







# HiCoCS: High Concurrency Cross-Sharding on Permissioned Blockchains

Lingxiao Yang , *Graduate Student Member, IEEE*, Xuewen Dong , *Member, IEEE*,  
Zhiguo Wan , *Senior Member, IEEE*, Di Lu , *Member, IEEE*, Yushu Zhang , *Senior Member, IEEE*,  
and Yulong Shen , *Member, IEEE*

**Abstract**—As the foundation of the Web3 trust system, blockchain technology faces increasing demands for scalability. Sharding emerges as a promising solution, but it struggles to handle highly concurrent cross-shard transactions (CSTxs), primarily due to simultaneous ledger operations on the same account. Hyperledger Fabric, a permissioned blockchain, employs multi-version concurrency control for parallel processing. Existing solutions use channels and intermediaries to achieve cross-sharding in Hyperledger Fabric. However, the conflict problem caused by highly concurrent CSTxs has not been adequately resolved. To fill this gap, we propose HiCoCS, a high concurrency cross-shard scheme for permissioned blockchains. HiCoCS creates a unique virtual sub-broker for each CSTx by introducing a composite key structure, enabling conflict-free concurrent transaction processing while reducing resource overhead. The challenge lies in managing large numbers of composite keys and mitigating intermediary privacy risks. HiCoCS utilizes virtual sub-brokers to receive and process CSTxs concurrently while maintaining a transaction pool. Batch processing is employed to merge multiple CSTxs in the pool, improving efficiency. We explore composite key reuse to reduce the number of virtual sub-brokers and lower system overhead. Privacy preservation is enhanced using homomorphic encryption. Evaluations show that

HiCoCS improves cross-shard transaction throughput by 3.5-20.2 times compared to the baselines.

**Index Terms**—Blockchain scalability, cross-shard transaction, high concurrency processing, permissioned blockchain.

## I. INTRODUCTION

THE advent of Web3 marks a significant evolution in the Internet landscape, with blockchain technology playing a crucial role in establishing trust within this new paradigm [1], [2], [3], [4]. Despite its potential, blockchain technology faces significant scalability challenges, which limit its performance in large-scale applications [5]. Sharding, a technique borrowed from distributed databases, has emerged as a promising solution to enhance blockchain scalability by partitioning the network into smaller, manageable segments that can process transactions independently, thereby increasing overall throughput [6].

Most existing blockchain sharding solutions [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17], [18], [19], [20], [21], [22], [23], [24], [25], such as Elastico [7], Omniledger [8], Rapidchain [9], and Pyramid [12], primarily focus on permissionless blockchains [26]. However, permissioned blockchains like Hyperledger Fabric [14], which are widely used in enterprise settings, also require effective sharding solutions to meet the growing demand for scalable and efficient blockchain applications. MDIoTSP explores utilizing Fabric's channels as sub-shards to enhance scalability in multi-domain Internet of Things (IoT) systems [15]. However, efficiently managing highly concurrent cross-shard transactions (CSTxs) remains a significant challenge. Existing solutions [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17], [20], [21], [22], [23], [24], [25] frequently experience high transaction abort rates due to conflicts arising when multiple CSTxs attempt to access the same ledger state simultaneously. These conflicts are particularly problematic in permissioned blockchains, where maintaining high throughput and low latency is crucial for enterprise applications.

We further elucidate the existing problems. As shown in Fig. 1(a), Fabric implements concurrent transaction data consistency based on multi-version concurrency control (MVCC) [27], [28]. The concept is that each transaction's key-value pair data has a version number, and a new version is generated each time the data is modified. When a transaction reads or writes data, it checks whether the version number of the data is

Received 15 March 2024; revised 19 February 2025; accepted 28 March 2025. Date of publication 4 April 2025; date of current version 11 June 2025. This work was supported in part by the National Key R&D Program of China under Grant 2023YFB3107500; in part by the National Natural Science Foundation of China under Grant 62220106004, Grant 62232013, Grant 62272425, and Grant U22B2032; in part by the Technology Innovation Leading Program of Shaanxi under Grant 2022KXJ-093 and Grant 2023KXJ-033; in part by the Innovation Capability Support Program of Shaanxi under Grant 2023-CX-TD-02; and in part by Ganpo Talent Program of Jiangxi Province under Grant gpyc20240012. Recommended for acceptance by D. Gizopoulos. (*Corresponding author: Xuewen Dong.*)

Lingxiao Yang and Xuewen Dong are with the School of Computer Science and Technology, Xidian University, Xi'an 710071, China, also with the Engineering Research Center of Blockchain Technology Application and Evaluation, Ministry of Education, Xi'an 710071, China, and also with Shaanxi Key Laboratory of Blockchain and Secure Computing, Xi'an 710071, China (e-mail: lxyang@stu.xidian.edu.cn; xwdong@xidian.edu.cn).

Zhiguo Wan is with Zhejiang Lab, Hangzhou, Zhejiang 311121, China (e-mail: wanzhiguo@zhejianglab.com).

Di Lu and Yulong Shen are with the School of Computer Science and Technology, Xidian University, Xi'an 710071, China, and also with the Shaanxi Key Laboratory of Network and System Security, Xi'an 710071, China (e-mail: dlu@xidian.edu.cn; ylshen@mail.xidian.edu.cn).

Yushu Zhang is with the School of Computing and Artificial Intelligence, Jiangxi University of Finance and Economics, Nanchang 330013, China (e-mail: yushu@nuaa.edu.cn).

Digital Object Identifier 10.1109/TC.2025.3558001

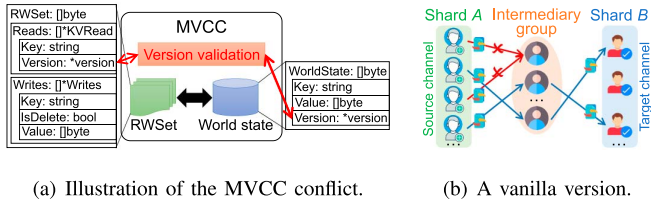


Fig. 1. The MVCC conflict and a cross-shard example in hyperledger fabric.

consistent with the expected value. If it is not, the transaction needs to be rolled back and re-executed. Thus, MVCC improves read concurrency but may increase transaction abort rates when handling write operations. Fig. 1(b) shows a *vanilla version* of cross-shard implementation in Fabric using channels and intermediaries (or brokers [6]). A source channel (i.e., shard A) initiates CSTxs, and shard B is a target channel that receives CSTxs. Each intermediary joins both shard A and shard B. Each CSTx needs to be transferred to an intermediary first, and then the intermediary transfers the assets to the target-shard user. As a result, when the concurrency of CSTxs is high, the ledger state of the intermediary account is frequently read and written, which causes MVCC conflicts due to data contention. The retries of aborted CSTxs increase overhead and degrade the quality of cross-shard service.

**Motivation.** As interoperability requirements expand, the volume of CSTxs increases rapidly, and mitigating the conflicts that often arise between them is key to improving the efficiency of CSTxs. With the adoption of sharding, inter-contract calls between contracts in different shards result in massive CSTxs. According to public data from Ethereum, more than 70% of inter-contract calls occur more than twice [12]. Large enterprises typically involve heavy partitioned transactions and data flows, which require CSTxs to manage data interactions between different partitions. Surprisingly, however, *there is almost no research on high concurrency cross-sharding for Hyperledger Fabric*. In addition, traditional concurrency control mechanisms, such as two-phase locking (2PL) [8], [10] and optimistic concurrency control (OCC) [11], [12], are ineffective at addressing these conflicts in high concurrency environments, leading to significant performance bottlenecks. Thus, to fill this gap, we conduct a systematic study to utilize Fabric's internal features to achieve high concurrency cross-sharding.

**Challenges.** We mainly face two challenges: (i) How to lightweight and effectively resolve the contradiction between the demand for highly concurrent CSTxs and MVCC conflicts among intermediaries? The naive approach is to directly add new intermediaries, but this increases resource consumption and system complexity. The added intermediaries still need to coordinate with other nodes when processing CSTxs, which may lead to new MVCC conflicts. (ii) How to balance concurrent transaction efficiency with privacy? The vanilla version overlooks the privacy-preserving issue of cross-sharding. In practice, intermediaries are semi-trusted. Each intermediary may honestly complete the CSTx processing, but it could be honest-but-curious, attempting to steal privacy (e.g., transaction amount) from data generated by the participants.

**Contributions.** To address the above challenges, we focus on mitigating the conflict problem of highly concurrent CSTxs and propose HiCoCS, a novel **highly concurrent cross-shard** scheme. Different from prior work, HiCoCS introduces a unique virtual sub-broker mechanism using Fabric's composite key functionality. It only requires smart contract API calls, not the actual addition of new nodes, which greatly reduces resource consumption. By creating virtual sub-brokers on existing intermediary nodes, CSTxs can be refined to a smaller granularity, effectively reducing the frequency of MVCC conflicts. Batch management of virtual sub-brokers by intermediaries also improves transaction efficiency. On the other hand, HiCoCS combines homomorphic encryption to address the privacy preservation problem of transaction amounts calculated at the intermediaries. The use of composite keys efficiently identifies and manages CSTxs to avoid data conflicts, and homomorphic encryption allows operations on encrypted data without decryption, enabling the accumulation of concurrent CSTxs while maintaining data privacy and security. The combination of the two reduces conflicts and rollbacks in traditional concurrency control mechanisms. It also balances the security and performance of highly concurrent CSTxs. We summarize the contributions of HiCoCS as follows:

- **High concurrency cross-sharding.** To the best of our knowledge, HiCoCS is the first proposed solution to address the problem of highly concurrent CSTxs on Hyperledger Fabric. It utilizes composite keys to construct virtual sub-brokers for cross-shard intermediaries to mitigate concurrency conflicts, supporting the high concurrency of receiving and processing CSTxs. Based on maintaining a transaction pool, HiCoCS adopts the idea of batch processing to design an incremental accumulation module that summarizes the transactions in the pool, and the merged processing of multiple CSTxs reduces conflicts and improves efficiency.

- **Privacy-preserving cross-sharding.** For the privacy risk posed by semi-trusted intermediaries, we utilize Cheon-Kim-Kim-Song (CKKS) fully homomorphic encryption to achieve privacy preservation for CSTxs. It allows the incremental accumulation of CSTxs by intermediaries for virtual sub-brokers to be computed under ciphertext, balancing security and concurrency performance. We analyze and prove the security of the scheme.

- **Composite key reuse mechanism.** To further reduce the resource consumption caused by managing composite keys, we design a composite key reuse mechanism. It includes a Composite Key Proof of Equivalence (CKPoE) protocol that summarizes and regenerates composite keys to reduce the number of virtual sub-brokers and lower system overhead.

- **Prototype evaluation.** We implement a prototype of HiCoCS on Hyperledger Fabric and perform comprehensive comparisons with baselines. Evaluation results show that HiCoCS outperforms the state-of-the-art schemes in terms of transaction success rate (improved by 2.2 to 8.1 times), throughput (improved by 3.5 to 20.2 times), latency (reduced by 43.9% to 62.0%), and CPU & memory utilization rates.

## II. RELATED WORK

In this section, we categorize the literature related to **CSTx** conflict resolution based on its implementation and compare the corresponding features.

Existing work [6], [7], [8], [9], [10], [11], [12], [19], [13], [14], [15], [16], [17], [18], [20], [21], [22], [23], [24], [25] mainly employs two concurrency control mechanisms to mitigate **CSTx** conflicts: (i) *Two-phase locking (2PL)*. It is a pessimistic concurrency control approach that assumes transaction conflicts occur frequently, thus ensuring isolation by adding locks during transaction execution. (ii) *Optimistic concurrency control (OCC)*. It assumes that conflicts are relatively infrequent, does not add locks during execution, and verifies whether a conflict arises when the transaction is committed. Based on this, we illustrate representative sharded permissionless and permissioned blockchains, providing a feature comparison in Table I.

**2PL schemes:** Omniledger [8] proposes a Byzantine shard atomic commit protocol, Atomix, to ensure the consistency of transactions. Rapidchain [9] parallelizes data and computation through full node sharding. Chainspace [10] proposes object-oriented smart contract sharding, which assigns different contracts and transactions to different shards for processing. Tong et al. [15] implemented a sharding system for Hyperledger Fabric using channels. AHL+ [29] relies on trusted hardware to enhance the Hyperledger Fabric to handle cross-shard distributed transactions. Aeolus [30] proposes distributed state update sharding to maintain consistency across different clusters. Set et al. [31] proposed a service-aware dynamic sharding that utilizes a reference committee to act as a coordinator for concurrency control.

**OCC schemes:** Monoxide [11] achieves fast processing and eventual consistency of **CSTx**s through asynchronous cross-zone validation. Pyramid [12] employs a hierarchical sharding architecture and a recursive consensus protocol to ensure efficient communication and global consistency across different layers and shards. CoChain [13] designed a cross-shard Consensus on Consensus mechanism to securely configure small shards and enhance concurrency. Androulaki et al. [32] achieved sharding on Hyperledger Fabric using multiple channels and utilized Merkle Tree to process **CSTx**s. Meepo [33] introduces cross-epoch and cross-call protocols for ordered cross-shard communication.

**Comparison.** Existing approaches have their own merits. However, none of these efforts properly address the conflict problem in highly concurrent **CSTx** scenarios. According to the evaluation of PROPHET [19], more than half of the **CSTx**s are aborted or rolled back due to race conditions (i.e., frequent read/write to the same ledger state). Thus, 2PL and OCC schemes usually exhibit high transaction abort rates (i.e., aborted **CSTx**s may require multiple retries to succeed), sacrificing efficiency for the serializability of **CSTx**s. Our proposed HiCoCS uses composite keys to create virtual sub-brokers for conflicted intermediary accounts. It uses a message-passing approach to ensure the consistency of **CSTx**s, utilizing storage space in exchange for high concurrency **CSTx** efficiency. In addition, most existing work does not consider **CSTx** privacy

TABLE I  
FEATURE COMPARISON WITH EXISTING SHARDING SOLUTIONS

Schemes	Features*	CCM	BT	Fabric-oriented	HiCo CSTxs	PP CSTxs	BP CSTxs
Ref. [8], [9]	2PL	Pl	-	×	×	×	×
Chainspace [10]	2PL	Pl	-	×	✓	×	×
Ref. [15], [29], [31]	2PL	Pd	✓	×	×	×	×
Aeolus-Geth [30]	2PL	Pd	-	×	×	×	×
Ref. [11], [12], [13]	OCC	Pl	-	×	×	×	×
Ref. [32]	OCC	Pd	✓	×	×	×	×
Meepo-OE [33]	OCC	Pd	-	×	×	×	×
HiCoCS (This work)	CK	Pd/Pl	✓	✓	✓	✓	✓

\*Abbreviation explanation: Concurrency Control Mechanism (CCM); Blockchain Type (BT); Highly Concurrent (HiCo); Privacy-Preserving (PP); Batch Processing (BP); Permissionless (Pl); Permissioned (Pd); Composite Key (CK). ✓: Satisfied; ×: Unsatisfied; -: Inapplicable.

preservation. HiCoCS combines homomorphic encryption to balance performance and security. Meanwhile, HiCoCS supports batch processing of **CSTx**s by utilizing composite keys for accumulated summarization of transaction ciphertexts. Although HiCoCS is a Hyperledger Fabric-oriented permissioned blockchain sharding scheme, it can also be extended to permissionless blockchains with simple modifications (see Section V-F).

Note: \*Abbreviation explanation: Concurrency Control Mechanism (CCM); Blockchain Type (BT); Highly Concurrent (HiCo); Privacy-Preserving (PP); Batch Processing (BP); Permissionless (Pl); Permissioned (Pd); Composite Key (CK). ✓: Satisfied; ×: Unsatisfied; -: Inapplicable.

## III. BACKGROUND AND PRELIMINARIES

### A. EOVS Transaction Processing Architecture

Unlike the order-execute-validate (OEV) transaction processing flow adopted by permissionless blockchains (e.g., Bitcoin and Ethereum), permissioned blockchains (e.g., Hyperledger Fabric) use an execute-order-validate (EOV) architecture. Fig. 2 shows the transaction processing in Fabric: ① Clients initiate transaction proposals. ② Peer nodes simulate the execution of transactions (endorsements). ③ Clients compare the endorsement results. ④ The endorsement results are sent to the ordering service as transaction messages. ⑤ The ordering nodes order and pack the transactions into blocks. ⑥ The new blocks are broadcasted and validated in the peer cluster. ⑦ The peer nodes append the block to its channel's ledger.

Transactions can be executed concurrently on multiple nodes during the simulation stage, while the correct order of transaction submission is determined in the ordering and validation stages. This approach performs well with few read/write conflicts and low transaction submission latency.

### B. Multi-Version Concurrency Control (MVCC)

In Hyperledger Fabric, MVCC defines the version number as the height of a transaction and stores it in the world state along with the key-value pair. The version of a key is contained only in the read set, which is used to check the validity of a transaction. The write set is used to update the value corresponding to a key, which is incremented after each successful update. This



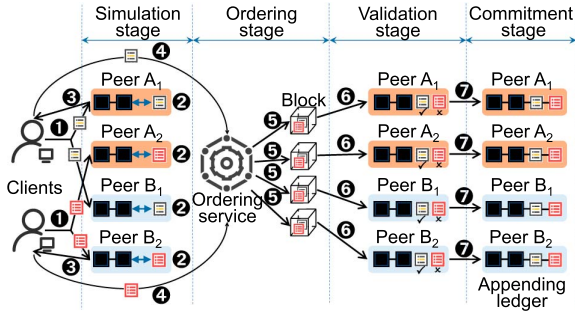


Fig. 2. Hyperledger Fabric's transaction processing flow.

ensures transaction isolation; read and write operations do not interfere with each other, and conflict detection occurs only at the commitment stage. If the key version in the read set matches that in the world state, the transaction is valid; otherwise, it is considered an MVCC conflict.

Specific conflict cases include: (i) *Write-write conflict*. If two concurrent transactions attempt to modify the same data item, only the first committed transaction succeeds, and the others abort due to the conflict. Because the data operated on by each transaction is a “snapshot”, concurrent transactions cannot see the changes made by other transactions and may make decisions based on outdated data. (ii) *Repeatable read problem*. If a transaction reads a data item and then another transaction modifies it, the data has changed when the original transaction reads it again, which may lead to an abort because it needs to make a decision based on the latest data. (iii) *Validation phase abort*. In MVCC-enabled systems (e.g., Oracle database, Ethereum blockchain, and other OCC policy-enabled systems), conflict detection is performed when the transaction commits, and the transaction is aborted if a conflict is found.

### C. Composite Key in Hyperledger Fabric

The composite key in Hyperledger Fabric is a data structure used in state databases (e.g., CouchDB or LevelDB). It consists of multiple attributes/fields combined into a unique key. It supports efficient retrieval based on different combinations of attributes, enhancing the flexibility and complexity of business logic [34]. The main steps of composite key usage in Fabric include: (i) *Creation*. Call the `CreateCompositeKey()` function of the chaincode API<sup>1</sup> to concatenate the prefix and attribute array to generate a composite key. (ii) *Store*. Call the `PutState()` function to store the composite key and the corresponding value in the database. (iii) *Query*. Call the `GetStateByPartialCompositeKey()` function to query the data in the database based on a given partial composite key.

Composite keys are mainly used in Fabric for chaincode querying and logical indexing of state data, without directly affecting the physical storage structure of the state database.

<sup>1</sup><https://hyperledger.github.io/fabric-chaincode-node/release-2.4/api/fabric-shim.ChaincodeStub.html>

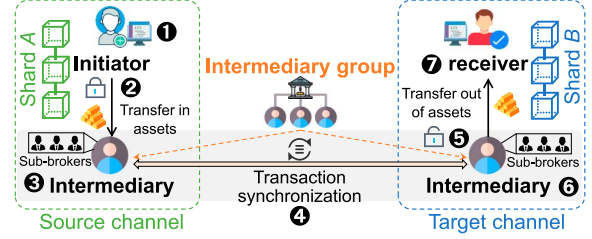


Fig. 3. System overview of HiCoCS.

This provides an opportunity to construct composite keys for intermediaries to process transactions as virtual sub-brokers and share the pressure of CSTx conflicts when realizing Fabric's high concurrency cross-sharding.

### D. Homomorphic Encryption Techniques

Homomorphic encryption is a public key encryption algorithm designed to perform data operations without leaking private data. Based on their arithmetic capabilities, homomorphic encryption schemes are classified into three categories [35]: (i) Partially homomorphic encryption (PHE) [36]; (ii) Somewhat homomorphic encryption (SHE) [37]; (iii) Fully homomorphic encryption (FHE). PHE supports only one of additive or multiplicative homomorphic operations, and the number of operations is unlimited. SHE supports both additive and multiplicative homomorphisms with a limited number of operations. FHE supports not only additive and multiplicative homomorphisms but also an unlimited number of operations.

In the vanilla version of Fabric's cross-sharding, a semi-trusted intermediary can batch process non-integer cross-shard assets, thus requiring privacy computations that support addition and multiplication. This paper uses an approximate FHE algorithm, i.e., the Cheon-Kim-Kim-Song (CKKS) [38], which supports high-performance fully homomorphic encryption operations on floating-point numbers.

## IV. SYSTEM OVERVIEW OF HICOCS

### A. System Model

Fig. 3 shows the overall interaction model of HiCoCS. The system roles include the transaction *initiator* in the source channel, the *intermediary group*, and the transaction *receiver* in the target channel. Their capabilities are as follows.

- **Initiator**. As an initiator user of CSTxs, it first transfers assets in the source channel to an intermediary account.
- **Intermediary group**. It consists of multiple intermediary nodes, each of which should be satisfied with owning assets on both the source and target channels. An intermediary summarizes and processes multiple CSTxs in a unified manner to realize cross-shard asset transfers between the source and target channels, i.e., it receives the source channel's transactions and distributes them to the target channel. In the system's building block perspective, each intermediary performs CSTx pre-processing (including the construction of *composite keys/virtual sub-brokers*),

incremental accumulation (calculated under ciphertext), transaction synchronization, and composite key reuse.

- **Receiver.** As a user on the target channel, it receives the assets from the intermediary for each CSTx.

The cross-shard trading process of HiCoCS is mainly divided into the following steps.

- 1) **CSTx initiation.** ① First, the initiator initiates an asset transfer request through its client. The transaction information contains the initiator's address (key), the receiver's address, and the transaction amount. ② Then, the initiator's CSTx message is encrypted and sent to an intermediary.
- 2) **Intermediary processing.** ③ The system transfers the initiator's transfer assets to an intermediary account (i.e., its virtual sub-broker accounts) in the source channel through the smart contract. ④ The intermediary of the source channel collects the transaction ciphertexts, converts them into CKKS ciphertext vectors, and accumulates and summarizes the transaction ciphertexts. Finally, the target channel intermediary synchronizes the summarized results.
- 3) **CSTx completion.** ⑤ The source channel calls a decryption function of smart contract to restore the intermediary's cipher state summarized results to plaintext and complete the final accumulated amount to be written to the target channel's intermediary ledger. ⑥ Then, the intermediary in the target channel first cross-channel queries the set of successfully received transactions on the source channel as its set of transactions to be transferred. ⑦ Finally, it traverses the pending set and transfers the assets to the final target account in proportion to an exchange rate.

We give a concise example to illustrate the core idea of HiCoCS in handling high concurrency CSTxs, as shown in Fig. 4. Suppose there are multiple initiators  $\{O_1, O_2, O_3, O_4\}$  initiating  $\{CSTx_1, CSTx_2, CSTx_3, CSTx_4\}$  to the receivers  $\{D_1, D_2, D_3, D_4\}$  respectively in a short period of time. These CSTxs are all relayed and handled by an intermediary  $g_1$ . In the vanilla version, most of the CSTxs will be aborted due to MVCC conflicts, as the ledger state of  $g_1$  is read and written multiple times. However, in HiCoCS, the intermediary generates a virtual sub-broker for each CSTx, i.e., invokes the smart contract to quickly generate the composite keys  $\{g_1 - O_i - D_i - V_i\}_{i=1}^4$ . The  $V_i$  is the amount's ciphertext for each CSTx. Since multiple virtual sub-brokers are writing to the ledger, the MVCC conflicts of a single intermediary are effectively mitigated. The overhead of creating a composite key is much smaller than maintaining a new intermediary, thus significantly reducing the transaction cost for the users.

**Insight.** The core principle of HiCoCS support for high concurrency CSTx processing is to *build multiple virtual sub-brokers through the composite keys to avoid concurrent conflicts and realize batch processing of transactions. Each intermediary then counts the final amount by querying the pool of composite key transactions, and multiple CSTxs are processed at once* (see Section V). Actually, the inspiration

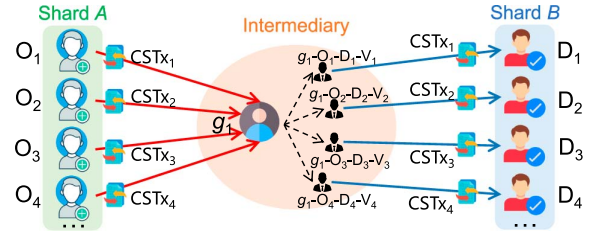


Fig. 4. An example illustrating the HiCoCS.

originally came from blockchain layer-2 techniques such as the payment channel network (PCN) [5].

### B. Threat Model

We follow Microsoft's STRIDE model [39] to comprehensively analyze the potential threats of semi-trusted intermediaries to HiCoCS. (i) *Spoofing*. An attacker spoofs as an intermediary to perform CSTx processing to steal transaction data for additional profit. (ii) *Tampering*. An intermediary may maliciously modify transaction data. (iii) *Repudiation*. An intermediary denies specific operations performed in CSTxs, such as denying receipt of transferred assets from its initiator. (iv) *Information disclosure*. An intermediary may expose the private data of the participants, such as transaction flows and asset holdings. (v) *Denial of service*. An intermediary may actively or passively make CSTx services unavailable [40]. (vi) *Elevation of privilege*. An intermediary with limited privileges impersonates an intermediary with privileges to gain the ability to process CSTxs.

We state the following **assumptions**: The Hyperledger Fabric's channels (equivalent to shards in this paper) are secure and reliable. There is at least one honest intermediary in the intermediary group that joins the source and target channels to provide cross-shard service. The intermediary is usually well-funded to cope with concurrent CSTxs during a period (for potential liquidity issues, we discuss introducing a remedial mechanism to ensure the robustness of the system in Section V-D). The public-private key distribution of the encryption and decryption functions is secure and does not involve key transmission security issues and quantum threats.

### C. System Goals

To meet the performance and privacy requirements for highly concurrent cross-shard transaction processing, HiCoCS needs to achieve the following goals.

- **Robustness.** It allows large-scale CSTxs to be sent to the system simultaneously and ensures that CSTxs are properly received and processed with a high transaction success ratio.
- **Efficiency.** The system can process CSTxs efficiently and cost-effectively, i.e., it is characterized by high throughput, low confirmation latency, and low resource overhead.
- **Security.** The security of CSTxs includes (i) *Data confidentiality*. The system ensures that the semi-trusted intermediaries cannot extract the transaction amount privacy.

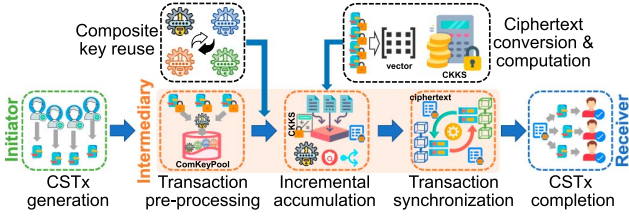


Fig. 5. Building blocks of HiCoCS.

- (ii) *Transaction atomicity*. The system needs to satisfy the eventual atomicity of CSTxs. (iii) *Service availability*. The system is able to provide continuous and effective service.

We emphasize that the *focus* of HiCoCS is on achieving *robustness* and *efficiency*, and that privacy preservation in security is an optional feature provided. In this paper, no improvements are made to fully homomorphic cryptography (e.g., CKKS), as this is another work of independent interest, which we leave for future work.

## V. SYSTEM DESIGN OF HiCoCS

### A. Design Outline

Fig. 5 is the design outline of HiCoCS, which shows the system's building blocks, mainly including the *transaction generation module*, *pre-processing module*, *incremental accumulation module*, *transaction synchronization module*, and *transaction completion module*. In addition, the *composite key reuse mechanism* is crucial to reduce the resource overhead of HiCoCS. The *ciphertext conversion and computation mechanisms* are the key to achieving privacy protection. Their main functionalities are summarized below.

- **Transaction generation module** is mainly responsible for packaging transactions. The packaged content includes the addresses of the transaction initiator and receiver, and the transaction inclusion (we omit its details).
- **Pre-processing module** mainly consists of collecting CSTx ciphertexts, constructing composite keys, and maintaining a composite key transaction pool ComKeyPool.
- **Incremental accumulation module** adopts the idea of batch processing to summarize the intermediary-related CSTxs in the ComKeyPool, including the operations of fuzzy query composite key, splitting composite key, and accumulating the final amount to be received under ciphertext.
- **Transaction synchronization module** requests the ciphertext processing result at the source channel from the incremental accumulation module via a cross-channel query, and synchronizes the pending CSTxs on the target channel with the intermediary's received CSTxs on the source channel.
- **Transaction completion module** distributes CSTxs to be transferred to accounts in the target shard (details omitted).
- **Composite key reuse mechanism** transforms multiple associated composite keys in ComKeyPool into a single composite key, including composite key summarization

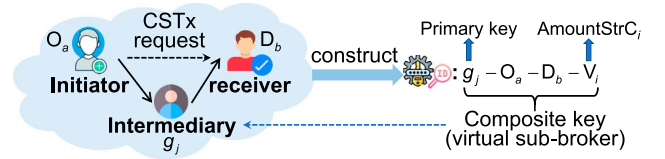


Fig. 6. Composite key construction.

and regeneration operations. It hands over the updated simplified ComKeyPool to the incremental accumulation module.

- **Ciphertext conversion & computation mechanisms** first convert the transaction ciphertext array into the CKKS ciphertext vectors for computation. Then, the ciphertext amounts are summarized (incrementally accumulated) to produce the ciphertext result, which is passed to the source channel for decryption and subsequent processing.

### B. Transaction Pre-Processing

Following the workflow, HiCoCS first encrypts the packaged CSTxs in the source channel to ensure the security of the CSTx transmission. Then, composite keys (virtual sub-brokers) are created for each intermediary under the CSTx ciphertext.

**Transmission pre-processing.** We use the advanced encryption standard (AES) algorithm [41] to pre-process the CSTx messages. This serves two purposes: (i) The transaction initiator performs AES encryption of its initiated CSTx messages in the source channel, which ensures the security of CSTx message transmission. Of course, this requires ensuring the secure storage of keys. We utilize Fabric's private data collection to store the sender's AES key, and control that only authorized smart contract functions to access and use it for decryption. (ii) HiCoCS uses AES to convert packaged transaction messages (which may have inconsistent data lengths) into a uniformly formatted ciphertext (128-bit), which serves as the input to the CKKS algorithm used in the subsequent incremental accumulation module. This ensures a lightweight, encrypted transmission of CSTxs to the sharding network.

First, an initiator generates an AES symmetric key  $skey$  for the encryption and decryption of each CSTx in the source channel. Then, for the transaction amount  $Amount_i$ , the initiator uses  $skey$  to encrypt and obtain the CSTx ciphertext, i.e.,  $AmountStrC_i = \text{EncryptAES}(skey, Amount_i)$ .

**Composite key pre-processing.** To avoid concurrent CSTxs creating access conflicts to a single intermediary account/key, HiCoCS uses composite keys to combine multiple fields related to each CSTx. It constructs different composite keys as virtual sub-brokers of an intermediary to cache CSTxs, and adds each CSTx to a composite key transaction pool ComKeyPool. Thus, it transforms the client's direct modification of the intermediary's state into the creation of composite keys, avoiding frequent access to a single key.

The construction of a composite key is shown schematically in Fig. 6. The intermediary group  $\mathcal{G}$  contains  $|\mathcal{G}|$  intermediaries, where each intermediary has an address/key of  $g_j$ .  $O_a$  and  $D_b$



denote the address/key of user  $a$  on the source (original) channel and user  $b$  on the target (destination) channel, respectively. Thus, a CSTx is denoted as  $\text{CSTx}_i(\text{O}_a, \text{D}_b, g_j, \text{Amount}_i)$ . The CSTx ciphertext message sent by the client via gRPC is  $\text{CSTx}'_i(\text{O}_a, \text{D}_b, g_j, \text{AmountStrC}_i)$ . The CSTx amount (value) ciphertext  $\text{AmountStrC}_i$  is simplified to  $V_i$ . In addition, to ensure the uniqueness of the composite key,  $V_i$  contains the timestamp of the transaction (for the case of multiple concurrent CSTxs with the same initiator, receiver, intermediary, and transaction amount). Thus, the pre-processing module constructs a composite key (virtual sub-broker) of  $\text{CSTx}'_i$  as  $\text{CK}_i : g_j - \text{O}_a - \text{D}_b - V_i$ , and  $g_j$  is used as the primary key of this composite key. The intermediary then adds  $\text{CK}_i$  to the  $\text{ComKeyPool} \leftarrow \{\text{CK}_1, \text{CK}_2, \dots, \text{CK}_{i-1}\}$ . When the time reaches the periodic settlement time threshold, i.e.,  $t = T_{\text{settle}}$ , the intermediary group settles  $i$  CSTxs corresponding to  $\text{ComKeyPool} \leftarrow \{\text{CK}_1, \text{CK}_2, \dots, \text{CK}_i\}$ .

**Discussion.** We explore a potential double-spending attack and its corresponding countermeasure. Suppose an attacker initiates two CSTxs simultaneously, with a combined total amount exceeding its account balance, and these two CSTxs are processed by different intermediaries and packaged into separate transaction batches. During validation, only one of the CSTxs can succeed, while the other fails due to insufficient balance, leading to the rejection of the entire batch and negatively impacting other valid CSTxs. HiCoCS employs timestamps to ensure that even if two CSTxs are initiated simultaneously, they will have distinct timestamps corresponding to the composite key, causing the latter transaction in the queue to fail due to insufficient balance. Consequently, HiCoCS prevents this attack at its source. Even if an attack occurs, since the composite key contains the amount of transactions that failed due to malicious initiation, HiCoCS rolls back only the failed CSTx and a small number of dependent CSTxs, rather than the entire batch. This ensures that other valid CSTxs are completed successfully.

### C. Incremental Accumulation

The process of transaction incremental accumulation under ciphertext is shown in Algorithm 1.

**Amount ciphertext collection.** (Lines 2-9) If the current time  $t = T_{\text{settle}}$ , the intermediary starts to settle the CSTxs accumulated in the last period. First, a fuzzy query is performed on the  $\text{ComKeyPool}$  based on each intermediary's key  $g_j$  (primary key). As a result, the system obtains a CSTx set associated with the intermediary  $g_j$ , i.e.,  $\text{ComKeyPool}_j \leftarrow \{\text{CK}_1, \text{CK}_2, \dots, \text{CK}_i\}$ . Then, the intermediary traverses  $\text{ComKeyPool}_j$  and calls Fabric's composite key splitting function  $\text{SplitCompositeKey}()$  to obtain the set of CSTx amount ciphertexts  $\text{aesStrCipher} = \{V_1, V_2, \dots, V_n\}$ . Also, it adds  $\{D_i, V_i\}$  to the pending transaction set.

**Ciphertext conversion.** (Lines 10-16) Next, the system performs a ciphertext conversion on  $\text{aesStrCipher}$  for CKKS homomorphic privacy calculation of the accumulated CSTxs' amount, as shown in Fig. 7. First, the intermediary traverses  $\text{aesStrCipher}$  and calls the AES decryption function to decrypt

### Algorithm 1: Incremental Accumulation Algorithm.

---

**Input:** The intermediary's key  $g_j$ , a plaintext scaling factor  $\Delta$ , an exchange rate  $C_{\text{rate}}$

**Output:** The final ciphertext summation result  $C_{\text{finalSum}}$

---

```

1 Function cstxAcc( $\cdot$ ):
2   if  $t = T_{\text{settle}}$  then
3     // Ciphertext collection
4     // The _ symbol below denotes the prefix
5      $\text{ComKeyPool}_j \leftarrow \text{GetStateByPartialCompositeKey}(\_, g_j)$ 
6     for  $i = 0$  to  $|\text{ComKeyPool}_j| - 1$  do
7        $\text{compositeKeyObject}_i \leftarrow \text{ComKeyPool}_{j,i}$ 
8       // Get compositeKey
9        $\text{CK}_i \leftarrow \text{compositeKeyObject}_i.\text{getKey}()$ 
10      // Split compositeKey
11       $\_, D_i, V_i \leftarrow \text{SplitCompositeKey}(\text{CK}_i)$ 
12      Add  $\{D_i, V_i\}$  to the pending transaction set
13       $\text{aesStrCipher.add}(V_i)$ 
14    // Ciphertext conversion
15    for  $i = 0$  to  $|\text{aesStrCipher}| - 1$  do
16      // Call the convert() interface
17       $\text{Amount}_i \leftarrow \text{DecryptAES}(\text{skey}, V_i)$ 
18       $\text{Amounts}[i] \leftarrow \text{complex}(\text{Amount}_i, 0)$ 
19       $\text{Amounts.add}(\text{Amounts}[i])$ 
20     $m(X) \leftarrow \text{Encode}(\text{Amounts}, \Delta)$ 
21     $(pk, sk) \leftarrow \text{NewKeyPair}()$ 
22     $\text{CKKSCipher} \leftarrow \text{EncryptCKKS}(pk, m(X))$ 
23    // Ciphertext computation
24     $\text{rlk} \leftarrow \text{GenRelinearizationKey}()$ 
25     $\text{gk} \leftarrow \text{GenGaloisKey}()$ 
26     $\text{evaluator} \leftarrow \text{NewEvaluator}()$ 
27     $\text{RotationKey} \leftarrow \text{GenRotationKeys}(\text{gk}, sk)$ 
28     $\text{eval} \leftarrow \text{evaluator.WithKey}(\text{RotationKey}, \text{rlk})$ 
29    for  $i = 0$  to  $\lfloor \text{batch}/n \rfloor - 1$  do
30       $\text{eval.InnerSum}(\text{CKKSCipher}, \text{batch}, n, \text{CKKSCipher})$ 
31     $C_{\text{sum}} \leftarrow \text{CKKSCipher}[0]$ 
32    // Asset exchange
33     $C_{\text{finalSum}} \leftarrow \text{evaluator.MulNew}(C_{\text{sum}}, C_{\text{rate}})$ 
34  return  $C_{\text{finalSum}}$ 

```

---

each  $V_i$  to get the amount of each CSTx, i.e., line 11. Note that  $\text{skey}$  is not leaked here because  $\text{skey}$  is stored within the initiator's private data collection, and the intermediary calls a ciphertext conversion interface  $\text{convert}()$  to get a CKKS ciphertext vector, i.e.,  $\text{Amount}_i$  is a computed intermediate value, which is not available to the intermediary. Since CKKS is represented in complex space, if an operation is performed on a real number, the imaginary part of the complex number needs to be set to zero first, i.e., line 12. Then, the array ( $\text{Amounts}$ ) is encoded as a CKKS plaintext  $m(X)$  in integer form, i.e.,  $m(X) = \text{Amounts} \cdot \Delta$ , where  $\Delta$  is a plaintext scaling factor and  $\Delta > 0$ . Then, the system generates a public-private key pair  $(pk, sk)$  ( $sk$  in the privacy data collection) required for CKKS in the source channel. It encrypts the plaintext  $m(X)$  into ciphertext, i.e., line 16. It satisfies: (i)  $\text{CKKSCipher} = (c_0 + m, c_1) \in R_Q^2$ , where  $(c_0, c_1)$  is the randomized instance of ring learning with errors (RLWE).  $Q$  is the maximum ciphertext modulus. Also, (ii)  $c_0 + c_1 \cdot sk = e$ , where  $e$  is the noise.

**Ciphertext computation.** (Lines 17-24) After obtaining  $\text{CKKSCipher}$ , the system computes the accumulated amount of the CSTxs in ciphertext, i.e., sums up the components of the ciphertext vector ( $c_i$ ). We realize the incremental accumulation

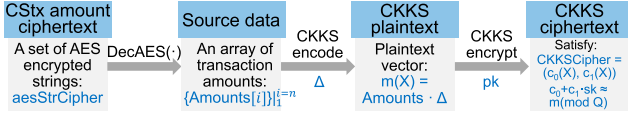


Fig. 7. Ciphertext conversion process.

of the CSTx amount through the ciphertext rotation operation in the following form:

$$E(c_0, c_1, \dots, c_{n-1}) \xrightarrow{\text{Rotate } k \text{ vectors}} E(c_k, \dots, c_{n-1}, c_0, \dots, c_{k-1}).$$

Let the number of components in the ciphertext vector be  $n$  and the ciphertext group size be batch. First, initialize the parameters, including a relinearization key  $\text{rlk}$  (line 17) and a Galois key  $\text{gk}$  (line 18). Then, a ciphertext evaluator is created, i.e., line 19. The private key  $\text{sk}$  and the Galois key  $\text{gk}$  are utilized to generate a key for internal rotation  $\text{RotationKey}$  (line 20). Then, create a shallow copy of the evaluator, i.e., line 21.  $\text{eval}$  is a new  $\text{evaluationKey}$  and shares the temporary buffer with the previous one. The batch components of the ciphertext vector are then rotated  $\lceil \text{batch}/n \rceil$  times in groups of  $n$ , each time evaluating the group's inner sum (calling  $\text{evaluator.InnerSum}()$ ), and finally, the groups are summed (lines 22-23). The final value of all ciphertext slots is an inner sum, and we take the first slot returned as the sum of the transaction ciphertexts, i.e.,  $C_{\text{sum}}$  (line 24).

We emphasize that the above ciphertext conversion and computation are performed in the source channel. Thus, no transaction amount privacy is leaked by intermediaries.

**Confidential asset exchange.** (Line 25) Finally, since the asset values of the two shards may be different, i.e., there exists an exchange rate  $C_{\text{rate}}$ . To prevent an attacker from deriving the value of the two assets through the exchange rate, it is also necessary to encrypt the exchange rate into a ciphertext. Thus, we utilize ciphertext multiplication to achieve asset cross-shard exchange, i.e., the final ciphertext summation result is  $C_{\text{finalSum}} = \text{evaluator.MulNew}(C_{\text{sum}}, C_{\text{rate}})$ .

**Discussion.** HiCoCS uses homomorphic encryption techniques to preserve the privacy of CSTxs. It focuses only on the privacy of the data and not on the identity of the participants. If participants are concerned about the privacy of their identities, they may consider obfuscating the addresses before the transactions [42]. As it is not the focus of this paper, we only briefly describe this approach here. When users need to protect their identity privacy, HiCoCS provides an optional mixing service for identity obfuscation. This service can be provided by an organization consisting of multiple intermediaries, who split each transaction served by each of them into multiple sub-transactions to be mixed within the organization, and ultimately, multiple intermediaries transfer funds to the receiver in multiple passes. The level of transaction obfuscation is correlated with an additional fee paid by the user. In any case, compared to the vanilla version, our approach still has the advantage in guaranteeing the confidentiality of the original transaction data. The intermediaries perform the cumulative transaction amount computation in the ciphertext space, which can effectively mitigate the threats stated in §IV-B.

#### D. Transaction Synchronization and Completion

After obtaining the CKKS ciphertext processing results, the source and target channels/shards synchronize that cipher state results, including the original and exchanged results, i.e.,  $C_{\text{sum}}$  and  $C_{\text{finalSum}}$ . Then, they call the  $\text{DecryptCKKS}()$  function to decrypt the two ciphertext results and decode them in plaintext space, respectively. The initiator of the source channel gets the decryption results and records them in its ledger. The plaintext code for the amount to be transferred to the receiver of the target channel is as follows

$$\text{inAmount} = \text{encoder.Decode}(\text{DecryptCKKS}(\text{sk}, C_{\text{finalSum}})).$$

The plaintext code for the amount ultimately to be deducted by the intermediary is as follows

$$\text{outAmount} = \text{encoder.Decode}(\text{DecryptCKKS}(\text{sk}, C_{\text{sum}})).$$

Finally, since the decoded plaintext is in the form of a complex array, we only need to obtain its real part. The system updates the ledger states of the receivers and intermediaries based on the pending transaction set. Eventually, the CSTxs are completed.

**Discussion.** If affected by liquidity issues, the intermediary accounts may not have sufficient funds to complete the current period of CSTxs. To enhance the system's robustness, we propose introducing a remedial mechanism to address this issue. We adopt the concepts of real-time monitoring via smart contracts [43] and the joint maintenance of liquidity pools to ensure the stability and continuity of cross-shard fund transfers under suboptimal conditions in HiCoCS. We briefly describe the multidimensional components of the mechanism: (i) *Dynamic fund management*. By running real-time monitoring algorithms on smart contracts, the system adjusts the intermediary's pool configuration to replenish funds automatically. (ii) *Distributed liquidity pool*. Establish a liquidity pool jointly maintained by multiple intermediaries to share the funding pressure caused by highly concurrent transactions. (iii) *Prioritized processing mechanism*. In the event of fund constraints, prioritize the processing of small amount transactions to improve the efficiency of fund usage.

#### E. Composite Key Reuse

We adopt an idea of Proof-of-Equivalence (PoE) [44]. It periodically summarizes data and generates equivalent blocks that require less storage space, which significantly saves resources. We implement a periodically running Composite Key Proof of Equivalence (CKPoE) protocol in the composite key reuse mechanism. It consists of composite key summarization and regeneration phases.

A randomly selected intermediary  $g_j \in \mathcal{G}$  in the intermediary group  $\mathcal{G}$  stores the new set of composite keys, combines the composite keys generated from CSTxs in which the participants are (partially) the same, and then regenerates their equivalent



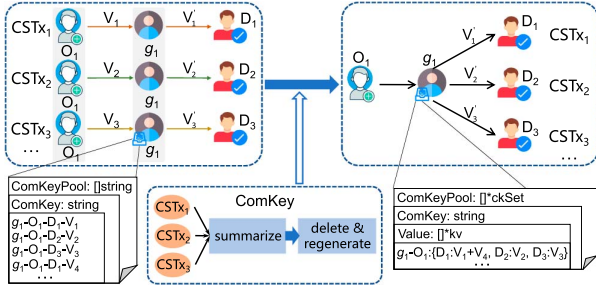


Fig. 8. Composite key reuse.

composite keys. For example, in Fig. 8, assume that the composite key transaction pool (ComKeyPool1) (left) has four composite keys.  $CK_1: g_1 - O_1 - D_1 - V_1$ ,  $CK_2: g_1 - O_1 - D_2 - V_2$ ,  $CK_3: g_1 - O_1 - D_3 - V_3$ , and  $CK_4: g_1 - O_1 - D_1 - V_4$ . Actually, the initiator  $O_1$  transfers a total amount of  $V_1 + V_2 + V_3 + V_4$  to the intermediary  $g_j$ , where a total of  $V_1 + V_4$  needs to be transferred to the receiver  $D_1$ . Thus, we create a new ComKeyPool (right) of pending CSTxs, which deletes the original 4 composite keys and adds a new composite key  $g_1 - O_1: \{D_1: V_1 + V_4, D_2: V_2, D_3: V_3\}$ .

We briefly describe the CKPoE protocol process in Algorithm 2.

**Composite key summarization.** (Lines 2-13) The periodically elected intermediary  $g_j$  listens to the composite keys added to ComKeyPool1, checks all the accounts involved, and summarizes the composite keys with the same participants and their amounts. The idea is to count the final execution results of multiple transactions at once and then record the equivalent transaction results. First, the intermediary group  $\mathcal{G}$  is traversed to obtain the key of each intermediary. Then, the pending transaction set (CKSet) associated with each intermediary is queried based on its key. A map set (ComKeyMap) is constructed to store the new composite keys. Next, the CKSet is traversed, and each composite key is split to obtain its original account's key, the destination account's key, and the transaction amount. Then (lines 7-11), the original account's key and the intermediary's key are combined as a new composite key. Meanwhile, the total amount of the destination account is counted under the ciphertext and used as the value of the new composite key. Finally (lines 12-13), the new composite key is constructed to append a temporary composite key transaction pool (TempComKeyPool).

**Composite key regeneration.** (Lines 14-17) Intermediary  $g_j$  updates ComKeyPool based on the result of the summarization phase, i.e., TempComKeyPool. After validation by other intermediaries, the new ComKeyPool is broadcast. Each user who receives it can delete the previously outdated ComKeyPool and update it to the latest equivalent.

#### F. Ideas for Extension to Other Blockchains

Further, we discuss ideas for applying HiCoCS to other blockchains. While our main focus is on solving the problem in Hyperledger Fabric, it proposes a way to mitigate the problem of cross-shard transaction conflicts in permissioned

#### Algorithm 2: Composite Key Reuse Algorithm.

**Input:** The current composite key transaction pool ComKeyPool1, the intermediary group  $\mathcal{G}$   
**Output:** The equivalent composite key transaction pool after reusing updates ComKeyPool

```

1 Function ckReuse (·):
2   for  $j = 0$  to  $|\mathcal{G}| - 1$  do
3     // Composite key summarization
4     // Query the pending transaction set
5     CKSet  $\leftarrow$  queryCompositeKeyByPartial ( $g_j$ , ComKeyPool)
6     ComKeyMap =  $\emptyset$ 
7     for  $i = 0$  to  $|\text{CKSet}| - 1$  do
8        $\_, O_i, D_i, V_i \leftarrow \text{SplitCompositeKey}(CK_i)$ 
9        $CK_{New_i} \leftarrow g_j \sim O_i$  //  $\sim$ : A concatenator
10      if IsExist ( $D_i$ , ComKeyMap) then
11        ComKeyMap[ $D_i$ ] +=  $V_i$ 
12      else
13        ComKeyMap[ $D_i$ ] =  $V_i$ 
14      // Construct new composite keys
15      TempCK $_j \leftarrow \text{createCKNew}(CK_{New_i}, \text{ComKeyMap})$ 
16      TempComKeyPool.add (TempCK $_j$ )
17      // Composite key regeneration
18      for  $i = 0$  to  $|\text{ComKeyPool}| - 1$  do
19        delete ( $CK_i$ )
20      ComKeyPool  $\leftarrow$  TempComKeyPool
21      destroy (TempComKeyPool)
22   return ComKeyPool

```

#### Solidity code 1: Composite Key Implementation Example.

```

// CSTx structure
1 struct CSTx {
2   address intermediary;
3   address initiator;
4   address receiver;
5   string amountC; // Amount ciphertext
6 }
// Data mapping
7 mapping (string  $\Rightarrow$  CSTx) private cstxs;
// Composite key creation
8 function createCompositeKey (string memory objectType,
9   address intermediary, address initiator, address receiver,
10  string memory amountC) public {
11   string memory CK = abi.encodePacked (objectType, "|",
12     intermediary, "|", initiator, "|", receiver, "|", amountC);
13   cstxs[CK] = CSTx (intermediary, initiator, receiver, amountC);
14 }
// Composite key query
15 function queryCompositeKey (string memory CK)
16   public view returns (CSTx memory) {
17   require (cstxs[CK].initiator != address (0), "CSTx does
18     not exist.");
19   return cstxs[CK];
20 }

```

blockchain systems. We also consider that similar techniques and approaches can be applied in other blockchain systems, and thus, HiCoCS has a certain degree of generalizability.

Rich Web3 applications need to be served by different types of blockchains. Our vision is to design HiCoCS as a generalized cross-sharding middleware. Thus, HiCoCS

needs to provide an easily scalable paradigm. Though only Hyperledger Fabric's chaincode currently provides the APIs for composite keys, other blockchains can implement similar functionality. As long as the blockchain smart contract can implement the composite key, then HiCoCS can be deployed on it. For example, EEA<sup>2</sup> and ChainMaker<sup>3</sup> are the mainstream enterprise-grade permissionless and permissioned blockchains, respectively. They both support the Solidity language for developing smart contracts. We provide a simplified example, as shown in Solidity code 1. First (lines 1-6), the data structure associated with the composite key and CSTx is defined. We use a mapping to store the data related to the composite key (line 7). Then, insert the concatenator “|” between each of the two attributes to create the composite key (line 9). Finally (lines 12-15), a query composite key function is shown.

## VI. SECURITY ANALYSIS

In this section, we briefly analyze the security of HiCoCS with respect to the stated threats in Section IV-B and the security goals in Section IV-C.

### A. Data Confidentiality

**Theorem 1:** In HiCoCS, for all cross-shard transactions, there is no probabilistic polynomial time (PPT) attacker  $\mathcal{A}$  can spoof as an intermediary to successfully extract or infer transaction amount privacy information from the intercepted data.

*Proof:* HiCoCS uses the AES encryption algorithm to encrypt and pre-process the transmission of cross-shard transactions, and there is no unauthorized entity (including intermediaries) can decrypt the message without the key. Further, HiCoCS performs fully homomorphic encryption computation on the cross-shard transactions using the CKKS encryption algorithm. According to the security properties of the CKKS encryption algorithm [38], the intermediary can only operate in the ciphertext space when processing transactions. Due to the use of Fabric's private data collection to manage the keys, even in the face of a passive attack [45], attacker  $\mathcal{A}$  cannot crack the private key by algebraic operations based on the hints and does not have the prerequisites to crack the private key. Thus, HiCoCS ensures that even in the existence of attacker  $\mathcal{A}$ , the semi-trusted intermediary cannot directly or indirectly obtain the plaintext transaction amount data.  $\square$

As HiCoCS provides data confidentiality, the threats of *spoofing*, *tampering*, *information disclosure*, and *elevation of privilege* are effectively defended against.

### B. Transaction Atomicity

**Theorem 2:** The cross-shard transactions in HiCoCS satisfy eventual atomicity, including the conditions that (i) if a cross-shard transaction is successfully executed, the states of the sharding ledgers involved in the transaction are consistent, and (ii) if a cross-shard transaction fails to execute, it must be rolled back on the involved shards.

*Proof:* HiCoCS uses a message-passing approach to process cross-shard transactions to guarantee atomicity. Specifically, HiCoCS collects transactions through a composite key transaction pool and then processes transactions in batches in the source and target channels. This means that the execution of transactions does not immediately satisfy atomicity. Only when the target channel listens for all sending transactions to be confirmed and executed and the final settlement performed is atomicity finally achieved. While this approach does not require immediate atomicity, it guarantees eventual atomicity [6], [11]. Regardless of the circumstances, HiCoCS will eventually ensure that cross-shard transactions are either completed successfully and result in consistent state changes or are rolled back to prevent any partial or inconsistent outcomes. Due to the uniqueness of the composite key corresponding to a transaction, the system can precisely roll back invalid transactions and their dependencies. Thus, HiCoCS ensures that cross-shard transactions satisfy eventual atomicity.  $\square$

Existing cross-sharding schemes [8], [10] achieve strong atomicity based on a two-phase commit protocol. It is unsuitable for high concurrency scenarios as a locking mechanism can seriously affect performance. Thus, HiCoCS employs the message-passing method to guarantee the eventual atomicity, mitigating the threat of *repudiation*.

### C. Service Availability

**Theorem 3:** HiCoCS ensures high service availability by deploying an intermediary group  $\mathcal{G}$  to provide cross-shard transaction services to ensure that the system can still provide services in the face of disruptions or attacks.

*Proof:* In the HiCoCS architecture, multiple intermediary nodes work together to participate in the highly concurrent processing of transactions, and even if some nodes are attacked or fail, at least one node  $g_j \in \mathcal{G}$  can still take over their work and keep the system running normally. This design effectively spreads the risk and reduces the possibility of a single point of failure, thus ensuring the service availability of the system.  $\square$

Thus, HiCoCS can effectively resist *denial of service* threats and fulfill high availability requirements.

## VII. PERFORMANCE EVALUATION

### A. Settings

**Experimental prototype.** We use Golang in Hyperledger Fabric v2.4<sup>4</sup> to develop and implement a HiCoCS prototype. It leverages Hyperledger Fabric's multi-channel architecture to construct a scalable, multi-shard network comprising up to 128 nodes across 32 shards. We utilize Docker containers<sup>5</sup> as the execution environment for smart contracts. We are going to open-source the code<sup>6</sup> following the paper's acceptance.

**Testbed.** We evaluate the performance of the prototype on a machine with an Intel i7-13700 CPU and 128GB of RAM. Fabric's BatchTimeout is set to 2 seconds. We adjust the

<sup>2</sup> Enterprise Ethereum Alliance (EEA), <https://entethalliance.org>

<sup>3</sup> ChainMaker, <https://chainmaker.org.cn>

<sup>4</sup> <https://github.com/hyperledger/fabric/tree/release-2.4>

<sup>5</sup> <https://github.com/jenkinsci/docker>

<sup>6</sup> <https://github.com/cwf1999/HiCoCS>

block size setting from 10 MB to 160 MB. We evaluate the performance of HiCoCS with and without homomorphic encryption enabled for privacy preservation in concurrent cross-shard trading scenarios (with 1,000 concurrent threads). The transfer amounts for CSTxs are randomly selected from positive real numbers in blocks collected from the Ethereum blockchain (block height: 9,000,000-10,000,000). To model the system's transaction conflicts, we adopt both active and passive approaches: (i) *Active*. Keeping the block size constant, we vary the skewness  $f$  of the generated transactions, i.e., the proportion of CSTxs processed through the same intermediary account. (ii) *Passive*. Fixing the skewness  $f$ , we vary the block size, and transactions are transferred among randomly selected participants. Changing the block size indirectly controls the probability of transaction conflicts within a block.

### B. Baselines and Metrics

**Baselines.** We compare HiCoCS with three baselines: an implemented vanilla version, and two simulated state-of-the-art 2PL/OCC sharding schemes. (i) *Vanilla version*. Since HiCoCS is the first scheme to propose high concurrency cross-sharding on Hyperledger Fabric, we compare its vanilla version as a baseline. The concept is introduced in Section I. (ii) *AHL+* [29]. This scheme ensures the consistency and atomicity of CSTxs by locking resources and reaching agreements across committees through a 2PL protocol. (iii) *Meepo* [33]. It reduces transaction conflicts and enhances communication efficiency by introducing cross-epoch and cross-call protocols for ordered cross-shard communication (i.e., OCC) between blocks.

**Metrics.** We measure the performance of HiCoCS using the following metrics. (i) *Transaction success rate (TSR)*. The percentage of successfully executed transactions out of the total number of initiated transactions. This is a key metric to measure the system's ability of conflict resolution in highly concurrent CSTx scenarios, because in the worst case, only the first CSTx in a block may be successful and all other CSTxs are aborted due to concurrent data conflicts. (ii) *Transaction throughput*. The number of transactions per second (TPS) successfully processed by the system. This is also an important measure of concurrency capacity. (iii) *Transaction latency*. The time taken by the user from the initiation of a CSTx to the final successful write to the ledger. (iv) *CPU & memory utilization*. The percentage of CPU and memory resources utilized by the system during operation.

### C. Evaluation Results

**High concurrency testing.** The focus of our work is on resolving highly concurrent conflicts in CSTxs. Thus, we first present the system's performance without enabling the homomorphic encryption module for privacy preservation. To evaluate HiCoCS and the baselines' ability to handle transaction conflicts, we measure the transaction success rate and average throughput by actively and passively introducing conflicts during testing. We then evaluate the energy efficiency of concurrent transactions and the dynamic performance under varying numbers of highly concurrent transactions.

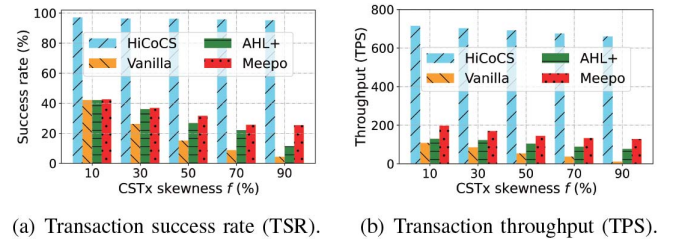


Fig. 9. Comparison of concurrency performance under varying skewness  $f$ .

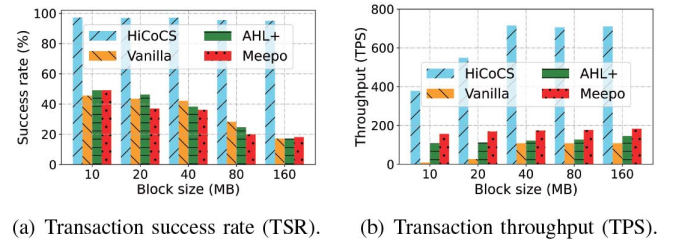


Fig. 10. Comparison of concurrency performance under varying block sizes.

1) *Active test results*: We fix the block size at 40 MB and change the transaction skewness  $f$  to perform transaction conflict testing. Fig. 9 shows the influence of skewness  $f$  on concurrent transactions. The results of Fig. 9(a) indicate that all baseline transaction success rates decrease as skewness  $f$  increases. However, HiCoCS experiences minimal decrease, stabilizing above 95%. HiCoCS improves TSR by an average factor of 2.2 to 8.1 compared to the baselines. We analyze that as skewness  $f$  increases, HiCoCS generates more composite keys for the intermediaries of high-frequency services, thereby minimizing the increase in transaction conflict rates. In contrast, the baselines experience more transaction aborts due to competitive conditions. Fig. 9(b) further illustrates the comparison of average throughput. It is observed that the throughput of all schemes decreases as skewness  $f$  increases. However, HiCoCS improves in TPS by an average of 3.5 to 20.2 times compared to the baselines. This occurs because the baselines experience a significant number of transaction retries as transaction aborts increase. HiCoCS effectively mitigates concurrency conflicts by using virtual sub-brokers.

2) *Passive test results*: We set the skewness  $f$  to 10% and vary the block size for passive conflict testing. Fig. 10 illustrates the impact of different block sizes. Fig. 10(a) demonstrates that the baseline transaction success rates decrease as block size increases. However, similar to the active test, HiCoCS experiences almost no decrease. On average, HiCoCS improves TSR by a factor of 2.1 to 2.3 compared to the baselines. This aligns with expectations, as larger blocks increase the probability of CSTx conflicts; however, HiCoCS pre-processes concurrent transactions to minimize conflict occurrences, effectively avoiding most of them. Fig. 10(b) illustrates that TPS increases across all schemes as block size increases. This is consistent with expectations, as larger blocks reduce the frequency of network



TABLE II  
 COMPARISON OF CONCURRENT ENERGY EFFICIENCY  
 (CPU & MEMORY UTILIZATIONS, UNIT:%)

Skewness	10	30	50	70	90
HiCoCS	55.6 & 58.2	62.5 & 66.4	75.4 & 71.2	87.9 & 76.8	90.3 & 80.1
Vanilla	72.1 & 75.0	78.9 & 82.4	87.9 & 88.0	95.4 & 91.3	98.5 & 93.7
AHL+	68.5 & 71.2	75.6 & 79.1	84.5 & 85.2	93.1 & 89.8	97.0 & 92.1
Meppo	64.1 & 67.9	71.8 & 76.1	81.3 & 82.9	90.4 & 87.2	94.0 & 90.3

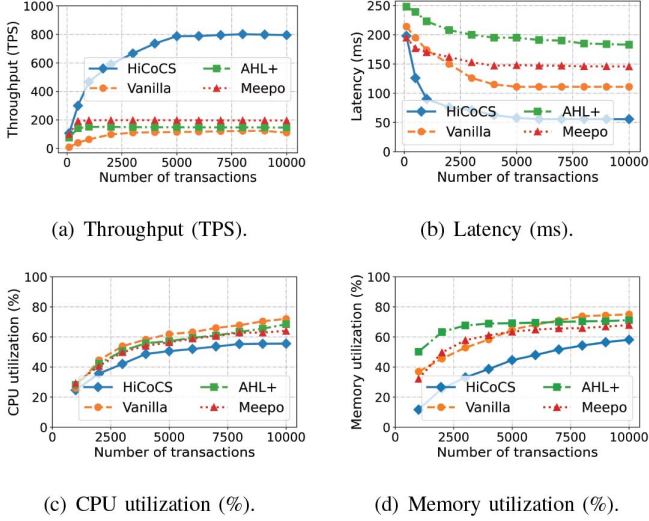


Fig. 11. Dynamic performance comparison for varying numbers of transactions.

communications. On average, HiCoCS improves throughput by a factor of 2.5 to 15.7 compared to the baselines.

3) *Concurrent energy efficiency results:* Table II presents the average CPU and memory usage of different schemes for each shard pair under the load of 10,000 highly concurrent transactions, with a block size of 40 MB and varying skewness. Overall, the resource overhead of all schemes increases as skewness increases. However, HiCoCS reduces CPU and memory consumption by an average of 8.0% to 14.8% and 12.9% to 18.3%, respectively, compared to the baselines. This reflects, on the one hand, the efficiency advantage of HiCoCS in handling highly concurrent transaction conflicts without overloading due to frequent transaction reissuance. On the other hand, it also demonstrates the optimization of resource allocation enabled by composite key reuse in HiCoCS.

4) *Dynamic performance results:* We further compare the dynamic performance of HiCoCS and the baselines under varying numbers of highly concurrent transactions. The skewness  $f$  is set to 10%, and the block size is fixed at 40 MB. Fig. 11 shows the variation in transaction throughput, latency, and CPU & memory utilization. The results of Fig. 11(a) indicate that the throughput of HiCoCS only begins to level off when transaction volume is larger compared to the baselines, demonstrating HiCoCS's stronger concurrent transaction processing capability. Fig. 11(b) shows that the average transaction latency of HiCoCS is 43.9%-62.0% lower than that of the baselines. This reflects HiCoCS's high efficiency in batch processing transactions.

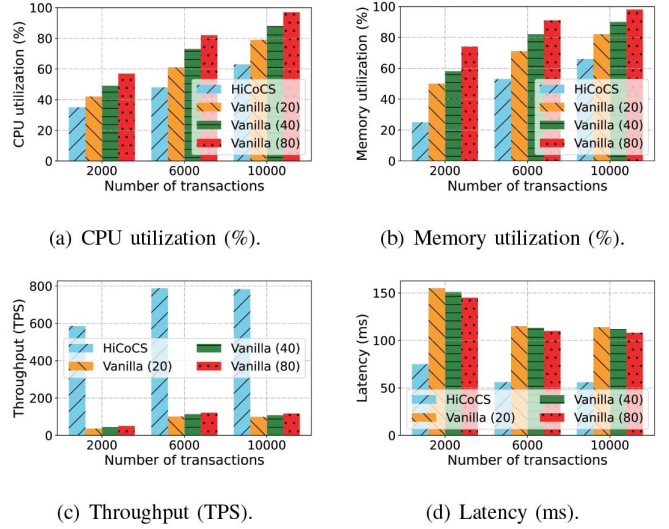


Fig. 12. A quantitative comparison of system overhead and performance between using composite keys and adding intermediaries.

Fig. 11(c) and 11(d) show that CPU and memory utilization in HiCoCS are 12.4%-18.0% and 31.6%-38.5% lower than those of the baselines, respectively. This demonstrates HiCoCS's superiority in terms of resource utilization.

**Composite key testing.** First, we quantitatively test composite keys to compare the system overhead and performance when using composite keys versus adding new intermediaries. Next, we tested the memory consumption and query time before and after composite key reuse to verify its effectiveness.

1) *Quantitative test and analysis:* The default setting for the intermediary group  $\mathcal{G}$  between each shard pair consists of 20 accounts providing cross-shard trading services. We vary the vanilla version's size of  $\mathcal{G}$  to 40 and 80 to compare it with HiCoCS. The skewness  $f$  is set to 30%, and HiCoCS generates and reuses composite keys based on conflicting transactions. Fig. 12(a) and 12(b) present the comparative results of CPU and memory utilization for varying numbers of transactions. The results indicate that HiCoCS reduces CPU and memory usage by an average of 19.4%-38.4% and 31.6%-46.9%, respectively, compared to the method of adding intermediaries. We analyze this because the effect of adding a virtual sub-broker is nearly equivalent to that of adding a new intermediary. However, the former incurs minimal memory overhead, whereas the latter introduces significant overhead for authentication, account creation & maintenance, and transaction processing scheduling. Thus, this test validates that HiCoCS's approach of using virtual sub-brokers is more efficient than adding new intermediaries. Fig. 12(c) and 12(d) present the comparative results for average transaction throughput and latency. The results in Fig. 12(c) indicate that adding intermediaries can slightly improve throughput. This is because contention conflicts among intermediaries remain severe under highly concurrent transactions. HiCoCS demonstrates an average improvement of 7.3 to 9.7 times in throughput compared to the method of adding intermediaries. The results in Fig. 12(d) indicate that adding intermediaries slightly reduces latency due to the reduction in conflict locking

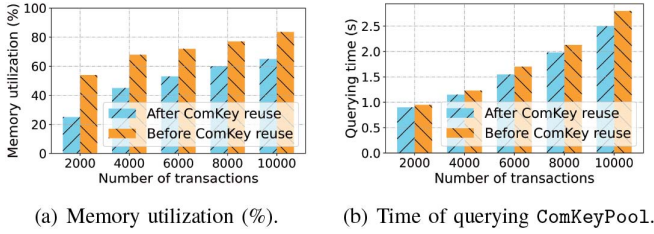


Fig. 13. Performance comparison before and after composite key reuse optimization in HiCoCS.

time. HiCoCS reduces latency by an average of 48.5% to 51.3% compared to them.

2) *Reuse effectiveness test*: The number of composite keys primarily affects system memory usage. Fig. 13(a) presents the results of memory utilization before and after composite key optimization, showing that memory utilization gradually increases and stabilizes as the number of CSTx increases. However, memory utilization decreases significantly after optimization. The average memory utilization of the scheme with composite key reuse enabled is reduced by 31.6%. The time taken for the intermediary to query the ComKeyPool before and after composite key reuse optimization is shown in Fig. 13(b). As the number of CSTx increases, the time taken by the intermediary to query the ComKeyPool also increases. This is because more composite keys are created within ComKeyPool, expanding the range of the intermediary's fuzzy query and consequently increasing query time. After composite key reuse optimization, the average query time for CSTx is reduced by 8.3%.

**Privacy preservation-enabled testing.** We first evaluate the impact on system performance after enabling the privacy-preserving mechanism, followed by an evaluation of the performance changes after scaling the sharded network. Finally, we evaluate the results of ciphertext computation.

1) *Performance impact of FHE*: Fig. 14 shows the performance change of the system before and after adding the privacy-preserving mechanism (i.e., FHE). The results of Fig. 14(a) HiCoCS throughput decreases by an average of 19.5% due to the series of encryption operations after FHE is enabled. However, compared to the vanilla version, throughput still improves by 5.7 times. HiCoCS (with FHE) throughput reaches 702.3 TPS when the number of transactions reaches 8,000, and then stabilizes due to machine performance limitations. Fig. 14(b) shows the impact of privacy preservation on system latency. The maximum latency of HiCoCS (with FHE) is 203.2 ms, and the average latency is 118.7 ms, representing a 32.6% increase compared to HiCoCS (without FHE), which has an average latency of 80.0 ms. However, compared to the vanilla version, latency in HiCoCS (with FHE) is still reduced by an average of 13.2%. The average processing latency of the system decreases as transaction volume increases because the number of concurrent transactions processed per unit of time increases, and latency stabilizes after the system reaches its processing limit.

2) *Network scaling test*: The default test environment is conducted in a 16-shard, 64-node network to avoid reaching the

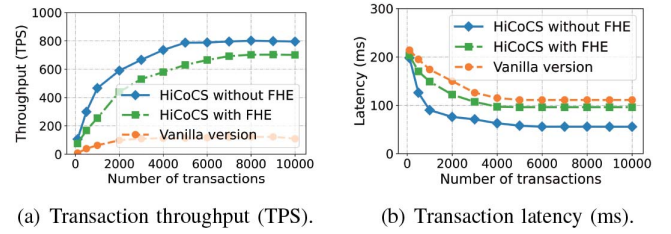


Fig. 14. Performance comparison of HiCoCS before and after enabling privacy-preserving mechanism (under the 16-shard, 64-node network).

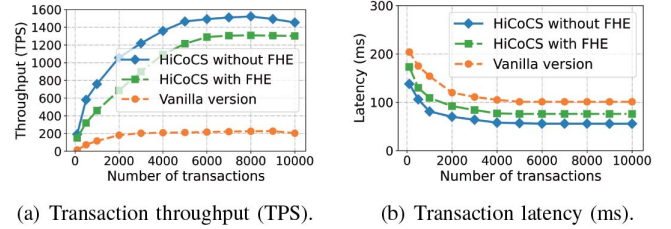


Fig. 15. Performance comparison of HiCoCS before and after enabling privacy-preserving mechanism (under the 32-shard, 128-node network).

machine performance bottleneck. To evaluate the scalability of the overall HiCoCS scheme, we present the scaling results in a 32-shard, 128-node network in Fig. 15. In this larger network, as shown in Fig. 15(a), compared to previous test results in a 16-shard, 64-node network, the throughput exhibits a nearly twofold linear growth trend. This indicates that HiCoCS demonstrates good scalability with all building blocks enabled, processing more transactions securely in parallel. Fig. 15(b) shows transaction latency in the 32-shard, 128-node network, and the results indicate that HiCoCS latency is reduced by an average of 21.3% compared to the 16-shard, 64-node network. We analyze that although increasing the number of shards distributes the network's transaction load and speeds up transaction processing within each shard, it also increases communication latency due to the greater number of cross-shard transactions. HiCoCS is more resource-efficient than the vanilla version, leading to a more significant reduction in transaction latency.

3) *Ciphertext calculation results*: To ensure the accuracy of the ciphertext calculation, we evaluate the gap between the approximate CKKS ciphertext homomorphic computations and the actual calculated values. We randomly initiated 10,000 CSTxs, with their transaction amounts encrypted using CKKS, before entering the ciphertext summation. Finally, we decrypt the summation ciphertext results and compare them with the summation results of the original data. The results show that the error rate is within  $10^{-5}$  compared to the actual transaction amounts. In practice, this error can be ignored or offset by the transaction fee.

## VIII. CONCLUSION

This paper proposes HiCoCS, the first Hyperledger Fabric-based implementation of cross-shard transaction middleware featuring high concurrency and privacy preservation. We utilize

composite keys to build virtual sub-brokers for intermediaries in the vanilla version to mitigate concurrent transaction conflicts. We also consider composite key reuse to their number and lower system overhead. HiCoCS utilizes fully homomorphic encryption to ensure the privacy preservation of intermediaries in cross-shard transactions. Our evaluation of the developed prototype demonstrates that HiCoCS outperforms the vanilla version and state-of-the-art schemes across all metrics. In future work, we plan to enhance the generality of HiCoCS and extend this work to more blockchains and a wide range of Web3 applications.

## REFERENCES

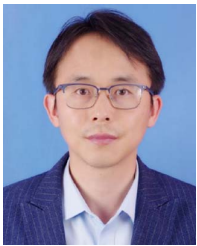
- [1] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Proc. IEEE Int. Congr. Big Data (BigData Congr.)*. Piscataway, NJ, USA: IEEE Press, 2017, pp. 557–564.
- [2] X. Zhu, J. Zheng, B. Ren, X. Dong, and Y. Shen, "Microthingschain: Blockchain-based controlled data sharing platform in multi-domain IOT," *J. Netw. Netw. Appl.*, 2021.
- [3] W. Tong et al., "Ti-biov: Traffic information interaction for blockchain-based iov with trust and incentive," *IEEE Internet Things J.*, vol. 10, no. 24, pp. 21528–21543, Dec. 2023.
- [4] L. Yang et al., "Asyncsc: An asynchronous sidechain for multi-domain data exchange in internet of things," in *Proc. IEEE INFOCOM 2025-IEEE Conf. Comput. Commun.*, 2025.
- [5] L. Yang et al., "Optimal hub placement and deadlock-free routing for payment channel network scalability," in *Proc. IEEE 43th Int. Conf. Distrib. Comput. Syst. (ICDCS)*. Piscataway, NJ, USA: IEEE Press, 2023.
- [6] H. Huang et al., "Brokerchain: A cross-shard blockchain protocol for account/balance-based state sharding," in *Proc. IEEE INFOCOM 2022-IEEE Conf. Comput. Commun.*, 2022, pp. 1968–1977.
- [7] L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, and P. Saxena, "A secure sharding protocol for open blockchains," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2016, pp. 17–30.
- [8] E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, E. Syta, and B. Ford, "Omniledger: A secure, scale-out, decentralized ledger via sharding," in *Proc. IEEE Symp. Secur. Privacy (SP)*. Piscataway, NJ, USA: IEEE Press, 2018, pp. 583–598.
- [9] M. Zamani, M. Movahedi, and M. Raykova, "Rapidchain: Scaling blockchain via full sharding," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2018, pp. 931–948.
- [10] M. Al-Bassam, A. Sonnino, S. Bano, D. Hryczyszyn, and G. Danezis, "Chainspace: A sharded smart contracts platform," in *Proc. Netw. Distrib. Syst. Secur. Symp.*, 2018.
- [11] J. Wang and H. Wang, "Monoxide: Scale out blockchains with asynchronous consensus zones," in *Proc. 16th USENIX Symp. Networked Syst. Des. implement. (NSDI)*, 2019, pp. 95–112.
- [12] Z. Hong, S. Guo, P. Li, and W. Chen, "Pyramid: A layered sharding blockchain system," in *Proc. IEEE INFOCOM 2021-IEEE Conf. Comput. Commun.*, 2021, pp. 1–10.
- [13] M. Li, Y. Lin, J. Zhang, and W. Wang, "Cochain: High concurrency blockchain sharding via consensus on consensus," in *Proc. IEEE INFOCOM 2023-IEEE Conf. Comput. Commun.*, 2023.
- [14] E. Androulaki, A. Barger, V. Bortnikov, and C. Cachin, "Hyperledger fabric: A distributed operating system for permissioned blockchains," in *Proc. 13th EuroSys Conf.*, 2018, pp. 1–15.
- [15] W. Tong, X. Dong, Y. Shen, and X. Jiang, "A hierarchical sharding protocol for multi-domain IoT blockchains," in *Proc. IEEE Int. Conf. Commun.*. Piscataway, NJ, USA: IEEE Press, 2019, pp. 1–6.
- [16] Z. Hong, S. Guo, and P. Li, "Scaling blockchain via layered sharding," *IEEE J. Sel. Areas Commun.*, vol. 40, no. 12, pp. 3575–3588, 2022.
- [17] Z. Cai et al., "Benzene: Scaling blockchain with cooperation-based sharding," *IEEE Trans. Parallel Distrib. Syst.*, vol. 34, no. 2, pp. 639–654, 2022.
- [18] Z. Peng et al., "Neuchain: A fast permissioned blockchain system with deterministic ordering," *Proc. VLDB Endowment*, vol. 15, no. 11, pp. 2585–2598, 2022.
- [19] Z. Hong et al., "Prophet: Conflict-free sharding blockchain via byzantine-tolerant deterministic ordering," in *Proc. IEEE INFOCOM-IEEE Conf. Comput. Commun.*, 2023.
- [20] C. Li et al., "Achieving scalability and load balance across blockchain shards for state sharding," in *Proc. 41st Int. Symp. Reliable Distrib. Syst. (SRDS)*. Piscataway, NJ, USA: IEEE Press, 2022, pp. 284–294.
- [21] Y. Liu et al., "A flexible sharding blockchain protocol based on cross-shard byzantine fault tolerance," *IEEE Trans. Inf. Forensics Secur.*, vol. 18, pp. 2276–2291, 2023.
- [22] Z. Hong, S. Guo, E. Zhou, W. Chen, H. Huang, and A. Zomaya, "Gridb: Scaling blockchain database via sharding and off-chain cross-shard mechanism," *Proc. VLDB Endowment*, vol. 16, no. 7, pp. 1685–1698, 2023.
- [23] X. Qi and Y. Li, "Lightcross: Sharding with lightweight cross-shard execution for smart contracts," in *Proc. IEEE INFOCOM-IEEE Conf. Comput. Commun.*, 2024, pp. 1681–1690.
- [24] J. Xu, Y. Ming, Z. Wu, C. Wang, and X. Jia, "X-shard: Optimistic cross-shard transaction processing for sharding-based blockchains," *IEEE Trans. Parallel Distrib. Syst.*, vol. 35, no. 4, pp. 548–559, Apr. 2024.
- [25] S. Jiang, J. Cao, C. L. Tung, Y. Wang, and S. Wang, "Sharon: Secure and efficient cross-shard transaction processing via shard rotation," in *Proc. IEEE INFOCOM-IEEE Conf. Comput. Commun.*, 2024, pp. 2418–2427.
- [26] M. M. Al Bara, S. Li, C. Du, Y. T. Hou, and W. Lou, "Sok: Public blockchain sharding," in *Proc. IEEE Int. Conf. Blockchain Cryptocurrency (ICBC)*. Piscataway, NJ, USA: IEEE Press, 2024, pp. 766–783.
- [27] S. Muro, T. Kameda, and T. Minoura, "Multi-version concurrency control scheme for a database system," *J. Comput. Syst. Sci.*, vol. 29, no. 2, pp. 207–224, 1984.
- [28] Y. Wu, J. Arulraj, J. Lin, R. Xian, and A. Pavlo, "An empirical evaluation of in-memory multi-version concurrency control," *Proc. VLDB Endowment*, vol. 10, no. 7, pp. 781–792, 2017.
- [29] H. Dang, T. T. A. Dinh, D. Loghin, E.-C. Chang, Q. Lin, and B. C. Ooi, "Towards scaling blockchain systems via sharding," in *Proc. Int. Conf. Manage. Data*, 2019, pp. 123–140.
- [30] P. Zheng et al., "Aeolus: Distributed execution of permissioned blockchain transactions via state sharding," *IEEE Trans. Ind. Inform.*, vol. 18, no. 12, pp. 9227–9238, 2022.
- [31] S. K. Set and G. S. Park, "Service-aware dynamic sharding approach for scalable blockchain," *IEEE Trans. Serv. Comput.*, vol. 16, no. 4, pp. 2954–2969, 2022.
- [32] E. Androulaki, C. Cachin, A. De Caro, and E. Kokoris-Kogias, "Channels: Horizontal scaling and confidentiality on permissioned blockchains," in *Proc. Comput. Secur.: 23rd Eur. Symp. Res. Comput. Secur.*, 2018, pp. 111–131.
- [33] P. Zheng, Q. Xu, Z. Zheng, Z. Zhou, Y. Yan, and H. Zhang, "Meepo: Multiple execution environments per organization in sharded consortium blockchain," *IEEE J. Sel. Areas Commun.*, vol. 40, no. 12, pp. 3562–3574, Dec. 2022.
- [34] Y. Sismanis, P. Brown, P. J. Haas, and B. Reinwald, "Gordian: Efficient and scalable discovery of composite keys," in *Proc. 32nd Int. Conf. Very Large Data Bases (VLDB)*. VLDB Endowment, 2006, pp. 691–702.
- [35] A. Acar, H. Aksu, A. S. Uluagac, and M. Conti, "A survey on homomorphic encryption schemes: Theory and implementation," *ACM Comput. Surveys (CSUR)*, vol. 51, no. 4, pp. 1–35, 2018.
- [36] S. Yaji, K. Bangera, and B. Neelima, "Privacy preserving in blockchain based on partial homomorphic encryption system for ai applications," in *Proc. IEEE 25th Int. Conf. High Perform. Comput. Workshops (HiPCW)*. Piscataway, NJ, USA: IEEE Press, 2018, pp. 81–85.
- [37] Y. Shoukry et al., "Privacy-aware quadratic optimization using partially homomorphic encryption," in *Proc. IEEE 55th Conf. Decis. Control (CDC)*. Piscataway, NJ, USA: IEEE Press, 2016, pp. 5053–5058.
- [38] J. H. Cheon, A. Kim, M. Kim, and Y. Song, "Homomorphic encryption for arithmetic of approximate numbers," in *Adv. Cryptol. (ASIACRYPT): 23rd Int. Conf. Theory Appl. Cryptol. Inf. Secur.*, 2017, pp. 409–437.
- [39] A. Shostack, "Experiences threat modeling at microsoft," *MODSEC@MoDELS*, vol. 2008, p. 35, 2008.
- [40] R. F. Hayat, S. Aurangzeb, and M. Aleem, "ML-DDoS: A blockchain-based multilevel DDoS mitigation mechanism for IoT environments," *IEEE Trans. Eng. Manage.*, vol. 71, pp. 12605–12618, 2024.
- [41] D. Selent, "Advanced encryption standard," *Rivier Academic J.*, vol. 6, no. 2, pp. 1–14, 2010.
- [42] L. Wu et al., "Towards understanding and demystifying bitcoin mixing services," in *Proc. Web Conf.*, 2021, pp. 33–44.
- [43] P. Zheng, Z. Zheng, X. Luo, X. Chen, and X. Liu, "A detailed and real-time performance monitoring framework for blockchain systems," in *Proc. 40th Int. Conf. Softw. Eng.: Softw. Eng. Pract.*, 2018, pp. 134–143.



- [44] D. Chatzopoulos, S. Gujar, B. Faltings, and P. Hui, "Mneme: A mobile distributed ledger," in *Proc. IEEE INFOCOM-IEEE Conf. Comput. Commun.*, 2020, pp. 1897–1906.
- [45] B. Li and D. Micciancio, "On the security of homomorphic encryption on approximate numbers," in *Proc. Adv. Cryptol. (EUROCRYPT): 40th Annu. Int. Conf. Theory Appl. Cryptogr. Techn.*, Zagreb, Croatia, Part I 40. New York: Springer, 2021, pp. 648–677.



**Lingxiao Yang** (Graduate Student Member, IEEE) received the B.E. degree in network engineering from Xidian University, in 2018. He is currently working toward the Ph.D. degree with the School of Computer Science and Technology, Xidian University, Xi'an, China. He is a member of the Shaanxi Key Laboratory of Network and System Security. His research interests include Web3 and blockchain applications.



**Xuewen Dong** (Member, IEEE) received the B.E., M.S., and Ph.D. degrees in computer science and technology from Xidian University, Xi'an, China, in 2003, 2006, and 2011, respectively. From 2016 to 2017, he was a Visiting Scholar with Oklahoma State University, Stillwater, OK, USA. Currently, he is a Professor with the School of Computer Science and Technology, Xidian University. His research interests include blockchain and smart system security.



**Zhiguo Wan** (Senior Member, IEEE) is currently a Principal Investigator with Zhejiang Lab, Hangzhou, Zhejiang, China. He is a senior member of China Computer Federation (CCF). His main research interests include security and privacy for distributed systems, such as cloud computing, Internet of Things, and blockchain. He has led four projects funded by the National Natural Science Foundation of China (NSFC) and the Major Basic Research Program of Shandong Provincial Natural Science Foundation. He published over 100 academic papers, including those in top international conferences and journals such as IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, IEEE TRANSACTIONS ON MOBILE COMPUTING, and IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS. His works have been cited over 5000 times according to Google Scholar, with a single paper cited more than 700 times. He received the Second Prize of the Zhejiang Provincial Science and Technology Progress Award, in 2022.



**Di Lu** (Member, IEEE) received the B.S., M.S., and Ph.D. degrees in computer science and technology from Xidian University, China, in 2006, 2009, and 2014, respectively. Currently, he is an Associate Professor with the School of Computer Science and Technology, Xidian University. His research interests include trusted computing, cloud computing, system, and network security.



**Yushu Zhang** (Senior Member, IEEE) received the Ph.D. degree in computer science from Chongqing University, Chongqing, China, in 2014. He held various research positions with the City University of Hong Kong; Southwest University; University of Macau; Deakin University; and Nanjing University of Aeronautics and Astronautics. Currently, he is a Professor with the School of Computing and Artificial Intelligence, Jiangxi University of Finance and Economics; and Jiangxi Provincial Key Laboratory of Multimedia Intelligent Processing, Nanchang, China. His research interests include multimedia processing and security, artificial intelligence, and blockchain.



**Yulong Shen** (Member, IEEE) received the B.S. and M.S. degrees in computer science and the Ph.D. degree in cryptography from Xidian University, Xi'an, China, in 2002, 2005, and 2008, respectively. Currently, he is a Professor with the School of Computer Science and Technology, Xidian University, where he is also an Associate Director of the Shaanxi Key Laboratory of Network and System Security and a member of the State Key Laboratory of Integrated Services Networks. His research interests include wireless network security and cloud computing security. He has also served on the technical program committees of several international conferences.