Appendix A
Security Analysis

Numerous state-of-the-art consensus protocols have now unanimously chosen to employ threshold signatures to reduce the communication overhead and simplify the verification process. However, it is extremely difficult to guarantee a consensus protocol's adaptive security if it employs a static threshold cryptographic primitive. Therefore, to achieve dynamic defence against adaptive adversaries and high-performance scaling, we adopt an adaptively secure BLS threshold signature, AdaptiveBLS [57], and reimplement it in a large-scale scenario. We follow the mathematical assumptions and proof principles presented in [31], [33], [34], [56]–[59]. Formal proofs of adaptive security for AdaptiveBLS and AdaptiveBFT are as follows.

Reimplementation of AdaptiveBLS [57]. Let $\bar{g}_1, \tilde{g}_1, \hat{g}_1 \in \mathbb{G}_1$ be uniformly random independent generators of $\mathbb{G}_1$. H_0, H_1, and $\mathsf{H}_2 : \{0,1\}^* \rightarrow \mathbb{G}_2$ are different cryptographic hash functions modeled as random oracles. Let $\mathsf{sk}_i := (u(i), v(i), w(i))$, $\{\mathsf{pk}_j := \bar{g}_1^{u(j)} \tilde{g}_1^{v(j)} \hat{g}_1^{w(j)}\}_{j \in [n]}$, $\mathsf{pk} := \bar{g}_1^{u(0)} \tilde{g}_1^{v(0)} \hat{g}_1^{w(0)} = \bar{g}_1^{u(0)}$, where $u(\cdot)$, $v(\cdot)$, and $w(\cdot)$ are different uniformly random polynomials of degree t and $v(0) = w(0) = 0$. We introduce Bulletproof, a zero-knowledge proof construction without trustworthy setup, transforming the signature σ_i of i for m into (π_i, σ_i), where π_i is the correctness proof for verification of σ_i provided by Bulletproof. Let the reimplemented AdaptiveBLS be AdaptiveBLS*.

Next, we prove the adaptive security of AdaptiveBLS* with a series of games $\mathsf{SEUF-CMA}_{\Sigma}^{\mathcal{A}}$.

GAME $\mathbf{G_0}$**:** Define the security game $\mathsf{SEUF-CMA}_{\Sigma}^{\mathcal{A}}$, which follows the honest protocol and allows an adaptive adversary $\mathcal{A}$ to access random oracle. Let $\mathcal{A}$ always output the forgery $(\tilde{\sigma}, \tilde{m})$ after querying $\mathsf{H}_0(\tilde{m})$, w.l.o.g., the advantage of $\mathcal{A}$ follows:

$$\mathsf{Adv}_{\mathsf{SEUF-CMA}}^{\mathcal{A},\Sigma}(\lambda) = \Pr\left[\mathbf{G_0} \Rightarrow 1\right] = \varepsilon_\sigma$$

GAME $\mathbf{G_1}$**:** Let $\tilde{m}_r$ be input to r-th random oracle query and $s \xleftarrow{\$} [q_h]$. If $\mathcal{A}$ forges a message $\tilde{m}_r$ with $r \neq s$ or queries over $t - |\mathcal{C}|$ partial signatures for $\tilde{m}_s$, the game aborts. $\mathbf{G_1}$ is identical to $\mathbf{G_0}$, by standard argument, there:

$$\Pr\left[\mathbf{G_1} \Rightarrow 1\right] \geq 1/q_h \cdot \Pr\left[\mathbf{G_0} \Rightarrow 1\right]$$

GAME $\mathbf{G_2}$**:** Let $\xi_{\tilde{g}_1}, \xi_{\hat{g}_1} \xleftarrow{\$} \mathbb{Z}_p$, $\tilde{g}_1 := \bar{g}_1^{\xi_{\tilde{g}_1}}$, and $\hat{g}_1 := \bar{g}_1^{\xi_{\hat{g}_1}}$. $\mathbf{G_2}$ is identical to $\mathbf{G_1}$, by the standard argument, there:

$$\Pr[\mathbf{G_1} \Rightarrow 1] = \Pr[\mathbf{G_2} \Rightarrow 1]$$

GAME $\mathbf{G_3}$**:** Let $\xi := \xi_{\tilde{g}_1} + \omega \xi_{\hat{g}_1}$, where $\omega \xleftarrow{\$} \mathbb{Z}_p$. Others are identical to $\mathbf{G_2}$. Let $\mu_r \xleftarrow{\$} \mathbb{Z}_p$. Only for the r-th random oracle query, the following changes are made to the random oracles:

$$\mathsf{H}_0(\tilde{m}_r) := {g_2}^{\mu_r}$$
$$\mathsf{H}_1(\tilde{m}_r) := {g_2}^{\xi \cdot \mu_r}$$

Lemma 4. $|\Pr[\mathbf{G_2} \Rightarrow 1] - \Pr[\mathbf{G_3} \Rightarrow 1]| \leq \varepsilon_{\mathsf{DDH}} + 1/|\mathbb{Z}_p|$.

Proof. Based on Lemma 2 and Lemma 3 of AdaptiveBLS, distributions D_0 and D_1 are indistinguishable; D_0 and $\mathsf{D}_{1,r}$ are indistinguishable, respectively:

$$\xi \xleftarrow{\$} \mathbb{Z}_p, (\mu_s, \nu_s) \xleftarrow{\$} \mathbb{Z}_p^2;\ \ \mathsf{D}_0 := g_2, g_2^{\xi}, \{(g_2^{\mu_s}, g_2^{\nu_s})\}_{s \in [q_h]}$$
$$\xi \xleftarrow{\$} \mathbb{Z}_p, \mu_s \xleftarrow{\$} \mathbb{Z}_p; \qquad \mathsf{D}_1 := g_2, g_2^{\xi}, \{(g_2^{\mu_s}, g_2^{\xi \cdot \mu_s})\}_{s \in [q_h]}$$
$$\xi, \mu_s \xleftarrow{\$} \mathbb{Z}_p, \nu_s := \xi \cdot \mu_s;\ \ \mathsf{D}_{1,r} := g_2, \{(g_2^{\mu_s}, g_2^{\nu_s})\}_{s \in [q_h]}$$

Thus, samples from distributions D_0 and $\mathsf{D}_{1,s}$ are computationally indistinguishable with:

$$|\Pr[\mathbf{G_2} \Rightarrow 1] - \Pr[\mathbf{G_3} \Rightarrow 1]| \leq \varepsilon_{\mathsf{DDH}} + 1/|\mathbb{Z}_p|$$

□

GAME $\mathbf{G_4}$**:** $\mathbf{G_4}$ is identical to $\mathbf{G_3}$. Simulated Bulletproof provides proof of correctness for partial signatures without revealing information about sk_i. Denote the random oracle query of $\mathcal{A}$ conflicts with the H_2 query as $\mathcal{I}$, then the game abort probability is:

$$\begin{aligned} |\Pr[\mathbf{G_3} \Rightarrow 1] - \Pr[\mathbf{G_4} \Rightarrow 1]| &= |\Pr[\mathbf{G_3} \Rightarrow 1 : \mathcal{I}] \\ &\quad - \Pr[\mathbf{G_4} \Rightarrow 1 : \mathcal{I}]| \cdot \Pr[\mathcal{I}] \\ &\leq \Pr[\mathcal{I}] \\ &\leq (n \cdot q_s \cdot q^*)/|\mathbb{Z}_p|^2 \end{aligned}$$

where q^* is the maximum count of random oracle queries from $\mathcal{A}$ to H_2, and q_s is the maximum count of signature queries (up to n partial signatures per simulation) from $\mathcal{A}$.

GAME $\mathbf{G_5}$**:** Change only the sampling method of the keys for signing. Based on Lemma 6 of AdaptiveBLS, sampling the signature key polynomials for $\mathbf{G_4}$ and $\mathbf{G_5}$, respectively, both of which are random degree t polynomials. Thus, the view of $\mathcal{A}$ is identical in $\mathbf{G_4}$ as in $\mathbf{G_5}$, i.e.,

$$\Pr[\mathbf{G_4} \Rightarrow 1] = \Pr[\mathbf{G_5} \Rightarrow 1]$$

GAME $\mathbf{G_6}$**:** $\mathbf{G_6}$ is identical to $\mathbf{G_5}$. Change only the simulated Bulletproof to actual Bulletproof for partial signatures. Thus, the view of $\mathcal{A}$ is identical in $\mathbf{G_5}$ as in $\mathbf{G_6}$, i.e.,

$$|\Pr[\mathbf{G_5} \Rightarrow 1] - \Pr[\mathbf{G_6} \Rightarrow 1]| \leq (n \cdot q_s \cdot q^*)/|\mathbb{Z}_p|^2$$

Thus, from the series of games above, there:

$$\begin{aligned} |\Pr[\mathbf{G_0} \Rightarrow 1] - \Pr[\mathbf{G_6} \Rightarrow 1]| &\leq (1 - 1/q_h) \cdot \Pr[\mathbf{G_0} \Rightarrow 1] \\ &\quad + \varepsilon_{\mathsf{DDH}} + 1/|\mathbb{Z}_p| \\ &\quad + 2(n \cdot q_s \cdot q^*)/|\mathbb{Z}_p|^2 \\ \Longrightarrow \qquad \Pr[\mathbf{G_6} \Rightarrow 1] &\geq 1/q_h \cdot \varepsilon_\sigma \\ &\quad - \varepsilon_{\mathsf{DDH}} - 1/|\mathbb{Z}_p| \\ &\quad - 2(n \cdot q_s \cdot q^*)/|\mathbb{Z}_p|^2 \end{aligned}$$

Theorem 3 (Adaptive Security of AdaptiveBLS*)**.** *Let* $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_\mathrm{T}, \mathbb{F}_p, p)$ *be the public parameters of AdaptiveBLS*. Assuming any PPT adaptive adversary* $\mathcal{A}$ *that conducts at most* q_s *signature queries (maximum* n *partial signatures per session), at most* q_h *hash queries (also known as random oracle queries) to* H_0 *and* H_1*, and at most* q^* *random oracle queries to* H_2 *wins the game* $\mathsf{SEUF-CMA}_{\Sigma}^{\mathcal{A}}$ *with probability:*

$$\varepsilon_\sigma \leq q_h \cdot \left(\varepsilon_{\mathsf{DDH}} + \varepsilon_{\mathsf{CDH}} + 1/|\mathbb{Z}_p| + 2(n \cdot q_s \cdot q^*)/|\mathbb{Z}_p|^2\right)$$

Proof. Based on the formal analysis of $\mathbf{G_0} - \mathbf{G_6}$ above, it is clear that for an adaptive adversary $\mathcal{A}$ that outputs a forgery on message $\tilde{m}_s$ with probability $\varepsilon_\sigma/q_h - \varepsilon_{\mathsf{DDH}} - 1/|\mathbb{Z}_p| - 2(n \cdot q_s \cdot q^*)/|\mathbb{Z}_p|^2$, we can compute the $\mathsf{co-CDH}$ solution efficiently using the forgery on $\tilde{m}_s$. And ε_σ is negligible. Thus, our AdaptiveBLS* is $(T, q_h, q_s, \varepsilon)$-secure against strong existential forgery under adaptive chosen message attacks (SEUF-CMA). This demonstrates that AdaptiveBLS* realizes adaptive security. □

AdaptiveBLS* enhances and ensures the adaptive security of AdaptiveBFT under strong adaptive adversaries, which is proved as follows.

Theorem 4 (Adaptive Security of AdaptiveBFT)**.** *Let* $0 < \varepsilon_{\mathcal{A}} < 1$*. Assume that AdaptiveBFT is a partially synchronous BFT consensus protocol with the threshold signature using AdaptiveBLS***. Then AdaptiveBFT is secure up to* $\mathcal{T} \leq (1 - \varepsilon_{\mathcal{A}})\, n/2$ *adaptive corruptions, where* $\varepsilon_{\mathcal{A}}^{min} = 1 - 2t/n$*.*

Proof. Denote the case where the honest replica $R^* \in \mathcal{H}$ is corrupted by an adaptive adversary $\mathcal{A}$ as $\mathcal{I}^*$. Then, the advantage of $\mathcal{A}$ in the AdaptiveBFT is:

$$\mathsf{Adv}_{\mathsf{BFT}}^{\mathcal{A}}(\lambda) = \Pr\left[\mathcal{I}^*\right] = \varepsilon_{\mathsf{BFT}}$$

Therefore, we have:

$$\varepsilon_{\mathsf{BFT}} \leq q_h \cdot \left(\varepsilon_{\mathsf{DDH}} + \varepsilon_{\mathsf{CDH}} + 1/|\mathbb{Z}_p| + 2(n \cdot q_s \cdot q^*)/|\mathbb{Z}_p|^2\right)$$

Thus, AdaptiveBFT is $(T, q_h, q_s, \varepsilon)$-secure against strong existential forgery under adaptive chosen message attacks (SEUF-CMA). This demonstrates that our AdaptiveBFT realizes adaptive security. □

Appendix B
TLA+ Formal Specification and Verification

To rigorously validate the safety and liveness properties of AdaptiveBFT, particularly its novel *Adaptive View-Change* (AVC) and *Adaptive Pipeline Scheduling* (APS) mechanisms, we developed a comprehensive formal specification using the TLA+ language. Unlike static BFT protocols, AdaptiveBFT incorporates dynamic behaviors (specifically probabilistic leader election driven by reputation and runtime parameter reconfiguration) which introduce non-determinism and an infinite state space. We address these verification challenges by abstracting cryptographic primitives and employing symbolic model checking via Apalache, enabling the verification of safety properties against an unbounded stream of adaptive configuration changes.

A. System Modeling and State Abstraction

The system is modeled as a set of replicas $\mathcal{R} = \{r_1, \ldots, r_n\}$ communicating over a partially synchronous network. The global system state Σ is defined as a tuple $\Sigma = \langle \mathit{chain}, \mathit{pool}, \mathit{replicaState}, \mathit{config}, \mathit{reputation} \rangle$.

Blockchain and Message Abstraction. We model the blockchain as a directed acyclic graph (DAG). To mitigate state space explosion, we abstract cryptographic hashes and digital signatures using symbolic references. A block b is rigorously defined as a record:

$$b \triangleq [\mathit{view} \in \mathbb{N}, \mathit{parent} \in \mathit{Ref}, \mathit{qc} \in QC, \mathit{payload} \in Tx^*] \tag{7}$$

The message pool pool represents the network state, storing all emitted messages. A Quorum Certificate (QC) is modeled not as a set of signatures, but as a state predicate $IsQC(v, b)$, which evaluates to true if and only if a supermajority of valid votes for block b in view v exists in pool. This abstraction preserves the causal dependencies required for BFT safety while eliminating the overhead of cryptographic operations.

B. Formalizing Adaptive View-Change (AVC)

The primary challenge in verifying AVC lies in modeling the *Reputation-Weighted Verifiable Random Cryptographic Sortition* (RVS) without implementing the complex arithmetic of Verifiable Random Functions (VRF). We introduce an abstract operator $\mathit{IsElected}(r, v, \rho)$ to model the probabilistic election outcome deterministically within the model checker's scope.

RVS Abstraction. Let $\rho : \mathcal{R} \to \mathbb{R}_{\geq 0}$ be the global reputation vector. We define a non-deterministic oracle $\mathcal{O} : \mathbb{N} \times [\mathcal{R} \to \mathbb{R}] \to \mathcal{R}$. In TLA+, we specify this to cover all valid sortition outcomes where a node's selection probability is non-zero, as shown in Listing 1.

Listing 1: TLA+ abstraction of RVS.

```
(* Abstracting Algorithm 1: RVS *)
VARIABLES reputation

(* Predicate: Is replica r a valid primary for view v?
    *)
IsElected(r, v) ==
   LET totalRep == Sum(reputation)
       (* Abstracting the VRF threshold check Eq.(1) *)
       threshold == reputation[r] / totalRep
   IN
   (* Model check covers all potential elections
      supported by non-zero reputation *)
   threshold > 0 /\ Oracle(v) = r
```

Listing 2: Modeling dynamic configuration updates.

```
VARIABLES config

(* Modeling the APS Explore and Update cycle *)
UpdateConfig ==
   /\ \E newParams \in ValidParameterSpace :
       (* Only allow updates via metric triggers *)
       /\ ShouldTriggerUpdate(metrics)
       (* Ensure new config maintains safety invariants
            *)
       /\ config' = newParams
   /\ UNCHANGED <<chain, pool, replicaState,
         reputation>>
```

The View-Change logic is integrated into the *Propose* action. The validity of a proposal is strictly context-dependent on the dynamic reputation state, formally preventing low-reputation nodes from successfully proposing blocks even if they are Byzantine.

C. Formalizing Adaptive Pipeline Scheduling (APS)

The APS mechanism introduces dynamic reconfiguration of system parameters $\mathcal{S} = \mathcal{A} \times \mathcal{P} \times \mathcal{D} \times \mathcal{T}$, which are typically treated as constants in static protocols. In our specification, we promote the configuration to a mutable state variable config. We define a dedicated action $\mathit{UpdateConfig}$ (Listing 2) to model the behavior of the $\mathit{Monitor}$ and $\mathit{Explorer}$ modules. This allows the model checker to explore interleavings between parameter updates and consensus steps, verifying that runtime parameter changes do not violate safety guarantees.

D. Verification Strategy and Theorems

We utilize Apalache to verify *Agreement* and *Chain Consistency* using Inductive Invariants. Given the complexity of RVS and APS, we constructed a hierarchical invariant $Inv \triangleq Inv_{type} \wedge Inv_{lock} \wedge Inv_{safety}$.

Theorem 5 (Safety under Adaptive Scheduling)**.** *For all execution traces σ and any valid sequence of configuration changes determined by APS, the committed chain remains linear:*

$$\Box(\forall b_1, b_2 \in \mathit{Committed}(\sigma) : b_1.\mathit{view} = b_2.\mathit{view} \implies b_1 = b_2) \tag{8}$$

This theorem confirms that aggressive optimizations by the APS module (such as asynchronous pre-ordering) do not violate the fundamental safety rules regarding locking and commit criteria.

Theorem 6 (AVC Soundness)**.** *The AVC mechanism guarantees that a view finalized via RVS preserves the safety of previous views. This is verified by the inductive invariant $LockedQCPreservation$:*

$$\Box(\mathit{IsElected}(r, v) \implies \mathit{ExtendsLockedChain}(r, v)) \tag{9}$$

E. Model Checking Results

We conducted bounded model checking on instances with $n = 4$ replicas ($f = 1$) and dynamic parameter spaces using Apalache. The verification process explored a state space depth of up to 20 steps, confirming the following:

- **Resilience to Low-Reputation Attacks:** The $\mathit{IsElected}$ constraint effectively prevents nodes with degraded reputation (simulating adaptive adversary corruption) from equivocating. The model checker found no traces where a low-reputation adversary successfully forked the chain.
- **Safety of Decoupling:** The $\mathit{UpdateConfig}$ action was verified to be safe. Despite altering message propagation delays and priorities, the invariant that a Commit implies a supermajority of locks holds true, validating the Triple-Decoupling strategy.