

PolyShard: Coded Sharding Achieves Linearly Scaling Efficiency and Security Simultaneously

Songze Li, Mingchao Yu, Chien-Sheng Yang, A. Salman Avestimehr, Sreeram Kannan and Pramod Viswanath

Abstract—Today’s blockchain designs suffer from a trilemma claiming that no blockchain system can simultaneously achieve decentralization, security, and performance scalability. For current blockchain systems, as more nodes join the network, the efficiency of the system (computation, communication, and storage) stays constant at best. A leading idea for enabling blockchains to scale efficiency is the notion of sharding: different subsets of nodes handle different portions of the blockchain, thereby reducing the load for each individual node. However, existing sharding proposals achieve efficiency scaling by compromising on trust - corrupting the nodes in a given shard will lead to the permanent loss of the corresponding portion of data. In this paper, we settle the trilemma by demonstrating a new protocol for coded storage and computation in blockchains. In particular, we propose PolyShard: “polynomially coded sharding” scheme that achieves information-theoretic upper bounds on the efficiency of the storage, system throughput, as well as on trust, thus enabling a truly scalable system. We provide simulation results that numerically demonstrate the performance improvement over state of the arts, and the scalability of the PolyShard system. Finally, we discuss potential enhancements, and highlight practical considerations in building such a system.

Index Terms—Scalability; Blockchain; Security and Trust; Decentralized networks; Coded Sharding; Information Theory.

I. INTRODUCTION

WHILE Blockchain systems promise a host of new and exciting applications, such as digital cryptocurrency [1], industrial IoT [2], and healthcare management [3], their scalability remains a critical challenge [4]. In fact, a well-known blockchain trilemma (see Figure 1) has been raised [5]

Manuscript received January 23, 2020; revised May 27, 2020; accepted June 24, 2020. This material is based upon work supported by the Distributed Technology Research Foundation, Input-Output Hong Kong, the National Science Foundation under grants CCF-1705007, CCF-1763673 and CCF-1703575, and the Army Research Office under grant W911NF1810332. This material is also based upon work supported by Defense Advanced Research Projects Agency (DARPA) under Contract No. HR001117C0053. The views, opinions, and/or findings expressed are those of the authors and should not be interpreted as representing the official views or policies of the Department of Defense or the U.S. Government. A part of this paper was presented in IEEE ISIT 2020. The associate editor coordinating the review of this manuscript and approving it for publication was Associate Editor Prof. Debdeep Mukhopadhyay. (Corresponding author: Chien-Sheng Yang.)

S. Li, M. Yu, C.-S. Yang and A. S. Avestimehr are with the Department of Electrical and Computer Engineering, University of Southern California, Los Angeles, CA 90089 USA (e-mail: songzeli@usc.edu; mingchay@usc.edu; chienhsy@usc.edu; avestimehr@ee.usc.edu).

S. Kannan is with the Department of Electrical and Computer Engineering Department, University of Washington, Seattle, WA 98195, USA (e-mail: ksreeram@uw.edu).

P. Viswanath is with the Department of Electrical and Computer Engineering Department, University of Illinois at Urbana-Champaign, IL 61820, USA (e-mail: pramodv@illinois.edu).

claiming that no decentralized ledger system can simultaneously achieve 1) security (against adversarial attacks), 2) decentralization (of computation and storage resources), and 3) scalability (of throughput with the network size). All existing major blockchains either achieve decentralization at the cost of efficiency, or efficiency at the cost of decentralization and/or security.

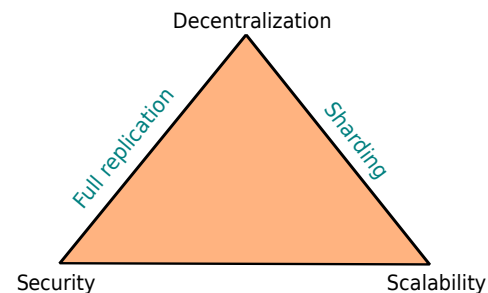


Fig. 1: Blockchain trilemma. No current blockchain system can simultaneously achieve decentralization, security, and scalability.

The focus of this paper is to formalize and study a version of the blockchain trilemma, in order to understand whether it is fundamental to blockchain systems. Corresponding to the three traits in the trilemma, we study the following performance measures of blockchain systems: security - measured as the number of malicious nodes the system can tolerate, decentralization - measured as the fraction of the block chain (or ledger) that is stored and processed by each node (we denote its inverse by *storage efficiency*), and scalability - measured as the total *throughput* of the system (e.g., number of computations performed in the system (e.g., number of transactions verified) in a unit period of time).

Within this context, let us first examine the current blockchain systems. Bitcoin [1] and Ethereum [6] are designed based on a *full replication* system, in which each network node stores the entire blockchain and replicates all the computations (e.g., transaction verifications), as demonstrated in Figure 2(a). This feature enables high security (of tolerating 49% adversarial nodes), however drastically limits the storage efficiency and throughput of the system: they stay constant regardless of the number of nodes N . For example, Bitcoin currently restricts its block size to 1 MB, and processing rate to 7 transactions/sec [7]. In practice, the computational burden even increases with N (e.g., mining puzzles get harder as time progresses and more users participate), causing the throughput to drop.

To scale out throughput and storage efficiency, the leading solution being discussed in the blockchain literature is via

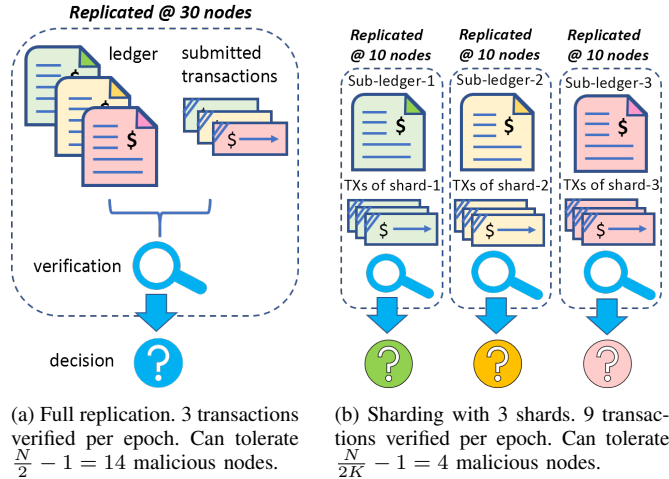


Fig. 2: A blockchain system with 30 nodes, each of which is capable of verifying 3 transactions per epoch. With 3-sharding, the ledger is partitioned into 3 sub-ledgers, and transactions are limited to between the accounts within the same sub-ledger. Sharding improves the storage and throughput efficiency by 3 times, at the cost of compromising security by about 3 times.

sharding [8]–[10]. The key idea is to partition the blockchain into K independent sub-chains, which are then replicated separately at $q = N/K$ nodes to yield K smaller full-replication systems, a.k.a., shards (Figure 2(b)). This way, both storage efficiency and throughput are improved by a factor of K . However, to scale this improvement with network size, K must increase linearly with N . Consequently, the number of nodes q per shard has to be held constant, which allows an attacker to corrupt as few as $q/2$ nodes to compromise a shard. This yields a security level of $q/2$, which approaches zero as N grows. Although various efforts have been made to alleviate this security issue (e.g., by periodically shuffling the nodes [9]), they are susceptible to powerful adversaries (e.g., who can corrupt the nodes *after* the shuffling), yet none scale security.

In summary, both full replication and sharding based blockchain systems make trade-offs between the scalability of throughput, storage efficiency, and security. However, such a trade-off is far from optimal from information theoretical point of view. Given the $N \times$ computation and $N \times$ storage resources across all the N network nodes, the following information-theoretic upper bounds hold: security $\leq \Theta(N)$; throughput $\leq \Theta(N)$; storage efficiency $\leq \Theta(N)$. It is intuitive that these bounds can be *simultaneously* achieved by a centralized system, allowing all the three metrics to scale. However, as pointed out by the trilemma, this has not been achieved by any existing decentralized system. This raises the following fundamental open problem:

Is there a blockchain design that *simultaneously* scales storage efficiency, security, and throughput?

We answer this question affirmatively by introducing the concept of *coded sharding*. In particular, we propose PolyShard (polynomially coded sharding), a scheme that simultaneously achieves linear scaling in throughput, storage

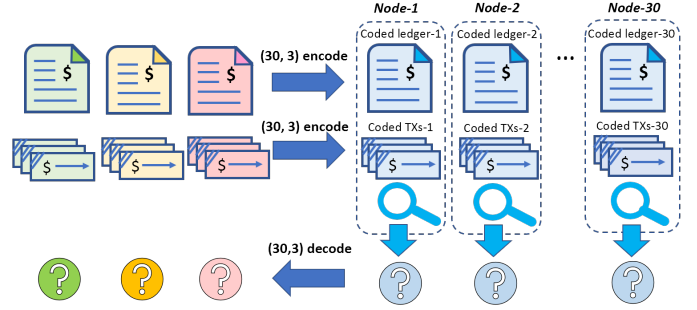


Fig. 3: The proposed PolyShard system with 30 nodes. Each node computes a verification function on a coded sub-ledger and a coded block, which are created by a distinct linear combination of the original sub-ledgers, and the proposed blocks respectively. Since encoding does not change the size of the sub-ledger, PolyShard achieves the same storage and throughput efficiency (i.e., 9 transactions per epoch) as the conventional sharding solution. Additionally, PolyShard improves the security guarantee to protect against $(N - K)/2 = 13$ malicious nodes, for degree-1 verification functions.

efficiency, and security (i.e., $\Theta(N)$). We show mathematically that PolyShard achieves all three information-theoretic upper bounds and enables a truly scalable blockchain system (see Table I).

	Storage efficiency	Security	Throughput
Full replication	$O(1)$	$\Theta(N)$	$O(1)$
Sharding	$\Theta(N)$	$O(1)$	$\Theta(N)$
Information-theoretic limit	$\Theta(N)$	$\Theta(N)$	$\Theta(N)$
PolyShard (this paper)	$\Theta(N)$	$\Theta(N)$	$\Theta(N)$

TABLE I: Performance comparison of the proposed PolyShard verification scheme with other benchmarks and the information-theoretic limits.

PolyShard is inspired by recent developments in *coded computing* [11]–[19], in particular Lagrange Coded Computing [19], which provides a transformative framework for injecting computation redundancy in unorthodox coded forms in order to deal with failures and errors in distributed computing. The key idea behind PolyShard is that instead of storing and processing a single uncoded shard as done conventionally, each node stores and computes on a coded shard of the same size that is generated by linearly mixing uncoded shards (Figure 3), using the well-known Lagrange polynomial. This coding provides computation redundancy to simultaneously provide security against erroneous results from malicious nodes, which is enabled by noisy polynomial interpolation techniques (e.g., Reed-Solomon decoding).

While coding is generally applicable in many distributed computing scenarios, the following two salient features make PolyShard particularly suitable for blockchain systems.

- *Oblivious*: The coding strategy applied to generate coded shards is oblivious of the verification function. That means, the same coded data can be simultaneously used for multiple verification items (examples: digital signature verification and balance checking in a payment system);
- *Incremental*: PolyShard allows each node to grow its local coded shard by coding over the newest verified blocks, without needing to access the previous ones. This helps to maintain a constant coding overhead as the chain grows.

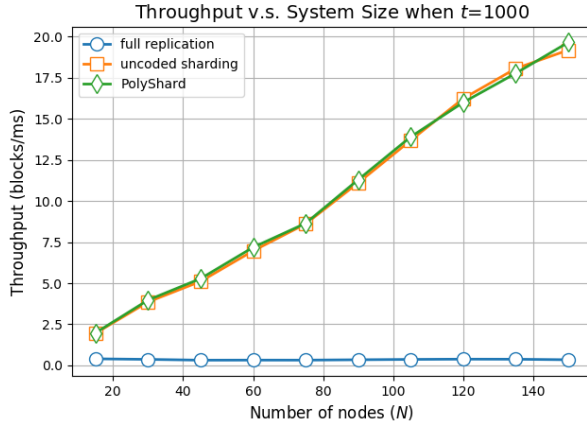


Fig. 4: Measured throughput of verification schemes; here number of epochs $t = 1000$.

As a proof of concept, we simulate a payment blockchain system, which keeps records of balance transfers between accounts, and verifies new blocks by checking the senders' fund sufficiency. We run experiments on this system for various combinations of network size and chain length, and measure/evaluate the throughput, storage, and security achieved by the full replication, sharding, and the PolyShard schemes. As we can see from the measurements plotted in Figure 4, PolyShard indeed achieves the throughput scaling with network size as the uncoded sharding scheme, improving significantly over the full replication scheme. These experiments provide an empirical verification of the theoretical guarantees of PolyShard in simultaneously scaling storage efficiency, security, and throughput.

To improve the number of supported shards, we also present iterative PolyShard in Appendix B. The key idea is to first represent verification functions as low-depth arithmetic circuits and then apply PolyShard iteratively to each layer of circuits.

In summary, the main contributions of this paper are as follows:

- Formalizing and resolving a version of the blockchain trilemma by proposing a radically different design methodology called PolyShard that for the first time leverages coding in both storage and computation of blockchain systems.
- Demonstrating that PolyShard simultaneously achieves linear scaling in throughput, storage efficiency, and security; hence meeting the information-theoretic limits.
- Numerical evaluation of PolyShard in a payment blockchain system and demonstrating its scalability in terms of throughput, storage efficiency, and security.
- Improving the maximum number of supported shards by proposing iterative PolyShard in Appendix B.

Other related works. Prominent sharding proposals in the literature are [8]–[10], [20]–[31]. As an example, ELASTICO [8] partitions the incoming transactions into shards, and each shard is verified by a disjoint committee of nodes in parallel. OmniLedger [9] improved upon ELASTICO in multiple avenues, including new methods to assign nodes into shards

with a higher security guarantee, an atomic protocol for cross-shard transactions, and further optimization on the communication and storage designs. Finally, there is also a growing interest for leveraging coding to deal with the issues of data availability, computation verification, and storage overhead in decentralized blockchain systems (e.g., [32]–[36]).

II. PROBLEM FORMULATION: BLOCK VERIFICATION

A blockchain system manages a decentralized ledger of its clients' transactions, over a large number of untrusted network nodes. The clients submit their transactions to the network nodes, who group the transactions into blocks that to be included in the system. The accepted blocks are organized into a chain where each block contains a hash pointer to its predecessor. The chain structure provides high security guarantee since for an adversary to tamper the contents of any block, it has to re-grow the entire chain afterwards, which is extremely expensive in computation power. Here we consider a *sharded* blockchain system whose grand ledger is partitioned into K independent shards, each of which maintains a disjoint sub-chain that records the transactions between the accounts associated with the same shard.¹ At a high level, at each time epoch, every shard proposes one block of transactions, and verifies it over the current state of its sub-chain. Once the block passes the verification, it will be appended to the corresponding sub-chain. We now define the system in more details.

A. Computation model

Each shard k ($k \in [1, K]$) maintains its own sub-chain. We denote the state of the k -th sub-chain before epoch t by $Y_k^{t-1} = (Y_k(1), \dots, Y_k(t-1))$, where $Y_k(t) \in \mathbb{U}$ denotes the block accepted to shard k at epoch t , and \mathbb{U} is a vector space over a field \mathbb{F} . When a new block $X_k(t) \in \mathbb{U}$ is proposed for shard k in epoch t (using some consensus algorithm like proof-of-work (PoW)), the blockchain system needs to verify its legitimacy (e.g., sender accounts have sufficient fund, no double-spending) over the current state Y_k^{t-1} . We abstract out the mechanism which generates the proposals and focus on verifying the proposed blocks.

We denote the verification function by $f^t : \mathbb{U}^t \rightarrow \mathbb{V}$, over $X_k(t)$ and the sub-chain Y_k^{t-1} , for some vector space \mathbb{V} over \mathbb{F} . For instance, for a cryptocurrency blockchain that keeps records of balance transfers between accounts (e.g., Bitcoin), typical verification functions include

- *Balance checking*: to check each transaction has more input values than those spent in its outputs; and also check that the transactions in a block contain sufficient funds to pay the transaction fees/mining rewards.
- *Signature checking*: to verify that a payment transaction spending some funds in an account is indeed submitted by the owner of that account. This often involves computing

¹We focus on transactions that are verifiable intra-shard for the sake of clarity. Extensions such as cross-shard transactions and their verification is an added complexity yet complementary to the contributions of this paper. For instance, the atomic payment and locking mechanisms of [9] can be naturally incorporated with the ideas in this paper.

cryptographic hashes using the account's public key, and verifying the results with the digital signature.

Having obtained $h_k^t = f^t(X_k(t), Y_k^{t-1})$, shard k computes an indicator variable $e_k^t \triangleq \mathbb{1}(h_k^t \in \mathcal{W})$, where $\mathcal{W} \subseteq \mathbb{V}$ denotes the set of function outputs that affirm $X_k(t)$. Finally, the verified block $Y_k(t)$ is computed as $Y_k(t) = e_k^t X_k(t)$, and added to the sub-chain of shard k . We note that if the block is invalid, an all-zero block will be added at epoch t .

B. Networking model

The above blockchain system is implemented distributedly over N untrusted nodes. We consider a homogeneous and synchronous network, i.e., all nodes have similar process power, and the delay of communication between any pair of nodes is bounded by some known constant. A subset $\mathcal{M} \subset \{1, \dots, N\}$ of the nodes may be corrupted, and are subject to Byzantine faults, i.e., they may compute and communicate arbitrary erroneous results during block verification. We aim to design secure verification schemes against the following strong adversary model:

- The adversaries can corrupt a fixed fraction of the network node, i.e., the number of malicious nodes grows linearly with N .²
- If a conventional sharding solution were employed, the adversaries know the allocation of nodes to the shards, and are able to adaptively select the subset \mathcal{M} of nodes to attack.

We note that under this adversary model, the random shard rotation approach [8], [9] is no longer secure since the adversaries can focus their power to attack a single shard after knowing which nodes are assigned into this shard. As illustrated in Fig. 5, we present the networking protocol that will be followed by the honest nodes. Note that adversarial nodes are not required to follow this protocol.

Storage. At epoch t , each node i , $i = 1, \dots, N$, locally stores some data, denoted by $Z_i^{t-1} = (Z_i(1), \dots, Z_i(t-1))$, where $Z_i(j) \in \mathbb{W}$ for some vector space \mathbb{W} over \mathbb{F} . The locally stored data Z_i^{t-1} is generated from all shards of the blockchain using some function ϕ_i^{t-1} , i.e., $Z_i^{t-1} = \phi_i^{t-1}(Y_1^{t-1}, \dots, Y_K^{t-1})$.

Verification. Given the K proposed blocks $\{X_k(t)\}_{k=1}^K$, one for each shard, the goal of block verification is to compute $\{f^t(X_k(t), Y_k^{t-1})\}_{k=1}^K$ distributedly over untrusted nodes. We implement this verification process in two steps. In the first step, each node i computes an intermediate result g_i^t using some function ρ_i^t on the proposed blocks and its local storage, such that $g_i^t = \rho_i^t(X_1(t), \dots, X_K(t), Z_i^{t-1})$, and then broadcasts the result g_i^t to all other nodes.

The nodes exploit the received computation results to reduce the final verification results in the second step. Specifically, each node i decodes the verification results for all K shards $\hat{h}_{1i}^t, \dots, \hat{h}_{Ki}^t$, using some function ψ_i^t , i.e., $(\hat{h}_{1i}^t, \dots, \hat{h}_{Ki}^t) = \psi_i^t(g_1^t, \dots, g_N^t)$. Using these decoded results, node i computes the indicator variables $\hat{e}_{ki}^t = \mathbb{1}(\hat{h}_{ki}^t \in \mathcal{W})$, and then the verified blocks $\hat{Y}_{ki}(t) = \hat{e}_{ki}^t X_k(t)$, for all $k =$

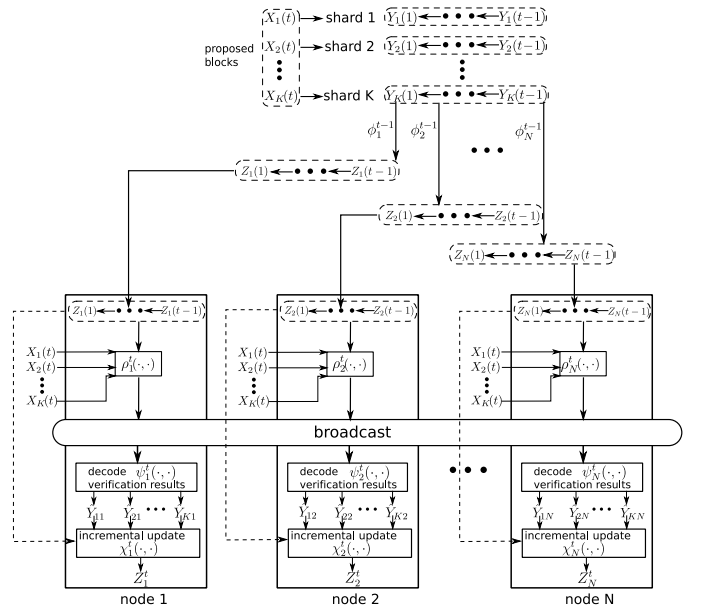


Fig. 5: Networking Model of blockchain system.

$1, \dots, K$. Finally, each node i utilizes the verified blocks to update its local storage using some function χ_i^t , i.e., $Z_i^t = \chi_i^t(\hat{Y}_{1i}(t), \dots, \hat{Y}_{Ki}(t), Z_i^{t-1}) = \phi_i^t(\hat{Y}_{1i}^t, \dots, \hat{Y}_{Ki}^t)$. Here \hat{Y}_{ki}^t is the sequence of blocks in shard k verified at node i up to time t . To update the local storage Z_i^t , while node i can always apply ϕ_i^t on the uncoded shards $\hat{Y}_{1i}^t, \dots, \hat{Y}_{Ki}^t$, it is highly desirable for χ_i^t to be *incremental*: we only need to create a coded block from $\hat{Y}_{1i}(t), \dots, \hat{Y}_{Ki}(t)$, and append it to Z_i^{t-1} . This helps to significantly reduce the computational and storage complexities.

C. Performance metrics

We denote a block verification scheme by S , defined as a sequence of collections of the functions, i.e., $S = (\{\phi_i^t, \rho_i^t, \psi_i^t, \chi_i^t\}_{i=1}^N)_{t=1}^\infty$. We are interested in the following three performance metrics of S .

Storage efficiency. Denoted by γ_S , it is defined as the ratio between the size of the entire block chain and the size of the data stored at each node, i.e.,

$$\gamma_S \triangleq \frac{K \log |\mathbb{U}|}{\log |\mathbb{W}|}. \quad (1)$$

The above definition also applies to a probabilistic formulation where the blockchain elements $Y_k(j)$ s and the storage elements $Z_i(j)$ s are modelled as i.i.d. random variables with uniform distribution in their respective fields, where the storage efficiency is defined using the entropy of the random variables.

Security. We say S is b -secure if the honest nodes can recover all the correct verification results under the presence of up to b malicious nodes. More precisely, for any subset $\mathcal{M} \subset \{1, \dots, N\}$ of malicious nodes with $|\mathcal{M}| \leq b$, and each node $i \notin \mathcal{M}$, a b -secure scheme will guarantee that $(\hat{h}_{1i}^t, \dots, \hat{h}_{Ki}^t) = (h_{1i}^t, \dots, h_{Ki}^t)$, for all $t = 1, 2, \dots$. We define

²While here the adversary model is defined in a permissioned setting, the model and the proposed solution can directly extend to a permissionless setting where e.g., in a PoW system, the adversaries can control a fixed fraction of the entire hashing power.

the security of S , denoted by β_S , as the maximum b it could achieve:

$$\beta_S \triangleq \sup\{b : S \text{ is } b\text{-secure}\}. \quad (2)$$

Throughput. We measure throughput of the system by taking into account the number of blocks verified per epoch and the associated computational cost. We denote by $c(f)$ the computational complexity of a function f , which is the number of additions and multiplications performed in the domain of f to evaluate f .

We define the throughput of S , denoted by λ_S , as the average number of blocks that are correctly verified per unit discrete round, which includes all the computations performed at all N nodes to verify the incoming K blocks. That is,

$$\lambda_S \triangleq \liminf_{t \rightarrow \infty} \frac{K}{\sum_{i=1}^N (c(\rho_i^t) + c(\psi_i^t) + c(\chi_i^t)) / (Nc(f^t))}. \quad (3)$$

The above three metrics correspond to the three traits in the blockchain trilemma, and all current blockchain systems have to trade off one for another. The goal of this paper is to understand the information-theoretic limits on these metrics, and design verification schemes that can simultaneously achieve the limits, hence settling the trilemma.

III. BASELINE PERFORMANCE

We first present the information-theoretic *upper* bounds on the three performance metrics for any blockchain. We then study the performance of two state-of-the-art blockchain schemes and comment on the gaps with respect to the upper bounds.

Information-theoretic upper bounds. In terms of security, the maximum number of adversaries any verification scheme can tolerate cannot exceed half of the number of network nodes N . Thus, the security $\beta \leq \frac{N}{2}$. In terms of storage, for the verification to be successful, the size of the chain should not exceed the aggregated storage resources of the N nodes. Otherwise, the chain cannot be fully stored. We thus have $\gamma \leq N$. Finally, to verify the K incoming blocks, the verification function f^t must be executed at least K times in total. Hence, the system throughput $\lambda \leq \frac{K}{K/N} = N$. Therefore, the information-theoretic upper bounds of security, storage efficiency, and throughput all scale linearly with the network size N .

Full replication. In terms of storage efficiency, since each node stores all the K shards of the entire blockchain, full replication scheme yields $\gamma_{\text{full}} = 1$. Since every node verifies all the K blocks, the throughput of the full replication scheme is $\lambda_{\text{full}} = \frac{K}{Nc(f^t) / (Nc(f^t))} = 1$. Thus the full replication scheme does not scale with the network size, as both the storage and the throughput remain constant as N increases. The advantage is that the simple majority-rule will allow the correct verification and update of every block as long as there are less than $N/2$ malicious nodes. Thus, $\beta_{\text{full}} = N/2$.

Uncoded sharding scheme. In conventional *sharding*, the blockchain consists of K disjoint sub-chains known as shards. The N nodes are partitioned into K groups of equal size $q = N/K$, and each group of nodes manage a single shard;

this is a full replication system with $K' = 1$ shard and $N' = q$ nodes. Since each node stores and verifies a single shard, the storage efficiency and throughput become $\gamma_{\text{sharding}} = K$ and $\lambda_{\text{sharding}} = \frac{K}{Nc(f^t) / (Nc(f^t))} = K$, respectively. For these two metrics to scale linearly with N , it must be true that $K = \Theta(N)$. Consequently, the group size q becomes a constant. Hence, compromising as few as $q/2$ nodes will corrupt one shard and the chain. Thus, this scheme only has a constant security of $\beta_{\text{sharding}} = q/2 = O(1)$. Although system solutions such as shard rotations can help achieve linearly scaling security guarantees, they are only secure when the adversary is non-adaptive (or very slowly adaptive). When the adversary is dynamic, it can corrupt all nodes belonging to a particular shard instantaneously after the shard assignment has been made. Under this model, the security reduces to a constant.

In summary, neither full replication nor the above sharding scheme exempts from the blockchain trilemma, and has to make tradeoff in scaling towards the information-theoretic limits. Motivated by the recent advances on leveraging coding theory to optimize the performance of distributed computation (see, i.e., [11]–[13], [15], [16], [18], [19]), we propose **PolyShard** (polynomially coded sharding) to achieve all of the three upper bounds simultaneously. Using **PolyShard**, each node stores coded data of the blockchain, and computes verification functions directly on the coded data.

IV. POLYSHARD FOR BALANCE CHECKING

We consider a simple cryptocurrency blockchain system that records balance transfers between accounts. We assume that there are M accounts (or addresses) associated with each shard, for some constant M that does not scale with t . For the purpose of balance checking, we can compactly represent the block of transactions submitted to shard k at epoch t , $X_k(t)$, as a pair of real vectors $X_k(t) = (X_k^{\text{send}}(t), X_k^{\text{receive}}(t)) \in \mathbb{R}^M \times \mathbb{R}^M$. Given a transaction in the block that reads “Account p sends s units to account q ”, we will have $X_k^{\text{send}}(t)[p] = -s$, and $X_k^{\text{receive}}(t)[q] = s$. Accounts that do no send/receive funds will have their entries in the send/receive vectors set to zeros. To verify $X_k(t)$, we need to check that all the sender accounts in $X_k(t)$ have accumulated enough unspent funds from previous transactions. This naturally leads to the following verification function.

$$f^t(X_k(t), Y_k^{t-1}) = X_k^{\text{send}}(t) + \sum_{i=1}^{t-1} (Y_k^{\text{send}}(i) + Y_k^{\text{receive}}(i)). \quad (4)$$

This function is linear in its input, and has computational complexity $c(f^t) = O(t)$. We claim the block $X_k(t)$ valid (i.e., $e_k^t = 1$) if no entry in the function’s output vector is negative, and invalid (i.e., $e_k^t = 0$) otherwise. After computation, we have the verified block $Y_k(t) = (Y_k^{\text{send}}(t), Y_k^{\text{receive}}(t)) = e_k^t X_k(t)$. We note that this balance checking can be alternatively implemented by having each shard simply store a dimension- M vector that records the aggregated balances of all associated accounts, and the storage and the verification complexity will stay constant as time progresses. However,

important transaction statistics including how many transactions occur in each block, and the input/output values in each transaction, and how these statistics evolve over time will be lost in this simplified implementation. Moreover, storing a single block in each shard without the protection of a long chain makes the shard more vulnerable to malicious tampering, compromising the security guarantee. Therefore, we stick to the chain structure where all past transactions are kept in the ledger.

We consider operating this sharded payment blockchain over a network of N nodes, with a maximum μ fraction of which are corrupted by quickly-adaptive adversaries. For this system, we propose a coded transaction verification scheme, named PolyShard, which simultaneously scales the storage efficiency, security, and throughput with the network size.

A. Coded sub-chain

In PolyShard, at epoch t , each node i stores a coded sub-chain $\tilde{Y}_i^t = (\tilde{Y}_i(1), \dots, \tilde{Y}_i(t))$ where each component $\tilde{Y}_i(m)$ is a coded block generated by the verified blocks $Y_1(m), \dots, Y_K(m)$ from all K shards in epoch m . The coding is through evaluation of the well-known Lagrange interpolation polynomial. Specifically, we pick K arbitrarily distinct real numbers $\omega_1, \dots, \omega_K \in \mathbb{R}$, each corresponding to a shard k . Then for each $m = 1, \dots, t$, we create a Lagrange polynomial in variable z as follows.

$$u_m(z) = \sum_{k=1}^K Y_k(m) \prod_{j \neq k} \frac{z - \omega_j}{\omega_k - \omega_j}. \quad (5)$$

We note that this polynomial is designed such that $u_m(\omega_k) = Y_k(m)$ for all $k = 1, \dots, K$.

Next, as shown in Figure 6, we pick N arbitrarily distinct numbers $\alpha_1, \dots, \alpha_N \in \mathbb{R}$, one for each node. For each $i = 1, \dots, N$, we create a coded block $\tilde{Y}_i(m)$ that is stored at node i , by evaluating the above $u_m(z)$ at the point α_i . That is,

$$\tilde{Y}_i(m) = u_m(\alpha_i) = \sum_{k=1}^K Y_k(m) \prod_{j \neq k} \frac{\alpha_i - \omega_j}{\omega_k - \omega_j} = \sum_{k=1}^K \ell_{ik} Y_k(m). \quad (6)$$

We note that $\tilde{Y}_i(m)$ is a linear combination of the uncoded blocks $Y_1(m), \dots, Y_K(m)$, and the coefficients $\ell_{ik} = \prod_{j \neq k} \frac{\alpha_i - \omega_j}{\omega_k - \omega_j}$ do not depend on the time index m . Therefore, one can think of each node i as having a fixed vector ℓ_{ik} by which it mixes the different shards to create \tilde{Y}_i^t , and stores it locally. The size of each coded sub-chain is K times smaller than the size of the entire blockchain, and the storage efficiency of PolyShard is $\gamma_{\text{PolyShard}} = K$.

Remark 1. The above data encoding is oblivious of the verification function, i.e., the coefficients ℓ_{ik} are independent of f^t . Therefore, the block encoding of PolyShard can be carried out independent of the verification, and the same coded sub-chain can be simultaneously used for all other types of verification items, which could include verifying digital signatures and checking smart contracts.

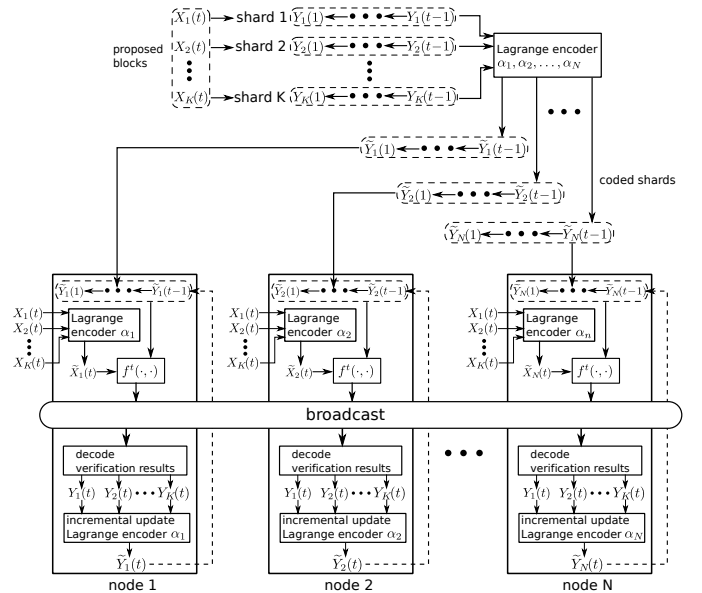


Fig. 6: Illustration of PolyShard scheme.

B. Coded verification

At epoch t , each shard k proposes and broadcasts a new block $X_k(t)$ to be added to the sub-chain after balance checking. PolyShard scheme verifies these blocks in three steps.

Step 1: block encoding. Upon receiving the K proposed blocks, each node i computes a coded block $\tilde{X}_i(t)$ as a linear combination using the same set of coefficients in (6). That is, $\tilde{X}_i(t) = (\tilde{X}_i^{\text{send}}(t), \tilde{X}_i^{\text{receive}}(t)) = \sum_{k=1}^K \ell_{ik} X_k(t)$. We note that this encoding operation can also be viewed as evaluating the polynomial $v_t(z) = \sum_{k=1}^K X_k(t) \prod_{j \neq k} \frac{z - \omega_j}{\omega_k - \omega_j}$ at the point α_i . This step incurs $O(NK)$ operations across the network, since each of the N nodes computes a linear combination of K blocks.

Step 2: coded computation. Each node i applies the verification function f^t in (4) directly to the coded block $\tilde{X}_i(t)$, and its locally stored coded sub-chain \tilde{Y}_i^{t-1} to compute an intermediate vector

$$g_i^t = \tilde{X}_i^{\text{send}}(t) + \sum_{m=1}^{t-1} (\tilde{Y}_i^{\text{send}}(m) + \tilde{Y}_i^{\text{receive}}(m)). \quad (7)$$

Each node i carries out $\Theta(t)$ operations to compute g_i^t , and broadcasts it to all other nodes.

Step 3: decoding. It is easy to see that $f^t(v_t(z), u_1(z), \dots, u_{t-1}(z))$ is a univariate polynomial of degree $K - 1$, and g_i^t can be viewed as evaluating this polynomial at α_i . Given the evaluations at N distinct points g_1^t, \dots, g_N^t , each node can recover the coefficients of $f^t(v_t(z), u_1(z), \dots, u_{t-1}(z))$ following the process of decoding a Reed-Solomon code with dimension K and length N (see, e.g., [37]). In order for this decoding to be robust to μN erroneous results (i.e., achieving security $\beta_{\text{PolyShard}} = \mu N$), we must have $2\mu N \leq N - K$. In other words, a node can successfully decode $f^t(v_t(z), u_1(z), \dots, u_{t-1}(z))$ only if the number of shards K is upper bounded by $K \leq (1 - 2\mu)N$. Based on this

constraint, we set the number of shards of the PolyShard scheme, $K_{\text{PolyShard}} = \lfloor (1 - 2\mu)N \rfloor$, which scales linearly with network size N .

The complexity of decoding a length- N Reed-Solomon code at each node is $O(N \log^2 N \log \log N)$, and the total complexity of the decoding step is $O(N^2 \log^2 N \log \log N)$.

Having decoded $f^t(v_i(z), u_1(z), \dots, u_{t-1}(z))$, each node evaluates it at $\omega_1, \dots, \omega_K$ to recover $\{f^t(X_k(t), Y_k^{t-1})\}_{k=1}^K$, to obtain the verification results $\{e_k^t\}_{k=1}^K$ and the verified blocks $\{Y_k(t) = e_k^t X_k(t)\}_{k=1}^K$. Finally, each node i computes $\tilde{Y}_i(t)$ following (6), and appends it to its local coded sub-chain. Updating the sub-chains has the same computational complexity with the block encoding step, which is $O(NK)$.

Remark 2. The sub-chain update process in PolyShard is incremental, i.e., appending a coded block to a coded sub-chain is equivalent to appending uncoded blocks to the uncoded sub-chains, and then encoding from the updated sub-chains. This commutativity between sub-chain growth and shard encoding allows each node to update its local sub-chain incrementally by accessing only the newly verified blocks instead of the entire block history.

C. Performance of PolyShard

So far, we have shown that PolyShard achieves a storage efficiency $\gamma_{\text{PolyShard}} = K_{\text{PolyShard}} = \Theta(N)$, and it is also robust against $\mu N = \Theta(N)$ quickly-adaptive adversaries. The total number of operations during the verification and the sub-chain update processes is $O(NK) + N\Theta(t) + O(N^2 \log^2 N \log \log N)$, where the term $O(NK) + O(N^2 \log^2 N \log \log N)$ is the additional coding overhead compared with the uncoded sharding scheme. Since $K_{\text{PolyShard}} \leq N$, the coding overhead reduces to $O(N^2 \log^2 N \log \log N)$. The throughput of PolyShard for balance checking is computed as

$$\lambda_{\text{PolyShard}} = \liminf_{t \rightarrow \infty} \frac{K_{\text{PolyShard}} N \Theta(t)}{N \Theta(t) + O(N^2 \log^2 N \log \log N)} \quad (8)$$

$$= \liminf_{t \rightarrow \infty} \frac{K_{\text{PolyShard}}}{1 + \frac{O(N \log^2 N \log \log N)}{\Theta(t)}} = \Theta(N). \quad (9)$$

We can see that since the complexities of the encoding and decoding operations of PolyShard do not scale with t , the coding overhead becomes irrelevant as the chain grows. The PolyShard scheme simultaneously achieves information-theoretically optimal scaling on security, storage efficiency, and throughput.

We note that when the verification function is linear with the block data, codes designed for distributed storage (see, e.g., [38], [39]) can be used to achieve similar scaling as PolyShard. However, PolyShard is designed for a much more general class of verification functions including arbitrary multivariate polynomials, which cannot be handled by state-of-the-art storage codes.

V. POLYSHARD FOR GENERAL VERIFICATION FUNCTIONS

In this section, we describe the PolyShard scheme for a more general class of verification functions f^t that can be represented as a multivariate polynomial with maximum degree

of d . Cryptographic hash functions, which are extensively used in computing account addresses, validating transaction Merkle trees, and verifying digital signatures, are often evaluated as polynomials of its input data. For example, the Z  mor-Tillich hash function is computed by multiplying 2×2 matrices in a finite field of characteristic 2, whose degree is proportional to the number of input bits [40]. On the other hand, for hash functions that are based on bit mixing, and often lack algebraic structures (e.g., SHA-2, and Keccak [41]), we can represent the corresponding Boolean verification functions (indicating whether the block is valid or not) as polynomials using the following result [42]: any Boolean function $\{0, 1\}^n \rightarrow \{0, 1\}$ can be represented by a polynomial of degree $\leq n$ with at most 2^{n-1} terms. The explicit construction of this polynomial is described in Appendix A.

As one of the main advantages of PolyShard, the system design is almost independent of the verification functions, and the PolyShard scheme for high-degree ($d \geq 1$) polynomials is almost identical to that of balance checking. In particular, at epoch t , the latest block stored at node i , i.e., $\tilde{Y}_i(t-1)$, is generated as in (6). In contrast to the case of balance checking that operates over real numbers, when the underlying field \mathbb{F} is finite, we will need the field size $|\mathbb{F}|$ to be at least N for this block encoding to be viable. For small field (e.g., binary field), we can overcome this issue by using field extension and applying PolyShard on the extended field (see details in Appendix A).

The block verification process is similar to that of the balance checking example. Having created the coded block $\tilde{X}_i(t)$, node i directly applies the verification function to compute $g_i^t = f^t(\tilde{X}_i(t), \tilde{Y}_i^{t-1})$, and broadcasts it to all other nodes. Since f^t is a polynomial of degree d , $f^t(v_t(z), u_1(z), \dots, u_{t-1}(z))$ becomes a polynomial of degree $(K-1)d$. Now to decode $f^t(v_t(z), u_1(z), \dots, u_{t-1}(z))$ from g_1^t, \dots, g_N^t , each node needs to decode a Reed-Solomon code with dimension $(K-1)d+1$ and length N . Successful decoding would require the number of errors $\mu N \leq (N - (K-1)d - 1)/2$. That is, the maximum number of shards K that can be securely supported is $K_{\text{PolyShard}} = \lfloor \frac{(1-2\mu)N-1}{d} \rfloor + 1$.

While it is fairly clear that PolyShard achieves storage efficiency $\gamma_{\text{PolyShard}} = K_{\text{PolyShard}} = \Theta(N)$ and security $\beta_{\text{PolyShard}} = \mu N = \Theta(N)$ for a degree- d verification function, the throughput of PolyShard is

$$\lambda_{\text{PolyShard}} = \liminf_{t \rightarrow \infty} \frac{K_{\text{PolyShard}}}{1 + \frac{O(N \log^2 N \log \log N)}{c(f^t)}}. \quad (10)$$

When $c(f^t)$ grows with t , (e.g., $c(f^t) = \Theta(t)$ for the above balance checking function that scans the entire sub-chain to find sufficient funds), the throughput of PolyShard becomes $\lambda_{\text{PolyShard}} = K_{\text{PolyShard}} = \Theta(N)$. We summarize the scaling results of the PolyShard scheme in the following theorem.

Theorem 1. Consider a sharded blockchain whose blocks in each shard are verified by computing a multivariate polynomial of degree d on the blocks in that shard. When implementing this blockchain over N network nodes, up to μ (for some constant $0 \leq \mu < \frac{1}{2}$) fraction of which may be corrupted by quickly-adaptive adversaries, the proposed

PolyShard scheme supports secure block verification from up to $K_{\text{PolyShard}} = \lfloor \frac{(1-2\mu)N-1}{d} + 1 \rfloor = \Theta(N)$ shards, and simultaneously achieves the following performance metrics,

$$\begin{aligned} \text{Storage efficiency} \quad \gamma_{\text{PolyShard}} &= K_{\text{PolyShard}} = \Theta(N), \\ \text{Security} \quad \beta_{\text{PolyShard}} &= \mu N = \Theta(N), \\ \text{Throughput} \quad \lambda_{\text{PolyShard}} &= K_{\text{PolyShard}} = \Theta(N), \end{aligned}$$

when computational complexity of the verification function grows with the length of the sub-chain in each shard. Therefore, PolyShard simultaneously achieves the information-theoretically optimal storage efficiency, security, and throughput to within constant multiplicative gaps.

The number of shards supported by PolyShard decreases as degree of polynomial increases. One can remove such limitation by using PolyShard iteratively. The main idea of iterative PolyShard is to represent the verification function as a low-depth arithmetic circuit which can be implemented iteratively by computing low-degree polynomials, and then apply PolyShard to the low-degree polynomial iteratively. We show that the number of supported shards can be independent of the degree of function by the following theorem. (see details in Appendix B).

Theorem 2. *Consider a sharded blockchain whose blocks in each shard are verified by computing a multivariate polynomial of degree d on the blocks in that shard. When implementing this blockchain over N network nodes, up to μ (for some constant $0 \leq \mu < \frac{1}{2}$) fraction of which may be corrupted by quickly-adaptive adversaries, the proposed iterative PolyShard scheme supports secure block verification from up to $K_{\text{Iterative}} = \lfloor \frac{(1-2\mu)N+1}{2} \rfloor$.*

Remark 3. The shard encoding and computation decoding schemes of PolyShard are developed based on the coded computation techniques proposed in [19], which are used for distributed computing multivariate polynomials subject to arbitrary computation errors. Specifically, it is proposed in [19] to create coded data batches using Lagrange polynomial interpolation, and perform computations directly on coded data. However, in contrast to the scenario of one-shot computation on static data in [19], the locally stored data at each node is growing in a blockchain system, as more verified blocks are appended to the chain. The requirement of dynamically updating the local coded sub-chain that is compatible with the upcoming coded verification poses new challenges on the design of the PolyShard scheme. Utilizing the data structure of the blockchain, and the algebraic properties of the encoding strategy, we propose a simple *incremental* sub-chain update policy for PolyShard that requires accessing the minimum amount of data.

Remark 4. The additional coding overhead, including the operations required to encode the incoming blocks, decode verification results, and update the coded shards, does not scale with the length of the sub-chain t . When the complexity of computing f^t , i.e., $c(f^t)$, grows with t , the coding overhead becomes negligible as the chain grows, and the throughput of PolyShard scales linearly with the network size. However,

on the other hand, when $c(f^t)$ is independent of chain length (e.g., verifying digital signature that only requires data from the current block), the coding overhead will dominate the local computation. In this case, while PolyShard still achieves scalability on storage and security, its throughput remains constant as the network grows.

VI. SIMULATION RESULTS

We perform detailed simulations to assess the performance of PolyShard for balance checking described in Section IV. The blockchain system keeps records of all the balance transfers between accounts, and verifies new blocks by comparing them with the sum of the previously verified blocks (i.e., computing the verification function in (4)). More specifically, the system contains K shards, each managing M accounts. At each time epoch t , each shard k proposes a block of transactions for verification. On a single computer, we simulate this blockchain system over N network nodes, using full replication, uncoded sharding, and PolyShard schemes respectively. During the simulation, we execute a serial program that performs the local computations of the nodes one after another, and measure each of these computation times in serial. All node instances share the same memory, so the communication delay between nodes is negligible.

We compute the throughput of each scheme under different values of N and t to understand its scalability. Throughput is defined as the number of blocks verified per time unit, and is computed by dividing K (the number of blocks proposed per epoch) by the average computation time (measured during simulation) of the N nodes. For PolyShard, the computation time also includes the time each node spends on encoding the blocks. However, since the encoding time is a constant, whilst the balance summation time increases with t as the chain becomes longer, it is expected that the encoding time is becoming negligible. We note that the storage efficiency and security level of each scheme are decided by system parameters and, thus, do not need measurements.

We simulate this system for $t = 1000$ epochs, using different number of shards $K \in [5, 50]$. Each shard manages $M = 2000$ accounts. We fix the ratio $N/K = 3$. Thus, the number of nodes is $N \in [15, 150]$. We plot the complete relationship between N , t , and throughput of the three schemes in Figure 7. For a closer look, We plot the relationship between the sub-chain length t and throughput when $N = 150$ in Figure 8, and the relationship between the network size N and throughput when $t = 1000$ in Figure 4 in Section I.

Results and discussions

1) **Throughput:** As expected, PolyShard provides the same throughput as uncoded sharding, which is about K times of the throughput of full replication. From Figure 8, we observe that the throughput of all three schemes drops as the time progresses. This is because that the computational complexity of verifying a block increases as more blocks are appended to each shard. In terms of scalability, Fig. 4 indicates that the throughput of PolyShard and uncoded sharding both increases linearly with the network size N (and K), whilst the throughput of full replication almost stays the same.

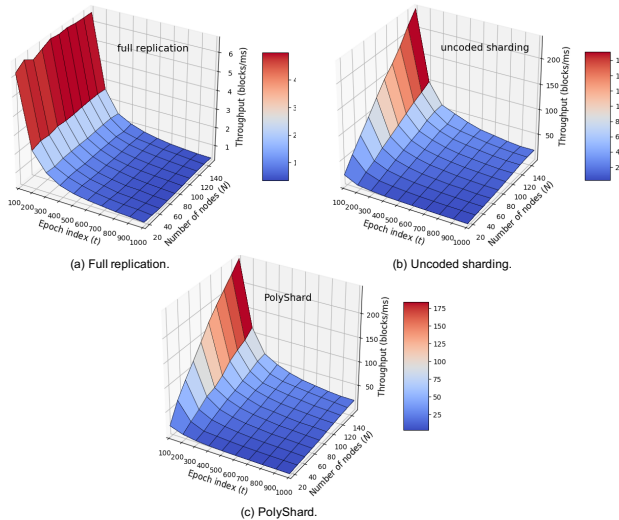


Fig. 7: Throughput of the three schemes with respect to time and number of nodes.

- 2) Storage: It is straightforward to see that PolyShard provides the same storage gain over full replication as uncoded sharding, with a factor of K . Thus, PolyShard and uncoded sharding are scalable in storage, but full replication is not (Table IIa).
- 3) Security: As we have analyzed, full replication can tolerate up to 50% of malicious nodes, achieving the maximum security level $\beta_{\text{full}} = \frac{N}{2}$. The error-correcting process of PolyShard provides robustness to $\beta_{\text{PolyShard}} = \frac{N-K}{2} = \frac{N-N/3}{2} = \frac{N}{3}$ malicious nodes. In contrast, under uncoded sharding, each shard is only managed by 3 nodes. Thus, its security level is only 1 regardless of N , which is not scalable (Table IIb).

N	15	30	60	90	120	150
γ_{full}	1	1	1	1	1	1
γ_{sharding}	5	10	20	30	40	50
$\gamma_{\text{PolyShard}}$	5	10	20	30	40	50

(a) Storage efficiency.

N	15	30	60	90	120	150
β_{full}	7	15	30	45	60	75
β_{sharding}	1	1	1	1	1	1
$\beta_{\text{PolyShard}}$	5	10	20	30	40	50

(b) Security.

TABLE II: Storage efficiency and security of the three schemes under different network size N .

In summary, PolyShard outperforms both full replication and uncoded sharding because it is the only scheme that can simultaneously 1) alleviate the storage load at each node; and 2) boost the verification throughput by scaling out the system, and 3) without sacrificing the safety requirement even when the number of adversaries also grows with network size.

VII. DISCUSSION

In this section, we discuss how PolyShard fits into the overall architecture of a contemporary blockchain system.

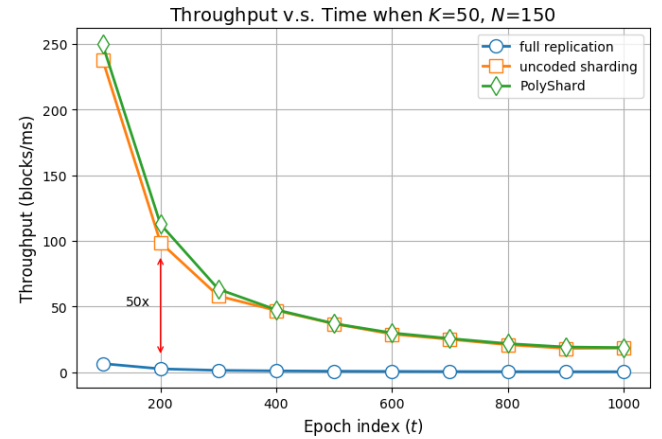


Fig. 8: Throughput of the three schemes when number of nodes $N = 150$.

Integration into blockchain systems. We note that PolyShard has so far been described in a simple setting where each shard produces one block in lock-step. We highlight one instantiation of how PolyShard could fit into the architecture of an existing blockchain system, which combines a standard sharding method for proposal followed by PolyShard for finalization. The K shards are obtained by assigning users to shards via a user-assignment algorithm. The N nodes are partitioned into K shards using a standard sharding system (see [9]). Inside of the shard, the nodes run a standard blockchain along with a finalization algorithm to get a *locally finalized* version of the block.

Each node is also assigned a coded shard via a coded-shard-assignment algorithm, which assigns a random field element $\alpha_i \in \mathbb{F}$ to a node so that the node can compute which linear combination it will use for coding. We point out here that in a permissionless setting, it is easy to handle churn (users joining and leaving) by this method if the size of the finite field \mathbb{F} is much larger than N - since at this point, the probability of collision (two users getting assigned the same field element) becomes negligible. Thus each node plays a role in both an uncoded shard as well as a coded shard, thus its storage requirement will be doubled; however, our system still has storage efficiency scaling with N . The PolyShard algorithm now gets the locally finalized blocks from the different shards at regular intervals and it acts as a global finalization step performing coded validation at the level of the locally finalized blocks. We point out that users requiring high trust should wait for this global finalization stamp before confirming a payment, whereas users requiring short latency can immediately utilize the local-finalization for confirmation.

Beyond the aforementioned issues, there may be cross-shard transactions present in the system, which are payments or smart contracts with inputs and outputs distributed across multiple shards. In such a case, we will use a locking-based method, which locks the payment at the source shard and produces a certificate to the destination shard so that the amount can be spent; this idea has been proposed as well as implemented in *Elastico* [8] and *Omniledger* [9].

Relationship to verifiable computing. An alternative

paradigm for accelerating computing in blockchain is verifiable computing [43]–[47], where a single node executes a set of computations (for example, payment validation) and integrity of these computations are then cryptographically certified. A major difference between our framework and verifiable computing is that our scheme is *information-theoretically secure* against a computationally unbounded adversary as against the computational security offered by verifiable computing schemes. However, verifiable computing schemes can provide zero-knowledge proofs, whereas our scheme does not offer zero-knowledge capability. Finally, verifiable computing is relevant in an asymmetric setting, where one computer is much more powerful than the others, unlike PolyShard that is designed for a symmetric setup comprising of equally powerful and decentralized nodes.

REFERENCES

- [1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.
- [2] A. Bahga and V. K. Madiseti, "Blockchain platform for industrial internet of things," *Journal of Software Engineering and Applications*, vol. 9, no. 10, p. 533, 2016.
- [3] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in *IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom)*, pp. 1–3, IEEE, 2016.
- [4] K. Croman, C. Decker, I. Eyal, A. E. Gencer, A. Juels, A. Kosba, A. Miller, P. Saxena, E. Shi, E. G. Sirer, et al., "On scaling decentralized blockchains," in *International Conference on Financial Cryptography and Data Security*, pp. 106–125, Springer, 2016.
- [5] T. Ometoruwa, "Solving the blockchain trilemma: Decentralization, security & scalability," <https://www.coinbureau.com/analysis/solving-blockchain-trilemma/>, 2018. Accessed: 2018-12-21.
- [6] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum project yellow paper*, vol. 151, pp. 1–32, 2014.
- [7] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun, "On the security and performance of proof of work blockchains," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pp. 3–16, ACM, 2016.
- [8] L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, and P. Saxena, "A secure sharding protocol for open blockchains," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pp. 17–30, ACM, 2016.
- [9] E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, and B. Ford, "Omiledger: A secure, scale-out, decentralized ledger," *IACR Cryptology ePrint Archive*, vol. 2017, p. 406, 2017.
- [10] A. E. Gencer, R. van Renesse, and E. G. Sirer, "Short paper: Service-oriented sharding for blockchains," in *International Conference on Financial Cryptography and Data Security*, pp. 393–401, Springer, 2017.
- [11] S. Li, M. A. Maddah-Ali, and A. S. Avestimehr, "Coded MapReduce," *53rd Allerton Conference*, Sept. 2015.
- [12] S. Li, M. A. Maddah-Ali, Q. Yu, and A. S. Avestimehr, "A fundamental tradeoff between computation and communication in distributed computing," *IEEE Transactions on Information Theory*, vol. 64, Jan. 2018.
- [13] K. Lee, M. Lam, R. Pedarsani, D. Papailiopoulos, and K. Ramchandran, "Speeding up distributed machine learning using codes," *IEEE Transactions on Information Theory*, vol. 64, no. 3, pp. 1514–1529, 2018.
- [14] S. Li, M. A. Maddah-Ali, and A. S. Avestimehr, "A unified coding framework for distributed computing with straggling servers," *IEEE Workshop on Network Coding and Applications*, Sept. 2016.
- [15] S. Dutta, V. Cadambe, and P. Grover, "Short-dot: Computing large linear transforms distributedly using coded short dot products," in *NIPS*, pp. 2100–2108, 2016.
- [16] Q. Yu, M. A. Maddah-Ali, and A. S. Avestimehr, "Polynomial codes: an optimal design for high-dimensional coded matrix multiplication," in *NIPS*, pp. 4406–4416, 2017.
- [17] C. Karakus, Y. Sun, S. Diggavi, and W. Yin, "Straggler mitigation in distributed optimization through data encoding," in *NIPS*, pp. 5440–5448, 2017.
- [18] R. Tandon, Q. Lei, A. G. Dimakis, and N. Karampatziakis, "Gradient coding: Avoiding stragglers in distributed learning," in *Proceedings of the 34th International Conference on Machine Learning*, pp. 3368–3376, Aug. 2017.
- [19] Q. Yu, S. Li, N. Raviv, S. M. M. Kalan, M. Soltanolkotabi, and A. S. Avestimehr, "Lagrange coded computing: Optimal design for resiliency, security, and privacy," in *NIPS Systems for ML Workshop*, 2018.
- [20] Y. Gao and H. Nobuhara, "A proof of stake sharding protocol for scalable blockchains," *Proceedings of the Asia-Pacific Advanced Network*, vol. 44, pp. 13–16, 2017.
- [21] M. Zamani, M. Movahedi, and M. Raykova, "Rapidchain: A fast blockchain protocol via full sharding," *Cryptology ePrint Archive*, 2018. <https://eprint.iacr.org/2018/460.pdf>.
- [22] S. Bano, M. Al-Bassam, and G. Danezis, "The road to scalable blockchain designs," *USENIX; login: magazine*, 2017.
- [23] Z. Ren and Z. Erkin, "A scale-out blockchain for value transfer with spontaneous sharding," *e-print arXiv:1801.02531*, 2018.
- [24] H. Yoo, J. Yim, and S. Kim, "The blockchain for domain based static sharding," in *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (Trust-Com/BigDataSE)*, pp. 1689–1692, IEEE, 2018.
- [25] S. Cai, N. Yang, and Z. Ming, "A decentralized sharding service network framework with scalability," in *International Conference on Web Services*, pp. 151–165, Springer, 2018.
- [26] A. Chauhan, O. P. Malviya, M. Verma, and T. S. Mor, "Blockchain and scalability," in *2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, pp. 122–128, IEEE, 2018.
- [27] M. H. Manshaei, M. Jadliwala, A. Maiti, and M. Fooladgar, "A game-theoretic analysis of shard-based permissionless blockchains," *e-print arXiv:1809.07307*, 2018.
- [28] "Ethereum sharding FAQs," <https://github.com/ethereum/wiki/wiki/Sharding-FAQs>.
- [29] A. E. Gencer, R. van Renesse, and E. G. Sirer, "Service-oriented sharding with aspen," *e-print arXiv:1611.06816*, 2016.
- [30] M. Al-Bassam, A. Sonnino, S. Bano, D. Hryczyszyn, and G. Danezis, "Chainspace: A sharded smart contracts platform," *e-print arXiv:1708.03778*, 2017.
- [31] S. Forestier, "Blockclique: scaling blockchains through transaction sharding in a multithreaded block graph," *e-print arXiv:1803.09029*, 2018.
- [32] M. Yu, S. Sahraei, S. Li, S. Avestimehr, S. Kannan, and P. Viswanath, "Coded merkle tree: Solving data availability attacks in blockchains," *arXiv preprint arXiv:1910.01247*, 2019.
- [33] S. Sahraei and A. S. Avestimehr, "Interpol: Information theoretically verifiable polynomial evaluation," in *2019 IEEE International Symposium on Information Theory (ISIT)*, pp. 1112–1116, IEEE, 2019.
- [34] S. Kadhe, J. Chung, and K. Ramchandran, "Sef: A secure fountain architecture for slashing storage costs in blockchains," *arXiv preprint arXiv:1906.12140*, 2019.
- [35] S. Sahraei, M. A. Maddah-Ali, and S. Avestimehr, "Interactive verifiable polynomial evaluation," *arXiv preprint arXiv:1907.04302*, 2019.
- [36] D. Mitra and L. Dolecek, "Patterned erasure correcting codes for low storage-overhead blockchain systems," in *2019 53rd Asilomar Conference on Signals, Systems, and Computers*, pp. 1734–1738, IEEE, 2019.
- [37] R. Roth, *Introduction to coding theory*. Cambridge University Press, 2006.
- [38] A. G. Dimakis, K. Ramchandran, Y. Wu, and C. Suh, "A survey on network codes for distributed storage," *Proceedings of the IEEE*, vol. 99, no. 3, pp. 476–489, 2011.
- [39] K. V. Rashmi, N. B. Shah, and P. V. Kumar, "Optimal exact-regenerating codes for distributed storage at the msr and mbr points via a product-matrix construction," *IEEE Transactions on Information Theory*, vol. 57, no. 8, pp. 5227–5239, 2011.
- [40] J.-P. Tillich and G. Zémor, "Hashing with sl_2 ," in *Annual International Cryptology Conference*, pp. 40–49, Springer, 1994.
- [41] G. Bertoni, J. Daemen, M. Peeters, G. Van Assche, and R. Van Keer, "Keccak specifications summary," https://keccak.team/keccak_specs_summary.html. Accessed: 2018-12-21.
- [42] Y. M. Zou, "Representing boolean functions using polynomials: more can offer less," in *International Symposium on Neural Networks*, pp. 290–296, Springer, 2011.
- [43] R. Gennaro, C. Gentry, and B. Parno, "Non-interactive verifiable computing: Outsourcing computation to untrusted workers," in *Annual Cryptology Conference*, pp. 465–482, Springer, 2010.
- [44] N. Bitansky, R. Canetti, A. Chiesa, and E. Tromer, "From extractable collision resistance to succinct non-interactive arguments of knowledge, and back again," in *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference*, pp. 326–349, ACM, 2012.

- [45] B. Parno, J. Howell, C. Gentry, and M. Raykova, “Pinocchio: Nearly practical verifiable computation,” *Communications of the ACM*, vol. 59, no. 2, pp. 103–112, 2016.
- [46] E. Ben-Sasson, A. Chiesa, E. Tromer, and M. Virza, “Succinct non-interactive zero knowledge for a von neumann architecture,” in *USENIX Security Symposium*, pp. 781–796, 2014.
- [47] E. Ben-Sasson, I. Bentov, Y. Horesh, and M. Riabzev, “Scalable, transparent, and post-quantum secure computational integrity,” *Cryptol. ePrint Arch., Tech. Rep.*, vol. 46, p. 2018, 2018.

APPENDIX A

FIELD EXTENSION FOR GENERAL BOOLEAN FUNCTIONS

For general blockchain systems that verify incoming blocks based on the most recent $0 \leq P \leq t-1$ verified blocks, we can generally model each incoming block $X_k(t)$, and each verified block $Y_k(m)$ as a binary bit stream of length T , and the verification function $f^t : \{0,1\}^{T(P+1)} \rightarrow \{0,1\}$ as a Boolean function that indicates whether $X_k(t)$ is valid or not.

Using the construction of [42, Theorem 2], we can represent any arbitrary Boolean function $f : \{0,1\}^n \rightarrow \{0,1\}$ whose inputs are n binary variables as a multivariate polynomial p of degree n as follows. For each vector $\mathbf{a} = (a_1, \dots, a_n) \in \{0,1\}^n$, we define $h_{\mathbf{a}} = z_1 z_2 \dots z_n$, where $z_i = x_i$ if $a_i = 1$, and $z_i = y_i$ if $a_i = 0$. Next, we partition $\{0,1\}^n$ into two disjoint subsets S_0 and S_1 as follows.

$$S_0 = \{\mathbf{a} \in \{0,1\}^n : f(\mathbf{a}) = 0\}, \quad (11)$$

$$S_1 = \{\mathbf{a} \in \{0,1\}^n : f(\mathbf{a}) = 1\}. \quad (12)$$

The polynomial p is then constructed as

$$\begin{aligned} f(x_1, \dots, x_n) &= p(x_1, \dots, x_n, y_1, \dots, y_n) \\ &= \sum_{\mathbf{a} \in S_1} h_{\mathbf{a}} = 1 + \sum_{\mathbf{a} \in S_0} h_{\mathbf{a}}, \end{aligned} \quad (13)$$

where $y_i = x_i + 1$.

We note that this model applies to verifying the digital signatures, where the verification does not depend on past blocks, i.e., $P = 0$. Utilizing the above technique, we can transfer any non-polynomial computations like inversions and cryptographic hash functions (e.g., SHA-2) into polynomial evaluations.

For Boolean verification polynomials over binary field as in (13), the PolyShard data encoding (6) does not directly apply since it requires the underlying field size $|\mathbb{F}|$ to be at least the network size N . To use PolyShard in this case, we can embed each element $y_k[i] \in \{0,1\}$ of a verified block Y_k (time index omitted) into a binary extension field \mathbb{F}_{2^m} with $2^m \geq N$. Specifically, the embedding $\bar{y}_k[i] \in \mathbb{F}_{2^m}$ of the element $y_k[i]$ is generated such that

$$\bar{y}_k[i] = \begin{cases} \underbrace{00 \dots 0}_m, & y_k[i] = 0, \\ \underbrace{00 \dots 0}_m 1, & y_k[i] = 1. \end{cases} \quad (14)$$

Then we can select distinct elements $\alpha_1, \dots, \alpha_N \in \mathbb{F}_{2^m}$ to apply the encoding strategy in (6) on the block elements in the extension field.

Verification over extension field still generates the correct result. To see that, we can easily verify that the value of the verification polynomial p as constructed in (13) is invariant

with the embedding operation in (14). That is, since the polynomial p is the summation of monomials in \mathbb{F}_2 , when we replace each input bit with its embedding, the value of p equals $\underbrace{00 \dots 0}_m$ if the verification result is 0, and equals $\underbrace{00 \dots 0}_m 1$ if the result is 1.

APPENDIX B

ITERATIVE POLYSHARD

In Section V, we show that the number of shards can be supported by PolyShard is up to $K_{\text{PolyShard}} = \lfloor \frac{(1-2\mu)N-1}{d} + 1 \rfloor$, which decreases as the degree of polynomial increases. To remove this limitation, we propose iterative PolyShard which can work with polynomials whose degree is high. The main idea of iterative PolyShard is to represent the verification function as a *low-depth* arithmetic circuit which can be implemented iteratively by computing low-degree polynomials, and then apply the PolyShard scheme to the low-degree polynomial of each iteration.

A. Arithmetic circuit modeling for verification functions

Before applying iterative PolyShard to the verification functions, we model functions to some arithmetic circuits. An arithmetic circuit is a directed acyclic graph that can be used to compute a polynomial of inputs over certain field. Nodes of the graph are referred to as gates. Every node with zero indegree is an *input gate* and is labeled by either a variable or an element of the underlying field. Every other node is either a *addition gate* or a *multiplication gate* labeled by $+$ and \times , respectively. Gate u is a child of gate v if there is a directed edge from v to u in the graph. Each addition (multiplication) gate computes the sum (product) of the polynomials computed by their parent gates. See Figure 9 for an example of an arithmetic circuit that computes the polynomial $f(x_1, x_2) = x_1^2 x_2 + x_1 x_2$. To model verification functions, we consider the class of arithmetic circuits in which each layer satisfies the following conditions:

- 1) Each multiplication gate has two inputs.
- 2) Each addition gate has arbitrary number of inputs.
- 3) Each layer consists of addition gates followed by multiplication gates.
- 4) Edges within each layer are only from addition gates to multiplication gates.
- 5) The outputs of multiplication gates are the inputs of addition gates in the following layer.

Remark 5. For any polynomial with degree d , there exists an arithmetic circuit satisfying the above conditions with $\lceil \log d \rceil + 1$ layers. It implies that the arithmetic circuits of verification function can be low-depth.

For the arithmetic function of verification function f^t , we define the following terms. For each layer $l \in [1 : L]$ (L is the number of layers), we denote the number of multiplication gates by A_l . In layer l , there are A_l intermediate polynomials (outputs of multiplication gates) denoted by $f_{(l,1)}^t, \dots, f_{(l,A_l)}^t$. The inputs of layer l are denoted by $(X_1^l(t), \dots, X_K^l(t))$. For layer 1, we have $X_k^1(t) = \{X_k(t), Y_k^{t-1}\}$. Because of the structure of arithmetic circuits we consider, for each layer $l \in [2 : L]$, we

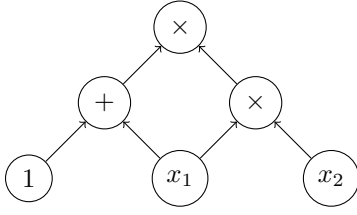


Fig. 9: An arithmetic circuit that computes the polynomial $f = x_1^2 x_2 + x_1 x_2$.

have $X_k^l(t) = \{f_{(l-1,1)}^t(X_k^{l-1}(t)), \dots, f_{(l-1,A_{l-1})}^t(X_k^{l-1}(t))\}$. Then, the outputs of multiplication gates in layer L is the computation of verification function, i.e., $f^t(X_k(t), Y_k^{t-1}) = (f_{(L,1)}^t(X_k^L(t)), \dots, f_{(L,A_L)}^t(X_k^L(t)))$.

Let's illustrate the arithmetic circuits through the following example.

Example. We consider verification function

$$f^t(x_1, \dots, x_5) = (x_2 + x_3) \times (x_3 + x_4) \times (x_1 + x_2 + x_3 + x_4) \times (x_2 + x_3 + x_4 + x_5).$$

An arithmetic circuit satisfying the above conditions that computes f^t is depicted in Figure 10. The arithmetic circuit for function f^t consists two layers. The input of the first layer is $(X_1^1(t), \dots, X_K^1(t))$, where $X_k^1(t) = X_k = (x_{k1}, \dots, x_{k5})$, for each $k \in [1 : K]$. At the end of the first layer, $f_{(1,1)}^t(X_k), f_{(1,2)}^t(X_k), f_{(1,3)}^t(X_k)$ for each $k \in [1 : K]$ are computed. The inputs of layer 2 is $(X_1^2(t), \dots, X_K^2(t))$, where $X_k^2(t) = (f_{(1,1)}^t(X_k), f_{(1,2)}^t(X_k), f_{(1,3)}^t(X_k))$. At the end of the layer 2, $f_{(2,1)}^t(X_k^2(t)) = f_{(2,1)}^t(f_{(1,1)}^t(X_k), f_{(1,2)}^t(X_k), f_{(1,3)}^t(X_k)) = f(X_k)$, for each $k \in [1 : K]$ are computed.

B. Iterative coded verification

The block verification process of iterative PolyShard has L iterations. Each iteration $l \in [1 : L]$ has the following three steps.

Step 1: block encoding. Each node i generates a coded block $\tilde{X}_i^l(t) = v_i^l(\alpha_i)$ where $v_i^l(z) = \sum_{k=1}^K X_k^l(t) \prod_{j \neq k} \frac{z - \omega_j}{\omega_k - \omega_j}$ as a linear combination using the same set of coefficients in (6), i.e., $\tilde{X}_i^l(t) = v_i^l(\alpha_i) = \sum_{k=1}^K \ell_{ik} X_k^l(t)$. This step incurs $O(NK)$ operations across the network, since each of the N nodes computes a linear combination of K blocks.

Step 2: coded computation. Each node i applies intermediate functions $f_{(1,1)}^t, \dots, f_{(1,A_1)}^t$ directly to the coded input $\tilde{X}_i^l(t)$ to compute $g_{(1,i)}^t = (f_{(1,1)}^t(\tilde{X}_i^l(t)), \dots, f_{(1,A_1)}^t(\tilde{X}_i^l(t)))$, and broadcasts it to all other nodes. We note that the total computational complexity of one node incurred in this step is the complexity of computing arithmetic circuit of f^t . We assume that the computational complexity of arithmetic circuit of function $f^t \approx c(f^t)$.

Step 3: decoding. Since each intermediate function $f_{(l,a)}^t$ is a polynomial of degree 2 over the inputs of layer l . To decode $f_{(1,1)}^t, \dots, f_{(1,A_1)}^t$ from $g_{(1,1)}^t, \dots, g_{(1,N)}^t$, each node needs to decode a Reed-Solomon code with dimension $2(K-1)+1$ and length N . To successfully decode the results, it requires the number of errors $\mu N \leq (N - 2(K-1) - 1)/2$. That is, the

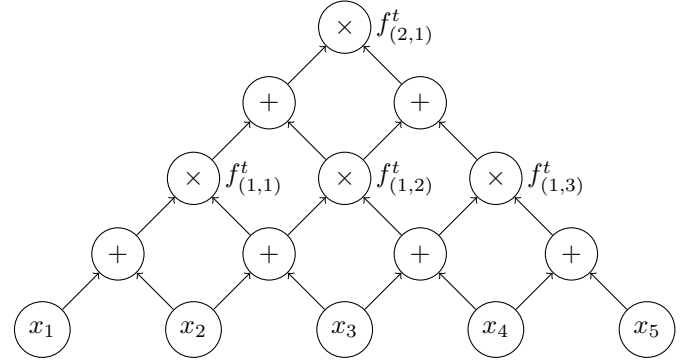


Fig. 10: An arithmetic circuit that computes the verification function $f^t = (x_2 + x_3) \times (x_3 + x_4) \times (x_1 + x_2 + x_3 + x_4) \times (x_2 + x_3 + x_4 + x_5)$.

maximum number of shards K that can be securely supported is $K_{\text{Iterative}} = \lfloor \frac{(1-2\mu)N+1}{2} \rfloor$.

After computation of L iterations, each node evaluates $f_{(L,1)}^t(v_i^L(z)), \dots, f_{(L,A_L)}^t(v_i^L(z))$ at $\omega_1, \dots, \omega_K$ to recover $\{(f_{(L,1)}^t(X_k^L(t)), \dots, f_{(L,A_L)}^t(X_k^L(t)))\}_{k=1}^K = \{f^t(X_k(t), Y_k^{t-1})\}_{k=1}^K$, to obtain the verification results $\{e_k^t\}_{k=1}^K$ and the verified blocks $\{Y_k(t) = e_k^t X_k(t)\}_{k=1}^K$. Finally, each node i computes $\tilde{Y}_i(t)$ following (6), and appends it to its local coded sub-chain which incurs the computational complexity which is $O(NK)$.

C. Performance of iterative PolyShard

As shown in Theorem 2, we have that the maximum number of shards supported by iterative PolyShard is independent of the degree of verification function. Moreover, iterative PolyShard achieves a storage efficiency $\gamma_{\text{Iterative}} = \gamma_{\text{PolyShard}} = \Theta(N)$, and it is also robust against $\mu N = \Theta(N)$ quickly-adaptive adversaries. Then, the total number of operations during the verification and the sub-chain update processes is $O(NK) + Nc(f^t) + O(N^2 \log^2 N \log \log N)$. The coding overhead reduces to $O(N^2 \log^2 N \log \log N)$ since $K_{\text{Iterative}} \leq N$. The throughput of iterative PolyShard is computed as

$$\lambda_{\text{Iterative}} = \liminf_{t \rightarrow \infty} \frac{K_{\text{Iterative}}}{1 + \frac{O(N \log^2 N \log \log N)}{c(f^t)}}. \quad (15)$$

When $c(f^t)$ grows with t , the throughput of iterative PolyShard becomes $\lambda_{\text{Iterative}} = \Theta(N)$, i.e., iterative PolyShard simultaneously achieves the information-theoretically optimal storage efficiency, security, and throughput to within constant multiplicative gaps.

Songze Li is a researcher with the electrical engineering department of Stanford University. Songze received his B.Sc. degree from Tandon School of Engineering at New York University in 2011, and Ph.D. degree from Viterbi School of Engineering at University of Southern California in 2018, both in Electrical Engineering. In 2019, Songze was with Applied Protocol Research working on designing and implementing scalable blockchain systems. Songze's research interests lie on the intersection of theory and system of designing efficient, scalable, and secure distributed computing solutions for machine learning and blockchain. Songze is a Qualcomm Innovation Fellowship finalist in 2017, and received the USC Viterbi School of Engineering Doctoral Fellowship in 2011.

Mingchao Yu obtained his B. E. degree in 2008 from Northwestern Polytechnical University, China. He obtained his M. Phil and Ph.D. degrees in 2011 and 2016, respectively, both from Australian National University, under the supervision of Prof. Parastoo Sadeghi. In 2015, he joined a start-up called IntereferX Communications Pty. Ltd., which was acquired in 2017 with him as the chief engineer. During 2017 and 2018, he was a post-doc research fellow in Viterbi School of Engineering, University of Southern California, under the supervision of Prof. Salman Avestimehr. In 2018, he joined Dolby Laboratory, and is currently a staff engineer in CTO's office, leading the R&D in cloud-based media platform. His areas of interests include information theory, network coding, distributed computing, cryptography, and blockchain.

Chien-Sheng Yang received his the B.S. degree in electrical and computer engineering from National Chiao Tung University (NCTU), Hsinchu, Taiwan in 2015 and is currently pursuing his Ph.D. in Electrical and Computer Engineering from the University of Southern California (USC), Los Angeles. He received the Annenberg Graduate Fellowship in 2016. He was a finalist of the ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc) Best Paper Award in 2019. His interests include task scheduling, information theory and machine learning.

A. Salman Avestimehr is a Professor and director of the Information Theory and Machine Learning (vITAL) research lab at the Electrical and Computer Engineering Department of University of Southern California. He received his Ph.D. in 2008 and M.S. degree in 2005 in Electrical Engineering and Computer Science, both from the University of California, Berkeley. Prior to that, he obtained his B.S. in Electrical Engineering from Sharif University of Technology in 2003. His research interests include information theory, coding theory, and large-scale distributed computing and machine learning.

Dr. Avestimehr has received a number of awards for his research, including the James L. Massey Research & Teaching Award from IEEE Information Theory Society, an Information Theory Society and Communication Society Joint Paper Award, a Presidential Early Career Award for Scientists and Engineers (PECASE) from the White House, a Young Investigator Program (YIP) award from the U.S. Air Force Office of Scientific Research, a National Science Foundation CAREER award, the David J. Sakrison Memorial Prize, and several Best Paper Awards at Conferences. He has been an Associate Editor for IEEE Transactions on Information Theory. He is currently a general Co-Chair of the 2020 International Symposium on Information Theory (ISIT).

Sreeram Kannan is currently an assistant professor at University of Washington, Seattle. He was a postdoctoral scholar at University of California, Berkeley between 2012–2014 before which he received his Ph.D. in Electrical Engineering and M.S. in mathematics from the University of Illinois Urbana Champaign. He is a recipient of the 2017 NSF Faculty Early CAREER award, the 2013 Van Valkenburg outstanding dissertation award from UIUC, a co-recipient of the 2010 Qualcomm Cognitive Radio Contest first prize, a recipient of 2010 Qualcomm (CTO) Roberto Padovani outstanding intern award, a recipient of the SVC Aiya medal from the Indian Institute of Science, 2008, and a co-recipient of Intel India Student Research Contest first prize, 2006. His research interests include the applications of information theory and learning to computational biology and wireless networks.

Pramod Viswanath received the Ph.D. degree in electrical engineering and computer science from University of California at Berkeley in 2000. From 2000 to 2001, he was a member of research staff at Flarion technologies, NJ. Since 2001, he is on the faculty at University of Illinois at Urbana Champaign in Electrical and Computer Engineering, where he is currently the Gilmore Family Endowed Professor.

He received the Eliahu Jury Award from the EECS department of UC Berkeley in 2000, the Bernard Friedman Prize from the mathematics department of UC Berkeley in 2000, a NSF CAREER award in 2002, the Xerox faculty research award from the college of engineering of UIUC in 2010 and the Best Paper Award at the Sigmetrics conference in 2015. He is a coauthor, with David Tse, of the text Fundamentals of Wireless Communication, which has been used in over 60 institutions around the world. He is coinventor of the opportunistic beamforming method and codesigner of Flash-OFDM communication algorithms used in fourth-generation cellular systems.

His current research interests are in first principles design of blockchains. He is co-founder and CEO of Applied Protocol Research, a startup company developing full stack blockchain solutions.