Efficient Concurrent Execution of Smart Contracts in Blockchains using Object-based Transactional Memory

Parwat Singh Anjana1, Hagit Attiya2, Sweta Kumari2, Sathya Peri1, and Archit Somani2

1 Department of Computer Science & Engineering, IIT Hyderabad, India
   cs17mtech11014@iith.ac.in, sathya_p@cse.iith.ac.in
2 Department of Computer Science, Technion, Israel
   (hagit, sweta, archit)@cs.technion.ac.il

Abstract. Several popular blockchains such as Ethereum execute complex transactions through user-defined scripts. A block of the chain typically consists of multiple smart contract transactions (SCTs). To append a block into the blockchain, a miner executes these SCTs. On receiving this block, other nodes act as validators, who re-execute these SCTs as part of the consensus protocol to validate the block. In Ethereum and other blockchains that support cryptocurrencies, a miner gets an incentive every time such a valid block is successfully added to the blockchain. When executing SCTs sequentially, miners and validators fail to harness the power of multiprocessing offered by the prevalence of multi-core processors, thus degrading throughput. By leveraging multiple threads to execute SCTs, we can achieve better efficiency and higher throughput. Recently, Read-Write Software Transactional Memory Systems (RWSTMs) were used for concurrent execution of SCTs. It is known that Object-based STMs (OSTMs), using higher-level objects (such as hash-tables or lists), achieve better throughput as compared to RWSTMs. Even greater concurrency can be obtained using Multi-Version OSTMs (MVOSTMs), which maintain multiple versions for each shared data-item as opposed to Single-Version OSTMs (SVOSTMs).

This paper proposes an efficient framework to execute SCTs concurrently based on object semantics, using optimistic SVOSTMs and MVOSTMs. In our framework, a multi-threaded miner constructs a Block Graph (BG), capturing the object-conflicts relations between SCTs, and stores it in the block. Later, validators re-execute the same SCTs concurrently and deterministically relying on this BG.

A malicious miner can modify the BG to harm the blockchain, e.g., to cause double spending. To identify malicious miners, we propose Smart Multi-threaded Validator (SMV). Experimental analysis shows that proposed multi-threaded miner and validator achieve significant performance gains over state-of-the-art SCT execution framework.

* This paper is eligible for Best Student Paper award as Parwat is full-time Ph.D. student.
1 Introduction

Blockchains like Bitcoin [18] and Ethereum [3] have become very popular. Due to their usefulness, they are now considered for automating and securely storing user records such as land sale documents, vehicle, and insurance records. Clients, external users of the system, send requests to nodes to execute on the blockchain, as smart contracts transactions (SCTs). An SCT is similar to the methods of a class in an object-oriented language, which encode business logic relating to the contract [5,9].

Blocks are added to the blockchain by block-creator nodes also known as miners. A miner $m$ packs some number of SCTs received from various (possibly different) clients, to form a block $B$. Then, $m$ executes the SCTs of the block sequentially to obtain the final state of the blockchain, which it stores in the block. To maintain the chain structure, $m$ adds the hash of the previous block to the current block $B$ and proposes this new block to be added to the blockchain.

On receiving the block $B$, every other node acts as a validator. The validators execute a global consensus protocol to decide the order of $B$ in the blockchain. As a part of the consensus protocol, validators validate the contents of $B$. They re-execute all the SCTs of $B$ sequentially to obtain the final state of the blockchain, assuming that $B$ will be added to the blockchain. If the computed final state matches the one stored in $B$ by the miner $m$ then $B$ is accepted by the validators. In this case, the miner $m$ gets an incentive for adding $B$ to the blockchain (in Ethereum and other cryptocurrency-based blockchains). Otherwise, $B$ is rejected, and $m$ does not get any reward. Ethereum follows order-execute model [6], as do several other blockchains such as Bitcoin [18], EOS [2].

Related Work: Dickerson et al. [9] observed that both miner and validators can execute SCTs concurrently and harness the power of multi-core processors. They observed another interesting advantage of concurrent execution of SCTs in Ethereum, where only the miner receives an incentive for adding a valid block while all the validators execute the SCTs in the block. Given a choice, it is natural for a validator to pick a block that supports concurrent execution and hence obtain higher throughput.

Concurrent execution of SCTs poses challenge. Consider a miner $m$ that executes the SCTs in a block concurrently. Later, a validator $v$ may re-execute same SCTs concurrently, in an order that may yield a different final state than given by $m$ in $B$. In this case, $v$ incorrectly rejects the valid block $B$ proposed by $m$. We denote this as False Block Rejection (FBR), noting that FBR may negate the benefits of concurrent execution.

Dickerson et al. [9] proposed a multi-threaded miner algorithm that is based on a pessimistic Software Transactional Memory (STM) and uses locks for synchronization between threads executing SCTs. To avoid FBR, the miner iden-
tifies the dependencies between SCTs in the block while executing them by multiple threads. Two SCTs are dependent if they are conflicting, i.e., both of them access the same data-item and at least one of them is a write. These dependencies among SCTs are recorded in the block in form of a Block Graph (BG). Two SCTs that have a path in the BG are dependent on each other and cannot be executed concurrently. Later, a validator $v$ relies on the BG to identify the dependencies among the SCTs, and concurrently execute SCTs only if there is no path between them in the BG. In the course of the execution by $v$, the size of BG dynamically decreases and the dependencies change. Dickerson et al. [9] use a fork-join approach to execute the SCTs, where a master thread allocates SCTs without dependencies to different slave threads to execute.

Anjana et al. [7] used an optimistic Read-Write STM (RWSTM), which identifies the conflicts between SCTs using timestamps. Those are used by miner threads to build the BG. A validator processes a block using BG in a completely decentralized manner using multiple threads, unlike the centralized fork-join approach of [9]. Each validator thread identifies an independent SCT and executes it concurrently with other threads. They showed that the decentralized approach yields significant performance gains over fork-join [9].

Saraph and Herlihy [21] used a speculative bin approach to execute SCTs of Ethereum in parallel. A miner maintains two bins for storing SCTs: concurrent and sequential. The SCTs are sorted into these bins using read-write locks. The concurrent bin stores non-conflicting SCTs while the sequential bin stores the remaining SCTs. If an SCT $T_i$ requests a lock held by another SCT $T_j$, then $T_i$ is rolled back and placed in the sequential bin. Otherwise, $T_i$ is placed in the concurrent bin. To save the cost of rollback and retries of SCTs, they have used static conflict prediction which identifies conflicting SCTs before executing them speculatively. The multi-threaded validator in this approach executes all the SCTs of the concurrent bin concurrently and then executes the SCTs of the sequential bin sequentially. We call this the Static Bin approach. Zhang and Zhang [24] used multi-version timestamp order (MVTO) for the concurrent execution of SCTs, in a pessimistic manner.

**Exploiting Object-Based Semantics:** The STM-based solution of Anjana et al. [7] and others [24], rely on read-write conflicts (rwconflicts) for synchronization. In contrast, object-based STMs (OSTMs) track higher-level, more advanced conflicts between operations like insert, delete, lookup on a hash-table, enqueue/dequeue on queues, push/pop on the stack [12], [13], [20]. It has been shown in literature that OSTMs provide greater concurrency than RWSTMs (see Fig. 5 in Appendix A). This observation is important since Solidity [5], the language used for writing SCTs for Ethereum, extensively uses a hash-table structure called mapping. This indicates that a hash-table based OSTM is a natural candidate for concurrent execution of these SCTs.

The lock-based solution proposed by Dickerson et al. [9] used abstract locks on hash-table keys, exploiting the object-based semantics with locks. In this

---

1. For clarity, we denote smart contract transactions as SCTs and an STM transaction as a transaction in the paper.
Fig. 1: (a) demonstrates two transactions $T_1$ and $T_2$. Between two $get\_balance()$ (or $get()$) of $T_1$ on account $A_1$ and $A_2$ (initially both accounts maintain $10$ in each), $T_2$ sends money from account $A_1$ to $A_2$. Thus, $T_1$ gets older balance for $A_1$ while newer balance of $A_2$. Hence, it cannot be serialized [19] (or opaque [10]). The corresponding conflict-graph has a cycle as shown in (c). To ensure the correctness, SVOSTMs abort $T_1$, (b) shows the execution using MVOSTM under the same scenario as (a). By maintaining multiple versions, MVOSTM allows transaction $T_1$ to get the older balance for both accounts $A_1$ and $A_2$. Hence, for this execution the equivalent serial schedule is $T_1, T_2$ as shown in (d).

To capture the dependencies between the SCTs in a block, miner threads construct the BG concurrently and append it to the block. The dependencies between the transactions are given by the object-conflicts (oconflicts) (as opposed to rwconflicts) which ensure that the execution is correct, i.e., satisfies conflict-opacity [20]. It has been shown [12,13,20] that there are fewer oconflicts than rwconflicts. Since there are fewer oconflicts, the BG has fewer edges which in turn, allows validators to execute more SCTs concurrently. This also reduces the size of the BG leading to a smaller communication cost.

Multi-version object STMs (MVOSTMs) [16] demonstrate that by maintaining multiple versions for each shared data-item (object), even greater concurrency can be obtained as compared to traditional single-version OSTMs (SVOSTMs). Fig. [1] illustrates the benefits of concurrent execution of SCTs by miner using MVOSTM over SVOSTM. Thus a BG based on MVOSTM will have fewer edges than an SVOSTM-based BG, and will further reduce the size of the BG stored in the block. These advantages motivated us to use MVOSTMs for concurrent execution of SCTs by miners.

Concurrent executions of SCTs may cause inconsistent behaviors such as infinite loops, divide by zero, crash failures. Some of these behaviors, such as crash failures can be mitigated when SCTs are executed in a controlled environment, for example, the Ethereum Virtual Machine (EVM) [3]. However, not all anomalies such as infinite loop can be prevented by the virtual machine. The inconsistent executions can be prevented by ensuring that the executions produced by the STM system are opaque [10] or one of its variants such as co-opacity [20]. Our MVOSTM satisfies the former condition, opacity, while our SVOSTM satisfies the latter one, co-opacity.
Handling a Malicious Miner: A drawback of some of the approaches mentioned above is that a malicious miner can make the final state of the blockchain inconsistent. In the BG approach, the miner proposes an incorrect BG which does not include all necessary edges. With the bin-based approach, the miner could place the conflicting transactions in the concurrent bin [21]. This can result in inconsistent states in the blockchain due to double spending, e.g., when two concurrent transactions incorrectly transfer the same amount of money simultaneously from a source account to two different destination accounts. If a malicious miner $m$ does not add an edge between these two transactions in the BG [7] or put these two transactions in concurrent bin [21] then both SCTs can execute concurrently by validators. Similarly, if a majority of validators accept the block containing these two transactions, then the state of the blockchain becomes inconsistent. We denote this problem as edge missing BG (EMB) in the case of the BG approach [7] and faulty bin (FBin) in the case of the bin-based approach [21]. In Section 4, we show the effect of malicious miners (EMB or FBin) through experiments on the blockchain system.

To handle EMB and FBin errors, the validator must reject a block when edges are missing in the BG or when conflicting SCTs are in the concurrent bin. Execution of such a graph or concurrent bin by the validator threads can lead to an inconsistent state. To detect such an execution, the validator threads watch and identify transactions performing conflicting access on the same data-items while executing concurrently. In Section 3, we propose a Smart Multi-threaded Validator (SMV) which uses counters to detect this condition and reject the corresponding blocks.

Dickerson et al. [9] suggest a lock-based solution to handle EMB errors. The miner generates and stores the lock profile required to execute the SCTs of a block along with the BG. The validator then records a trace of the locks each of its thread would have acquired, had it been executing speculatively independent of the BG. The validator would then compare the lock profiles it generated with the one provided by the miner present in the block. If the profiles are different then the block is rejected. This check is in addition to the check of the final state generated and the state in the block. This solution is effective in handling EMB errors caused by malicious miners. However, it is lock-based and cannot be used for preventing EMB issue in optimistic approaches such as [7]. The advantage of our SMV solution is that it works well with both optimistic and lock-based approaches.

Our Contributions: This paper develops an efficient object semantics framework to execute SCTs concurrently by a miner using optimistic hash-table (both single and multi-version) OSTM. We use two methodologies to re-execute the SCTs concurrently by validators. In addition to the fork-join approach employed by Dickerson et al. [9], we also use a decentralized approach [7] in which the validator threads execute independent SCTs concurrently in a decentralized manner. To handle EMB and FBin errors, we propose a decentralized Smart Multi-threaded Validator. To summarize:
We introduce an efficient object-based framework for the concurrent execution of SCTs by miners (Section 3.2). We propose a novel way to execute the SCTs efficiently using optimistic SVOSTM by miner while ensuring co-opacity. To further increase concurrency, we propose a new way for the execution of SCTs by the miner using optimistic MVOSTM while satisfying opacity.

We propose the concurrent execution of SCTs by validators using BG given by miner to avoid FBR error (Section 3.3). The validator executes the SCTs using either fork-join or decentralized approaches.

We propose a Smart Multi-threaded Validator to handle EMB and FBIn errors caused by malicious miners (Section 3.4).

Extensive simulations (Section 4) show that concurrent execution of SCTs by SVOSTM and MVOSTM miner provide an average speedup of 3.41× and 3.91× over serial miner, respectively. SVOSTM and MVOSTM based decentralized validator provide on average of 46.35× and 48.45× over serial validator, respectively.

2 System Model

As in [11,17], we consider \( n \) threads, \( p_1, \ldots, p_n \) in a system that access shared data-items (or objects/keys) in a completely asynchronous fashion. We assume that none of the threads/processes will crash or fail unexpectedly.

Events: A thread invokes the transactions and the transaction calls object level (or higher-level) methods which internally invokes read/write atomic events on the shared data-items to communicate with other threads. Method invocations (or \( \text{inv} \)) and responses (or \( \text{rsp} \)) are also considered as events.

History: It is a sequence of invocations and responses of different transactional methods. We consider sequential history in which invocation on each transactional method follows the immediate matching response.

In this paper, we consider only well-formed histories in which a new transaction will not begin until the invocation of previous transaction has not been committed or aborted.

Software Transactional Memory (STM): STM [17,22] is a convenient concurrent programming interface for a programmer to access the shared memory using multiple threads. A typical STM works at lower-level (read-write) and exports following methods: (1) \( \text{STM}_{\text{begin}}() \): begins a transaction with unique id. (2) \( \text{STM}_{\text{read}}(k) \) (or \( \text{r}(k) \)): reads the value of data-item \( k \) from shared memory. (3) \( \text{STM}_{\text{write}}(k, v) \) (or \( \text{w}(k, v) \)): writes the value of data-item \( k \) as \( v \) in its local log. (4) \( \text{STM}_{\text{tryC}}() \): validates the transaction. If all updates made by the transaction is consistent then the updates will be reflected onto shared memory and transaction returns commit (or \( \text{C} \)). Otherwise, transaction returns abort (or \( \text{A} \)).

Transaction \( T_i \) starts with \( \text{STM}_{\text{begin}}() \) and completes when any of its methods return abort (or \( \text{A} \)) or commit (or \( \text{C} \)). The \( \text{STM}_{\text{read}}() \) and \( \text{STM}_{\text{tryC}}() \) methods may return \( \text{A} \).

OSTMs export higher-level methods: (1) \( \text{STM}_{\text{begin}}() \): begins a transaction with unique id. (2) \( \text{STM}_{\text{lookup}}(k) \) (or \( \text{t}(k) \)): does a lookup on data-item \( k \) from
shared memory. (3) STM_insert\((k, v)\) (or \(i(k, v)\)): inserts the value of data-item \(k\) as \(v\) in its local log. (4) STM_delete\((k)\) (or \(d(k)\)): deletes the data-item \(k\). (5) STM\(\text{tryC()}\): validates the transaction. After successful validation, the actual effects of STM_insert() and STM_delete() will be visible in the shared memory and transaction returns \(C\). Otherwise, it will return \(A\). We represent STM_lookup(), and STM_delete() as return-value (rv) methods because both methods return the value from hash-table. We represent STM_insert(), and STM_delete() as update (upd) methods as on successful STM\(\text{tryC()}\) both methods update the shared memory. Methods rv() and STM\(\text{tryC()}\) may return \(A\). For a transaction \(T_i\), we denote all the objects accessed by its rv\(_i\)() and upd\(_i\)() methods as \(rvSet_i\) and \(updSet_i\), respectively.

**Valid and Legal History:** If the successful \(rv_j(k, v)\) (i.e., \(v \neq A\)) method of a transaction \(T_j\) returns the value from any of previously committed transaction \(T_i\) that has performed upd() on key \(k\) with value \(v\) then such \(rv_j(k, v)\) method is valid. If all the \(rv()\) methods of history \(H\) is valid then \(H\) is valid history [20].

If the successful \(rv_j(k, v)\) (i.e., \(v \neq A\)) method of a transaction \(T_j\) returns the value from previous closest committed transaction \(T_i\) that \(k \in updSet_i\) \((T_i\) can also be \(T_0\)) and updates the \(k\) with value \(v\) then such \(rv_j(k, v)\) method is legal. If all the \(rv()\) methods of history \(H\) is legal then \(H\) is legal history [20]. A legal history is also valid history.

Two histories \(H\) and \(H'\) are equivalent if they have the same set of events. \(H\) and \(H'\) are multi-version view equivalent [23, Chap. 5] if they are valid and equivalent. \(H\) and \(H'\) are view equivalent [23, Chap. 3] if they are legal and equivalent. Additional definitions are in Appendix B.

### 3 Proposed Mechanism

This section describes our approach to the construction, data structures, and methods of concurrent BG, concurrent execution of SCTs by multi-threaded miner using optimistic object-based STMs, multi-threaded validator, and detection of a malicious miner.

#### 3.1 The Block Graph

The multi-threaded miner executes the SCTs concurrently and stores the dependencies among them in a BG. Each committed transaction corresponding to an SCT is a vertex in the BG while edges capture the dependencies, based on the STM protocol. Multi-threaded miner uses SVOSTM and MVOSTM to execute the SCTs concurrently, using timestamps. The challenge here is to construct the BG concurrently without missing any dependencies.

SVOSTM-based miner maintains three types of edges based on oconflicts between the transactions. An edge \(T_i \rightarrow T_j\) between two transaction is defined when: (1) \(rv_i(k, v) - STM\_tryC_j()\) edge : if \(rv_i(k, v) <_H STM\_tryC_j()\), \(k \in updSet(T_j)\) and \(v \neq A\); (2) \(STM\_tryC_i() - rv_j(k, v)\) edge : if \(STM\_tryC_i() <_H rv_j(k, v)\), \(k \in updSet(T_i)\) and \(v \neq A\); (3) \(STM\_tryC_i() - STM\_tryC_j()\) edge : if \(STM\_tryC_i() <_H STM\_tryC_j()\) and \((updSet(T_i) \cap updSet(T_j)) \neq \emptyset\).
MVOSTM-based miner maintains two types of edges based on multi-version conflicts (mvoconflicts) \[16\].  
(1) return value from (rvf) edge: if \( \text{STM\_tryC}_i() <_H \text{rvf}_j(k,v) \), \( k \in \text{updSet}(T_i) \) and \( v \neq A \) then there exist an rvf edge from \( T_i \) to \( T_j \), i.e., \( T_i \rightarrow T_j \);  
(2) multi-version (mv) edge: consider a triplet, \( \text{STM\_tryC}_i(), \text{rvm}(k,v), \text{STM\_tryC}_j() \) in which \( (\text{updSet}(T_i) \cap \text{updSet}(T_j) \cap \text{rvSet}(T_m) \neq \emptyset) \), \( (T_i \text{ and } T_j \text{ update the key } k \text{ with value } v \text{ and } u \text{ respectively}) \) and \( (u, v \neq A) \); then there are two types of mv edge: (a) if \( \text{STM\_tryC}_i() <_H \text{STM\_tryC}_j() \) then there exist a mv edge from \( T_m \) to \( T_j \), (b) if \( \text{STM\_tryC}_j() <_H \text{STM\_tryC}_i() \) then there exist a mv edge from \( T_j \) to \( T_i \). We modified SVOSTM and MVOSTM to capture oconflicts and mvoconflicts in the BG.  

**Data Structure for the Block Graph:** We use adjacency lists to maintain the BG \((V,E)\). \( V \) is the set of vertices (or SCTs) stored as a vertex list and \( E \) is the set of edges (conflicts between SCTs) stored as edge list. Two lock-free methods build the BG (see details in Appendix C.1): \textit{addVertex()} adds a vertex and \textit{addEdge()} adds an edge in BG. To execute the SCTs, validator threads use three methods of block graph library: \textit{globalSearch()} identifies the independent vertex with indegree 0 to execute it concurrently, \textit{remExNode()} decrements the indegree of conflicting vertices and \textit{localSearch()} identifies the independent vertex in thread local.  

### 3.2 Multi-threaded Miner  
A miner \( m \) receives requests to execute SCTs from different clients. The miner \( m \) then forms a block with several SCTs (the precise number of SCTs depend on the blockchain), \( m \) execute these SCTs while executing the non-conflicting SCTs concurrently to obtain the final state of the blockchain. Identifying the non-conflicting SCTs statically is not straightforward because smart contracts are written in a turing-complete language \[11\] (e.g., Solidity \[5\] for Ethereum). We use optimistic STMs to execute the SCTs concurrently as in Anjana et al. \[7\] but adapted to object-based STMs on hash-tables to identify the conflicts.  

Algorithm 1 shows how SCTs are executed by an \( m \) threaded miner. The input is an array of SCTs, \textit{sctList} and a object-based STM, (SVOSTM or MVOSTM). We assume that both libraries support the BG methods described above. The multi-threaded miner uses a global index into the sctList \textit{gIndex} which is accessed by all the threads. A thread \( Th_x \) first reads the current value of \textit{gIndex} into a local value \textit{curInd} and increments \textit{gIndex} atomically (Line 2).  

Having obtained the current index in \textit{curInd}, \( Th_x \) gets the corresponding SCT, \textit{curTrn} from \textit{sctList[]} (Line 4). \( Th_x \) then begins a STM transaction corresponding to \textit{curTrn} (Line 8). For every hash-table insert, delete and lookup encountered while executing the scFun of \textit{curTrn}, \( Th_x \) invokes the corresponding STM methods: \textit{STM\_lookup()}, \textit{STM\_insert()}, \textit{STM\_delete()}, either on an SVOSTM or on an MVOSTM. Otherwise, it executes the step normally. If any of these steps fail, \( Th_x \) begins a new STM transaction (Line 8) and re-executes these steps.  

Upon successful completion of transaction \( T_i \), \( Th_x \) creates a vertex node for \( T_i \) in the block graph (Line 21). Then, \( Th_x \) obtains the transactions (SCTs) with
Algorithm 1 Multi-threaded Miner(sctList[], STM): \(m\) threads concurrently execute the SCTs from sctList with STMs.

1. **procedure** Multi-threaded Miner (sctList[], STM)
2.  \(\text{curInd} = \text{gIndex.get}\&\text{Inc}();\) // Atomically read the index and increment it.
3.  \(\text{while} (\text{curInd} < \text{sctList.length}) \text{ do} \) // Execute until all SCTs have not been executed
4.   \(\text{curTrn} = \text{sctList[\text{curInd}]};\) // Get the current SCT to execute
5.   \(T_i = \text{STM.begin}();\) // Begins a new transaction. Here \(i\) is unique id
6.  for all (curStep \(\in \text{curTrn.scFun}\)) do // scFun is a list of steps
7.    switch(curStep)
8.     case lookup(k):
9.        \(v \leftarrow \text{STM.lookup}(k);\) // Lookup data-item \(k\) from a shared memory
10.       if \((v == A)\) then goto Line 5; end if break;
11.     case insert(k, v):
12.        \(\text{STM.insert}(k, v);\) break;
13.     case delete(k):
14.        \(v \leftarrow \text{STM.delete}(k);\) // Actual deletion of data-item \(k\) happens in STM.tryC()
15.       if \((v == A)\) then goto Line 5; end if break;
16.   default: Execute the step normally // Any step apart from lookup, insert, delete
17.  endswitch
18.  end for
19.  \(v \leftarrow \text{STM.tryC}();\) // Try to commit the transaction \(T_i\)
20.  if \((v == A)\) then goto Line 5; end if
21.  addVertex(i); // Create vertex node for \(T_i\) with scFun
22.  BG(i, STMs); // Add the conflicts of \(T_i\) to block graph
23.  \(\text{curInd} = \text{gIndex.get}\&\text{Inc}();\) // Atomically read the index and increment it.
24.  end while
25.  build-block(); // Here the miner builds the block.
26. **end procedure**

which \(T_i\) is conflicting from the OSTM, and adds the corresponding edges to the BG (Line 22). \(Th_x\) then gets the index of the next SCT to execute (Line 23).

An important step here is how the underlying OSTMs (either SVOSTM or MVOSTM) maintain the conflicts among the transactions which is used by \(Th_x\) (see Appendix C.2). Both SVOSTM and the MVOSTM use timestamps to identify the conflicts.

Once all the SCTs of sctList have been executed successfully and the BG is constructed concurrently, it is stored in the proposed block. The miner then stores the final state \((FS_m)\) of the blockchain (which is the state of all shared data-items), resulting from the execution of SCTs of sctList in the block. The miner then computes the operations related to the blockchain. For Ethereum, this would constitute the hash of the previous block. Then the multi-threaded miner proposes a block which consists of all the SCTs, BG, \(FS_m\) of all the shared data-items and hash of the previous block (Line 25). The block is then broadcast to all the other nodes in the blockchain.

Appendix D proves the following theorems:

**Theorem 1.** The BG captures all the dependencies between the conflicting nodes.

**Theorem 2.** A history \(H_m\) generated by the multi-threaded miner with SVOSTM satisfies co-opacity.

**Theorem 3.** A history \(H_m\) generated by multi-threaded miner with MVOSTM satisfies opacity.
3.3 Multi-threaded Validator

The validator re-executes the SCTs deterministically relying on the BG provided by the miner in the block. BG consists of dependency among the conflicting SCTs and restrict validator threads to execute them serially to avoid the False Block Rejection (FBR) error while non-conflicting SCTs execute concurrently to obtain greater throughput. The validator uses \textbf{globalSearch()}, \textbf{localSearch()}, and \textbf{remExNode()} methods of the BG library as described in Section 3.1.

After successful execution of the SCTs, validator threads compute the final state \((FS_v)\) of the blockchain which is the state of all shared data items. If it matches the final state \((FS_m)\) provided by the miner then the validator accepts the block. If a majority of the validators accept the block, then it is added to the blockchain. Detailed description appears in Appendix C.3.

Appendix D proves the following theorems:

\textbf{Theorem 4.} A history \(H_m\) generated by the multi-threaded miner with SVOSTM and history \(H_v\) generated by a multi-threaded validator are view equivalent.

\textbf{Theorem 5.} A history \(H_m\) generated by the multi-threaded miner with MVOSTM and history \(H_v\) generated by a multi-threaded validator are multi-version view equivalent.

3.4 Detection of Malicious Miners by Smart Multi-threaded Validator (SMV)

We propose a technique to handle edge missing BG (EMB) and Faulty Bin (FBin) caused by the malicious miner as explained in Section 1. A malicious miner \(mm\) can remove some edges from the BG and set the final state in the block accordingly. A multi-threaded validator executes the SCTs concurrently relying on the BG provided by the \(mm\) and results the same final state. Hence, incorrectly accepts the block. Similarly, if a majority of the validators accept the block then the state of the blockchain becomes inconsistent. For instance, a double spending can be executed.

A similar inconsistency can be caused by a \(mm\) in bin-based approach: \(mm\) can maliciously add conflicting SCTs to the concurrent bin resulting in FBin error. This may cause multi-threaded validator \(v\) to access shared data items concurrently leading to synchronization errors. To prevent this, the SMV checks to see if two concurrent threads end up accessing the same shared data item concurrently. If this situation is detected, then the miner is malicious.

To identify such situations, SMV uses \textbf{counters}, inspired by the \textbf{basic timestamp ordering (BTO)} protocol in databases [23, Chap. 4]. SMV keeps track of each global data item that can be accessed across multiple transactions by different threads. Specifically, SMV maintains two global counters for each key of hash-table (shared data item) \(k\) (a) \(k.gUC\) - global update counter (b) \(k.gLC\) - global lookup counter. These respectively keep track of number of \textbf{updates} and \textbf{lookups} that are concurrently performed by different threads on \(k\). Both counters are initially 0.
When an SMV thread $T_h_x$ is executing an SCT $T_i$ it maintains two local variables corresponding to each global data item $k$ which is accessible only by $T_h_x$ (c) $k.lUC_i$: local update counter (d) $k.lLC_i$: local lookup counter. These respectively keep track of number of updates and lookups performed by $T_h_x$ on $k$ while executing $T_i$. These counters are initialized to 0 before the start of $T_i$.

Having described the counters, we will explain the algorithm at a high level. Suppose the next step to be performed by $T_h_x$ is:

1. $lookup(k)$: Thread $T_h_x$ will check for equality of the local and global update counters, i.e., ($k.lUC_i == k.gUC$). If they are not same then SMV will report the miner as malicious. Otherwise, (i) $T_h_x$ will atomically increment $k.gLC_i$. (ii) $T_h_x$ will increment $k.lLC_i$. (iii) Perform the lookup on the key $k$ from shared memory.

2. $update(k, val)$: Here $T_h_x$ wants to update (insert/delete) $k$ with value $val$. So, $T_h_x$ will check for the equality of both global, local update and lookup counters, i.e., ($k.lUC_i == k.gUC$) and ($k.lLC_i == k.gLC$). If they are not same then SMV will report the miner as malicious. Otherwise, (i) $T_h_x$ will atomically increment $k.gUC$. (ii) $T_h_x$ will increment $k.lUC_i$. (iii) Perform the update on the key $k$ with value $val$ on shared memory.

Once $T_i$ terminates, $T_h_x$ will atomically decrements $k.gUC, k.gLC$ by the value of $k.lUC_i, k.lLC_i$, respectively. Then $T_h_x$ will reset $k.lUC_i, k.lLC_i$ to 0.

The reason for performing these steps and the correctness of the algorithm is as follows: if $T_h_x$ is performing a lookup on $k$ then no other thread should be performing an update on $k$. Here, $k.gUC$ represents the number of updates to $k$ currently executed by all the threads while $k.lUC_i$ represents the number of updates to $k$ on behalf of $T_i$ by $T_h_x$. Thus the value of $gUC$ should be same as $lUC$. Otherwise, some other thread is also concurrently performing the updates to $k$. Similarly, if $T_h_x$ is performing an update on $k$, then no other thread should be performing an update or lookup on $k$. This can be verified by checking if $lLC, lUC$ are respectively same as $gLC, gUC$.

**Theorem 6.** *Smart Multi-threaded Validator rejects malicious blocks with BG that allow concurrent execution of dependent SCTs.*

The same SMV technique can be applied to identify the faulty bin error as explained in Section 1. See Appendix C.4 for detailed description along with the pseudo code of smart multi-threaded validator and Appendix D for proof of Theorem 6.

4 Experimental Evaluation

The goal of this section is to demonstrates the performance gains by proposed multi-threaded miner and validator against state-of-the-art miners and validators. To evaluate our approach, we considered Ethereum smart contracts. In Ethereum blockchain, contracts are written in Solidity language and are executed on the *Ethereum Virtual Machine (EVM)*. EVM does not support
multi-threading [3,9]. So, we converted the smart contracts of Ethereum as described in Solidity documentation [5] into C++ multi-threaded contracts similar to the approach of [7,9]. Then we integrated them into object-based STM framework (SVOSTM and MVOSTM) for concurrent execution of SCTs by the miner.

We chose a diverse set of smart contracts described in Solidity documentation [5] as benchmarks to analyze the performance of our proposed approach as was done in [7,9]. The selected benchmark contracts are (1) Coin: a financial contract, (2) Ballot: an electronic voting contract, (3) Simple Auction: an auction contract, and (4) finally, a Mix contract: combination of three contracts mentioned above in equal proportion in which block consists of multiple SCTs belonging to different smart contracts and seems more realistic.

We compared the proposed SVOSTM and MVOSTM miner with state-of-the-art multi-threaded: BTO [7], MVTO [7], Speculative Bin (or SpecBin) [21], Static Bin (or StaticBin) [21], and Serial miner [2]. We could not compare our work with Dickerson et al. [9] as their source code is not available in public domain. We converted the code of StaticBin and SpecBin [21] from Java to C++ for comparing with our algorithms.

Concurrent execution of SCTs by the validator does not use any STM protocol; however it uses the BG provided by the multi-threaded miner, which does use STM. To identify malicious miners and prevent any malicious block from being added to the blockchain, we proposed Smart Multi-threaded Validator (SMV) for SVOSTM, MVOSTM as SVOSTM SMV, MVOSTM SMV. Additionally, we proposed SMV for state-of-the-art validators as BTO SMV, MVTO SMV, SpecBin SMV, and StaticBin SMV and analysed the performance.

Experimental Setup: The experimental system consists of two sockets, each comprised of 14 cores 2.60 GHz Intel (R) Xeon (R) CPU E5-2690, and each core supports 2 hardware threads. Thus the system supports a total of 56 hardware threads. The machine runs Ubuntu 16.04.2 LTS operating system and has 32GB RAM.

To analyze the performance, we evaluated the speedup achieved by each contract on two workloads. In the first workload (W1), the number of SCTs varied from 50 to 300 while the number of threads fixed is at 50. The maximum number of SCTs in a block of Ethereum is approximately 250 [4,9], but is growing over time. In the second workload (W2), the number of threads varied from 10 to 60, while the number of SCTs is fixed at 100. The average number of SCTs in a block of Ethereum is around 100 [4]. The hash-table size and shared data-items are fixed to 30 and 500 respectively for both workloads. For accuracy, results are averaged over 26 runs in which the first run is discarded and considered as a warm-up run. The results of serial execution is treated as the baseline for evaluating the speedup. This section describes the detailed analysis for the mix contract and analysis of Coin, Ballot and Simple auction benchmark contracts are in Appendix E.

Experimental Results: Fig. 2(a) and Fig. 2(b) show the speedup of MVOSTM, SVOSTM, MVTO, BTO, SpecBin, and StaticBin miner over serial miner for mix contract.
The average speedup achieved by MVOSTM, SVOSTM, MVTO, BTO, SpecBin, and StaticBin miner over serial miner is $3.91 \times$, $3.41 \times$, $1.98 \times$, $1.5 \times$, $3.02 \times$, and $1.12 \times$, respectively.

As shown in Fig. 2 (a), increasing the number of SCTs leads to high contention (because shared data-items are fixed to 500). So the speedup of multi-threaded miner reduces. MVOSTM and SVOSTM miners outperform SpecBin miner because MVOSTM and SVOSTM miners use optimistic object-based STMs to execute SCTs concurrently and construct the BG whereas SpecBin uses locks to execute SCTs concurrently and constructs two bins using the pessimistic approach. SpecBin miner does not release the locks until the construction of the concurrent bin, which gives less concurrency. However, for the smaller numbers of SCTs in a block, SpecBin is slightly better than MVOSTM and SVOSTM miners, which can be observed in the Fig. 2 (a) at 50 SCTs. MVOSTM and SVOSTM miners outperform MVTO and BTO miners because both of them are consider rwconflicts. It can also be observed that MVOSTM miner outperforms all other STM miners as it has fewer conflicts, which gets reflected (see Fig. 4) as the least number of dependencies in the BG as compared to other STM miners. For the multi-version (MVOSTM and MVTO) miners, we did not

---

3 In the figures, legend items in bold.
limit the number of versions because the number of SCTs in a block is finite. The speedup by StaticBin miner is worse than serial miner for more than 100 SCTs because it takes time for static conflict prediction before executing SCTs.

Fig. 2 (b) shows that speedup achieved by multi-threaded miner increases while increasing the number of threads, limited by the number of hardware threads available on the underlying experimental setup. Since, our system has 56 logical threads, the speedup decreases beyond 56 threads. MVOSTM miner outperforms all other miners with similar reasoning, as explained for Fig. 2 (a). Another observation is that when the number of threads is less, the serial miner dominates BTO and MVTO miner due to the overhead of the STM system.

The average number of dependencies in BG by all the STM miners presented in Fig. 1 It shows that BG constructed by the MVOSTM has the least number of edges for all the contracts on both workloads. However, there is no BG for bin-based approaches (both SpecBin and StaticBin). So, from the block size perspective, bin-based approaches are efficient. But the speedup of the validator obtained by the bin-based approaches is significantly lesser than STM validators.

Fig. 2 (c) and Fig. 2 (d) show the speedup of Smart Multi-threaded Validators (SMVs) over serial validator on the workloads W1 and W2, respectively. The average speedup achieved by MVOSTM, SVOSTM, MVTO, BTO, SpecBin, and StaticBin decentralized SMVs are 48.45×, 46.35×, 43.89×, 41.44×, 5.39×, and 4.81× over serial validator, respectively.

It can be observed that decentralized MVOSTM SMV is best among all other STM validators due to fewer dependencies in the BG. Though the block size is less in bin-based approaches as compared to STM based approaches due to the absence of BG, however, STM validators outperform bin-based validators because STM validators precisely determines the concurrent SCTs based on BG. In contrast, bin-based validator gives less concurrency using a lock-based pessimistic approach.

The speedup of SMV is significantly higher than multi-threaded miner because the miner has to execute the SCTs concurrently either using STMs (including the retries of aborted transactions) and constructs the BG or prepare two bins (concurrent and sequential bin using locks in SpecBin and static analysis in StaticBin). On the other hand, the validator executes the SCTs concurrently and deterministically relying on BG (without any retries) or bins provided by miner.

A malicious miner may cause either EMB or FBin errors in a block. Fig. 3 illustrates the percentage of validators without SMV logic embedded, i.e., Non-SMVs accepting a malicious block on workloads W1 and W2, respectively. Here, we considered 50 validators and ran the experiments for the mix contract. The Fig. 3 shows that less than 50% of validators (except bin-based NonSMV) accept a malicious block. However, SpecBin and StaticBin NonSMVs show more than 50% acceptance of malicious blocks. Though, it is to be noted that the acceptance of even a single malicious block result in the blockchain going into inconsistent state.
To solve this problem, we developed a Smart Multi-threaded Validator (SMV), which identifies the malicious miner (described in Section 3.4). We prove that the SMV detects malicious block with the help of counter and rejects it. In fact all the validators shown in Fig. 2 (c) & (d) are SMV based. Another advantage of SMV is that once it detects a malicious miner during the concurrent execution of SCTs, it can immediately reject the block and need not execute the remaining SCTs in the block thus saving time.

Appendix E presents additional experiments that cover the average number of dependencies in the BG and additional space required to store the BG into the block. In addition to W1 and W2, we consider a third workload, W3 in which the number of shared data-items varied from 100 to 600 while the number of threads, SCTs, and hash-table size is fixed to 50, 100, and 30, respectively. We have shown that the performance of SMV validators for Mix contract on W3 and several other experiments for all the benchmarks. We compared the time taken by the SMV and NonSMV. We analyzed the speedup of fork-join validator for all the three workloads. We showed the actual time (microseconds) taken by all the miners and validators on W1 for the aforementioned four smart contract benchmarks in Tables 4 - 11.
5 Conclusion and Future Directions

This paper presents a framework for the concurrent execution of smart contracts by miner and validator, which has achieved better performance using object semantics. In blockchains that follow order-execute model [6] such as Ethereum [3], Bitcoin [18], each Smart Contract Transaction (SCT) is executed in two different contexts: first by the multi-threaded miner to propose a block and later by the multi-threaded validator to verify the proposed block by the miner as part of the consensus. To avoid FBR errors, the miner on concurrent execution of SCTs capture the dependencies among them in the form of a BG as in [7,9]. The validator then re-executes the SCTs concurrently while respecting the dependencies recorded in the BG to avoid FBR errors.

The miner executes the SCTs concurrently using STMs that exploit the object semantics: Single-Version Object-based STM (SVOSTM) and Multi-Version Object-based STM (MVOSTM). The dependencies among the SCTs collected during this execution are used by the miner threads to construct the BG concurrently. Due to the use of object semantics, the number of edges in the BG is smaller, which benefits both miners and validators by enabling them to execute SCTs quickly in a concurrent setting.

Another interesting aspect that we considered in this paper is the issue of malicious miners. Suppose that in the BG approach, a malicious miner proposes an incorrect BG which does not have all the edges resulting in edge missing BG (EMB) error. With the bin-based approach, the miner could place the conflicting transactions in the concurrent bin [21] resulting in faulty bin (FBin) error. To handle malicious miner, we have proposed a smart multi-threaded validator (SMV) which can identify these errors and reject the corresponding blocks.

Proposed SVOSTM and MVOSTM miner achieve on average speedup of $3.41 \times$ and $3.91 \times$ over serial miner respectively. Proposed SVOSTM and MVOSTM decentralized validator outperform with an average speedup of $46.35 \times$ and $48.45 \times$ over serial validator, respectively on Ethereum smart contracts.

Future Directions: There are several directions for future work. A natural question is whether the size of BG can become an overhead. Currently, the average number of SCTs in a block is $\approx 100$ in Ethereum. So, storing BG inside the block does not consume much space. The BG constructed by MVOSTMs has fewer dependencies as compared with state-of-the-art SCT execution as shown in Fig. 4. However, the number of SCTs in a block can increase over time and as a result the BG size can grow, and storing it will consume more space. Hence, constructing storage optimal BG is an interesting challenge. Or achieving the concurrent execution of SCTs correctly without incurring any extra storage overhead without compromising with the speedup will be another interesting direction. So, a related relevant question is what the optimal storage required for achieving the best possible speedup?

Another interesting research direction is optimizing power consumption. Nowadays, multi-core systems are ubiquitous while serial execution fails to harness the power of multiple cores. So, as discussed in the paper concurrent execution of
SCTs by invoking multiple threads on a multi-core system ensures better performance than serial. But, multi-threading on the multi-core system consumes more power. Additional power is consumed by the multiple miner and validator threads to propose and validate the blocks concurrently. Hence, we would like to explore trade-off between harnessing the number of cores and power consumption.

Finally, since Ethereum Virtual Machine (EVM) [3] does not support multi-threading, it is not possible to test the proposed approach on Ethereum. So, another research direction is to design multi-threaded EVM. We plan to test our proposed approach on other blockchains such as Bitcoin [18], EOS [2] which follow the order-execute model and support multi-threading.

References

1. Bitcoin Block Size. [Accessed 08-03-2020].
2. EOS. [Accessed 08-03-2020].
3. Ethereum. [Accessed 08-03-2020].
4. Ethereum Stats. [Accessed 08-03-2020].
5. Solidity Documentation. [Accessed 08-03-2020].
6. Elli Androulaki, Artem Barger, Vita Bortnikov, Christian Cachin, Konstantinos Christidis, Angelo De Caro, David Eynard, Christopher Ferris, Gennady Laventman, Yaacov Manevich, Srinivasan Muralidharan, Chet Murthy, Binh Nguyen, Manish Sethi, Gari Singh, Keith Smith, Alessandro Sorniotti, Chrysoula Stathakopoulou, Marko Vukolić, Sharon Weed, and Jason Yellick. Hyperledger fabric: A distributed operating system for permissioned blockchains. EuroSys, 2018.
7. P. S. Anjana, S. Kumari, S. Peri, S. Rathor, and A. Somani. An efficient framework for optimistic concurrent execution of smart contracts. In PDP, pages 83–92, 2019.
8. Bapi Chatterjee, Sathya Peri, Muktikanta Sa, and Nandini Singh. A Simple and Practical Concurrent Non-blocking Unbounded Graph with Linearizable Reachability Queries. In ICDCN, 2019.
9. Thomas Dickerson, Paul Gazzillo, Maurice Herlihy, and Eric Koskinen. Adding Concurrency to Smart Contracts. PODC ’17, pages 303–312, New York, NY, USA, 2017. ACM.
10. Rachid Guerraoui and Michal Kapalka. On the Correctness of Transactional Memory. PPoPP, 2008.
11. Rachid Guerraoui and Michal Kapalka. Principles of Transactional Memory, Synthesis Lectures on Distributed Computing Theory. 2010.
12. Ahmed Hassan, Roberto Palmieri, and Binoy Ravindran. Optimistic Transactional Boosting. volume 49, pages 387–388, New York, NY, USA, February 2014. ACM.
13. Maurice Herlihy and Eric Koskinen. Transactional Boosting: A Methodology for Highly-concurrent Transactional Objects. PPoPP ’08, New York, NY, USA, 2008. ACM.
14. Maurice Herlihy and Nir Shavit. On the nature of progress. OPODIS 2011.
15. Maurice P. Herlihy and Jeannette M. Wing. Linearizability: A correctness condition for concurrent objects. ACM Trans. Program. Lang. Syst., 1990, 1990.
16. Chirag Juyal, Sandeep Kulkarni, Sweta Kumari, Sathyia Peri, and Archit Somani. An innovative approach to achieve compositionality efficiently using multi-version object based transactional systems. In Taisuke Izumi and Petr Kuznetsov, editors, *SSS*, pages 284–300, Cham, 2018. Springer International Publishing.
17. Petr Kuznetsov and Sathyia Peri. Non-interference and local correctness in transactional memory. *Theor. Comput. Sci.*, 688:103–116, 2017.
18. Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2009.
19. Christos H. Papadimitriou. The serializability of concurrent database updates. *J. ACM*, 26(4):631–653, 1979.
20. Sathyia Peri, Ajay Singh, and Archit Somani. Efficient means of Achieving Composability using Transactional Memory. NETYS ’18, 2018.
21. Vikram Saraph and Maurice Herlihy. An Empirical Study of Speculative Concurrency in Ethereum Smart Contracts. Tokenomics ’19, 2019.
22. Nir Shavit and Dan Touitou. Software transactional memory. PODC, 1995.
23. Gerhard Weikum and Gottfried Vossen. *Transactional Info Systems: Theory, Algorithms, and the Practice of Concurrency Control and Recovery*, 2002.
24. An Zhang and Kunlong Zhang. Enabling concurrency on smart contracts using multiversion ordering. In *Web and Big Data*, 2018.
A Appendix

This section is organized as follows:

| Section No.| Section Name                                      |
|------------|--------------------------------------------------|
| Appendix A | Advantage of OSTMs over RWSTMs                  |
| Appendix B | Remaining System Model                           |
| Appendix C | Detailed Proposed Mechanism                     |
| Appendix D | Correctness of BG, Multi-threaded Miner and Validator |
| Appendix E | Detailed Experimental Evaluation                 |

A Advantage of OSTMs over RWSTMs

Fig. 5: Advantage of OSTMs over RWSTMs on SCTs

We now illustrate the advantage of OSTMs over RWSTMs. Consider an OSTM for hash-table which invokes the following methods: (1) STM\_begin(), (2) STM\_lookup(k) (or l(k)), (3) STM\_insert(k, v) (or i(k, v)), (4) STM\_delete(k) (or d(k)), and (5) STM\_tryC() explained in Section 2.

Consider Fig. 5, which demonstrates the advantage of OSTMs over RWSTMs on SCTs. Fig. 5 (a) shows two transactions $T_1$ and $T_2$ in the form of a tree structure which is working on a hash-table with $B$ buckets. Fig. 5 (b) illustrates a bucket of the hash-table with four accounts (shared data-items) $A_1, A_2, A_3$ and $A_4$ which are accessed by these transactions. Accounts are stored in the form of a list. Thus to access account $A_4$, a thread has to access $A_1, A_2, A_3$ before access it.

Suppose $T_1$ wants to send $50$ from account $A_1$ to $A_3$ and $T_2$ wants to send $70$ from account $A_2$ to $A_4$. Before performing these transfers, the respective SCTs verify that each account has sufficient balance. After checking, the SCT $T_1$ deletes $50$ from $A_1$ and adds it to $A_3$. At a lower-level, these operations involve reading and writing to both accounts $A_1$ and $A_3$. The execution is shown in Fig. 5 (a) in form of a tree following the notation used by Weikum et al. [23, Chap 6]. Here, level 0 (or $L_0$) shows the operations as read and write while $L_1$ shows higher-level operations insert, delete and lookup.

Consider the execution at $L_0$ of Fig. 5 (a). The dotted red circles represent conflicting operations: $r_2(A_1)$ conflicts with $w_1(A_1)$ while $r_1(A_2)$ conflicts with
As a result, this execution cannot be serialized as we cannot find any equivalent serial schedule because of cyclic conflict among $T_1$ and $T_2$ as shown in Fig. 5 (c). Hence for serializability [19] (or opacity [10]) either $T_1$ or $T_2$ has to abort. However, execution at level $L_1$ depicts that both transactions are working on different accounts and the higher-level methods (insert and lookup) are isolated. So, we can prune [23, Chap 6] this tree and isolate the transaction executions [20] at the higher-level with equivalent serial schedule $T_1T_2$ or $T_2T_1$ as shown in Fig. 5 (d). Essentially not all the conflicts of lower-level or read-write level matter at higher-level. In a typical execution, object-conflicts (or oconflicts) [20] are fewer than read-write conflicts (or rconflicts). Therefore, OSTMs provides greater concurrency while reducing the number of aborts than RWSTMs.

B Remaining System Model

This section describes the remaining execution model and the notions of STMs used in this paper.

**History:** It is a sequence of invocations and responses of different transactional methods. In other words, a history $H$ is a sequence of events represented as $evts(H)$. $H$ internally invokes multiple transactions by multiple threads concurrently. Each transaction calls higher-level methods, and each method comprises of read/write events. Here, we consider sequential history in which invocation on each transactional method follows the immediate matching response. It helps to make each transactional method as an atomic event. We denote the total order of the transactional method as $<_H$, so history is represented as $\langle evts(H), <_H \rangle$.

In this paper, we consider only well-formed histories in which a new transaction will not begin until the invocation of previous transaction has not been committed or aborted. History $H$ comprises of the set of transactions as $txns(H)$. The set of committed and aborted transactions in $H$ is denoted as $\text{committed}(H)$ and $\text{aborted}(H)$ respectively. So, the set of incomplete or live transactions in $H$ is represented as $H_{incomp} = H_{live} = (txns(H) - \text{committed}(H) - \text{aborted}(H))$.

**Transaction Real-Time Order:** Consider two transactions $T_i, T_j \in txns(H)$, if $T_i$ terminates, i.e. either committed or aborted before $STM\text{\_begin\_}j()$ of $T_j$ then $T_i$ and $T_j$ respects real-time [19] order represented as $T_i <^\text{RT}_H T_j$.

**MVSR, VSR, and CSR:** A history $H$ is in Multi-Version View Serializable (or MVSR) [23, Chap. 5], if there exists a serial history $S$ such that $S$ is multi-version view equivalent to $H$. It keeps multiple versions with respect to each key. A history $H$ is in View Serializable (or VSR) [23, Chap. 3], if there exists a serial history $S$ such that $S$ is view equivalent to $H$. It has shown that verifying the membership of MVSR and VSR in the database is NP-Complete [19]. So, researchers came across with an efficient equivalence notion which is Conflict Serializable (or CSR) [23, Chap. 3]. It is a sub-class of VSR which uses conflict graph characterization to verify the membership in polynomial time. A history
$H$ is in CSR if there exists a serial history $S$ such that $S$ is conflict equivalent to $H$.

**Serializability and Opacity:** Serializability\cite{19} is a popular correctness criteria in databases. But it considers only *committed* transactions. This property is not suitable for STMs. Hence, Guerraoui and Kapalka propose a new correctness criteria opacity \cite{10} for STMs which considers *aborted* transactions along with *committed* transactions as well. A history $H$ is opaque \cite{10,11}, if there exist an equivalent serial history $S$ with (1) set of events in $S$ and complete history of $H$ are same (2) $S$ satisfies the properties of legal history and (3) The real-time order of $S$ and $H$ are preserved.

**Linearizability:** A linearizable \cite{15} history $H$ has the following properties: (1) In order to get a valid sequential history, the invocation and response events can be reordered. (2) The obtained sequential history should satisfy the sequential specification of the objects. (3) The real-time order should respect in sequential reordering as in $H$.

**Lock Freedom:** It is a non-blocking progress property in which if multiple threads are running for a sufficiently long time, then at least one of the threads will always make progress. Lock-free \cite{14} guarantees system-wide progress, but individual threads may starve.

## C Detailed Proposed Mechanism

This section describes the data structure and methods of concurrent BG in Appendix C.1. Then we describe the data structure of SVOSTM and MVOSTM in Appendix C.2. Later, we describes the execution of SCTs by Multi-threaded Validator rely on the BG provided by the miner in Appendix C.3 and detection of malicious miner by *Smart Multi-threaded Validator* in Appendix C.4.
C.1 Data Structure of the Block Graph

We use adjacency list to maintain the Block Graph $BG(V, E)$ inspired from [7,8]. Here $V$ is the set of vertices ($vrtNodes$) is stored as a vertex list ($vrtList$). Similarly E is the set of Edges ($egNodes$) is stored as edge list ($egList$ or conflict list) as shown in the Fig. 6 (a), both vrtList and egList store between the two sentinel nodes $Head(-\infty)$ and $Tail(+\infty)$. Each vrtNode maintains a tuple: $\langle ts, scFun, indegree, egNext, vrtNext \rangle$. Here, $ts$ is the unique timestamp $i$ of the transaction $T_i$ to which this node corresponds to. $scFun$ is the smart contract function executed by the transaction $T_i$ which is stored in vrtNode. The number of incoming edges to the transaction $T_i$, i.e. the number of transactions on which $T_i$ depends, is captured by indegree. Field egNext and vrtNext points the next egNode and vrtNode in the egList and vrtList respectively.

Each egNode of $T_i$ similarly maintains a tuple: $\langle ts, vrtRef, egNext \rangle$. Here, $ts$ stores the unique timestamp $j$ of $T_j$ which has an edge coming from $T_i$ in the graph. BG maintains the conflict edge from lower timestamp transaction to higher timestamp transaction. This ensures that the block graph is acyclic. The egNodes in egList are stored in increasing order of the ts Field vrtRef is a vertex reference pointer which points to its own vrtNode present in the vrtList. This reference pointer helps to maintain the indegree count of vrtNode efficiently.

Fig. 6 (b) demonstrates the high level overview of BG which consist of three transaction $T_1$, $T_2$ and $T_3$. Here, $T_1$, $T_2$ are in conflict while $T_3$ is independent. The underlying representation of it illustrated in Fig. 6(a). For each transactions ($T_1$, $T_2$ and $T_3$) there exists a vrtNode in the vrtList of BG along with their conflicts. Since there is an edge from $T_1$ to $T_2$, an egNode corresponding to $T_2$ is in the egList of $T_1$. As mentioned earlier, the conflict edges go from lower timestamp to higher timestamp to ensure acyclicity of the block graph. After adding the egNode, the indegree of the vrtNode of $T_2$ in the vrtList is incremented as shown in Fig. 6 (a).

**Block Graph Library Methods Accessed by Multi-threaded Miner:**
Multi-threaded miner uses multiple threads to build the block graph. Specifically, the multi-threaded miner uses two methods to build the block graph: addVertex() and addEdge(). These two methods are lock-free [14]. Here, addVertex(i), as the names suggests adds a vrtNode with $ts = i$ for respective scFun to the vrtList of the BG if such a vertex is not already present. This node is atomically added to vrtList using CAS operations.

The addEdge($u,v$) method creates an egNode for $v$ in $u$’s vrtNode if it does not already exist. First, it identifies the egNode in the egList of vrtNode. If egNode does not exist then it creates the node and adds into the egList of vrtNode atomically using CAS. The edges from $u$ to $v$ captures the conflicts between these transactions. This implies that $v$ is dependent on $u$ and the scFun of $v$ has to be executed only after $u$’s execution.

**Block Graph Library Methods Accessed by Multi-threaded Validator:**
Multi-threaded validator uses multiple threads to re-executes the SCTs concurrently and deterministically with the help of BG given by the multi-threaded miner. To execute the SCTs, validator threads use three methods of block graph
library: globalSearch(), remExNode() and localSearch(). First a validator thread 
Thr invokes the globalSearch() method which searches for a vrtNode n in the block graph having indegree 0 (i.e., source node). Such a node corresponds to a 
SCT, which does not depend on other transactions and hence can be executed independently without worrying about synchronization issues. On identifying n, 
Thr atomically tries to claim it if not already claimed by some other thread. It 
does this by performing a CAS operation on the indegree to -1. After successful 
exection of scFun of n, Thr invokes remExNode method which decrements the 
indegree count for all the nodes which have an incoming edge from n. This 
list of nodes is maintained in the egList of n.

While decrementing the indegree count of conflicting nodes if the validator 
thread Thr finds any other vrtNode with the indegree as 0 then it adds that 
reference to that node in its thread-local log thLog. The thLog is used for 
optimization so that Thr needs not to search in the global BG to find the next 
source node. If a reference to the source node exists in the local log of validator, 
it is identified by the localSearch() method. Thr on identifying such a node n, 
atomically claims n (if not already claimed by another thread). Then it executes 
the scFun of n and then remExNode as explained above. A detailed description 
of BG methods, along with pseudocode is as follows:

\[ BG(vrtNode, STM) \]

\[ procedure BG(vrtNode, STM) \]
\[ /*STM provides conflictList of committed transaction Ti */ \]
\[ conflist = STM.getConflictList(vrtNode.ts_i); \]
\[ /*Ti, Tj are in conflict and Tj exists in conflict list of Ti */ \]
\[ for all (ts_j \in conflist) do \]
\[ addVertext(ts_i); \]
\[ addVertext(vrtNode.ts_i); \]
\[ if (ts_j > vrtNode.ts_i) then \]
\[ addEdge(vrtNode.ts_i, ts_j); \]
\[ else \]
\[ addEdge(ts_j, vrtNode.ts_i); \]
\[ end if \]
\[ end for \]
\[ end procedure \]

\[ addVertext(ts_i) \]
This BG method is called by the multi-threaded miner. First, it 
identifies the correct location of vrtNode for transaction Ti in the BG at Line 42.
If vrtNode is not exist in BG then it creates a vrtNode node of Ti at Line 44.
Finally, It adds the vrtNode of transaction Ti in the vrtList[] of BG atomically at Line 45 with the help of compare and swap operation. If CAS fails then 
addVertext() again identifies the location of vrtNode node in the vrtList[] with 
the help of current vertex predecessor node (vrtpred) at Line 50. Eventually, 
vrtNode will be the part of BG. This method of the BG is lock-free.
Algorithm 3: addVertex(ts_i)

1. procedure addVertex(ts_i)
2. Search (vrtPred, vrtCurr) of vrtNode of ts_i in vrtList[] of BG;
3. if (vrtCurr.ts_i ≠ vrtNode.ts_i) then
4. Create new BG Node (or vrtNode) of ts_i in vrtList[];
5. /*vrtNode successfully added in vrtList[]*/
6. return(Vertext added);
7. end if
8. /*Start with current vrtPred to search the new (vrtPred, vrtCurr)*/
9. goto Line 12;
10. else
11. /*vrtNode is already exist in vrtList[]*/
12. return(Vertext already exist);
13. end if
14. end procedure

addEdge(conflictNode_1, conflictNode_2): This BG method is called by the concurrent miner. First, It identifies the location of conflictNode_2 in the egList[] of conflictNode_1 at Line 57. If egNode of conflictNode_2 is not part of BG then it creates a egNode at Line 59. Atomically, it adds an egNode in the egList[] of conflictNode_1 with the help of CAS at Line 60. After successful addition of egNode it increments the indegree atomically with the help of egNode.vrtRef pointer to maintain the dependency of it at Line 61. If CAS fails than addEdge() again identifies the location of egNode node in the egList[] with the help of current edge predecessor node (egPred) at Line 66. Eventually, egNode will be the part of BG. This method of the BG is lock-free.

Algorithm 4: addEdge(conflictNode_1, conflictNode_2)

1. procedure addEdge(conflictNode_1, conflictNode_2)
2. Search (egPred, egCurr) of conflictNode_2 in egList[] of the conflictNode_1 vertex in BG;
3. if (egCurr.ts_i ≠ conflictNode_2.ts_i) then
4. Create new BG Node (or egNode) in egList[];
5. if (egPred.egNext.CAS(egCurr, egNode)) then
6. Increment the indegree atomically of egNode.vrtRef in vrtList[];
7. /*conflictNode_2 is successfully inserted*/
8. return(Edge added);
9. end if
10. /*Start with current egPred to search the new (egPred, egCurr)*/
11. goto Line 59;
12. else
13. /*conflictNode_2 is already exist in egList[]*/
14. return(Edge already present);
15. end if
16. end procedure

localSearch(thLog_i): This BG method is called by the multi-threaded validator. Validator thread identifies the source node in threads local log thLog_i at Line 73. If it finds any source node in thLog_i then it claims that node and atomically sets its indegree field to -1 so that no other multi-threaded validator threads claim this node at Line 74. After claiming of source node it executes smart contract function (associated with the identified source node) using executeScFun() at Line 77.

globalSearch(BG): The multi-threaded validator calls this BG method. Validator thread identifies the source node (with indegree 0) in BG at Line 86. If it finds
Algorithm 5 localSearch(thLog_i)

72: procedure localSearch(thLog_i)
73:  Identify local log vertex(llVertex) with indegree 0 in thLog_i.
74:  if (llVertex.indegree.CAS(0, -1)) then
75:    sctCount ← sctCount.get&Inc();
76:    /*Concurrently execute SCT corresponds to llVertex*/.
77:    executeScFun(llVertex.scFun).
78:  return ⟨llVertex⟩;
79:  else
80:    return ⟨nil⟩;
81:  end if
82: end procedure

Algorithm 6 globalSearch(BG)

83: procedure globalSearch(BG)
84:  vrtNode ← BG.vrtHead; /*Start from the Head of the list*/
85:  /*Identify the vrtNode with indegree 0 in BG*/
86:  while (vrtNode.vrtNext ≠ BG.vrtTail) do
87:    if (vrtNode.indegree.CAS(0, -1)) then
88:      sctCount ← sctCount.get&Inc();
89:      /*Concurrently execute SCT corresponds to Node*/.
90:      executeScFun(vrtNode.scFun).
91:      return ⟨vrtNode⟩;
92:  end if
93:  vrtNode ← vrtNode.vrtNext;
94:  end while
95:  return ⟨nil⟩;
96: end procedure

remExecNode(remNode): This BG method is called by the multi-threaded validator. It atomically decrements the indegree for each conflicting node of source node with the help of vertex reference pointer (vrtRef) at Line 99. vrtRef pointer helps to decrement the indegree count of conflicting node efficiently because thread need not to travels from head of the vrtList[] to identify the vrtNode node for decrementing the indegree of it. With the help of vrtRef, it directly decrements the indegree of vrtNode. While decrementing the indegree of vrtNode if it identifies the new source node than it keeps that node information in thread local log thLog_i at Line 101.

Algorithm 7 remExecNode(remNode)

97: procedure remExecNode(remNode)
98:  while (remNode.egNext ≠ remNode.egTail) do
99:    Atomically decrement the indegree of conflicting node using remNode.vrtRef pointer.
100:   if (remNode.vrtRef.indegree == 0) then
101:     Add remNode.vrtRef node into thLog_i.
102:    end if
103:    remNode ← remNode.egNext.vrtRef;
104:  end while
105:  return ⟨nil⟩;
106: end procedure

executeScFun(scFun): It executes the SCTs concurrently without the help of concurrency control protocol. First, it identifies the smart contract function (sc-
Fun) steps and executes them one after another at Line 109. If the current step (curStep) is lookup on key $k$, then it lookup the shared data item for key $k$ from the shared memory at Line 112. If curStep is insert on key $k$ with value $v$, then it inserts the shared data item of key $k$ with value $v$ in the shared memory at Line 114. If curStep is delete on key $k$, then it deletes the shared data item of key $k$ from the shared memory at Line 116. All these curStep of scFun can run concurrently with the other validator threads because only non-conflicting transactions will execute concurrently with the help of BG given by the multi-threaded miner.

Algorithm 8 executeScFun(scFun)

107: procedure executeScFun(scFun) /*scFun is a list of steps*/
108: while (scFun.steps.hasNext()) do /*Get next step to execute*/
109: curStep = scFun.steps.next(). /*scFun is a list of steps*/
110: switch (curStep) do
111: case lookup($k$):
112: Lookup $k$ from a shared memory.
113: case insert($k$, $v$):
114: Insert $k$ in shared memory with value $v$.
115: case delete($k$):
116: Delete $k$ from shared memory.
117: case default: curStep is not lookup, insert and delete;
118: end while
119: return ⟨void⟩
120: end procedure

C.2 Data Structure of SVOSTM and MVOSTM

This subsection describes the internal details about the data structure used to store shared data items in SVOSTM and MVOSTM.

As shown in Fig. 5 (b) of Appendix A, we have used a hash-table with a fixed size of buckets, where each bucket consists of a list of corresponding shared data items. The data structure used to store the data items depends on the protocol (SVOSTM, MVOSTM).

Data Structure of SVOSTM: Fig. 7 (a) demonstrates the structure of a shared data item in SVOSTM. Each shared data item consist of eight fields ⟨Account, val, Lock, $max_L$, $max_U$, $cL_{list}$, $cU_{list}$, next⟩. Where Account is a unique identifier which represents the shared data item or key or account (e.g., A1), val field stores the value corresponding to data item. Lock is use to provide synchronization among the operations of different transactions working on same data items. Lock is acquired by the transaction before updating (inserting/deleting) the shared data item and released after the successful execution. Next two fields, i.e., $max_L$ and $max_U$, are counter variable initialize as 0. Whenever a transaction performs any operation (STM_lookup() / STM_insert() / STM_delete()) on the shared data item, they update the corresponding value of the $max_L$/$max_U$. If current value of $max_L$/$max_U$ is smaller than the timestamp of the transaction $i$ then it updates $max_L$/$max_U$ with the $i$. Otherwise, transaction with timestamp $i$ returns abort and retry again. Field $cL_{list}$ and $cU_{list}$ store the timestamp of all committed transactions (transaction ids).
who has performed the STM\_lookup() and update operations (STM\_insert() / STM\_delete()) on the shared data item respectively. These fields are used to generate the conflicts (dependencies) between the transactions. Finally, the next field is point to the next shared data item in the list of the respective bucket. The shared data item in the list of the corresponding bucket is stored in the increasing order of the keys.

To understand conflicts generation for concurrent execution of SCTs in SVOSTM, we consider three transactions $T_0$, $T_5$, and $T_7$. In SVOSTM, a transaction $T_i$ conflict with transaction $T_j$, if both are accessing a common data item $k$ and at least one of them is update operation (insert or delete). The conflicts of SVOSTM is defined in Section 3.1.

Fig. 7 (b) shows the timeline view and respective operations of these transactions. Here, $T_0$ performed insert operation on shared data item as account $A_1$ with value $v_0$ (i.e., $i_0(A_1, v_0)$), and committed successfully. Therefore, the timestamp (ts) of $T_0$ is inserted in $cU\_ist[]$ as shown in Fig. 7(a). Similarly, $T_5$, and $T_7$ are two concurrent execution performing insert (i.e., $i_5(A_1, v_5)$) and lookup (i.e., $l_7(A_1, v_5)$) operation respectively. Since $T_5$ performed insert on account $A_1$, the max$U$ field is set to 5 and later it committed successfully so its transaction id $T_5$ is inserted in $cU\_ist[]$. Further, $T_7$ performed lookup on $A_1$ so max$L$ field is set to 7 and committed successfully so its transaction id $T_7$ is inserted in $cL\_ist[]$.

Fig. 7 (c) illustrates the transactions conflict list. As shown in the concurrent execution, $T_0$ is the first transaction, so it does not find any conflict with other transactions; hence, its conflict list is empty. Later, $T_5$ committed, so $T_5$ conflict list consists of $T_0$ since both $T_0$ and $T_5$ performed update operation on $A_1$. A
transaction which performs update operation (insert or delete) conflicts with all
the transactions present in both \( cU_{list} \) and \( cL_{list} \) lists corresponding to shared
data item. At the commit time of \( T_5 \), \( cL_{list} \) was empty so, \( T_5 \) conflicts with \( T_0 \)
only. Finally, transaction \( T_7 \) committed with the lookup on \( A_1 \). A transaction
which performs lookup operation, conflicts with all the transactions present in
the \( cU_{list} \) list. So, \( T_7 \) conflict list consists all the transactions present in \( cU_{list} \)
which is \( T_0 \) and \( T_5 \). Hence, \( T_7 \) conflicts with \( T_0 \) and \( T_5 \).

**Data Structure of MVOSTM:** SVOSTM stores only one version corresponding
to each data item; however, MVOSTM maintains multiple versions. In the
proposed framework, we have a fixed number of SCTs in each block, so we do
not restrict the number of versions with each shared data item. Fig. 8 (a) shows
the data structure used to store the shared data item in MVOSTM protocol.
Here, each shared data item consists of four fields as \( \langle Account, Lock, vl, next \rangle \).
Where \( Account \), \( Lock \), and \( next \) field are same as defined earlier for SVOSTM.
A new field \( vl \) stands for version list, which maintains version created by update
operations (insert and delete) on the shared data item.

To store the versions of the shared data item, we used a list \( \langle \text{version list or } vl \rangle \).
Here, each entry of the version list consists of five fields \( \langle ts, val, max_L, rvl, vNext \rangle \).
It stores the version in increasing order of transaction’s timestamps. The first
field \( ts \) shows the timestamp of the transaction which created this version (see
Fig. 8 (a)). The next field is \( val \), which stores the value corresponding to that
version. Field \( max_L \) is used to store the maximum id/ts of the transaction that
has performed lookup on this version. A transaction \( T_i \) looks up from the ver-
sion \( j \) such that \( j \) is largest version timestamp smaller than \( i \). The \( rvl[\] \) stands
for return value list, which stores the timestamp of the committed transactions
that have lookup from a particular version. Finally, the last field \( vNext \) is used
to store a pointer to the next available version in the version list. As Fig. 8 (a)
illustrates account \( A_1 \) maintains of three versions as 0, 5, and 10. Version 0, 5,
and 10 is created by transaction \( T_0 \), \( T_5 \), and \( T_{10} \) respectively.

Consider Fig. 8 (b) to understand conflicts generation in MVOSTM, which
demonstrates the timeline view and respective operations of four transactions
\( T_0, T_5, T_7, \) and \( T_{10} \). Here, transactions \( T_0, T_5, \) and \( T_{10} \) perform insert operation
while \( T_7 \) performs a lookup on account \( A_1 \). Due to insert operation by \( T_0, T_5, \)
and \( T_{10} \) three different versions of account \( A_1 \) has been created, as shown in
Fig. 8 (a). Here, transaction \( T_0 \) executed first, so it created version 0 and then
\( T_5 \) performed insert operation \( \langle i_5(A_1, v_5) \rangle \); therefore version 5 is created. After
that \( T_7 \) performed lookup on \( A_1 \) which returns the value as \( v_5 \) (i.e., \( l_7(A_1, v_5) \)).
After the successful commit of \( T_7 \), it inserts ts 7 in \( max_L \) of version 5 as
demonstrated in Fig. 8 (a). Here, transaction \( T_{10} \) began after the beginning of \( T_7 \)
and committed before \( T_7 \) but still transaction \( T_7 \) is allowed to commit. Due to
multiple versions, \( T_7 \) finds the older value of \( A_1 \) as \( v_5 \) created by \( T_5 \) and hence
not abort; otherwise, in SVOSTM transaction \( T_7 \) has to return abort.

Fig. 8 (c) Illustrates the conflict list of transactions. Here, \( T_0 \) is the first
transaction and created version 0 of \( A_1 \), so it does not conflict with any other
transaction; hence, its conflict list is empty. Next, transaction \( T_5 \), which created
a new version of $A_1$ and committed successfully, so $T_5$ conflict list consists of $T_0$. So, while generating conflict list, for an update (insert or delete) operation on account $A_1$ transaction first checks if the $rvl[]$ list is empty for the largest version smaller than its ts (transaction ts), then if the list is empty it adds that version ts in its conflict list otherwise adds all the ts in $rvl[]$ list of that version. For a lookup operation, a transaction adds the ts/id of the version which it has looked up and also the next version in the version list (if available) in its conflict list. Next is transaction $T_{10}$ since it committed before $T_7$, so in $T_{10}$ conflict list, $T_5$ is added. The reason why only $T_5$ and not $T_7$, this is because $rvl[]$ list consist only committed transaction ts and at the time when $T_{10}$ committed $T_7$ was still live and not yet committed so $rvl[]$ of $T_5$ was empty. Finally, $T_7$ committed and as it performed a lookup on account $A_1$ from version 5, so it adds $T_5$ and the next version ts, which is $T_{10}$ in its conflict list. Hence, $T_7$ conflicts with $T_5$ and $T_{10}$.

C.3 Multi-threaded Validator

Multi-threaded validator re-executes the SCTs concurrently and deterministically rely on the BG provided by the multi-threaded miner. To access the BG, validator uses $globalSearch()$, $localSearch()$, and $remExNode()$ methods of block graph library. The descriptions of all these methods are given in Appendix C.1.

High level overview of Algorithm 9 shows the execution of SCTs by multi-threaded validator with the help of BG. First, multiple validator threads con-
currently identify the source node (indegree 0) in the BG using globalSearch() at Line 124. After identifying the source node, thread claims it (sets indegree to -1) atomically so that other multi-threaded validator threads can not claim it. Then it executes the scFun of SCT corresponding to the source node. After successful execution of scFun, it decrements the indegree count of conflicting node of source node using remExNode() at Line 125. While decrementing the indegree of conflicting node validator thread checks if it found new source node then it store that node in its thread local log thLog to execute next SCT at Line 127 efficiently.

**Algorithm 9** Multi-threaded validator(sctList, BG): $v$ threads concurrently and deterministically executes the SCTs using BG.

```plaintext
121: procedure Multi-threaded validator(sctList, BG)
122:     /*Execute until all the SCTs successfully completed*/
123:     while (sctCount < size(sctList)) do /*Initially, sctCount=0 to maintain count.*/
124:         vrtNode = globalSearch(BG); /*Identify the source node (indegree 0) in the BG*/
125:         remExNode(vrtNode); /*Decrement the indegree of conflicting nodes*/
126:         while (thLog ≠ nil) do /*Identify source node in thread local log (thLog)*/
127:             vrtNode = localSearch(thLog);
128:             remExNode(vrtNode);
129:         end while
130:     end while
131: end procedure
```

Finally, validator thread compares the $FS_m$ given by the multi-threaded miner and $FS_v$ computed by itself corresponding to each shared data item. If final state matches and proposed block reaches the global consensus, then it is added into the blockchain and respective miner awarded with the incentive.

C.4 Detection of Malicious Miner by Smart Multi-threaded Validator (SMV)

In this subsection, we propose a technique to detect malicious miner using *Smart Multi-threaded Validator*. As we have seen the functionality of multi-threaded validator in Appendix C.3 it executes the SCTs concurrently rely on the BG provided by the multi-threaded miner. Suppose the miner that produces a block is malicious and does not add some edges to the BG. This can result in the blockchain systems entering inconsistent states due to *double spend*. We motivate this with an example. Consider three bank accounts $A,B,C$ maintained on the blockchain with the current balance being $100 in each of them. Now consider two SCTs $T_i, T_j$ which are conflicting where (a) $T_i$ transfers $50 from $A$ to $B$; (b) $T_j$ transfers $60 from $A$ to $C$. Considering the initial balance of $100 in A account, both transactions cannot be executed.

If a malicious miner, say $mm$ does not add an edge between these two transactions in the BG then both these SCTs can execute concurrently by validators. Then such execution could result in the final state with the balances in the accounts $A, B, C$ as 40, 150, 160 respectively or 50, 150, 160. As we can see, neither of these final states can be obtained from any serial execution and are not correct states. Suppose the miner $mm$ stores 40, 150, 160 for $A, B, C$ in the
final state, and a validator \( v \) on concurrent execution arrives at the same state. Then, \( v \) will accept this block, which results in its state becoming inconsistent. If the majority of validators similarly accept this block, then the state of the blockchain essentially has become inconsistent. We denote this problem as edge missing BG or EMB.

**Counter Based Solution to Catch the Malicious Miner:** So, to avoid this issue, we propose a a Smart Multi-threaded Validator (SMV), which uses the concept of counters and identifies the malicious behavior of miner and rejects the proposed malicious block. Our algorithm is inspired by BTO in databases [23 Chap. 4]. SMV keeps track of each global data item that can be accessed across multiple transactions by different threads. Specifically, SMV maintains two global counters for each key of hash-table (shared data item) \( k \) - (a) \( k.gUC \) (b) \( k.gLC \). These respectively keep track of number of updates and lookups that are concurrently performed by different threads on \( k \). Both these global counters are initialized to 0.

When a SMV thread \( Th_x \) is executing an SCT \( T_i \) then SMV similarly maintains two local variables corresponding to each global data item \( k \) which is accessible only by \( Th_x \) - (c) \( k.lUC_i \) (d) \( k.lLC_i \). These respectively keep track of number of updates and lookups performed by \( Th_x \) on \( k \) while executing \( T_i \). These counters are initialized to 0 before the start of \( T_i \).

Having described the counters, we will explain the high level design of SMV approach is shown in Algorithm 10. To access the BG, validator uses the block graph library methods `globalSearch()`, `localSearch()`, and `remExecNode()` as explained in Appendix C.1. Internally they use the `executeScFun()` method to execute the smart contract function (scFun). First, it identifies the scFun steps and executes them one after another at Line 132.

If current step (curStep) is lookup (at Line 135) on shared data-item key \( k \) then it checks the \( k.gUC \) counter value. If \( k.gUC \) counter value is not equal to \( k.lLC \) at Line 136, that means another concurrent conflicting thread is also working on the same key \( k \), i.e., conflict edge among them are missing in BG given by the miner. Then SMV reports the miner is malicious.

If \( k.gUC \) counter value is zero means equal to \( k.lLC \) then it atomically increments the \( k.gLC \) counter of key \( k \) in shared memory at Line 137, so, any other concurrent conflicting thread checks the value as non zero it will detect the malicious miner. It also increments the local \( k.lLC \) value by one at Line 138. Finally, validator thread lookups the key \( k \) from the shared memory and return the value as \( v \) at Line 139.

If curStep is insert on key \( k \) with value as \( v \) (at Line 143) then before inserting the key \( k \) with value \( v \) in the shared memory it checks both global counter values \( k.gLC == k.lLC \) & \( k.gUC == k.lUC \) at Line 144. If anyone of the counter value is not equal to corresponding to the local variable value, that means another concurrent conflicting thread is also working on the same key \( k \), i.e., conflict edge among them is missing in BG given by the miner. Then SMV reports the miner is malicious.
If both global counter value is equal to corresponding local variables value, then it atomically increments the \( k.gUC \) counter of key \( k \) in shared memory at Line \[145\] so, any other concurrent conflicting thread checks the value as non zero it will detect the malicious miner. It also increments the local \( k.iUC \) value by one at Line \[146\] Finally, validator thread inserts the key \( k \) with value \( v \) in the shared memory at Line \[147\] Same things works if curStep is deleted on key \( k \) at Line \[151\].

After successful execution of each scFun, thread atomically decrements \( k.gUC, k.gLC \) by the value of \( k.iUC_i, k.iLC_i \) respectively at Line \[163\]. Then thread will reset \( k.iUC_i, k.iLC_i \) to 0. Thus with the help of \textit{counter}, validator threads are able to detect the malicious miner, and straightforward reject that block.

\textbf{Algorithm 10} \texttt{executeScFun (scFun)}: Execute the smart contract function (scFun) with atomic global lookup/update counter. Initially, lookup counter \( k.gLC \) and update counter \( k.gUC \) value is 0 corresponding to each shared data-items key \( k \). Each transaction maintains local \( k.iLC_i \) and local \( k.iUC_i \) as 0 in transaction local log, \( txLog \) corresponding to each key.

\begin{verbatim}
while (scFun.steps.hasNext()) /*Assume that scFun is a list of steps*/
curStep = scFun.steps.next(); /*Get the next step to execute*/
switch (curStep) do
  case lookup(k):
    if (k.gUC == k.lLC_i) then /*Check for update counter (uc) value*/
      Atomically increment the lookup counter, k.gLC;
      Increment k.iLC_i by 1. /*Maintain k.iLC_i in transaction local log txLog*/
    Lookup k from a shared memory;
    else
      return \langle Miner is malicious \rangle;
    end if
  case insert(k, v):
    if ((k.gLC == k.iLC_i) && (k.gUC == k.iUC_i)) then /*Check lookup/update counter value*/
      Atomically increment the update counter, k.gUC;
      Increment k.iUC_i by 1. /*Maintain k.iUC_i in transaction local log txLog*/
    Insert k in shared memory with value v;
    else
      return \langle Miner is malicious \rangle;
    end if
  case delete(k):
    if ((k.gLC == k.iLC_i) && (k.gUC == k.iUC_i)) then /*Check lookup/update counter value*/
      Atomically increment the update counter, k.gUC;
      Increment k.iUC_i by 1. /*Maintain k.iUC_i in transaction local log txLog*/
    Delete k in shared memory.
    else
      return \langle Miner is malicious \rangle;
    end if
  case default:
    curStep is not lookup, insert and delete;
    execute curStep;
end while

Atomically decrement the k.gLC and k.gUC corresponding to each shared data-item key k.
\end{verbatim}

\section{Correctness of BG, Multi-threaded Miner and Validator}

This section describes the proof of theorems stated for the correctness of BG, multi-threaded miner, and validator in Section 3. In order to define the cor-
rectness of BG, we identify the linearization points (LPs) of each method as follows:

1. $\text{addVertext}(\text{vrtNode})$: $(\text{vrtPred}.\text{vrtNext}.\text{CAS}(\text{vrtCurr}, \text{vrtNode}))$ in Line 45 is the LP point of $\text{addVertext}()$ method if $\text{vrtNode}$ is not exist in the BG. If $\text{vrtNode}$ exist in the BG then $(\text{vrtCurr}.ts_i \neq \text{vrtNode}.ts_i)$ in Line 43 is the LP point.

2. $\text{addEdge}(\text{conflictNode}_1, \text{conflictNode}_2)$: $(\text{egPred}.\text{egNext}.\text{CAS}(\text{egCurr}, \text{egNode}))$ in Line 60 is the LP point of $\text{addEdge}()$ method if $\text{egNode}$ is not exist in the BG. If $\text{egNode}$ is exist in the BG then $(\text{egCurr}.ts_i \neq \text{conflictNode}_2.ts_i)$ in Line 58 is the LP point.

3. $\text{localSearch}(\text{thLog})$: $(\text{llVertex}.\text{indegree}.\text{CAS}(0, -1))$ in Line 74 is the LP point of $\text{localSearch}()$ method.

4. $\text{globalSearch}(\text{BG})$: $(\text{vrtNode}.\text{indegree}.\text{CAS}(0, -1))$ in Line 87 is the LP point of $\text{globalSearch}()$ method.

5. $\text{remExecNode}(\text{removeNode})$: Line 99 is the LP point of $\text{remExecNode}()$ method.

**Theorem 7.** The BG captures all the dependencies between the conflicting nodes.

**Proof.** Section 3.1 represents the construction of BG by multi-threaded miner using SVOSTM and MVOSTM protocol. BG considers each committed SCT as a vertex and edges (or dependencies) depends on the used STM protocols such as SVOSTM and MVOSTM. So, the underlying STM protocol ensures that all the dependencies have been covered correctly among the conflicting nodes of BG. Hence, all the dependencies between the conflicting nodes are captured in the BG.

**Theorem 8.** A history $H_m$ generated by the multi-threaded miner with SVOSTM satisfies co-opacity.

**Proof.** Multiple miner threads execute SCTs concurrently using SVOSTM and generate a concurrent history $H_m$. The underlying SVOSTM protocol ensures the correctness of concurrent execution of $H_m$. SVOSTM proves that any history generated by it satisfies co-opacity [20]. So, implicitly SVOSTM proves that the history $H_m$ generated by multi-threaded miner using SVOSTM satisfies co-opacity.

**Theorem 9.** A history $H_m$ generated by a multi-threaded miner with MVOSTM satisfies opacity.

**Proof.** In order to achieve the greater concurrency further, a multi-threaded miner uses the MVOSTM protocol, which maintains multiple versions corresponding to each shared data-item. MVOSTM ensures the correct concurrent execution of the history $H_m$ with the equivalent serial history $S_m$. Any history generated by MVOSTM satisfies opacity [16]. So, implicitly MVOSTM proves that the history $H_m$ generated by multi-threaded miner using MVOSTM satisfies opacity.
Theorem 10. A history $H_m$ generated by the multi-threaded miner with SVOSTM and history $H_v$ generated by a multi-threaded validator are view equivalent.

Proof. Multi-threaded miner execute the SCTs concurrently using SVOSTM protocol to propose a block and generates $H_m$ along with BG. After that multi-threaded miner broadcasts $H_m$ and BG to multi-threaded validators to verify the proposed block. Multi-threaded validator applies the topological sort on BG and obtained an equivalent serial schedule $H_v$. Since BG constructed from $H_m$ while considering all the conflicts and $H_v$ obtained from the topological sort on BG. So, $H_v$ will be equivalent to $H_m$. Similarly, $H_v$ will also follow the return value from relation to $H_m$. Hence, $H_v$ is legal. Since $H_v$ and $H_m$, are equivalent to each other, and $H_v$ is legal. So, $H_m$ and $H_v$ are view equivalent.

Theorem 11. A history $H_m$ generated by the multi-threaded miner with MVOSTM and history $H_v$ generated by a multi-threaded validator are multi-version view equivalent.

Proof. Following the proof of Theorem 10, multi-threaded miner executes $H_m$ using MVOSTM and constructs the BG. MVOSTM maintains multiple-version corresponding to each shared data-item while executing the SCTs by multi-threaded miner. Later, multi-threaded validator obtained $H_v$ by applying topological sort on BG given by miner. Since, $H_v$ obtained from topological sort on BG so, $H_v$ will be equivalent to $H_m$. Similarly, BG maintains the return value from relations of $H_m$. So, from MVOSTM protocol if $T_i$ returns a value of the method for shared data-item $k$ say $rv_j(k)$ from $T_i$ in $H_m$ then $T_i$ committed before $rv_j(k)$ in $H_v$. Therefore, $H_v$ is valid. Since $H_v$ and $H_m$ are equivalent to each other and $H_v$ is valid. So, $H_m$ and $H_v$ are multi-version view equivalent.

Theorem 12. Smart Multi-threaded Validator rejects malicious blocks with BG that allow concurrent execution of dependent SCTs.

Proof. With the help of global counter Smart Multi-threaded Validator (SMV) identifies the concurrent execution of dependent SCTs at Line 136, Line 144, and Line 152 of Algorithm 10 and reject the malicious block. Detail description of SMV is available in Appendix C.4. We have tested our proposed counter-based approach with the existence of malicious block shown in Appendix E. SMV straightforward reject the malicious block and notify to the other nodes part of the network. Hence, SMV rejects malicious blocks with BG that allow concurrent execution of dependent SCTs.

E Detailed Experimental Evaluation

This section presents a detailed description of the benchmark contracts that we have considered in this paper. It also includes the additional experiments which show the performance benefits of proposed multi-threaded miner and validator over state-of-the-art miners and validators on various workloads. Along with this, we proposed smart multi-threaded validator to identify malicious miners.
Smart Contracts: Clients (possibly different) send transactions to the miners in the form of complex code known as smart contracts. It provides several complex services such as managing the system state, ensuring rules, or credentials checking of the parties involved. For better understanding, we have described Coin, Ballot, Simple Auction Smart Contracts from Solidity documentation. We consider one more smart contract as Mix Contract, which is the combination of the three contracts as mentioned above in equal proportion and seems more realistic.

1) **Coin Contract:** It is a sub-currency contract which implements simplistic form of a cryptocurrency and is used to transfer coins from one account to another account using `send()`, or used to check the account balance using `get_balance()` function. Accounts (unique addresses in Ethereum) are shared objects. A conflict will occur when two or more transaction consists of at least one common account, and one of them is updating the account balance.

Algorithm 11 shows the functionality of the coin contract, where `mint()`, `send()`, and `get_balance()` are the functions of the contract. These functions can be called by the miners or through other contracts. It initialized by the contract creator (or contract deployer) to a special public state variable `minter` (Line 165). Accounts are identified by Solidity mapping data structure essentially a (key-value) pair (Line 167), where a key is the unique Ethereum address and value is unsigned integer depicts the coins (or balance) in respective account. Initially, the contract deployer (aka `minter`) creates new coins and allocate it to each receiver (Line 173). Further, `send()` function is used to transfer the coin from the sender account to the receiver account. The function ensures that the sender has sufficient balance in his account (Line 178). If sufficient balance found in the sender’s account, the coin transferred from the sender account to the receiver account. By calling `get_balance()`, anyone can query the specific account balance (Line 183).

2) **Ballot Contract:** This contract is used to organize electronic voting where voters and proposals are the shared objects and stored at unique Ethereum addresses. At the beginning of voting, the chairman of the ballot gives rights to voters to vote. Later, voters either delegate their vote to other voter using `delegate()` or directly vote to specific proposal using `vote()`. Voters are allowed to delegate or vote only once per ballot. A conflict will occur when two or more voters vote for the same proposal, or they delegate their votes to the same voter simultaneously.

3) **Simple Auction Contract:** In this contract, an auction is conducted where a bidder places their bids. Here bidders, `maxBid`, `maxBidder`, and auction end time are the shared object which can be accessed by multiple threads. The auction will end when the bidding period (or end time) of the auction is over. The auction end time is initialized at the beginning by the auction master. A `bid()` function is used to bid the amount by a bidder for the auction. In the end, the bidder with the highest bid amount will be the winner, and all other bidders amount is then returned to them using `withdraw()`. A conflict will occur when more than two bidders try to bid using `bidPlusOne()` at the same time.
Algorithm 11 Coin(): A sub-currency contract used to depict the simplest form of a cryptocurrency.

```
procedure Coin()
   address public minter;/*Minter is a unique public address*/
   /*Map (key-value) pair of hash-table as (address-balance)*/
   mapping(address => uint) balances.
Constructor() public
minter = msg.sender. /*Set the sender as minter*/
function mint(address receiver, uint amount )
   if (msg.sender == minter) then
      /*Initially, add the balance into receiver account*/
      balances[receiver] += amount.
   end if
end function
function send(address receiver, uint amount)
   /*Sender don’t have sufficient balance*/
   if (balances[msg.sender] < amount) then return (fail);
   end if
   balances[msg.sender] -= amount;
   balances[receiver] += amount;
end function
function get_balance(address account)
   return (balance);
end function
end procedure
```

(4) Mix Contract: In this contract, aforementioned smart contracts are executed simultaneously. This contract is designed to show real-time scenarios in which a block consists of SCTs from different contracts. For the experiment, we combined SCTs for three contracts in a block.

Performance Analysis: To analyze the proposed approach further, we show the performance analysis on remaining benchmark contracts and workloads. Additionally, we consider one more workload W3, in which the number of shared objects (data-items) vary from 100 to 600, while threads, SCTs, and hash-table size are fixed to 50, 100, and 30, respectively. For W3, with the increase in the number of shared objects, contention will decrease.

In Fig. 9 to Fig. 11 numbering (a), (b), (c) show the multi-threaded miner speedup over serial miner on W1, W2, and W3 for coin, ballot, and auction contract respectively. Further, (d), (e), (f) shows the smart multi-threaded validator speedup over serial validator on W1, W2, and W3 for the coin, ballot, and auction contract respectively. It shows that the speedup decreases for multi-threaded miner on W1; however, it increases on W2 on all benchmark contracts. The observation for W1 and W2 are the same as explained in Section 4. Finally, Fig. 12 (a) and Fig. 12 (b) shows the speedup for multi-threaded miner and SMV for mix contract on workload W3.

For W3, as shown in Fig. 9 (c), Fig. 10 (c), Fig. 11 (c), and Fig. 12 (a) the speedup increase for multi-threaded miner with increase in shared objects (contention decreases). However in mix contract (as shown in Fig. 12 (a)) small decrements for BTO and MVTO miner can be observed. Also, static bin miner is performing worse than serial due to the overhead of static conflict prediction before executing SCTs speculatively. Similarly Fig. 9 (f), Fig. 10 (f), Fig. 11 (f),
and Fig. 12 (b) shows the speedup achieve by SMV over serial validator on W3. The speedup of bin-based SMV is less than STM validator. Thus for the better visualization, we have shown speedup for STM validator on $y_1$ axis whereas for bin-based SMV on $y_2$ axis. As we can observe, MVOSTM SMV outperforms all other validators; however, performance decreases with increasing shared objects.

**Dependencies in the BG:** Fig. 13 to Fig. 15 shows the average dependencies in the Block Graph (BG) generated by STM based multi-threaded miners for the coin, ballot, and auction contract on all workloads. While Fig. 16(a) shows the average number of dependencies in the BG for mix contract on W3. There is no BG in bin-based static bin and speculative bin miner; instead, there is a sequential and concurrent bin. So from block size consideration, bin-based approach is efficient, though, from validator speedup consideration, STM based approach is better as shown in all smart multi-threaded validators figures.

As shown in figures for W1 with the increase in SCTs, the number of dependencies increases in BG. However, for W2, there is no much variation since we fixed the number of SCTs to 100 in W2. Moreover, the analysis of W3 is quite impressive. Here for the ballot and mix contracts with the increase in shared data items, the dependencies in BG increases for BTO and MVTO. However, it decreases for SVOSTM and MVOSTM as shown in Fig. 14 (c). Also, for coin contract, dependencies in BG decreases with an increase in shared data-item. In the Auction contract, it depends on the highest bid; if the highest bid is bided in the beginning, then there will be least dependencies in BG.

The average speedup (averaged across the workloads) achieved by the multi-threaded miners and smart multi-threaded validators on workload W1, W2, and W3 on all benchmarks are shown in Table 1 and Table 2 respectively. Note that the average speedup result shown in Section 4 for mix contract is averaged on workload W1 and W2.

Table 1: Overall Average Speedup on all Workloads by Multi-threaded Miner over Serial

| Contract | BTO Miner | MVTO Miner | SVOSTM Miner | MVOSTM Miner | SpecBin Miner | Static Bin Miner
|----------|-----------|------------|--------------|--------------|---------------|------------------|
| Coin     | 1.596     | 1.959      | 4.391        | 5.572        | 1.279         | 6.689            |
| Ballot   | 0.960     | 1.065      | 2.229        | 2.431        | 1.175         | 2.233            |
| Auction  | 2.305     | 2.675      | 4.456        | 4.885        | 3.241         | 4.232            |
| Mix      | 1.966     | 2.119      | 4.425        | 4.896        | 1.102         | 3.986            |
| **Total Avg. Speedup** | **1.61** | **1.95** | **3.38** | **3.95** | **1.27** | **3.56** |

Table 2: Overall Average Speedup on all Workloads by SMV over Serial

| Contract | Smart Multi-threaded Validator (SMV) | Smart Multi-threaded Validator (SMV) | Smart Multi-threaded Validator (SMV) | Smart Multi-threaded Validator (SMV) |
|----------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| Coin     | 26.576                              | 28.635                              | 30.344                              | 32.864                              |
| Ballot   | 26.037                              | 28.333                              | 33.695                              | 36.698                              |
| Auction  | 27.772                              | 31.781                              | 29.803                              | 32.709                              |
| Mix      | 36.279                              | 39.304                              | 42.139                              | 45.332                              |
| **Total Avg. Speedup** | **29.17** | **32.01** | **34.00** | **36.90** | **4.46** | **5.26** |
Fig. 9: Multi-threaded Miner and Smart Multi-threaded Validator Speedup Over Serial Miner and Validator Across all Workloads for Coin Contract

Fig. 10: Multi-threaded Miner and Smart Multi-threaded Validator Speedup Over Serial Miner and Validator Across all Workloads for Ballot Contract
Fig. 11: Multi-threaded Miner and Smart Multi-threaded Validator Speedup Over Serial Miner and Validator Across all Workloads for Auction Contract

Fig. 12: Multi-threaded Miner and Smart Multi-threaded Validator Speedup Over Serial Miner and Validator on W3 for Mix Contract

Fig. 13: Average Number of Dependencies in Block Graph for Coin Contract
Experiments on Malicious Miner: A multi-threaded validator deterministically executes the SCTs rely on the BG provided by the miner in the block. However, what if a miner is malicious and embeds an incorrect BG? To answer this question, we have done experiments for the malicious miner. As explained earlier, we proposed a Smart Multi-threaded Validator (SMV) to prevent such malicious activity due to concurrent execution of SCTs of the block. This experiment shows how many validators (NonSMV) accept malicious block proposed by a malicious miner.
To obtain the malicious miner activity, we generate two SCTs of double-spending (explained in Appendix C.4) in coin contract and ballot contract (double voting: a voter votes two different proposals with one voting right). After that, malicious miner added such SCTs into the block, manipulate the final state accordingly, but did not add the respective dependencies in BG, i.e., for these two SCTs, indegrees will be 0. Finally, malicious miner broadcast the malicious block in the network. Then multi-threaded NonSMV validators re-executes the SCTs concurrently using BG provided by the malicious miner. However, the validators may execute double-spending SCTs concurrently and compute the same final state as provided by the malicious miner. So, some of the validators accept the malicious block. If they reach a consensus, then they will add this malicious block into the blockchain. It may cause a severe issue in the blockchain.

Fig. 3, Fig. 16 (b), Fig. 17, and Fig. 18 demonstrates the average percentage of validators accepting a malicious block on different workloads and benchmark contracts. Here, we consider 50 validators and run the experiments for the Coin, Ballot, and Mix contract. So, we can conclude that if the malicious miner is present in the network, then some validators may agree on the malicious block, and harm the blockchain. Therefore, we should ensure the rejection of such a malicious block in the blockchain. To address this issue, we proposed Smart Multi-threaded Validator (describe in Appendix C.4), which always detects the malicious block at the time of concurrent execution of malicious SCTs (double-spending and double voting) with the help of counter and straightforward reject that block. Analysis of SMVs is presented for mix contract in Section 4 and other contracts at the beginning of this section.

So, the next obvious question is, how much extra time does SMVs is taking to serve the purpose of identifying the malicious miner over NonSMVs? We observe that the counter-based multi-threaded validator (i.e., Smart Multi-threaded Validator (SMV)) approach is giving a bit less speedup than without counter-based multi-threaded validator (i.e., NonSMV) however this decrement in speedup is very low on considered workloads. Instead of small decrement in speedup, it is evident to use counter-based multi-threaded validators (SMVs) to preserve the correctness of the blockchain.
Fig. 17: Percentage of Average Multi-threaded Validator (NonSMV) Accepted a Malicious Block for Coin Contract

Fig. 18: Percentage of Average Multi-threaded Validator (NonSMV) Accepted a Malicious Block for Ballot Contract

Experiments on Block Graph Size: We also measure the additional space required to append the BG into the block. In Ethereum and Bitcoin average block size is ≈ 20.98 [4] and ≈ 1123.34 KB [1] respectively for the interval of 1st Jan. 2019 to 8th March 2020, which is keep on increasing every year. The average number of transactions in a block of Ethereum is ≈ 100 [4]. So, on an average, each transaction requires 0.2 KB (≈ 200 bytes) in Ethereum. Based on this simple calculation, we have computed block size with an increase in SCTs per block for workload W1. To compute the block size Equation 1 is used.

\[ B = 200 \times N_{SCTs} \]  

(1)

Where, \( B \) is block size in bytes, \( N_{SCTs} \), number of smart contract transactions (SCTs) in block, and 200 is the average size of an SCT in bytes.

We use adjacency list to maintain the Block Graph \( BG(V, E) \) inspired from [7,8]. Here \( V \) is the set of vertices \( (\text{vrtNodes}) \) is stored as a vertex list, \( \text{vrtList} \). Similarly \( E \) is the set of Edges \( (\text{egNodes}) \) is stored as edge list \( (\text{egList} \text{ or conflict list}) \) as shown in the Fig. 6 (a) of Appendix C.1. Both \( \text{vrtList} \) and \( \text{egList} \) store between the two sentinel nodes \( \text{Head}(−\infty) \) and \( \text{Tail}(+\infty) \). Each \( \text{vrtNode} \) maintains a tuple: \( \langle ts, scFun, indegree, egNext, vrtNext \rangle \). Here, \( ts \) (an integer) is the
unique timestamp $i$ of the transaction $T_i$ to which this node corresponds to. $sc$-Fun (an integer) is the ID of smart contract function executed by the transaction $T_i$ which is stored in virtNode. The number of incoming edges to the transaction $T_i$, i.e. the number of transactions on which $T_i$ depends, is captured by indegree (an integer). Field egNext (an address) and virtNext (an address) points the next egNode and virtNode in the egList and virtList respectively. So a vertex node $V_s$ size is 28 bytes in the experimental system, which is sum of the size of 3 integer variables and 2 pointers.

Each egNode of $T_i$ similarly maintains a tuple: $\langle ts, \text{virtRef}, \text{egNext} \rangle$. Here, $ts$ (an integer) stores the unique timestamp $j$ of $T_j$ which has an edge coming from $T_i$ in the graph. BG maintains the conflict edge from lower timestamp transaction to higher timestamp transaction. This ensures that the block graph is acyclic. The egNodes in egList are stored in increasing order of the $ts$. Field virtRef (an address) is a vertex reference pointer which points to its own virtNode present in the virtList. This reference pointer helps to maintain the indegree count of virtNode efficiently. The egNext (an address) is a pointer to next edge node, so edge node $E_s$ requires a total of 20 bytes in the experimental system.

The experimental results on the percentage of additional space required to store BG in the block are shown in Fig. 19 to Fig. 22 for all benchmark contracts and workloads. The size of BG ($\beta$) in bytes is computed using Equation 2, while to compute the percentage of additional space ($\beta_p$) required to store BG in the block is calculated using Equation 3.

$$\beta = (V_s \times N_{SCTs}) + (E_s \times M_e) \quad (2)$$

Where, $\beta$ is size of Block Graph (BG) in bytes, $V_s$ is size of a vertex node of BG in bytes, $N_{SCTs}$ are number of smart contract transactions (SCTs) in a block, $E_s$ is size of a edge node in bytes of BG, and $M_e$ is number of edges in BG.

$$\beta_p = (\beta \times 100)/B \quad (3)$$

As shown in Fig. 19 to Fig. 22, it can be observed that with an increase in the number of dependencies, the space requirements also increase. The number of dependencies in the Ballot contract (Fig. 14 (a)) for $W_1$ is higher compared to other contracts, so the space requirement is also high. In all the figures, the space requirements of BG by MVOSTM, SVOSTM is smaller than MVTO and BTO miner. The average space required for BG in % concerning block size is 14.24%, 14.95%, 21.20%, and 22.70% by MVOSTM, SVOSTM, MVTO, and BTO miner, respectively on $W_1$ (As shown in Table 3). Since the number of dependencies in BG developed by MVOSTM is smaller than BG generated by other STM protocols, so it requires less space to store BG. In the future, we are planning to reduce space further to store the BG in the block by keeping the optimized or compressed BG.
Table 3: On W1 Average % Increase in Block Size due to BG in Ethereum

| Contract  | BTO Miner | MVTO Miner | SVOSTM Miner | MVOSTM Miner |
|-----------|-----------|------------|--------------|--------------|
| Coin      | 14.225    | 13.702     | 13.712       | 13.220       |
| Ballot    | 44.542    | 40.633     | 17.377       | 16.073       |
| Auction   | 13.811    | 13.427     | 13.534       | 13.392       |
| Mix       | 18.238    | 17.043     | 15.180       | 14.264       |
| Total Avg. Change | 22.70 | 21.20 | 14.95 | 14.24 |

Fig. 19: Percentage of Additional Space Required to Store Block Graph (BG) in Ethereum Block for Coin Contract

Fig. 20: Percentage of Additional Space Required to Store Block Graph (BG) in Ethereum Block for Ballot Contract
Fig. 21: Percentage of Additional Space Required to Store Block Graph (BG) in Ethereum Block for Auction Contract

Fig. 22: Percentage of Additional Space Required to Store Block Graph (BG) in Ethereum Block for Mix Contract

Performance Analysis of Decentralized NonSMV Validator: Fig. 23 and Fig. 24 show the performance of Decentralized NonSMV validator. Here we can observe that average speedup achieved by decentralized NonSMV validator is slightly better than SMV including bin-based and fork-join validators. However, NonSMV validators are prone to accepting a malicious block (the acceptance of malicious block is shown in Fig. 3, Fig. 17, and Fig. 18).
Performance Analysis of Fork-join SMV Validator: Fig. 25 and Fig. 26 show the performance of the fork-join validator [7,9]. Here we can observe that the average speedup achieved by the fork-join validator is very less compared to other SMV. The reason for low speedups by multi-threaded fork-join validators is possibly due to the working of the master thread, which becomes slow to allocate the SCTs to the slave threads and hence becomes the bottleneck.
Fig. 25: Multi-threaded Fork-join Validator Speedup over Serial Validator for Coin and Ballot Contract

Fig. 26: Multi-threaded Fork-join Validator Speedup over Serial Validator for Auction and Mix Contract
Time Taken by Multi-threaded Miner and SMV on Workload-1 Benchmark Contracts: For the better clarity, we present the actual time taken by the miner and validators on W1. Table 4 to Table 7 show the time taken by the miners for all the four benchmark contracts, while Table 8 to Table 11 show the time taken by the validators. The time shown in the table is in the microsecond (µs) and averaged over 26 runs where the first run is considered as warm-up run and discarded.

Table 4: Multi-threaded v/s Serial Miner Time on W1 for Coin Contract (in µs)

| # SCTs | Serial | BTO Miner | MVTO Miner | SVOSTM Miner | MVOSTM Miner | StaticBin Miner | SpecBin Miner |
|--------|--------|-----------|------------|--------------|--------------|----------------|---------------|
| 50     | 150.65 | 68.1112   | 50.3176    | 22.8232      | 14.9664      | 86.1328        | 12.7848       |
| 100    | 272.71 | 146.647   | 123.096    | 44.5568      | 37.364       | 159.595        | 33.1864       |
| 150    | 379.18 | 262.93    | 233.871    | 76.3768      | 55.384       | 271.694        | 72.2712       |
| 200    | 487.52 | 352.554   | 297.997    | 166.834      | 97.5192      | 527.921        | 72.2712       |
| 250    | 587.21 | 450.446   | 390.727    | 208.166      | 122.653      | 982.792        | 91.472        |
| 300    | 696.44 | 534.891   | 444.716    | 261.277      | 173.087      | 982.792        | 150.039       |

Table 5: Multi-threaded v/s Serial Miner Time on W1 for Ballot Contract (in µs)

| # SCTs | Serial | BTO Miner | MVTO Miner | SVOSTM Miner | MVOSTM Miner | StaticBin Miner | SpecBin Miner |
|--------|--------|-----------|------------|--------------|--------------|----------------|---------------|
| 50     | 159.68 | 118.534   | 105.431    | 61.324       | 44.068       | 90.9888        | 35.4624       |
| 100    | 270.72 | 228.384   | 200.039    | 95.8848      | 86.2352      | 189.968        | 98.7128       |
| 150    | 426.24 | 425.461   | 357.151    | 171.871      | 162.211      | 424.124        | 310.022       |
| 200    | 524.64 | 656.821   | 723.909    | 264.23       | 274.261      | 674.95         | 423.346       |
| 250    | 633.32 | 897.225   | 919.69     | 338.452      | 410.184      | 846.106        | 737.346       |
| 300    | 775.96 | 955.438   | 1033.51    | 428.401      | 519.42       | 990.503        | 584.247       |

Table 6: Multi-threaded v/s Serial Miner Time on W1 for Auction Contract (in µs)

| # SCTs | Serial | BTO Miner | MVTO Miner | SVOSTM Miner | MVOSTM Miner | StaticBin Miner | SpecBin Miner |
|--------|--------|-----------|------------|--------------|--------------|----------------|---------------|
| 50     | 106.8  | 18.0744   | 15.5328    | 14.3912      | 12.9552      | 45.8104        | 22.0304       |
| 100    | 239.04 | 86.7432   | 70.0488    | 45.6224      | 42.373       | 113.296        | 88.044        |
| 150    | 341.28 | 142.105   | 135.961    | 93.825       | 93.825       | 218.606        | 170.866       |
| 200    | 441.04 | 217.049   | 191.782    | 177.425      | 177.425      | 410.184        | 330.482       |
| 250    | 541.32 | 315.15    | 269.503    | 227.241      | 227.241      | 686.099        | 431.722       |
| 300    | 634.24 | 593.994   | 541.058    | 381.154      | 370.016      | 756.739        | 479.808       |

Table 7: Multi-threaded v/s Serial Miner Time on W1 for Mix Contract (in µs)

| # SCTs | Serial | BTO Miner | MVTO Miner | SVOSTM Miner | MVOSTM Miner | StaticBin Miner | SpecBin Miner |
|--------|--------|-----------|------------|--------------|--------------|----------------|---------------|
| 50     | 101.96 | 44.8776   | 31.352     | 21.5408      | 20.0272      | 69.6816        | 19.3464       |
| 100    | 192.2  | 92.4168   | 66.972     | 44.2504      | 38.2416      | 140.606        | 52.9          |
| 150    | 236.03 | 182.362   | 155.381    | 66.3584      | 56.3176      | 240.262        | 70.8404       |
| 200    | 318.01 | 296.35    | 221.89     | 94.5632      | 82.5976      | 430.153        | 97.808        |
| 250    | 421.32 | 418.263   | 319.533    | 141.498      | 123.091      | 421.934        | 172.095       |
| 300    | 515.56 | 605.805   | 477.872    | 197.78       | 152.14       | 615.446        | 212.537       |
### Table 8: SMV v/s Serial Validator Time on W1 for Coin Contract (in µs)

| # SCTs | Serial | BTO SMV | MVTO SMV | SVOSTM SMV | MVOSTM SMV | StaticBin SMV | SpecBin SMV |
|--------|--------|---------|----------|------------|------------|---------------|-------------|
| 50     | 141.63 | 4.9848  | 4.7008   | 4.5784     | 4.6784     | 22.4432       | 21.5008     |
| 100    | 263.4  | 8.936   | 8.1272   | 7.2986     | 6.8432     | 47.392        | 26.2848     |
| 150    | 399.84 | 12.7562 | 11.5888  | 10.7256    | 9.6768     | 74.6168       | 57.9472     |
| 200    | 438.83 | 14.7144 | 13.1834  | 12.6072    | 11.9136    | 112.474       | 78.2856     |
| 250    | 562.24 | 19.4272 | 18.6376  | 16.6352    | 16.1696    | 152.474       | 87.956      |
| 300    | 664.305| 23.658  | 22.439   | 22.3       | 20.0271    | 145.223       | 127.9308    |

### Table 9: SMV v/s Serial Validator Time on W1 for Ballot Contract (in µs)

| # SCTs | Serial | BTO SMV | MVTO SMV | SVOSTM SMV | MVOSTM SMV | StaticBin SMV | SpecBin SMV |
|--------|--------|---------|----------|------------|------------|---------------|-------------|
| 50     | 156.24 | 5.2896  | 5.0248   | 4.2376     | 4.0416     | 26.564        | 30.776      |
| 100    | 289.8  | 10.484  | 9.8752   | 7.5848     | 6.3024     | 68.3032       | 63.1488     |
| 150    | 425.2  | 13.4    | 12.792   | 9.7368     | 9.62       | 112.822       | 120.214     |
| 200    | 516.84 | 16.2848 | 15.3904  | 13.1784    | 12.4192    | 155.313       | 147.697     |
| 250    | 627.2  | 21.5944 | 19.6976  | 16.4096    | 15.3408    | 254.764       | 232.866     |
| 300    | 757.8  | 25.1328 | 23.8872  | 19.332     | 19.0984    | 293.702       | 261.422     |

### Table 10: SMV v/s Serial Validator Time on W1 for Auction Contract (in µs)

| # SCTs | Serial | BTO SMV | MVTO SMV | SVOSTM SMV | MVOSTM SMV | StaticBin SMV | SpecBin SMV |
|--------|--------|---------|----------|------------|------------|---------------|-------------|
| 50     | 103.4  | 3.2096  | 3.112    | 3.1424     | 3.1224     | 10.4136       | 8.6112      |
| 100    | 190.08 | 6.1088  | 5.2912   | 5.5068     | 5.2752     | 33.0736       | 30.668      |
| 150    | 280.6  | 9.916   | 8.0408   | 8.4896     | 7.9392     | 55.9136       | 48.576      |
| 200    | 406.48 | 12.4556 | 11.0552  | 11.524     | 10.8424    | 115.154       | 98.404      |
| 250    | 531.8  | 15.9936 | 14.2556  | 15.4562    | 13.8392    | 150.586       | 94.8384     |
| 300    | 606.4  | 19.048  | 16.0512  | 17.1448    | 15.1544    | 168.833       | 118.31      |

### Table 11: SMV v/s Serial Validator Time on W1 for Mix Contract (in µs)

| # SCTs | Serial | BTO SMV | MVTO SMV | SVOSTM SMV | MVOSTM SMV | StaticBin SMV | SpecBin SMV |
|--------|--------|---------|----------|------------|------------|---------------|-------------|
| 50     | 2.1936 | 2.0072  | 1.8232   | 1.7088     | 1.4024     | 16.3112       | 8.6112      |
| 100    | 4.1016 | 4.088   | 3.6      | 3.4512     | 3.1432     | 31.042        | 30.668      |
| 150    | 5.6902 | 4.812   | 4.704    | 4.4384     | 4.2916     | 42.975        | 38.576      |
| 200    | 7.3952 | 6.704   | 6.224    | 6.0672     | 5.7756     | 75.0021       | 58.404      |
| 250    | 9.4328 | 8.6696  | 8.208    | 7.2904     | 7.9208     | 93.9526       | 94.8384     |
| 300    | 11.6916| 10.6342 | 9.3392   | 8.9192     | 8.164      | 116.43        | 118.31      |