Randomized Consensus Protocols for Asynchronous Systems: Survey, Theoretical Analysis, and a Committee-Based Approach

Thomas Bordino

Columbia University, New York, USA
tb3145@columbia.edu

Abstract. This paper presents a comprehensive survey and theoretical analysis of asynchronous Multi-Valued Byzantine Agreement (MVBA) protocols that use randomization to circumvent the Fischer-Lynch-Paterson (FLP) impossibility result. We systematically examine existing approaches, including HMVBA, Reducer, Reducer++, and FIN-MVBA, analyzing their trade-offs between Byzantine fault tolerance, communication complexity, and cryptographic assumptions. Our analysis reveals a persistent gap between protocols achieving optimal resilience ($t < n/3$) and those with lower message complexity and minimal cryptographic assumptions. Building on this foundation, we introduce EABA (Efficient Asynchronous Byzantine Agreement), a committee-based framework that employs verifiable random functions for committee selection to balance resilience and efficiency. We provide rigorous theoretical analysis demonstrating that EABA can approach optimal Byzantine resilience while maintaining sub-quadratic message complexity under standard cryptographic assumptions. We further contribute theoretic lower bounds on the resilience-efficiency trade-offs inherent to the asynchronous consensus problem, proving that our approach approaches theoretical optimality in multiple dimensions. The paper concludes with an examination of open challenges, including post-quantum security considerations and potential extensions to the basic framework, establishing directions for future research in scalable asynchronous consensus protocols.

1 Introduction

In this paper, we study the asynchronous Multi-Valued Byzantine Agreement (MVBA) protocols and aim to addresses critical bottlenecks impeding the practical deployment of asynchronous Byzantine Fault Tolerance (BFT) systems across multiple industries. Our pursuit of a $t < n/3$ threshold directly enables blockchain scalability revolutions, facilitating 1000+ node blockchain shards with 1-second finality, enabling quantum-resistant decentralized finance (DeFi) capable of processing millions of

transactions per second across shards, and reducing cross-shard communication overhead compared to existing solutions. Furthermore, the enhanced resilience offered by our work is paramount for mission-critical infrastructure, impacting financial settlement through atomic cross-chain swaps with high Byzantine resilience, smart grids with distributed coordination of millions of IoT edge devices, and aerospace applications requiring Byzantine-tolerant sensor fusion for drone swarms. By eliminating random oracle dependencies, this research contributes to post-quantum preparedness, enabling the migration of cloud Key Management Systems (KMS) to quantum-safe consensus ahead of established timelines and protecting substantial blockchain assets from quantum computing attacks. Finally, this work lays the foundations for emerging technologies such as metaverse economics, decentralized AI organizations, and space networks by creating secure means of reaching Byzantine agreement in distributed systems. The resulting protocols will be evaluated in real-world scenarios, such as enterprise blockchain platforms, and will contribute to the development of scalable, attack-resistant BFT systems capable of supporting next-generation decentralized applications.

2 Preliminaries

In this section, we formally define the problems and discuss the related work.

2.1 Framework of Consensus Protocol in Asynchrony with Byzantine Validators

The system consists of:

- **Validators**: A set of n validators $\mathcal{V} = \{v_1, v_2, \ldots, v_n\}$, where each validator communicates via authenticated point-to-point channels.
- **Byzantine Validators**: Up to $b \leq t$ validators may be *Byzantine-faulty*, where t is the security threshold ($t < n/3$). A Byzantine validator may deviate arbitrarily from the protocol (e.g., crash, equivocate, or delay messages). Validators not Byzantine-faulty are *correct*.
- **Asynchrony**: The network is asynchronous:
  - Message delays are unbounded but finite (no timing assumptions).
  - The adversary controls message scheduling but cannot indefinitely delay messages between correct validators.

– **Adaptive Adversary**: The adversary corrupts validators dynamically during execution, subject to $b \leq t$ at all times. A validator corrupted after sending a message may have that message suppressed (*after-the-fact removal*).

The protocol must satisfy consistency and liveness as follow.

– **Consistency (No Fork)**: For any two chains $\mathcal{C}_1$ and $\mathcal{C}_2$ decided by correct validators, one must be a prefix of the other. Formally:

$$\mathcal{C}_1 \preceq \mathcal{C}_2 \quad \text{or} \quad \mathcal{C}_2 \preceq \mathcal{C}_1,$$

where $\preceq$ denotes the prefix relation.
Implication: Byzantine validators cannot cause two correct validators to finalize conflicting chains.

– **Liveness**: Every valid transaction proposed by a correct validator is eventually included in the chain of all correct validators.
Implication: Despite asynchrony and Byzantine behavior, the protocol makes progress.

The bound $t < n/3$ is fundamental for Byzantine consensus in asynchronous networks due to:

– **Quorum Intersection**: To prevent forks, any two quorums must intersect in at least one correct validator. For quorums of size $\lceil \frac{2n}{3} \rceil$:

$$2 \times \left\lceil \frac{2n}{3} \right\rceil - n \geq t + 1,$$

ensuring overlap even if t validators are Byzantine. With $t \geq n/3$, quorums may not intersect, breaking consistency.

– **Optimal Resilience**: The $t < n/3$ bound is tight. For $t \geq n/3$, Byzantine validators can:
  - Simulate disjoint network partitions (violating consistency),
  - Censor messages indefinitely (violating liveness).

– **Adaptive Adversary Mitigation**: Dynamic corruption requires $t < n/3$ to ensure that, even if the adversary corrupts validators *after* they send messages, enough correct validators remain to guarantee progress.

The *Fischer-Lynch-Paterson (FLP) Impossibility Theorem* states: In an asynchronous network, no deterministic protocol can achieve consensus with even one crash fault if messages may be delayed arbitrarily. In an asynchronous network with Byzantine faults ($t \geq 1$), correct validators cannot reliably distinguish between a slow (but honest) validator and a Byzantine validator intentionally delaying messages. This ambiguity makes it impossible for deterministic protocols to guarantee both consistency and liveness, as waiting for a response could stall the protocol indefinitely (if the validator is slow) or expose it to manipulation (if the validator is Byzantine).

2.2 Multi-Valued Byzantine Agreement (MVBA) Framework

In this survey, we aim to propose a protocol for MVBA following the existing studies [1, 3, 4, 7, 12, 13], which operates under the described model. In simple terms, MVBA ensures that all correct processes reach agreement on a *valid* ℓ-bit value. The formal definition of MVBA can be found below.

MVBA Protocol Definition

1: $\text{Value}_{\text{MVBA}}$ is the set of all ℓ-bit values.
2: valid : $\text{Value}_{\text{MVBA}} \to \{true, false\}$, where a value $v \in \text{Value}_{\text{MVBA}}$ is valid iff $\text{valid}(v) = true$.
3: **Input:** $\texttt{propose}(v)$ where $v \in \text{Value}_{\text{MVBA}}$ (a process proposes v).
4: **Output:** $\texttt{decide}(v')$ where $v' \in \text{Value}_{\text{MVBA}}$ (a process decides v').
5: **Assumed Behavior:**
6: Every correct process makes a single proposal, ensuring the proposed value is valid.
7: **Properties:**
8: *External Validity:* No correct process decides on an invalid value.
9: *Weak Validity:* If all processes are correct and a correct process decides $v \in \text{Value}_{\text{MVBA}}$, then v was proposed by a correct process.
10: *Agreement:* No two correct processes decide different values.
11: *Integrity:* No correct process decides more than once.
12: *Termination:* Every correct process eventually reaches a decision.
13: *Quality:* If a correct process decides $v \in \text{Value}_{\text{MVBA}}$, then the probability that v is chosen by the adversary is at most $q < 1$.

The MVBA protocol enables n validators to reach agreement on an arbitrary ℓ-bit value under asynchronous network conditions with up to $t < n/3$ Byzantine faults. The framework operates as follows:

– Each value v must satisfy $\mathsf{valid}(v)$ predicate
– **Protocol Phases**:
  1. *Proposal*: Each validator broadcasts its proposed value. Values are accompanied by validity proofs (e.g., Merkle proofs)
  2. *Gathering*: Validators collect proposals into a candidate set. Erasure coding ensures tolerance for missing messages
  3. *Reduction*: Candidate set is reduced through multiple rounds. Each round applies Byzantine-resistant filtering rules
  4. *Agreement*: Final value is selected through quorum voting. Selection ensures all correct validators decide same value
– **Termination Conditions**: Protocol terminates when:
  - All correct validators decide same valid value
  - No correct validator decides conflicting value
  - Every proposed valid value has been considered

2.3 Related Work

The foundation of this work builds on seminal advances in asynchronous MVBA protocols. The HMVBA protocol introduced a hash-based design using Merkle trees and Reed-Solomon coding, achieving $O(1)$ time complexity and $O(n\ell + n^2\lambda \log n)$ bit complexity but limited to $t < n/5$ resilience due to quorum intersection constraints [10]. In 2024, the Reducer framework improved resilience to $t < n/4$ through collision-resistant hashes, while Reducer++ further extended it to $t < (1/3 - \epsilon)n$ under random oracle assumptions, maintaining quasi-quadratic bit complexity [11]. The FIN-MVBA protocol demonstrated $t < n/3$ resilience but at the cost of cubic communication overhead, highlighting unresolved trade-offs between robustness and scalability [6]. Earlier works, such as CKPS01-MVBA by Cachin et al. [2], established threshold signatures as a core primitive, while VABA protocol by Abraham et al. [1] introduced accountable consistency for asynchronous BFT. These contributions collectively outline a roadmap for balancing resilience, efficiency, and adaptability in modern consensus systems. A summary of the existing MVBA algorithms/protocols can be found below.

3 The State of the Art Protocols

In this section, we introduce three fundamental protocol frameworks in the literature of Multi-Valued Byzantine Agreement (MVBA) protocols.

Table 1: **Summary of adaptively-secure asynchronous MVBA algorithms.**

Algorithm	Hash-based	Messages	Bits	Time	Resilience
CKPS01-MVBA [2] [TS]	×	$\mathcal{O}(n^2)$	$\mathcal{O}(n^2\ell + n^2\lambda + n^3)$	$\mathcal{O}(1)$	$t < \frac{1}{3}n$
CKPS01-MVBA/HS [2] [H-CR]	✓	$\mathcal{O}(n^2)$	$\mathcal{O}(n^2\ell + n^3\lambda)$	$\mathcal{O}(1)$	$t < \frac{1}{3}n$
VABA [1] [TS]	×	$\mathcal{O}(n^2)$	$\mathcal{O}(n^2\ell + n^2\lambda)$	$\mathcal{O}(1)$	$t < \frac{1}{3}n$
VABA/HS [1] [H-CR]	✓	$\mathcal{O}(n^2)$	$\mathcal{O}(n^2\ell + n^3\lambda)$	$\mathcal{O}(1)$	$t < \frac{1}{3}n$
Dumbo-MVBA [13] [TS]	×	$\mathcal{O}(n^2)$	$\mathcal{O}(nl + n^2\lambda)$	$\mathcal{O}(1)$	$t < \frac{1}{3}n$
Dumbo-MVBA/HS [13] [H-CR]	✓	$\mathcal{O}(n^2)$	$\mathcal{O}(nl + n^3\lambda)$	$\mathcal{O}(1)$	$t < \frac{1}{3}n$
sMVBA [9] [TS]	×	$\mathcal{O}(n^2)$	$\mathcal{O}(n^2\ell + n^2\lambda)$	$\mathcal{O}(1)$	$t < \frac{1}{3}n$
sMVBA/HS [9] [H-CR]	✓	$\mathcal{O}(n^2)$	$\mathcal{O}(n^2\ell + n^3\lambda)$	$\mathcal{O}(1)$	$t < \frac{1}{3}n$
FIN-MVBA [6] [H-CR]	✓	$\mathcal{O}(n^3)$	$\mathcal{O}(n^2\ell + n^3\lambda)$	$\mathcal{O}(1)$	$t < \frac{1}{3}n$
FIN-MVBA [6] [NO]	✓	$\mathcal{O}(n^3)$	$\mathcal{O}(n^2\ell + n^2\lambda + n^3 \log n)$	$\mathcal{O}(1)$	$t < \frac{1}{3}n$
HMVBA [7] [H-CR]	✓	$\mathcal{O}(n^2)$	$\mathcal{O}(nl + n^2\lambda \log n)$	$\mathcal{O}(1)$	$t < \frac{1}{5}n$
OciorMVBArr [5] [NO†]	✓	$\mathcal{O}(n^2)$	$\mathcal{O}(nl + n^2\lambda \log n)$	$\mathcal{O}(1)$	$t < \frac{1}{5}n$
OciorMVBA [5] [NO†]	✓	$\mathcal{O}(n^2)$	$\mathcal{O}(nl \log n + n^2 \log n)$	$\mathcal{O}(\log n)$	$t < \frac{1}{3}n$
OciorMVBAh [5] [H-CR†]	✓	$\mathcal{O}(n^3)$	$\mathcal{O}(nl + n^3\lambda)$	$\mathcal{O}(1)$	$t < \frac{1}{3}n$
FLT24-MVBA [8] [H-CR†]	✓	$\mathcal{O}(n^2\kappa)$	$\mathcal{O}(nl + n^2\lambda \log n + n^2\kappa\lambda)$	$\mathcal{O}(\log \kappa)$	$t < \frac{1}{3}n$
Reducer [11] [H-CR†]	✓	$\mathcal{O}(n^2)$	$\mathcal{O}(nl + n^2\lambda \log n)$	$\mathcal{O}(1)$	$t < \frac{1}{4}n$
Reducer++ [11] [H-CR†]	✓	$\mathcal{O}(n^2)$	$\mathcal{O}(nl + n^2\lambda \log n)$	$\mathcal{O}(1)$	$t < (\frac{1}{3} - \epsilon)n$

3.1 HMVBA Protocol Framework

The **Hash-based Multi-Valued Byzantine Agreement (HMVBA)** protocol enables asynchronous agreement on ℓ-bit values with $t < n/5$ Byzantine resilience [7]. Its structure is as follows:

System Model

- **Validators**: n processes $\mathcal{V} = \{v_1, \ldots, v_n\}$ with authenticated channels
- **Adversary**: Static Byzantine faults ($t < n/5$), may crash/equivocate
- **Network**: Fully asynchronous (unbounded delays)

Protocol Phases

1. **Dissemination Phase**:
   - Each v_i proposes value v with *Merkle proof* π_v
   - Values are *erasure-coded* (Reed-Solomon) into n fragments

- Broadcast $H(v)$ and fragments to all validators

2. **Quorum Formation**:
   - Collect $H(v_j)$ (i.e., the commitment vc) hashes until $n - 3f \geq 2f + 1$ are received
   - Construct *quorum certificate* QC of received hashes
   - Reconstruct missing values from fragments when needed
3. **Multi-valued Byzantine agreement (MBA) Phase**:
   - Execute leaderless voting on QC-certified values
   - Finalize value v^* receiving $\geq \lceil 2n/3 \rceil$ votes
   - Output v^* after verifying $\mathsf{valid}(v^*)$

Cryptographic Components

- **Merkle Trees**: Compress validity proofs ($|\pi_v| = O(\lambda \log \ell)$)
- **Reed-Solomon Codes**: Tolerate t fragment losses
- **Hash-Based QCs**: Replace signatures with $O(n\lambda)$-size certificates

Theoretical Guarantees

- **Resilience**: $t < n/5$ Byzantine validators
- **Complexity**:
  - Time: $O(1)$ rounds
  - Communication: $O(n\ell + n^2\lambda \log n)$ bits
- **Properties**:
  - External validity ($\mathsf{valid}(v^*)$)
  - Agreement (no forks)
  - Termination (eventual under $t < n/5$)

3.2 Reducer Protocol Framework

The **Reducer** protocol achieves asynchronous Multi-Valued Byzantine Agreement with $t < n/4$ resilience through a multi-round reduction approach [11].

System Model

- **Validators**: n processes $\mathcal{V} = \{v_1, \ldots, v_n\}$ with authenticated channels
- **Adversary**: Adaptive Byzantine faults ($t < n/4$), may corrupt validators dynamically
- **Network**: Fully asynchronous with eventual delivery

Our protocol assumes:

- **Reliable Message Delivery**: Messages between correct validators are eventually delivered, though with potentially unbounded delay.
- **Message Authentication**: Validators can authenticate the sender of any message using digital signatures.
- **Point-to-Point Channels**: Each validator can send messages directly to any other validator, without relying on broadcast primitives.
- **Non-equivocation**: Correct validators cannot be framed as equivocating by Byzantine validators due to the use of unforgeable digital signatures.

These communication assumptions are standard in asynchronous Byzantine agreement protocols and are necessary to circumvent the FLP impossibility result through cryptographic means while maintaining the optimal resilience threshold.

Protocol Phases

1. **Initial Proposal**:
   - Each v_i broadcasts value v_i with collision-resistant hash $H(v_i)$
   - Values must satisfy $\mathsf{valid}(v_i)$ predicate
2. **Multi-Round Reduction**:
   - Round 1: Validators exchange hashes, filter out non-common values
   - Round 2: Apply interactive consistency to reduce candidate set
   - Final Round: Reach ϵ-agreement on candidate subset
3. **Final Agreement**:
   - Execute threshold-based voting on reduced candidate set
   - Decide value v^* appearing in all honest validator sets
   - Consistency ensured through quorum intersection

Cryptographic Components

- **Collision-Resistant Hashes**: Compact representation of proposals
- **Threshold Cryptography**: Used for final voting phase
- **Interactive Consistency**: Ensures common view of candidates

Theoretical Guarantees

- **Resilience**: $t < n/4$ Byzantine validators
- **Complexity**:
  - Time: $O(1)$ expected rounds
  - Communication: $O(n\ell + n^2\lambda)$ bits
- **Properties**:
  - Strong validity (decided value was proposed)
  - Optimal message complexity
  - Tolerates adaptive adversaries

3.3 Reducer++ Protocol Framework

The **Reducer++** protocol enhances the Reducer approach to achieve $t < (1/3 - \epsilon)n$ Byzantine resilience through advanced cryptographic techniques [11].

System Model

- **Validators**: n processes $\mathcal{V} = \{v_1, \ldots, v_n\}$ with authenticated channels
- **Adversary**: Byzantine adversary corrupting up to $t < n/3$ validators. Our protocol primarily addresses the static corruption model, though we analyze adaptive adversary scenarios in Section 6.1.2. The adversary controls message scheduling but cannot indefinitely delay messages between correct validators.
- **Network**: Fully asynchronous with adversary-controlled scheduling
- **Trust Assumptions**: Random oracle model

Protocol Phases

1. **Enhanced Proposal**:
   - Values committed via random oracle-based proofs
   - Each v_i generates non-interactive proofs π_i for v_i

   - Proofs are $O(\lambda)$-size regardless of value length ℓ
2. **Two-Stage Reduction**:
   - Stage 1: Random oracle-based filtering of candidate values
   - Stage 2: Multi-valued validated Byzantine agreement (MVBA)
   - Achieves ϵ-agreement with constant expected rounds
3. **Finalization**:
   - Threshold signature aggregation for final decision
   - Outputs certified value v^* with $2n/3$ signatures
   - Eliminates need for explicit voting rounds

Cryptographic Components

- **Random Oracle**: Enables compact proofs and leader election
- **Threshold Signatures**: $O(1)$-size final certificates
- **Adaptive Security**: Corruption-resistant construction

Theoretical Guarantees

- **Resilience**: $t < (1/3 - \epsilon)n$ Byzantine validators
- **Complexity**:
  - Time: $O(1)$ expected rounds
  - Communication: $O(n\ell + n^2\lambda \log n)$ bits
- **Properties**:
  - Optimal resilience approaching $n/3$
  - Post-quantum security for reduction phase
  - Strong fairness guarantees

4 Efficient Asynchronous BA (EABA) Protocol Framework

In this section, we propose the **EABA** protocol. The **EABA** protocol employs secure committee selection, and achieves $t < n/3$ Byzantine resilience with sub-quadratic message complexity through committee-based sampling and threshold cryptography.

4.1 System Model

- **Validators**: n processes $\mathcal{V} = \{v_1, \ldots, v_n\}$ with authenticated channels
- **Committees**: m committees $\mathcal{C} = \{c_1, \ldots, c_m\}$ that can communicate with each other via authenticated channels
- **Adversary**: Static Byzantine adversary corrupting up to $t < n/3$ validators
- **Network**: Fully asynchronous with adversary-controlled scheduling
- **Trust Assumptions**: Standard cryptographic primitives, no random oracle

4.2 Cryptographic Components

- **Verifiable Random Functions (VRFs)**: Secure committee selection with verifiable outputs
- **Threshold Signatures**: Compact committee decisions and efficient verification
- **Standard Digital Signatures**: Message authentication between validators

4.3 Protocol Phases

1. **Committee Formation**:
   - Each validator v_i computes VRF output $y_i = \text{VRF}_{sk_i}(seed)$ with proof π_i
   - Committee assignment function $\mathcal{C} : \mathcal{V} \times [m] \to \{0, 1\}$ determines validator-to-committee mapping
   - Each validator belongs to $c \cdot \log n$ committees on average, where c is a security parameter
   - Each committee selects a leader using a deterministic function of the VRF outputs. By Lemma 1, with high probability, an honest validator will be selected as leader in each committee.
   - Total of $m = O(n/\log n)$ committees, each of size $O(\log n)$
2. **Value Proposal**:
   - Each validator v_i sends proposal (val_i, σ_i) only to members of its assigned committees
   - Proposals include validator signature σ_i for authenticity
   - Message complexity: $O(n \log n)$ messages

3. **Committee Validation**:
   - Each committee C_j locally executes simplified Byzantine agreement on received proposals
   - Valid proposals are aggregated into committee decision val_j
   - Committee generates $(t_j + 1, |C_j|)$-threshold signature τ_j on val_j
   - Committee leaders broadcast (val_j, τ_j) to other committees and their members
4. **Global Agreement**:
   - Validators collect committee decisions with valid threshold signatures
   - A value val is accepted if it has threshold signatures from at least $\lceil \frac{m}{2} \rceil + t_c$ distinct committees
   - If multiple values reach threshold, validators select based on deterministic rule $\min_{\text{hash}}(val)$
   - Timeout mechanism triggers backup agreement protocol if no value reaches threshold

4.4 Theoretical Analysis and Security Guarantees

We now provide a formal theoretical analysis of our proposed EABA protocol, focusing on its security guarantees, resilience properties, and complexity bounds.

Committee Security Analysis The security of our protocol critically depends on the property that each committee contains a sufficient number of honest validators. We can formalize this through the following lemma:

Lemma 1 (Committee Honesty). *With probability at least* $1 - n^{-\Omega(1)}$*, every committee* C_j *contains an honest majority.*

Proof. Let X_j denote the number of honest validators in committee C_j of size $s = c \cdot \log n$. The expected number of honest validators is $\mathbb{E}[X_j] = s \cdot (1 - \frac{t}{n}) > \frac{2s}{3}$ since $t < \frac{n}{3}$. By Chernoff bounds, for $\delta = \frac{1}{4}$ and $\mu = \frac{2s}{3}$, we have:

$$\Pr[X_j < \frac{s}{2}] = \Pr[X_j < (1-\delta)\mu] < e^{-\delta^2\mu/2} = e^{-\frac{1}{16} \cdot \frac{2s}{3} \cdot \frac{1}{2}} = e^{-\frac{s}{48}} = e^{-\Omega(c \log n)}$$

. This gives $\Pr[X_j < \frac{s}{2}] < e^{-\Omega(c \log n)}$. Using the union bound over all $m = O(\frac{n}{\log n})$ committees:

$$\Pr[\text{any committee lacks honest majority}] < m \cdot e^{-\Omega(c \log n)} < n^{-\Omega(1)}$$

for sufficiently large constant c.

This lemma establishes that, with high probability, all committees maintain honest majorities throughout the protocol execution. A direct implication is that malicious validators cannot compromise committee decisions, provided that the quorum size for each committee is appropriately set.

Verifiable Random Function Security The committee formation phase relies on Verifiable Random Functions (VRFs) to ensure unpredictable but verifiable committee assignments. The security of VRFs under our model can be characterized as follows:

Theorem 1 (VRF Security). *If the VRF scheme satisfies pseudorandomness, uniqueness, and verifiability, then:*

1. *An adversary cannot predict committee assignments before the VRF outputs are revealed.*
2. *Committee assignments are verifiable by all validators.*
3. *The adversary cannot selectively assign corrupt validators to committees.*

These properties ensure that committee formation remains secure even against adaptive adversaries, provided they cannot corrupt more than $t < n/3$ validators. The unpredictability property is particularly important as it prevents the adversary from strategically positioning corrupt validators to compromise specific committees.

Agreement Analysis Now we establish the agreement property of our protocol through the following theorem:

Theorem 2 (Agreement Guarantee). *If all honest validators follow the EABA protocol, then with high probability, all honest validators that make a decision will agree on the same value.*

Proof. Assume two honest validators decide on different values v_1 and v_2. Each value must have received threshold signatures from at least $\lceil \frac{m}{2} \rceil + t_c$ committees.

By the pigeonhole principle, there are at least $2(\lceil \frac{m}{2} \rceil + t_c) - m > 2t_c$ committees that signed both v_1 and v_2 (where t_c is the maximum

number of committees that can be corrupted, bounded by $t_c < \frac{m}{3}$ with high probability due to Lemma 1).

Since, with high probability, all committees have honest majorities (from the Committee Security Lemma), and threshold signatures require participation of at least $t_j + 1$ honest committee members, at least $t_c + 1$ honest validators must have signed both v_1 and v_2.

This contradicts the property that honest validators never sign conflicting values, implying $v_1 = v_2$.

This theorem guarantees consistency among honest validators, ensuring that the protocol maintains consistency under Byzantine conditions. The proof leverages the intersection property of committee quorums, which is essential for agreement in distributed systems.

Validity Analysis The validity property ensures that if all honest validators propose the same value, then this value will ultimately be decided:

Theorem 3 (Validity Guarantee). *If all honest validators propose the same value v, then with high probability, any honest validator that decides will decide on v.*

Proof. If all honest validators propose v, then each committee with honest majority will receive v from at least $\frac{2s}{3}$ validators. By the validity property of the local Byzantine agreement used within committees, each such committee will decide on v and generate a threshold signature for it.

With high probability (by the Committee Security Lemma), at least $\lceil \frac{m}{2} \rceil + t_c$ committees have honest majorities and will produce threshold signatures for v. Therefore, v will reach the global threshold and be the only value that honest validators can decide on.

This theorem ensures that when there is consensus among honest validators about a proposed value, the protocol will preserve and reflect this consensus in its final decision.

Termination Analysis The termination property guarantees that all honest validators eventually reach a decision:

Theorem 4 (Termination Guarantee). *With high probability, all honest validators eventually decide on a value.*

Proof. By the Committee Security Lemma, with high probability, all committees with honest majorities will eventually complete their local Byzantine agreement due to the termination property of the local agreement protocol.

These committees will generate valid threshold signatures that will eventually reach all honest validators due to the reliability of authenticated channels.

If any value reaches the global threshold, all honest validators will decide on it based on the deterministic selection rule.

If no value reaches the threshold within the timeout period, the backup agreement protocol is triggered, which guarantees termination in asynchronous networks with $t < \frac{n}{3}$ Byzantine faults.

Therefore, all honest validators will eventually decide with probability 1.

The inclusion of a backup agreement mechanism is crucial for ensuring termination under all possible network conditions and adversarial strategies.

Asymptotic Complexity Analysis We now analyze the theoretical complexity bounds of our protocol:

Theorem 5 (Complexity Bounds). *The EABA protocol achieves the following complexity bounds:*

- ***Message Complexity:*** $O(n \log n)$ *messages*
- ***Time Complexity:*** $O(1)$ *expected asynchronous rounds*
- ***Bit Complexity:*** $O(n \log n \cdot \lambda + n \cdot |val|)$ *bits*

where λ *is the security parameter and* $|val|$ *is the size of the proposed value.*

Proof. For message complexity, each validator sends proposal messages to $O(\log n)$ committee members and receives committee decisions from $O(m) = O(\frac{n}{\log n})$ committees, yielding $O(n \log n)$ total messages.

The time complexity is constant in expectation because all protocol phases complete in a constant number of asynchronous rounds with high probability, assuming the committee structure functions correctly.

For bit complexity, each message contains either a proposal of size $|val|$ plus a signature of size λ, or a committee decision with a threshold signature of size λ. With $O(n \log n)$ messages total, this yields a bit complexity of $O(n \log n \cdot \lambda + n \cdot |val|)$.

These complexity bounds demonstrate the efficiency advantages of our committee-based approach compared to traditional MVBA protocols. Particularly notable is the sub-quadratic message complexity, which enables better scalability for large-scale distributed systems.

4.5 Comparative Theoretical Analysis

To position EABA within the landscape of asynchronous Byzantine agreement protocols, we provide a direct comparison with state-of-the-art alternatives along several key theoretical dimensions:

Table 2: Theoretical comparison of EABA with leading asynchronous MVBA protocols

Protocol	Resilience	Message Complexity	Bit Complexity	Time Complexity	Cryptographic Assumptions
HMVBA [7]	$t < n/5$	$\mathcal{O}(n^2)$	$\mathcal{O}(n\ell + n^2\lambda \log n)$	$\mathcal{O}(1)$	Collision-resistant hash functions
Reducer [11]	$t < n/4$	$\mathcal{O}(n^2)$	$\mathcal{O}(n\ell + n^2\lambda \log n)$	$\mathcal{O}(1)$	Collision-resistant hash functions
Reducer++ [11]	$t < (1/3 - \epsilon)n$	$\mathcal{O}(n^2)$	$\mathcal{O}(n\ell + n^2\lambda \log n)$	$\mathcal{O}(1)$	Random oracle model
FIN-MVBA [6]	$t < n/3$	$\mathcal{O}(n^3)$	$\mathcal{O}(n^2\ell + n^3\lambda)$	$\mathcal{O}(1)$	Collision-resistant hash functions
EABA (Our Work)	$t < n/3$	$\mathcal{O}(n \log n)$	$\mathcal{O}(n \log n \cdot \lambda + n \cdot \ell)$	$\mathcal{O}(1)$	Standard cryptographic primitives

Resilience-Efficiency Trade-off EABA achieves the optimal resilience threshold of $t < n/3$ while maintaining sub-quadratic message complexity. In contrast, HMVBA sacrifices resilience for efficiency, while FIN-MVBA achieves optimal resilience but at the cost of cubic message complexity. Reducer++ approaches our resilience threshold but requires stronger cryptographic assumptions (random oracle model).

Asymptotic Efficiency The committee-based structure of EABA enables an asymptotic improvement in message complexity to $\mathcal{O}(n \log n)$ compared to the $\mathcal{O}(n^2)$ or $\mathcal{O}(n^3)$ of alternatives. This represents a fundamental advance in scalability for optimal-resilience protocols, enabling practical deployment in large-scale distributed systems.

Cryptographic Requirements EABA relies only on standard cryptographic primitives (VRFs, threshold signatures, and digital signatures), avoiding the stronger random oracle assumptions required by Reducer++. This makes EABA more suitable for deployment in settings where theoretical security guarantees must be rigorously justified.

5 Information-Theoretic Bounds and Optimality Analysis

In this section, we analyze the fundamental limits on resilience, communication complexity, and time complexity for asynchronous Byzantine agreement protocols. We demonstrate that our EABA protocol approaches these theoretical bounds under specific conditions, establishing its near-optimality.

5.1 Lower Bounds for Resilience in Asynchronous BA

We first establish a fundamental lower bound on the resilience threshold for asynchronous Byzantine agreement:

Theorem 6 (Optimal Resilience Bound). *No asynchronous Byzantine agreement protocol can tolerate $t \geq n/3$ Byzantine faulty processes while guaranteeing both consistency and liveness.*

Proof. The proof follows from quorum intersection requirements. In asynchronous systems, decisions must be made after receiving messages from at least $n - t$ processes (a quorum) to ensure termination despite t potentially crashed processes. For consistency, any two such quorums must intersect in at least one honest process to prevent conflicting decisions.

Therefore, we need:

$$2(n - t) - n > t \tag{1}$$

Simplifying: $n - 2t > t$ or $n > 3t$, yielding $t < n/3$ as necessary.

Furthermore, for $t \geq n/3$, an adversary can create scenarios with conflicting quorums of size $n - t$ that have no honest process in their intersection, leading to potential consistency violations.

This theorem establishes that our targeted resilience threshold of $t < n/3$ is theoretically optimal, and our EABA protocol achieves this optimal bound.

5.2 Communication Complexity Lower Bounds

Next, we establish lower bounds on communication complexity:

Theorem 7 (Message Complexity Lower Bound). *Any asynchronous Byzantine agreement protocol must use at least $\Omega(n)$ messages in the worst case.*

Proof. To achieve agreement, at least a constant fraction of honest processes must communicate with each other. Since each honest process must send or receive at least one message, and there are $\Theta(n)$ honest processes, the message complexity must be $\Omega(n)$.

While the lower bound is $\Omega(n)$, practical protocols typically require $\Omega(n^2)$ messages. Our EABA protocol achieves $O(n \log n)$ message complexity, which is sub-quadratic and approaches the theoretical minimum for practical protocols.

Theorem 8 (Bit Complexity Lower Bound). *Any asynchronous Byzantine agreement protocol for ℓ-bit values must communicate at least $\Omega(n\ell + n\lambda)$ bits in the worst case, where λ is the security parameter.*

Proof. For ℓ-bit values, at least one honest process must receive the decided value (requiring $\Omega(\ell)$ bits), and this must occur for $\Omega(n)$ processes. Additionally, cryptographic operations require at least $\Omega(n\lambda)$ bits for signatures or hash values.

Our protocol achieves $O(n \log n \cdot \lambda + n \cdot |val|)$ bit complexity, which is within a logarithmic factor of the lower bound, demonstrating its near-optimal efficiency.

5.3 Time-Space Trade-offs in Asynchronous Settings

We now analyze fundamental trade-offs between time and communication complexity:

Theorem 9 (Time-Communication Trade-off). *For any asynchronous Byzantine agreement protocol with resilience $t < n/3$ and constant expected time complexity $O(1)$, the message complexity is at least $\Omega(n \log n)$ in the worst case.*

Proof. We prove this by contradiction. Assume there exists a protocol Π with $O(1)$ expected time complexity and $o(n \log n)$ message complexity.

Fact 1: For any honest validator to decide correctly, it must receive information (directly or indirectly) from at least $n - 2t$ distinct validators. This follows from the standard quorum intersection requirement for Byzantine agreement with $t < n/3$ faults.

Fact 2: In an asynchronous model, an adversary controls message scheduling and can delay any message by an arbitrary (but finite) amount.

Consider an execution where the adversary selects a set S of $\Theta(n)$ honest validators. For each validator $v \in S$, we analyze its information propagation tree:

Claim: To achieve $O(1)$ expected time despite asynchrony, each validator must receive information through $\Omega(\log n)$ distinct and independent paths.

Proof of claim: If a validator relies on fewer than $\Omega(\log n)$ distinct paths, the adversary can delay messages on these paths to force expected time $\omega(1)$. This follows from standard results on fault-tolerant information propagation in asynchronous networks.

Given the claim, each validator in S must receive $\Omega(\log n)$ messages to decide in constant expected time. With $|S| = \Theta(n)$, this requires $\Omega(n \log n)$ total messages.

However, our protocol Π uses only $o(n \log n)$ messages. By the pigeonhole principle, some validators in S must receive fewer than $\Omega(\log n)$ messages. The adversary can exploit this to delay messages such that these validators cannot decide in constant expected time, contradicting our assumption about Π.

Therefore, any asynchronous Byzantine agreement protocol with resilience $t < n/3$ and $O(1)$ expected time complexity must have message complexity $\Omega(n \log n)$.

This theorem demonstrates that our EABA protocol's $O(n \log n)$ message complexity is optimal for protocols with constant expected time complexity, establishing a provable time-communication trade-off.

6 Theoretical Extensions, Limitations and Future Directions

This section explores theoretical extensions of our EABA protocol, examines its limitations, and outlines future research directions. Rather than providing formal proofs, we offer intuitive explanations of why our approach works and identify areas for further improvement.

6.1 Advanced Protocol Extensions

Adaptive Quorum Sampling While our base EABA protocol uses static committee sizes, real-world networks exhibit dynamic behavior where some validators may be more reliable than others. An adaptive quorum sampling approach would dynamically adjust committee structures based on observed network conditions. The key intuition is that by monitoring validator performance and reliability over time, we can optimize committee composition to include more reliable validators in critical roles, particularly as committee leaders. As the protocol execution progresses, validators would accumulate reputation scores based on their observed behavior, with these scores influencing their probability of selection for critical committees. This approach naturally enhances both performance and security without compromising the theoretical $t < n/3$ resilience guarantee, as the protocol would converge toward optimal committee structures through iterative refinement.

The power of adaptive quorum sampling lies in its ability to harness empirical observations about network behavior to improve theoretical guarantees. As validators demonstrate consistent reliability, the effective resilience of the system increases beyond the worst-case $t < n/3$ bound, while maintaining formal security guarantees. This adaptation helps the protocol perform better in practical deployments with heterogeneous validator reliability, potentially achieving near-optimal performance in stable network conditions while gracefully degrading under attack.

Sophisticated Adversary Resilience Our basic analysis assumes a static Byzantine adversary, but real-world systems face more sophisticated threats. One particularly challenging adversarial capability is after-the-fact removal, which occurs when an adversary corrupts validators after they've

sent messages, potentially allowing the adversary to suppress those messages retroactively. EABA remains secure against this threat because committee threshold signatures cannot be invalidated once generated, even if validators are later corrupted. The adversary cannot corrupt enough validators to invalidate threshold signatures without exceeding the $t < n/3$ bound, and the VRF-based committee selection prevents the adversary from predicting which validators will be critical for each committee.

Similarly, EABA maintains security against adversaries with network control capabilities, who may manipulate message delivery scheduling, selectively accelerate messages between corrupt validators, or introduce bounded delays. The asynchronous model already assumes unbounded but finite message delays, and the committee structure ensures progress even if some committees are delayed. If the primary protocol stalls due to message manipulation, the backup agreement mechanism triggers, ensuring eventual termination. The committee-based structure provides inherent robustness against network manipulation because the adversary would need to disrupt communication for a significant fraction of committees simultaneously to prevent progress.

Cryptographic Efficiency Improvements The bit complexity of our protocol could be further optimized through advanced cryptographic techniques without sacrificing security guarantees. Aggregatable signatures represent a promising approach for reducing the size of committee decisions from $O(\lambda \cdot |C_j|)$ to $O(\lambda)$, substantially decreasing communication overhead for large committees. These schemes allow multiple signatures to be combined into a single constant-size signature that can be verified against the original messages and public keys, preserving the security semantics of individual signatures while dramatically reducing communication costs.

Succinct non-interactive arguments could similarly compress validity proofs for proposed values, allowing validators to verify complex predicates with minimal communication overhead. These cryptographic tools enable a validator to prove that a value satisfies arbitrary computational predicates without revealing the value itself or requiring interactive verification, which aligns perfectly with EABA's asynchronous execution model. Integrating these advanced primitives would preserve all security properties while further reducing communication complexity, making the

protocol more efficient for large-scale deployments with complex validation requirements.

6.2 Post-Quantum Considerations

Quantum computing poses significant threats to current cryptographic primitives, necessitating careful analysis of EABA's security in post-quantum settings. Digital signatures used for message authentication are highly vulnerable to Shor's algorithm, which can efficiently solve the discrete logarithm and integer factorization problems underlying most current signature schemes. Similarly, Verifiable Random Functions used for committee selection would be compromised if based on these same mathematical problems. Hash functions used for data integrity are moderately weakened by Grover's algorithm, which provides a quadratic speedup for brute-force attacks, but they remain usable with increased security parameters. This vulnerability assessment highlights the need for systematic replacement of quantum-vulnerable components to ensure long-term security.

Fortunately, EABA can be made quantum-resistant through careful cryptographic substitutions. Hash-based signatures like SPHINCS+ offer provable security against quantum attacks and could replace conventional digital signatures with minimal protocol modifications. Lattice-based cryptographic primitives provide efficient alternatives for VRFs and other public-key operations, with security reductions to problems believed to resist quantum attacks. Hash-based accumulators could provide efficient data integrity verification even against quantum adversaries. The modular design of EABA allows these substitutions without changing the protocol's fundamental structure or security properties.

These quantum-resistant replacements do introduce efficiency trade-offs that must be carefully managed. Post-quantum signatures are typically larger than their classical counterparts, sometimes by factors of 10-100×, increasing communication complexity. Computational overhead for signature generation and verification also increases, potentially affecting latency in time-sensitive applications. However, these trade-offs are manageable for most applications, especially considering the long-term security benefits. The committee-based structure of EABA actually helps mitigate these costs by limiting the number of signatures that must

be transmitted throughout the network, making the protocol relatively efficient even with quantum-resistant primitives.

6.3 Open Challenges and Research Directions

Despite EABA's theoretical advances, several challenges and opportunities for improvement remain:

Practical Implementation Challenges EABA faces practical deployment hurdles that warrant further investigation. The committee formation process introduces coordination overhead in dynamic networks, and our asymptotic bounds may have substantial constant factors in smaller deployments ($n < 100$). The protocol also requires secure infrastructure for VRF-based committee selection, distributed key generation for threshold signatures, and reliable validator identification to prevent Sybil attacks.

Theoretical Refinements Key theoretical challenges include:

- Reducing reliance on computational hardness assumptions while preserving efficiency
- Identifying minimal cryptographic requirements for achieving $t < n/3$ resilience with sub-quadratic complexity
- Developing hybrid security models combining computational and information-theoretic guarantees
- Supporting dynamic validator participation without compromising security

Efficiency Optimizations Promising directions for efficiency improvements include:

- Cross-layer optimizations with network-level broadcast primitives
- Application-specific validation procedure optimizations
- More sophisticated committee selection mechanisms to reduce constant factors
- Hardware acceleration for cryptographic operations

Future research building on EABA can create more efficient and practical asynchronous Byzantine agreement protocols suitable for critical infrastructure. The committee-based paradigm we've introduced establishes a solid foundation for innovations that balance theoretical optimality with practical efficiency.

7 Conclusion

In this paper, we have presented a comprehensive survey and theoretical analysis of asynchronous Multi-Valued Byzantine Agreement (MVBA) protocols that use randomization to circumvent the FLP impossibility result. Our systematic examination of existing approaches, including HMVBA, Reducer, Reducer++, and FIN-MVBA, reveals a persistent gap between protocols achieving optimal resilience ($t < n/3$) and those with lower message complexity and minimal cryptographic assumptions.

Building on these insights, we introduced EABA, a committee-based Byzantine agreement protocol that achieves optimal $t < n/3$ resilience while maintaining sub-quadratic $O(n \log n)$ message complexity under standard cryptographic assumptions. Through rigorous security analysis, we demonstrated that EABA provides agreement, validity, and termination despite Byzantine adversaries in asynchronous networks. Our information-theoretic bounds in Section 5 establish fundamental trade-offs between resilience, communication complexity, and time complexity, proving that any asynchronous Byzantine agreement protocol with $O(1)$ expected time requires $\Omega(n \log n)$ messages, a bound that EABA matches.

The theoretical significance of our work extends beyond EABA itself. Theorem 6 confirms that $t < n/3$ is the optimal resilience threshold for asynchronous Byzantine agreement, while Theorems 7-9 establish lower bounds on communication complexity that demonstrate EABA's near-optimality along multiple dimensions. This contributes to a deeper understanding of the inherent limitations in asynchronous consensus systems.

We have addressed potential extensions and limitations of EABA, including its security against sophisticated adversarial capabilities like after-the-fact removal and network control. We examined post-quantum considerations, identifying paths to quantum resistance through hash-based signatures and lattice-based cryptographic primitives while acknowledging the efficiency trade-offs these introduce. Finally, we identified open challenges including practical implementation hurdles, reducing reliance on computational hardness assumptions, and potential efficiency optimizations through cross-layer approaches.

This work advances the state of the art in asynchronous Byzantine agreement by bridging the gap between theoretical optimality and prac-

tical efficiency, establishing a foundation for more scalable fault-tolerant distributed systems while identifying promising directions for future research.

References

1. ABRAHAM, I., MALKHI, D., AND SPIEGELMAN, A. Asymptotically optimal validated asynchronous byzantine agreement. In *Proceedings of the 2019 ACM Symposium on Principles of Distributed Computing* (2019), pp. 337–346.
2. CACHIN, C., KURSAWE, K., PETZOLD, F., AND SHOUP, V. Secure and efficient asynchronous broadcast protocols. In *Annual International Cryptology Conference* (2001), Springer, pp. 524–541.
3. CACHIN, C., AND TESSARO, S. Asynchronous verifiable information dispersal. In *24th IEEE Symposium on Reliable Distributed Systems (SRDS'05)* (2005), IEEE, pp. 191–201.
4. CASTRO, M., AND LISKOV, B. Practical byzantine fault tolerance and proactive recovery. *ACM Transactions on Computer Systems (TOCS) 20*, 4 (2002), 398–461.
5. CHEN, J. Ociormvba: Near-optimal error-free asynchronous mvba. *arXiv preprint arXiv:2501.00214* (2024).
6. DUAN, S., WANG, X., AND ZHANG, H. Fin: Practical signature-free asynchronous common subset in constant time. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security* (2023), pp. 815–829.
7. FENG, H., LU, Z., MAI, T., AND TANG, Q. Making hash-based mvba great again. *Cryptology ePrint Archive* (2024).
8. FENG, H., LU, Z., AND TANG, Q. $\tilde{O}$ptimal adaptively secure hash-based asynchronous common subset. *Cryptology ePrint Archive* (2024).
9. GUO, B., LU, Y., LU, Z., TANG, Q., XU, J., AND ZHANG, Z. Speeding dumbo: Pushing asynchronous bft closer to practice. *Cryptology ePrint Archive* (2022).
10. KOKORIS-KOGIAS, E. Robust and scalable consensus for sharded distributed ledgers. *Cryptology ePrint Archive* (2019).
11. KOMATOVIC, J., NEU, J., AND ROUGHGARDEN, T. Toward optimal-complexity hash-based asynchronous mvba with optimal resilience. *arXiv preprint arXiv:2410.12755* (2024).
12. KOTLA, R., ALVISI, L., DAHLIN, M., CLEMENT, A., AND WONG, E. Zyzzyva: speculative byzantine fault tolerance. In *Proceedings of twenty-first ACM SIGOPS symposium on Operating systems principles* (2007), pp. 45–58.
13. LU, Y., LU, Z., TANG, Q., AND WANG, G. Dumbo-mvba: Optimal multi-valued validated asynchronous byzantine agreement, revisited. In *Proceedings of the 39th symposium on principles of distributed computing* (2020), pp. 129–138.