsf{ABA}}^{t_a}$ using $\Pi_{\mathsf{GC}}^{t_a}$ as a subroutine. This protocol illustrates our main ideas, and achieves the properties claimed in Theorem 2 except termination. We then discuss how termination can be added using existing techniques.

Our protocol is based on the work of Mostéfaoui et al. [25], but allows for variable thresholds. Also, our description simplifies theirs by presenting the protocol in a modular fashion.

3.2.1 Validity-Optimized Graded Consensus

Our graded consensus protocol relies on a sub-protocol $\Pi_{\mathsf{prop}}^{t_s}$ for proposing values that is shown in Figure 3. This protocol is parameterized by a value t_s which determines its security thresholds. We begin by proving some properties of $\Pi_{\mathsf{prop}}^{t_s}$. Throughout, we let n denote the number of parties.

Protocol $\Pi_{\mathsf{prop}}^{t_s}$

We describe the protocol from the point of view of a party with input $v \in \{0, 1, \lambda\}$.

1. Set $\mathsf{vals} := \emptyset$.
2. Send $(\mathsf{prepare}, v)$ to all parties.
3. Upon receiving the message $(\mathsf{prepare}, b)$, for some $b \in \{0, 1, \lambda\}$, from strictly more than t_s parties, do: If $(\mathsf{prepare}, b)$ has not been sent, then send $(\mathsf{prepare}, b)$ to all parties.
4. Upon receiving the message $(\mathsf{prepare}, b)$, for some $b \in \{0, 1, \lambda\}$, from at least $n - t_s$ parties, set $\mathsf{vals} := \mathsf{vals} \cup \{b\}$.
5. Upon adding the first value $b \in \{0, 1, \lambda\}$ to vals (breaking ties lexicographically), send $(\mathsf{propose}, b)$ to all parties.
6. Once at least $n - t_s$ messages $(\mathsf{propose}, b)$ have been received on values $b \in \mathsf{vals}$, let $\mathsf{prop} \subseteq \mathsf{vals}$ be the set of values carried by those messages. Output prop and terminate.

Figure 3: A sub-protocol for proposing values, parameterized by t_s.

Lemma 2. *Assume $t_a < n - 2 \cdot t_s$ parties are corrupted in an execution of $\Pi_{\mathsf{prop}}^{t_s}$. If two honest parties P_i, P_j output $\{b\}$, $\{b'\}$, respectively, then $b = b'$.*

Proof. Since P_i outputs $\{b\}$, it must have received at least $n - t_s$ messages $(\mathsf{propose}, b)$, of which at least $n - t_s - t_a$ of those were sent by honest parties. Similarly, P_j must have received at least $n - t_s - t_a$ messages $(\mathsf{propose}, b')$ that were sent by honest parties. If $b \neq b'$, then because

$2 \cdot (n - t_s - t_a)$ is strictly greater than the number of honest parties $n - t_a$, this would mean that some honest party sent $\mathsf{propose}$ messages on two different values, which is impossible. $\square$

Lemma 3. *Assume $t_a \leq t_s$ parties are corrupted in an execution of $\Pi^{t_s}_{\mathsf{prop}}$. If no honest party has input v, then no honest party outputs prop containing v.*

Proof. If v was not input by any honest party, then at most $t_a \leq t_s$ messages $(\mathsf{prepare}, v)$ are sent in step 2. Thus, no honest party ever sends a message $(\mathsf{prepare}, v)$, and consequently no honest party ever sends a message $(\mathsf{propose}, v)$. It follows that no honest party ever adds v to vals, and so no honest party outputs prop containing v. $\square$

Lemma 4. *Assume t_a parties are corrupted in an execution of $\Pi^{t_s}_{\mathsf{prop}}$, where $t_a < n - 2 \cdot t_s$ and $t_a \leq t_s$. If an honest party sends a message $(\mathsf{propose}, b)$, all honest parties add b to vals.*

Proof. Suppose some honest party P_i sends $(\mathsf{propose}, b)$. Then P_i must have received at least $n - t_s$ messages $(\mathsf{prepare}, b)$. At least $n - t_s - t_a > t_s$ of these must have been sent by honest parties, and so eventually all other honest parties also receive strictly more than t_s messages $(\mathsf{prepare}, b)$. We thus see that any honest party who has not already sent $(\mathsf{prepare}, b)$ will do so in step 3. Therefore, every honest party will eventually receive at least $n - t_a \geq n - t_s$ messages $(\mathsf{prepare}, b)$, and consequently every honest party will add b to vals. $\square$

Note that whenever parties in $\Pi^{t_s}_{\mathsf{prop}}$ generate output, they terminate. While $\Pi^{t_s}_{\mathsf{prop}}$ does not necessarily terminate (for example, if honest parties are split evenly among 0, 1, and λ), they do terminate as long as honest parties hold at most two different input values.

Lemma 5. *Assume t_a parties are corrupted in an execution of $\Pi^{t_s}_{\mathsf{prop}}$, where $t_a < n - 2 \cdot t_s$ and $t_a \leq t_s$. If all honest parties hold one of two different inputs, then all honest parties terminate.*

Proof. We first argue that every honest party sends a $\mathsf{propose}$ message. Indeed, there are $n - t_a$ honest parties, so at least $\frac{1}{2}(n - t_a) > t_s$ honest parties must have the same input v. Therefore, all honest parties receive strictly more than t_s messages $(\mathsf{prepare}, v)$. Consequently, all honest parties that have not already sent $(\mathsf{prepare}, v)$ will do so in step 3. Thus, every honest party receives $n - t_a \geq n - t_s$ messages $(\mathsf{prepare}, v)$ and adds v to vals. In particular, vals is nonempty and so every honest party sends a $\mathsf{propose}$ message.

Each honest party thus receives at least $n - t_a \geq n - t_s$ $\mathsf{propose}$ messages sent by honest parties. Let prop denote the set of values carried by those messages. By Lemma 4, for any b proposed by an honest party, all honest parties eventually have $b \in \mathsf{vals}$. Thus, eventually all honest parties hold at least $n - t_s$ propose messages such that the set of their carried values prop satisfies $\mathsf{prop} \subset \mathsf{vals}$, and therefore all honest parties terminate. $\square$

$\Pi^{t_s}_{\mathsf{prop}}$ satisfies a notion of validity even for t_s corrupted parties.

Lemma 6. *Assume $t_s < n/2$ parties are corrupted in an execution of $\Pi^{t_s}_{\mathsf{prop}}$. If all honest parties hold the same input v, then all honest parties output $\mathsf{prop} = \{v\}$.*

Proof. Suppose t_s parties are corrupted, and all honest parties hold the same input v. In step 2, all $n - t_s$ honest parties send $(\mathsf{prepare}, v)$, and so all honest parties add v to vals. Any $\mathsf{prepare}$ messages on other values in step 2 are sent by the $t_s < n - t_s$ corrupted parties, and so no honest party ever adds a value other than v to vals. Thus, all honest parties send their (single) $\mathsf{propose}$ message on the value v in step 5. It follows that every honest party outputs $\mathsf{prop} = \{v\}$ in step 6. $\square$

Protocol $\Pi^{t_s}_{\mathsf{GC}}$

We describe the protocol from the point of view of a party with input $v \in \{0,1\}$.

- Set $b_1 := v$.
- Run protocol $\Pi^{t_s}_{\mathsf{prop}}$ using input b_1, and let prop_1 denote the output.
- If $\mathsf{prop}_1 = \{b\}$, then set $b_2 := b$. Otherwise, set $b_2 := \lambda$.
- Run protocol $\Pi^{t_s}_{\mathsf{prop}}$ using input b_2, and let prop_2 denote the output.
- If $\mathsf{prop}_2 = \{b'\}$ for $b' \neq \lambda$, then output $(b', 2)$ and terminate. If $\mathsf{prop}_2 = \{b', \lambda\}$ for $b' \neq \lambda$, then output $(b', 1)$ and terminate. If $\mathsf{prop}_2 = \{\lambda\}$, then output $(\perp, 0)$ and terminate.

Figure 4: A protocol for graded consensus.

In Figure 4 we show a graded consensus protocol $\Pi^{t_s}_{\mathsf{GC}}$ that relies on $\Pi^{t_s}_{\mathsf{prop}}$ as a subroutine. Note that parties terminate upon generating output. We now analyze the protocol.

Lemma 7. *If $t_s < n/2$, then $\Pi^{t_s}_{\mathsf{GC}}$ achieves t_s-graded validity.*

Proof. Suppose at most t_s parties are corrupted, and every honest party's input is equal to the same value v. By Lemma 6, all honest parties have $\mathsf{prop}_1 = \{v\}$ following the first execution of $\Pi^{t_s}_{\mathsf{prop}}$, and therefore use v as the input for the second execution of $\Pi^{t_s}_{\mathsf{prop}}$. By the same reasoning, all honest parties then have $\mathsf{prop}_2 = \{v\}$ after the second execution of $\Pi^{t_s}_{\mathsf{prop}}$. Thus, all honest parties output $(v, 2)$. □

Lemma 8. *Assume $t_a \leq t_s$ and $t_a + 2 \cdot t_s < n$. Then $\Pi^{t_s}_{\mathsf{GC}}$ achieves t_a-graded consistency.*

Proof. Suppose at most t_a parties are corrupted. First, we show that the grades output by two honest parties P_i, P_j differ by at most 1. The only way this can possibly fail is if one of the parties (say, P_i) outputs a grade of 2. P_i must then have received $\mathsf{prop}_2 = \{b\}$, for some $b \in \{0,1\}$, as its output from the second execution of $\Pi^{t_s}_{\mathsf{prop}}$. It follows from Lemma 2 that P_j could not have received $\mathsf{prop}_2 = \{\lambda\}$. Therefore, it is not possible for P_j to output grade 0.

Next, we show that any two honest parties that output grades ≥ 1 must output the same value. Observe first that there is a bit b such that the inputs of all the honest parties in the second execution of $\Pi^{t_s}_{\mathsf{prop}}$ lie in $\{b, \lambda\}$. (Indeed, if all honest parties set $b_2 := \lambda$ this claim is immediate. On the other hand, if some honest party sets $b_2 := b$ then they must have $\mathsf{prop}_1 = \{b\}$; but then Lemma 2 implies that any other honest party who sets b_2 to anything other than λ will set it equal to b as well.) Lemma 3 thus implies that no honest party outputs a set prop_2 after the second execution of $\Pi^{t_s}_{\mathsf{prop}}$ that contains a value other than b or λ. Thus, any two honest parties that output a grade ≥ 1 must output the same value b. □

Lemma 9. *Assume $t_a \leq t_s$ and $t_a + 2 \cdot t_s < n$. Then $\Pi^{t_s}_{\mathsf{GC}}$ achieves t_a-liveness.*

Proof. All honest parties hold input in $\{0,1\}$ in the first execution of $\Pi^{t_s}_{\mathsf{prop}}$, so Lemma 5 shows that all honest parties terminate that execution. As in the proof of the previous lemma, there is a bit b such that the inputs of all the honest parties in the second execution of $\Pi^{t_s}_{\mathsf{prop}}$ lie in $\{b, \lambda\}$; so, by Lemma 5 again, that execution also terminates. Moreover, by Lemma 3, the set prop_2 output by any honest party is either $\{b\}, \{b, \lambda\}$, or $\{\lambda\}$. Thus, every honest party generates output (of the appropriate form) and terminates in $\Pi^{t_s}_{\mathsf{GC}}$. □

3.2.2 Validity-Optimized Byzantine Agreement

We present a Byzantine agreement protocol $\Pi_{\mathsf{ABA}}^{t_s}$ in Figure 5. Recall from Section 2 that we assume an atomic primitive $\mathsf{CoinFlip}(k)$ that allows all parties to generate and learn an unbiased value $\mathsf{Coin}_k \in \{0,1\}$ in each iteration k. We refer there for a discussion as to how it can be realized.

Protocol $\Pi_{\mathsf{ABA}}^{t_s}$

We describe the protocol from the point of view of a party with input $v \in \{0,1\}$.

Set $b := v$, $\mathsf{Coin} := \bot$, $b_{out} := \mathsf{false}$, and $k := 1$. Then repeat the following steps forever:

- Run $\Pi_{\mathsf{GC}}^{t_s}$ on input b, and let (b, g) denote the output.
- $\mathsf{Coin}_k \leftarrow \mathsf{CoinFlip}(k)$.
- If $g < 2$ then set $b := \mathsf{Coin}_k$.
- Run $\Pi_{\mathsf{GC}}^{t_s}$ on input b, and let (b, g) denote the output.
- If $g = 2$ and $b_{out} = \mathsf{false}$, then output b and set $b_{out} := \mathsf{true}$.
- Set $k := k + 1$.

Figure 5: A protocol for Byzantine agreement.

Lemma 10. *If $t_s < n/2$, then protocol $\Pi_{\mathsf{ABA}}^{t_s}$ satisfies t_s-validity. Moreover, if all honest parties initially hold v, then all honest parties output v at the end of the first iteration of $\Pi_{\mathsf{ABA}}^{t_s}$.*

Proof. Suppose there are at most t_s corrupted parties and all honest parties initially hold $v \in \{0,1\}$. All honest parties use input v in the first execution of $\Pi_{\mathsf{GC}}^{t_s}$ in the first iteration; t_s-graded validity of $\Pi_{\mathsf{GC}}^{t_s}$ implies that they all output $(v, 2)$ from that execution. Thus, all honest parties ignore the result of the coin flip. Instead, they immediately run a second instance of $\Pi_{\mathsf{GC}}^{t_s}$ using input v, again unanimously obtaining $(v, 2)$ as output. Thus, all honest parties output v in the first iteration. □

Lemma 11. *Assume $t_a \le t_s$ and $t_a + 2 \cdot t_s < n$. Then $\Pi_{\mathsf{ABA}}^{t_s}$ satisfies t_a-consistency. Moreover, if an honest party generates output b for the first time in iteration k, then every other honest party outputs b in iteration k or $k + 1$.*

Proof. Suppose at most t_a parties are corrupted, and that P_i is the first honest party to output $b \in \{0,1\}$ in some iteration k. Thus, it must have seen $(b, 2)$ as the output of the second execution of $\Pi_{\mathsf{GC}}^{t_s}$ in iteration k. By t_a-graded consistency of $\Pi_{\mathsf{GC}}^{t_s}$, every honest party obtains either $(b, 1)$ or $(b, 2)$ as output from that execution of $\Pi_{\mathsf{GC}}^{t_s}$. Clearly, all honest parties in the second situation output b in iteration k. We argue that all honest parties in the first situation (namely, who obtain output $(b, 1)$) will output b in iteration $k + 1$. This can be seen as follows. Since all honest parties use input b in the first execution of $\Pi_{\mathsf{GC}}^{t_s}$ in iteration $k + 1$, all honest parties output $(b, 2)$ in that execution (by t_s-validity of $\Pi_{\mathsf{GC}}^{t_s}$). As in the previous lemma, all honest parties the participate in the coin flip but ignore its result, and all use input b in the next execution of $\Pi_{\mathsf{GC}}^{t_s}$. Thus, all honest parties obtain output $(b, 2)$ from the second execution of $\Pi_{\mathsf{GC}}^{t_s}$ in iteration $k + 1$, and any that did not output b in the previous iteration will output it now. □

Lemma 12. *Assume $t_a \le t_s$ and $t_a + 2 \cdot t_s < n$. Then $\Pi_{\mathsf{ABA}}^{t_s}$ satisfies t_a-liveness. Moreover, all honest parties generate output in an expected constant number of iterations.*

Proof. Assume at most t_a parties are corrupted, and consider some iteration k of the protocol by which no honest party has yet generated output. Note that if all honest parties use the same input in the second execution of $\Pi_{\mathsf{GC}}^{t_s}$ in that iteration, then t_s-graded validity of $\Pi_{\mathsf{GC}}^{t_s}$ implies that all honest parties will obtain a grade of 2 in that execution and hence generate output in iteration k. We show that this with probability at least 1/2, thus proving the lemma. We distinguish two cases.

- Say some honest party outputs $(b, 2)$ after the first execution of $\Pi_{\mathsf{GC}}^{t_s}$ in iteration k. By t_a-graded consistency, all honest parties output either $(b, 2)$ or $(b, 1)$ in that execution of $\Pi_{\mathsf{GC}}^{t_s}$. Since Coin_k is not chosen until the first honest party terminates the first execution of $\Pi_{\mathsf{GC}}^{t_s}$, this means in particular that b is fixed before Coin_k is chosen. If $\mathsf{Coin}_k = b$, which occurs with probability 1/2, then all parties will use the same input in the second execution of $\Pi_{\mathsf{GC}}^{t_s}$ in iteration k.

- If no honest party outputs $(b, 2)$ after the first execution of $\Pi_{\mathsf{GC}}^{t_s}$, then all honest parties will use Coin_k as their input in the second execution of $\Pi_{\mathsf{GC}}^{t_s}$ in iteration k.

This completes the proof. □

Corollary 1. *For any t_a, t_s with $t_a < n/3$ and $t_a + 2 \cdot t_s < n$, there is an n-party protocol for Byzantine agreement that, when run in an asynchronous network, achieves t_s-validity, t_a-consistency, and t_a-liveness.*

Proof. We may assume $t_a \leq t_s$, as if not we can set $t_s = t_a$ and $t_a + 2 \cdot t_s < n$ will still hold. Note also that the stated conditions imply $t_s < n/2$. The corollary thus follows from Lemmas 10–12. □

Adding termination. Corollary 1 proves all the claims of Theorem 2 except for termination and, indeed, parties in $\Pi_{\mathsf{ABA}}^{t_s}$ participate indefinitely and so the protocol does not terminate. However, we can obtain a terminating protocol $\Pi_{\mathsf{ABA}^*}^{t_s}$ (and hence complete the proof of Theorem 2) using existing techniques [25]. We refer to Appendix A for further discussion.

4 Main Protocol

Fix n, t_a, t_s with $t_a < n/3$ and $2t_s + t_a < n$. As in the proof of Corollary 1 we may assume $t_a \leq t_s$. Our main protocol $\Pi_{\mathsf{HBA}}^{t_a,t_s}$ is given in Figure 6. It relies on the following sub-protocols:

- $\Pi_{\mathsf{SBA}}^{t_a}$ is an n-party BA protocol that is t_s-secure when run in a synchronous network, and t_a-weakly valid when run in an asynchronous network. Moreover, all honest parties terminate by time $n \cdot \Delta$. The existence of such a protocol is guaranteed by Theorem 1.

- $\Pi_{\mathsf{ABA}^*}^{t_s}$ is an n-party BA protocol that is t_a-secure and t_s-valid with termination when run in an asynchronous network. (Of course, these properties also hold if the protocol is run in a synchronous network.) The existence of such a protocol is guaranteed by Theorem 2.

Theorem 3. *Let n, t_a, t_s be as above. Then protocol $\Pi_{\mathsf{HBA}}^{t_a,t_s}$ satisfies the following properties:*

1. *When the protocol is run in a synchronous network, it is t_s-secure.*

2. *When the protocol is run in an asynchronous network, it is t_a-secure.*

Protocol $\Pi_{\mathsf{HBA}}^{t_a,t_s}$

Each P_i initially holds a bit v_i. The protocol proceeds as follows:

- Each party P_i runs $\Pi_{\mathsf{SBA}}^{t_a}$ using input v_i for time $n \cdot \Delta$. Let b_i denote the output of P_i from this protocol, with $b_i = \perp$ denoting no output.
- Each party P_i does the following: if $b_i \neq \perp$, set $v_i^* := b_i$; otherwise set $v_i^* := v_i$. Then run $\Pi_{\mathsf{ABA}^*}^{t_s}$ using input v_i^*, output the result, and terminate.

Figure 6: A Byzantine agreement protocol.

Proof. First consider the case when $\Pi_{\mathsf{HBA}}^{t_a,t_s}$ is run in a synchronous network, and at most t_s parties are corrupted. By t_s-security of $\Pi_{\mathsf{SBA}}^{t_a}$, after running $\Pi_{\mathsf{SBA}}^{t_a}$ there is a value $b \neq \perp$ such that $b_i = b$ for every honest P_i. Moreover, if every honest party's input was equal to the same value v, then $b = v$. Thus, all honest parties set v_i^* to the same value b and, if every party's input was the same value v, then $v_i^* = v$. By t_s-validity with termination of $\Pi_{\mathsf{ABA}^*}^{t_s}$, all honest parties terminate and agree on their output from $\Pi_{\mathsf{HBA}}^{t_a,t_s}$, proving t_s-consistency, t_s-liveness, and t_s-termination. Moreover, if every honest party's original input was equal to the same value v, then the output of $\Pi_{\mathsf{ABA}^*}^{t_s}$ (and thus of $\Pi_{\mathsf{HBA}}^{t_a,t_s}$) is equal to v. This proves t_s-validity.

Next consider the case when $\Pi_{\mathsf{HBA}}^{t_a,t_s}$ is run in an asynchronous network, and at most t_a parties are corrupted. The protocol inherits t_a-consistency, t_a-liveness, and t_a-termination from t_a-security of $\Pi_{\mathsf{ABA}^*}^{t_s}$, and so it only remains to argue t_a-validity. Assume every honest party's initial input is equal to the same value v. Then t_a-weak validity of $\Pi_{\mathsf{SBA}}^{t_a}$, plus the fact that it always terminates, imply that $b_i \in \{v, \perp\}$, and hence $v_i^* = v$, for every honest P_i. It follows from t_a-validity (note $t_a \leq t_s$) of $\Pi_{\mathsf{ABA}^*}^{t_s}$ that all honest parties output v. $\square$

5 Impossibility Result

We show here that our positive result from the previous section is tight. That is:

Theorem 4. *For any n, if $t_a \geq n/3$ or $t_a + 2 \cdot t_s \geq n$ there is no n-party protocol for Byzantine agreement that is t_s-secure in a synchronous network and t_a-secure in an asynchronous network.*

The case of $t_a \geq n/3$ follows from existing impossibility results for asynchronous consensus, so the interesting case is when $t_a < n/3$ but $t_a + 2 \cdot t_s \geq n$. Theorem 4 follows from the lemma below.

Lemma 13. *Fix n, t_a, t_s with $t_a + 2t_s \geq n$. If an n-party Byzantine agreement protocol is t_s-valid in a synchronous network, then it cannot also be t_a-weakly consistent in an asynchronous network.*

Proof. We show impossibility assuming $t_a + 2t_s = n$. Fix a BA protocol Π. Partition the n parties into sets S_0, S_1, S_a where $|S_0| = |S_1| = t_s$ and $|S_a| = t_a$, and consider the following experiment:

- Parties in S_0 run Π using input 0, and parties in S_1 run Π using input 1. All communication between parties in S_0 and parties in S_1 is blocked (but all other messages are delivered within time Δ).
- Create virtual copies of each party in S_a, call them S_a^0 and S_a^1. Parties in S_a^0 run Π using input 0, and communicate only with each other and parties in S_0. Parties in S_a^1 run Π using input 1, and communicate only with each other and parties in S_1.

Consider an execution of Π in a synchronous network where parties in S_1 are corrupted and simply abort, and all remaining (honest) parties use input 0. The views of the honest parties in this execution are distributed identically to the views of $S_0 \cup S_a^0$ in the above experiment. In particular, t_s-validity of Π implies that all parties in S_0 output 0. Analogously, all parties in S_1 output 1.

Next consider an execution of Π in an asynchronous network where parties in S_a are corrupted, and run Π using input 0 when interacting with S_0 while running Π using input 1 when interacting with S_1. Moreover, all communication between the (honest) parties in S_0 and S_1 is delayed indefinitely. The views of the honest parties in this execution are distributed identically to the views of $S_0 \cup S_1$ in the above experiment, yet the conclusion of the preceding paragraph shows that weak consistency is violated. □

References

[1] Ittai Abraham, Danny Dolev, and Joseph Y. Halpern. An almost-surely terminating polynomial protocol for asynchronous Byzantine agreement with optimal resilience. In *27th Annual ACM Symp. on Principles of Distributed Computing (PODC)*, pages 405–414. ACM Press, 2008.

[2] Ittai Abraham, Dahlia Malkhi, Kartik Nayak, Ling Ren, and Maofan Yin. Sync HotStuff: Simple and practical synchronous state machine replication, 2019. Available at `http://eprint.iacr.org/2019/270`.

[3] Zuzana Beerliová-Trubíniová, Martin Hirt, and Jesper Buus Nielsen. On the theoretical gap between synchronous and asynchronous MPC protocols. In *29th Annual ACM Symp. on Principles of Distributed Computing (PODC)*, pages 211–218. ACM Press, 2010.

[4] Christian Cachin, Klaus Kursawe, and Victor Shoup. Random oracles in Constantinople: Practical asynchronous Byzantine agreement using cryptography. *J. Cryptology*, 18(3):219–246, 2005.

[5] Ran Canetti and Tal Rabin. Fast asynchronous Byzantine agreement with optimal resilience. In *25th Annual ACM Symp. on Theory of Computing (STOC)*, pages 42–51. ACM Press, 1993.

[6] Miguel Castro and Barbara Liskov. Practical Byzantine fault tolerance and proactive recovery. *ACM Trans. Computer Systems*, 20(4):398–461, 2002.

[7] Ivan Damgård, Martin Geisler, Mikkel Krøigaard, and Jesper Buus Nielsen. Asynchronous multiparty computation: Theory and implementation. In *12th Intl. Conference on Theory and Practice of Public Key Cryptography—PKC 2009*, volume 5443 of *LNCS*, pages 160–179. Springer, 2009.

[8] Danny Dolev and H. Raymond Strong. Authenticated algorithms for Byzantine agreement. *SIAM J. Computing*, 12(4):656–666, 1983.

[9] Pesech Feldman and Silvio Micali. An optimal probabilistic protocol for synchronous Byzantine agreement. *SIAM J. Comput.*, 26(4):873–933, 1997.

[10] Michael J. Fischer, Nancy A. Lynch, and Mike Paterson. Impossibility of distributed consensus with one faulty process. *J. ACM*, 32(2):374–382, 1985.

[11] Matthias Fitzi, Martin Hirt, Thomas Holenstein, and Jürg Wullschleger. Two-threshold broadcast and detectable multi-party computation. In *Advances in Cryptology—Eurocrypt 2003*, volume 2656 of *LNCS*, pages 51–67. Springer, 2003.

[12] Matthias Fitzi and Jesper Buus Nielsen. On the number of synchronous rounds sufficient for authenticated Byzantine agreement. In *23rd International Symposium on Distributed Computing (DISC)*, volume 5805 of *LNCS*, pages 449–463. Springer, 2009.

[13] Yossi Gilad, Rotem Hemo, Silvio Micali, Georgios Vlachos, and Nickolai Zeldovich. Algorand: Scaling Byzantine agreements for cryptocurrencies, 2017. Available at `http://eprint.iacr.org/2017/454`.

[14] Shafi Goldwasser and Yehuda Lindell. Secure multi-party computation without agreement. *J. Cryptology*, 18(3):247–287, 2005.

[15] Yue Guo, Rafael Pass, and Elaine Shi. Synchronous, with a chance of partition tolerance, 2019. Available at `http://eprint.iacr.org/2019/179`.

[16] Timo Hanke, Mahnush Movahedi, and Dominic Williams. Dfinity technology overview series consensus system, rev. 1, 2018. Available at `https://dfinity.org/faq`.

[17] Ethan Heilman, Alison Kendler, Aviv Zohar, and Sharon Goldberg. Eclipse attacks on Bitcoin's peer-to-peer network. In *24th USENIX Security Symposium*, pages 129–144. USENIX Association, 2015.

[18] Jonathan Katz and Chiu-Yuen Koo. On expected constant-round protocols for Byzantine agreement. *J. Computer and System Sciences*, 75(2):91–112, 2009.

[19] Ramakrishna Kotla, Lorenzo Alvisi, Michael Dahlin, Allen Clement, and Edmund L. Wong. Zyzzyva: Speculative Byzantine fault tolerance. *ACM Trans. Computer Systems*, 27(4):7:1–7:39, 2009.

[20] Klaus Kursawe. Optimistic Byzantine agreement. In *21st Symposium on Reliable Distributed Systems (SRDS)*, pages 262–267. IEEE Computer Society, 2002.

[21] Leslie Lamport. The part-time parliament. Technical Report 49, DEC Systems Research Center, 1989.

[22] Leslie Lamport, Robert E. Shostak, and Marshall C. Pease. The Byzantine generals problem. *ACM Trans. Programming Language Systems*, 4(3):382–401, 1982.

[23] Chen-Da Liu-Zhang, Julian Loss, Tal Moran, Ueli Maurer, and Daniel Tschudi. Robust MPC: Asynchronous responsiveness yet synchronous security, 2019. Available at `http://eprint.iacr.org/2019/159`.

[24] Julian Loss and Tal Moran. Combining asynchronous and synchronous Byzantine agreement: The best of both worlds, 2018. Available at `http://eprint.iacr.org/2018/235`.

[25] Achour Mostéfaoui, Moumen Hamouma, and Michel Raynal. Signature-free asynchronous Byzantine consensus with $t < n/3$ and $O(n^2)$ messages. In *33rd Annual ACM Symp. on Principles of Distributed Computing (PODC)*, pages 2–9. ACM Press, 2014.

[26] Diego Ongaro and John K. Ousterhout. In search of an understandable consensus algorithm. In *USENIX Annual Technical Conference*, pages 305–319. USENIX Association, 2014.

[27] Rafael Pass and Elaine Shi. Hybrid consensus: Efficient consensus in the permissionless model. In *31st International Symposium on Distributed Computing (DISC)*, volume 91 of *LIPIcs*, pages 39:1–39:16. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2017.

[28] Rafael Pass and Elaine Shi. Thunderella: Blockchains with optimistic instant confirmation. In *Advances in Cryptology—Eurocrypt 2018, Part II*, volume 10821 of *LNCS*, pages 3–33. Springer, 2018.

[29] Arpita Patra, Ashish Choudhary, and C. Pandu Rangan. Simple and efficient asynchronous byzantine agreement with optimal resilience. In *28th Annual ACM Symp. on Principles of Distributed Computing (PODC)*, pages 92–101. ACM Press, 2009.

[30] Arpita Patra and Divya Ravi. On the power of hybrid networks in multi-party computation. *IEEE Trans. Information Theory*, 64(6):4207–4227, 2018.

[31] M. Pease, Robert E. Shostak, and Leslie Lamport. Reaching agreement in the presence of faults. *J. ACM*, 27(2):228–234, 1980.

A Adding Termination

Protocol $\Pi^{t_s}_{\mathsf{ABA}}$ has the property that parties never terminate. It is worth noting that the naive solution, in which honest parties participate in one more iteration after generating output, is not sufficient to allow the remaining honest parties to terminate. To see why, suppose that some honest party P_i receives $(b, 2)$ as output from the second instance of $\Pi^{t_s}_{GC}$ in iteration k, and some other honest party P_j receives $(b, 1)$. Now P_i will participate in iteration $k+1$, helping P_j to output $(b, 2)$ in that iteration. However, P_i then terminates and does not participate in iteration $k+2$, while P_j still needs to complete iteration $k+2$ in order to terminate. P_j will not receive messages from P_i when running $\Pi^{t_s}_{GC}$, and (since the network may be asynchronous) has no way of knowing whether P_i has terminated or is sending messages that have been delayed. Thus, P_j may never terminate its execution of $\Pi^{t_s}_{GC}$.

Nevertheless, we can obtain a terminating protocol $\Pi^{t_s}_{\mathsf{ABA}^*}$ using existing techniques [25]. The basic idea is that when an honest party generates output, it announces that fact to all other parties and terminates; the remaining honest parties can then simulate its behavior for the rest of the execution. Specifically, we modify $\Pi^{t_s}_{\mathsf{ABA}}$ as follows: when an honest party P_i outputs b^*, it sends (notify, b^*) to all parties. Upon receiving such a message, the remaining parties locally simulate the behavior of P_i in the rest of the protocol, and specifically simulate receiving $(\mathsf{prepare}, b^*)$ and $(\mathsf{propose}, b^*)$ from P_i in each execution of the $\Pi^{t_s}_{\mathsf{prop}}$ subroutines. The following lemma shows that this is sufficient to simulate the behavior honest parties who have already terminated.

Lemma 14. *Let t_a, t_s be such that $t_a \leq t_s$ and $t_a + 2 \cdot t_s < n$, and assume at most t_a parties are corrupted in an execution of $\Pi^{t_s}_{\mathsf{ABA}}$. If an honest party outputs b^*, then in every future execution of $\Pi^{t_s}_{\mathsf{prop}}$ within $\Pi^{t_s}_{\mathsf{ABA}}$ that party will send exactly the messages* $(\mathsf{prepare}, b^*)$ *and* $(\mathsf{propose}, b^*)$.

Proof. Say honest party P_i outputs $b^* \in \{0, 1\}$ in some iteration k. Then P_i must have received $(b^*, 2)$ as the output of the second execution of $\Pi^{t_s}_{\mathsf{GC}}$ in iteration k. By t_a-graded consistency of

$\Pi^{t_s}_{\mathsf{GC}}$, every honest party obtained $(b^*, 1)$ or $(b^*, 2)$ as output from the second execution of $\Pi^{t_s}_{\mathsf{GC}}$ in iteration k. Therefore, in the first execution of $\Pi^{t_s}_{\mathsf{GC}}$ in iteration $k+1$, all honest parties use input b^*. Using the same argument as in the proof of Lemma 3, observe that no value other than b^* receives enough prepare messages to be echoed (and therefore proposed) in this execution of $\Pi^{t_s}_{\mathsf{prop}}$. Therefore every honest party sends $(\mathsf{prepare}, b^*)$ in that execution of $\Pi^{t_s}_{\mathsf{prop}}$, and hence every honest party sends $(\mathsf{propose}, b^*)$ as in the proof of Lemma 5. This establishes that honest parties send exactly the messages $(\mathsf{prepare}, b^*)$ and $(\mathsf{propose}, b^*)$ in the first execution of $\Pi^{t_s}_{\mathsf{prop}}$ (as a subroutine of the first execution of $\Pi^{t_s}_{\mathsf{GC}}$). Since, by Lemma 6, all honest parties terminate with $\{b^*\}$ in that execution, they all use input b^* in the second execution of $\Pi^{t_s}_{\mathsf{prop}}$ (still in the first execution of $\Pi^{t_s}_{\mathsf{GC}}$), and we can repeat the argument. Moreover, t_s-graded validity of $\Pi^{t_s}_{\mathsf{GC}}$ ensures that all parties output $(b^*, 2)$ from the first execution of $\Pi^{t_s}_{\mathsf{GC}}$. Therefore, all honest parties input b^* to the second execution of $\Pi^{t_s}_{\mathsf{GC}}$ in iteration $k+1$ and we can apply the same argument to show that during iteration $k+1$ of $\Pi^{t_s}_{\mathsf{ABA}}$, all honest parties send exactly the messages $(\mathsf{prepare}, b^*)$ and $(\mathsf{propose}, b^*)$. Now, t_s-graded validity of $\Pi^{t_s}_{\mathsf{GC}}$ ensures that all honest parties output $(b^*, 2)$ in the second execution of $\Pi^{t_s}_{\mathsf{GC}}$ in iteration $k+1$ as well, and hence set $b = b^*$ for iteration $k+2$. We can therefore repeat the same argument inductively for any iteration $k' > k+1$. □

Putting everything together, we have:

Lemma 15. *For any t_a, t_s with $t_a \leq t_s$ and $t_a + 2 \cdot t_s < n$, protocol $\Pi^{t_s}_{\mathsf{ABA}^*}$ is t_a-secure and also achieves t_s-validity with termination.*

Proof. Protocol $\Pi^{t_s}_{\mathsf{ABA}^*}$ inherits t_a-validity, t_a-consistency, and t_a-liveness directly from $\Pi^{t_s}_{\mathsf{ABA}}$. Furthermore, t_a-liveness of $\Pi^{t_s}_{\mathsf{ABA}}$ implies t_a-termination of $\Pi^{t_s}_{\mathsf{ABA}^*}$.

It remains only to show that $\Pi^{t_s}_{\mathsf{ABA}^*}$ is t_s-valid with termination. Suppose at most t_s parties are corrupted during an execution of $\Pi^{t_s}_{\mathsf{ABA}^*}$, and all honest parties hold input $v \in \{0, 1\}$. The execution proceeds exactly as described in Lemma 10, and so all honest parties output v in the first iteration and terminate. □

On Realizing CoinFlip(k). Mostéfaoui et al. [25] and the above analysis treat the coin flip as an atomic primitive that outputs the kth coin when the first honest party invokes CoinFlip(k), even if some honest parties have terminated. However, when the coin flip is realized by an interactive protocol, this may no longer be true. When realizing the coin flip via a threshold unique signature scheme, however, there is a simple way to fix this issue: When an honest party terminates in iteration k, it appends its share of the signature for iteration $k+1$ to its notify message. Then, all parties can compute the signature in iteration $k+1$ as needed. It is crucial here to note that since an honest party terminated in iteration k, the value of Coin_{k+1} will be ignored by all honest parties anyway, so it does not matter that the adversary can learn Coin_{k+1} in advance of iteration $k+1$.